

# IsarMathLib

Slawomir Kolodynski

February 23, 2013

## Abstract

This is the proof document of the IsarMathLib project version 1.8.0.  
IsarMathLib is a library of formalized mathematics for Isabelle 2013  
(ZF logic).

## Contents

<b>1</b>	<b>Introduction.thy</b>	<b>8</b>
1.1	How to read IsarMathLib proofs - a tutorial . . . . .	8
1.2	Overview of the project . . . . .	10
<b>2</b>	<b>Order_ZF.thy</b>	<b>13</b>
2.1	Definitions . . . . .	13
2.2	Intervals . . . . .	16
2.3	Bounded sets . . . . .	17
<b>3</b>	<b>Order_ZF_1a.thy</b>	<b>25</b>
3.1	Maximum and minimum of a set . . . . .	25
3.2	Supremum and Infimum . . . . .	32
3.3	Strict versions of order relations . . . . .	35
<b>4</b>	<b>NatOrder_ZF.thy</b>	<b>39</b>
4.1	Order on natural numbers . . . . .	39
<b>5</b>	<b>func_ZF.thy</b>	<b>41</b>
5.1	Lifting operations to a function space . . . . .	41
5.2	Associative and commutative operations . . . . .	43
5.3	Restricting operations . . . . .	45
5.4	Compositions . . . . .	48
5.5	Identity function . . . . .	49
5.6	Lifting to subsets . . . . .	51
5.7	Distributive operations . . . . .	56

<b>6</b>	<b>func_ZF_1.thy</b>	<b>58</b>
6.1	Functions and order . . . . .	58
6.2	Projections in cartesian products . . . . .	62
6.3	Induced relations and order isomorphisms . . . . .	63
<b>7</b>	<b>Generalization_ZF.thy</b>	<b>71</b>
7.1	Generalization situation . . . . .	71
7.2	Arbitrary generalizations . . . . .	72
7.3	ZF generalization . . . . .	73
<b>8</b>	<b>NatGenIntEx_ZF.thy</b>	<b>77</b>
<b>9</b>	<b>Finite_ZF.thy</b>	<b>78</b>
9.1	Definition and basic properties of finite powerset . . . . .	78
<b>10</b>	<b>Finite1.thy</b>	<b>88</b>
10.1	Finite powerset . . . . .	88
10.2	Finite range functions . . . . .	95
<b>11</b>	<b>Finite_ZF_1.thy</b>	<b>97</b>
11.1	Finite vs. bounded sets . . . . .	97
<b>12</b>	<b>FinOrd_ZF.thy</b>	<b>101</b>
12.1	Finite vs. bounded sets . . . . .	101
12.2	Order isomorphisms of finite sets . . . . .	102
<b>13</b>	<b>EquivClass1.thy</b>	<b>109</b>
13.1	Congruent functions and projections on the quotient . . . . .	109
13.2	Projecting commutative, associative and distributive operations. . . . .	115
13.3	Saturated sets . . . . .	117
<b>14</b>	<b>Fold_ZF.thy</b>	<b>121</b>
14.1	Folding in ZF . . . . .	121
<b>15</b>	<b>Partitions_ZF.thy</b>	<b>126</b>
15.1	Bisections . . . . .	126
15.2	Partitions . . . . .	128
<b>16</b>	<b>Enumeration_ZF.thy</b>	<b>131</b>
16.1	Enumerations: definition and notation . . . . .	131
16.2	Properties of enumerations . . . . .	132

<b>17 Semigroup_ZF.thy</b>	<b>135</b>
17.1 Products of sequences of semigroup elements . . . . .	135
17.2 Products over sets of indices . . . . .	139
17.3 Commutative semigroups . . . . .	142
<b>18 Semigroup_ZF.thy</b>	<b>155</b>
18.1 Sum of a function over a set . . . . .	155
<b>19 Monoid_ZF.thy</b>	<b>159</b>
19.1 Definition and basic properties . . . . .	159
<b>20 Group_ZF.thy</b>	<b>164</b>
20.1 Definition and basic properties of groups . . . . .	164
20.2 Subgroups . . . . .	174
<b>21 Group_ZF_1.thy</b>	<b>181</b>
21.1 Translations . . . . .	181
21.2 Odd functions . . . . .	187
<b>22 Group_ZF_1b.thy</b>	<b>189</b>
22.1 An alternative definition of group . . . . .	189
<b>23 AbelianGroup_ZF.thy</b>	<b>192</b>
23.1 Rearrangement formulae . . . . .	192
<b>24 Group_ZF_2.thy</b>	<b>205</b>
24.1 Lifting groups to function spaces . . . . .	205
24.2 Equivalence relations on groups . . . . .	210
24.3 Normal subgroups and quotient groups . . . . .	213
24.4 Function spaces as monoids . . . . .	218
<b>25 Group_ZF_3.thy</b>	<b>219</b>
25.1 Group valued finite range functions . . . . .	219
25.2 Almost homomorphisms . . . . .	221
25.3 The classes of almost homomorphisms . . . . .	229
25.4 Compositions of almost homomorphisms . . . . .	232
25.5 Shifting almost homomorphisms . . . . .	241
<b>26 DirectProduct_ZF.thy</b>	<b>243</b>
26.1 Definition . . . . .	243
26.2 Associative and commutative operations . . . . .	244
<b>27 OrderedGroup_ZF.thy</b>	<b>245</b>
27.1 Ordered groups . . . . .	245
27.2 Inequalities . . . . .	251

27.3	The set of positive elements . . . . .	263
27.4	Intervals and bounded sets . . . . .	270
<b>28</b>	<b>OrderedGroup_ZF_1.thy</b>	<b>277</b>
28.1	Absolute value and the triangle inequality . . . . .	277
28.2	Maximum absolute value of a set . . . . .	289
28.3	Alternative definitions . . . . .	291
28.4	Odd Extensions . . . . .	294
28.5	Functions with infinite limits . . . . .	296
<b>29</b>	<b>Ring_ZF.thy</b>	<b>301</b>
29.1	Definition and basic properties . . . . .	301
29.2	Rearrangement lemmas . . . . .	308
<b>30</b>	<b>Ring_ZF_1.thy</b>	<b>312</b>
30.1	The ring of classes of almost homomorphisms . . . . .	312
<b>31</b>	<b>OrderedRing_ZF.thy</b>	<b>315</b>
31.1	Definition and notation . . . . .	315
31.2	Absolute value for ordered rings . . . . .	323
31.3	Positivity in ordered rings . . . . .	325
<b>32</b>	<b>Field_ZF.thy</b>	<b>333</b>
32.1	Definition and basic properties . . . . .	333
32.2	Equations and identities . . . . .	336
32.3	$1/0=0$ . . . . .	337
<b>33</b>	<b>OrderedField_ZF.thy</b>	<b>339</b>
33.1	Definition and basic properties . . . . .	339
33.2	Inequalities . . . . .	342
33.3	Definition of real numbers . . . . .	346
<b>34</b>	<b>Int_ZF.thy</b>	<b>347</b>
34.1	Addition and multiplication as ZF-functions. . . . .	347
34.2	Integers as an ordered group . . . . .	354
34.3	Induction on integers. . . . .	366
34.4	Bounded vs. finite subsets of integers . . . . .	369
<b>35</b>	<b>Int_ZF_1.thy</b>	<b>374</b>
35.1	Integers as a ring . . . . .	374
35.2	Rearrangement lemmas . . . . .	376
35.3	Integers as an ordered ring . . . . .	383
35.4	Maximum and minimum of a set of integers . . . . .	393
35.5	The set of nonnegative integers . . . . .	397
35.6	Functions with infinite limits . . . . .	404

35.7	Miscellaneous . . . . .	409
<b>36</b>	<b>IntDiv_ZF_IML.thy</b>	<b>411</b>
36.1	Quotient and reminder . . . . .	411
<b>37</b>	<b>Int_ZF_2.thy</b>	<b>414</b>
37.1	Slopes . . . . .	414
37.2	Composing slopes . . . . .	436
<b>38</b>	<b>Int_ZF_3.thy</b>	<b>443</b>
38.1	Positive slopes . . . . .	443
38.2	Inverting slopes . . . . .	454
38.3	Completeness . . . . .	462
<b>39</b>	<b>Real_ZF.thy</b>	<b>469</b>
39.1	The definition of real numbers . . . . .	469
<b>40</b>	<b>Real_ZF_1.thy</b>	<b>478</b>
40.1	Definitions and notation . . . . .	478
40.2	Multiplication of real numbers . . . . .	480
40.3	The order on reals . . . . .	484
40.4	Inverting reals . . . . .	493
40.5	Completeness . . . . .	496
<b>41</b>	<b>Complex_ZF.thy</b>	<b>517</b>
41.1	From complete ordered fields to complex numbers . . . . .	517
41.2	Axioms of complex numbers . . . . .	521
<b>42</b>	<b>Topology_ZF.thy</b>	<b>534</b>
42.1	Basic definitions and properties . . . . .	534
42.2	Interior of a set . . . . .	538
42.3	Closed sets, closure, boundary. . . . .	539
<b>43</b>	<b>Topology_ZF_1.thy</b>	<b>545</b>
43.1	Separation axioms. . . . .	545
43.2	Bases and subbases. . . . .	546
43.3	Product topology . . . . .	550
<b>44</b>	<b>Topology_ZF_1b.thy</b>	<b>556</b>
44.1	Compact sets are closed - no need for AC . . . . .	556
<b>45</b>	<b>Topology_ZF_2.thy</b>	<b>559</b>
45.1	Continuous functions. . . . .	559
45.2	Homeomorphisms . . . . .	564
45.3	Topologies induced by mappings . . . . .	566

45.4	Partial functions and continuity . . . . .	568
45.5	Product topology and continuity . . . . .	571
45.6	Pasting lemma . . . . .	573
<b>46</b>	<b>Topology_ZF_3.thy</b>	<b>577</b>
46.1	The base of the product topology . . . . .	577
46.2	Finite product of topologies . . . . .	579
<b>47</b>	<b>Topology_ZF_4.thy</b>	<b>589</b>
47.1	Convergence on topological spaces . . . . .	589
47.1.1	Nets . . . . .	589
47.1.2	Filters . . . . .	592
47.1.3	Relation between nets and filters . . . . .	597
<b>48</b>	<b>Topology_ZF_examples.thy</b>	<b>608</b>
48.1	Some new ideas on cardinals . . . . .	608
48.1.1	cases-type results . . . . .	608
48.1.2	Relations between a cardinal and its successor . . . . .	610
48.1.3	Main result on cardinals (without the <i>Axiom of Choice</i> )	612
48.2	CoCardinal Topology of a set $X$ . . . . .	615
48.2.1	CoCardinal topology is a topology. . . . .	615
48.2.2	Total set, Closed sets, Interior, Closure and Boundary	617
48.2.3	Special cases and subspaces . . . . .	621
48.3	Excluded Set Topology . . . . .	623
48.3.1	Excluded set topology is a topology. . . . .	623
48.3.2	Total set, Closed sets, Interior, Closure and Boundary	624
48.3.3	Special cases and subspaces . . . . .	628
48.4	Included Set Topology . . . . .	629
48.4.1	Included set topology is a topology. . . . .	629
48.4.2	Total set, Closed sets, Interior, Closure and Boundary	630
48.4.3	Special cases and subspaces . . . . .	633
<b>49</b>	<b>Topology_ZF_examples_1.thy</b>	<b>635</b>
49.1	New ideas using a base for a topology . . . . .	635
49.1.1	The topology of a base . . . . .	635
49.1.2	Dual Base for Closed Sets . . . . .	639
49.2	Partition topology . . . . .	641
49.2.1	Partition topology is a topology. . . . .	642
49.2.2	Total set, Closed sets, Interior, Closure and Boundary	643
49.2.3	Special cases and subspaces . . . . .	648
49.3	Order topologies . . . . .	650
49.3.1	Order topology is a topology . . . . .	650
49.3.2	Total set . . . . .	662
49.3.3	Right order and Left order topologies. . . . .	663

49.3.4	Right and Left Order topologies are topologies . . . .	663
49.3.5	Total set . . . . .	664
49.4	Union of Topologies . . . . .	665
<b>50</b>	<b>Topology_ZF_properties.thy</b>	<b>667</b>
50.1	Properties of compactness . . . . .	667
50.2	Properties of numerability . . . . .	670
50.2.1	Some cardinal related results . . . . .	672
50.2.2	Relations between numerability properties . . . . .	673
50.3	Relation between numerability and compactness . . . . .	679
<b>51</b>	<b>Topology_ZF_5.thy</b>	<b>693</b>
51.1	Some results for separation axioms . . . . .	693
51.1.1	Hereditability . . . . .	702
51.2	Spectrum and anti-properties . . . . .	705
<b>52</b>	<b>Topology_ZF_6.thy</b>	<b>735</b>
52.1	Image filter . . . . .	735
52.2	Continuous at a point vs. globally continuous . . . . .	736
52.3	Continuous functions and filters . . . . .	737
<b>53</b>	<b>Topology_ZF_7.thy</b>	<b>741</b>
53.1	Connection Properties . . . . .	741
<b>54</b>	<b>TopologicalGroup_ZF.thy</b>	<b>773</b>
54.1	Topological group: definition and notation . . . . .	773
54.2	Interval arithmetic, translations and inverse of set . . . . .	777
54.3	Neighborhoods of zero . . . . .	778
54.4	Closure in topological groups . . . . .	779
54.5	Sums of sequences of elements and subsets . . . . .	781
<b>55</b>	<b>Metamath_interface.thy</b>	<b>785</b>
55.1	MMisar0 and complex0 contexts. . . . .	785
<b>56</b>	<b>Metamath_sampler.thy</b>	<b>792</b>
56.1	Extended reals and order . . . . .	792
56.2	Natural real numbers . . . . .	796
56.3	Infimum and supremum in real numbers . . . . .	798

# 1 Introduction.thy

**theory** Introduction imports equalities

**begin**

This theory does not contain any formalized mathematics used in other theories, but is an introduction to IsarMathLib project.

## 1.1 How to read IsarMathLib proofs - a tutorial

Isar (the Isabelle's formal proof language) was designed to be similar to the standard language of mathematics. Any person able to read proofs in a typical mathematical paper should be able to read and understand Isar proofs without having to learn a special proof language. However, Isar is a formal proof language and as such it does contain a couple of constructs whose meaning is hard to guess. In this tutorial we will define a notion and prove an example theorem about that notion, explaining Isar syntax along the way. This tutorial may also serve as a style guide for IsarMathLib contributors. Note that this tutorial aims to help in reading the presentation of the Isar language that is used in IsarMathLib proof document and HTML rendering on the FormalMath.org site, but does not teach how to write proofs that can be verified by Isabelle. This presentation is different than the source processed by Isabelle (the concept that the source and presentation look different should be familiar to any LaTeX user). To learn how to write Isar proofs one needs to study the source of this tutorial as well.

The first thing that mathematicians typically do is to define notions. In Isar this is done with the **definition** keyword. In our case we define a notion of two sets being disjoint. We will use the infix notation, i.e. the string `{is disjoint with}` put between two sets to denote our notion of disjointness. The left side of the  $\equiv$  symbol is the notion being defined, the right side says how we define it. In Isabelle `0` is used to denote both zero (of natural numbers) and the empty set, which is not surprising as those two things are the same in set theory.

**definition**

```
AreDisjoint (infix {is disjoint with} 90) where  
A {is disjoint with} B  $\equiv$   $A \cap B = 0$ 
```

We are ready to prove a theorem. Here we show that the relation of being disjoint is symmetric. We start with one of the keywords "theorem", "lemma" or "corollary". In Isar they are synonymous. Then we provide a name for the theorem. In standard mathematics theorems are numbered. In Isar we can do that too, but it is considered better to give theorems meaningful names. After the "shows" keyword we give the statement to show.



The  $\longleftrightarrow$  symbol denotes the equivalence in Isabelle/ZF. Here we want to show that "A is disjoint with B iff and only if B is disjoint with A". To prove this fact we show two implications - the first one that A {is disjoint with} B implies B {is disjoint with} A and then the converse one. Each of these implications is formulated as a statement to be proved and then proved in a subproof like a mini-theorem. Each subproof uses a proof block to show the implication. Proof blocks are delimited with curly brackets in Isar. Proof block is one of the constructs that does not exist in informal mathematics, so it may be confusing. When reading a proof containing a proof block I suggest to focus first on what is that we are proving in it. This can be done by looking at the first line or two of the block and then at the last statement. In our case the block starts with "assume A {is disjoint with} B" and the last statement is "then have B {is disjoint with} A". It is a typical pattern when someone needs to prove an implication: one assumes the antecedent and then shows that the consequent follows from this assumption. Implications are denoted with the  $\longrightarrow$  symbol in Isabelle. After we prove both implications we collect them using the "moreover" construct. The keyword "ultimately" indicates that what follows is the conclusion of the statements collected with "moreover". The "show" keyword is like "have", except that it indicates that we have arrived at the claim of the theorem (or a subproof).

```

theorem disjointness_symmetric:
  shows A {is disjoint with} B  $\longleftrightarrow$  B {is disjoint with} A
proof -
  have A {is disjoint with} B  $\longrightarrow$  B {is disjoint with} A
  proof -
    { assume A {is disjoint with} B
      then have A  $\cap$  B = 0 using AreDisjoint_def by simp
      hence B  $\cap$  A = 0 by auto
      then have B {is disjoint with} A
        using AreDisjoint_def by simp
    } thus thesis by simp
  qed
  moreover have B {is disjoint with} A  $\longrightarrow$  A {is disjoint with} B
  proof -
    { assume B {is disjoint with} A
      then have B  $\cap$  A = 0 using AreDisjoint_def by simp
      hence A  $\cap$  B = 0 by auto
      then have A {is disjoint with} B
        using AreDisjoint_def by simp
    } thus thesis by simp
  qed
  ultimately show thesis by blast
qed

```

## 1.2 Overview of the project

The `Fo11`, `ZF1` and `Nat_ZF_IML` theory files contain some background material that is needed for the remaining theories.

`Order_ZF` and `Order_ZF_1a` reformulate material from standard Isabelle's `Order` theory in terms of non-strict (less-or-equal) order relations. `Order_ZF_1` on the other hand directly continues the `Order` theory file using strict order relations (less and not equal). This is useful for translating theorems from Metamath.

In `NatOrder_ZF` we prove that the usual order on natural numbers is linear. The `func1` theory provides basic facts about functions. `func_ZF` continues this development with more advanced topics that relate to algebraic properties of binary operations, like lifting a binary operation to a function space, associative, commutative and distributive operations and properties of functions related to order relations. `func_ZF_1` is about properties of functions related to order relations.

The standard Isabelle's `Finite` theory defines the finite powerset of a set as a certain "datatype" (?) with some recursive properties. IsarMathLib's `Finite1` and `Finite_ZF_1` theories develop more facts about this notion. These two theories are obsolete now. They will be gradually replaced by an approach based on set theory rather than tools specific to Isabelle. This approach is presented in `Finite_ZF` theory file.

In `FinOrd_ZF` we talk about ordered finite sets.

The `EquivClass1` theory file is a reformulation of the material in the standard Isabelle's `EquivClass` theory in the spirit of ZF set theory.

`FiniteSeq_ZF` discusses the notion of finite sequences (a.k.a. lists).

`InductiveSeq_ZF` provides the definition and properties of (what is known in basic calculus as) sequences defined by induction, i. e. by a formula of the form  $a_0 = x$ ,  $a_{n+1} = f(a_n)$ .

`Fold_ZF` shows how the familiar from functional programming notion of fold can be interpreted in set theory.

`Partitions_ZF` is about splitting a set into non-overlapping subsets. This is a common trick in proofs.

`Semigroup_ZF` treats the expressions of the form  $a_0 \cdot a_1 \dots a_n$ , (i.e. products of finite sequences), where  $\cdot$  is an associative binary operation.

`CommutativeSemigroup_ZF` is another take on a similar subject. This time we consider the case when the operation is commutative and the result of depends only on the set of elements we are summing (additively speaking), but not the order.

The `Topology_ZF` series covers basics of general topology: interior, closure, boundary, compact sets, separation axioms and continuous functions.

`Group_ZF`, `Group_ZF_1`, `Group_ZF_1b` and `Group_ZF_2` provide basic facts of the group theory. `Group_ZF_3` considers the notion of almost homomorphisms that is needed for the real numbers construction in `Real_ZF`.

The `TopologicalGroup` connects the `Topology_ZF` and `Group_ZF` series and starts the subject of topological groups with some basic definitions and facts. In `DirectProduct_ZF` we define direct product of groups and show some its basic properties.

The `OrderedGroup_ZF` theory treats ordered groups. This is a surprisingly large theory for such relatively obscure topic.

`Ring_ZF` defines rings. `Ring_ZF_1` covers the properties of rings that are specific to the real numbers construction in `Real_ZF`.

The `OrderedRing_ZF` theory looks at the consequences of adding a linear order to the ring algebraic structure.

`Field_ZF` and `OrderedField_ZF` contain basic facts about (you guessed it) fields and ordered fields.

`Int_ZF_IML` theory considers the integers as a monoid (multiplication) and an abelian ordered group (addition). In `Int_ZF_1` we show that integers form a commutative ring. `Int_ZF_2` contains some facts about slopes (almost homomorphisms on integers) needed for real numbers construction, used in `Real_ZF_1`.

In the `IntDiv_ZF_IML` theory translates some properties of the integer quotient and remainder functions studied in the standard Isabelle's `IntDiv_ZF` theory to the notation used in `IsarMathLib`.

The `Real_ZF` and `Real_ZF_1` theories contain the construction of real numbers based on the paper [2] by R. D. Arthan (not Cauchy sequences, not Dedekind sections). The heavy lifting is done mostly in `Group_ZF_3`, `Ring_ZF_1` and `Int_ZF_2`. `Real_ZF` contains the part of the construction that can be done starting from generic abelian groups (rather than additive group of integers). This allows to show that real numbers form a ring. `Real_ZF_1` continues the construction using properties specific to the integers and showing that real numbers constructed this way form a complete ordered field.

In `Complex_ZF` we construct complex numbers starting from a complete ordered field (a model of real numbers). We also define the notation for writing about complex numbers and prove that the structure of complex numbers constructed there satisfies the axioms of complex numbers used in `Metamath`.

`MMI_prelude` defines the `mmisar0` context in which most theorems translated from `Metamath` are proven. It also contains a chapter explaining how the translation works.

In the `Metamath_interface` theory we prove a theorem that the `mmisar0` context is valid (can be used) in the `complex0` context. All theories us-

ing the translated results will import the `Metamath_interface` theory. The `Metamath_sampler` theory provides some examples of using the translated theorems in the `complex0` context.

The theories `MMI_logic_and_sets`, `MMI_Complex`, `MMI_Complex_1` and `MMI_Complex_2` contain the theorems imported from the Metamath's `set.mm` database. As the translated proofs are rather verbose these theories are not printed in this proof document. The full list of translated facts can be found in the `Metamath_theorems.txt` file included in the `IsarMathLib` distribution. The `MMI_examples` provides some theorems imported from Metamath that are printed in this proof document as examples of how translated proofs look like.

**end**

## 2 Order\_ZF.thy

**theory** Order\_ZF **imports** Fol1

**begin**

This theory file considers various notion related to order. We redefine the notions of a total order, linear order and partial order to have the same terminology as Wikipedia (I found it very consistent across different areas of math). We also define and study the notions of intervals and bounded sets. We show the inclusion relations between the intervals with endpoints being in certain order. We also show that union of bounded sets are bounded. This allows to show in `Finite_ZF.thy` that finite sets are bounded.

### 2.1 Definitions

In this section we formulate the definitions related to order relations.

A relation  $r$  is "total" on a set  $X$  if for all elements  $a, b$  of  $X$  we have  $a$  is in relation with  $b$  or  $b$  is in relation with  $a$ . An example is the  $\leq$  relation on numbers.

**definition**

`IsTotal (infixl {is total on} 65) where`  
`r {is total on} X  $\equiv$  ( $\forall a \in X. \forall b \in X. \langle a, b \rangle \in r \vee \langle b, a \rangle \in r$ )`

A relation  $r$  is a partial order on  $X$  if it is reflexive on  $X$  (i.e.  $\langle x, x \rangle$  for every  $x \in X$ ), antisymmetric (if  $\langle x, y \rangle \in r$  and  $\langle y, x \rangle \in r$ , then  $x = y$ ) and transitive ( $\langle x, y \rangle \in r$  and  $\langle y, z \rangle \in r$  implies  $\langle x, z \rangle \in r$ ).

**definition**

`IsPartOrder(X,r)  $\equiv$  (refl(X,r)  $\wedge$  antisym(r)  $\wedge$  trans(r))`

We define a linear order as a binary relation that is antisymmetric, transitive and total. Note that this terminology is different than the one used the standard `Order.thy` file.

**definition**

`IsLinOrder(X,r)  $\equiv$  ( antisym(r)  $\wedge$  trans(r)  $\wedge$  (r {is total on} X))`

A set is bounded above if there is that is an upper bound for it, i.e. there are some  $u$  such that  $\langle x, u \rangle \in r$  for all  $x \in A$ . In addition, the empty set is defined as bounded.

**definition**

`IsBoundedAbove(A,r)  $\equiv$  ( A=0  $\vee$  ( $\exists u. \forall x \in A. \langle x, u \rangle \in r$ ))`

We define sets bounded below analogously.

**definition**

`IsBoundedBelow(A,r)  $\equiv$  (A=0  $\vee$  ( $\exists l. \forall x \in A. \langle l, x \rangle \in r$ ))`

A set is bounded if it is bounded below and above.

**definition**

$$\text{IsBounded}(A, r) \equiv (\text{IsBoundedAbove}(A, r) \wedge \text{IsBoundedBelow}(A, r))$$

The notation for the definition of an interval may be mysterious for some readers, see lemma `Order_ZF_2_L1` for more intuitive notation.

**definition**

$$\text{Interval}(r, a, b) \equiv r\{a\} \cap r-\{b\}$$

We also define the maximum (the greater of) two elements in the obvious way.

**definition**

$$\text{GreaterOf}(r, a, b) \equiv (\text{if } \langle a, b \rangle \in r \text{ then } b \text{ else } a)$$

The definition of a minimum (the smaller of) two elements.

**definition**

$$\text{SmallerOf}(r, a, b) \equiv (\text{if } \langle a, b \rangle \in r \text{ then } a \text{ else } b)$$

We say that a set has a maximum if it has an element that is not smaller than any other one. We show that under some conditions this element of the set is unique (if exists).

**definition**

$$\text{HasAmaximum}(r, A) \equiv \exists M \in A. \forall x \in A. \langle x, M \rangle \in r$$

A similar definition what it means that a set has a minimum.

**definition**

$$\text{HasAminimum}(r, A) \equiv \exists m \in A. \forall x \in A. \langle m, x \rangle \in r$$

Definition of the maximum of a set.

**definition**

$$\text{Maximum}(r, A) \equiv \text{THE } M. M \in A \wedge (\forall x \in A. \langle x, M \rangle \in r)$$

Definition of a minimum of a set.

**definition**

$$\text{Minimum}(r, A) \equiv \text{THE } m. m \in A \wedge (\forall x \in A. \langle m, x \rangle \in r)$$

The supremum of a set  $A$  is defined as the minimum of the set of upper bounds, i.e. the set  $\{u. \forall a \in A. \langle a, u \rangle \in r\} = \bigcap_{a \in A} r\{a\}$ . Recall that in Isabelle/ZF  $r-(A)$  denotes the inverse image of the set  $A$  by relation  $r$  (i.e.  $r-(A) = \{x : \langle x, y \rangle \in r \text{ for some } y \in A\}$ ).

**definition**

$$\text{Supremum}(r, A) \equiv \text{Minimum}(r, \bigcap_{a \in A} r\{a\})$$

Infimum is defined analogously.

**definition**

$$\text{Infimum}(r, A) \equiv \text{Maximum}(r, \bigcap_{a \in A} r-\{a\})$$

We define a relation to be complete if every nonempty bounded above set has a supremum.

**definition**

`IsComplete (_ {is complete}) where`  
`r {is complete}  $\equiv$`   
 `$\forall A. \text{IsBoundedAbove}(A, r) \wedge A \neq \emptyset \longrightarrow \text{HasAminimum}(r, \bigcap_{a \in A} r-\{a\})$`

The essential condition to show that a total relation is reflexive.

**lemma** `Order_ZF_1_L1: assumes r {is total on} X and a  $\in$  X`  
`shows  $\langle a, a \rangle \in r$  using assms IsTotal_def by auto`

A total relation is reflexive.

**lemma** `total_is_refl:`  
`assumes r {is total on} X`  
`shows  $\text{refl}(X, r)$  using assms Order_ZF_1_L1 refl_def by simp`

A linear order is partial order.

**lemma** `Order_ZF_1_L2: assumes IsLinOrder(X, r)`  
`shows IsPartOrder(X, r)`  
`using assms IsLinOrder_def IsPartOrder_def refl_def Order_ZF_1_L1`  
`by auto`

Partial order that is total is linear.

**lemma** `Order_ZF_1_L3:`  
`assumes IsPartOrder(X, r) and r {is total on} X`  
`shows IsLinOrder(X, r)`  
`using assms IsPartOrder_def IsLinOrder_def`  
`by simp`

Relation that is total on a set is total on any subset.

**lemma** `Order_ZF_1_L4: assumes r {is total on} X and  $A \subseteq X$`   
`shows r {is total on} A`  
`using assms IsTotal_def by auto`

A linear relation is linear on any subset.

**lemma** `ord_linear_subset: assumes IsLinOrder(X, r) and  $A \subseteq X$`   
`shows IsLinOrder(A, r)`  
`using assms IsLinOrder_def Order_ZF_1_L4 by blast`

If the relation is total, then every set is a union of those elements that are nongreater than a given one and nonsmaller than a given one.

**lemma** `Order_ZF_1_L5:`  
`assumes r {is total on} X and  $A \subseteq X$  and  $a \in X$`   
`shows  $A = \{x \in A. \langle x, a \rangle \in r\} \cup \{x \in A. \langle a, x \rangle \in r\}$`   
`using assms IsTotal_def by auto`

A technical fact about reflexive relations.

```
lemma refl_add_point:
  assumes refl(X,r) and A ⊆ B ∪ {x} and B ⊆ X and
  x ∈ X and ∀y∈B. ⟨y,x⟩ ∈ r
  shows ∀a∈A. ⟨a,x⟩ ∈ r
  using assms refl_def by auto
```

## 2.2 Intervals

In this section we discuss intervals.

The next lemma explains the notation of the definition of an interval.

```
lemma Order_ZF_2_L1:
  shows x ∈ Interval(r,a,b) ⟷ ⟨ a,x⟩ ∈ r ∧ ⟨ x,b⟩ ∈ r
  using Interval_def by auto
```

Since there are some problems with applying the above lemma (seems that simp and auto don't handle equivalence very well), we split `Order_ZF_2_L1` into two lemmas.

```
lemma Order_ZF_2_L1A: assumes x ∈ Interval(r,a,b)
  shows ⟨ a,x⟩ ∈ r  ⟨ x,b⟩ ∈ r
  using assms Order_ZF_2_L1 by auto
```

`Order_ZF_2_L1`, implication from right to left.

```
lemma Order_ZF_2_L1B: assumes ⟨ a,x⟩ ∈ r  ⟨ x,b⟩ ∈ r
  shows x ∈ Interval(r,a,b)
  using assms Order_ZF_2_L1 by simp
```

If the relation is reflexive, the endpoints belong to the interval.

```
lemma Order_ZF_2_L2: assumes refl(X,r)
  and a∈X  b∈X and ⟨ a,b⟩ ∈ r
  shows
  a ∈ Interval(r,a,b)
  b ∈ Interval(r,a,b)
  using assms refl_def Order_ZF_2_L1 by auto
```

Under the assumptions of `Order_ZF_2_L2`, the interval is nonempty.

```
lemma Order_ZF_2_L2A: assumes refl(X,r)
  and a∈X  b∈X and ⟨ a,b⟩ ∈ r
  shows Interval(r,a,b) ≠ 0
```

**proof -**

```
  from assms have a ∈ Interval(r,a,b)
    using Order_ZF_2_L2 by simp
  then show Interval(r,a,b) ≠ 0 by auto
```

**qed**

If  $a, b, c, d$  are in this order, then  $[b, c] \subseteq [a, d]$ . We only need transitivity for this to be true.



```

lemma Order_ZF_2_L3:
  assumes A1: trans(r) and A2:  $\langle a,b \rangle \in r \ \langle b,c \rangle \in r \ \langle c,d \rangle \in r$ 
  shows Interval(r,b,c)  $\subseteq$  Interval(r,a,d)
proof
  fix x assume A3:  $x \in \text{Interval}(r, b, c)$ 
  note A1
  moreover from A2 A3 have  $\langle a,b \rangle \in r \wedge \langle b,x \rangle \in r$  using Order_ZF_2_L1A
  by simp
  ultimately have T1:  $\langle a,x \rangle \in r$  by (rule Fol1_L3)
  note A1
  moreover from A2 A3 have  $\langle x,c \rangle \in r \wedge \langle c,d \rangle \in r$  using Order_ZF_2_L1A
  by simp
  ultimately have  $\langle x,d \rangle \in r$  by (rule Fol1_L3)
  with T1 show  $x \in \text{Interval}(r,a,d)$  using Order_ZF_2_L1B
  by simp
qed

```

For reflexive and antisymmetric relations the interval with equal endpoints consists only of that endpoint.

```

lemma Order_ZF_2_L4:
  assumes A1: refl(X,r) and A2: antisym(r) and A3:  $a \in X$ 
  shows Interval(r,a,a) = {a}
proof
  from A1 A3 have  $\langle a,a \rangle \in r$  using refl_def by simp
  with A1 A3 show {a}  $\subseteq$  Interval(r,a,a) using Order_ZF_2_L2 by simp
  from A2 show Interval(r,a,a)  $\subseteq$  {a} using Order_ZF_2_L1A Fol1_L4
  by fast
qed

```

For transitive relations the endpoints have to be in the relation for the interval to be nonempty.

```

lemma Order_ZF_2_L5: assumes A1: trans(r) and A2:  $\langle a,b \rangle \notin r$ 
  shows Interval(r,a,b) = 0
proof -
  { assume Interval(r,a,b)  $\neq$  0 then obtain x where  $x \in \text{Interval}(r,a,b)$ 
    by auto
    with A1 A2 have False using Order_ZF_2_L1A Fol1_L3 by fast
  } thus thesis by auto
qed

```

If a relation is defined on a set, then intervals are subsets of that set.

```

lemma Order_ZF_2_L6: assumes A1:  $r \subseteq X \times X$ 
  shows Interval(r,a,b)  $\subseteq X$ 
  using assms Interval_def by auto

```

## 2.3 Bounded sets

In this section we consider properties of bounded sets.

For reflexive relations singletons are bounded.

```
lemma Order_ZF_3_L1: assumes refl(X,r) and a∈X
  shows IsBounded({a},r)
  using assms refl_def IsBoundedAbove_def IsBoundedBelow_def
    IsBounded_def by auto
```

Sets that are bounded above are contained in the domain of the relation.

```
lemma Order_ZF_3_L1A: assumes r ⊆ X×X
  and IsBoundedAbove(A,r)
  shows A⊆X using assms IsBoundedAbove_def by auto
```

Sets that are bounded below are contained in the domain of the relation.

```
lemma Order_ZF_3_L1B: assumes r ⊆ X×X
  and IsBoundedBelow(A,r)
  shows A⊆X using assms IsBoundedBelow_def by auto
```

For a total relation, the greater of two elements, as defined above, is indeed greater of any of the two.

```
lemma Order_ZF_3_L2: assumes r {is total on} X
  and x∈X y∈X
  shows
    ⟨x, GreaterOf(r,x,y)⟩ ∈ r
    ⟨y, GreaterOf(r,x,y)⟩ ∈ r
    ⟨SmallerOf(r,x,y), x⟩ ∈ r
    ⟨SmallerOf(r,x,y), y⟩ ∈ r
  using assms IsTotal_def Order_ZF_1_L1 GreaterOf_def SmallerOf_def
    by auto
```

If  $A$  is bounded above by  $u$ ,  $B$  is bounded above by  $w$ , then  $A \cup B$  is bounded above by the greater of  $u, w$ .

```
lemma Order_ZF_3_L2B:
  assumes A1: r {is total on} X and A2: trans(r)
  and A3: u∈X w∈X
  and A4: ∀x∈A. ⟨ x,u⟩ ∈ r ∀x∈B. ⟨ x,w⟩ ∈ r
  shows ∀x∈A∪B. ⟨x, GreaterOf(r,u,w)⟩ ∈ r
proof
  let v = GreaterOf(r,u,w)
  from A1 A3 have T1: ⟨ u,v⟩ ∈ r and T2: ⟨ w,v⟩ ∈ r
    using Order_ZF_3_L2 by auto
  fix x assume A5: x∈A∪B show ⟨x,v⟩ ∈ r
  proof -
    { assume x∈A
      with A4 T1 have ⟨ x,u⟩ ∈ r ∧ ⟨ u,v⟩ ∈ r by simp
      with A2 have ⟨x,v⟩ ∈ r by (rule Fol1_L3) }
  moreover
    { assume x∉A
      with A5 A4 T2 have ⟨ x,w⟩ ∈ r ∧ ⟨ w,v⟩ ∈ r by simp
      with A2 have ⟨x,v⟩ ∈ r by (rule Fol1_L3) }
```

ultimately show thesis by auto  
qed  
qed

For total and transitive relation the union of two sets bounded above is bounded above.

lemma Order\_ZF\_3\_L3:  
 assumes A1:  $r$  {is total on}  $X$  and A2:  $\text{trans}(r)$   
 and A3:  $\text{IsBoundedAbove}(A, r)$   $\text{IsBoundedAbove}(B, r)$   
 and A4:  $r \subseteq X \times X$   
 shows  $\text{IsBoundedAbove}(A \cup B, r)$   
 proof -  
 { assume  $A = 0 \vee B = 0$   
 with A3 have  $\text{IsBoundedAbove}(A \cup B, r)$  by auto }  
 moreover  
 { assume  $\neg (A = 0 \vee B = 0)$   
 then have T1:  $A \neq 0 \wedge B \neq 0$  by auto  
 with A3 obtain  $u \ w$  where D1:  $\forall x \in A. \langle x, u \rangle \in r \ \forall x \in B. \langle x, w \rangle \in r$   
 using  $\text{IsBoundedAbove\_def}$  by auto  
 let  $U = \text{GreaterOf}(r, u, w)$   
 from T1 A4 D1 have  $u \in X \ w \in X$  by auto  
 with A1 A2 D1 have  $\forall x \in A \cup B. \langle x, U \rangle \in r$   
 using Order\_ZF\_3\_L2B by blast  
 then have  $\text{IsBoundedAbove}(A \cup B, r)$   
 using  $\text{IsBoundedAbove\_def}$  by auto }  
 ultimately show thesis by auto  
qed

For total and transitive relations if a set  $A$  is bounded above then  $A \cup \{a\}$  is bounded above.

lemma Order\_ZF\_3\_L4:  
 assumes A1:  $r$  {is total on}  $X$  and A2:  $\text{trans}(r)$   
 and A3:  $\text{IsBoundedAbove}(A, r)$  and A4:  $a \in X$  and A5:  $r \subseteq X \times X$   
 shows  $\text{IsBoundedAbove}(A \cup \{a\}, r)$   
 proof -  
 from A1 have  $\text{refl}(X, r)$   
 using  $\text{total\_is\_refl}$  by simp  
 with assms show thesis using  
 Order\_ZF\_3\_L1  $\text{IsBounded\_def}$  Order\_ZF\_3\_L3 by simp  
qed

If  $A$  is bounded below by  $l$ ,  $B$  is bounded below by  $m$ , then  $A \cup B$  is bounded below by the smaller of  $u, w$ .

lemma Order\_ZF\_3\_L5B:  
 assumes A1:  $r$  {is total on}  $X$  and A2:  $\text{trans}(r)$   
 and A3:  $l \in X \ m \in X$   
 and A4:  $\forall x \in A. \langle l, x \rangle \in r \ \forall x \in B. \langle m, x \rangle \in r$   
 shows  $\forall x \in A \cup B. \langle \text{SmallerOf}(r, l, m), x \rangle \in r$

```

proof
  let k = SmallerOf(r,l,m)
  from A1 A3 have T1:  $\langle k, l \rangle \in r$  and T2:  $\langle k, m \rangle \in r$ 
    using Order_ZF_3_L2 by auto
  fix x assume A5:  $x \in A \cup B$  show  $\langle k, x \rangle \in r$ 
  proof -
    { assume  $x \in A$ 
      with A4 T1 have  $\langle k, l \rangle \in r \wedge \langle l, x \rangle \in r$  by simp
      with A2 have  $\langle k, x \rangle \in r$  by (rule Fol1_L3) }
    moreover
    { assume  $x \notin A$ 
      with A5 A4 T2 have  $\langle k, m \rangle \in r \wedge \langle m, x \rangle \in r$  by simp
      with A2 have  $\langle k, x \rangle \in r$  by (rule Fol1_L3) }
    ultimately show thesis by auto
  qed
qed

```

For total and transitive relation the union of two sets bounded below is bounded below.

```

lemma Order_ZF_3_L6:
  assumes A1:  $r$  {is total on}  $X$  and A2:  $\text{trans}(r)$ 
  and A3:  $\text{IsBoundedBelow}(A, r)$   $\text{IsBoundedBelow}(B, r)$ 
  and A4:  $r \subseteq X \times X$ 
  shows  $\text{IsBoundedBelow}(A \cup B, r)$ 
proof -
  { assume  $A = 0 \vee B = 0$ 
    with A3 have thesis by auto }
  moreover
  { assume  $\neg (A = 0 \vee B = 0)$ 
    then have T1:  $A \neq 0 \wedge B \neq 0$  by auto
    with A3 obtain l m where D1:  $\forall x \in A. \langle l, x \rangle \in r \ \forall x \in B. \langle m, x \rangle \in r$ 
      using IsBoundedBelow_def by auto
    let L = SmallerOf(r,l,m)
    from T1 A4 D1 have T1:  $l \in X \wedge m \in X$  by auto
    with A1 A2 D1 have  $\forall x \in A \cup B. \langle L, x \rangle \in r$ 
      using Order_ZF_3_L5B by blast
    then have  $\text{IsBoundedBelow}(A \cup B, r)$ 
      using IsBoundedBelow_def by auto }
  ultimately show thesis by auto
qed

```

For total and transitive relations if a set  $A$  is bounded below then  $A \cup \{a\}$  is bounded below.

```

lemma Order_ZF_3_L7:
  assumes A1:  $r$  {is total on}  $X$  and A2:  $\text{trans}(r)$ 
  and A3:  $\text{IsBoundedBelow}(A, r)$  and A4:  $a \in X$  and A5:  $r \subseteq X \times X$ 
  shows  $\text{IsBoundedBelow}(A \cup \{a\}, r)$ 
proof -
  from A1 have refl( $X, r$ )

```

```

    using total_is_refl by simp
  with assms show thesis using
    Order_ZF_3_L1 IsBounded_def Order_ZF_3_L6 by simp
qed

```

For total and transitive relations unions of two bounded sets are bounded.

```

theorem Order_ZF_3_T1:
  assumes r {is total on} X and trans(r)
  and IsBounded(A,r) IsBounded(B,r)
  and  $r \subseteq X \times X$ 
  shows IsBounded(A  $\cup$  B,r)
  using assms Order_ZF_3_L3 Order_ZF_3_L6 Order_ZF_3_L7 IsBounded_def
  by simp

```

For total and transitive relations if a set  $A$  is bounded then  $A \cup \{a\}$  is bounded.

```

lemma Order_ZF_3_L8:
  assumes r {is total on} X and trans(r)
  and IsBounded(A,r) and  $a \in X$  and  $r \subseteq X \times X$ 
  shows IsBounded(A  $\cup$  {a},r)
  using assms total_is_refl Order_ZF_3_L1 Order_ZF_3_T1 by blast

```

A sufficient condition for a set to be bounded below.

```

lemma Order_ZF_3_L9: assumes A1:  $\forall a \in A. \langle 1, a \rangle \in r$ 
  shows IsBoundedBelow(A,r)
proof -
  from A1 have  $\exists 1. \forall x \in A. \langle 1, x \rangle \in r$ 
  by auto
  then show IsBoundedBelow(A,r)
  using IsBoundedBelow_def by simp
qed

```

A sufficient condition for a set to be bounded above.

```

lemma Order_ZF_3_L10: assumes A1:  $\forall a \in A. \langle a, u \rangle \in r$ 
  shows IsBoundedAbove(A,r)
proof -
  from A1 have  $\exists u. \forall x \in A. \langle x, u \rangle \in r$ 
  by auto
  then show IsBoundedAbove(A,r)
  using IsBoundedAbove_def by simp
qed

```

Intervals are bounded.

```

lemma Order_ZF_3_L11: shows
  IsBoundedAbove(Interval(r,a,b),r)
  IsBoundedBelow(Interval(r,a,b),r)
  IsBounded(Interval(r,a,b),r)
proof -

```

```

{ fix x assume x ∈ Interval(r,a,b)
  then have ⟨ x,b ⟩ ∈ r  ⟨ a,x ⟩ ∈ r
    using Order_ZF_2_L1A by auto
} then have
  ∃u. ∀x∈Interval(r,a,b). ⟨ x,u ⟩ ∈ r
  ∃l. ∀x∈Interval(r,a,b). ⟨ l,x ⟩ ∈ r
  by auto
then show
  IsBoundedAbove(Interval(r,a,b),r)
  IsBoundedBelow(Interval(r,a,b),r)
  IsBounded(Interval(r,a,b),r)
  using IsBoundedAbove_def IsBoundedBelow_def IsBounded_def
  by auto
qed

```

A subset of a set that is bounded below is bounded below.

```

lemma Order_ZF_3_L12: assumes A1: IsBoundedBelow(A,r) and A2: B⊆A
  shows IsBoundedBelow(B,r)
proof -
  { assume A = 0
    with assms have IsBoundedBelow(B,r)
      using IsBoundedBelow_def by auto }
  moreover
  { assume A ≠ 0
    with A1 have ∃l. ∀x∈A. ⟨ l,x ⟩ ∈ r
      using IsBoundedBelow_def by simp
    with A2 have ∃l. ∀x∈B. ⟨ l,x ⟩ ∈ r by auto
    then have IsBoundedBelow(B,r) using IsBoundedBelow_def
      by auto }
  ultimately show IsBoundedBelow(B,r) by auto
qed

```

A subset of a set that is bounded above is bounded above.

```

lemma Order_ZF_3_L13: assumes A1: IsBoundedAbove(A,r) and A2: B⊆A
  shows IsBoundedAbove(B,r)
proof -
  { assume A = 0
    with assms have IsBoundedAbove(B,r)
      using IsBoundedAbove_def by auto }
  moreover
  { assume A ≠ 0
    with A1 have ∃u. ∀x∈A. ⟨ x,u ⟩ ∈ r
      using IsBoundedAbove_def by simp
    with A2 have ∃u. ∀x∈B. ⟨ x,u ⟩ ∈ r by auto
    then have IsBoundedAbove(B,r) using IsBoundedAbove_def
      by auto }
  ultimately show IsBoundedAbove(B,r) by auto
qed

```

If for every element of  $X$  we can find one in  $A$  that is greater, then the  $A$

can not be bounded above. Works for relations that are total, transitive and antisymmetric, (i.e. for linear order relations).

```

lemma Order_ZF_3_L14:
  assumes A1: r {is total on} X
  and A2: trans(r) and A3: antisym(r)
  and A4: r  $\subseteq$  X×X and A5: X≠0
  and A6:  $\forall x \in X. \exists a \in A. x \neq a \wedge \langle x, a \rangle \in r$ 
  shows  $\neg$ IsBoundedAbove(A,r)
proof -
  { from A5 A6 have I: A≠0 by auto
    moreover assume IsBoundedAbove(A,r)
    ultimately obtain u where II:  $\forall x \in A. \langle x, u \rangle \in r$ 
      using IsBounded_def IsBoundedAbove_def by auto
    with A4 I have u∈X by auto
    with A6 obtain b where b∈A and III:  $u \neq b$  and  $\langle u, b \rangle \in r$ 
      by auto
    with II have  $\langle b, u \rangle \in r$   $\langle u, b \rangle \in r$  by auto
    with A3 have b=u by (rule Foll_L4)
    with III have False by simp
  } thus  $\neg$ IsBoundedAbove(A,r) by auto
qed

```

The set of elements in a set  $A$  that are nongreater than a given element is bounded above.

```

lemma Order_ZF_3_L15: shows IsBoundedAbove( $\{x \in A. \langle x, a \rangle \in r\}$ ,r)
  using IsBoundedAbove_def by auto

```

If  $A$  is bounded below, then the set of elements in a set  $A$  that are nongreater than a given element is bounded.

```

lemma Order_ZF_3_L16: assumes A1: IsBoundedBelow(A,r)
  shows IsBounded( $\{x \in A. \langle x, a \rangle \in r\}$ ,r)
proof -
  { assume A=0
    then have IsBounded( $\{x \in A. \langle x, a \rangle \in r\}$ ,r)
      using IsBoundedBelow_def IsBoundedAbove_def IsBounded_def
      by auto }
  moreover
  { assume A≠0
    with A1 obtain l where I:  $\forall x \in A. \langle l, x \rangle \in r$ 
      using IsBoundedBelow_def by auto
    then have  $\forall y \in \{x \in A. \langle x, a \rangle \in r\}. \langle l, y \rangle \in r$  by simp
    then have IsBoundedBelow( $\{x \in A. \langle x, a \rangle \in r\}$ ,r)
      by (rule Order_ZF_3_L9)
    then have IsBounded( $\{x \in A. \langle x, a \rangle \in r\}$ ,r)
      using Order_ZF_3_L15 IsBounded_def by simp }
  ultimately show thesis by blast
qed

```

end



### 3 Order\_ZF\_1a.thy

**theory** Order\_ZF\_1a **imports** Order\_ZF

**begin**

This theory is a continuation of `Order_ZF` and talks about maxima and minimum of a set, supremum and infimum and strict (not reflexive) versions of order relations.

#### 3.1 Maximum and minimum of a set

In this section we show that maximum and minimum are unique if they exist. We also show that union of sets that have maxima (minima) has a maximum (minimum). We also show that singletons have maximum and minimum. All this allows to show (in `Finite_ZF`) that every finite set has well-defined maximum and minimum.

For antisymmetric relations maximum of a set is unique if it exists.

**lemma** Order\_ZF\_4\_L1: **assumes** A1: `antisym(r)` **and** A2: `HasAmaximum(r,A)`  
**shows**  $\exists! M. M \in A \wedge (\forall x \in A. \langle x, M \rangle \in r)$

**proof**

**from** A2 **show**  $\exists M. M \in A \wedge (\forall x \in A. \langle x, M \rangle \in r)$

**using** `HasAmaximum_def` **by** `auto`

**fix** M1 M2 **assume**

A2:  $M1 \in A \wedge (\forall x \in A. \langle x, M1 \rangle \in r)$   $M2 \in A \wedge (\forall x \in A. \langle x, M2 \rangle \in r)$

**then have**  $\langle M1, M2 \rangle \in r$   $\langle M2, M1 \rangle \in r$  **by** `auto`

**with** A1 **show**  $M1 = M2$  **by** `(rule Fol1_L4)`

**qed**

For antisymmetric relations minimum of a set is unique if it exists.

**lemma** Order\_ZF\_4\_L2: **assumes** A1: `antisym(r)` **and** A2: `HasAminimum(r,A)`  
**shows**  $\exists! m. m \in A \wedge (\forall x \in A. \langle m, x \rangle \in r)$

**proof**

**from** A2 **show**  $\exists m. m \in A \wedge (\forall x \in A. \langle m, x \rangle \in r)$

**using** `HasAminimum_def` **by** `auto`

**fix** m1 m2 **assume**

A2:  $m1 \in A \wedge (\forall x \in A. \langle m1, x \rangle \in r)$   $m2 \in A \wedge (\forall x \in A. \langle m2, x \rangle \in r)$

**then have**  $\langle m1, m2 \rangle \in r$   $\langle m2, m1 \rangle \in r$  **by** `auto`

**with** A1 **show**  $m1 = m2$  **by** `(rule Fol1_L4)`

**qed**

Maximum of a set has desired properties.

**lemma** Order\_ZF\_4\_L3: **assumes** A1: `antisym(r)` **and** A2: `HasAmaximum(r,A)`  
**shows** `Maximum(r,A) ∈ A`  $\forall x \in A. \langle x, \text{Maximum}(r,A) \rangle \in r$

**proof** -

**let** Max = `THE M. M ∈ A ∧ (∀ x ∈ A. ⟨ x, M ⟩ ∈ r)`

**from** A1 A2 **have**  $\exists! M. M \in A \wedge (\forall x \in A. \langle x, M \rangle \in r)$

```

    by (rule Order_ZF_4_L1)
  then have Max  $\in A \wedge (\forall x \in A. \langle x, \text{Max} \rangle \in r)$ 
    by (rule theI)
  then show Maximum(r,A)  $\in A \wedge (\forall x \in A. \langle x, \text{Maximum}(r,A) \rangle \in r)$ 
    using Maximum_def by auto
qed

```

Minimum of a set has desired properties.

```

lemma Order_ZF_4_L4: assumes A1: antisym(r) and A2: HasAminimum(r,A)
  shows Minimum(r,A)  $\in A \wedge (\forall x \in A. \langle \text{Minimum}(r,A), x \rangle \in r)$ 
proof -
  let Min = THE m. m  $\in A \wedge (\forall x \in A. \langle m, x \rangle \in r)$ 
  from A1 A2 have  $\exists ! m. m \in A \wedge (\forall x \in A. \langle m, x \rangle \in r)$ 
    by (rule Order_ZF_4_L2)
  then have Min  $\in A \wedge (\forall x \in A. \langle \text{Min}, x \rangle \in r)$ 
    by (rule theI)
  then show Minimum(r,A)  $\in A \wedge (\forall x \in A. \langle \text{Minimum}(r,A), x \rangle \in r)$ 
    using Minimum_def by auto
qed

```

For total and transitive relations a union of two sets that have maxima has a maximum.

```

lemma Order_ZF_4_L5:
  assumes A1: r {is total on} (A  $\cup$  B) and A2: trans(r)
  and A3: HasAmaximum(r,A) HasAmaximum(r,B)
  shows HasAmaximum(r,A  $\cup$  B)
proof -
  from A3 obtain M K where
    D1: M  $\in A \wedge (\forall x \in A. \langle x, M \rangle \in r)$  K  $\in B \wedge (\forall x \in B. \langle x, K \rangle \in r)$ 
    using HasAmaximum_def by auto
  let L = GreaterOf(r,M,K)
  from D1 have T1: M  $\in A \cup B$  K  $\in A \cup B$ 
     $\forall x \in A. \langle x, M \rangle \in r \forall x \in B. \langle x, K \rangle \in r$ 
    by auto
  with A1 A2 have  $\forall x \in A \cup B. \langle x, L \rangle \in r$  by (rule Order_ZF_3_L2B)
  moreover from T1 have L  $\in A \cup B$  using GreaterOf_def IsTotal_def
    by simp
  ultimately show HasAmaximum(r,A  $\cup$  B) using HasAmaximum_def by auto
qed

```

For total and transitive relations A union of two sets that have minima has a minimum.

```

lemma Order_ZF_4_L6:
  assumes A1: r {is total on} (A  $\cup$  B) and A2: trans(r)
  and A3: HasAminimum(r,A) HasAminimum(r,B)
  shows HasAminimum(r,A  $\cup$  B)
proof -
  from A3 obtain m k where

```

```

    D1: m ∈ A ∧ (∀x ∈ A. ⟨ m, x ⟩ ∈ r) k ∈ B ∧ (∀x ∈ B. ⟨ k, x ⟩ ∈ r)
    using HasAminimum_def by auto
  let l = SmallerOf(r, m, k)
  from D1 have T1: m ∈ A ∪ B k ∈ A ∪ B
    ∀x ∈ A. ⟨ m, x ⟩ ∈ r ∀x ∈ B. ⟨ k, x ⟩ ∈ r
    by auto
  with A1 A2 have ∀x ∈ A ∪ B. ⟨ l, x ⟩ ∈ r by (rule Order_ZF_3_L5B)
  moreover from T1 have l ∈ A ∪ B using SmallerOf_def IsTotal_def
    by simp
  ultimately show HasAminimum(r, A ∪ B) using HasAminimum_def by auto
qed

```

Set that has a maximum is bounded above.

```

lemma Order_ZF_4_L7:
  assumes HasAmaximum(r, A)
  shows IsBoundedAbove(A, r)
  using assms HasAmaximum_def IsBoundedAbove_def by auto

```

Set that has a minimum is bounded below.

```

lemma Order_ZF_4_L8A:
  assumes HasAminimum(r, A)
  shows IsBoundedBelow(A, r)
  using assms HasAminimum_def IsBoundedBelow_def by auto

```

For reflexive relations singletons have a minimum and maximum.

```

lemma Order_ZF_4_L8: assumes refl(X, r) and a ∈ X
  shows HasAmaximum(r, {a}) HasAminimum(r, {a})
  using assms refl_def HasAmaximum_def HasAminimum_def by auto

```

For total and transitive relations if we add an element to a set that has a maximum, the set still has a maximum.

```

lemma Order_ZF_4_L9:
  assumes A1: r {is total on} X and A2: trans(r)
  and A3: A ⊆ X and A4: a ∈ X and A5: HasAmaximum(r, A)
  shows HasAmaximum(r, A ∪ {a})
proof -
  from A3 A4 have A ∪ {a} ⊆ X by auto
  with A1 have r {is total on} (A ∪ {a})
    using Order_ZF_1_L4 by blast
  moreover from A1 A2 A4 A5 have
    trans(r) HasAmaximum(r, A) by auto
  moreover from A1 A4 have HasAmaximum(r, {a})
    using total_is_refl Order_ZF_4_L8 by blast
  ultimately show HasAmaximum(r, A ∪ {a}) by (rule Order_ZF_4_L5)
qed

```

For total and transitive relations if we add an element to a set that has a minimum, the set still has a minimum.

```

lemma Order_ZF_4_L10:
  assumes A1: r {is total on} X and A2: trans(r)
  and A3:  $A \subseteq X$  and A4:  $a \in X$  and A5: HasAminimum(r,A)
  shows HasAminimum(r,A $\cup\{a\}$ )
proof -
  from A3 A4 have  $A \cup \{a\} \subseteq X$  by auto
  with A1 have r {is total on} (A $\cup\{a\}$ )
    using Order_ZF_1_L4 by blast
  moreover from A1 A2 A4 A5 have
    trans(r) HasAminimum(r,A) by auto
  moreover from A1 A4 have HasAminimum(r,{a})
    using total_is_refl Order_ZF_4_L8 by blast
  ultimately show HasAminimum(r,A $\cup\{a\}$ ) by (rule Order_ZF_4_L6)
qed

```

If the order relation has a property that every nonempty bounded set attains a minimum (for example integers are like that), then every nonempty set bounded below attains a minimum.

```

lemma Order_ZF_4_L11:
  assumes A1: r {is total on} X and
  A2: trans(r) and
  A3:  $r \subseteq X \times X$  and
  A4:  $\forall A. \text{IsBounded}(A,r) \wedge A \neq \emptyset \longrightarrow \text{HasAminimum}(r,A)$  and
  A5:  $B \neq \emptyset$  and A6: IsBoundedBelow(B,r)
  shows HasAminimum(r,B)
proof -
  from A5 obtain b where T:  $b \in B$  by auto
  let L = {x $\in$ B.  $\langle x,b \rangle \in r$ }
  from A3 A6 T have T1:  $b \in X$  using Order_ZF_3_L1B by blast
  with A1 T have T2:  $b \in L$ 
    using total_is_refl refl_def by simp
  then have  $L \neq \emptyset$  by auto
  moreover have IsBounded(L,r)
  proof -
    have  $L \subseteq B$  by auto
    with A6 have IsBoundedBelow(L,r)
      using Order_ZF_3_L12 by simp
    moreover have IsBoundedAbove(L,r)
      by (rule Order_ZF_3_L15)
    ultimately have IsBoundedAbove(L,r)  $\wedge$  IsBoundedBelow(L,r)
      by blast
    then show IsBounded(L,r) using IsBounded_def
      by simp
  qed
  ultimately have IsBounded(L,r)  $\wedge$   $L \neq \emptyset$  by blast
  with A4 have HasAminimum(r,L) by simp
  then obtain m where I:  $m \in L$  and II:  $\forall x \in L. \langle m,x \rangle \in r$ 
    using HasAminimum_def by auto
  then have III:  $\langle m,b \rangle \in r$  by simp

```

```

from I have m ∈ B by simp
moreover have ∀ x ∈ B. ⟨m, x⟩ ∈ r
proof
  fix x assume A7: x ∈ B
  from A3 A6 have B ⊆ X using Order_ZF_3_L1B by blast
  with A1 A7 T1 have x ∈ L ∪ {x ∈ B. ⟨b, x⟩ ∈ r}
    using Order_ZF_1_L5 by simp
  then have x ∈ L ∨ ⟨b, x⟩ ∈ r by auto
  moreover
  { assume x ∈ L
    with II have ⟨m, x⟩ ∈ r by simp }
  moreover
  { assume ⟨b, x⟩ ∈ r
    with A2 III have trans(r) and ⟨m, b⟩ ∈ r ∧ ⟨b, x⟩ ∈ r
  }
by auto
  then have ⟨m, x⟩ ∈ r by (rule Fol1_L3) }
ultimately show ⟨m, x⟩ ∈ r by auto
qed
ultimately show HasAminimum(r, B) using HasAminimum_def
by auto
qed

```

A dual to Order\_ZF\_4\_L11: If the order relation has a property that every nonempty bounded set attains a maximum (for example integers are like that), then every nonempty set bounded above attains a maximum.

```

lemma Order_ZF_4_L11A:
  assumes A1: r {is total on} X and
  A2: trans(r) and
  A3: r ⊆ X × X and
  A4: ∀ A. IsBounded(A, r) ∧ A ≠ 0 ⟶ HasAmaximum(r, A) and
  A5: B ≠ 0 and A6: IsBoundedAbove(B, r)
  shows HasAmaximum(r, B)
proof -
  from A5 obtain b where T: b ∈ B by auto
  let U = {x ∈ B. ⟨b, x⟩ ∈ r}
  from A3 A6 T have T1: b ∈ X using Order_ZF_3_L1A by blast
  with A1 T have T2: b ∈ U
    using total_is_refl refl_def by simp
  then have U ≠ 0 by auto
  moreover have IsBounded(U, r)
  proof -
    have U ⊆ B by auto
    with A6 have IsBoundedAbove(U, r)
      using Order_ZF_3_L13 by blast
    moreover have IsBoundedBelow(U, r)
      using IsBoundedBelow_def by auto
    ultimately have IsBoundedAbove(U, r) ∧ IsBoundedBelow(U, r)
      by blast
    then show IsBounded(U, r) using IsBounded_def
  -

```

```

      by simp
qed
ultimately have IsBounded(U,r)  $\wedge$  U  $\neq$  0 by blast
with A4 have HasAmaximum(r,U) by simp
then obtain m where I: m $\in$ U and II:  $\forall x \in U. \langle x, m \rangle \in r$ 
  using HasAmaximum_def by auto
then have III:  $\langle b, m \rangle \in r$  by simp
from I have m $\in$ B by simp
moreover have  $\forall x \in B. \langle x, m \rangle \in r$ 
proof
  fix x assume A7: x $\in$ B
  from A3 A6 have B $\subseteq$ X using Order_ZF_3_L1A by blast
  with A1 A7 T1 have x  $\in$  {x $\in$ B.  $\langle x, b \rangle \in r$ }  $\cup$  U
    using Order_ZF_1_L5 by simp
  then have x $\in$ U  $\vee$   $\langle x, b \rangle \in r$  by auto
  moreover
  { assume x $\in$ U
    with II have  $\langle x, m \rangle \in r$  by simp }
  moreover
  { assume  $\langle x, b \rangle \in r$ 
    with A2 III have trans(r) and  $\langle x, b \rangle \in r \wedge \langle b, m \rangle \in r$ 
  }
by auto
  then have  $\langle x, m \rangle \in r$  by (rule Fol1_L3) }
ultimately show  $\langle x, m \rangle \in r$  by auto
qed
ultimately show HasAmaximum(r,B) using HasAmaximum_def
  by auto
qed

```

If a set has a minimum and  $L$  is less or equal than all elements of the set, then  $L$  is less or equal than the minimum.

```

lemma Order_ZF_4_L12:
  assumes antisym(r) and HasAminimum(r,A) and  $\forall a \in A. \langle L, a \rangle \in r$ 
  shows  $\langle L, \text{Minimum}(r,A) \rangle \in r$ 
  using assms Order_ZF_4_L4 by simp

```

If a set has a maximum and all its elements are less or equal than  $M$ , then the maximum of the set is less or equal than  $M$ .

```

lemma Order_ZF_4_L13:
  assumes antisym(r) and HasAmaximum(r,A) and  $\forall a \in A. \langle a, M \rangle \in r$ 
  shows  $\langle \text{Maximum}(r,A), M \rangle \in r$ 
  using assms Order_ZF_4_L3 by simp

```

If an element belongs to a set and is greater or equal than all elements of that set, then it is the maximum of that set.

```

lemma Order_ZF_4_L14:
  assumes A1: antisym(r) and A2: M  $\in$  A and
  A3:  $\forall a \in A. \langle a, M \rangle \in r$ 

```

```

    shows Maximum(r,A) = M
  proof -
    from A2 A3 have I: HasAmaximum(r,A) using HasAmaximum_def
    by auto
    with A1 have  $\exists! M. M \in A \wedge (\forall x \in A. \langle x, M \rangle \in r)$ 
    using Order_ZF_4_L1 by simp
    moreover from A2 A3 have  $M \in A \wedge (\forall x \in A. \langle x, M \rangle \in r)$  by simp
    moreover from A1 I have
      Maximum(r,A)  $\in A \wedge (\forall x \in A. \langle x, \text{Maximum}(r,A) \rangle \in r)$ 
    using Order_ZF_4_L3 by simp
    ultimately show Maximum(r,A) = M by auto
  qed

```

If an element belongs to a set and is less or equal than all elements of that set, then it is the minimum of that set.

```

lemma Order_ZF_4_L15:
  assumes A1: antisym(r) and A2:  $m \in A$  and
  A3:  $\forall a \in A. \langle m, a \rangle \in r$ 
  shows Minimum(r,A) = m
proof -
  from A2 A3 have I: HasAminimum(r,A) using HasAminimum_def
  by auto
  with A1 have  $\exists! m. m \in A \wedge (\forall x \in A. \langle m, x \rangle \in r)$ 
  using Order_ZF_4_L2 by simp
  moreover from A2 A3 have  $m \in A \wedge (\forall x \in A. \langle m, x \rangle \in r)$  by simp
  moreover from A1 I have
    Minimum(r,A)  $\in A \wedge (\forall x \in A. \langle \text{Minimum}(r,A), x \rangle \in r)$ 
  using Order_ZF_4_L4 by simp
  ultimately show Minimum(r,A) = m by auto
qed

```

If a set does not have a maximum, then for any its element we can find one that is (strictly) greater.

```

lemma Order_ZF_4_L16:
  assumes A1: antisym(r) and A2: r {is total on} X and
  A3:  $A \subseteq X$  and
  A4:  $\neg \text{HasAmaximum}(r,A)$  and
  A5:  $x \in A$ 
  shows  $\exists y \in A. \langle x, y \rangle \in r \wedge y \neq x$ 
proof -
  { assume A6:  $\forall y \in A. \langle x, y \rangle \notin r \vee y = x$ 
    have  $\forall y \in A. \langle y, x \rangle \in r$ 
    proof
      fix y assume A7:  $y \in A$ 
      with A6 have  $\langle x, y \rangle \notin r \vee y = x$  by simp
      with A2 A3 A5 A7 show  $\langle y, x \rangle \in r$ 
    using IsTotal_def Order_ZF_1_L1 by auto
  }
  qed
  with A5 have  $\exists x \in A. \forall y \in A. \langle y, x \rangle \in r$ 

```

```

      by auto
    with A4 have False using HasAmaximum_def by simp
  } then show  $\exists y \in A. \langle x, y \rangle \in r \wedge y \neq x$  by auto
qed

```

### 3.2 Supremum and Infimum

In this section we consider the notions of supremum and infimum a set.

Elements of the set of upper bounds are indeed upper bounds. Isabelle also thinks it is obvious.

```

lemma Order_ZF_5_L1: assumes  $u \in (\bigcap a \in A. r\{a\})$  and  $a \in A$ 
  shows  $\langle a, u \rangle \in r$ 
  using assms by auto

```

Elements of the set of lower bounds are indeed lower bounds. Isabelle also thinks it is obvious.

```

lemma Order_ZF_5_L2: assumes  $l \in (\bigcap a \in A. r-\{a\})$  and  $a \in A$ 
  shows  $\langle l, a \rangle \in r$ 
  using assms by auto

```

If the set of upper bounds has a minimum, then the supremum is less or equal than any upper bound. We can probably do away with the assumption that  $A$  is not empty, (ab)using the fact that intersection over an empty family is defined in Isabelle to be empty.

```

lemma Order_ZF_5_L3: assumes A1: antisym(r) and A2:  $A \neq 0$  and
  A3: HasAminimum( $r, \bigcap a \in A. r\{a\}$ ) and
  A4:  $\forall a \in A. \langle a, u \rangle \in r$ 
  shows  $\langle \text{Supremum}(r, A), u \rangle \in r$ 
proof -
  let U =  $\bigcap a \in A. r\{a\}$ 
  from A4 have  $\forall a \in A. u \in r\{a\}$  using image_singleton_iff
  by simp
  with A2 have  $u \in U$  by auto
  with A1 A3 show  $\langle \text{Supremum}(r, A), u \rangle \in r$ 
    using Order_ZF_4_L4 Supremum_def by simp
qed

```

Infimum is greater or equal than any lower bound.

```

lemma Order_ZF_5_L4: assumes A1: antisym(r) and A2:  $A \neq 0$  and
  A3: HasAmaximum( $r, \bigcap a \in A. r-\{a\}$ ) and
  A4:  $\forall a \in A. \langle l, a \rangle \in r$ 
  shows  $\langle l, \text{Infimum}(r, A) \rangle \in r$ 
proof -
  let L =  $\bigcap a \in A. r-\{a\}$ 
  from A4 have  $\forall a \in A. l \in r-\{a\}$  using vimage_singleton_iff
  by simp
  with A2 have  $l \in L$  by auto

```



```

with A1 A3 show  $\langle 1, \text{Infimum}(r, A) \rangle \in r$ 
  using Order_ZF_4_L3 Infimum_def by simp
qed

```

If  $z$  is an upper bound for  $A$  and is greater or equal than any other upper bound, then  $z$  is the supremum of  $A$ .

```

lemma Order_ZF_5_L5: assumes A1: antisym(r) and A2:  $A \neq 0$  and
  A3:  $\forall x \in A. \langle x, z \rangle \in r$  and
  A4:  $\forall y. (\forall x \in A. \langle x, y \rangle \in r) \longrightarrow \langle z, y \rangle \in r$ 
  shows
    HasAminimum( $r, \bigcap a \in A. r\{a\}$ )
     $z = \text{Supremum}(r, A)$ 
proof -
  let B =  $\bigcap a \in A. r\{a\}$ 
  from A2 A3 A4 have I:  $z \in B \quad \forall y \in B. \langle z, y \rangle \in r$ 
    by auto
  then show HasAminimum( $r, \bigcap a \in A. r\{a\}$ )
    using HasAminimum_def by auto
  from A1 I show  $z = \text{Supremum}(r, A)$ 
    using Order_ZF_4_L15 Supremum_def by simp
qed

```

If a set has a maximum, then the maximum is the supremum.

```

lemma Order_ZF_5_L6:
  assumes A1: antisym(r) and A2:  $A \neq 0$  and
  A3: HasAmaximum( $r, A$ )
  shows
    HasAminimum( $r, \bigcap a \in A. r\{a\}$ )
     $\text{Maximum}(r, A) = \text{Supremum}(r, A)$ 
proof -
  let M =  $\text{Maximum}(r, A)$ 
  from A1 A3 have I:  $M \in A$  and II:  $\forall x \in A. \langle x, M \rangle \in r$ 
    using Order_ZF_4_L3 by auto
  from I have III:  $\forall y. (\forall x \in A. \langle x, y \rangle \in r) \longrightarrow \langle M, y \rangle \in r$ 
    by simp
  with A1 A2 II show HasAminimum( $r, \bigcap a \in A. r\{a\}$ )
    by (rule Order_ZF_5_L5)
  from A1 A2 II III show  $M = \text{Supremum}(r, A)$ 
    by (rule Order_ZF_5_L5)
qed

```

Properties of supremum of a set for complete relations.

```

lemma Order_ZF_5_L7:
  assumes A1:  $r \subseteq X \times X$  and A2: antisym(r) and
  A3:  $r$  {is complete} and
  A4:  $A \subseteq X \quad A \neq 0$  and A5:  $\exists x \in X. \forall y \in A. \langle y, x \rangle \in r$ 
  shows
     $\text{Supremum}(r, A) \in X$ 
     $\forall x \in A. \langle x, \text{Supremum}(r, A) \rangle \in r$ 

```

```

proof -
  from A5 have IsBoundedAbove(A,r) using IsBoundedAbove_def
    by auto
  with A3 A4 have HasAminimum(r,  $\bigcap a \in A. r\{a\}$ )
    using IsComplete_def by simp
  with A2 have Minimum(r,  $\bigcap a \in A. r\{a\}$ )  $\in$  (  $\bigcap a \in A. r\{a\}$  )
    using Order_ZF_4_L4 by simp
  moreover have Minimum(r,  $\bigcap a \in A. r\{a\}$ ) = Supremum(r,A)
    using Supremum_def by simp
  ultimately have I: Supremum(r,A)  $\in$  (  $\bigcap a \in A. r\{a\}$  )
    by simp
  moreover from A4 obtain a where a  $\in A$  by auto
  ultimately have  $\langle a, \text{Supremum}(r,A) \rangle \in r$  using Order_ZF_5_L1
    by simp
  with A1 show Supremum(r,A)  $\in X$  by auto
  from I show  $\forall x \in A. \langle x, \text{Supremum}(r,A) \rangle \in r$  using Order_ZF_5_L1
    by simp
qed

```

If the relation is a linear order then for any element  $y$  smaller than the supremum of a set we can find one element of the set that is greater than  $y$ .

**lemma Order\_ZF\_5\_L8:**  
 assumes A1:  $r \subseteq X \times X$  and A2: IsLinOrder( $X, r$ ) and  
 A3:  $r$  {is complete} and  
 A4:  $A \subseteq X$   $A \neq 0$  and A5:  $\exists x \in X. \forall y \in A. \langle y, x \rangle \in r$  and  
 A6:  $\langle y, \text{Supremum}(r,A) \rangle \in r$   $y \neq \text{Supremum}(r,A)$   
 shows  $\exists z \in A. \langle y, z \rangle \in r \wedge y \neq z$

```

proof -
  from A2 have
    I: antisym(r) and
    II: trans(r) and
    III: r {is total on} X
    using IsLinOrder_def by auto
  from A1 A6 have T1:  $y \in X$  by auto
  { assume A7:  $\forall z \in A. \langle y, z \rangle \notin r \vee y=z$ 
    from A4 I have antisym(r) and  $A \neq 0$  by auto
    moreover have  $\forall x \in A. \langle x, y \rangle \in r$ 
    proof
      fix x assume A8:  $x \in A$ 
      with A4 have T2:  $x \in X$  by auto
      from A7 A8 have  $\langle y, x \rangle \notin r \vee y=x$  by simp
      with III T1 T2 show  $\langle x, y \rangle \in r$ 
    using IsTotal_def total_is_refl refl_def by auto
    qed
    moreover have  $\forall u. (\forall x \in A. \langle x, u \rangle \in r) \longrightarrow \langle y, u \rangle \in r$ 
    proof-
      { fix u assume A9:  $\forall x \in A. \langle x, u \rangle \in r$ 
        from A4 A5 have IsBoundedAbove(A,r) and  $A \neq 0$ 
          using IsBoundedAbove_def by auto

```

```

with A3 A4 A6 I A9 have
  ⟨y, Supremum(r,A)⟩ ∈ r ∧ ⟨Supremum(r,A), u⟩ ∈ r
  using IsComplete_def Order_ZF_5_L3 by simp
with II have ⟨y,u⟩ ∈ r by (rule Fol1_L3)
} then show ∀u. (∀x∈A. ⟨x,u⟩ ∈ r) ⟶ ⟨y,u⟩ ∈ r
by simp
qed
ultimately have y = Supremum(r,A)
  by (rule Order_ZF_5_L5)
with A6 have False by simp
} then show ∃z∈A. ⟨y,z⟩ ∈ r ∧ y ≠ z by auto
qed

```

### 3.3 Strict versions of order relations

One of the problems with translating formalized mathematics from Metamath to IsarMathLib is that Metamath uses strict orders (of the  $<$  type) while in IsarMathLib we mostly use nonstrict orders (of the  $\leq$  type). This doesn't really make any difference, but is annoying as we have to prove many theorems twice. In this section we prove some theorems to make it easier to translate the statements about strict orders to statements about the corresponding non-strict order and vice versa.

We define a strict version of a relation by removing the  $y = x$  line from the relation.

**definition**

$\text{StrictVersion}(r) \equiv r - \{\langle x, x \rangle. x \in \text{domain}(r)\}$

A reformulation of the definition of a strict version of an order.

**lemma** `def_of_strict_ver`: **shows**

$\langle x, y \rangle \in \text{StrictVersion}(r) \longleftrightarrow \langle x, y \rangle \in r \wedge x \neq y$   
**using** `StrictVersion_def` `domain_def` **by** `auto`

The next lemma is about the strict version of an antisymmetric relation.

**lemma** `strict_of_antisym`:

**assumes** `A1`: `antisym(r)` **and** `A2`:  $\langle a, b \rangle \in \text{StrictVersion}(r)$   
**shows**  $\langle b, a \rangle \notin \text{StrictVersion}(r)$

**proof** -

{ **assume** `A3`:  $\langle b, a \rangle \in \text{StrictVersion}(r)$   
**with** `A2` **have**  $\langle a, b \rangle \in r$  **and**  $\langle b, a \rangle \in r$   
**using** `def_of_strict_ver` **by** `auto`  
**with** `A1` **have**  $a=b$  **by** (rule `Fol1_L4`)  
**with** `A2` **have** `False` **using** `def_of_strict_ver`  
**by** `simp`

} **then show**  $\langle b, a \rangle \notin \text{StrictVersion}(r)$  **by** `auto`

**qed**

The strict version of totality.

```

lemma strict_of_tot:
  assumes r {is total on} X and a∈X b∈X a≠b
  shows ⟨a,b⟩ ∈ StrictVersion(r) ∨ ⟨b,a⟩ ∈ StrictVersion(r)
  using assms IsTotal_def def_of_strict_ver by auto

```

A trichotomy law for the strict version of a total and antisymmetric relation. It is kind of interesting that one does not need the full linear order for this.

```

lemma strict_ans_tot_trich:
  assumes A1: antisym(r) and A2: r {is total on} X
  and A3: a∈X b∈X
  and A4: s = StrictVersion(r)
  shows Exactly_1_of_3_holds(⟨a,b⟩ ∈ s, a=b, ⟨b,a⟩ ∈ s)
proof -
  let p = ⟨a,b⟩ ∈ s
  let q = a=b
  let r = ⟨b,a⟩ ∈ s
  from A2 A3 A4 have p ∨ q ∨ r
    using strict_of_tot by auto
  moreover from A1 A4 have p ⟶ ¬q ∧ ¬r
    using def_of_strict_ver strict_of_antisym by simp
  moreover from A4 have q ⟶ ¬p ∧ ¬r
    using def_of_strict_ver by simp
  moreover from A1 A4 have r ⟶ ¬p ∧ ¬q
    using def_of_strict_ver strict_of_antisym by auto
  ultimately show Exactly_1_of_3_holds(p, q, r)
    by (rule Foll_L5)
qed

```

A trichotomy law for linear order. This is a special case of `strict_ans_tot_trich`.

```

corollary strict_lin_trich: assumes A1: IsLinOrder(X,r) and
  A2: a∈X b∈X and
  A3: s = StrictVersion(r)
  shows Exactly_1_of_3_holds(⟨a,b⟩ ∈ s, a=b, ⟨b,a⟩ ∈ s)
  using assms IsLinOrder_def strict_ans_tot_trich by auto

```

For an antisymmetric relation if a pair is in relation then the reversed pair is not in the strict version of the relation.

```

lemma geq_impl_not_less:
  assumes A1: antisym(r) and A2: ⟨a,b⟩ ∈ r
  shows ⟨b,a⟩ ∉ StrictVersion(r)
proof -
  { assume A3: ⟨b,a⟩ ∈ StrictVersion(r)
    with A2 have ⟨a,b⟩ ∈ StrictVersion(r)
      using def_of_strict_ver by auto
    with A1 A3 have False using strict_of_antisym
      by blast
  } then show ⟨b,a⟩ ∉ StrictVersion(r) by auto
qed

```

If an antisymmetric relation is transitive, then the strict version is also transitive, an explicit version `strict_of_transB` below.

```

lemma strict_of_transA:
  assumes A1: trans(r) and A2: antisym(r) and
  A3: s= StrictVersion(r) and A4: ⟨a,b⟩ ∈ s ⟨b,c⟩ ∈ s
  shows ⟨a,c⟩ ∈ s
proof -
  from A3 A4 have I: ⟨a,b⟩ ∈ r ∧ ⟨b,c⟩ ∈ r
    using def_of_strict_ver by simp
  with A1 have ⟨a,c⟩ ∈ r by (rule Fol1_L3)
  moreover
  { assume a=c
    with I have ⟨a,b⟩ ∈ r and ⟨b,a⟩ ∈ r by auto
    with A2 have a=b by (rule Fol1_L4)
    with A3 A4 have False using def_of_strict_ver by simp
  } then have a≠c by auto
  ultimately have ⟨a,c⟩ ∈ StrictVersion(r)
    using def_of_strict_ver by simp
  with A3 show thesis by simp
qed

```

If an antisymmetric relation is transitive, then the strict version is also transitive.

```

lemma strict_of_transB:
  assumes A1: trans(r) and A2: antisym(r)
  shows trans(StrictVersion(r))
proof -
  let s = StrictVersion(r)
  from A1 A2 have
    ∀ x y z. ⟨x, y⟩ ∈ s ∧ ⟨y, z⟩ ∈ s ⟶ ⟨x, z⟩ ∈ s
    using strict_of_transA by blast
  then show trans(StrictVersion(r)) by (rule Fol1_L2)
qed

```

The next lemma provides a condition that is satisfied by the strict version of a relation if the original relation is a complete linear order.

```

lemma strict_of_compl:
  assumes A1: r ⊆ X×X and A2: IsLinOrder(X,r) and
  A3: r {is complete} and
  A4: A⊆X A≠0 and A5: s = StrictVersion(r) and
  A6: ∃u∈X. ∀y∈A. ⟨y,u⟩ ∈ s
  shows
    ∃x∈X. ( ∀y∈A. ⟨x,y⟩ ∉ s ) ∧ (∀y∈X. ⟨y,x⟩ ∈ s ⟶ (∃z∈A. ⟨y,z⟩ ∈ s))
proof -
  let x = Supremum(r,A)
  from A2 have I: antisym(r) using IsLinOrder_def
    by simp
  moreover from A5 A6 have ∃u∈X. ∀y∈A. ⟨y,u⟩ ∈ r

```

```

    using def_of_strict_ver by auto
  moreover note A1 A3 A4
  ultimately have II:  $x \in X \quad \forall y \in A. \langle y, x \rangle \in r$ 
    using Order_ZF_5_L7 by auto
  then have III:  $\exists x \in X. \forall y \in A. \langle y, x \rangle \in r$  by auto
  from A5 I II have  $x \in X \quad \forall y \in A. \langle x, y \rangle \notin s$ 
    using geq_impl_not_less by auto
  moreover from A1 A2 A3 A4 A5 III have
     $\forall y \in X. \langle y, x \rangle \in s \longrightarrow (\exists z \in A. \langle y, z \rangle \in s)$ 
    using def_of_strict_ver Order_ZF_5_L8 by simp
  ultimately show
     $\exists x \in X. ( \forall y \in A. \langle x, y \rangle \notin s ) \wedge ( \forall y \in X. \langle y, x \rangle \in s \longrightarrow (\exists z \in A. \langle y, z \rangle \in s) )$ 
    by auto
qed

```

Strict version of a relation on a set is a relation on that set.

```

lemma strict_ver_rel: assumes A1:  $r \subseteq A \times A$ 
  shows  $\text{StrictVersion}(r) \subseteq A \times A$ 
  using assms StrictVersion_def by auto

```

end

## 4 NatOrder\_ZF.thy

**theory** NatOrder\_ZF **imports** Nat\_ZF\_IML Order\_ZF

**begin**

This theory proves that  $\leq$  is a linear order on  $\mathbb{N}$ .  $\leq$  is defined in Isabelle's Nat theory, and linear order is defined in Order\_ZF theory. Contributed by Seo Sanghyeon.

### 4.1 Order on natural numbers

This is the only section in this theory.

To prove that  $\leq$  is a total order, we use a result on ordinals.

```
lemma NatOrder_ZF_1_L1:
  assumes a $\in$ nat and b $\in$ nat
  shows a  $\leq$  b  $\vee$  b  $\leq$  a
proof -
  from assms have I: Ord(a)  $\wedge$  Ord(b)
    using nat_into_Ord by auto
  then have a  $\in$  b  $\vee$  a = b  $\vee$  b  $\in$  a
    using Ord_linear by simp
  with I have a < b  $\vee$  a = b  $\vee$  b < a
    using ltI by auto
  with I show a  $\leq$  b  $\vee$  b  $\leq$  a
    using le_iff by auto
qed
```

$\leq$  is antisymmetric, transitive, total, and linear. Proofs by rewrite using definitions.

```
lemma NatOrder_ZF_1_L2:
  shows
    antisym(Le)
    trans(Le)
    Le {is total on} nat
    IsLinOrder(nat,Le)
proof -
  show antisym(Le)
    using antisym_def Le_def le_anti_sym by auto
  moreover show trans(Le)
    using trans_def Le_def le_trans by blast
  moreover show Le {is total on} nat
    using IsTotal_def Le_def NatOrder_ZF_1_L1 by simp
  ultimately show IsLinOrder(nat,Le)
    using IsLinOrder_def by simp
qed
```

The order on natural numbers is linear on every natural number. Recall that each natural number is a subset of the set of all natural numbers (as well as a member).

```
lemma natord_lin_on_each_nat:
  assumes A1:  $n \in \text{nat}$  shows IsLinOrder( $n, \text{Le}$ )
proof -
  from A1 have  $n \subseteq \text{nat}$  using nat_subset_nat
  by simp
  then show thesis using NatOrder_ZF_1_L2 ord_linear_subset
  by blast
qed
end
```



## 5 func\_ZF.thy

```
theory func_ZF imports func1
```

```
begin
```

In this theory we consider properties of functions that are binary operations, that is they map  $X \times X$  into  $X$ .

### 5.1 Lifting operations to a function space

It happens quite often that we have a binary operation on some set and we need a similar operation that is defined for functions on that set. For example once we know how to add real numbers we also know how to add real-valued functions: for  $f, g : X \rightarrow \mathbf{R}$  we define  $(f + g)(x) = f(x) + g(x)$ . Note that formally the  $+$  means something different on the left hand side of this equality than on the right hand side. This section aims at formalizing this process. We will call it "lifting to a function space", if you have a suggestion for a better name, please let me know.

Since we are writing in generic set notation, the definition below is a bit complicated. Here it what it says: Given a set  $X$  and another set  $f$  (that represents a binary function on  $X$ ) we are defining  $f$  lifted to function space over  $X$  as the binary function (a set of pairs) on the space  $F = X \rightarrow \text{range}(f)$  such that the value of this function on pair  $\langle a, b \rangle$  of functions on  $X$  is another function  $c$  on  $X$  with values defined by  $c(x) = f\langle a(x), b(x) \rangle$ .

#### definition

```
Lift2FcnSpce (infix {lifted to function space over} 65) where
  f {lifted to function space over} X  $\equiv$ 
    { $\langle p, \{x, f(\text{fst}(p)(x), \text{snd}(p)(x))\}. x \in X \rangle$ .
       $p \in (X \rightarrow \text{range}(f)) \times (X \rightarrow \text{range}(f))$ }
```

The result of the lift belongs to the function space.

```
lemma func_ZF_1_L1:
```

```
  assumes A1: f : Y×Y→Y
  and A2: p ∈ (X→range(f))×(X→range(f))
  shows
    { $\langle x, f(\text{fst}(p)(x), \text{snd}(p)(x)) \rangle. x \in X \} : X \rightarrow \text{range}(f)$ 
  proof -
    have  $\forall x \in X. f(\text{fst}(p)(x), \text{snd}(p)(x)) \in \text{range}(f)$ 
    proof
      fix x assume x∈X
      let p =  $\langle \text{fst}(p)(x), \text{snd}(p)(x) \rangle$ 
      from A2 'x∈X' have
        fst(p)(x) ∈ range(f)  snd(p)(x) ∈ range(f)
    using apply_type by auto
    with A1 have p ∈ Y×Y
```

```

using func1_1_L5B by blast
  with A1 have  $\langle p, f(p) \rangle \in f$ 
using apply_Pair by simp
  with A1 show
 $f(p) \in \text{range}(f)$ 
using rangeI by simp
  qed
then show thesis using ZF_fun_from_total by simp
qed

```

The values of the lift are defined by the value of the liftee in a natural way.

```

lemma func_ZF_1_L2:
  assumes A1:  $f : Y \times Y \rightarrow Y$ 
  and A2:  $p \in (X \rightarrow \text{range}(f)) \times (X \rightarrow \text{range}(f))$  and A3:  $x \in X$ 
  and A4:  $P = \{\langle x, f(\text{fst}(p)(x), \text{snd}(p)(x)) \rangle \mid x \in X\}$ 
  shows  $P(x) = f(\text{fst}(p)(x), \text{snd}(p)(x))$ 
proof -
  from A1 A2 have
     $\{\langle x, f(\text{fst}(p)(x), \text{snd}(p)(x)) \rangle \mid x \in X\} : X \rightarrow \text{range}(f)$ 
  using func_ZF_1_L1 by simp
  with A4 have  $P : X \rightarrow \text{range}(f)$  by simp
  with A3 A4 show  $P(x) = f(\text{fst}(p)(x), \text{snd}(p)(x))$ 
    using ZF_fun_from_tot_val by simp
qed

```

Function lifted to a function space results in function space operator.

```

theorem func_ZF_1_L3:
  assumes  $f : Y \times Y \rightarrow Y$ 
  and  $F = f \text{ \{lifted to function space over\} } X$ 
  shows  $F : (X \rightarrow \text{range}(f)) \times (X \rightarrow \text{range}(f)) \rightarrow (X \rightarrow \text{range}(f))$ 
  using assms Lift2FcnSpce_def func_ZF_1_L1 ZF_fun_from_total
  by simp

```

The values of the lift are defined by the values of the liftee in the natural way.

```

theorem func_ZF_1_L4:
  assumes A1:  $f : Y \times Y \rightarrow Y$ 
  and A2:  $F = f \text{ \{lifted to function space over\} } X$ 
  and A3:  $s : X \rightarrow \text{range}(f)$   $r : X \rightarrow \text{range}(f)$ 
  and A4:  $x \in X$ 
  shows  $(F(s, r))(x) = f(s(x), r(x))$ 
proof -
  let  $p = \langle s, r \rangle$ 
  let  $P = \{\langle x, f(\text{fst}(p)(x), \text{snd}(p)(x)) \rangle \mid x \in X\}$ 
  from A1 A3 A4 have
     $f : Y \times Y \rightarrow Y$   $p \in (X \rightarrow \text{range}(f)) \times (X \rightarrow \text{range}(f))$ 
     $x \in X$   $P = \{\langle x, f(\text{fst}(p)(x), \text{snd}(p)(x)) \rangle \mid x \in X\}$ 
  by auto
  then have  $P(x) = f(\text{fst}(p)(x), \text{snd}(p)(x))$ 

```

```

    by (rule func_ZF_1_L2)
  hence  $P(x) = f\langle s(x), r(x) \rangle$  by auto
  moreover have  $P = F\langle s, r \rangle$ 
  proof -
    from A1 A2 have  $F : (X \rightarrow \text{range}(f)) \times (X \rightarrow \text{range}(f)) \rightarrow (X \rightarrow \text{range}(f))$ 
    using func_ZF_1_L3 by simp
    moreover from A3 have  $p \in (X \rightarrow \text{range}(f)) \times (X \rightarrow \text{range}(f))$ 
    by auto
    moreover from A2 have
       $F = \{ \langle p, \{ \langle x, f(\text{fst}(p)(x), \text{snd}(p)(x)) \rangle \}. x \in X \} \}.$ 
       $p \in (X \rightarrow \text{range}(f)) \times (X \rightarrow \text{range}(f)) \}$ 
    using Lift2FcnSpce_def by simp
    ultimately show thesis using ZF_fun_from_tot_val
    by simp
  qed
  ultimately show  $(F\langle s, r \rangle)(x) = f\langle s(x), r(x) \rangle$  by auto
qed

```

## 5.2 Associative and commutative operations

In this section we define associative and commutative operations and prove that they remain such when we lift them to a function space.

Typically we say that a binary operation  $\cdot$  on a set  $G$  is "associative" if  $(x \cdot y) \cdot z = x \cdot (y \cdot z)$  for all  $x, y, z \in G$ . Our actual definition below does not use the multiplicative notation so that we can apply it equally to the additive notation  $+$  or whatever infix symbol we may want to use. Instead, we use the generic set theory notation and write  $P\langle x, y \rangle$  to denote the value of the operation  $P$  on a pair  $\langle x, y \rangle \in G \times G$ .

### definition

```

IsAssociative (infix {is associative on} 65) where
P {is associative on} G  $\equiv P : G \times G \rightarrow G \wedge$ 
 $(\forall x \in G. \forall y \in G. \forall z \in G.$ 
 $( P(\langle P(\langle x, y \rangle), z) = P(\langle x, P(\langle y, z \rangle) \rangle) ) )$ 

```

A binary function  $f : X \times X \rightarrow Y$  is commutative if  $f\langle x, y \rangle = f\langle y, x \rangle$ . Note that in the definition of associativity above we talk about binary "operation" and here we say use the term binary "function". This is not set in stone, but usually the word "operation" is used when the range is a factor of the domain, while the word "function" allows the range to be a completely unrelated set.

### definition

```

IsCommutative (infix {is commutative on} 65) where
f {is commutative on} G  $\equiv \forall x \in G. \forall y \in G. f\langle x, y \rangle = f\langle y, x \rangle$ 

```

The lift of a commutative function is commutative.

**lemma** func\_ZF\_2\_L1:

```

assumes A1: f : G×G→G
and A2: F = f {lifted to function space over} X
and A3: s : X→range(f) r : X→range(f)
and A4: f {is commutative on} G
shows F⟨s,r⟩ = F⟨r,s⟩
proof -
  from A1 A2 have
    F : (X→range(f))×(X→range(f))→(X→range(f))
    using func_ZF_1_L3 by simp
  with A3 have
    F⟨s,r⟩ : X→range(f) and F⟨r,s⟩ : X→range(f)
    using apply_type by auto
  moreover have
    ∀x∈X. (F⟨s,r⟩)(x) = (F⟨r,s⟩)(x)
  proof
    fix x assume x∈X
    from A1 have range(f)⊆G
      using func1_1_L5B by simp
    with A3 'x∈X' have s(x) ∈ G and r(x) ∈ G
      using apply_type by auto
    with A1 A2 A3 A4 'x∈X' show
      (F⟨s,r⟩)(x) = (F⟨r,s⟩)(x)
      using func_ZF_1_L4 IsCommutative_def by simp
    qed
  ultimately show thesis using fun_extension_iff
    by simp
qed

```

The lift of a commutative function is commutative on the function space.

```

lemma func_ZF_2_L2:
  assumes f : G×G→G
  and f {is commutative on} G
  and F = f {lifted to function space over} X
  shows F {is commutative on} (X→range(f))
  using assms IsCommutative_def func_ZF_2_L1 by simp

```

The lift of an associative function is associative.

```

lemma func_ZF_2_L3:
  assumes A2: F = f {lifted to function space over} X
  and A3: s : X→range(f) r : X→range(f) q : X→range(f)
  and A4: f {is associative on} G
  shows F⟨F⟨s,r⟩,q⟩ = F⟨s,F⟨r,q⟩⟩
proof -
  from A4 A2 have
    F : (X→range(f))×(X→range(f))→(X→range(f))
    using IsAssociative_def func_ZF_1_L3 by auto
  with A3 have I:
    F⟨s,r⟩ : X→range(f)
    F⟨r,q⟩ : X→range(f)

```

```

    F⟨F⟨s,r⟩,q⟩ : X→range(f)
    F⟨s,F⟨r,q⟩⟩ : X→range(f)
    using apply_type by auto
  moreover have
    ∀x∈X. (F⟨F⟨s,r⟩,q⟩)(x) = (F⟨s,F⟨r,q⟩⟩)(x)
  proof
    fix x assume x∈X
    from A4 have f:G×G→G
      using IsAssociative_def by simp
    then have range(f)⊆G
      using func1_1_L5B by simp
    with A3 'x∈X' have
      s(x) ∈ G r(x) ∈ G q(x) ∈ G
      using apply_type by auto
    with A2 I A3 A4 'x∈X' 'f:G×G→G' show
      (F⟨F⟨s,r⟩,q⟩)(x) = (F⟨s,F⟨r,q⟩⟩)(x)
      using func_ZF_1_L4 IsAssociative_def by simp
  qed
  ultimately show thesis using fun_extension_iff
    by simp
qed

```

The lift of an associative function is associative on the function space.

```

lemma func_ZF_2_L4:
  assumes A1: f {is associative on} G
  and A2: F = f {lifted to function space over} X
  shows F {is associative on} (X→range(f))
proof -
  from A1 A2 have
    F : (X→range(f))×(X→range(f))→(X→range(f))
    using IsAssociative_def func_ZF_1_L3 by auto
  moreover from A1 A2 have
    ∀s ∈ X→range(f). ∀ r ∈ X→range(f). ∀ q ∈ X→range(f).
    F⟨F⟨s,r⟩,q⟩ = F⟨s,F⟨r,q⟩⟩
    using func_ZF_2_L3 by simp
  ultimately show thesis using IsAssociative_def
    by simp
qed

```

### 5.3 Restricting operations

In this section we consider conditions under which restriction of the operation to a set inherits properties like commutativity and associativity.

The commutativity is inherited when restricting a function to a set.

```

lemma func_ZF_4_L1:
  assumes A1: f:X×X→Y and A2: A⊆X
  and A3: f {is commutative on} X
  shows restrict(f,A×A) {is commutative on} A

```

```

proof -
  { fix x y assume x∈A and y∈A
    with A2 have x∈X and y∈X by auto
    with A3 'x∈A' 'y∈A' have
      restrict(f,A×A)⟨x,y⟩ = restrict(f,A×A)⟨y,x⟩
      using IsCommutative_def restrict_if by simp }
    then show thesis using IsCommutative_def by simp
qed

```

Next we define what it means that a set is closed with respect to an operation.

**definition**

```

IsOpClosed (infix {is closed under} 65) where
  A {is closed under} f ≡ ∀x∈A. ∀y∈A. f⟨x,y⟩ ∈ A

```

Associative operation restricted to a set that is closed with resp. to this operation is associative.

```

lemma func_ZF_4_L2: assumes A1: f {is associative on} X
  and A2: A⊆X and A3: A {is closed under} f
  and A4: x∈A y∈A z∈A
  and A5: g = restrict(f,A×A)
  shows g⟨g⟨x,y⟩,z⟩ = g⟨x,g⟨y,z⟩⟩

```

```

proof -
  from A4 A2 have I: x∈X y∈X z∈X
    by auto
  from A3 A4 A5 have
    g⟨g⟨x,y⟩,z⟩ = f⟨f⟨x,y⟩,z⟩
    g⟨x,g⟨y,z⟩⟩ = f⟨x,f⟨y,z⟩⟩
    using IsOpClosed_def restrict_if by auto
  moreover from A1 I have
    f⟨f⟨x,y⟩,z⟩ = f⟨x,f⟨y,z⟩⟩
    using IsAssociative_def by simp
  ultimately show thesis by simp
qed

```

An associative operation restricted to a set that is closed with resp. to this operation is associative on the set.

```

lemma func_ZF_4_L3: assumes A1: f {is associative on} X
  and A2: A⊆X and A3: A {is closed under} f
  shows restrict(f,A×A) {is associative on} A

```

```

proof -
  let g = restrict(f,A×A)
  from A1 have f:X×X→X
    using IsAssociative_def by simp
  moreover from A2 have A×A ⊆ X×X by auto
  moreover from A3 have ∀p ∈ A×A. g(p) ∈ A
    using IsOpClosed_def restrict_if by auto
  ultimately have g : A×A→A

```

```

    using func1_2_L4 by simp
  moreover from A1 A2 A3 have
     $\forall x \in A. \forall y \in A. \forall z \in A.$ 
     $g\langle g\langle x, y \rangle, z \rangle = g\langle x, g\langle y, z \rangle \rangle$ 
    using func_ZF_4_L2 by simp
  ultimately show thesis
    using IsAssociative_def by simp
qed

```

The essential condition to show that if a set  $A$  is closed with respect to an operation, then it is closed under this operation restricted to any superset of  $A$ .

```

lemma func_ZF_4_L4: assumes A {is closed under} f
  and A ⊆ B and x ∈ A y ∈ A and g = restrict(f, B × B)
  shows g⟨x, y⟩ ∈ A
  using assms IsOpClosed_def restrict by auto

```

If a set  $A$  is closed under an operation, then it is closed under this operation restricted to any superset of  $A$ .

```

lemma func_ZF_4_L5:
  assumes A1: A {is closed under} f
  and A2: A ⊆ B
  shows A {is closed under} restrict(f, B × B)
proof -
  let g = restrict(f, B × B)
  from A1 A2 have  $\forall x \in A. \forall y \in A. g\langle x, y \rangle \in A$ 
    using func_ZF_4_L4 by simp
  then show thesis using IsOpClosed_def by simp
qed

```

The essential condition to show that intersection of sets that are closed with respect to an operation is closed with respect to the operation.

```

lemma func_ZF_4_L6:
  assumes A {is closed under} f
  and B {is closed under} f
  and x ∈ A ∩ B y ∈ A ∩ B
  shows f⟨x, y⟩ ∈ A ∩ B using assms IsOpClosed_def by auto

```

Intersection of sets that are closed with respect to an operation is closed under the operation.

```

lemma func_ZF_4_L7:
  assumes A {is closed under} f
  B {is closed under} f
  shows A ∩ B {is closed under} f
  using assms IsOpClosed_def by simp

```

## 5.4 Compositions

For any set  $X$  we can consider a binary operation on the set of functions  $f : X \rightarrow X$  defined by  $C(f, g) = f \circ g$ . Composition of functions (or relations) is defined in the standard Isabelle distribution as a higher order function and denoted with the letter  $\circ$ . In this section we consider the corresponding two-argument ZF-function (binary operation), that is a subset of  $((X \rightarrow X) \times (X \rightarrow X)) \times (X \rightarrow X)$ .

We define the notion of composition on the set  $X$  as the binary operation on the function space  $X \rightarrow X$  that takes two functions and creates the their composition.

**definition**

```
Composition(X)  $\equiv$ 
  {⟨p, fst(p)  $\circ$  snd(p)⟩. p  $\in$  (X $\rightarrow$ X)  $\times$  (X $\rightarrow$ X)}
```

Composition operation is a function that maps  $(X \rightarrow X) \times (X \rightarrow X)$  into  $X \rightarrow X$ .

```
lemma func_ZF_5_L1: shows Composition(X) : (X $\rightarrow$ X)  $\times$  (X $\rightarrow$ X)  $\rightarrow$  (X $\rightarrow$ X)
  using comp_fun Composition_def ZF_fun_from_total by simp
```

The value of the composition operation is the composition of arguments.

```
lemma func_ZF_5_L2: assumes f:X $\rightarrow$ X and g:X $\rightarrow$ X
  shows Composition(X)⟨f,g⟩ = f  $\circ$  g
proof -
  from assms have
    Composition(X) : (X $\rightarrow$ X)  $\times$  (X $\rightarrow$ X)  $\rightarrow$  (X $\rightarrow$ X)
    ⟨f,g⟩  $\in$  (X $\rightarrow$ X)  $\times$  (X $\rightarrow$ X)
    Composition(X) = {⟨p, fst(p)  $\circ$  snd(p)⟩. p  $\in$  (X $\rightarrow$ X)  $\times$  (X $\rightarrow$ X)}
    using func_ZF_5_L1 Composition_def by auto
  then show Composition(X)⟨f,g⟩ = f  $\circ$  g
    using ZF_fun_from_tot_val by auto
qed
```

What is the value of a composition on an argument?

```
lemma func_ZF_5_L3: assumes f:X $\rightarrow$ X and g:X $\rightarrow$ X and x $\in$ X
  shows (Composition(X)⟨f,g⟩)(x) = f(g(x))
  using assms func_ZF_5_L2 comp_fun_apply by simp
```

The essential condition to show that composition is associative.

```
lemma func_ZF_5_L4: assumes A1: f:X $\rightarrow$ X g:X $\rightarrow$ X h:X $\rightarrow$ X
  and A2: C = Composition(X)
  shows C⟨C⟨f,g⟩,h⟩ = C⟨ f,C⟨g,h⟩⟩
proof -
  from A2 have C : ((X $\rightarrow$ X)  $\times$  (X $\rightarrow$ X))  $\rightarrow$  (X $\rightarrow$ X)
    using func_ZF_5_L1 by simp
  with A1 have I:
```



```

    C⟨f,g⟩ : X→X
    C⟨g,h⟩ : X→X
    C⟨C⟨f,g⟩,h⟩ : X→X
    C⟨ f,C⟨g,h⟩⟩ : X→X
    using apply_funtype by auto
  moreover have
    ∀ x ∈ X. C⟨C⟨f,g⟩,h⟩(x) = C⟨f,C⟨g,h⟩⟩(x)
  proof
    fix x assume x∈X
    with A1 A2 I have
      C⟨C⟨f,g⟩,h⟩ (x) = f(g(h(x)))
      C⟨ f,C⟨g,h⟩⟩(x) = f(g(h(x)))
      using func_ZF_5_L3 apply_funtype by auto
    then show C⟨C⟨f,g⟩,h⟩(x) = C⟨ f,C⟨g,h⟩⟩(x)
      by simp
    qed
  ultimately show thesis using fun_extension_iff by simp
qed

```

Composition is an associative operation on  $X \rightarrow X$  (the space of functions that map  $X$  into itself).

```

lemma func_ZF_5_L5: shows Composition(X) {is associative on} (X→X)
proof -
  let C = Composition(X)
  have ∀f∈X→X. ∀g∈X→X. ∀h∈X→X.
    C⟨C⟨f,g⟩,h⟩ = C⟨f,C⟨g,h⟩⟩
    using func_ZF_5_L4 by simp
  then show thesis using func_ZF_5_L1 IsAssociative_def
    by simp
qed

```

## 5.5 Identity function

In this section we show some additional facts about the identity function defined in the standard Isabelle's Perm theory.

A function that maps every point to itself is the identity on its domain.

```

lemma identity_fun: assumes A1: f:X→Y and A2:∀x∈X. f(x)=x
  shows f = id(X)
proof -
  from assms have f:X→Y and id(X):X→X and ∀x∈X. f(x) = id(X)(x)
    using id_type id_conv by auto
  then show thesis by (rule func_eq)
qed

```

Composing a function with identity does not change the function.

```

lemma func_ZF_6_L1A: assumes A1: f : X→X
  shows Composition(X)⟨f,id(X)⟩ = f

```

```

Composition(X)⟨id(X),f⟩ = f
proof -
  have Composition(X) : (X→X)×(X→X)→(X→X)
    using func_ZF_5_L1 by simp
  with A1 have Composition(X)⟨id(X),f⟩ : X→X
    Composition(X)⟨f,id(X)⟩ : X→X
    using id_type apply_funtype by auto
  moreover note A1
  moreover from A1 have
    ∀x∈X. (Composition(X)⟨id(X),f⟩)(x) = f(x)
    ∀x∈X. (Composition(X)⟨f,id(X)⟩)(x) = f(x)
    using id_type func_ZF_5_L3 apply_funtype id_conv
    by auto
  ultimately show Composition(X)⟨id(X),f⟩ = f
    Composition(X)⟨f,id(X)⟩ = f
    using fun_extension_iff by auto
qed

```

A trivial fact: identity is the only function from a singleton to itself.

```

lemma singleton_fun_id: shows ({x} → {x}) = {id({x})}
proof
  show {id({x})} ⊆ ({x} → {x})
    using id_def by simp
  { let g = id({x})
    fix f assume f : {x} → {x}
    then have f : {x} → {x} and g : {x} → {x}
      using id_def by auto
    moreover from 'f : {x} → {x}' have ∀x ∈ {x}. f(x) = g(x)
      using apply_funtype id_def by auto
    ultimately have f = g by (rule func_eq)
  } then show ({x} → {x}) ⊆ {id({x})} by auto
qed

```

Another trivial fact: identity is the only bijection of a singleton with itself.

```

lemma single_bij_id: shows bij({x},{x}) = {id({x})}
proof
  show {id({x})} ⊆ bij({x},{x}) using id_bij
    by simp
  { fix f assume f ∈ bij({x},{x})
    then have f : {x} → {x} using bij_is_fun
      by simp
    then have f ∈ {id({x})} using singleton_fun_id
      by simp
  } then show bij({x},{x}) ⊆ {id({x})} by auto
qed

```

A kind of induction for the identity: if a function  $f$  is the identity on a set with a fixpoint of  $f$  removed, then it is the identity on the whole set.

```

lemma id_fixpoint_rem: assumes A1: f:X→X and

```

```

A2: p ∈ X and A3: f(p) = p and
A4: restrict(f, X-{p}) = id(X-{p})
shows f = id(X)
proof -
  from A1 have f: X → X and id(X) : X → X
    using id_def by auto
  moreover
  { fix x assume x ∈ X
    { assume x ∈ X-{p}
      then have f(x) = restrict(f, X-{p})(x)
    }
  }
  using restrict by simp
  with A4 'x ∈ X-{p}' have f(x) = x
  using id_def by simp
  with A2 A3 'x ∈ X' have f(x) = x by auto
} then have ∀ x ∈ X. f(x) = id(X)(x)
  using id_def by simp
ultimately show f = id(X) by (rule func_eq)
qed

```

## 5.6 Lifting to subsets

Suppose we have a binary operation  $f : X \times X \rightarrow X$  written additively as  $f\langle x, y \rangle = x + y$ . Such operation naturally defines another binary operation on the subsets of  $X$  that satisfies  $A + B = \{x + y : x \in A, y \in B\}$ . This new operation which we will call " $f$  lifted to subsets" inherits many properties of  $f$ , such as associativity, commutativity and existence of the neutral element. This notion is useful for considering interval arithmetics.

The next definition describes the notion of a binary operation lifted to subsets. It is written in a way that might be a bit unexpected, but really it is the same as the intuitive definition, but shorter. In the definition we take a pair  $p \in \text{Pow}(X) \times \text{Pow}(X)$ , say  $p = \langle A, B \rangle$ , where  $A, B \subseteq X$ . Then we assign this pair of sets the set  $\{f\langle x, y \rangle : x \in A, y \in B\} = \{f(x') : x' \in A \times B\}$ . The set on the right hand side is the same as the image of  $A \times B$  under  $f$ . In the definition we don't use  $A$  and  $B$  symbols, but write  $\text{fst}(p)$  and  $\text{snd}(p)$ , resp. Recall that in Isabelle/ZF  $\text{fst}(p)$  and  $\text{snd}(p)$  denote the first and second components of an ordered pair  $p$ . See the lemma `lift_subsets_explained` for a more intuitive notation.

### definition

```

Lift2Subsets (infix {lifted to subsets of} 65) where
f {lifted to subsets of} X ≡
{⟨p, f(fst(p) × snd(p))⟩. p ∈ Pow(X) × Pow(X)}

```

The lift to subsets defines a binary operation on the subsets.

```

lemma lift_subsets_binop: assumes A1: f : X × X → Y
  shows (f {lifted to subsets of} X) : Pow(X) × Pow(X) → Pow(Y)
proof -

```

```

let F = {⟨p, f(fst(p)×snd(p))⟩. p ∈ Pow(X)×Pow(X)}
from A1 have ∀p ∈ Pow(X) × Pow(X). f(fst(p)×snd(p)) ∈ Pow(Y)
  using func1_1_L6 by simp
then have F : Pow(X) × Pow(X) → Pow(Y)
  by (rule ZF_fun_from_total)
then show thesis unfolding Lift2Subsets_def by simp
qed

```

The definition of the lift to subsets rewritten in a more intuitive notation. We would like to write the last assertion as  $F\langle A, B \rangle = \{f\langle x, y \rangle. x \in A, y \in B\}$ , but Isabelle/ZF does not allow such syntax.

```

lemma lift_subsets_explained: assumes A1: f : X×X → Y
  and A2: A ⊆ X B ⊆ X and A3: F = f {lifted to subsets of} X
  shows
    F⟨A,B⟩ ⊆ Y and
    F⟨A,B⟩ = f(A×B)
    F⟨A,B⟩ = {f(p). p ∈ A×B}
    F⟨A,B⟩ = {f⟨x,y⟩ . ⟨x,y⟩ ∈ A×B}
proof -
  let p = ⟨A,B⟩
  from assms have
    I: F : Pow(X) × Pow(X) → Pow(Y) and p ∈ Pow(X) × Pow(X)
    using lift_subsets_binop by auto
  moreover from A3 have F = {⟨p, f(fst(p)×snd(p))⟩. p ∈ Pow(X)×Pow(X)}
    unfolding Lift2Subsets_def by simp
  ultimately show F⟨A,B⟩ = f(A×B)
    using ZF_fun_from_tot_val by auto
  also
  from A1 A2 have A×B ⊆ X×X by auto
  with A1 have f(A×B) = {f(p). p ∈ A×B}
    by (rule func_imagedef)
  finally show F⟨A,B⟩ = {f(p) . p ∈ A×B} by simp
  also
  have ∀x∈A. ∀y ∈ B. f⟨x,y⟩ = f⟨x,y⟩ by simp
  then have {f(p). p ∈ A×B} = {f⟨x,y⟩. ⟨x,y⟩ ∈ A×B}
    by (rule ZF1_1_L4A)
  finally show F⟨A,B⟩ = {f⟨x,y⟩ . ⟨x,y⟩ ∈ A×B}
    by simp
  from A2 I show F⟨A,B⟩ ⊆ Y using apply_funtype by blast
qed

```

A sufficient condition for a point to belong to a result of lifting to subsets.

```

lemma lift_subset_suff: assumes A1: f : X × X → Y and
  A2: A ⊆ X B ⊆ X and A3: x∈A y∈B and
  A4: F = f {lifted to subsets of} X
  shows f⟨x,y⟩ ∈ F⟨A,B⟩
proof -
  from A3 have f⟨x,y⟩ ∈ {f(p) . p ∈ A×B} by auto
  moreover from A1 A2 A4 have {f(p). p ∈ A×B} = F⟨A,B⟩

```

```

    using lift_subsets_explained by simp
    ultimately show  $f\langle x, y \rangle \in F\langle A, B \rangle$  by simp
qed

```

A kind of converse of `lift_subset_apply`, providing a necessary condition for a point to be in the result of lifting to subsets.

```

lemma lift_subset_nec: assumes A1:  $f : X \times X \rightarrow Y$  and
  A2:  $A \subseteq X$   $B \subseteq X$  and
  A3:  $F = f$  {lifted to subsets of}  $X$  and
  A4:  $z \in F\langle A, B \rangle$ 
  shows  $\exists x y. x \in A \wedge y \in B \wedge z = f\langle x, y \rangle$ 
proof -
  from A1 A2 A3 have  $F\langle A, B \rangle = \{f(p). p \in A \times B\}$ 
    using lift_subsets_explained by simp
  with A4 show thesis by auto
qed

```

Lifting to subsets inherits commutativity.

```

lemma lift_subset_comm: assumes A1:  $f : X \times X \rightarrow Y$  and
  A2:  $f$  {is commutative on}  $X$  and
  A3:  $F = f$  {lifted to subsets of}  $X$ 
  shows  $F$  {is commutative on}  $\text{Pow}(X)$ 
proof -
  have  $\forall A \in \text{Pow}(X). \forall B \in \text{Pow}(X). F\langle A, B \rangle = F\langle B, A \rangle$ 
  proof -
    { fix A assume  $A \in \text{Pow}(X)$ 
      fix B assume  $B \in \text{Pow}(X)$ 
      have  $F\langle A, B \rangle = F\langle B, A \rangle$ 
      proof -
        have  $\forall z \in F\langle A, B \rangle. z \in F\langle B, A \rangle$ 
        proof
          fix z assume I:  $z \in F\langle A, B \rangle$ 
          with A1 A3 ' $A \in \text{Pow}(X)$ ' ' $B \in \text{Pow}(X)$ ' have
             $\exists x y. x \in A \wedge y \in B \wedge z = f\langle x, y \rangle$ 
            using lift_subset_nec by simp
          then obtain x y where  $x \in A$  and  $y \in B$  and  $z = f\langle x, y \rangle$ 
            by auto
          with A2 ' $A \in \text{Pow}(X)$ ' ' $B \in \text{Pow}(X)$ ' have  $z = f\langle y, x \rangle$ 
            using IsCommutative_def by auto
          with A1 A3 I ' $A \in \text{Pow}(X)$ ' ' $B \in \text{Pow}(X)$ ' ' $x \in A$ ' ' $y \in B$ '
            show  $z \in F\langle B, A \rangle$  using lift_subset_suff by simp
        qed
      qed
    }
  qed
  moreover have  $\forall z \in F\langle B, A \rangle. z \in F\langle A, B \rangle$ 
  proof
    fix z assume I:  $z \in F\langle B, A \rangle$ 
    with A1 A3 ' $A \in \text{Pow}(X)$ ' ' $B \in \text{Pow}(X)$ ' have
       $\exists x y. x \in B \wedge y \in A \wedge z = f\langle x, y \rangle$ 
      using lift_subset_nec by simp
    then obtain x y where  $x \in B$  and  $y \in A$  and  $z = f\langle x, y \rangle$ 

```

```

    by auto
  with A2 'A ∈ Pow(X)' 'B ∈ Pow(X)' have z = f⟨y,x⟩
    using IsCommutative_def by auto
  with A1 A3 I 'A ∈ Pow(X)' 'B ∈ Pow(X)' 'x∈B' 'y∈A'
  show z ∈ F⟨A,B⟩ using lift_subset_suff by simp
qed
ultimately show F⟨A,B⟩ = F⟨B,A⟩ by auto
qed
} thus thesis by auto
qed
then show F {is commutative on} Pow(X)
  unfolding IsCommutative_def by auto
qed

```

Lifting to subsets inherits associativity. To show that  $F\langle\langle A, B \rangle C\rangle = F\langle A, F\langle B, C \rangle\rangle$  we prove two inclusions and the proof of the second inclusion is very similar to the proof of the first one.

```

lemma lift_subset_assoc: assumes A1: f : X × X → X and
  A2: f {is associative on} X and
  A3: F = f {lifted to subsets of} X
  shows F {is associative on} Pow(X)
proof -
  from A1 A3 have F : Pow(X) × Pow(X) → Pow(X)
    using lift_subsets_binop by simp
  moreover have ∀ A ∈ Pow(X). ∀ B ∈ Pow(X). ∀ C ∈ Pow(X).
    F⟨F⟨A,B⟩,C⟩ = F⟨A,F⟨B,C⟩⟩
  proof -
    { fix A B C
      assume A ∈ Pow(X) B ∈ Pow(X) C ∈ Pow(X)
      have F⟨F⟨A,B⟩,C⟩ ⊆ F⟨A,F⟨B,C⟩⟩
      proof
fix z assume I: z ∈ F⟨F⟨A,B⟩,C⟩
from A1 A3 'A ∈ Pow(X)' 'B ∈ Pow(X)'
have F⟨A,B⟩ ∈ Pow(X)
  using lift_subsets_binop apply_funtype by blast
with A1 A3 'C ∈ Pow(X)' I have
  ∃ x y. x ∈ F⟨A,B⟩ ∧ y ∈ C ∧ z = f⟨x,y⟩
  using lift_subset_nec by simp
then obtain x y where
  II: x ∈ F⟨A,B⟩ and y ∈ C and III: z = f⟨x,y⟩
  by auto
from A1 A3 'A ∈ Pow(X)' 'B ∈ Pow(X)' II have
  ∃ s t. s ∈ A ∧ t ∈ B ∧ x = f⟨s,t⟩
  using lift_subset_nec by auto
then obtain s t where s∈A and t∈B and x = f⟨s,t⟩
  by auto
with A2 'A ∈ Pow(X)' 'B ∈ Pow(X)' 'C ∈ Pow(X)' III
  's∈A' 't∈B' 'y∈C' have IV: z = f⟨s, f⟨t,y⟩⟩
  using IsAssociative_def by blast

```

```

from A1 A3 'B ∈ Pow(X)' 'C ∈ Pow(X)' 't∈B' 'y∈C'
have f⟨t,y⟩ ∈ F⟨B,C⟩ using lift_subset_suff by simp
moreover from A1 A3 'B ∈ Pow(X)' 'C ∈ Pow(X)'
have F⟨B,C⟩ ⊆ X using lift_subsets_binop apply_funtype
  by blast
moreover note A1 A3 'A ∈ Pow(X)' 's∈A' IV
ultimately show z ∈ F⟨A,F⟨B,C⟩⟩
  using lift_subset_suff by simp
  qed
  moreover have F⟨A,F⟨B,C⟩⟩ ⊆ F⟨F⟨A,B⟩,C⟩
  proof
fix z assume I: z ∈ F⟨A,F⟨B,C⟩⟩
from A1 A3 'B ∈ Pow(X)' 'C ∈ Pow(X)'
have F⟨B,C⟩ ∈ Pow(X)
  using lift_subsets_binop apply_funtype by blast
with A1 A3 'A ∈ Pow(X)' I have
  ∃x y. x ∈ A ∧ y ∈ F⟨B,C⟩ ∧ z = f⟨x,y⟩
  using lift_subset_nec by simp
then obtain x y where
  x ∈ A and II: y ∈ F⟨B,C⟩ and III: z = f⟨x,y⟩
  by auto
from A1 A3 'B ∈ Pow(X)' 'C ∈ Pow(X)' II have
  ∃ s t. s ∈ B ∧ t ∈ C ∧ y = f⟨s,t⟩
  using lift_subset_nec by auto
then obtain s t where s∈B and t∈C and y = f⟨s,t⟩
  by auto
with III have z = f⟨x,f⟨s,t⟩⟩ by simp
moreover from A2 'A ∈ Pow(X)' 'B ∈ Pow(X)' 'C ∈ Pow(X)'
  'x∈A' 's∈B' 't∈C' have f⟨f⟨x,s⟩,t⟩ = f⟨x,f⟨s,t⟩⟩
  using IsAssociative_def by blast
ultimately have IV: z = f⟨f⟨x,s⟩,t⟩ by simp
from A1 A3 'A ∈ Pow(X)' 'B ∈ Pow(X)' 'x∈A' 's∈B'
have f⟨x,s⟩ ∈ F⟨A,B⟩ using lift_subset_suff by simp
moreover from A1 A3 'A ∈ Pow(X)' 'B ∈ Pow(X)'
have F⟨A,B⟩ ⊆ X using lift_subsets_binop apply_funtype
  by blast
moreover note A1 A3 'C ∈ Pow(X)' 't∈C' IV
ultimately show z ∈ F⟨F⟨A,B⟩,C⟩
  using lift_subset_suff by simp
  qed
  ultimately have F⟨F⟨A,B⟩,C⟩ = F⟨A,F⟨B,C⟩⟩ by auto
} thus thesis by auto
qed
ultimately show thesis unfolding IsAssociative_def
  by auto
qed

```

## 5.7 Distributive operations

In this section we deal with pairs of operations such that one is distributive with respect to the other, that is  $a \cdot (b + c) = a \cdot b + a \cdot c$  and  $(b + c) \cdot a = b \cdot a + c \cdot a$ . We show that this property is preserved under restriction to a set closed with respect to both operations. In `EquivClass1` theory we show that this property is preserved by projections to the quotient space if both operations are congruent with respect to the equivalence relation.

We define distributivity as a statement about three sets. The first set is the set on which the operations act. The second set is the additive operation (a ZF function) and the third is the multiplicative operation.

**definition**

```
IsDistributive(X,A,M) ≡ (∀ a∈X.∀ b∈X.∀ c∈X.
  M⟨a,A⟨b,c⟩⟩ = A⟨M⟨a,b⟩,M⟨a,c⟩⟩ ∧
  M⟨A⟨b,c⟩,a⟩ = A⟨M⟨b,a⟩,M⟨c,a⟩⟩)
```

The essential condition to show that distributivity is preserved by restrictions to sets that are closed with respect to both operations.

**lemma** `func_ZF_7_L1`:

```
  assumes A1: IsDistributive(X,A,M)
  and A2: Y⊆X
  and A3: Y {is closed under} A  Y {is closed under} M
  and A4: Ar = restrict(A,Y×Y) Mr = restrict(M,Y×Y)
  and A5: a∈Y  b∈Y  c∈Y
  shows Mr⟨ a,Ar⟨b,c⟩ ⟩ = Ar⟨ Mr⟨a,b⟩,Mr⟨a,c⟩ ⟩ ∧
  Mr⟨ Ar⟨b,c⟩,a ⟩ = Ar⟨ Mr⟨b,a⟩, Mr⟨c,a⟩ ⟩
proof -
  from A3 A5 have A⟨b,c⟩ ∈ Y  M⟨a,b⟩ ∈ Y  M⟨a,c⟩ ∈ Y
  M⟨b,a⟩ ∈ Y  M⟨c,a⟩ ∈ Y using IsOpClosed_def by auto
  with A5 A4 have
    Ar⟨b,c⟩ ∈ Y  Mr⟨a,b⟩ ∈ Y  Mr⟨a,c⟩ ∈ Y
    Mr⟨b,a⟩ ∈ Y  Mr⟨c,a⟩ ∈ Y
    using restrict by auto
  with A1 A2 A4 A5 show thesis
    using restrict IsDistributive_def by auto
qed
```

Distributivity is preserved by restrictions to sets that are closed with respect to both operations.

**lemma** `func_ZF_7_L2`:

```
  assumes IsDistributive(X,A,M)
  and Y⊆X
  and Y {is closed under} A
  Y {is closed under} M
  and Ar = restrict(A,Y×Y) Mr = restrict(M,Y×Y)
  shows IsDistributive(Y,Ar,Mr)
proof -
```



```

from assms have  $\forall a \in Y. \forall b \in Y. \forall c \in Y.$ 
   $M_r \langle a, A_r \langle b, c \rangle \rangle = A_r \langle M_r \langle a, b \rangle, M_r \langle a, c \rangle \rangle \wedge$ 
   $M_r \langle A_r \langle b, c \rangle, a \rangle = A_r \langle M_r \langle b, a \rangle, M_r \langle c, a \rangle \rangle$ 
  using func_ZF_7_L1 by simp
  then show thesis using IsDistributive_def by simp
qed

end

```

## 6 func\_ZF\_1.thy

**theory** func\_ZF\_1 **imports** Order Order\_ZF\_1a func\_ZF

**begin**

In this theory we consider some properties of functions related to order relations

### 6.1 Functions and order

This section deals with functions between ordered sets.

If every value of a function on a set is bounded below by a constant, then the image of the set is bounded below.

**lemma** func\_ZF\_8\_L1:  
  **assumes**  $f:X \rightarrow Y$  **and**  $A \subseteq X$  **and**  $\forall x \in A. \langle L, f(x) \rangle \in r$   
  **shows**  $\text{IsBoundedBelow}(f(A), r)$   
**proof** -  
  **from** **assms** **have**  $\forall y \in f(A). \langle L, y \rangle \in r$   
    **using** func\_imagedef **by** simp  
  **then show**  $\text{IsBoundedBelow}(f(A), r)$   
    **by** (rule Order\_ZF\_3\_L9)  
**qed**

If every value of a function on a set is bounded above by a constant, then the image of the set is bounded above.

**lemma** func\_ZF\_8\_L2:  
  **assumes**  $f:X \rightarrow Y$  **and**  $A \subseteq X$  **and**  $\forall x \in A. \langle f(x), U \rangle \in r$   
  **shows**  $\text{IsBoundedAbove}(f(A), r)$   
**proof** -  
  **from** **assms** **have**  $\forall y \in f(A). \langle y, U \rangle \in r$   
    **using** func\_imagedef **by** simp  
  **then show**  $\text{IsBoundedAbove}(f(A), r)$   
    **by** (rule Order\_ZF\_3\_L10)  
**qed**

Identity is an order isomorphism.

**lemma** id\_ord\_iso: **shows**  $\text{id}(X) \in \text{ord\_iso}(X, r, X, r)$   
  **using** id\_bij id\_def ord\_iso\_def **by** simp

Identity is the only order automorphism of a singleton.

**lemma** id\_ord\_auto\_singleton:  
  **shows**  $\text{ord\_iso}(\{x\}, r, \{x\}, r) = \{\text{id}(\{x\})\}$   
  **using** id\_ord\_iso ord\_iso\_def single\_bij\_id  
  **by** auto

The image of a maximum by an order isomorphism is a maximum. Note that from the fact the  $r$  is antisymmetric and  $f$  is an order isomorphism

between  $(A, r)$  and  $(B, R)$  we can not conclude that  $R$  is antisymmetric (we can only show that  $R \cap (B \times B)$  is).

```

lemma max_image_ord_iso:
  assumes A1: antisym(r) and A2: antisym(R) and
  A3: f ∈ ord_iso(A,r,B,R) and
  A4: HasAmaximum(r,A)
  shows HasAmaximum(R,B) and Maximum(R,B) = f(Maximum(r,A))
proof -
  let M = Maximum(r,A)
  from A1 A4 have M ∈ A using Order_ZF_4_L3 by simp
  from A3 have f:A→B using ord_iso_def bij_is_fun
    by simp
  with 'M ∈ A' have I: f(M) ∈ B
    using apply_funtype by simp
  { fix y assume y ∈ B
    let x = converse(f)(y)
    from A3 have converse(f) ∈ ord_iso(B,R,A,r)
      using ord_iso_sym by simp
    then have converse(f): B → A
      using ord_iso_def bij_is_fun by simp
    with 'y ∈ B' have x ∈ A
      by simp
    with A1 A3 A4 'x ∈ A' 'M ∈ A' have ⟨f(x), f(M)⟩ ∈ R
      using Order_ZF_4_L3 ord_iso_apply by simp
    with A3 'y ∈ B' have ⟨y, f(M)⟩ ∈ R
      using right_inverse_bij ord_iso_def by auto
  } then have II: ∀y ∈ B. ⟨y, f(M)⟩ ∈ R by simp
  with A2 I show Maximum(R,B) = f(M)
    by (rule Order_ZF_4_L14)
  from I II show HasAmaximum(R,B)
    using HasAmaximum_def by auto
qed

```

Maximum is a fixpoint of order automorphism.

```

lemma max_auto_fixpoint:
  assumes antisym(r) and f ∈ ord_iso(A,r,A,r)
  and HasAmaximum(r,A)
  shows Maximum(r,A) = f(Maximum(r,A))
  using assms max_image_ord_iso by blast

```

If two sets are order isomorphic and we remove  $x$  and  $f(x)$ , respectively, from the sets, then they are still order isomorphic.

```

lemma ord_iso_rem_point:
  assumes A1: f ∈ ord_iso(A,r,B,R) and A2: a ∈ A
  shows restrict(f,A-{a}) ∈ ord_iso(A-{a},r,B-{f(a)},R)
proof -
  let f0 = restrict(f,A-{a})
  have A-{a} ⊆ A by auto

```

```

with A1 have f0 ∈ ord_iso(A-{a},r,f(A-{a}),R)
  using ord_iso_restrict_image by simp
moreover
from A1 have f ∈ inj(A,B)
  using ord_iso_def bij_def by simp
with A2 have f(A-{a}) = f(A) - f{a}
  using inj_image_dif by simp
moreover from A1 have f(A) = B
  using ord_iso_def bij_def surj_range_image_domain
  by auto
moreover
from A1 have f: A→B
  using ord_iso_def bij_is_fun by simp
with A2 have f{a} = {f(a)}
  using singleton_image by simp
ultimately show thesis by simp
qed

```

If two sets are order isomorphic and we remove maxima from the sets, then they are still order isomorphic.

```

corollary ord_iso_rem_max:
  assumes A1: antisym(r) and f ∈ ord_iso(A,r,B,R) and
  A4: HasAmaximum(r,A) and A5: M = Maximum(r,A)
  shows restrict(f,A-{M}) ∈ ord_iso(A-{M}, r, B-{f(M)},R)
  using assms Order_ZF_4_L3 ord_iso_rem_point by simp

```

Lemma about extending order isomorphisms by adding one point to the domain.

```

lemma ord_iso_extend: assumes A1: f ∈ ord_iso(A,r,B,R) and
  A2: MA ∉ A MB ∉ B and
  A3: ∀a∈A. ⟨a, MA⟩ ∈ r ∀b∈B. ⟨b, MB⟩ ∈ R and
  A4: antisym(r) antisym(R) and
  A5: ⟨MA,MA⟩ ∈ r ⟷ ⟨MB,MB⟩ ∈ R
  shows f ∪ {⟨ MA,MB⟩} ∈ ord_iso(A∪{MA},r,B∪{MB},R)

```

**proof -**

```

let g = f ∪ {⟨ MA,MB⟩}
from A1 A2 have
  g : A∪{MA} → B∪{MB} and
  I: ∀x∈A. g(x) = f(x) and II: g(MA) = MB
  using ord_iso_def bij_def inj_def func1_1_L11D
  by auto

```

```

from A1 A2 have g ∈ bij(A∪{MA},B∪{MB})
  using ord_iso_def bij_extend_point by simp
moreover have ∀x ∈ A∪{MA}. ∀ y ∈ A∪{MA}.
  ⟨x,y⟩ ∈ r ⟷ ⟨g(x), g(y)⟩ ∈ R

```

**proof -**

```

{ fix x y
  assume x ∈ A∪{MA} and y ∈ A∪{MA}
  then have x∈A ∧ y ∈ A ∨ x∈A ∧ y = MA ∨

```

```

x = MA ∧ y ∈ A ∨ x = MA ∧ y = MA
by auto
  moreover
    { assume x ∈ A ∧ y ∈ A
with A1 I have ⟨x,y⟩ ∈ r ⟷ ⟨g(x), g(y)⟩ ∈ R
  using ord_iso_def by simp }
  moreover
    { assume x ∈ A ∧ y = MA
with A1 A3 I II have ⟨x,y⟩ ∈ r ⟷ ⟨g(x), g(y)⟩ ∈ R
  using ord_iso_def bij_def inj_def apply_funtype
  by auto }
  moreover
    { assume x = MA ∧ y ∈ A
with A2 A3 A4 have ⟨x,y⟩ ∉ r
  using antisym_def by auto
moreover
  { assume A6: ⟨g(x), g(y)⟩ ∈ R
    from A1 I II 'x = MA ∧ y ∈ A' have
      III: g(y) ∈ B g(x) = MB
      using ord_iso_def bij_def inj_def apply_funtype
      by auto
    with A3 have ⟨g(y), g(x)⟩ ∈ R by simp
    with A4 A6 have g(y) = g(x) using antisym_def
      by auto
    with A2 III have False by simp
  } hence ⟨g(x), g(y)⟩ ∉ R by auto
ultimately have ⟨x,y⟩ ∈ r ⟷ ⟨g(x), g(y)⟩ ∈ R
by simp }
  moreover
    { assume x = MA ∧ y = MA
with A5 II have ⟨x,y⟩ ∈ r ⟷ ⟨g(x), g(y)⟩ ∈ R
  by simp }
  ultimately have ⟨x,y⟩ ∈ r ⟷ ⟨g(x), g(y)⟩ ∈ R
by auto
} thus thesis by auto
qed
ultimately show thesis using ord_iso_def
  by simp
qed

```

A kind of converse to `ord_iso_rem_max`: if two linearly ordered sets are order isomorphic after removing the maxima, then they are order isomorphic.

```

lemma rem_max_ord_iso:
  assumes A1: IsLinOrder(X,r) IsLinOrder(Y,R) and
  A2: HasAmaximum(r,X) HasAmaximum(R,Y)
  ord_iso(X - {Maximum(r,X)},r,Y - {Maximum(R,Y)},R) ≠ 0
  shows ord_iso(X,r,Y,R) ≠ 0
proof -

```

```

let MA = Maximum(r,X)
let A = X - {MA}
let MB = Maximum(R,Y)
let B = Y - {MB}
from A2 obtain f where f ∈ ord_iso(A,r,B,R)
  by auto
moreover have MA ∉ A and MB ∉ B
  by auto
moreover from A1 A2 have
  ∀a∈A. ⟨a,MA⟩ ∈ r and ∀b∈B. ⟨b,MB⟩ ∈ R
  using IsLinOrder_def Order_ZF_4_L3 by auto
moreover from A1 have antisym(r) and antisym(R)
  using IsLinOrder_def by auto
moreover from A1 A2 have ⟨MA,MA⟩ ∈ r ⟷ ⟨MB,MB⟩ ∈ R
  using IsLinOrder_def Order_ZF_4_L3 IsLinOrder_def
  total_is_refl refl_def by auto
ultimately have
  f ∪ {⟨MA,MB⟩} ∈ ord_iso(A∪{MA},r,B∪{MB},R)
  by (rule ord_iso_extend)
moreover from A1 A2 have
  A∪{MA} = X and B∪{MB} = Y
  using IsLinOrder_def Order_ZF_4_L3 by auto
ultimately show ord_iso(X,r,Y,R) ≠ 0
  using ord_iso_extend by auto
qed

```

## 6.2 Projections in cartesian products

In this section we consider maps arising naturally in cartesian products.

There is a natural bijection between  $X = Y \times \{y\}$  (a "slice") and  $Y$ . We will call this the `SliceProjection`( $Y \times \{y\}$ ). This is really the ZF equivalent of the meta-function `fst(x)`.

**definition**

$\text{SliceProjection}(X) \equiv \{\langle p, \text{fst}(p) \rangle. p \in X\}$

A slice projection is a bijection between  $X \times \{y\}$  and  $X$ .

**lemma slice\_proj\_bij: shows**

$\text{SliceProjection}(X \times \{y\}): X \times \{y\} \rightarrow X$   
 $\text{domain}(\text{SliceProjection}(X \times \{y\})) = X \times \{y\}$   
 $\forall p \in X \times \{y\}. \text{SliceProjection}(X \times \{y\})(p) = \text{fst}(p)$   
 $\text{SliceProjection}(X \times \{y\}) \in \text{bij}(X \times \{y\}, X)$

**proof -**

let P =  $\text{SliceProjection}(X \times \{y\})$   
have  $\forall p \in X \times \{y\}. \text{fst}(p) \in X$  by simp  
moreover from this have  
 $\{\langle p, \text{fst}(p) \rangle. p \in X \times \{y\}\} : X \times \{y\} \rightarrow X$   
by (rule ZF\_fun\_from\_total)  
ultimately show

```

I: P: X×{y} → X and II: ∀p∈X×{y}. P(p) = fst(p)
using ZF_fun_from_tot_val SliceProjection_def by auto
hence
  ∀a ∈ X×{y}. ∀ b ∈ X×{y}. P(a) = P(b) → a=b
  by auto
with I have P ∈ inj(X×{y},X) using inj_def
  by simp
moreover from II have ∀x∈X. ∃p∈X×{y}. P(p) = x
  by simp
with I have P ∈ surj(X×{y},X) using surj_def
  by simp
ultimately show P ∈ bij(X×{y},X)
  using bij_def by simp
from I show domain(SliceProjection(X×{y})) = X×{y}
  using func1_1_L1 by simp
qed

```

### 6.3 Induced relations and order isomorphisms

When we have two sets  $X, Y$ , function  $f : X \rightarrow Y$  and a relation  $R$  on  $Y$  we can define a relation  $r$  on  $X$  by saying that  $x r y$  if and only if  $f(x) R f(y)$ . This is especially interesting when  $f$  is a bijection as all reasonable properties of  $R$  are inherited by  $r$ . This section treats mostly the case when  $R$  is an order relation and  $f$  is a bijection. The standard Isabelle's `Order` theory defines the notion of a space of order isomorphisms between two sets relative to a relation. We expand that material proving that order isomorphisms preserve interesting properties of the relation.

We call the relation created by a relation on  $Y$  and a mapping  $f : X \rightarrow Y$  the `InducedRelation(f,R)`.

**definition**

```

InducedRelation(f,R) ≡
{p ∈ domain(f)×domain(f). ⟨f(fst(p)),f(snd(p))⟩ ∈ R}

```

A reformulation of the definition of the relation induced by a function.

```

lemma def_of_ind_relA:
  assumes ⟨x,y⟩ ∈ InducedRelation(f,R)
  shows ⟨f(x),f(y)⟩ ∈ R
  using assms InducedRelation_def by simp

```

A reformulation of the definition of the relation induced by a function, kind of converse of `def_of_ind_relA`.

```

lemma def_of_ind_relB: assumes f:A→B and
  x∈A y∈A and ⟨f(x),f(y)⟩ ∈ R
  shows ⟨x,y⟩ ∈ InducedRelation(f,R)
  using assms func1_1_L1 InducedRelation_def by simp

```

A property of order isomorphisms that is missing from standard Isabelle's `Order.thy`.

```
lemma ord_iso_apply_conv:
  assumes f ∈ ord_iso(A,r,B,R) and
  ⟨f(x),f(y)⟩ ∈ R and x∈A y∈A
  shows ⟨x,y⟩ ∈ r
  using assms ord_iso_def by simp
```

The next lemma tells us where the induced relation is defined

```
lemma ind_rel_domain:
  assumes R ⊆ B×B and f:A→B
  shows InducedRelation(f,R) ⊆ A×A
  using assms func1_1_L1 InducedRelation_def
  by auto
```

A bijection is an order homomorphisms between a relation and the induced one.

```
lemma bij_is_ord_iso: assumes A1: f ∈ bij(A,B)
  shows f ∈ ord_iso(A,InducedRelation(f,R),B,R)
proof -
  let r = InducedRelation(f,R)
  { fix x y assume A2: x∈A y∈A
    have ⟨x,y⟩ ∈ r ⟷ ⟨f(x),f(y)⟩ ∈ R
    proof
      assume ⟨x,y⟩ ∈ r then show ⟨f(x),f(y)⟩ ∈ R
    using def_of_ind_relA by simp
    next assume ⟨f(x),f(y)⟩ ∈ R
      with A1 A2 show ⟨x,y⟩ ∈ r
    using bij_is_fun def_of_ind_relB by blast
    qed }
  with A1 show f ∈ ord_iso(A,InducedRelation(f,R),B,R)
  using ord_isoI by simp
qed
```

An order isomorphism preserves antisymmetry.

```
lemma ord_iso_pres_antisym: assumes A1: f ∈ ord_iso(A,r,B,R) and
  A2: r ⊆ A×A and A3: antisym(R)
  shows antisym(r)
proof -
  { fix x y
    assume A4: ⟨x,y⟩ ∈ r ⟨y,x⟩ ∈ r
    from A1 have f ∈ inj(A,B)
      using ord_iso_is_bij bij_is_inj by simp
    moreover
    from A1 A2 A4 have
      ⟨f(x), f(y)⟩ ∈ R and ⟨f(y), f(x)⟩ ∈ R
      using ord_iso_apply by auto
    with A3 have f(x) = f(y) by (rule Fol1_L4)
```



```

    moreover from A2 A4 have  $x \in A \quad y \in A$  by auto
    ultimately have  $x=y$  by (rule inj_apply_equality)
  } then have  $\forall x y. \langle x,y \rangle \in r \wedge \langle y,x \rangle \in r \longrightarrow x=y$  by auto
  then show antisym(r) using imp_conj antisym_def
  by simp
qed

```

Order isomorphisms preserve transitivity.

```

lemma ord_iso_pres_trans: assumes A1:  $f \in \text{ord\_iso}(A,r,B,R)$  and
  A2:  $r \subseteq A \times A$  and A3:  $\text{trans}(R)$ 
  shows  $\text{trans}(r)$ 
proof -
  { fix x y z
    assume A4:  $\langle x, y \rangle \in r \quad \langle y, z \rangle \in r$ 
    note A1
    moreover
    from A1 A2 A4 have
       $\langle f(x), f(y) \rangle \in R \wedge \langle f(y), f(z) \rangle \in R$ 
      using ord_iso_apply by auto
    with A3 have  $\langle f(x), f(z) \rangle \in R$  by (rule Fol1_L3)
    moreover from A2 A4 have  $x \in A \quad z \in A$  by auto
    ultimately have  $\langle x, z \rangle \in r$  using ord_iso_apply_conv
    by simp
  } then have  $\forall x y z. \langle x, y \rangle \in r \wedge \langle y, z \rangle \in r \longrightarrow \langle x, z \rangle \in r$ 
  by blast
  then show  $\text{trans}(r)$  by (rule Fol1_L2)
qed

```

Order isomorphisms preserve totality.

```

lemma ord_iso_pres_tot: assumes A1:  $f \in \text{ord\_iso}(A,r,B,R)$  and
  A2:  $r \subseteq A \times A$  and A3:  $R \text{ {is total on} } B$ 
  shows  $r \text{ {is total on} } A$ 
proof -
  { fix x y
    assume  $x \in A \quad y \in A \quad \langle x,y \rangle \notin r$ 
    with A1 have  $\langle f(x), f(y) \rangle \notin R$  using ord_iso_apply_conv
    by auto
    moreover
    from A1 have  $f:A \rightarrow B$  using ord_iso_is_bij bij_is_fun
    by simp
    with A3 ' $x \in A$ ' ' $y \in A$ ' have
       $\langle f(x), f(y) \rangle \in R \vee \langle f(y), f(x) \rangle \in R$ 
      using apply_funtype IsTotal_def by simp
    ultimately have  $\langle f(y), f(x) \rangle \in R$  by simp
    with A1 ' $x \in A$ ' ' $y \in A$ ' have  $\langle y,x \rangle \in r$ 
    using ord_iso_apply_conv by simp
  } then have  $\forall x \in A. \forall y \in A. \langle x,y \rangle \in r \vee \langle y,x \rangle \in r$ 
  by blast
  then show  $r \text{ {is total on} } A$  using IsTotal_def

```

by simp  
qed

Order isomorphisms preserve linearity.

lemma ord\_iso\_pres\_lin: assumes  $f \in \text{ord\_iso}(A, r, B, R)$  and  
 $r \subseteq A \times A$  and  $\text{IsLinOrder}(B, R)$   
shows  $\text{IsLinOrder}(A, r)$   
using assms ord\_iso\_pres\_antisym ord\_iso\_pres\_trans ord\_iso\_pres\_tot  
 $\text{IsLinOrder\_def}$  by simp

If a relation is a linear order, then the relation induced on another set by a bijection is also a linear order.

lemma ind\_rel\_pres\_lin:  
assumes A1:  $f \in \text{bij}(A, B)$  and A2:  $\text{IsLinOrder}(B, R)$   
shows  $\text{IsLinOrder}(A, \text{InducedRelation}(f, R))$   
proof -  
let  $r = \text{InducedRelation}(f, R)$   
from A1 have  $f \in \text{ord\_iso}(A, r, B, R)$  and  $r \subseteq A \times A$   
using bij\_is\_ord\_iso domain\_of\_bij InducedRelation\_def  
by auto  
with A2 show  $\text{IsLinOrder}(A, r)$  using ord\_iso\_pres\_lin  
by simp  
qed

The image by an order isomorphism of a bounded above and nonempty set is bounded above.

lemma ord\_iso\_pres\_bound\_above:  
assumes A1:  $f \in \text{ord\_iso}(A, r, B, R)$  and A2:  $r \subseteq A \times A$  and  
A3:  $\text{IsBoundedAbove}(C, r)$   $C \neq \emptyset$   
shows  $\text{IsBoundedAbove}(f(C), R)$   $f(C) \neq \emptyset$   
proof -  
from A3 obtain  $u$  where I:  $\forall x \in C. \langle x, u \rangle \in r$   
using IsBoundedAbove\_def by auto  
from A1 have  $f: A \rightarrow B$  using ord\_iso\_is\_bij bij\_is\_fun  
by simp  
from A2 A3 have  $C \subseteq A$  using Order\_ZF\_3\_L1A by blast  
from A3 obtain  $x$  where  $x \in C$  by auto  
with A2 I have  $u \in A$  by auto  
{ fix  $y$  assume  $y \in f(C)$   
with ' $f: A \rightarrow B$ ' ' $C \subseteq A$ ' obtain  $x$  where  $x \in C$  and  $y = f(x)$   
using func\_imagedef by auto  
with A1 I ' $C \subseteq A$ ' ' $u \in A$ ' have  $\langle y, f(u) \rangle \in R$   
using ord\_iso\_apply by auto  
} then have  $\forall y \in f(C). \langle y, f(u) \rangle \in R$  by simp  
then show  $\text{IsBoundedAbove}(f(C), R)$  by (rule Order\_ZF\_3\_L10)  
from A3 ' $f: A \rightarrow B$ ' ' $C \subseteq A$ ' show  $f(C) \neq \emptyset$  using func1\_1\_L15A  
by simp  
qed

Order isomorphisms preserve the property of having a minimum.

```

lemma ord_iso_pres_has_min:
  assumes A1:  $f \in \text{ord\_iso}(A, r, B, R)$  and A2:  $r \subseteq A \times A$  and
  A3:  $C \subseteq A$  and A4:  $\text{HasAminimum}(R, f(C))$ 
  shows  $\text{HasAminimum}(r, C)$ 
proof -
  from A4 obtain m where
    I:  $m \in f(C)$  and II:  $\forall y \in f(C). \langle m, y \rangle \in R$ 
  using HasAminimum_def by auto
  let k = converse(f)(m)
  from A1 have  $f: A \rightarrow B$  using ord_iso_is_bij bij_is_fun
  by simp
  from A1 have  $f \in \text{inj}(A, B)$  using ord_iso_is_bij bij_is_inj
  by simp
  with A3 I have  $k \in C$  and III:  $f(k) = m$ 
  using inj_inv_back_in_set by auto
  moreover
  { fix x assume A5:  $x \in C$ 
    with A3 II ' $f: A \rightarrow B$ ' ' $k \in C$ ' III have
       $k \in A \quad x \in A \quad \langle f(k), f(x) \rangle \in R$ 
    using func_imagedef by auto
    with A1 have  $\langle k, x \rangle \in r$  using ord_iso_apply_conv
    by simp
  } then have  $\forall x \in C. \langle k, x \rangle \in r$  by simp
  ultimately show  $\text{HasAminimum}(r, C)$  using HasAminimum_def by auto
qed

```

Order isomorphisms preserve the images of relations. In other words taking the image of a point by a relation commutes with the function.

```

lemma ord_iso_pres_rel_image:
  assumes A1:  $f \in \text{ord\_iso}(A, r, B, R)$  and
  A2:  $r \subseteq A \times A \quad R \subseteq B \times B$  and
  A3:  $a \in A$ 
  shows  $f(r\{a\}) = R\{f(a)\}$ 
proof
  from A1 have  $f: A \rightarrow B$  using ord_iso_is_bij bij_is_fun
  by simp
  moreover from A2 A3 have I:  $r\{a\} \subseteq A$  by auto
  ultimately have I:  $f(r\{a\}) = \{f(x). x \in r\{a\}\}$ 
  using func_imagedef by simp
  { fix y assume A4:  $y \in f(r\{a\})$ 
    with I obtain x where
       $x \in r\{a\}$  and II:  $y = f(x)$ 
    by auto
    with A1 A2 have  $\langle f(a), f(x) \rangle \in R$  using ord_iso_apply
    by auto
    with II have  $y \in R\{f(a)\}$  by auto
  } then show  $f(r\{a\}) \subseteq R\{f(a)\}$  by auto
  { fix y assume A5:  $y \in R\{f(a)\}$ 

```

```

let x = converse(f)(y)
from A2 A5 have
   $\langle f(a), y \rangle \in R$   $f(a) \in B$  and IV:  $y \in B$ 
  by auto
with A1 have III:  $\langle converse(f)(f(a)), x \rangle \in r$ 
  using ord_iso_converse by simp
moreover from A1 A3 have  $converse(f)(f(a)) = a$ 
  using ord_iso_is_bij left_inverse_bij by blast
ultimately have  $f(x) \in \{f(x). x \in r\{a\}\}$ 
  by auto
moreover from A1 IV have  $f(x) = y$ 
  using ord_iso_is_bij right_inverse_bij by blast
moreover from A1 I have  $f(r\{a\}) = \{f(x). x \in r\{a\}\}$ 
  using ord_iso_is_bij bij_is_fun func_imagedef by blast
ultimately have  $y \in f(r\{a\})$  by simp
} then show  $R\{f(a)\} \subseteq f(r\{a\})$  by auto
qed

```

Order isomorphisms preserve collections of upper bounds.

```

lemma ord_iso_pres_up_bounds:
  assumes A1:  $f \in \text{ord\_iso}(A, r, B, R)$  and
  A2:  $r \subseteq A \times A$   $R \subseteq B \times B$  and
  A3:  $C \subseteq A$ 
  shows  $\{f(r\{a\}). a \in C\} = \{R\{b\}. b \in f(C)\}$ 
proof
  from A1 have  $f: A \rightarrow B$ 
    using ord_iso_is_bij bij_is_fun by simp
  { fix Y assume  $Y \in \{f(r\{a\}). a \in C\}$ 
    then obtain a where  $a \in C$  and I:  $Y = f(r\{a\})$ 
      by auto
    from A3 ' $a \in C$ ' have  $a \in A$  by auto
    with A1 A2 have  $f(r\{a\}) = R\{f(a)\}$ 
      using ord_iso_pres_rel_image by simp
    moreover from A3 ' $f: A \rightarrow B$ ' ' $a \in C$ ' have  $f(a) \in f(C)$ 
      using func_imagedef by auto
    ultimately have  $f(r\{a\}) \in \{R\{b\}. b \in f(C)\}$ 
      by auto
    with I have  $Y \in \{R\{b\}. b \in f(C)\}$  by simp
  } then show  $\{f(r\{a\}). a \in C\} \subseteq \{R\{b\}. b \in f(C)\}$ 
    by blast
  { fix Y assume  $Y \in \{R\{b\}. b \in f(C)\}$ 
    then obtain b where  $b \in f(C)$  and II:  $Y = R\{b\}$ 
      by auto
    with A3 ' $f: A \rightarrow B$ ' obtain a where  $a \in C$  and  $b = f(a)$ 
      using func_imagedef by auto
    with A3 II have  $a \in A$  and  $Y = R\{f(a)\}$  by auto
    with A1 A2 have  $Y = f(r\{a\})$ 
      using ord_iso_pres_rel_image by simp
    with ' $a \in C$ ' have  $Y \in \{f(r\{a\}). a \in C\}$  by auto
  }

```

```

    } then show  $\{R\{b\}. b \in f(C)\} \subseteq \{f(r\{a\}). a \in C\}$ 
      by auto
qed

```

The image of the set of upper bounds is the set of upper bounds of the image.

```

lemma ord_iso_pres_min_up_bounds:
  assumes A1:  $f \in \text{ord\_iso}(A, r, B, R)$  and A2:  $r \subseteq A \times A$   $R \subseteq B \times B$  and
  A3:  $C \subseteq A$  and A4:  $C \neq 0$ 
  shows  $f(\bigcap_{a \in C}. r\{a\}) = (\bigcap_{b \in f(C)}. R\{b\})$ 
proof -
  from A1 have  $f \in \text{inj}(A, B)$ 
    using ord_iso_is_bij bij_is_inj by simp
  moreover note A4
  moreover from A2 A3 have  $\forall a \in C. r\{a\} \subseteq A$  by auto
  ultimately have
     $f(\bigcap_{a \in C}. r\{a\}) = (\bigcap_{a \in C}. f(r\{a\}))$ 
    using inj_image_of_Inter by simp
  also from A1 A2 A3 have
     $(\bigcap_{a \in C}. f(r\{a\})) = (\bigcap_{b \in f(C)}. R\{b\})$ 
    using ord_iso_pres_up_bounds by simp
  finally show  $f(\bigcap_{a \in C}. r\{a\}) = (\bigcap_{b \in f(C)}. R\{b\})$ 
    by simp
qed

```

Order isomorphisms preserve completeness.

```

lemma ord_iso_pres_compl:
  assumes A1:  $f \in \text{ord\_iso}(A, r, B, R)$  and
  A2:  $r \subseteq A \times A$   $R \subseteq B \times B$  and A3:  $R$  {is complete}
  shows  $r$  {is complete}
proof -
  { fix C
    assume A4:  $\text{IsBoundedAbove}(C, r)$   $C \neq 0$ 
    with A1 A2 A3 have
       $\text{HasAminimum}(R, \bigcap_{b \in f(C)}. R\{b\})$ 
      using ord_iso_pres_bound_above IsComplete_def
      by simp
    moreover
    from A2 ' $\text{IsBoundedAbove}(C, r)$ ' have  $I: C \subseteq A$  using Order_ZF_3_L1A
      by blast
    with A1 A2 ' $C \neq 0$ ' have  $f(\bigcap_{a \in C}. r\{a\}) = (\bigcap_{b \in f(C)}. R\{b\})$ 
      using ord_iso_pres_min_up_bounds by simp
    ultimately have  $\text{HasAminimum}(R, f(\bigcap_{a \in C}. r\{a\}))$ 
      by simp
    moreover
    from A2 have  $\forall a \in C. r\{a\} \subseteq A$ 
      by auto
    with ' $C \neq 0$ ' have  $(\bigcap_{a \in C}. r\{a\}) \subseteq A$  using ZF1_1_L7
      by simp
  }

```

```

    moreover note A1 A2
    ultimately have HasAminimum(r,  $\bigcap_{a \in C}. r\{a\}$  )
      using ord_iso_pres_has_min by simp
  } then show r {is complete} using IsComplete_def
    by simp
qed

```

If the original relation is complete, then the induced one is complete.

```

lemma ind_rel_pres_compl: assumes A1: f ∈ bij(A,B)
  and A2: R ⊆ B×B and A3: R {is complete}
  shows InducedRelation(f,R) {is complete}
proof -
  let r = InducedRelation(f,R)
  from A1 have f ∈ ord_iso(A,r,B,R)
    using bij_is_ord_iso by simp
  moreover from A1 A2 have r ⊆ A×A
    using bij_is_fun ind_rel_domain by simp
  moreover note A2 A3
  ultimately show r {is complete}
    using ord_iso_pres_compl by simp
qed

```

end

## 7 Generalization\_ZF.thy

**theory** Generalization\_ZF **imports** func1

**begin**

This theory formalizes the intuitive notion of *generalization*.

See <http://www.mathematics21.org/generalization.html> for more details.

Contributed by Victor Porton.

### 7.1 Generalization situation

In mathematics it is often encountered that a small set  $S$  naturally bijectively corresponds to a subset  $R$  of a larger set  $B$ . (In other words, there is specified an injection  $E$  from  $S$  to  $B$ .) It is a widespread practice to equate  $S$  with  $R$ . But strictly speaking this equating may contradict to the axioms of ZF/ZFC because we are not insured against  $S \cap B \neq \emptyset$  incidents. To work around of this (and formulate things exactly what could benefit computer proof assistants) we will replace the set  $B$  with a new set  $B$  having a bijection  $M : B \rightarrow B$  such that  $M \circ E = id_S$ . (I call this bijection  $M$  from the first letter of the word "move" which signifies the move from the old set  $B$  to a new set  $B$ . This section contains some basic lemmas holding in this setup.

The next locale defines our assumptions.

```
locale generalization =  
  fixes small and big  
  fixes embed  
  assumes embed_inj: embed  $\in$  inj(small, big)
```

We define the small2 set as the range of embed.

```
definition (in generalization) small2  $\equiv$  range(embed)
```

We define spec as the converse of embed.

```
definition (in generalization) spec  $\equiv$  converse(embed)
```

Spec is an injection from range of embed to small.

```
lemma (in generalization) spec_inj: shows spec  $\in$  inj(small2, small)  
  using embed_inj inj_converse_inj small2_def spec_def by simp
```

Spec maps range of embed to small.

```
lemma (in generalization) spec_fun: shows spec: small2 $\rightarrow$ small  
  using embed_inj inj_converse_fun small2_def spec_def by simp
```

Embed maps smallsmall to big.

```
lemma (in generalization) embed_fun: shows embed: small $\rightarrow$ big  
  using embed_inj inj_is_fun by simp
```

Embed is a surjection from `small` to `small2`.

```
lemma (in generalization) embed_surj: shows embed ∈ surj(small, small2)
  using fun_is_surj embed_fun small2_def by simp
```

Embed is a bijection between `small` and `small2`.

```
theorem (in generalization) embed_bij: shows embed ∈ bij(small, small2)
  using embed_inj inj_bij_range small2_def by simp
```

`small2` (i.e. range of `embed`) is a subset of `big`.

```
theorem (in generalization) small2_sub_big: shows small2 ⊆ big
  using embed_fun func1_1_L5B small2_def by simp
```

`spec` is a bijection between `small2` and `small`.

```
theorem (in generalization) spec_bij: shows spec ∈ bij(small2, small)
  using bij_converse_bij embed_bij spec_def by simp
```

## 7.2 Arbitrary generalizations

This section considers a more general situation.

The next locale extends `generalization` adding another `big` set and the `move` operation.

```
locale generalization1 = generalization +
  fixes newbig
  fixes move
  assumes move_bij: move ∈ bij(big, newbig)
  assumes move_embed: move 0 embed = id(small)
```

in `generalization1` context we define `ret` as the converse of `move`.

```
definition (in generalization1) ret ≡ converse(move)
```

`move` is a map from `big` to `newbig`.

```
lemma (in generalization1) move_fun: shows move: big → newbig
  using move_bij bij_is_fun by simp
```

`move` is an injection from `big` to `newbig`.

```
lemma (in generalization1) move_inj: shows move ∈ inj(big, newbig)
  using move_bij bij_is_inj by simp
```

`Move` is a surjection `big` to `newbig`.

```
lemma (in generalization1) move_surj: shows move ∈ surj(big, newbig)
  using move_bij bij_is_surj by simp
```

`big` is the domain of `move`.

```
lemma (in generalization1) move_domain: shows domain(move) = big
  using domain_of_fun move_fun by simp
```



Composing move with embed takes elements of small to themselves.

```
theorem (in generalization1) move_embed_plain: assumes x∈small
  shows move(embed(x)) = x
```

```
proof -
```

```
  from assms have move(embed(x)) = (move 0 embed)(x)
    using embed_fun comp_fun_apply by simp
  with assms show thesis using move_embed by simp
```

```
qed
```

ret is a bijection from newbignewbig to big.

```
lemma (in generalization1) ret_bij: shows ret∈bij(newbig, big)
  using move_bij ret_def by simp
```

ret is a injection from newbig onto big.

```
lemma (in generalization1) ret_inj: shows ret ∈ inj(newbig, big)
  using ret_bij bij_is_inj by simp
```

ret is a surjection from newbig onto big.

```
lemma (in generalization1) ret_surj: shows ret ∈ surj(newbig, big)
  using ret_bij bij_is_surj by simp
```

embed is a restriciton of ret to small.

```
lemma (in generalization1) ret_restrict: shows embed = restrict(ret,
small)
```

```
proof -
```

```
  have embed⊆small×big
    using fun_is_rel embed_fun by auto
  moreover
  have (converse(move) 0 move) 0 embed = converse(move) 0 id(small)
    using move_embed comp_assoc by auto
  then have a: id(big) 0 embed = converse(move) 0 id(small)
    using left_comp_inverse move_inj by simp
  ultimately show thesis using left_comp_id right_comp_id_any ret_def
    by auto
```

```
qed
```

### 7.3 ZF generalization

We continue material from the previous section.

We will need this lemma to assert that ZF generalization is an arbitrary generalization:

```
lemma mem_not_refl_2: shows {t} ∉ t
  using foundation by auto
```

Definition of token.

```
definition (in generalization) token  $\equiv$  Pow( $\bigcup$  ( $\bigcup$  (small)))
```

Definition of function moving the small set into big.

**definition** (in generalization)

$\text{zf\_move\_fun}(x) \equiv \text{if } x \in \text{small2} \text{ then } \text{spec}(x) \text{ else } \langle \text{token}, x \rangle$

Definition of  $\text{zf\_move}$  - the ZF version of  $\text{zf\_move\_fun}$ .

**definition** (in generalization)

$\text{zf\_move} \equiv \{ \langle x, \text{zf\_move\_fun}(x) \rangle \mid x \in \text{big} \}$

Definition of  $\text{zf\_newbig}$  as the range of  $\text{zf\_move}$ .

**definition** (in generalization)  $\text{zf\_newbig} \equiv \text{range}(\text{zf\_move})$

$\text{zf\_move}$  is a function that maps big to newbig.

**lemma** (in generalization)  $\text{zf\_move\_fun}$ : shows  $\text{zf\_move}: \text{big} \rightarrow \text{zf\_newbig}$   
 using  $\text{lam\_is\_fun\_range}$   $\text{zf\_move\_def}$   $\text{zf\_newbig\_def}$  by simp

token is not in small.

**lemma** (in generalization)  $\text{token\_not\_small}$ : shows  $\langle \text{token}, x \rangle \notin \text{small}$

**proof**

assume  $\langle \text{token}, x \rangle \in \text{small}$

then have  $\{\text{token}\} \in \text{token}$  using  $\text{token\_def}$   $\text{Pair\_def}$  by auto

then show False using  $\text{mem\_not\_refl\_2}$  by blast

qed

Domain of  $\text{zf\_move}$  is big.

**lemma** (in generalization)  $\text{zf\_move\_domain}$ : shows  $\text{domain}(\text{zf\_move}) = \text{big}$   
 using  $\text{zf\_move\_fun}$   $\text{func1\_1\_L1}$  by simp

small is a subset of big.

**theorem** (in generalization)  $\text{small\_less\_zf\_newbig}$ :

shows  $\text{small} \subseteq \text{zf\_newbig}$

**proof**

fix x

assume s:  $x \in \text{small}$

then have  $s1: \text{embed}(x) \in \text{small2}$

using  $\text{embed\_fun}$   $\text{apply\_rangeI}$   $\text{small2\_def}$

by simp

then have  $s2: \text{embed}(x) \in \text{big}$  using  $\text{small2\_sub\_big}$  by auto

with s1 s have  $x\_val: \text{zf\_move}(\text{embed}(x)) = x$

using  $\text{ZF\_fun\_from\_tot\_val}$   $\text{zf\_move\_fun}$   $\text{embed\_inj}$

$\text{left\_inverse}$   $\text{spec\_def}$   $\text{zf\_move\_def}$   $\text{zf\_move\_fun\_def}$

by simp

from s2 have  $\text{zf\_move}(\text{embed}(x)) \in \text{range}(\text{zf\_move})$

using  $\text{zf\_move\_fun}$   $\text{apply\_rangeI}$  by simp

with  $x\_val$  show  $x \in \text{zf\_newbig}$  using  $\text{zf\_newbig\_def}$  by auto

qed

$\text{zf\_move}$  is an injection from big to  $\text{zf\_newbig}$ .

```

theorem (in generalization) zf_move_inj: shows zf_move ∈ inj(big, zf_newbig)
proof -
  have  $\forall a \in \text{big}. \forall b \in \text{big}. \text{zf\_move}(a) = \text{zf\_move}(b) \longrightarrow a=b$ 
proof -
  {
    fix a b
    assume  $a \in \text{big}$  and  $b \in \text{big}$ 
    then have spec1_a:  $a \in \text{small2} \longrightarrow \text{zf\_move}(a) = \text{spec}(a)$  and
      spec2_a:  $a \notin \text{small2} \longrightarrow \text{zf\_move}(a) = \langle \text{token}, a \rangle$  and
      spec1_b:  $b \in \text{small2} \longrightarrow \text{zf\_move}(b) = \text{spec}(b)$  and
      spec2_b:  $b \notin \text{small2} \longrightarrow \text{zf\_move}(b) = \langle \text{token}, b \rangle$ 
      using ZF_fun_from_tot_val1 zf_move_fun_def zf_move_def
      by auto
    assume move_eq:  $\text{zf\_move}(a) = \text{zf\_move}(b)$ 
    have  $a=b$ 
    proof -
      { assume  $a \in \text{small2}$  and  $b \in \text{small2}$ 
        with 'a ∈ small2' spec1_a 'b ∈ small2' spec1_b move_eq
        have I:  $\text{spec}(a) = \text{spec}(b)$  by simp
        have  $\text{spec} \in \text{inj}(\text{small2}, \text{small1})$ 
          using spec_inj by simp
        then have  $\text{spec} \in \{f: \text{small2} \rightarrow \text{small1}. \forall w \in \text{small2}. \forall x \in \text{small2}. f(w)=f(x) \longrightarrow w=x\}$ 
          unfolding inj_def by auto
        hence  $\forall w \in \text{small2}. \forall x \in \text{small2}. \text{spec}(w)=\text{spec}(x) \longrightarrow w=x$  by auto
        with 'a ∈ small2' 'b ∈ small2' I have  $a=b$  by auto
      }
      moreover
      { assume  $a \in \text{small2}$   $b \notin \text{small2}$ 
        with spec1_a spec_fun have ma_s:  $\text{zf\_move}(a) \in \text{small1}$ 
          using apply_funtype by auto
        from 'b ∈ small2' spec2_b have  $\text{zf\_move}(b) \notin \text{small1}$ 
          using token_not_small by auto
        with move_eq ma_s have False by auto
      }
      moreover
      { assume  $a \notin \text{small2}$  and  $b \in \text{small2}$ 
        with spec1_b spec_fun have mb_s:  $\text{zf\_move}(b) \in \text{small1}$ 
          using apply_funtype by auto
        from 'a ∈ small2' spec2_a have  $\text{zf\_move}(a) \notin \text{small1}$ 
          using token_not_small by auto
        with move_eq mb_s have False by auto
      }
      moreover
      { assume  $a \notin \text{small2}$  and  $b \notin \text{small2}$ 
        with spec2_a spec2_b have
           $\text{zf\_move}(a) = \langle \text{token}, a \rangle$  and
           $\text{zf\_move}(b) = \langle \text{token}, b \rangle$ 

```

```

        by auto
      with move_eq have a=b by auto
    }
    ultimately show a=b by auto
  qed
}
thus thesis by auto
qed
with zf_move_fun show thesis using inj_def by simp
qed

```

zf\_move is a surjection of big onto zf\_newbig.

```

theorem (in generalization) zf_move_surj:
  shows zf_move ∈ surj(big,zf_newbig)
  using zf_move_fun fun_is_surj zf_newbig_def by simp

```

zf\_move is a bijection from big to zf\_newbig.

```

theorem (in generalization) zf_move_bij: shows zf_move ∈ bij(big, zf_newbig)
  using zf_move_inj inj_bij_range zf_newbig_def by simp

```

The essential condition to prove that composition of zf\_move and embed is identity.

```

theorem (in generalization) zf_move_embed:
  assumes x ∈ small shows zf_move(embed(x)) = x
  using assms embed_fun apply_rangeI small2_sub_big ZF_fun_from_tot_val1
  embed_inj small2_def spec_def zf_move_def zf_move_fun_def by auto

```

Composition of zf\_move and embed is identity.

```

theorem (in generalization) zf_embed_move: shows zf_move ∘ embed = id(small)
proof -
  have ∀y∈small. zf_move(embed y) = y and
    embed: small→big and zf_move: big→zf_newbig
  using zf_move_embed embed_fun zf_move_fun by auto
  then show thesis using comp_eq_id_iff1 by blast
qed

```

end

## 8 NatGenIntEx\_ZF.thy

```
theory NatGenIntEx_ZF imports Int_ZF Generalization_ZF
```

```
begin
```

This theory shows an example application of the setup for generalization presented in `Generalization_ZF`.

In this example I show that integers can be considered as a generalization of natural numbers. The next interpretation shows that we can use theorems proven in the `generalization` locale to sets `nat`, `int` and the natural embedding of natural numbers into integers.

```
interpretation int_interpr:
  generalization nat int {⟨n,int_of(n)⟩. n ∈ nat}
proof -
  let f = {⟨n,int_of(n)⟩. n ∈ nat}
  have f ∈ inj(nat,int)
  proof -
    have I: f: nat → int using ZF_fun_from_total by simp
    moreover from I have ∀n∈nat. f(n)= int_of(n)
      using ZF_fun_from_tot_val by simp
    moreover have ∀n∈nat.∀m∈nat. int_of(n)=int_of(m) ⟶ n=m
      using int_of_inject by simp
    ultimately show thesis using inj_def by simp
  qed
  then show generalization(nat,int,f) using generalization_def by simp
qed
```

Next we prove that ZF generalization is an arbitrary generalization. This allows to access notions defined in `generalization1` locale from within `generalization` locale.

```
sublocale
  generalization ⊆ generalization1 small big embed zf_newbig zf_move
proof
  show zf_move∈bij(big, zf_newbig) using zf_move_bij by auto
  show zf_move 0 embed = id(small) using zf_embed_move by auto
qed
```

```
abbreviation int_obj ≡ int_interpr.zf_newbig
```

Naturals are a subset of integers.

```
lemma nat ⊆ int_obj using int_interpr.small_less_zf_newbig by auto
```

An example of defining an operation on the generalization set.

```
definition add where
  add(x,y) ≡ int_interpr.zf_move(int_interpr.retx $+ int_interpr.rety)

end
```

## 9 Finite\_ZF.thy

**theory** Finite\_ZF **imports** ZF1 Nat\_ZF\_IML Cardinal

**begin**

Standard Isabelle Finite.thy contains a very useful notion of finite powerset: the set of finite subsets of a given set. The definition, however, is specific to Isabelle and based on the notion of "datatype", obviously not something that belongs to ZF set theory. This theory file develops the notion of finite powerset similarly as in Finite.thy, but based on standard library's Cardinal.thy. This theory file is intended to replace IsarMathLib's `Finite1` and `Finite_ZF_1` theories that are currently derived from the "datatype" approach.

### 9.1 Definition and basic properties of finite powerset

The goal of this section is to prove an induction theorem about finite powersets: if the empty set has some property and this property is preserved by adding a single element of a set, then this property is true for all finite subsets of this set.

We defined the finite powerset `FinPow(X)` as those elements of the powerset that are finite.

**definition**

$\text{FinPow}(X) \equiv \{A \in \text{Pow}(X) . \text{Finite}(A)\}$

The cardinality of an element of finite powerset is a natural number.

**lemma** `card_fin_is_nat`: **assumes**  $A \in \text{FinPow}(X)$   
**shows**  $|A| \in \text{nat}$  **and**  $A \approx |A|$   
**using** `assms FinPow_def Finite_def cardinal_cong nat_into_Card`  
`Card_cardinal_eq` **by** `auto`

A reformulation of `card_fin_is_nat`: for a finite set  $A$  there is a bijection between  $|A|$  and  $A$ .

**lemma** `fin_bij_card`: **assumes**  $A1: A \in \text{FinPow}(X)$   
**shows**  $\exists b. b \in \text{bij}(|A|, A)$   
**proof** -  
  **from**  $A1$  **have**  $|A| \approx A$  **using** `card_fin_is_nat eqpoll_sym`  
  **by** `blast`  
  **then show thesis using** `eqpoll_def` **by** `auto`  
**qed**

If a set has the same number of elements as  $n \in \mathbb{N}$ , then its cardinality is  $n$ . Recall that in set theory a natural number  $n$  is a set that has  $n$  elements.

**lemma** `card_card`: **assumes**  $A \approx n$  **and**  $n \in \text{nat}$

```

shows |A| = n
using assms cardinal_cong nat_into_Card Card_cardinal_eq
by auto

```

If we add a point to a finite set, the cardinality increases by one. To understand the second assertion  $|A \cup \{a\}| = |A| \cup \{|A|\}$  recall that the cardinality  $|A|$  of  $A$  is a natural number and for natural numbers we have  $n+1 = n \cup \{n\}$ .

```

lemma card_fin_add_one: assumes A1: A ∈ FinPow(X) and A2: a ∈ X-A
shows
  |A ∪ {a}| = succ( |A| )
  |A ∪ {a}| = |A| ∪ {|A|}
proof -
  from A1 A2 have cons(a,A) ≈ cons( |A|, |A| )
    using card_fin_is_nat mem_not_refl cons_eqpoll_cong
    by auto
  moreover have cons(a,A) = A ∪ {a} by (rule consdef)
  moreover have cons( |A|, |A| ) = |A| ∪ {|A|}
    by (rule consdef)
  ultimately have A ∪ {a} ≈ succ( |A| ) using succ_explained
    by simp
  with A1 show
    |A ∪ {a}| = succ( |A| ) and |A ∪ {a}| = |A| ∪ {|A|}
    using card_fin_is_nat card_card by auto
qed

```

We can decompose the finite powerset into collection of sets of the same natural cardinalities.

```

lemma finpow_decomp:
shows FinPow(X) = (⋃ n ∈ nat. {A ∈ Pow(X). A ≈ n})
using Finite_def FinPow_def by auto

```

Finite powerset is the union of sets of cardinality bounded by natural numbers.

```

lemma finpow_union_card_nat:
shows FinPow(X) = (⋃ n ∈ nat. {A ∈ Pow(X). A ≲ n})
proof -
  have FinPow(X) ⊆ (⋃ n ∈ nat. {A ∈ Pow(X). A ≲ n})
    using finpow_decomp FinPow_def eqpoll_imp_lepoll
    by auto
  moreover have
    (⋃ n ∈ nat. {A ∈ Pow(X). A ≲ n}) ⊆ FinPow(X)
    using lepoll_nat_imp_Finite FinPow_def by auto
  ultimately show thesis by auto
qed

```

A different form of `finpow_union_card_nat` (see above) - a subset that has not more elements than a given natural number is in the finite powerset.

```

lemma lepoll_nat_in_finpow:

```

```

assumes n ∈ nat    A ⊆ X  A ≲ n
shows A ∈ FinPow(X)
using assms finpow_union_card_nat by auto

```

Natural numbers are finite subsets of the set of natural numbers.

```

lemma nat_finpow_nat: assumes n ∈ nat shows n ∈ FinPow(nat)
  using assms nat_into_Finite nat_subset_nat FinPow_def
  by simp

```

A finite subset is a finite subset of itself.

```

lemma fin_finpow_self: assumes A ∈ FinPow(X) shows A ∈ FinPow(A)
  using assms FinPow_def by auto

```

If we remove an element and put it back we get the set back.

```

lemma rem_add_eq: assumes a ∈ A shows (A - {a}) ∪ {a} = A
  using assms by auto

```

Induction for finite powerset. This is similar to the standard Isabelle's `Fin_induct`.

```

theorem FinPow_induct: assumes A1: P(0) and
  A2: ∀ A ∈ FinPow(X). P(A) ⟶ (∀ a ∈ X. P(A ∪ {a})) and
  A3: B ∈ FinPow(X)
shows P(B)
proof -
  { fix n assume n ∈ nat
    moreover from A1 have I: ∀ B ∈ Pow(X). B ≲ 0 ⟶ P(B)
      using lepoll_0_is_0 by auto
    moreover have ∀ k ∈ nat.
      (∀ B ∈ Pow(X). (B ≲ k ⟶ P(B))) ⟶
      (∀ B ∈ Pow(X). (B ≲ succ(k) ⟶ P(B)))
    proof -
      { fix k assume A4: k ∈ nat
      assume A5: ∀ B ∈ Pow(X). (B ≲ k ⟶ P(B))
      fix B assume A6: B ∈ Pow(X)  B ≲ succ(k)
      have P(B)
      proof -
        have B = 0 ⟶ P(B)
        proof -
          { assume B = 0
            then have B ≲ 0 using lepoll_0_iff
          }
        by simp
        with I A6 have P(B) by simp
      } thus B = 0 ⟶ P(B) by simp
      qed
      moreover have B ≠ 0 ⟶ P(B)
      proof -
        { assume B ≠ 0
          then obtain a where II: a ∈ B by auto

```



```

    let A = B - {a}
    from A6 II have A  $\subseteq$  X and A  $\lesssim$  k
using Diff_sing_lepoll by auto
    with A4 A5 have A  $\in$  FinPow(X) and P(A)
using lepoll_nat_in_finpow finpow_decomp
by auto
    with A2 A6 II have P(A  $\cup$  {a})
by auto
    moreover from II have A  $\cup$  {a} = B
by auto
    ultimately have P(B) by simp
  } thus B $\neq$ 0  $\longrightarrow$  P(B) by simp
qed
ultimately show P(B) by auto
qed
  } thus thesis by blast
qed
ultimately have  $\forall B \in \text{Pow}(X). (B \lesssim n \longrightarrow P(B))$ 
  by (rule ind_on_nat)
} then have  $\forall n \in \text{nat}. \forall B \in \text{Pow}(X). (B \lesssim n \longrightarrow P(B))$ 
  by auto
with A3 show P(B) using finpow_union_card_nat
  by auto
qed

```

A subset of a finites subset is a finite subset.

```

lemma subset_finpow: assumes A  $\in$  FinPow(X) and B  $\subseteq$  A
  shows B  $\in$  FinPow(X)
  using assms FinPow_def subset_Finite by auto

```

If we subtract anything from a finite set, the resulting set is finite.

```

lemma diff_finpow:
  assumes A  $\in$  FinPow(X) shows A-B  $\in$  FinPow(X)
  using assms subset_finpow by blast

```

If we remove a point from a finites subset, we get a finite subset.

```

corollary fin_rem_point_fin: assumes A  $\in$  FinPow(X)
  shows A - {a}  $\in$  FinPow(X)
  using assms diff_finpow by simp

```

Cardinality of a nonempty finite set is a successor of some natural number.

```

lemma card_non_empty_succ:
  assumes A1: A  $\in$  FinPow(X) and A2: A  $\neq$  0
  shows  $\exists n \in \text{nat}. |A| = \text{succ}(n)$ 
proof -
  from A2 obtain a where a  $\in$  A by auto
  let B = A - {a}
  from A1 'a  $\in$  A' have

```

```

    B ∈ FinPow(X) and a ∈ X - B
    using FinPow_def fin_rem_point_fin by auto
  then have |B ∪ {a}| = succ( |B| )
    using card_fin_add_one by auto
  moreover from 'a ∈ A' 'B ∈ FinPow(X)' have
    A = B ∪ {a} and |B| ∈ nat
    using card_fin_is_nat by auto
  ultimately show ∃n ∈ nat. |A| = succ(n) by auto
qed

```

Nonempty set has non-zero cardinality. This is probably true without the assumption that the set is finite, but I couldn't derive it from standard Isabelle theorems.

```

lemma card_non_empty_non_zero:
  assumes A ∈ FinPow(X) and A ≠ 0
  shows |A| ≠ 0
proof -
  from assms obtain n where |A| = succ(n)
    using card_non_empty_succ by auto
  then show |A| ≠ 0 using succ_not_0
    by simp
qed

```

Another variation on the induction theme: If we can show something holds for the empty set and if it holds for all finite sets with at most  $k$  elements then it holds for all finite sets with at most  $k + 1$  elements, then it holds for all finite sets.

```

theorem FinPow_card_ind: assumes A1: P(0) and
  A2: ∀k∈nat.
    (∀A ∈ FinPow(X). A ≲ k ⟶ P(A)) ⟶
    (∀A ∈ FinPow(X). A ≲ succ(k) ⟶ P(A))
  and A3: A ∈ FinPow(X) shows P(A)
proof -
  from A3 have |A| ∈ nat and A ∈ FinPow(X) and A ≲ |A|
    using card_fin_is_nat eqpoll_imp_lepoll by auto
  moreover have ∀n ∈ nat. (∀A ∈ FinPow(X).
    A ≲ n ⟶ P(A))
  proof
    fix n assume n ∈ nat
    moreover from A1 have ∀A ∈ FinPow(X). A ≲ 0 ⟶ P(A)
      using lepoll_0_is_0 by auto
    moreover note A2
    ultimately show
      ∀A ∈ FinPow(X). A ≲ n ⟶ P(A)
      by (rule ind_on_nat)
  qed
  ultimately show P(A) by simp
qed

```

Another type of induction (or, maybe recursion). The induction step we try to find a point in the set that if we remove it, the fact that the property holds for the smaller set implies that the property holds for the whole set.

```

lemma FinPow_ind_rem_one: assumes A1: P(0) and
  A2:  $\forall A \in \text{FinPow}(X). A \neq 0 \longrightarrow (\exists a \in A. P(A - \{a\}) \longrightarrow P(A))$ 
  and A3:  $B \in \text{FinPow}(X)$ 
  shows P(B)
proof -
  note A1
  moreover have  $\forall k \in \text{nat}. (\forall B \in \text{FinPow}(X). B \lesssim k \longrightarrow P(B)) \longrightarrow (\forall C \in \text{FinPow}(X). C \lesssim \text{succ}(k) \longrightarrow P(C))$ 
  proof -
    { fix k assume k  $\in$  nat
      assume A4:  $\forall B \in \text{FinPow}(X). B \lesssim k \longrightarrow P(B)$ 
      have  $\forall C \in \text{FinPow}(X). C \lesssim \text{succ}(k) \longrightarrow P(C)$ 
      proof -
        { fix C assume C  $\in$  FinPow(X)
          assume C  $\lesssim$  succ(k)
          note A1
          moreover
          { assume C  $\neq$  0
            with A2 'C  $\in$  FinPow(X)' obtain a where
              a  $\in$  C and  $P(C - \{a\}) \longrightarrow P(C)$ 
            by auto
            with A4 'C  $\in$  FinPow(X)' 'C  $\lesssim$  succ(k)'
            have P(C) using Diff_sing_lepoll fin_rem_point_fin
            by simp }
          ultimately have P(C) by auto
        } thus thesis by simp
      qed
    } thus thesis by blast
  qed
  moreover note A3
  ultimately show P(B) by (rule FinPow_card_ind)
qed

```

Yet another induction theorem. This is similar, but slightly more complicated than `FinPow_ind_rem_one`. The difference is in the treatment of the empty set to allow to show properties that are not true for empty set.

```

lemma FinPow_rem_ind: assumes A1:  $\forall A \in \text{FinPow}(X). A = 0 \vee (\exists a \in A. A = \{a\} \vee P(A - \{a\}) \longrightarrow P(A))$ 
  and A2:  $A \in \text{FinPow}(X)$  and A3:  $A \neq 0$ 
  shows P(A)
proof -
  have  $0 = 0 \vee P(0)$  by simp
  moreover have
     $\forall k \in \text{nat}. (\forall B \in \text{FinPow}(X). B \lesssim k \longrightarrow P(B)) \longrightarrow (\forall C \in \text{FinPow}(X). C \lesssim \text{succ}(k) \longrightarrow P(C))$ 
  proof -
    { fix k assume k  $\in$  nat
      assume A4:  $\forall B \in \text{FinPow}(X). B \lesssim k \longrightarrow P(B)$ 
      have  $\forall C \in \text{FinPow}(X). C \lesssim \text{succ}(k) \longrightarrow P(C)$ 
      proof -
        { fix C assume C  $\in$  FinPow(X)
          assume C  $\lesssim$  succ(k)
          note A1
          moreover
          { assume C  $\neq$  0
            with A2 'C  $\in$  FinPow(X)' obtain a where
              a  $\in$  C and  $P(C - \{a\}) \longrightarrow P(C)$ 
            by auto
            with A4 'C  $\in$  FinPow(X)' 'C  $\lesssim$  succ(k)'
            have P(C) using Diff_sing_lepoll fin_rem_point_fin
            by simp }
          ultimately have P(C) by auto
        } thus thesis by simp
      qed
    } thus thesis by blast
  qed
  moreover note A3
  ultimately show P(A) by (rule FinPow_card_ind)
qed

```

```

(∀B ∈ FinPow(X). B ≲ k → (B=0 ∨ P(B))) →
(∀A ∈ FinPow(X). A ≲ succ(k) → (A=0 ∨ P(A)))
proof -
  { fix k assume k ∈ nat
    assume A4: ∀B ∈ FinPow(X). B ≲ k → (B=0 ∨ P(B))
    have ∀A ∈ FinPow(X). A ≲ succ(k) → (A=0 ∨ P(A))
    proof -
      { fix A assume A ∈ FinPow(X)
        assume A ≲ succ(k) A≠0
        from A1 'A ∈ FinPow(X)' 'A≠0' obtain a
          where a∈A and A = {a} ∨ P(A-{a}) → P(A)
          by auto
        let B = A-{a}
        from A4 'A ∈ FinPow(X)' 'A ≲ succ(k)' 'a∈A'
        have B = 0 ∨ P(B)
          using Diff_sing_lepoll fin_rem_point_fin
          by simp
        with 'a∈A' 'A = {a} ∨ P(A-{a}) → P(A)'
        have P(A) by auto
      } thus thesis by auto
    } thus thesis by blast
  } thus thesis by blast
qed
moreover note A2
ultimately have A=0 ∨ P(A) by (rule FinPow_card_ind)
with A3 show P(A) by simp
qed

```

If a family of sets is closed with respect to taking intersections of two sets then it is closed with respect to taking intersections of any nonempty finite collection.

```

lemma inter_two_inter_fin:
  assumes A1: ∀V∈T. ∀W∈T. V ∩ W ∈ T and
  A2: N ≠ 0 and A3: N ∈ FinPow(T)
  shows (⋂N ∈ T)
proof -
  have 0 = 0 ∨ (⋂0 ∈ T) by simp
  moreover have ∀M ∈ FinPow(T). (M = 0 ∨ ⋂M ∈ T) →
    (∀W ∈ T. M ∪ {W} = 0 ∨ ⋂(M ∪ {W}) ∈ T)
  proof -
    { fix M assume M ∈ FinPow(T)
      assume A4: M = 0 ∨ ⋂M ∈ T
      { assume M = 0
        hence ∀W ∈ T. M ∪ {W} = 0 ∨ ⋂(M ∪ {W}) ∈ T
        by auto }
      moreover
      { assume M ≠ 0
        with A4 have ⋂M ∈ T by simp
        { fix W assume W ∈ T

```

```

    from 'M ≠ 0' have  $\bigcap (M \cup \{W\}) = (\bigcap M) \cap W$ 
      by auto
    with A1 ' $\bigcap M \in T$ ' 'W ∈ T' have  $\bigcap (M \cup \{W\}) \in T$ 
      by simp
  } hence  $\forall W \in T. M \cup \{W\} = 0 \vee \bigcap (M \cup \{W\}) \in T$ 
    by simp }
    ultimately have  $\forall W \in T. M \cup \{W\} = 0 \vee \bigcap (M \cup \{W\}) \in T$ 
  by blast
} thus thesis by simp
qed
moreover note 'N ∈ FinPow(T)'
ultimately have  $N = 0 \vee (\bigcap N \in T)$ 
  by (rule FinPow_induct)
with A2 show  $(\bigcap N \in T)$  by simp
qed

```

If a family of sets contains the empty set and is closed with respect to taking unions of two sets then it is closed with respect to taking unions of any finite collection.

```

lemma union_two_union_fin:
  assumes A1:  $0 \in C$  and A2:  $\forall A \in C. \forall B \in C. A \cup B \in C$  and
  A3:  $N \in \text{FinPow}(C)$ 
  shows  $\bigcup N \in C$ 
proof -
  from '0 ∈ C' have  $\bigcup 0 \in C$  by simp
  moreover have  $\forall M \in \text{FinPow}(C). \bigcup M \in C \longrightarrow (\forall A \in C. \bigcup (M \cup \{A\}) \in C)$ 
  proof -
    { fix M assume M ∈ FinPow(C)
      assume  $\bigcup M \in C$ 
      fix A assume A ∈ C
      have  $\bigcup (M \cup \{A\}) = (\bigcup M) \cup A$  by auto
      with A2 ' $\bigcup M \in C$ ' 'A ∈ C' have  $\bigcup (M \cup \{A\}) \in C$ 
    }
  by simp
} thus thesis by simp
qed
moreover note 'N ∈ FinPow(C)'
ultimately show  $\bigcup N \in C$  by (rule FinPow_induct)
qed

```

Empty set is in finite power set.

```

lemma empty_in_finpow: shows  $0 \in \text{FinPow}(X)$ 
  using FinPow_def by simp

```

Singleton is in the finite powerset.

```

lemma singleton_in_finpow: assumes  $x \in X$ 
  shows  $\{x\} \in \text{FinPow}(X)$  using assms FinPow_def by simp

```

Union of two finite subsets is a finite subset.

```

lemma union_finpow: assumes A ∈ FinPow(X) and B ∈ FinPow(X)
  shows A ∪ B ∈ FinPow(X)
  using assms FinPow_def by auto

```

Union of finite number of finite sets is finite.

```

lemma fin_union_finpow: assumes M ∈ FinPow(FinPow(X))
  shows ⋃ M ∈ FinPow(X)
  using assms empty_in_finpow union_finpow union_two_union_fin
  by simp

```

If a set is finite after removing one element, then it is finite.

```

lemma rem_point_fin_fin:
  assumes A1: x ∈ X and A2: A - {x} ∈ FinPow(X)
  shows A ∈ FinPow(X)
proof -
  from assms have (A - {x}) ∪ {x} ∈ FinPow(X)
    using singleton_in_finpow union_finpow by simp
  moreover have A ⊆ (A - {x}) ∪ {x} by auto
  ultimately show A ∈ FinPow(X)
    using FinPow_def subset_Finite by auto
qed

```

An image of a finite set is finite.

```

lemma fin_image_fin: assumes ∀V∈B. K(V)∈C and N ∈ FinPow(B)
  shows {K(V). V∈N} ∈ FinPow(C)
proof -
  have {K(V). V∈0} ∈ FinPow(C) using FinPow_def
    by auto
  moreover have ∀A ∈ FinPow(B).
    {K(V). V∈A} ∈ FinPow(C) ⟶ (∀a∈B. {K(V). V ∈ (A ∪ {a})}) ∈ FinPow(C)
  proof -
    { fix A assume A ∈ FinPow(B)
      assume {K(V). V∈A} ∈ FinPow(C)
      fix a assume a∈B
      have {K(V). V ∈ (A ∪ {a})} ∈ FinPow(C)
        proof -
          have {K(V). V ∈ (A ∪ {a})} = {K(V). V∈A} ∪ {K(a)}
            by auto
          moreover note '{K(V). V∈A} ∈ FinPow(C)'
          moreover from '∀V∈B. K(V) ∈ C' 'a∈B' have {K(a)} ∈ FinPow(C)
            using singleton_in_finpow by simp
          ultimately show thesis using union_finpow by simp
        qed
      } thus thesis by simp
    qed
  moreover note 'N ∈ FinPow(B)'
  ultimately show {K(V). V∈N} ∈ FinPow(C)
    by (rule FinPow_induct)
qed

```

Union of a finite indexed family of finite sets is finite.

```
lemma union_fin_list_fin:
  assumes A1:  $n \in \text{nat}$  and A2:  $\forall k \in n. N(k) \in \text{FinPow}(X)$ 
  shows
     $\{N(k). k \in n\} \in \text{FinPow}(\text{FinPow}(X))$  and  $(\bigcup k \in n. N(k)) \in \text{FinPow}(X)$ 
proof -
  from A1 have  $n \in \text{FinPow}(n)$ 
  using nat_finpow_nat fin_finpow_self by auto
  with A2 show  $\{N(k). k \in n\} \in \text{FinPow}(\text{FinPow}(X))$ 
  by (rule fin_image_fin)
  then show  $(\bigcup k \in n. N(k)) \in \text{FinPow}(X)$ 
  using fin_union_finpow by simp
qed
end
```

## 10 Finite1.thy

**theory** Finite1 **imports** Finite func1 ZF1

**begin**

This theory extends Isabelle standard **Finite** theory. It is obsolete and should not be used for new development. Use the **Finite\_ZF** instead.

### 10.1 Finite powerset

In this section we consider various properties of **Fin** datatype (even though there are no datatypes in ZF set theory).

In **Topology\_ZF** theory we consider induced topology that is obtained by taking a subset of a topological space. To show that a topology restricted to a subset is also a topology on that subset we may need a fact that if  $T$  is a collection of sets and  $A$  is a set then every finite collection  $\{V_i\}$  is of the form  $V_i = U_i \cap A$ , where  $\{U_i\}$  is a finite subcollection of  $T$ . This is one of those trivial facts that require suprisingly long formal proof. Actually, the need for this fact is avoided by requiring intersection two open sets to be open (rather than intersection of a finite number of open sets). Still, the fact is left here as an example of a proof by induction. We will use **Fin\_induct** lemma from **Finite.thy**. First we define a property of finite sets that we want to show.

**definition**

$\text{Prfin}(T, A, M) \equiv (M = 0) \mid (\exists N \in \text{Fin}(T). \forall V \in M. \exists U \in N. (V = U \cap A))$

Now we show the main induction step in a separate lemma. This will make the proof of the theorem **FinRestr** below look short and nice. The premises of the **ind\_step** lemma are those needed by the main induction step in lemma **Fin\_induct** (see standard Isabelle's **Finite.thy**).

**lemma** **ind\_step**: **assumes**  $A: \forall V \in T. \exists U \in T. V = U \cap A$

**and**  $A1: W \in T$  **and**  $A2: M \in \text{Fin}(T)$

**and**  $A3: W \notin M$  **and**  $A4: \text{Prfin}(T, A, M)$

**shows**  $\text{Prfin}(T, A, \text{cons}(W, M))$

**proof** -

{ **assume**  $A7: M = 0$  **have**  $\text{Prfin}(T, A, \text{cons}(W, M))$

**proof**-

**from**  $A1$   $A$  **obtain**  $U$  **where**  $A5: U \in T$  **and**  $A6: W = U \cap A$  **by** **fast**

**let**  $N = \{U\}$

**from**  $A5$  **have**  $T1: N \in \text{Fin}(T)$  **by** **simp**

**from**  $A7$   $A6$  **have**  $T2: \forall V \in \text{cons}(W, M). \exists U \in N. V = U \cap A$  **by** **simp**

**from**  $A7$   $T1$   $T2$  **show**  $\text{Prfin}(T, A, \text{cons}(W, M))$

**using** **Prfin\_def** **by** **auto**

**qed** }

**moreover**



```

{ assume A8:M≠0 have Prfin(T, A, cons(W, M))
  proof-
    from A1 A obtain U where A5: U∈T and A6:W=U∩A by fast
    from A8 A4 obtain N0
  where A9: N0∈ Fin(T) and A10: ∀V∈ M. ∃ U0∈ N0. (V = U0∩A)
  using Prfin_def by auto
  let N = cons(U,N0)
  from A5 A9 have N ∈ Fin(T) by simp
  moreover from A10 A6 have ∀V∈ cons(W,M). ∃ U∈N. V=U∩A by simp
  ultimately have ∃ N∈ Fin(T).∀V∈ cons(W,M). ∃ U∈N. V=U∩A by auto
  with A8 show Prfin(T, A, cons(W, M))
  using Prfin_def by simp
  qed }
  ultimately show thesis by auto
qed

```

Now we are ready to prove the statement we need.

```

theorem FinRestr0: assumes A: ∀ V ∈ TA. ∃ U∈ T. V=U∩A
  shows ∀ M∈ Fin(TA). Prfin(T,A,M)
proof -
  { fix M
    assume M ∈ Fin(TA)
    moreover have Prfin(T,A,0) using Prfin_def by simp
    moreover
      { fix W M assume W∈TA M∈ Fin(TA) W≠M Prfin(T,A,M)
        with A have Prfin(T,A,cons(W,M)) by (rule ind_step) }
      ultimately have Prfin(T,A,M) by (rule Fin_induct)
    } thus thesis by simp
  }
qed

```

This is a different form of the above theorem:

```

theorem ZF1FinRestr:
  assumes A1:M∈ Fin(TA) and A2: M≠0
  and A3: ∀ V∈ TA. ∃ U∈ T. V=U∩A
  shows ∃N∈ Fin(T). (∀V∈ M. ∃ U∈ N. (V = U∩A)) ∧ N≠0
proof -
  from A3 A1 have Prfin(T,A,M) using FinRestr0 by blast
  then have ∃N∈ Fin(T). ∀V∈ M. ∃ U∈ N. (V = U∩A)
    using A2 Prfin_def by simp
  then obtain N where
    D1:N∈ Fin(T) ∧ (∀V∈ M. ∃ U∈ N. (V = U∩A)) by auto
  with A2 have N≠0 by auto
  with D1 show thesis by auto
qed

```

Purely technical lemma used in Topology\_ZF\_1 to show that if a topology is  $T_2$ , then it is  $T_1$ .

```

lemma Finite1_L2:
  assumes A:∃U V. (U∈T ∧ V∈T ∧ x∈U ∧ y∈V ∧ U∩V=0)

```

**shows**  $\exists U \in T. (x \in U \wedge y \notin U)$   
**proof** -  
**from** A **obtain** U V **where** D1:  $U \in T \wedge V \in T \wedge x \in U \wedge y \in V \wedge U \cap V = 0$  **by** auto  
**with** D1 **show** thesis **by** auto  
**qed**

A collection closed with respect to taking a union of two sets is closed under taking finite unions. Proof by induction with the induction step formulated in a separate lemma.

**lemma** Finite1\_L3\_IndStep:  
**assumes** A1:  $\forall A B. ((A \in C \wedge B \in C) \longrightarrow A \cup B \in C)$   
**and** A2:  $A \in C$  **and** A3:  $N \in \text{Fin}(C)$  **and** A4:  $A \notin N$  **and** A5:  $\bigcup N \in C$   
**shows**  $\bigcup \text{cons}(A, N) \in C$   
**proof** -  
**have**  $\bigcup \text{cons}(A, N) = A \cup \bigcup N$  **by** blast  
**with** A1 A2 A5 **show** thesis **by** simp  
**qed**

The lemma: a collection closed with respect to taking a union of two sets is closed under taking finite unions.

**lemma** Finite1\_L3:  
**assumes** A1:  $0 \in C$  **and** A2:  $\forall A B. ((A \in C \wedge B \in C) \longrightarrow A \cup B \in C)$  **and**  
A3:  $N \in \text{Fin}(C)$   
**shows**  $\bigcup N \in C$   
**proof** -  
**note** A3  
**moreover from** A1 **have**  $\bigcup 0 \in C$  **by** simp  
**moreover**  
**{ fix** A N  
**assume**  $A \in C \wedge N \in \text{Fin}(C) \wedge A \notin N \wedge \bigcup N \in C$   
**with** A2 **have**  $\bigcup \text{cons}(A, N) \in C$  **by** (rule Finite1\_L3\_IndStep) }  
**ultimately show**  $\bigcup N \in C$  **by** (rule Fin\_induct)  
**qed**

A collection closed with respect to taking a intersection of two sets is closed under taking finite intersections. Proof by induction with the induction step formulated in a separate lemma. This is slightly more involved than the union case in Finite1\_L3, because the intersection of empty collection is undefined (or should be treated as such). To simplify notation we define the property to be proven for finite sets as a separate notion.

**definition**  
 $\text{IntPr}(T, N) \equiv (N = 0 \mid \bigcap N \in T)$

The induction step.

**lemma** Finite1\_L4\_IndStep:  
**assumes** A1:  $\forall A B. ((A \in T \wedge B \in T) \longrightarrow A \cap B \in T)$   
**and** A2:  $A \in T$  **and** A3:  $N \in \text{Fin}(T)$  **and** A4:  $A \notin N$  **and** A5:  $\text{IntPr}(T, N)$

```

    shows IntPr(T, cons(A, N))
  proof -
    { assume A6: N=0
      with A2 have IntPr(T, cons(A, N))
        using IntPr_def by simp }
    moreover
    { assume A7: N≠0 have IntPr(T, cons(A, N))
      proof -
        from A7 A5 A2 A1 have  $\bigcap N \cap A \in T$  using IntPr_def by simp
        moreover from A7 have  $\bigcap \text{cons}(A, N) = \bigcap N \cap A$  by auto
        ultimately show IntPr(T, cons(A, N)) using IntPr_def by simp
      qed }
    ultimately show thesis by auto
  qed

```

The lemma.

```

lemma Finite1_L4:
  assumes A1:  $\forall A B. A \in T \wedge B \in T \longrightarrow A \cap B \in T$ 
  and A2:  $N \in \text{Fin}(T)$ 
  shows IntPr(T, N)
proof -
  note A2
  moreover have IntPr(T, 0) using IntPr_def by simp
  moreover
  { fix A N
    assume A∈T N∈Fin(T) A∉N IntPr(T, N)
    with A1 have IntPr(T, cons(A, N)) by (rule Finite1_L4_IndStep) }
  ultimately show IntPr(T, N) by (rule Fin_induct)
qed

```

Next is a restatement of the above lemma that does not depend on the IntPr meta-function.

```

lemma Finite1_L5:
  assumes A1:  $\forall A B. ((A \in T \wedge B \in T) \longrightarrow A \cap B \in T)$ 
  and A2:  $N \neq 0$  and A3:  $N \in \text{Fin}(T)$ 
  shows  $\bigcap N \in T$ 
proof -
  from A1 A3 have IntPr(T, N) using Finite1_L4 by simp
  with A2 show thesis using IntPr_def by simp
qed

```

The images of finite subsets by a meta-function are finite. For example in topology if we have a finite collection of sets, then closing each of them results in a finite collection of closed sets. This is a very useful lemma with many unexpected applications. The proof is by induction. The next lemma is the induction step.

```

lemma fin_image_fin_IndStep:
  assumes  $\forall V \in B. K(V) \in C$ 

```

and  $U \in B$  and  $N \in \text{Fin}(B)$  and  $U \notin N$  and  $\{K(V). V \in N\} \in \text{Fin}(C)$   
 shows  $\{K(V). V \in \text{cons}(U, N)\} \in \text{Fin}(C)$   
 using assms by simp

The lemma:

```
lemma fin_image_fin:
  assumes A1:  $\forall V \in B. K(V) \in C$  and A2:  $N \in \text{Fin}(B)$ 
  shows  $\{K(V). V \in N\} \in \text{Fin}(C)$ 
proof -
  note A2
  moreover have  $\{K(V). V \in 0\} \in \text{Fin}(C)$  by simp
  moreover
  { fix U N
    assume  $U \in B$   $N \in \text{Fin}(B)$   $U \notin N$   $\{K(V). V \in N\} \in \text{Fin}(C)$ 
    with A1 have  $\{K(V). V \in \text{cons}(U, N)\} \in \text{Fin}(C)$ 
      by (rule fin_image_fin_IndStep) }
  ultimately show thesis by (rule Fin_induct)
qed
```

The image of a finite set is finite.

```
lemma Finite1_L6A: assumes A1:  $f: X \rightarrow Y$  and A2:  $N \in \text{Fin}(X)$ 
  shows  $f(N) \in \text{Fin}(Y)$ 
proof -
  from A1 have  $\forall x \in X. f(x) \in Y$ 
    using apply_type by simp
  moreover note A2
  ultimately have  $\{f(x). x \in N\} \in \text{Fin}(Y)$ 
    by (rule fin_image_fin)
  with A1 A2 show thesis
    using FinD func_imagedef by simp
qed
```

If the set defined by a meta-function is finite, then every set defined by a composition of this meta function with another one is finite.

```
lemma Finite1_L6B:
  assumes A1:  $\forall x \in X. a(x) \in Y$  and A2:  $\{b(y). y \in Y\} \in \text{Fin}(Z)$ 
  shows  $\{b(a(x)). x \in X\} \in \text{Fin}(Z)$ 
proof -
  from A1 have  $\{b(a(x)). x \in X\} \subseteq \{b(y). y \in Y\}$  by auto
  with A2 show thesis using Fin_subset_lemma by blast
qed
```

If the set defined by a meta-function is finite, then every set defined by a composition of this meta function with another one is finite.

```
lemma Finite1_L6C:
  assumes A1:  $\forall y \in Y. b(y) \in Z$  and A2:  $\{a(x). x \in X\} \in \text{Fin}(Y)$ 
  shows  $\{b(a(x)). x \in X\} \in \text{Fin}(Z)$ 
proof -
```

```

let N = {a(x). x∈X}
from A1 A2 have {b(y). y ∈ N} ∈ Fin(Z)
  by (rule fin_image_fin)
moreover have {b(a(x)). x∈X} = {b(y). y∈ N}
  by auto
ultimately show thesis by simp
qed

```

If an intersection of a collection is not empty, then the collection is not empty. We are (ab)using the fact the the intesection of empty collection is defined to be empty and prove by contradiction. Should be in ZF1.thy

```

lemma Finite1_L9: assumes A1:  $\bigcap A \neq 0$  shows  $A \neq 0$ 
proof -
  { assume A2:  $\neg A \neq 0$ 
    with A1 have False by simp
  } thus thesis by auto
qed

```

Cartesian product of finite sets is finite.

```

lemma Finite1_L12: assumes A1:  $A \in \text{Fin}(A)$  and A2:  $B \in \text{Fin}(B)$ 
  shows  $A \times B \in \text{Fin}(A \times B)$ 
proof -
  have T1:  $\forall a \in A. \forall b \in B. \{\langle a, b \rangle\} \in \text{Fin}(A \times B)$  by simp
  have  $\forall a \in A. \{\{\langle a, b \rangle\}. b \in B\} \in \text{Fin}(\text{Fin}(A \times B))$ 
  proof
    fix a assume A3:  $a \in A$ 
    with T1 have  $\forall b \in B. \{\langle a, b \rangle\} \in \text{Fin}(A \times B)$ 
      by simp
    moreover note A2
    ultimately show  $\{\{\langle a, b \rangle\}. b \in B\} \in \text{Fin}(\text{Fin}(A \times B))$ 
      by (rule fin_image_fin)
  qed
  then have  $\forall a \in A. \bigcup \{\{\langle a, b \rangle\}. b \in B\} \in \text{Fin}(A \times B)$ 
    using Fin_UnionI by simp
  moreover have
     $\forall a \in A. \bigcup \{\{\langle a, b \rangle\}. b \in B\} = \{a\} \times B$  by blast
  ultimately have  $\forall a \in A. \{a\} \times B \in \text{Fin}(A \times B)$  by simp
  moreover note A1
  ultimately have  $\{\{a\} \times B. a \in A\} \in \text{Fin}(\text{Fin}(A \times B))$ 
    by (rule fin_image_fin)
  then have  $\bigcup \{\{a\} \times B. a \in A\} \in \text{Fin}(A \times B)$ 
    using Fin_UnionI by simp
  moreover have  $\bigcup \{\{a\} \times B. a \in A\} = A \times B$  by blast
  ultimately show thesis by simp
qed

```

We define the characterisic meta-function that is the identity on a set and assigns a default value everywhere else.

**definition**

$\text{Characteristic}(A, \text{default}, x) \equiv (\text{if } x \in A \text{ then } x \text{ else default})$

A finite subset is a finite subset of itself.

```
lemma Finite1_L13:
  assumes A1: A ∈ Fin(X) shows A ∈ Fin(A)
proof -
  { assume A=0 hence A ∈ Fin(A) by simp }
  moreover
  { assume A2: A≠0 then obtain c where D1:c∈A
    by auto
    then have ∀x∈X. Characteristic(A,c,x) ∈ A
      using Characteristic_def by simp
    moreover note A1
    ultimately have
      {Characteristic(A,c,x). x∈A} ∈ Fin(A)
      by (rule fin_image_fin)
    moreover from D1 have
      {Characteristic(A,c,x). x∈A} = A
      using Characteristic_def by simp
    ultimately have A ∈ Fin(A) by simp }
  ultimately show thesis by blast
qed
```

Cartesian product of finite subsets is a finite subset of cartesian product.

```
lemma Finite1_L14: assumes A1: A ∈ Fin(X) B ∈ Fin(Y)
  shows A×B ∈ Fin(X×Y)
proof -
  from A1 have A×B ⊆ X×Y using FinD by auto
  then have Fin(A×B) ⊆ Fin(X×Y) using Fin_mono by simp
  moreover from A1 have A×B ∈ Fin(A×B)
    using Finite1_L13 Finite1_L12 by simp
  ultimately show thesis by auto
qed
```

The next lemma is needed in the Group\_ZF\_3 theory in a couple of places.

```
lemma Finite1_L15:
  assumes A1: {b(x). x∈A} ∈ Fin(B) {c(x). x∈A} ∈ Fin(C)
  and A2: f : B×C→E
  shows {f⟨ b(x),c(x)⟩. x∈A} ∈ Fin(E)
proof -
  from A1 have {b(x). x∈A}×{c(x). x∈A} ∈ Fin(B×C)
    using Finite1_L14 by simp
  moreover have
    {⟨ b(x),c(x)⟩. x∈A} ⊆ {b(x). x∈A}×{c(x). x∈A}
    by blast
  ultimately have T0: {⟨ b(x),c(x)⟩. x∈A} ∈ Fin(B×C)
    by (rule Fin_subset_lemma)
  with A2 have T1: f{⟨ b(x),c(x)⟩. x∈A} ∈ Fin(E)
    using Finite1_L6A by auto
```

```

from T0 have  $\forall x \in A. \langle b(x), c(x) \rangle \in B \times C$ 
  using FinD by auto
with A2 have
   $f\{\langle b(x), c(x) \rangle. x \in A\} = \{f\langle b(x), c(x) \rangle. x \in A\}$ 
  using func1_1_L17 by simp
with T1 show thesis by simp
qed

```

Singletons are in the finite powerset.

```

lemma Finite1_L16: assumes  $x \in X$  shows  $\{x\} \in \text{Fin}(X)$ 
  using assms emptyI consI by simp

```

A special case of Finite1\_L15 where the second set is a singleton. Group\_ZF\_3 theory this corresponds to the situation where we multiply by a constant.

```

lemma Finite1_L16AA: assumes  $\{b(x). x \in A\} \in \text{Fin}(B)$ 
  and  $c \in C$  and  $f : B \times C \rightarrow E$ 
  shows  $\{f\langle b(x), c \rangle. x \in A\} \in \text{Fin}(E)$ 

```

```

proof -
  from assms have
     $\forall y \in B. f\langle y, c \rangle \in E$ 
     $\{b(x). x \in A\} \in \text{Fin}(B)$ 
    using apply_funtype by auto
  then show thesis by (rule Finite1_L6C)
qed

```

First order version of the induction for the finite powerset.

```

lemma Finite1_L16B: assumes A1:  $P(0)$  and A2:  $B \in \text{Fin}(X)$ 
  and A3:  $\forall A \in \text{Fin}(X). \forall x \in X. x \notin A \wedge P(A) \longrightarrow P(A \cup \{x\})$ 
  shows  $P(B)$ 

```

```

proof -
  note ' $B \in \text{Fin}(X)$ ' and ' $P(0)$ '
  moreover
  { fix A x
    assume  $x \in X \ A \in \text{Fin}(X) \ x \notin A \ P(A)$ 
    moreover have  $\text{cons}(x, A) = A \cup \{x\}$  by auto
    moreover note A3
    ultimately have  $P(\text{cons}(x, A))$  by simp }
  ultimately show  $P(B)$  by (rule Fin_induct)
qed

```

## 10.2 Finite range functions

In this section we define functions  $f : X \rightarrow Y$ , with the property that  $f(X)$  is a finite subset of  $Y$ . Such functions play a important role in the construction of real numbers in the Real\_ZF series.

Definition of finite range functions.

**definition**

$\text{FinRangeFunctions}(X,Y) \equiv \{f:X \rightarrow Y. f(X) \in \text{Fin}(Y)\}$

Constant functions have finite range.

```
lemma Finite1_L17: assumes c∈Y and X≠0
  shows ConstantFunction(X,c) ∈ FinRangeFunctions(X,Y)
  using assms func1_3_L1 func_imagedef func1_3_L2 Finite1_L16
  FinRangeFunctions_def by simp
```

Finite range functions have finite range.

```
lemma Finite1_L18: assumes f ∈ FinRangeFunctions(X,Y)
  shows {f(x). x∈X} ∈ Fin(Y)
  using assms FinRangeFunctions_def func_imagedef by simp
```

An alternative form of the definition of finite range functions.

```
lemma Finite1_L19: assumes f:X→Y
  and {f(x). x∈X} ∈ Fin(Y)
  shows f ∈ FinRangeFunctions(X,Y)
  using assms func_imagedef FinRangeFunctions_def by simp
```

A composition of a finite range function with another function is a finite range function.

```
lemma Finite1_L20: assumes A1:f ∈ FinRangeFunctions(X,Y)
  and A2: g : Y→Z
  shows g ∘ f ∈ FinRangeFunctions(X,Z)
proof -
  from A1 A2 have g{f(x). x∈X} ∈ Fin(Z)
    using Finite1_L18 Finite1_L6A
    by simp
  with A1 A2 have {(g ∘ f)(x). x∈X} ∈ Fin(Z)
    using FinRangeFunctions_def apply_funtype
    func1_1_L17 comp_fun_apply by auto
  with A1 A2 show thesis using
    FinRangeFunctions_def comp_fun Finite1_L19
    by auto
qed
```

Image of any subset of the domain of a finite range function is finite.

```
lemma Finite1_L21:
  assumes f ∈ FinRangeFunctions(X,Y) and A⊆X
  shows f(A) ∈ Fin(Y)
proof -
  from assms have f(X) ∈ Fin(Y) f(A) ⊆ f(X)
    using FinRangeFunctions_def func1_1_L8
    by auto
  then show f(A) ∈ Fin(Y) using Fin_subset_lemma
    by blast
qed
```

end



## 11 Finite\_ZF\_1.thy

**theory** Finite\_ZF\_1 imports Finite1 Order\_ZF\_1a

**begin**

This theory is based on `Finite1` theory and is obsolete. It contains properties of finite sets related to order relations. See the `FinOrd` theory for a better approach.

### 11.1 Finite vs. bounded sets

The goal of this section is to show that finite sets are bounded and have maxima and minima.

Finite set has a maximum - induction step.

**lemma** Finite\_ZF\_1\_1\_L1:

assumes A1:  $r$  {is total on}  $X$  and A2:  $\text{trans}(r)$   
and A3:  $A \in \text{Fin}(X)$  and A4:  $x \in X$  and A5:  $A=0 \vee \text{HasAmaximum}(r, A)$   
shows  $A \cup \{x\} = 0 \vee \text{HasAmaximum}(r, A \cup \{x\})$

**proof** -

{ assume  $A=0$  then have  $T1: A \cup \{x\} = \{x\}$  by simp  
from A1 have  $\text{refl}(X, r)$  using `total_is_refl` by simp  
with T1 A4 have  $A \cup \{x\} = 0 \vee \text{HasAmaximum}(r, A \cup \{x\})$   
using `Order_ZF_4_L8` by simp }  
moreover  
{ assume  $A \neq 0$   
with A1 A2 A3 A4 A5 have  $A \cup \{x\} = 0 \vee \text{HasAmaximum}(r, A \cup \{x\})$   
using `FinD Order_ZF_4_L9` by simp }  
ultimately show thesis by blast

**qed**

For total and transitive relations finite set has a maximum.

**theorem** Finite\_ZF\_1\_1\_T1A:

assumes A1:  $r$  {is total on}  $X$  and A2:  $\text{trans}(r)$   
and A3:  $B \in \text{Fin}(X)$   
shows  $B=0 \vee \text{HasAmaximum}(r, B)$

**proof** -

have  $0=0 \vee \text{HasAmaximum}(r, 0)$  by simp  
moreover note A3  
moreover from A1 A2 have  $\forall A \in \text{Fin}(X). \forall x \in X. x \notin A \wedge (A=0 \vee \text{HasAmaximum}(r, A)) \longrightarrow (A \cup \{x\}=0 \vee \text{HasAmaximum}(r, A \cup \{x\}))$   
using `Finite_ZF_1_1_L1` by simp  
ultimately show  $B=0 \vee \text{HasAmaximum}(r, B)$  by (rule `Finite1_L16B`)

**qed**

Finite set has a minimum - induction step.

**lemma** Finite\_ZF\_1\_1\_L2:

```

    assumes A1: r {is total on} X and A2: trans(r)
    and A3: A ∈ Fin(X) and A4: x ∈ X and A5: A=0 ∨ HasAminimum(r,A)
    shows AU{x} = 0 ∨ HasAminimum(r,AU{x})
  proof -
    { assume A=0 then have T1: AU{x} = {x} by simp
      from A1 have refl(X,r) using total_is_refl by simp
      with T1 A4 have AU{x} = 0 ∨ HasAminimum(r,AU{x})
        using Order_ZF_4_L8 by simp }
    moreover
    { assume A ≠ 0
      with A1 A2 A3 A4 A5 have AU{x} = 0 ∨ HasAminimum(r,AU{x})
        using FinD Order_ZF_4_L10 by simp }
    ultimately show thesis by blast
  qed

```

For total and transitive relations finite set has a minimum.

```

theorem Finite_ZF_1_1_T1B:
  assumes A1: r {is total on} X and A2: trans(r)
  and A3: B ∈ Fin(X)
  shows B=0 ∨ HasAminimum(r,B)
proof -
  have 0=0 ∨ HasAminimum(r,0) by simp
  moreover note A3
  moreover from A1 A2 have ∀A ∈ Fin(X). ∀x ∈ X.
    x ∉ A ∧ (A=0 ∨ HasAminimum(r,A)) ⟶ (AU{x}=0 ∨ HasAminimum(r,AU{x}))
    using Finite_ZF_1_1_L2 by simp
  ultimately show B=0 ∨ HasAminimum(r,B) by (rule Finite1_L16B)
qed

```

For transitive and total relations finite sets are bounded.

```

theorem Finite_ZF_1_T1:
  assumes A1: r {is total on} X and A2: trans(r)
  and A3: B ∈ Fin(X)
  shows IsBounded(B,r)
proof -
  from A1 A2 A3 have B=0 ∨ HasAminimum(r,B) B=0 ∨ HasAmaximum(r,B)
    using Finite_ZF_1_1_T1A Finite_ZF_1_1_T1B by auto
  then have
    B = 0 ∨ IsBoundedBelow(B,r) B = 0 ∨ IsBoundedAbove(B,r)
    using Order_ZF_4_L7 Order_ZF_4_L8A by auto
  then show IsBounded(B,r) using
    IsBounded_def IsBoundedBelow_def IsBoundedAbove_def
    by simp
qed

```

For linearly ordered finite sets maximum and minimum have desired properties. The reason we need linear order is that we need the order to be total and transitive for the finite sets to have a maximum and minimum and then we also need antisymmetry for the maximum and minimum to be unique.

```

theorem Finite_ZF_1_T2:
  assumes A1: IsLinOrder(X,r) and A2: A ∈ Fin(X) and A3: A≠0
  shows
    Maximum(r,A) ∈ A
    Minimum(r,A) ∈ A
    ∀x∈A. ⟨x,Maximum(r,A)⟩ ∈ r
    ∀x∈A. ⟨Minimum(r,A),x⟩ ∈ r
proof -
  from A1 have T1: r {is total on} X trans(r) antisym(r)
  using IsLinOrder_def by auto
  moreover from T1 A2 A3 have HasAmaximum(r,A)
  using Finite_ZF_1_1_T1A by auto
  moreover from T1 A2 A3 have HasAminimum(r,A)
  using Finite_ZF_1_1_T1B by auto
  ultimately show
    Maximum(r,A) ∈ A
    Minimum(r,A) ∈ A
    ∀x∈A. ⟨x,Maximum(r,A)⟩ ∈ r ∀x∈A. ⟨Minimum(r,A),x⟩ ∈ r
  using Order_ZF_4_L3 Order_ZF_4_L4 by auto
qed

```

A special case of Finite\_ZF\_1\_T2 when the set has three elements.

```

corollary Finite_ZF_1_L2A:
  assumes A1: IsLinOrder(X,r) and A2: a∈X b∈X c∈X
  shows
    Maximum(r,{a,b,c}) ∈ {a,b,c}
    Minimum(r,{a,b,c}) ∈ {a,b,c}
    Maximum(r,{a,b,c}) ∈ X
    Minimum(r,{a,b,c}) ∈ X
    ⟨a,Maximum(r,{a,b,c})⟩ ∈ r
    ⟨b,Maximum(r,{a,b,c})⟩ ∈ r
    ⟨c,Maximum(r,{a,b,c})⟩ ∈ r
proof -
  from A2 have I: {a,b,c} ∈ Fin(X) {a,b,c} ≠ 0
  by auto
  with A1 show II: Maximum(r,{a,b,c}) ∈ {a,b,c}
  by (rule Finite_ZF_1_T2)
  moreover from A1 I show III: Minimum(r,{a,b,c}) ∈ {a,b,c}
  by (rule Finite_ZF_1_T2)
  moreover from A2 have {a,b,c} ⊆ X
  by auto
  ultimately show
    Maximum(r,{a,b,c}) ∈ X
    Minimum(r,{a,b,c}) ∈ X
  by auto
  from A1 I have ∀x∈{a,b,c}. ⟨x,Maximum(r,{a,b,c})⟩ ∈ r
  by (rule Finite_ZF_1_T2)
  then show
    ⟨a,Maximum(r,{a,b,c})⟩ ∈ r

```

```

      <b,Maximum(r,{a,b,c})> ∈ r
      <c,Maximum(r,{a,b,c})> ∈ r
    by auto
qed

```

If for every element of  $X$  we can find one in  $A$  that is greater, then the  $A$  can not be finite. Works for relations that are total, transitive and antisymmetric.

```

lemma Finite_ZF_1_1_L3:
  assumes A1: r {is total on} X
  and A2: trans(r) and A3: antisym(r)
  and A4: r ⊆ X×X and A5: X≠0
  and A6: ∀x∈X. ∃a∈A. x≠a ∧ <x,a> ∈ r
  shows A ∉ Fin(X)
proof -
  from assms have ¬IsBounded(A,r)
    using Order_ZF_3_L14 IsBounded_def
    by simp
  with A1 A2 show A ∉ Fin(X)
    using Finite_ZF_1_T1 by auto
qed
end

```

## 12 FinOrd\_ZF.thy

**theory** FinOrd\_ZF **imports** Finite\_ZF func\_ZF\_1

**begin**

This theory file contains properties of finite sets related to order relations. Part of this is similar to what is done in `Finite_ZF_1` except that the development is based on the notion of finite powerset defined in `Finite_ZF` rather than the one defined in standard Isabelle `Finite` theory.

### 12.1 Finite vs. bounded sets

The goal of this section is to show that finite sets are bounded and have maxima and minima.

For total and transitive relations nonempty finite set has a maximum.

**theorem** fin\_has\_max:

**assumes** A1:  $r$  {is total on}  $X$  **and** A2:  $\text{trans}(r)$   
**and** A3:  $B \in \text{FinPow}(X)$  **and** A4:  $B \neq 0$   
**shows**  $\text{HasAmaximum}(r, B)$

**proof** -

**have**  $0=0 \vee \text{HasAmaximum}(r, 0)$  **by** simp

**moreover** **have**

$\forall A \in \text{FinPow}(X). A=0 \vee \text{HasAmaximum}(r, A) \longrightarrow$   
 $(\forall x \in X. (A \cup \{x\}) = 0 \vee \text{HasAmaximum}(r, A \cup \{x\}))$

**proof** -

{ **fix**  $A$

**assume**  $A \in \text{FinPow}(X)$   $A = 0 \vee \text{HasAmaximum}(r, A)$

**have**  $\forall x \in X. (A \cup \{x\}) = 0 \vee \text{HasAmaximum}(r, A \cup \{x\})$

**proof** -

{ **fix**  $x$  **assume**  $x \in X$

**note** ' $A = 0 \vee \text{HasAmaximum}(r, A)$ '

**moreover**

{ **assume**  $A = 0$

**then** **have**  $A \cup \{x\} = \{x\}$  **by** simp

**from** A1 **have**  $\text{refl}(X, r)$  **using** total\_is\_refl

**by** simp

**with** ' $x \in X$ ' ' $A \cup \{x\} = \{x\}$ ' **have**  $\text{HasAmaximum}(r, A \cup \{x\})$

**using** Order\_ZF\_4\_L8 **by** simp }

**moreover**

{ **assume**  $\text{HasAmaximum}(r, A)$

**with** A1 A2 ' $A \in \text{FinPow}(X)$ ' ' $x \in X$ '

**have**  $\text{HasAmaximum}(r, A \cup \{x\})$

**using** FinPow\_def Order\_ZF\_4\_L9 **by** simp }

**ultimately** **have**  $A \cup \{x\} = 0 \vee \text{HasAmaximum}(r, A \cup \{x\})$

**by** auto

} **thus**  $\forall x \in X. (A \cup \{x\}) = 0 \vee \text{HasAmaximum}(r, A \cup \{x\})$

```

    by simp
    qed
  } thus thesis by simp
qed
moreover note A3
ultimately have B = 0  $\vee$  HasAmaximum(r,B)
  by (rule FinPow_induct)
with A4 show HasAmaximum(r,B) by simp
qed

```

For linearly ordered nonempty finite sets the maximum is in the set and indeed it is the greatest element of the set.

```

lemma linord_max_props: assumes A1: IsLinOrder(X,r) and
  A2: A  $\in$  FinPow(X) A  $\neq$  0
shows
  Maximum(r,A)  $\in$  A
  Maximum(r,A)  $\in$  X
   $\forall a \in A. \langle a, \text{Maximum}(r,A) \rangle \in r$ 
proof -
  from A1 A2 show
    Maximum(r,A)  $\in$  A and  $\forall a \in A. \langle a, \text{Maximum}(r,A) \rangle \in r$ 
    using IsLinOrder_def fin_has_max Order_ZF_4_L3
    by auto
  with A2 show Maximum(r,A)  $\in$  X using FinPow_def
    by auto
qed

```

## 12.2 Order isomorphisms of finite sets

In this section we establish that if two linearly ordered finite sets have the same number of elements, then they are order-isomorphic and the isomorphism is unique. This allows us to talk about "enumeration" of a linearly ordered finite set. We define the enumeration as the order isomorphism between the number of elements of the set (which is a natural number  $n = \{0, 1, \dots, n-1\}$ ) and the set.

A really weird corner case - empty set is order isomorphic with itself.

```

lemma empty_ord_iso: shows ord_iso(0,r,0,R)  $\neq$  0
proof -
  have 0  $\approx$  0 using eqpoll_refl by simp
  then obtain f where f  $\in$  bij(0,0)
    using eqpoll_def by blast
  then show thesis using ord_iso_def by auto
qed

```

Even weirder than empty\_ord\_iso The order automorphism of the empty set is unique.

```

lemma empty_ord_iso_uniq:

```

```

    assumes f ∈ ord_iso(0,r,0,R)  g ∈ ord_iso(0,r,0,R)
    shows f = g
  proof -
    from assms have f : 0 → 0 and g: 0 → 0
      using ord_iso_def bij_def surj_def by auto
    moreover have ∀x∈0. f(x) = g(x) by simp
    ultimately show f = g by (rule func_eq)
  qed

```

The empty set is the only order automorphism of itself.

```

lemma empty_ord_iso_empty: shows ord_iso(0,r,0,R) = {0}
proof -
  have 0 ∈ ord_iso(0,r,0,R)
  proof -
    have ord_iso(0,r,0,R) ≠ 0 by (rule empty_ord_iso)
    then obtain f where f ∈ ord_iso(0,r,0,R) by auto
    then show 0 ∈ ord_iso(0,r,0,R)
      using ord_iso_def bij_def surj_def fun_subset_prod
      by auto
  qed
  then show ord_iso(0,r,0,R) = {0} using empty_ord_iso_uniq
    by blast
qed

```

An induction (or maybe recursion?) scheme for linearly ordered sets. The induction step is that we show that if the property holds when the set is a singleton or for a set with the maximum removed, then it holds for the set. The idea is that since we can build any finite set by adding elements on the right, then if the property holds for the empty set and is invariant with respect to this operation, then it must hold for all finite sets.

```

lemma fin_ord_induction:
  assumes A1: IsLinOrder(X,r) and A2: P(0) and
  A3: ∀A ∈ FinPow(X). A ≠ 0 → (P(A - {Maximum(r,A)}) → P(A))
  and A4: B ∈ FinPow(X) shows P(B)
proof -
  note A2
  moreover have ∀ A ∈ FinPow(X). A ≠ 0 → (∃a∈A. P(A-{a}) → P(A))
  proof -
    { fix A assume A ∈ FinPow(X) and A ≠ 0
      with A1 A3 have ∃a∈A. P(A-{a}) → P(A)
    }
  using IsLinOrder_def fin_has_max
  IsLinOrder_def Order_ZF_4_L3
  by blast
  } thus thesis by simp
qed
moreover note A4
ultimately show P(B) by (rule FinPow_ind_rem_one)
qed

```

A slightly more complicated version of `fin_ord_induction` that allows to prove properties that are not true for the empty set.

```

lemma fin_ord_ind:
  assumes A1: IsLinOrder(X,r) and A2:  $\forall A \in \text{FinPow}(X).$ 
     $A = 0 \vee (A = \{\text{Maximum}(r,A)\} \vee P(A - \{\text{Maximum}(r,A)\}) \longrightarrow P(A))$ 
  and A3:  $B \in \text{FinPow}(X)$  and A4:  $B \neq 0$ 
  shows  $P(B)$ 
proof -
  { fix A assume  $A \in \text{FinPow}(X)$  and  $A \neq 0$ 
    with A1 A2 have
       $\exists a \in A. A = \{a\} \vee P(A - \{a\}) \longrightarrow P(A)$ 
      using IsLinOrder_def fin_has_max
    IsLinOrder_def Order_ZF_4_L3
      by blast
  } then have  $\forall A \in \text{FinPow}(X).$ 
     $A = 0 \vee (\exists a \in A. A = \{a\} \vee P(A - \{a\}) \longrightarrow P(A))$ 
    by auto
  with A3 A4 show  $P(B)$  using FinPow_rem_ind
    by simp
qed

```

Yet another induction scheme. We build a linearly ordered set by adding elements that are greater than all elements in the set.

```

lemma fin_ind_add_max:
  assumes A1: IsLinOrder(X,r) and A2:  $P(0)$  and A3:  $\forall A \in \text{FinPow}(X).$ 
     $(\forall x \in X - A. P(A) \wedge (\forall a \in A. \langle a, x \rangle \in r) \longrightarrow P(A \cup \{x\}))$ 
  and A4:  $B \in \text{FinPow}(X)$ 
  shows  $P(B)$ 
proof -
  note A1 A2
  moreover have
     $\forall C \in \text{FinPow}(X). C \neq 0 \longrightarrow (P(C - \{\text{Maximum}(r,C)\}) \longrightarrow P(C))$ 
  proof -
    { fix C assume  $C \in \text{FinPow}(X)$  and  $C \neq 0$ 
      let x = Maximum(r,C)
      let A = C - {x}
      assume P(A)
      moreover from ' $C \in \text{FinPow}(X)$ ' have  $A \in \text{FinPow}(X)$ 
        using fin_rem_point_fin by simp
      moreover from A1 ' $C \in \text{FinPow}(X)$ ' ' $C \neq 0$ ' have
         $x \in C$  and  $x \in X - A$  and  $\forall a \in A. \langle a, x \rangle \in r$ 
        using linord_max_props by auto
      moreover note A3
      ultimately have  $P(A \cup \{x\})$  by auto
      moreover from ' $x \in C$ ' have  $A \cup \{x\} = C$ 
        by auto
      ultimately have  $P(C)$  by simp
    } thus thesis by simp
  end

```



```

qed
moreover note A4
ultimately show P(B) by (rule fin_ord_induction)
qed

```

The only order automorphism of a linearly ordered finite set is the identity.

```

theorem fin_ord_auto_id: assumes A1: IsLinOrder(X,r)
  and A2: B ∈ FinPow(X) and A3: B≠0
  shows ord_iso(B,r,B,r) = {id(B)}
proof -
  note A1
  moreover
  { fix A assume A ∈ FinPow(X) A≠0
    let M = Maximum(r,A)
    let A0 = A - {M}
    assume A = {M} ∨ ord_iso(A0,r,A0,r) = {id(A0)}
    moreover
    { assume A = {M}
      have ord_iso({M},r,{M},r) = {id({M})}
    }
    using id_ord_auto_singleton by simp
    with 'A = {M}' have ord_iso(A,r,A,r) = {id(A)}
  } by simp
  moreover
  { assume ord_iso(A0,r,A0,r) = {id(A0)}
    have ord_iso(A,r,A,r) = {id(A)}
  } proof
  show {id(A)} ⊆ ord_iso(A,r,A,r)
  using id_ord_iso by simp
  { fix f assume f ∈ ord_iso(A,r,A,r)
    with A1 'A ∈ FinPow(X)' 'A≠0' have
      restrict(f,A0) ∈ ord_iso(A0, r, A-{f(M)},r)
      using IsLinOrder_def fin_has_max ord_iso_rem_max
      by auto
    with A1 'A ∈ FinPow(X)' 'A≠0' 'f ∈ ord_iso(A,r,A,r)'
      'ord_iso(A0,r,A0,r) = {id(A0)}'
    have restrict(f,A0) = id(A0)
      using IsLinOrder_def fin_has_max max_auto_fixpoint
      by auto
    moreover from A1 'f ∈ ord_iso(A,r,A,r)'
      'A ∈ FinPow(X)' 'A≠0' have
      f : A → A and M ∈ A and f(M) = M
      using ord_iso_def bij_is_fun IsLinOrder_def
      fin_has_max Order_ZF_4_L3 max_auto_fixpoint
      by auto
    ultimately have f = id(A) using id_fixpoint_rem
      by simp
  } then show ord_iso(A,r,A,r) ⊆ {id(A)}
  by auto
qed

```

```

    }
    ultimately have ord_iso(A,r,A,r) = {id(A)}
    by auto
  } then have  $\forall A \in \text{FinPow}(X). A = 0 \vee$ 
    ( $A = \{\text{Maximum}(r,A)\} \vee$ 
     $\text{ord\_iso}(A - \{\text{Maximum}(r,A)\}, r, A - \{\text{Maximum}(r,A)\}, r) =$ 
     $\{\text{id}(A - \{\text{Maximum}(r,A)\})\} \longrightarrow \text{ord\_iso}(A,r,A,r) = \{\text{id}(A)\}$ )
    by auto
  moreover note A2 A3
  ultimately show  $\text{ord\_iso}(B,r,B,r) = \{\text{id}(B)\}$ 
    by (rule fin_ord_ind)
qed

```

Every two finite linearly ordered sets are order isomorphic. The statement is formulated to make the proof by induction on the size of the set easier, see `fin_ord_iso_ex` for an alternative formulation.

```

lemma fin_order_iso:
  assumes A1: IsLinOrder(X,r) IsLinOrder(Y,R) and
  A2:  $n \in \text{nat}$ 
  shows  $\forall A \in \text{FinPow}(X). \forall B \in \text{FinPow}(Y).$ 
     $A \approx n \wedge B \approx n \longrightarrow \text{ord\_iso}(A,r,B,R) \neq 0$ 
proof -
  note A2
  moreover have  $\forall A \in \text{FinPow}(X). \forall B \in \text{FinPow}(Y).$ 
     $A \approx 0 \wedge B \approx 0 \longrightarrow \text{ord\_iso}(A,r,B,R) \neq 0$ 
    using eqpoll_0_is_0 empty_ord_iso by blast
  moreover have  $\forall k \in \text{nat}.$ 
    ( $\forall A \in \text{FinPow}(X). \forall B \in \text{FinPow}(Y).$ 
     $A \approx k \wedge B \approx k \longrightarrow \text{ord\_iso}(A,r,B,R) \neq 0$ )  $\longrightarrow$ 
    ( $\forall C \in \text{FinPow}(X). \forall D \in \text{FinPow}(Y).$ 
     $C \approx \text{succ}(k) \wedge D \approx \text{succ}(k) \longrightarrow \text{ord\_iso}(C,r,D,R) \neq 0$ )
  proof -
    { fix k assume  $k \in \text{nat}$ 
      assume A3:  $\forall A \in \text{FinPow}(X). \forall B \in \text{FinPow}(Y).$ 
         $A \approx k \wedge B \approx k \longrightarrow \text{ord\_iso}(A,r,B,R) \neq 0$ 
      have  $\forall C \in \text{FinPow}(X). \forall D \in \text{FinPow}(Y).$ 
         $C \approx \text{succ}(k) \wedge D \approx \text{succ}(k) \longrightarrow \text{ord\_iso}(C,r,D,R) \neq 0$ 
      proof -
        { fix C assume  $C \in \text{FinPow}(X)$ 
          fix D assume  $D \in \text{FinPow}(Y)$ 
          assume  $C \approx \text{succ}(k) \ D \approx \text{succ}(k)$ 
          then have  $C \neq 0$  and  $D \neq 0$ 
            using eqpoll_succ_imp_not_empty by auto
          let  $M_C = \text{Maximum}(r,C)$ 
          let  $M_D = \text{Maximum}(R,D)$ 
          let  $C_0 = C - \{M_C\}$ 
          let  $D_0 = D - \{M_D\}$ 
          from ' $C \in \text{FinPow}(X)$ ' have  $C \subseteq X$ 
            using FinPow_def by simp

```

```

with A1 have IsLinOrder(C,r)
  using ord_linear_subset by blast
from 'D ∈ FinPow(Y)' have D ⊆ Y
  using FinPow_def by simp
with A1 have IsLinOrder(D,R)
  using ord_linear_subset by blast
from A1 'C ∈ FinPow(X)' 'D ∈ FinPow(Y)'
  'C ≠ 0' 'D ≠ 0' have
  HasAmaximum(r,C) and HasAmaximum(R,D)
  using IsLinOrder_def fin_has_max
  by auto
with A1 have MC ∈ C and MD ∈ D
  using IsLinOrder_def Order_ZF_4_L3 by auto
with 'C ≈ succ(k)' 'D ≈ succ(k)' have
  C0 ≈ k and D0 ≈ k using Diff_sing_eqpoll by auto
from 'C ∈ FinPow(X)' 'D ∈ FinPow(Y)'
have C0 ∈ FinPow(X) and D0 ∈ FinPow(Y)
  using fin_rem_point_fin by auto
with A3 'C0 ≈ k' 'D0 ≈ k' have
  ord_iso(C0,r,D0,R) ≠ 0 by simp
with 'IsLinOrder(C,r)' 'IsLinOrder(D,R)'
  'HasAmaximum(r,C)' 'HasAmaximum(R,D)'
have ord_iso(C,r,D,R) ≠ 0
  by (rule rem_max_ord_iso)
} thus thesis by simp
qed
} thus thesis by blast
qed
ultimately show thesis by (rule ind_on_nat)
qed

```

Every two finite linearly ordered sets are order isomorphic.

**lemma** fin\_ord\_iso\_ex:

```

assumes A1: IsLinOrder(X,r) IsLinOrder(Y,R) and
A2: A ∈ FinPow(X) B ∈ FinPow(Y) and A3: B ≈ A
shows ord_iso(A,r,B,R) ≠ 0

```

**proof** -

```

from A2 obtain n where n ∈ nat and A ≈ n
  using finpow_decomp by auto
from A3 'A ≈ n' have B ≈ n by (rule eqpoll_trans)
with A1 A2 'A ≈ n' 'n ∈ nat' show ord_iso(A,r,B,R) ≠ 0
  using fin_order_iso by simp

```

**qed**

Existence and uniqueness of order isomorphism for two linearly ordered sets with the same number of elements.

**theorem** fin\_ord\_iso\_ex\_uniq:

```

assumes A1: IsLinOrder(X,r) IsLinOrder(Y,R) and
A2: A ∈ FinPow(X) B ∈ FinPow(Y) and A3: B ≈ A

```

```

shows  $\exists! f. f \in \text{ord\_iso}(A, r, B, R)$ 
proof
  from assms show  $\exists f. f \in \text{ord\_iso}(A, r, B, R)$ 
    using fin_ord_iso_ex by blast
  fix f g
  assume A4:  $f \in \text{ord\_iso}(A, r, B, R)$   $g \in \text{ord\_iso}(A, r, B, R)$ 
  then have  $\text{converse}(g) \in \text{ord\_iso}(B, R, A, r)$ 
    using ord_iso_sym by simp
  with 'f  $\in \text{ord\_iso}(A, r, B, R)$ ' have
    I:  $\text{converse}(g) \circ f \in \text{ord\_iso}(A, r, A, r)$ 
    by (rule ord_iso_trans)
  { assume  $A \neq 0$ 
    with A1 A2 I have  $\text{converse}(g) \circ f = \text{id}(A)$ 
      using fin_ord_auto_id by auto
    with A4 have  $f = g$ 
      using ord_iso_def comp_inv_id_eq_bij by auto }
  moreover
  { assume  $A = 0$ 
    then have  $A \approx 0$  using eqpoll_0_iff
      by simp
    with A3 have  $B \approx 0$  by (rule eqpoll_trans)
    with A4 ' $A = 0$ ' have
       $f \in \text{ord\_iso}(0, r, 0, R)$  and  $g \in \text{ord\_iso}(0, r, 0, R)$ 
      using eqpoll_0_iff by auto
    then have  $f = g$  by (rule empty_ord_iso_uniq) }
  ultimately show  $f = g$ 
    using ord_iso_def comp_inv_id_eq_bij
    by auto
qed

end

```

## 13 EquivClass1.thy

**theory** EquivClass1 **imports** EquivClass func\_ZF ZF1

**begin**

In this theory file we extend the work on equivalence relations done in the standard Isabelle's EquivClass theory. That development is very good and all, but we really would prefer an approach contained within the a standard ZF set theory, without extensions specific to Isabelle. That is why this theory is written.

### 13.1 Congruent functions and projections on the quotient

Suppose we have a set  $X$  with a relation  $r \subseteq X \times X$  and a function  $f : X \rightarrow X$ . The function  $f$  can be compatible (congruent) with  $r$  in the sense that if two elements  $x, y$  are related then the values  $f(x), f(y)$  are also related. This is especially useful if  $r$  is an equivalence relation as it allows to "project" the function to the quotient space  $X/r$  (the set of equivalence classes of  $r$ ) and create a new function  $F$  that satisfies the formula  $F([x]_r) = [f(x)]_r$ . When  $f$  is congruent with respect to  $r$  such definition of the value of  $F$  on the equivalence class  $[x]_r$  does not depend on which  $x$  we choose to represent the class. In this section we also consider binary operations that are congruent with respect to a relation. These are important in algebra - the congruency condition allows to project the operation to obtain the operation on the quotient space.

First we define the notion of function that maps equivalent elements to equivalent values. We use similar names as in the Isabelle's standard EquivClass theory to indicate the conceptual correspondence of the notions.

**definition**

$$\text{Congruent}(r, f) \equiv (\forall x \ y. \langle x, y \rangle \in r \longrightarrow \langle f(x), f(y) \rangle \in r)$$

Now we will define the projection of a function onto the quotient space. In standard math the equivalence class of  $x$  with respect to relation  $r$  is usually denoted  $[x]_r$ . Here we reuse notation  $r\{x\}$  instead. This means the image of the set  $\{x\}$  with respect to the relation, which, for equivalence relations is exactly its equivalence class if you think about it.

**definition**

$$\text{ProjFun}(A, r, f) \equiv \{\langle c, \bigcup_{x \in c} r\{f(x)\} \rangle. \ c \in (A//r)\}$$

Elements of equivalence classes belong to the set.

**lemma** EquivClass\_1\_L1:

**assumes** A1: equiv(A, r) **and** A2:  $C \in A//r$  **and** A3:  $x \in C$

```

shows x∈A
proof -
  from A2 have C ⊆ ⋃ (A//r) by auto
  with A1 A3 show x∈A
    using Union_quotient by auto
qed

```

The image of a subset of  $X$  under projection is a subset of  $A/r$ .

```

lemma EquivClass_1_L1A:
  assumes A⊆X shows {r{x}. x∈A} ⊆ X//r
  using assms quotientI by auto

```

If an element belongs to an equivalence class, then its image under relation is this equivalence class.

```

lemma EquivClass_1_L2:
  assumes A1: equiv(A,r) C ∈ A//r and A2: x∈C
  shows r{x} = C
proof -
  from A1 A2 have x ∈ r{x}
    using EquivClass_1_L1 equiv_class_self by simp
  with A2 have I: r{x}∩C ≠ 0 by auto
  from A1 A2 have r{x} ∈ A//r
    using EquivClass_1_L1 quotientI by simp
  with A1 I show thesis
    using quotient_disj by blast
qed

```

Elements that belong to the same equivalence class are equivalent.

```

lemma EquivClass_1_L2A:
  assumes equiv(A,r) C ∈ A//r x∈C y∈C
  shows ⟨x,y⟩ ∈ r
  using assms EquivClass_1_L2 EquivClass_1_L1 equiv_class_eq_iff
  by simp

```

Every  $x$  is in the class of  $y$ , then they are equivalent.

```

lemma EquivClass_1_L2B:
  assumes A1: equiv(A,r) and A2: y∈A and A3: x ∈ r{y}
  shows ⟨x,y⟩ ∈ r
proof -
  from A2 have r{y} ∈ A//r
    using quotientI by simp
  with A1 A3 show thesis using
    EquivClass_1_L1 equiv_class_self equiv_class_nondisjoint by blast
qed

```

If a function is congruent then the equivalence classes of the values that come from the arguments from the same class are the same.

```

lemma EquivClass_1_L3:

```

```

    assumes A1: equiv(A,r) and A2: Congruent(r,f)
    and A3:  $C \in A//r$   $x \in C$   $y \in C$ 
    shows  $r\{f(x)\} = r\{f(y)\}$ 
  proof -
    from A1 A3 have  $\langle x,y \rangle \in r$ 
      using EquivClass_1_L2A by simp
    with A2 have  $\langle f(x),f(y) \rangle \in r$ 
      using Congruent_def by simp
    with A1 show thesis using equiv_class_eq by simp
  qed

```

The values of congruent functions are in the space.

```

lemma EquivClass_1_L4:
  assumes A1: equiv(A,r) and A2:  $C \in A//r$   $x \in C$ 
  and A3: Congruent(r,f)
  shows  $f(x) \in A$ 
  proof -
    from A1 A2 have  $x \in A$ 
      using EquivClass_1_L1 by simp
    with A1 have  $\langle x,x \rangle \in r$ 
      using equiv_def refl_def by simp
    with A3 have  $\langle f(x),f(x) \rangle \in r$ 
      using Congruent_def by simp
    with A1 show thesis using equiv_type by auto
  qed

```

Equivalence classes are not empty.

```

lemma EquivClass_1_L5:
  assumes A1: refl(A,r) and A2:  $C \in A//r$ 
  shows  $C \neq 0$ 
  proof -
    from A2 obtain x where I:  $C = r\{x\}$  and  $x \in A$ 
      using quotient_def by auto
    from A1 ' $x \in A$ ' have  $x \in r\{x\}$  using refl_def by auto
    with I show thesis by auto
  qed

```

To avoid using an axiom of choice, we define the projection using the expression  $\bigcup_{x \in C} r(\{f(x)\})$ . The next lemma shows that for congruent function this is in the quotient space  $A/r$ .

```

lemma EquivClass_1_L6:
  assumes A1: equiv(A,r) and A2: Congruent(r,f)
  and A3:  $C \in A//r$ 
  shows  $(\bigcup_{x \in C}. r\{f(x)\}) \in A//r$ 
  proof -
    from A1 have refl(A,r) unfolding equiv_def by simp
    with A3 have  $C \neq 0$  using EquivClass_1_L5 by simp
    moreover from A2 A3 A1 have  $\forall x \in C. r\{f(x)\} \in A//r$ 

```

```

    using EquivClass_1_L4 quotientI by auto
  moreover from A1 A2 A3 have
     $\forall x y. x \in C \wedge y \in C \longrightarrow r\{f(x)\} = r\{f(y)\}$ 
    using EquivClass_1_L3 by blast
  ultimately show thesis by (rule ZF1_1_L2)
qed

```

Congruent functions can be projected.

```

lemma EquivClass_1_T0:
  assumes equiv(A,r) Congruent(r,f)
  shows ProjFun(A,r,f) : A//r  $\rightarrow$  A//r
  using assms EquivClass_1_L6 ProjFun_def ZF_fun_from_total
  by simp

```

We now define congruent functions of two variables (binary funtions). The predicate `Congruent2` corresponds to `congruent2` in Isabelle's standard `EquivClass` theory, but uses ZF-functions rather than meta-functions.

**definition**

```

Congruent2(r,f)  $\equiv$ 
 $(\forall x_1 x_2 y_1 y_2. \langle x_1, x_2 \rangle \in r \wedge \langle y_1, y_2 \rangle \in r \longrightarrow$ 
 $\langle f\langle x_1, y_1 \rangle, f\langle x_2, y_2 \rangle \rangle \in r)$ 

```

Next we define the notion of projecting a binary operation to the quotient space. This is a very important concept that allows to define quotient groups, among other things.

**definition**

```

ProjFun2(A,r,f)  $\equiv$ 
 $\{ \langle p, \bigcup z \in \text{fst}(p) \times \text{snd}(p). r\{f(z)\} \rangle. p \in (A//r) \times (A//r) \}$ 

```

The following lemma is a two-variables equivalent of `EquivClass_1_L3`.

```

lemma EquivClass_1_L7:
  assumes A1: equiv(A,r) and A2: Congruent2(r,f)
  and A3: C1  $\in$  A//r C2  $\in$  A//r
  and A4: z1  $\in$  C1  $\times$  C2 z2  $\in$  C1  $\times$  C2
  shows r{f(z1)} = r{f(z2)}
proof -
  from A4 obtain x1 y1 x2 y2 where
    x1  $\in$  C1 and y1  $\in$  C2 and z1 =  $\langle x_1, y_1 \rangle$  and
    x2  $\in$  C1 and y2  $\in$  C2 and z2 =  $\langle x_2, y_2 \rangle$ 
  by auto
  with A1 A3 have  $\langle x_1, x_2 \rangle \in r$  and  $\langle y_1, y_2 \rangle \in r$ 
  using EquivClass_1_L2A by auto
  with A2 have  $\langle f\langle x_1, y_1 \rangle, f\langle x_2, y_2 \rangle \rangle \in r$ 
  using Congruent2_def by simp
  with A1 'z1 =  $\langle x_1, y_1 \rangle$ ' 'z2 =  $\langle x_2, y_2 \rangle$ ' show thesis
  using equiv_class_eq by simp
qed

```

The values of congruent functions of two variables are in the space.



```

lemma EquivClass_1_L8:
  assumes A1: equiv(A,r) and A2:  $C_1 \in A//r$  and A3:  $C_2 \in A//r$ 
  and A4:  $z \in C_1 \times C_2$  and A5: Congruent2(r,f)
  shows  $f(z) \in A$ 
proof -
  from A4 obtain x y where  $x \in C_1$  and  $y \in C_2$  and  $z = \langle x, y \rangle$ 
  by auto
  with A1 A2 A3 have  $x \in A$  and  $y \in A$ 
  using EquivClass_1_L1 by auto
  with A1 A4 have  $\langle x, x \rangle \in r$  and  $\langle y, y \rangle \in r$ 
  using equiv_def refl_def by auto
  with A5 have  $\langle f\langle x, y \rangle, f\langle x, y \rangle \rangle \in r$ 
  using Congruent2_def by simp
  with A1 ' $z = \langle x, y \rangle$ ' show thesis using equiv_type by auto
qed

```

The values of congruent functions are in the space. Note that although this lemma is intended to be used with functions, we don't need to assume that  $f$  is a function.

```

lemma EquivClass_1_L8A:
  assumes A1: equiv(A,r) and A2:  $x \in A$   $y \in A$ 
  and A3: Congruent2(r,f)
  shows  $f\langle x, y \rangle \in A$ 
proof -
  from A1 A2 have  $r\{x\} \in A//r$   $r\{y\} \in A//r$ 
   $\langle x, y \rangle \in r\{x\} \times r\{y\}$ 
  using equiv_class_self quotientI by auto
  with A1 A3 show thesis using EquivClass_1_L8 by simp
qed

```

The following lemma is a two-variables equivalent of EquivClass\_1\_L6.

```

lemma EquivClass_1_L9:
  assumes A1: equiv(A,r) and A2: Congruent2(r,f)
  and A3:  $p \in (A//r) \times (A//r)$ 
  shows  $(\bigcup z \in \text{fst}(p) \times \text{snd}(p). r\{f(z)\}) \in A//r$ 
proof -
  from A3 have  $\text{fst}(p) \in A//r$  and  $\text{snd}(p) \in A//r$ 
  by auto
  with A1 A2 have
    I:  $\forall z \in \text{fst}(p) \times \text{snd}(p). f(z) \in A$ 
  using EquivClass_1_L8 by simp
  from A3 A1 have  $\text{fst}(p) \times \text{snd}(p) \neq 0$ 
  using equiv_def EquivClass_1_L5 Sigma_empty_iff
  by auto
  moreover from A1 I have
     $\forall z \in \text{fst}(p) \times \text{snd}(p). r\{f(z)\} \in A//r$ 
  using quotientI by simp
  moreover from A1 A2 ' $\text{fst}(p) \in A//r$ ' ' $\text{snd}(p) \in A//r$ ' have
     $\forall z_1 z_2. z_1 \in \text{fst}(p) \times \text{snd}(p) \wedge z_2 \in \text{fst}(p) \times \text{snd}(p) \longrightarrow$ 

```

```

      r{f(z1)} = r{f(z2)}
      using EquivClass_1_L7 by blast
      ultimately show thesis by (rule ZF1_1_L2)
qed

```

Congruent functions of two variables can be projected.

```

theorem EquivClass_1_T1:
  assumes equiv(A,r)  Congruent2(r,f)
  shows ProjFun2(A,r,f) : (A//r)×(A//r) → A//r
  using assms EquivClass_1_L9 ProjFun2_def ZF_fun_from_total
  by simp

```

The projection diagram commutes. I wish I knew how to draw this diagram in LaTeX.

```

lemma EquivClass_1_L10:
  assumes A1: equiv(A,r) and A2: Congruent2(r,f)
  and A3: x∈A  y∈A
  shows ProjFun2(A,r,f)⟨r{x},r{y}⟩ = r{f⟨x,y⟩}
proof -
  from A3 A1 have r{x} × r{y} ≠ 0
    using quotientI equiv_def EquivClass_1_L5 Sigma_empty_iff
    by auto
  moreover have
    ∀z ∈ r{x}×r{y}.  r{f(z)} = r{f⟨x,y⟩}
  proof
    fix z assume A4: z ∈ r{x}×r{y}
    from A1 A3 have
      r{x} ∈ A//r  r{y} ∈ A//r
      ⟨x,y⟩ ∈ r{x}×r{y}
      using quotientI equiv_class_self by auto
    with A1 A2 A4 show
      r{f(z)} = r{f⟨x,y⟩}
      using EquivClass_1_L7 by blast
  qed
  ultimately have
    (⋃z ∈ r{x}×r{y}. r{f(z)}) = r{f⟨x,y⟩}
    by (rule ZF1_1_L1)
  moreover have
    ProjFun2(A,r,f)⟨r{x},r{y}⟩ = (⋃z ∈ r{x}×r{y}. r{f(z)})
  proof -
    from assms have
      ProjFun2(A,r,f) : (A//r)×(A//r) → A//r
      ⟨r{x},r{y}⟩ ∈ (A//r)×(A//r)
    using EquivClass_1_T1 quotientI by auto
    then show thesis using ProjFun2_def ZF_fun_from_tot_val
    by auto
  qed
  ultimately show thesis by simp
qed

```

## 13.2 Projecting commutative, associative and distributive operations.

In this section we show that if the operations are congruent with respect to an equivalence relation then the projection to the quotient space preserves commutativity, associativity and distributivity.

The projection of commutative operation is commutative.

```

lemma EquivClass_2_L1: assumes
  A1: equiv(A,r) and A2: Congruent2(r,f)
  and A3: f {is commutative on} A
  and A4: c1 ∈ A//r  c2 ∈ A//r
  shows ProjFun2(A,r,f)⟨c1,c2⟩ = ProjFun2(A,r,f)⟨c2,c1⟩
proof -
  from A4 obtain x y where D1:
    c1 = r{x}  c2 = r{y}
    x∈A  y∈A
  using quotient_def by auto
  with A1 A2 have ProjFun2(A,r,f)⟨c1,c2⟩ = r{f⟨x,y⟩}
    using EquivClass_1_L10 by simp
  also from A3 D1 have
    r{f⟨x,y⟩} = r{f⟨y,x⟩}
    using IsCommutative_def by simp
  also from A1 A2 D1 have
    r{f⟨y,x⟩} = ProjFun2(A,r,f) ⟨c2,c1⟩
    using EquivClass_1_L10 by simp
  finally show thesis by simp
qed

```

The projection of commutative operation is commutative.

```

theorem EquivClass_2_T1:
  assumes equiv(A,r) and Congruent2(r,f)
  and f {is commutative on} A
  shows ProjFun2(A,r,f) {is commutative on} A//r
  using assms IsCommutative_def EquivClass_2_L1 by simp

```

The projection of an associative operation is associative.

```

lemma EquivClass_2_L2:
  assumes A1: equiv(A,r) and A2: Congruent2(r,f)
  and A3: f {is associative on} A
  and A4: c1 ∈ A//r  c2 ∈ A//r  c3 ∈ A//r
  and A5: g = ProjFun2(A,r,f)
  shows g⟨g⟨c1,c2⟩,c3⟩ = g⟨c1,g⟨c2,c3⟩⟩
proof -
  from A4 obtain x y z where D1:
    c1 = r{x}  c2 = r{y}  c3 = r{z}
    x∈A  y∈A  z∈A
  using quotient_def by auto

```

```

with A3 have T1:  $f\langle x, y \rangle \in A$   $f\langle y, z \rangle \in A$ 
  using IsAssociative_def apply_type by auto
with A1 A2 D1 A5 have
   $g\langle g\langle c1, c2 \rangle, c3 \rangle = r\{f\langle f\langle x, y \rangle, z \rangle\}$ 
  using EquivClass_1_L10 by simp
also from D1 A3 have
   $\dots = r\{f\langle x, f\langle y, z \rangle \rangle\}$ 
  using IsAssociative_def by simp
also from T1 A1 A2 D1 A5 have
   $\dots = g\langle c1, g\langle c2, c3 \rangle \rangle$ 
  using EquivClass_1_L10 by simp
finally show thesis by simp
qed

```

The projection of an associative operation is associative on the quotient.

```

theorem EquivClass_2_T2:
  assumes A1: equiv(A,r) and A2: Congruent2(r,f)
  and A3: f {is associative on} A
  shows ProjFun2(A,r,f) {is associative on} A//r
proof -
  let g = ProjFun2(A,r,f)
  from A1 A2 have
     $g \in (A//r) \times (A//r) \rightarrow A//r$ 
    using EquivClass_1_T1 by simp
  moreover from A1 A2 A3 have
     $\forall c1 \in A//r. \forall c2 \in A//r. \forall c3 \in A//r.$ 
     $g\langle g\langle c1, c2 \rangle, c3 \rangle = g\langle c1, g\langle c2, c3 \rangle \rangle$ 
    using EquivClass_2_L2 by simp
  ultimately show thesis
    using IsAssociative_def by simp
qed

```

The essential condition to show that distributivity is preserved by projections to quotient spaces, provided both operations are congruent with respect to the equivalence relation.

```

lemma EquivClass_2_L3:
  assumes A1: IsDistributive(X,A,M)
  and A2: equiv(X,r)
  and A3: Congruent2(r,A) Congruent2(r,M)
  and A4:  $a \in X//r$   $b \in X//r$   $c \in X//r$ 
  and A5:  $A_p = \text{ProjFun2}(X,r,A)$   $M_p = \text{ProjFun2}(X,r,M)$ 
  shows  $M_p\langle a, A_p\langle b, c \rangle \rangle = A_p\langle M_p\langle a, b \rangle, M_p\langle a, c \rangle \rangle \wedge$ 
   $M_p\langle A_p\langle b, c \rangle, a \rangle = A_p\langle M_p\langle b, a \rangle, M_p\langle c, a \rangle \rangle$ 
proof
  from A4 obtain x y z where  $x \in X$   $y \in X$   $z \in X$ 
  a =  $r\{x\}$  b =  $r\{y\}$  c =  $r\{z\}$ 
  using quotient_def by auto
with A1 A2 A3 A5 show
   $M_p\langle a, A_p\langle b, c \rangle \rangle = A_p\langle M_p\langle a, b \rangle, M_p\langle a, c \rangle \rangle$  and

```

```

    Mp⟨ Ap⟨b,c⟩,a ⟩ = Ap⟨ Mp⟨b,a⟩, Mp⟨c,a⟩ ⟩
    using EquivClass_1_L8A EquivClass_1_L10 IsDistributive_def
    by auto
qed

```

Distributivity is preserved by projections to quotient spaces, provided both operations are congruent with respect to the equivalence relation.

```

lemma EquivClass_2_L4: assumes A1: IsDistributive(X,A,M)
  and A2: equiv(X,r)
  and A3: Congruent2(r,A) Congruent2(r,M)
  shows IsDistributive(X//r,ProjFun2(X,r,A),ProjFun2(X,r,M))
proof-
  let Ap = ProjFun2(X,r,A)
  let Mp = ProjFun2(X,r,M)
  from A1 A2 A3 have
    ∀ a∈X//r. ∀ b∈X//r. ∀ c∈X//r.
    Mp⟨ a,Ap⟨b,c⟩ ⟩ = Ap⟨ Mp⟨a,b⟩, Mp⟨a,c⟩ ⟩ ∧
    Mp⟨ Ap⟨b,c⟩,a ⟩ = Ap⟨ Mp⟨b,a⟩, Mp⟨c,a⟩ ⟩
    using EquivClass_2_L3 by simp
  then show thesis using IsDistributive_def by simp
qed

```

### 13.3 Saturated sets

In this section we consider sets that are saturated with respect to an equivalence relation. A set  $A$  is saturated with respect to a relation  $r$  if  $A = r^{-1}(r(A))$ . For equivalence relations saturated sets are unions of equivalence classes. This makes them useful as a tool to define subsets of the quotient space using properties of representants. Namely, we often define a set  $B \subseteq X/r$  by saying that  $[x]_r \in B$  iff  $x \in A$ . If  $A$  is a saturated set, this definition is consistent in the sense that it does not depend on the choice of  $x$  to represent  $[x]_r$ .

The following defines the notion of a saturated set. Recall that in Isabelle  $r^{-1}(A)$  is the inverse image of  $A$  with respect to relation  $r$ . This definition is not specific to equivalence relations.

#### definition

```

IsSaturated(r,A) ≡ A = r-1(r(A))

```

For equivalence relations a set is saturated iff it is an image of itself.

```

lemma EquivClass_3_L1: assumes A1: equiv(X,r)
  shows IsSaturated(r,A) ⟷ A = r(A)
proof
  assume IsSaturated(r,A)
  then have A = (converse(r) ∘ r)(A)
    using IsSaturated_def vimage_def image_comp
    by simp

```

```

    also from A1 have ... = r(A)
      using equiv_comp_eq by simp
    finally show A = r(A) by simp
next assume A = r(A)
  with A1 have A = (converse(r) 0 r)(A)
    using equiv_comp_eq by simp
  also have ... = r-(r(A))
    using vimage_def image_comp by simp
  finally have A = r-(r(A)) by simp
  then show IsSaturated(r,A) using IsSaturated_def
    by simp
qed

```

For equivalence relations sets are contained in their images.

```

lemma EquivClass_3_L2: assumes A1: equiv(X,r) and A2:  $A \subseteq X$ 
  shows  $A \subseteq r(A)$ 
proof
  fix a assume a ∈ A
  with A1 A2 have a ∈ r{a}
    using equiv_class_self by auto
  with 'a ∈ A' show a ∈ r(A) by auto
qed

```

The next lemma shows that if " $\sim$ " is an equivalence relation and a set  $A$  is such that  $a \in A$  and  $a \sim b$  implies  $b \in A$ , then  $A$  is saturated with respect to the relation.

```

lemma EquivClass_3_L3: assumes A1: equiv(X,r)
  and A2:  $r \subseteq X \times X$  and A3:  $A \subseteq X$ 
  and A4:  $\forall x \in A. \forall y \in X. \langle x, y \rangle \in r \longrightarrow y \in A$ 
  shows IsSaturated(r,A)
proof -
  from A2 A4 have  $r(A) \subseteq A$ 
    using image_iff by blast
  moreover from A1 A3 have  $A \subseteq r(A)$ 
    using EquivClass_3_L2 by simp
  ultimately have  $A = r(A)$  by auto
  with A1 show IsSaturated(r,A) using EquivClass_3_L1
    by simp
qed

```

If  $A \subseteq X$  and  $A$  is saturated and  $x \sim y$ , then  $x \in A$  iff  $y \in A$ . Here we show only one direction.

```

lemma EquivClass_3_L4: assumes A1: equiv(X,r)
  and A2: IsSaturated(r,A) and A3:  $A \subseteq X$ 
  and A4:  $\langle x, y \rangle \in r$ 
  and A5:  $x \in X \quad y \in A$ 
  shows  $x \in A$ 
proof -

```

```

from A1 A5 have x ∈ r{x}
  using equiv_class_self by simp
with A1 A3 A4 A5 have x ∈ r(A)
  using equiv_class_eq equiv_class_self
  by auto
with A1 A2 show x ∈ A
  using EquivClass_3_L1 by simp
qed

```

If  $A \subseteq X$  and  $A$  is saturated and  $x \sim y$ , then  $x \in A$  iff  $y \in A$ .

```

lemma EquivClass_3_L5: assumes A1: equiv(X,r)
  and A2: IsSaturated(r,A) and A3: A ⊆ X
  and A4: x ∈ X y ∈ X
  and A5: ⟨x,y⟩ ∈ r
  shows x ∈ A ⟷ y ∈ A
proof
  assume y ∈ A
  with assms show x ∈ A using EquivClass_3_L4
  by simp
next assume x ∈ A
  from A1 A5 have ⟨y,x⟩ ∈ r
    using equiv_is_sym by blast
  with A1 A2 A3 A4 'x ∈ A' show y ∈ A
    using EquivClass_3_L4 by simp
qed

```

If  $A$  is saturated then  $x \in A$  iff its class is in the projection of  $A$ .

```

lemma EquivClass_3_L6: assumes A1: equiv(X,r)
  and A2: IsSaturated(r,A) and A3: A ⊆ X and A4: x ∈ X
  and A5: B = {r{x}. x ∈ A}
  shows x ∈ A ⟷ r{x} ∈ B
proof
  assume x ∈ A
  with A5 show r{x} ∈ B by auto
next assume r{x} ∈ B
  with A5 obtain y where y ∈ A and r{x} = r{y}
  by auto
  with A1 A3 have ⟨x,y⟩ ∈ r
    using eq_equiv_class by auto
  with A1 A2 A3 A4 'y ∈ A' show x ∈ A
    using EquivClass_3_L4 by simp
qed

```

A technical lemma involving a projection of a saturated set and a logical expression with exclusive or. Note that we don't really care what  $\text{Xor}$  is here, this is true for any predicate.

```

lemma EquivClass_3_L7: assumes equiv(X,r)
  and IsSaturated(r,A) and A ⊆ X

```

```

and x∈X y∈X
and B = {r{x}. x∈A}
and (x∈A) Xor (y∈A)
shows (r{x} ∈ B) Xor (r{y} ∈ B)
using assms EquivClass_3_L6 by simp
end

```



## 14 Fold\_ZF.thy

**theory** Fold\_ZF **imports** InductiveSeq\_ZF

**begin**

Suppose we have a binary operation  $P : X \times X \rightarrow X$  written multiplicatively as  $P\langle x, y \rangle = x \cdot y$ . In informal mathematics we can take a sequence  $\{x_k\}_{k \in 0..n}$  of elements of  $X$  and consider the product  $x_0 \cdot x_1 \cdot \dots \cdot x_n$ . To do the same thing in formalized mathematics we have to define precisely what is meant by that "...". The definition we want to use is based on the notion of sequence defined by induction discussed in `InductiveSeq_ZF`. We don't really want to derive the terminology for this from the word "product" as that would tie it conceptually to the multiplicative notation. This would be awkward when we want to reuse the same notions to talk about sums like  $x_0 + x_1 + \dots + x_n$ . In functional programming there is something called "fold". Namely for a function  $f$ , initial point  $a$  and list  $[b, c, d]$  the expression `fold(f, a, [b,c,d])` is defined to be  $f(f(f(a,b),c),d)$  (in Haskell something like this is called `foldl`). If we write  $f$  in multiplicative notation we get  $a \cdot b \cdot c \cdot d$ , so this is exactly what we need. The notion of folds in functional programming is actually much more general than what we need here (not that I know anything about that). In this theory file we just make a slight generalization and talk about folding a list with a binary operation  $f : X \times Y \rightarrow X$  with  $X$  not necessarily the same as  $Y$ .

### 14.1 Folding in ZF

Suppose we have a binary operation  $f : X \times Y \rightarrow X$ . Then every  $y \in Y$  defines a transformation of  $X$  defined by  $T_y(x) = f\langle x, y \rangle$ . In `IsarMathLib` such transformation is called as `Fix2ndVar(f,y)`. Using this notion, given a function  $f : X \times Y \rightarrow X$  and a sequence  $y = \{y_k\}_{k \in N}$  of elements of  $Y$  we can get a sequence of transformations of  $X$ . This is defined in `Seq2TransSeq` below. Then we use that sequence of transformations to define the sequence of partial folds (called `FoldSeq`) by means of `InductiveSeqVarFN` (defined in `InductiveSeq_ZF` theory) which implements the inductive sequence determined by a starting point and a sequence of transformations. Finally, we define the fold of a sequence as the last element of the sequence of the partial folds.

Definition that specifies how to convert a sequence  $a$  of elements of  $Y$  into a sequence of transformations of  $X$ , given a binary operation  $f : X \times Y \rightarrow X$ .

**definition**

$$\text{Seq2TrSeq}(f,a) \equiv \{\langle k, \text{Fix2ndVar}(f,a(k)) \rangle \mid k \in \text{domain}(a)\}$$

Definition of a sequence of partial folds.

**definition**

$\text{FoldSeq}(f, x, a) \equiv$   
 $\text{InductiveSeqVarFN}(x, \text{fstdom}(f), \text{Seq2TrSeq}(f, a), \text{domain}(a))$

Definition of a fold.

**definition**

$\text{Fold}(f, x, a) \equiv \text{Last}(\text{FoldSeq}(f, x, a))$

If  $X$  is a set with a binary operation  $f : X \times Y \rightarrow X$  then  $\text{Seq2TransSeqN}(f, a)$  converts a sequence  $a$  of elements of  $Y$  into the sequence of corresponding transformations of  $X$ .

**lemma** `seq2trans_seq_props`:

assumes A1:  $n \in \text{nat}$  and A2:  $f : X \times Y \rightarrow X$  and A3:  $a : n \rightarrow Y$  and  
A4:  $T = \text{Seq2TrSeq}(f, a)$

shows

$T : n \rightarrow (X \rightarrow X)$  and  
 $\forall k \in n. \forall x \in X. (T(k))(x) = f(x, a(k))$

**proof** -

from 'a:n $\rightarrow$ Y' have D:  $\text{domain}(a) = n$  using `func1_1_L1` by `simp`  
with A2 A3 A4 show  $T : n \rightarrow (X \rightarrow X)$   
using `apply_funtype` `fix_2nd_var_fun` `ZF_fun_from_total` `Seq2TrSeq_def`  
by `simp`  
with A4 D have I:  $\forall k \in n. T(k) = \text{Fix2ndVar}(f, a(k))$   
using `Seq2TrSeq_def` `ZF_fun_from_tot_val0` by `simp`  
{ fix k fix x assume A5:  $k \in n \quad x \in X$   
with A1 A3 have  $a(k) \in Y$  using `apply_funtype`  
by `auto`  
with A2 A5 I have  $(T(k))(x) = f(x, a(k))$   
using `fix_var_val` by `simp`  
} thus  $\forall k \in n. \forall x \in X. (T(k))(x) = f(x, a(k))$   
by `simp`

**qed**

Basic properties of the sequence of partial folds of a sequence  $a = \{y_k\}_{k \in \{0, \dots, n\}}$ .

**theorem** `fold_seq_props`:

assumes A1:  $n \in \text{nat}$  and A2:  $f : X \times Y \rightarrow X$  and

A3:  $y : n \rightarrow Y$  and A4:  $x \in X$  and A5:  $Y \neq 0$  and

A6:  $F = \text{FoldSeq}(f, x, y)$

shows

$F : \text{succ}(n) \rightarrow X$

$F(0) = x$  and

$\forall k \in n. F(\text{succ}(k)) = f(F(k), y(k))$

**proof** -

let  $T = \text{Seq2TrSeq}(f, y)$   
from A1 A3 have D:  $\text{domain}(y) = n$   
using `func1_1_L1` by `simp`  
from 'f : X $\times$ Y  $\rightarrow$  X' 'Y $\neq$ 0' have I:  $\text{fstdom}(f) = X$   
using `fstdomdef` by `simp`

```

with A1 A2 A3 A4 A6 D show
  II:  $F: \text{succ}(n) \rightarrow X$  and  $F(0) = x$ 
  using seq2trans_seq_props FoldSeq_def fin_indseq_var_f_props
  by auto
from A1 A2 A3 A4 A6 I D have  $\forall k \in n. F(\text{succ}(k)) = T(k)(F(k))$ 
  using seq2trans_seq_props FoldSeq_def fin_indseq_var_f_props
  by simp
moreover
{ fix k assume A5:  $k \in n$  hence  $k \in \text{succ}(n)$  by auto
  with A1 A2 A3 II A5 have  $(T(k))(F(k)) = f(F(k), y(k))$ 
    using apply_funtype seq2trans_seq_props by simp }
ultimately show  $\forall k \in n. F(\text{succ}(k)) = f(F(k), y(k))$ 
  by simp
qed

```

A consistency condition: if we make the list shorter, then we get a shorter sequence of partial folds with the same values as in the original sequence. This can be proven as a special case of `fin_indseq_var_f_restrict` but a proof using `fold_seq_props` and induction turns out to be shorter.

```

lemma foldseq_restrict: assumes
  n ∈ nat    k ∈ succ(n) and
  i ∈ nat    f : X×Y → X    a : n → Y    b : i → Y and
  n ⊆ i      ∀ j ∈ n. b(j) = a(j)    x ∈ X    Y ≠ 0
shows FoldSeq(f,x,b)(k) = FoldSeq(f,x,a)(k)
proof -
  let P = FoldSeq(f,x,a)
  let Q = FoldSeq(f,x,b)
  from assms have
    n ∈ nat    k ∈ succ(n)
    Q(0) = P(0) and
    ∀ j ∈ n. Q(j) = P(j) → Q(succ(j)) = P(succ(j))
    using fold_seq_props by auto
  then show Q(k) = P(k) by (rule fin_nat_ind)
qed

```

A special case of `foldseq_restrict` when the longer sequence is created from the shorter one by appending one element.

```

corollary fold_seq_append:
  assumes n ∈ nat    f : X×Y → X    a:n → Y and
  x∈X    k ∈ succ(n)    y∈Y
  shows FoldSeq(f,x,Append(a,y))(k) = FoldSeq(f,x,a)(k)
proof -
  let b = Append(a,y)
  from assms have b : succ(n) → Y    ∀ j ∈ n. b(j) = a(j)
    using append_props by auto
  with assms show thesis using foldseq_restrict by blast
qed

```

What we really will be using is the notion of the fold of a sequence, which we

define as the last element of (inductively defined) sequence of partial folds.  
The next theorem lists some properties of the product of the fold operation.

```

theorem fold_props:
  assumes A1:  $n \in \text{nat}$  and
  A2:  $f : X \times Y \rightarrow X \quad a : n \rightarrow Y \quad x \in X \quad Y \neq 0$ 
  shows
   $\text{Fold}(f, x, a) = \text{FoldSeq}(f, x, a)(n)$  and
   $\text{Fold}(f, x, a) \in X$ 
proof -
  from assms have  $\text{FoldSeq}(f, x, a) : \text{succ}(n) \rightarrow X$ 
    using fold_seq_props by simp
  with A1 show
     $\text{Fold}(f, x, a) = \text{FoldSeq}(f, x, a)(n)$  and  $\text{Fold}(f, x, a) \in X$ 
    using last_seq_elem apply_funtype Fold_def by auto
qed

```

A corner case: what happens when we fold an empty list?

```

theorem fold_empty: assumes A1:  $f : X \times Y \rightarrow X$  and
  A2:  $a : 0 \rightarrow Y \quad x \in X \quad Y \neq 0$ 
  shows  $\text{Fold}(f, x, a) = x$ 
proof -
  let F =  $\text{FoldSeq}(f, x, a)$ 
  from assms have I:
     $0 \in \text{nat} \quad f : X \times Y \rightarrow X \quad a : 0 \rightarrow Y \quad x \in X \quad Y \neq 0$ 
    by auto
  then have  $\text{Fold}(f, x, a) = F(0)$  by (rule fold_props)
  moreover
  from I have
     $0 \in \text{nat} \quad f : X \times Y \rightarrow X \quad a : 0 \rightarrow Y \quad x \in X \quad Y \neq 0$  and
     $F = \text{FoldSeq}(f, x, a)$  by auto
  then have  $F(0) = x$  by (rule fold_seq_props)
  ultimately show  $\text{Fold}(f, x, a) = x$  by simp
qed

```

The next theorem tells us what happens to the fold of a sequence when we add one more element to it.

```

theorem fold_append:
  assumes A1:  $n \in \text{nat}$  and A2:  $f : X \times Y \rightarrow X$  and
  A3:  $a : n \rightarrow Y$  and A4:  $x \in X$  and A5:  $y \in Y$ 
  shows
   $\text{FoldSeq}(f, x, \text{Append}(a, y))(n) = \text{Fold}(f, x, a)$  and
   $\text{Fold}(f, x, \text{Append}(a, y)) = f(\text{Fold}(f, x, a), y)$ 
proof -
  let b =  $\text{Append}(a, y)$ 
  let P =  $\text{FoldSeq}(f, x, b)$ 
  from A5 have I:  $Y \neq 0$  by auto
  with assms show thesis1:  $P(n) = \text{Fold}(f, x, a)$ 
    using fold_seq_append fold_props by simp

```

```

from assms I have II:
  succ(n) ∈ nat    f : X×Y → X
  b : succ(n) → Y  x∈X  Y ≠ 0
  P = FoldSeq(f,x,b)
  using append_props by auto
then have
  ∀k ∈ succ(n). P(succ(k)) = f⟨P(k), b(k)⟩
  by (rule fold_seq_props)
with A3 A5 thesis1 have P(succ(n)) = f⟨Fold(f,x,a), y⟩
  using append_props by auto
moreover
from II have P : succ(succ(n)) → X
  by (rule fold_seq_props)
then have Fold(f,x,b) = P(succ(n))
  using last_seq_elem Fold_def by simp
ultimately show Fold(f,x,Append(a,y)) = f⟨Fold(f,x,a), y⟩
  by simp
qed

end

```

## 15 Partitions\_ZF.thy

**theory** Partitions\_ZF **imports** Finite\_ZF FiniteSeq\_ZF

**begin**

It is a common trick in proofs that we divide a set into non-overlapping subsets. The first case is when we split the set into two nonempty disjoint sets. Here this is modeled as an ordered pair of sets and the set of such divisions of set  $X$  is called  $\text{Bisections}(X)$ . The second variation on this theme is a set-valued function (aren't they all in ZF?) whose values are nonempty and mutually disjoint.

### 15.1 Bisections

This section is about dividing sets into two non-overlapping subsets.

The set of bisections of a given set  $A$  is a set of pairs of nonempty subsets of  $A$  that do not overlap and their union is equal to  $A$ .

**definition**

$\text{Bisections}(X) = \{p \in \text{Pow}(X) \times \text{Pow}(X) .$   
 $\text{fst}(p) \neq 0 \wedge \text{snd}(p) \neq 0 \wedge \text{fst}(p) \cap \text{snd}(p) = 0 \wedge \text{fst}(p) \cup \text{snd}(p) = X\}$

Properties of bisections.

**lemma** `bisec_props`: **assumes**  $\langle A, B \rangle \in \text{Bisections}(X)$  **shows**  
 $A \neq 0 \ B \neq 0 \ A \subseteq X \ B \subseteq X \ A \cap B = 0 \ A \cup B = X \ X \neq 0$   
**using** `assms Bisections_def` **by** `auto`

Kind of inverse of `bisec_props`: a pair of nonempty disjoint sets form a bisection of their union.

**lemma** `is_bisec`:  
**assumes**  $A \neq 0 \ B \neq 0 \ A \cap B = 0$   
**shows**  $\langle A, B \rangle \in \text{Bisections}(A \cup B)$  **using** `assms Bisections_def`  
**by** `auto`

Bisection of  $X$  is a pair of subsets of  $X$ .

**lemma** `bisec_is_pair`: **assumes**  $Q \in \text{Bisections}(X)$   
**shows**  $Q = \langle \text{fst}(Q), \text{snd}(Q) \rangle$   
**using** `assms Bisections_def` **by** `auto`

The set of bisections of the empty set is empty.

**lemma** `bisec_empty`: **shows**  $\text{Bisections}(0) = 0$   
**using** `Bisections_def` **by** `auto`

The next lemma shows what can we say about bisections of a set with another element added.

**lemma** `bisec_add_point`:

```

assumes A1:  $x \notin X$  and A2:  $\langle A, B \rangle \in \text{Bisections}(X \cup \{x\})$ 
shows  $(A = \{x\} \vee B = \{x\}) \vee (\langle A - \{x\}, B - \{x\} \rangle \in \text{Bisections}(X))$ 
proof -
  { assume  $A \neq \{x\}$  and  $B \neq \{x\}$ 
    with A2 have  $A - \{x\} \neq 0$  and  $B - \{x\} \neq 0$ 
  }
using singl_diff_empty Bisections_def
by auto
  moreover have  $(A - \{x\}) \cup (B - \{x\}) = X$ 
  proof -
    have  $(A - \{x\}) \cup (B - \{x\}) = (A \cup B) - \{x\}$ 
    by auto
  also from assms have  $(A \cup B) - \{x\} = X$ 
  using Bisections_def by auto
  finally show thesis by simp
qed
  moreover from A2 have  $(A - \{x\}) \cap (B - \{x\}) = 0$ 
using Bisections_def by auto
  ultimately have  $\langle A - \{x\}, B - \{x\} \rangle \in \text{Bisections}(X)$ 
using Bisections_def by auto
} thus thesis by auto
qed

```

A continuation of the lemma `bisec_add_point` that refines the case when the pair with removed point bisects the original set.

```

lemma bisec_add_point_case3:
  assumes A1:  $\langle A, B \rangle \in \text{Bisections}(X \cup \{x\})$ 
  and A2:  $\langle A - \{x\}, B - \{x\} \rangle \in \text{Bisections}(X)$ 
  shows
     $(\langle A, B - \{x\} \rangle \in \text{Bisections}(X) \wedge x \in B) \vee$ 
     $(\langle A - \{x\}, B \rangle \in \text{Bisections}(X) \wedge x \in A)$ 
  proof -
    from A1 have  $x \in A \cup B$ 
    using Bisections_def by auto
    hence  $x \in A \vee x \in B$  by simp
    from A1 have  $A - \{x\} = A \vee B - \{x\} = B$ 
    using Bisections_def by auto
    moreover
    { assume  $A - \{x\} = A$ 
      with A2 ' $x \in A \cup B$ ' have
         $\langle A, B - \{x\} \rangle \in \text{Bisections}(X) \wedge x \in B$ 
        using singl_diff_eq by simp }
    moreover
    { assume  $B - \{x\} = B$ 
      with A2 ' $x \in A \cup B$ ' have
         $\langle A - \{x\}, B \rangle \in \text{Bisections}(X) \wedge x \in A$ 
        using singl_diff_eq by simp }
    ultimately show thesis by auto
  qed

```

Another lemma about bisecting a set with an added point.

```
lemma point_set_bisec:
  assumes A1:  $x \notin X$  and A2:  $\langle \{x\}, A \rangle \in \text{Bisections}(X \cup \{x\})$ 
  shows  $A = X$  and  $X \neq 0$ 
proof -
  from A2 have  $A \subseteq X$  using Bisections_def by auto
  moreover
  { fix a assume  $a \in X$ 
    with A2 have  $a \in \{x\} \cup A$  using Bisections_def by simp
    with A1 ' $a \in X$ ' have  $a \in A$  by auto }
  ultimately show  $A = X$  by auto
  with A2 show  $X \neq 0$  using Bisections_def by simp
qed
```

Yet another lemma about bisecting a set with an added point, very similar to point\_set\_bisec with almost the same proof.

```
lemma set_point_bisec:
  assumes A1:  $x \notin X$  and A2:  $\langle A, \{x\} \rangle \in \text{Bisections}(X \cup \{x\})$ 
  shows  $A = X$  and  $X \neq 0$ 
proof -
  from A2 have  $A \subseteq X$  using Bisections_def by auto
  moreover
  { fix a assume  $a \in X$ 
    with A2 have  $a \in A \cup \{x\}$  using Bisections_def by simp
    with A1 ' $a \in X$ ' have  $a \in A$  by auto }
  ultimately show  $A = X$  by auto
  with A2 show  $X \neq 0$  using Bisections_def by simp
qed
```

If a pair of sets bisects a finite set, then both elements of the pair are finite.

```
lemma bisect_fin:
  assumes A1:  $A \in \text{FinPow}(X)$  and A2:  $Q \in \text{Bisections}(A)$ 
  shows  $\text{fst}(Q) \in \text{FinPow}(X)$  and  $\text{snd}(Q) \in \text{FinPow}(X)$ 
proof -
  from A2 have  $\langle \text{fst}(Q), \text{snd}(Q) \rangle \in \text{Bisections}(A)$ 
    using bisec_is_pair by simp
  then have  $\text{fst}(Q) \subseteq A$  and  $\text{snd}(Q) \subseteq A$ 
    using bisec_props by auto
  with A1 show  $\text{fst}(Q) \in \text{FinPow}(X)$  and  $\text{snd}(Q) \in \text{FinPow}(X)$ 
    using FinPow_def subset_Finite by auto
qed
```

## 15.2 Partitions

This sections covers the situation when we have an arbitrary number of sets we want to partition into.

We define a notion of a partition as a set valued function such that the values for different arguments are disjoint. The name is derived from the fact that



such function "partitions" the union of its arguments. Please let me know if you have a better idea for a name for such notion. We would prefer to say "is a partition", but that reserves the letter "a" as a keyword(?) which causes problems.

**definition**

```
Partition ( _ {is partition} [90] 91) where
P {is partition}  $\equiv \forall x \in \text{domain}(P). P(x) \neq 0 \wedge (\forall y \in \text{domain}(P). x \neq y \longrightarrow P(x) \cap P(y) = 0)$ 
```

A fact about lists of mutually disjoint sets.

**lemma** list\_partition: assumes A1:  $n \in \text{nat}$  and

A2:  $a : \text{succ}(n) \rightarrow X$   $a$  {is partition}

shows  $(\bigcup_{i \in n}. a(i)) \cap a(n) = 0$

**proof** -

```
{ assume  $(\bigcup_{i \in n}. a(i)) \cap a(n) \neq 0$ 
  then have  $\exists x. x \in (\bigcup_{i \in n}. a(i)) \cap a(n)$ 
    by (rule nonempty_has_element)
  then obtain x where  $x \in (\bigcup_{i \in n}. a(i))$  and I:  $x \in a(n)$ 
    by auto
  then obtain i where  $i \in n$  and  $x \in a(i)$  by auto
  with A2 I have False
    using mem_imp_not_eq func1_1_L1 Partition_def
    by auto
} thus thesis by auto
```

qed

We can turn every injection into a partition.

**lemma** inj\_partition:

assumes A1:  $b \in \text{inj}(X, Y)$

shows

$\forall x \in X. \{ \langle x, \{b(x)\} \rangle. x \in X \} (x) = \{b(x)\}$  and

$\{ \langle x, \{b(x)\} \rangle. x \in X \}$  {is partition}

**proof** -

```
let p =  $\{ \langle x, \{b(x)\} \rangle. x \in X \}$ 
{ fix x assume  $x \in X$ 
  from A1 have  $b : X \rightarrow Y$  using inj_def
    by simp
  with 'x  $\in X$ ' have  $\{b(x)\} \in \text{Pow}(Y)$ 
    using apply_funtype by simp
} hence  $\forall x \in X. \{b(x)\} \in \text{Pow}(Y)$  by simp
then have  $p : X \rightarrow \text{Pow}(Y)$  using ZF_fun_from_total
  by simp
then have  $\text{domain}(p) = X$  using func1_1_L1
  by simp
from 'p :  $X \rightarrow \text{Pow}(Y)$ ' show I:  $\forall x \in X. p(x) = \{b(x)\}$ 
  using ZF_fun_from_tot_val0 by simp
{ fix x assume  $x \in X$ 
  with I have  $p(x) = \{b(x)\}$  by simp
```

```

    hence  $p(x) \neq 0$  by simp
  moreover
    { fix t assume  $t \in X$  and  $x \neq t$ 
      with A1 ' $x \in X$ ' have  $b(x) \neq b(t)$  using inj_def
    by auto
      with I ' $x \in X$ ' ' $t \in X$ ' have  $p(x) \cap p(t) = 0$ 
    by auto }
    ultimately have
       $p(x) \neq 0 \wedge (\forall t \in X. x \neq t \longrightarrow p(x) \cap p(t) = 0)$ 
    by simp
  } with 'domain(p) = X' show { $\langle x, \{b(x)\} \rangle. x \in X$ } {is partition}
    using Partition_def by simp
qed

```

end

## 16 Enumeration\_ZF.thy

```
theory Enumeration_ZF imports NatOrder_ZF FiniteSeq_ZF FinOrd_ZF
```

```
begin
```

Suppose  $r$  is a linear order on a set  $A$  that has  $n$  elements, where  $n \in \mathbb{N}$ . In the `FinOrd_ZF` theory we prove a theorem stating that there is a unique order isomorphism between  $n = \{0, 1, \dots, n-1\}$  (with natural order) and  $A$ . Another way of stating that is that there is a unique way of counting the elements of  $A$  in the order increasing according to relation  $r$ . Yet another way of stating the same thing is that there is a unique sorted list of elements of  $A$ . We will call this list the `Enumeration` of  $A$ .

### 16.1 Enumerations: definition and notation

In this section we introduce the notion of enumeration and define a proof context (a "locale" in Isabelle terms) that sets up the notation for writing about enumerations.

We define enumeration as the only order isomorphism between a set  $A$  and the number of its elements. We are using the formula  $\bigcup\{x\} = x$  to extract the only element from a singleton. `Le` is the (natural) order on natural numbers, defined in `Nat_ZF` theory in the standard Isabelle library.

**definition**

$$\text{Enumeration}(A, r) \equiv \bigcup \text{ord\_iso}(|A|, \text{Le}, A, r)$$

To set up the notation we define a locale `enums`. In this locale we will assume that  $r$  is a linear order on some set  $X$ . In most applications this set will be just the set of natural numbers. Standard Isabelle uses  $\leq$  to denote the "less or equal" relation on natural numbers. We will use the  $\leq$  symbol to denote the relation  $r$ . Those two symbols usually look the same in the presentation, but they are different in the source. To shorten the notation the enumeration `Enumeration(A, r)` will be denoted as  $\sigma(A)$ . Similarly as in the `Semigroup` theory we will write  $a \leftarrow x$  for the result of appending an element  $x$  to the finite sequence (list)  $a$ . Finally,  $a \sqcup b$  will denote the concatenation of the lists  $a$  and  $b$ .

**locale** `enums` =

```
fixes X r
assumes linord: IsLinOrder(X, r)

fixes ler (infix ≤ 70)
defines ler_def[simp]: x ≤ y ≡ ⟨x, y⟩ ∈ r

fixes σ
```

```

defines  $\sigma\_def$  [simp]:  $\sigma(A) \equiv \text{Enumeration}(A,r)$ 

fixes append (infix  $\hookleftarrow$  72)
defines append_def[simp]:  $a \hookleftarrow x \equiv \text{Append}(a,x)$ 

fixes concat (infixl  $\sqcup$  69)
defines concat_def[simp]:  $a \sqcup b \equiv \text{Concat}(a,b)$ 

```

## 16.2 Properties of enumerations

In this section we prove basic facts about enumerations.

A special case of the existence and uniqueness of the order isomorphism for finite sets when the first set is a natural number.

```

lemma (in enums) ord_iso_nat_fin:
  assumes  $A \in \text{FinPow}(X)$  and  $n \in \text{nat}$  and  $A \approx n$ 
  shows  $\exists! f. f \in \text{ord\_iso}(n, \text{Le}, A, r)$ 
  using assms NatOrder_ZF_1_L2 linord nat_finpow_nat
  fin_ord_iso_ex_uniq by simp

```

An enumeration is an order isomorphism, a bijection, and a list.

```

lemma (in enums) enum_props: assumes  $A \in \text{FinPow}(X)$ 
  shows
     $\sigma(A) \in \text{ord\_iso}(|A|, \text{Le}, A, r)$ 
     $\sigma(A) \in \text{bij}(|A|, A)$ 
     $\sigma(A) : |A| \rightarrow A$ 
  proof -
    from assms have
       $\text{IsLinOrder}(\text{nat}, \text{Le})$  and  $|A| \in \text{FinPow}(\text{nat})$  and  $A \approx |A|$ 
      using NatOrder_ZF_1_L2 card_fin_is_nat nat_finpow_nat
      by auto
    with assms show  $\sigma(A) \in \text{ord\_iso}(|A|, \text{Le}, A, r)$ 
      using linord fin_ord_iso_ex_uniq singleton_extract
      Enumeration_def by simp
    then show  $\sigma(A) \in \text{bij}(|A|, A)$  and  $\sigma(A) : |A| \rightarrow A$ 
      using ord_iso_def bij_def surj_def
      by auto
  qed

```

A corollary from `enum_props`. Could have been attached as another assertion, but this slows down verification of some other proofs.

```

lemma (in enums) enum_fun: assumes  $A \in \text{FinPow}(X)$ 
  shows  $\sigma(A) : |A| \rightarrow X$ 
  proof -
    from assms have  $\sigma(A) : |A| \rightarrow A$  and  $A \subseteq X$ 
      using enum_props FinPow_def by auto
    then show  $\sigma(A) : |A| \rightarrow X$  by (rule func1_1_L1B)
  qed

```

If a list is an order isomorphism then it must be the enumeration.

```
lemma (in enums) ord_iso_enum: assumes A1: A ∈ FinPow(X) and
  A2: n ∈ nat and A3: f ∈ ord_iso(n,Le,A,r)
  shows f = σ(A)
proof -
  from A3 have n ≈ A using ord_iso_def eqpoll_def
  by auto
  then have A ≈ n by (rule eqpoll_sym)
  with A1 A2 have ∃!f. f ∈ ord_iso(n,Le,A,r)
  using ord_iso_nat_fin by simp
  with assms 'A ≈ n' show f = σ(A)
  using enum_props card_card by blast
qed
```

What is the enumeration of the empty set?

```
lemma (in enums) empty_enum: shows σ(0) = 0
proof -
  have
    0 ∈ FinPow(X) and 0 ∈ nat and 0 ∈ ord_iso(0,Le,0,r)
  using empty_in_finpow empty_ord_iso_empty
  by auto
  then show σ(0) = 0 using ord_iso_enum
  by blast
qed
```

Adding a new maximum to a set appends it to the enumeration.

```
lemma (in enums) enum_append:
  assumes A1: A ∈ FinPow(X) and A2: b ∈ X-A and
  A3: ∀a∈A. a ≤ b
  shows σ(A ∪ {b}) = σ(A) ↦ b
proof -
  let f = σ(A) ∪ {( |A|, b)}
  from A1 have |A| ∈ nat using card_fin_is_nat
  by simp
  from A1 A2 have A ∪ {b} ∈ FinPow(X)
  using singleton_in_finpow union_finpow by simp
  moreover from this have |A ∪ {b}| ∈ nat
  using card_fin_is_nat by simp
  moreover have f ∈ ord_iso(|A ∪ {b}|, Le, A ∪ {b}, r)
proof -
  from A1 A2 have
    σ(A) ∈ ord_iso(|A|, Le, A, r) and
    |A| < |A| and b < A
  using enum_props mem_not_refl by auto
  moreover from '|A| ∈ nat' have
    ∀k ∈ |A|. ⟨k, |A|⟩ ∈ Le
  using elem_nat_is_nat by blast
  moreover from A3 have ∀a∈A. ⟨a, b⟩ ∈ r by simp
  moreover have antisym(Le) and antisym(r)
```

```

        using linord NatOrder_ZF_1_L2 IsLinOrder_def by auto
    moreover
    from A2 ' $|A| \in \text{nat}$ ' have
         $\langle |A|, |A| \rangle \in \text{Le}$  and  $\langle b, b \rangle \in r$ 
        using linord NatOrder_ZF_1_L2 IsLinOrder_def
total_is_refl refl_def by auto
    hence  $\langle |A|, |A| \rangle \in \text{Le} \longleftrightarrow \langle b, b \rangle \in r$  by simp
    ultimately have  $f \in \text{ord\_iso}(|A| \cup \{|A|\}, \text{Le}, A \cup \{b\}, r)$ 
        by (rule ord_iso_extend)
    with A1 A2 show  $f \in \text{ord\_iso}(|A \cup \{b\}|, \text{Le}, A \cup \{b\}, r)$ 
        using card_fin_add_one by simp
qed
ultimately have  $f = \sigma(A \cup \{b\})$ 
    using ord_iso_enum by simp
moreover have  $\sigma(A) \leftarrow b = f$ 
proof -
    have  $\sigma(A) \leftarrow b = \sigma(A) \cup \{\langle \text{domain}(\sigma(A)), b \rangle\}$ 
        using Append_def by simp
    moreover from A1 have  $\text{domain}(\sigma(A)) = |A|$ 
        using enum_props func1_1_L1 by blast
    ultimately show  $\sigma(A) \leftarrow b = f$  by simp
qed
ultimately show  $\sigma(A \cup \{b\}) = \sigma(A) \leftarrow b$  by simp
qed

```

What is the enumeration of a singleton?

```

lemma (in enums) enum_singleton:
  assumes A1:  $x \in X$  shows  $\sigma(\{x\}): 1 \rightarrow X$  and  $\sigma(\{x\})(0) = x$ 
proof -
  from A1 have
     $0 \in \text{FinPow}(X)$  and  $x \in (X - 0)$  and  $\forall a \in 0. a \leq x$ 
    using empty_in_finpow by auto
  then have  $\sigma(0 \cup \{x\}) = \sigma(0) \leftarrow x$  by (rule enum_append)
  with A1 show  $\sigma(\{x\}): 1 \rightarrow X$  and  $\sigma(\{x\})(0) = x$ 
    using empty_enum empty_append1 by auto
qed

```

end

## 17 Semigroup\_ZF.thy

```
theory Semigroup_ZF imports Partitions_ZF Fold_ZF Enumeration_ZF
```

```
begin
```

It seems that the minimal setup needed to talk about a product of a sequence is a set with a binary operation. Such object is called "magma". However, interesting properties show up when the binary operation is associative and such algebraic structure is called a semigroup. In this theory file we define and study sequences of partial products of sequences of magma and semigroup elements.

### 17.1 Products of sequences of semigroup elements

Semigroup is a magma in which the binary operation is associative. In this section we mostly study the products of sequences of elements of semigroup. The goal is to establish the fact that taking the product of a sequence is distributive with respect to concatenation of sequences, i.e for two sequences  $a, b$  of the semigroup elements we have  $\prod(a \sqcup b) = (\prod a) \cdot (\prod b)$ , where " $a \sqcup b$ " is concatenation of  $a$  and  $b$  ( $a++b$  in Haskell notation). Less formally, we want to show that we can discard parantheses in expressions of the form  $(a_0 \cdot a_1 \cdot \dots \cdot a_n) \cdot (b_0 \cdot \dots \cdot b_k)$ .

First we define a notion similar to `Fold`, except that the initial element of the fold is given by the first element of sequence. By analogy with Haskell fold we call that `Fold1`

**definition**

```
Fold1(f,a)  $\equiv$  Fold(f,a(0),Tail(a))
```

The definition of the `semigr0` context below introduces notation for writing about finite sequences and semigroup products. In the context we fix the carrier and denote it  $G$ . The binary operation on  $G$  is called  $f$ . All theorems proven in the context `semigr0` will implicitly assume that  $f$  is an associative operation on  $G$ . We will use multiplicative notation for the semigroup operation. The product of a sequence  $a$  is denoted  $\prod a$ . We will write  $a \leftarrow x$  for the result of appending an element  $x$  to the finite sequence (list)  $a$ . This is a bit nonstandard, but I don't have a better idea for the "append" notation. Finally,  $a \sqcup b$  will denote the concatenation of the lists  $a$  and  $b$ .

```
locale semigr0 =
```

```
  fixes G f
```

```
  assumes assoc_assum: f {is associative on} G
```

```
  fixes prod (infixl  $\cdot$  72)
```

```

defines prod_def [simp]:  $x \cdot y \equiv f\langle x, y \rangle$ 

fixes seqprod ( $\prod$  _ 71)
defines seqprod_def [simp]:  $\prod a \equiv \text{Fold1}(f, a)$ 

fixes append (infix  $\leftarrow$  72)
defines append_def [simp]:  $a \leftarrow x \equiv \text{Append}(a, x)$ 

fixes concat (infixl  $\sqcup$  69)
defines concat_def [simp]:  $a \sqcup b \equiv \text{Concat}(a, b)$ 

```

The next lemma shows our assumption on the associativity of the semigroup operation in the notation defined in in the `semigr0` context.

```

lemma (in semigr0) semigr_assoc: assumes  $x \in G \quad y \in G \quad z \in G$ 
shows  $x \cdot y \cdot z = x \cdot (y \cdot z)$ 
using assms assoc_assum IsAssociative_def by simp

```

In the way we define associativity the assumption that  $f$  is associative on  $G$  also implies that it is a binary operation on  $X$ .

```

lemma (in semigr0) semigr_binop: shows  $f : G \times G \rightarrow G$ 
using assoc_assum IsAssociative_def by simp

```

Semigroup operation is closed.

```

lemma (in semigr0) semigr_closed:
assumes  $a \in G \quad b \in G$  shows  $a \cdot b \in G$ 
using assms semigr_binop apply_funtype by simp

```

Lemma `append_1elem` written in the notation used in the `semigr0` context.

```

lemma (in semigr0) append_1elem_nice:
assumes  $n \in \text{nat}$  and  $a : n \rightarrow X$  and  $b : 1 \rightarrow X$ 
shows  $a \sqcup b = a \leftarrow b(0)$ 
using assms append_1elem by simp

```

Lemma `concat_init_last_elem` rewritten in the notation used in the `semigr0` context.

```

lemma (in semigr0) concat_init_last:
assumes  $n \in \text{nat} \quad k \in \text{nat}$  and
 $a : n \rightarrow X$  and  $b : \text{succ}(k) \rightarrow X$ 
shows  $(a \sqcup \text{Init}(b)) \leftarrow b(k) = a \sqcup b$ 
using assms concat_init_last_elem by simp

```

The product of semigroup (actually, magma – we don't need associativity for this) elements is in the semigroup.

```

lemma (in semigr0) prod_type:
assumes  $n \in \text{nat}$  and  $a : \text{succ}(n) \rightarrow G$ 
shows  $(\prod a) \in G$ 
proof -

```



```

from assms have
  succ(n) ∈ nat  f : G×G → G  Tail(a) : n → G
  using semigr_binop tail_props by auto
moreover from assms have a(0) ∈ G and G ≠ 0
  using empty_in_every_succ apply_funtype
  by auto
ultimately show (∏ a) ∈ G using Fold1_def fold_props
  by simp
qed

```

What is the product of one element list?

```

lemma (in semigr0) prod_of_1elem: assumes A1: a: 1 → G
  shows (∏ a) = a(0)
proof -
  have f : G×G → G using semigr_binop by simp
  moreover from A1 have Tail(a) : 0 → G using tail_props
    by blast
  moreover from A1 have a(0) ∈ G and G ≠ 0
    using apply_funtype by auto
  ultimately show (∏ a) = a(0) using fold_empty Fold1_def
    by simp
qed

```

What happens to the product of a list when we append an element to the list?

```

lemma (in semigr0) prod_append: assumes A1: n ∈ nat and
  A2: a : succ(n) → G and A3: x∈G
  shows (∏ a↔x) = (∏ a) · x
proof -
  from A1 A2 have I: Tail(a) : n → G  a(0) ∈ G
    using tail_props empty_in_every_succ apply_funtype
    by auto
  from assms have (∏ a↔x) = Fold(f,a(0),Tail(a)↔x)
    using head_of_append tail_append_commute Fold1_def
    by simp
  also from A1 A3 I have ... = (∏ a) · x
    using semigr_binop fold_append Fold1_def
    by simp
  finally show thesis by simp
qed

```

The main theorem of the section: taking the product of a sequence is distributive with respect to concatenation of sequences. The proof is by induction on the length of the second list.

```

theorem (in semigr0) prod_conc_distr:
  assumes A1: n ∈ nat  k ∈ nat and
  A2: a : succ(n) → G  b: succ(k) → G
  shows (∏ a) · (∏ b) = ∏ (a ⧻ b)

```

```

proof -
  from A1 have k ∈ nat by simp
  moreover have ∀b ∈ succ(0) → G. (∏ a) · (∏ b) = ∏ (a ⊔ b)
  proof -
    { fix b assume A3: b : succ(0) → G
      with A1 A2 have
succ(n) ∈ nat  a : succ(n) → G  b : 1 → G
    by auto
      then have a ⊔ b = a ← b(0) by (rule append_1elem_nice)
      with A1 A2 A3 have (∏ a) · (∏ b) = ∏ (a ⊔ b)
    using apply_funtype prod_append semigr_binop prod_of_1elem
    by simp
  } thus thesis by simp
qed
moreover have ∀j ∈ nat.
  (∀b ∈ succ(j) → G. (∏ a) · (∏ b) = ∏ (a ⊔ b)) →
  (∀b ∈ succ(succ(j)) → G. (∏ a) · (∏ b) = ∏ (a ⊔ b))
proof -
  { fix j assume A4: j ∈ nat and
    A5: (∀b ∈ succ(j) → G. (∏ a) · (∏ b) = ∏ (a ⊔ b))
    { fix b assume A6: b : succ(succ(j)) → G
      let c = Init(b)
      from A4 A6 have T: b(succ(j)) ∈ G and
        I: c : succ(j) → G and II: b = c ← b(succ(j))
      using apply_funtype init_props by auto
      from A1 A2 A4 A6 have
succ(n) ∈ nat  succ(j) ∈ nat
        a : succ(n) → G  b : succ(succ(j)) → G
      by auto
      then have III: (a ⊔ c) ← b(succ(j)) = a ⊔ b
      by (rule concat_init_last)
      from A4 I T have (∏ c ← b(succ(j))) = (∏ c) · b(succ(j))
      by (rule prod_append)
      with II have
(∏ a) · (∏ b) = (∏ a) · ((∏ c) · b(succ(j)))
      by simp
      moreover from A1 A2 A4 T I have
(∏ a) ∈ G  (∏ c) ∈ G  b(succ(j)) ∈ G
      using prod_type by auto
      ultimately have
(∏ a) · (∏ b) = ((∏ a) · (∏ c)) · b(succ(j))
      using semigr_assoc by auto
      with A5 I have (∏ a) · (∏ b) = (∏ (a ⊔ c)) · b(succ(j))
      by simp
      moreover
      from A1 A2 A4 I have
T1: succ(n) ∈ nat  succ(j) ∈ nat and
        a : succ(n) → G  c : succ(j) → G
      by auto
    }
  }

```

```

then have Concat(a,c): succ(n) #+ succ(j) → G
  by (rule concat_props)
with A1 A4 T have
  succ(n #+ j) ∈ nat
  a ⊔ c : succ(succ(n #+j)) → G
  b(succ(j)) ∈ G
  using succ_plus by auto
then have
  (⋀ (a ⊔ c) ↔ b(succ(j))) = (⋀ (a ⊔ c)) · b(succ(j))
  by (rule prod_append)
with III have (⋀ (a ⊔ c)) · b(succ(j)) = ⋀ (a ⊔ b)
  by simp
ultimately have (⋀ a) · (⋀ b) = ⋀ (a ⊔ b)
  by simp
} hence (∀ b ∈ succ(succ(j)) → G. (⋀ a) · (⋀ b) = ⋀ (a ⊔ b))
by simp
} thus thesis by blast
qed
ultimately have ∀ b ∈ succ(k) → G. (⋀ a) · (⋀ b) = ⋀ (a ⊔ b)
  by (rule ind_on_nat)
with A2 show (⋀ a) · (⋀ b) = ⋀ (a ⊔ b) by simp
qed

```

## 17.2 Products over sets of indices

In this section we study the properties of expressions of the form  $\prod_{i \in \Lambda} a_i = a_{i_0} \cdot a_{i_1} \cdot \dots \cdot a_{i_{n-1}}$ , i.e. what we denote as  $\prod(\Lambda, a)$ .  $\Lambda$  here is a finite subset of some set  $X$  and  $a$  is a function defined on  $X$  with values in the semigroup  $G$ .

Suppose  $a : X \rightarrow G$  is an indexed family of elements of a semigroup  $G$  and  $\Lambda = \{i_0, i_1, \dots, i_{n-1}\} \subseteq \mathbb{N}$  is a finite set of indices. We want to define  $\prod_{i \in \Lambda} a_i = a_{i_0} \cdot a_{i_1} \cdot \dots \cdot a_{i_{n-1}}$ . To do that we use the notion of **Enumeration** defined in the **Enumeration\_ZF** theory file that takes a set of indices and lists them in increasing order, thus converting it to list. Then we use the **Fold1** to multiply the resulting list. Recall that in Isabelle/ZF the capital letter "O" denotes the composition of two functions (or relations).

### definition

$\text{SetFold}(f, a, \Lambda, r) = \text{Fold1}(f, a \circ \text{Enumeration}(\Lambda, r))$

For a finite subset  $\Lambda$  of a linearly ordered set  $X$  we will write  $\sigma(\Lambda)$  to denote the enumeration of the elements of  $\Lambda$ , i.e. the only order isomorphism  $|\Lambda| \rightarrow \Lambda$ , where  $|\Lambda| \in \mathbb{N}$  is the number of elements of  $\Lambda$ . We also define notation for taking a product over a set of indices of some sequence of semigroup elements. The product of semigroup elements over some set  $\Lambda \subseteq X$  of indices of a sequence  $a : X \rightarrow G$  (i.e.  $\prod_{i \in \Lambda} a_i$ ) is denoted  $\prod(\Lambda, a)$ . In the **semigr1** context we assume that  $a$  is a function defined on some linearly

ordered set  $X$  with values in the semigroup  $G$ .

```

locale semigr1 = semigr0 +

  fixes X r
  assumes linord: IsLinOrder(X,r)

  fixes a
  assumes a_is_fun: a : X → G

  fixes σ
  defines σ_def [simp]: σ(A) ≡ Enumeration(A,r)

  fixes setpr (∏)
  defines setpr_def [simp]: ∏(Λ,b) ≡ SetFold(f,b,Λ,r)

```

We can use the `enums` locale in the `semigr0` context.

```

lemma (in semigr1) enums_valid_in_semigr1: shows enums(X,r)
  using linord enums_def by simp

```

Definition of product over a set expressed in notation of the `semigr0` locale.

```

lemma (in semigr1) setproddef:
  shows ∏(Λ,a) = ∏ (a 0 σ(Λ))
  using SetFold_def by simp

```

A composition of enumeration of a nonempty finite subset of  $\mathbb{N}$  with a sequence of elements of  $G$  is a nonempty list of elements of  $G$ . This implies that a product over set of a finite set of indices belongs to the (carrier of) semigroup.

```

lemma (in semigr1) setprod_type: assumes
  A1: Λ ∈ FinPow(X) and A2: Λ ≠ 0
  shows
    ∃ n ∈ nat . |Λ| = succ(n) ∧ a 0 σ(Λ) : succ(n) → G
    and ∏(Λ,a) ∈ G
proof -
  from assms obtain n where n ∈ nat and |Λ| = succ(n)
    using card_non_empty_succ by auto
  from A1 have σ(Λ) : |Λ| → Λ
    using enums_valid_in_semigr1 enums.enum_props
    by simp
  with A1 have a 0 σ(Λ): |Λ| → G
    using a_is_fun FinPow_def comp_fun_subset
    by simp
  with 'n ∈ nat' and '|Λ| = succ(n)' show
    ∃ n ∈ nat . |Λ| = succ(n) ∧ a 0 σ(Λ) : succ(n) → G
    by auto
  from 'n ∈ nat' '|Λ| = succ(n)' 'a 0 σ(Λ): |Λ| → G'
  show ∏(Λ,a) ∈ G using prod_type setproddef
    by auto

```

qed

The `enum_append` lemma from the `Enumeration` theory specialized for natural numbers.

```
lemma (in semigr1) semigr1_enum_append:
  assumes  $\Lambda \in \text{FinPow}(X)$  and
   $n \in X - \Lambda$  and  $\forall k \in \Lambda. \langle k, n \rangle \in r$ 
  shows  $\sigma(\Lambda \cup \{n\}) = \sigma(\Lambda) \leftarrow n$ 
  using assms FinPow_def enums_valid_in_semigr1
  enums.enum_append by simp
```

What is product over a singleton?

```
lemma (in semigr1) gen_prod_singleton:
  assumes A1:  $x \in X$ 
  shows  $\prod(\{x\}, a) = a(x)$ 
proof -
  from A1 have  $\sigma(\{x\}): 1 \rightarrow X$  and  $\sigma(\{x\})(0) = x$ 
    using enums_valid_in_semigr1 enums.enum_singleton
    by auto
  then show  $\prod(\{x\}, a) = a(x)$ 
    using a_is_fun comp_fun setproddef prod_of_1elem
    comp_fun_apply by simp
```

qed

A generalization of `prod_append` to the products over sets of indices.

```
lemma (in semigr1) gen_prod_append:
  assumes
  A1:  $\Lambda \in \text{FinPow}(X)$  and A2:  $\Lambda \neq 0$  and
  A3:  $n \in X - \Lambda$  and
  A4:  $\forall k \in \Lambda. \langle k, n \rangle \in r$ 
  shows  $\prod(\Lambda \cup \{n\}, a) = (\prod(\Lambda, a)) \cdot a(n)$ 
proof -
  have  $\prod(\Lambda \cup \{n\}, a) = \prod (a \circ \sigma(\Lambda \cup \{n\}))$ 
    using setproddef by simp
  also from A1 A3 A4 have  $\dots = \prod (a \circ (\sigma(\Lambda) \leftarrow n))$ 
    using semigr1_enum_append by simp
  also have  $\dots = \prod ((a \circ \sigma(\Lambda)) \leftarrow a(n))$ 
  proof -
    from A1 A3 have
       $|\Lambda| \in \text{nat}$  and  $\sigma(\Lambda) : |\Lambda| \rightarrow X$  and  $n \in X$ 
      using card_fin_is_nat enums_valid_in_semigr1 enums.enum_fun
      by auto
    then show thesis using a_is_fun list_compose_append
      by simp
  qed
  also from assms have  $\dots = (\prod (a \circ \sigma(\Lambda))) \cdot a(n)$ 
    using a_is_fun setprod_type apply_funtype prod_append
    by blast
  also have  $\dots = (\prod(\Lambda, a)) \cdot a(n)$ 
```

```

    using SetFold_def by simp
    finally show  $\prod(\Lambda \cup \{n\}, a) = (\prod(\Lambda, a)) \cdot a(n)$ 
    by simp
qed

```

Very similar to `gen_prod_append`: a relation between a product over a set of indices and the product over the set with the maximum removed.

```

lemma (in semigr1) gen_product_rem_point:
  assumes A1:  $A \in \text{FinPow}(X)$  and
  A2:  $n \in A$  and A4:  $A - \{n\} \neq 0$  and
  A3:  $\forall k \in A. \langle k, n \rangle \in r$ 
  shows
     $(\prod(A - \{n\}, a)) \cdot a(n) = \prod(A, a)$ 
proof -
  let  $\Lambda = A - \{n\}$ 
  from A1 A2 have  $\Lambda \in \text{FinPow}(X)$  and  $n \in X - \Lambda$ 
  using fin_rem_point_fin FinPow_def by auto
  with A3 A4 have  $\prod(\Lambda \cup \{n\}, a) = (\prod(\Lambda, a)) \cdot a(n)$ 
  using a_is_fun gen_prod_append by blast
  with A2 show thesis using rem_add_eq by simp
qed

```

### 17.3 Commutative semigroups

Commutative semigroups are those whose operation is commutative, i.e.  $a \cdot b = b \cdot a$ . This implies that for any permutation  $s : n \rightarrow n$  we have  $\prod_{j=0}^n a_j = \prod_{j=0}^n a_{s(j)}$ , or, closer to the notation we are using in the `semigr0` context,  $\prod a = \prod(a \circ s)$ . Maybe one day we will be able to prove this, but for now the goal is to prove something simpler: that if the semigroup operation is commutative taking the product of a sequence is distributive with respect to the operation:  $\prod_{j=0}^n (a_j \cdot b_j) = \left(\prod_{j=0}^n a_j\right) \left(\prod_{j=0}^n b_j\right)$ . Many of the rearrangements (namely those that don't use the inverse) proven in the `AbelianGroup_ZF` theory hold in fact in semigroups. Some of them will be reproven in this section.

A rearrangement with 3 elements.

```

lemma (in semigr0) rearr3elems:
  assumes f {is commutative on} G and a ∈ G b ∈ G c ∈ G
  shows a · b · c = a · c · b
  using assms semigr_assoc IsCommutative_def by simp

```

A rearrangement of four elements.

```

lemma (in semigr0) rearr4elems:
  assumes A1: f {is commutative on} G and
  A2: a ∈ G b ∈ G c ∈ G d ∈ G
  shows a · b · (c · d) = a · c · (b · d)
proof -

```

```

from A2 have a·b·(c·d) = a·b·c·d
  using semigr_closed semigr_assoc by simp
also have a·b·c·d = a·c·(b·d)
proof -
  from A1 A2 have a·b·c·d = c·(a·b)·d
    using IsCommutative_def semigr_closed
    by simp
  also from A2 have ... = c·a·b·d
    using semigr_closed semigr_assoc
    by simp
  also from A1 A2 have ... = a·c·b·d
    using IsCommutative_def semigr_closed
    by simp
  also from A2 have ... = a·c·(b·d)
    using semigr_closed semigr_assoc
    by simp
  finally show a·b·c·d = a·c·(b·d) by simp
qed
finally show a·b·(c·d) = a·c·(b·d)
  by simp
qed

```

We start with a version of `prod_append` that will shorten a bit the proof of the main theorem.

```

lemma (in semigr0) shorter_seq: assumes A1: k ∈ nat and
  A2: a ∈ succ(succ(k)) → G
  shows (∏ a) = (∏ Init(a)) · a(succ(k))
proof -
  let x = Init(a)
  from assms have
    a(succ(k)) ∈ G and x : succ(k) → G
    using apply_funtype init_props by auto
  with A1 have (∏ x↔a(succ(k))) = (∏ x) · a(succ(k))
    using prod_append by simp
  with assms show thesis using init_props
    by simp
qed

```

A lemma useful in the induction step of the main theorem.

```

lemma (in semigr0) prod_distr_ind_step:
  assumes A1: k ∈ nat and
  A2: a : succ(succ(k)) → G and
  A3: b : succ(succ(k)) → G and
  A4: c : succ(succ(k)) → G and
  A5: ∀ j∈succ(succ(k)). c(j) = a(j) · b(j)
  shows
    Init(a) : succ(k) → G
    Init(b) : succ(k) → G
    Init(c) : succ(k) → G

```

```

 $\forall j \in \text{succ}(k). \text{Init}(c)(j) = \text{Init}(a)(j) \cdot \text{Init}(b)(j)$ 
proof -
  from A1 A2 A3 A4 show
     $\text{Init}(a) : \text{succ}(k) \rightarrow G$ 
     $\text{Init}(b) : \text{succ}(k) \rightarrow G$ 
     $\text{Init}(c) : \text{succ}(k) \rightarrow G$ 
    using init_props by auto
  from A1 have T:  $\text{succ}(k) \in \text{nat}$  by simp
  from T A2 have  $\forall j \in \text{succ}(k). \text{Init}(a)(j) = a(j)$ 
    by (rule init_props)
  moreover from T A3 have  $\forall j \in \text{succ}(k). \text{Init}(b)(j) = b(j)$ 
    by (rule init_props)
  moreover from T A4 have  $\forall j \in \text{succ}(k). \text{Init}(c)(j) = c(j)$ 
    by (rule init_props)
  moreover from A5 have  $\forall j \in \text{succ}(k). c(j) = a(j) \cdot b(j)$ 
    by simp
  ultimately show  $\forall j \in \text{succ}(k). \text{Init}(c)(j) = \text{Init}(a)(j) \cdot \text{Init}(b)(j)$ 
    by simp
qed

```

For commutative operations taking the product of a sequence is distributive with respect to the operation. This version will probably not be used in applications, it is formulated in a way that is easier to prove by induction. For a more convenient formulation see `prod_comm_distrib`. The proof by induction on the length of the sequence.

```

theorem (in semigr0) prod_comm_distr:
  assumes A1:  $f \text{ \{is commutative on\} } G$  and A2:  $n \in \text{nat}$ 
  shows  $\forall a b c.$ 
     $(a : \text{succ}(n) \rightarrow G \wedge b : \text{succ}(n) \rightarrow G \wedge c : \text{succ}(n) \rightarrow G \wedge$ 
     $(\forall j \in \text{succ}(n). c(j) = a(j) \cdot b(j))) \rightarrow$ 
     $(\prod c) = (\prod a) \cdot (\prod b)$ 
proof -
  note A2
  moreover have  $\forall a b c.$ 
     $(a : \text{succ}(0) \rightarrow G \wedge b : \text{succ}(0) \rightarrow G \wedge c : \text{succ}(0) \rightarrow G \wedge$ 
     $(\forall j \in \text{succ}(0). c(j) = a(j) \cdot b(j))) \rightarrow$ 
     $(\prod c) = (\prod a) \cdot (\prod b)$ 
  proof -
    { fix a b c
      assume  $a : \text{succ}(0) \rightarrow G \wedge b : \text{succ}(0) \rightarrow G \wedge c : \text{succ}(0) \rightarrow G \wedge$ 
       $(\forall j \in \text{succ}(0). c(j) = a(j) \cdot b(j))$ 
      then have
      I:  $a : 1 \rightarrow G \quad b : 1 \rightarrow G \quad c : 1 \rightarrow G$  and
      II:  $c(0) = a(0) \cdot b(0)$  by auto
      from I have
       $(\prod a) = a(0)$  and  $(\prod b) = b(0)$  and  $(\prod c) = c(0)$ 
      using prod_of_1elem by auto
      with II have  $(\prod c) = (\prod a) \cdot (\prod b)$  by simp
    } then show thesis using Fold1_def by simp

```



```

qed
moreover have  $\forall k \in \text{nat}.$ 
  ( $\forall a b c.$ 
    ( $a : \text{succ}(k) \rightarrow G \wedge b : \text{succ}(k) \rightarrow G \wedge c : \text{succ}(k) \rightarrow G \wedge$ 
      ( $\forall j \in \text{succ}(k). c(j) = a(j) \cdot b(j)$ ))  $\longrightarrow$ 
      ( $\prod c$ ) = ( $\prod a$ )  $\cdot$  ( $\prod b$ ))  $\longrightarrow$ 
      ( $\forall a b c.$ 
        ( $a : \text{succ}(\text{succ}(k)) \rightarrow G \wedge b : \text{succ}(\text{succ}(k)) \rightarrow G \wedge c : \text{succ}(\text{succ}(k)) \rightarrow G$ 
           $\wedge$ 
          ( $\forall j \in \text{succ}(\text{succ}(k)). c(j) = a(j) \cdot b(j)$ ))  $\longrightarrow$ 
            ( $\prod c$ ) = ( $\prod a$ )  $\cdot$  ( $\prod b$ ))
        )
      )
  )
proof
  fix k assume k  $\in$  nat
  show ( $\forall a b c.$ 
    a  $\in$   $\text{succ}(k) \rightarrow G \wedge$ 
    b  $\in$   $\text{succ}(k) \rightarrow G \wedge c \in \text{succ}(k) \rightarrow G \wedge$ 
    ( $\forall j \in \text{succ}(k). c(j) = a(j) \cdot b(j)$ )  $\longrightarrow$ 
    ( $\prod c$ ) = ( $\prod a$ )  $\cdot$  ( $\prod b$ ))  $\longrightarrow$ 
    ( $\forall a b c.$ 
      a  $\in$   $\text{succ}(\text{succ}(k)) \rightarrow G \wedge$ 
      b  $\in$   $\text{succ}(\text{succ}(k)) \rightarrow G \wedge$ 
      c  $\in$   $\text{succ}(\text{succ}(k)) \rightarrow G \wedge$ 
      ( $\forall j \in \text{succ}(\text{succ}(k)). c(j) = a(j) \cdot b(j)$ )  $\longrightarrow$ 
      ( $\prod c$ ) = ( $\prod a$ )  $\cdot$  ( $\prod b$ ))
    )
  )
  proof
    assume A3:  $\forall a b c.$ 
    a  $\in$   $\text{succ}(k) \rightarrow G \wedge$ 
    b  $\in$   $\text{succ}(k) \rightarrow G \wedge c \in \text{succ}(k) \rightarrow G \wedge$ 
    ( $\forall j \in \text{succ}(k). c(j) = a(j) \cdot b(j)$ )  $\longrightarrow$ 
    ( $\prod c$ ) = ( $\prod a$ )  $\cdot$  ( $\prod b$ )
    show  $\forall a b c.$ 
    a  $\in$   $\text{succ}(\text{succ}(k)) \rightarrow G \wedge$ 
    b  $\in$   $\text{succ}(\text{succ}(k)) \rightarrow G \wedge$ 
    c  $\in$   $\text{succ}(\text{succ}(k)) \rightarrow G \wedge$ 
    ( $\forall j \in \text{succ}(\text{succ}(k)). c(j) = a(j) \cdot b(j)$ )  $\longrightarrow$ 
    ( $\prod c$ ) = ( $\prod a$ )  $\cdot$  ( $\prod b$ )
  proof -
  { fix a b c
    assume
      a  $\in$   $\text{succ}(\text{succ}(k)) \rightarrow G \wedge$ 
      b  $\in$   $\text{succ}(\text{succ}(k)) \rightarrow G \wedge$ 
      c  $\in$   $\text{succ}(\text{succ}(k)) \rightarrow G \wedge$ 
      ( $\forall j \in \text{succ}(\text{succ}(k)). c(j) = a(j) \cdot b(j)$ )
    with 'k  $\in$  nat' have I:
      a :  $\text{succ}(\text{succ}(k)) \rightarrow G$ 
      b :  $\text{succ}(\text{succ}(k)) \rightarrow G$ 
      c :  $\text{succ}(\text{succ}(k)) \rightarrow G$ 
    and II:  $\forall j \in \text{succ}(\text{succ}(k)). c(j) = a(j) \cdot b(j)$ 
    by auto
  }
  }

```

```

let x = Init(a)
    let y = Init(b)
    let z = Init(c)
from 'k ∈ nat' I have III:
  (∏ a) = (∏ x) · a(succ(k))
  (∏ b) = (∏ y) · b(succ(k)) and
IV: (∏ c) = (∏ z) · c(succ(k))
  using shorter_seq by auto
moreover
from 'k ∈ nat' I II have
  x : succ(k) → G
  y : succ(k) → G
  z : succ(k) → G and
  ∀ j ∈ succ(k). z(j) = x(j) · y(j)
  using prod_distr_ind_step by auto
with A3 II IV have
  (∏ c) = (∏ x) · (∏ y) · (a(succ(k)) · b(succ(k)))
  by simp
moreover from A1 'k ∈ nat' I III have
  (∏ x) · (∏ y) · (a(succ(k)) · b(succ(k))) =
  (∏ a) · (∏ b)
  using init_props prod_type apply_funtype
  rearr4elems by simp
ultimately have (∏ c) = (∏ a) · (∏ b)
  by simp
} thus thesis by auto
qed
qed
qed
ultimately show thesis by (rule ind_on_nat)
qed

```

A reformulation of `prod_comm_distr` that is more convenient in applications.

```

theorem (in semigr0) prod_comm_distrib:
  assumes f {is commutative on} G and n ∈ nat and
  a : succ(n) → G b : succ(n) → G c : succ(n) → G and
  ∀ j ∈ succ(n). c(j) = a(j) · b(j)
  shows (∏ c) = (∏ a) · (∏ b)
  using assms prod_comm_distr by simp

```

A product of two products over disjoint sets of indices is the product over the union.

```

lemma (in semigr1) prod_bisect:
  assumes A1: f {is commutative on} G and A2: Λ ∈ FinPow(X)
  shows
  ∀ P ∈ Bisections(Λ). ∏ (Λ, a) = (∏ (fst(P), a)) · (∏ (snd(P), a))
proof -
  have IsLinOrder(X, r) using linord by simp
  moreover have

```

```

     $\forall P \in \text{Bisections}(0). \prod(0, a) = (\prod(\text{fst}(P), a)) \cdot (\prod(\text{snd}(P), a))$ 
    using bisec_empty by simp
  moreover have  $\forall A \in \text{FinPow}(X).$ 
    ( $\forall n \in X - A.$ 
      ( $\forall P \in \text{Bisections}(A). \prod(A, a) = (\prod(\text{fst}(P), a)) \cdot (\prod(\text{snd}(P), a))$ )
       $\wedge (\forall k \in A. \langle k, n \rangle \in r) \longrightarrow$ 
      ( $\forall Q \in \text{Bisections}(A \cup \{n\}).$ 
         $\prod(A \cup \{n\}, a) = (\prod(\text{fst}(Q), a)) \cdot (\prod(\text{snd}(Q), a))$ )))
  proof -
    { fix A assume A  $\in \text{FinPow}(X)$ 
      fix n assume n  $\in X - A$ 
      have ( $\forall P \in \text{Bisections}(A).$ 
         $\prod(A, a) = (\prod(\text{fst}(P), a)) \cdot (\prod(\text{snd}(P), a))$ )
       $\wedge (\forall k \in A. \langle k, n \rangle \in r) \longrightarrow$ 
      ( $\forall Q \in \text{Bisections}(A \cup \{n\}).$ 
         $\prod(A \cup \{n\}, a) = (\prod(\text{fst}(Q), a)) \cdot (\prod(\text{snd}(Q), a))$ ))
    proof -
      { assume I:
         $\forall P \in \text{Bisections}(A). \prod(A, a) = (\prod(\text{fst}(P), a)) \cdot (\prod(\text{snd}(P), a))$ 
        and II:  $\forall k \in A. \langle k, n \rangle \in r$ 
        have  $\forall Q \in \text{Bisections}(A \cup \{n\}).$ 
           $\prod(A \cup \{n\}, a) = (\prod(\text{fst}(Q), a)) \cdot (\prod(\text{snd}(Q), a))$ 
        proof -
          { fix Q assume Q  $\in \text{Bisections}(A \cup \{n\})$ 
            let Q0 = fst(Q)
            let Q1 = snd(Q)
            from 'A  $\in \text{FinPow}(X)$ ' 'n  $\in X - A$ ' have A  $\cup \{n\} \in \text{FinPow}(X)$ 
          using singleton_in_finpow union_finpow by auto
          with 'Q  $\in \text{Bisections}(A \cup \{n\})$ ' have
            Q0  $\in \text{FinPow}(X)$  Q0  $\neq 0$  and Q1  $\in \text{FinPow}(X)$  Q1  $\neq 0$ 
          using bisect_fin bisec_is_pair Bisections_def by auto
          then have  $\prod(Q_0, a) \in G$  and  $\prod(Q_1, a) \in G$ 
          using a_is_fun setprod_type by auto
          from 'Q  $\in \text{Bisections}(A \cup \{n\})$ ' 'A  $\in \text{FinPow}(X)$ ' 'n  $\in X - A$ '
            have refl(X, r) Q0  $\subseteq A \cup \{n\}$  Q1  $\subseteq A \cup \{n\}$ 
          A  $\subseteq X$  and n  $\in X$ 
          using linord IsLinOrder_def total_is_refl Bisections_def
          FinPow_def by auto
          from 'refl(X, r)' 'Q0  $\subseteq A \cup \{n\}$ ' 'A  $\subseteq X$ ' 'n  $\in X$ ' II
            have III:  $\forall k \in Q_0. \langle k, n \rangle \in r$  by (rule refl_add_point)
          from 'refl(X, r)' 'Q1  $\subseteq A \cup \{n\}$ ' 'A  $\subseteq X$ ' 'n  $\in X$ ' II
            have IV:  $\forall k \in Q_1. \langle k, n \rangle \in r$  by (rule refl_add_point)
          from 'n  $\in X - A$ ' 'Q  $\in \text{Bisections}(A \cup \{n\})$ ' have
            Q0 = {n}  $\vee$  Q1 = {n}  $\vee \langle Q_0 - \{n\}, Q_1 - \{n\} \rangle \in \text{Bisections}(A)$ 
          using bisec_is_pair bisec_add_point by simp
        moreover
          { assume Q1 = {n}
            from 'n  $\in X - A$ ' have n  $\notin A$  by auto
          moreover

```

```

from 'Q ∈ Bisections(A ∪ {n})'
have ⟨Q0, Q1⟩ ∈ Bisections(A ∪ {n})
  using bisec_is_pair by simp
with 'Q1 = {n}' have ⟨Q0, {n}⟩ ∈ Bisections(A ∪ {n})
  by simp
ultimately have Q0 = A and A ≠ 0
  using set_point_bisec by auto
with 'A ∈ FinPow(X)' 'n ∈ X - A' II 'Q1 = {n}'
have ∏(A ∪ {n}, a) = (∏(Q0, a)) · ∏(Q1, a)
  using a_is_fun gen_prod_append gen_prod_singleton
  by simp }
  moreover
  { assume Q0 = {n}
from 'n ∈ X - A' have n ∈ X by auto
then have {n} ∈ FinPow(X) and {n} ≠ 0
  using singleton_in_finpow by auto
from 'n ∈ X - A' have n ∉ A by auto
moreover
from 'Q ∈ Bisections(A ∪ {n})'
have ⟨Q0, Q1⟩ ∈ Bisections(A ∪ {n})
  using bisec_is_pair by simp
with 'Q0 = {n}' have ⟨{n}, Q1⟩ ∈ Bisections(A ∪ {n})
  by simp
ultimately have Q1 = A and A ≠ 0 using point_set_bisec
  by auto
with A1 'A ∈ FinPow(X)' 'n ∈ X - A' II
  '{n} ∈ FinPow(X)' '{n} ≠ 0' 'Q0 = {n}'
have ∏(A ∪ {n}, a) = (∏(Q0, a)) · (∏(Q1, a))
  using a_is_fun gen_prod_append gen_prod_singleton
  setprod_type IsCommutative_def by auto }
  moreover
  { assume A4: ⟨Q0 - {n}, Q1 - {n}⟩ ∈ Bisections(A)
with 'A ∈ FinPow(X)' have
  Q0 - {n} ∈ FinPow(X) Q0 - {n} ≠ 0 and
  Q1 - {n} ∈ FinPow(X) Q1 - {n} ≠ 0
  using FinPow_def Bisections_def by auto
with 'n ∈ X - A' have
  ∏(Q0 - {n}, a) ∈ G ∏(Q1 - {n}, a) ∈ G and
  T: a(n) ∈ G
  using a_is_fun setprod_type apply_funtype by auto
from 'Q ∈ Bisections(A ∪ {n})' A4 have
  (⟨Q0, Q1 - {n}⟩ ∈ Bisections(A) ∧ n ∈ Q1) ∨
  (⟨Q0 - {n}, Q1⟩ ∈ Bisections(A) ∧ n ∈ Q0)
  using bisec_is_pair bisec_add_point_case3 by auto
moreover
{ assume ⟨Q0, Q1 - {n}⟩ ∈ Bisections(A) and n ∈ Q1
then have A ≠ 0 using bisec_props by simp
with A2 'A ∈ FinPow(X)' 'n ∈ X - A' I II T IV
  '⟨Q0, Q1 - {n}⟩ ∈ Bisections(A)' '∏(Q0, a) ∈ G'

```

```

      '  $\prod(Q_1 - \{n\}, a) \in G$  ' '  $Q_1 \in \text{FinPow}(X)$  '
      '  $n \in Q_1$  ' '  $Q_1 - \{n\} \neq 0$  '
    have  $\prod(A \cup \{n\}, a) = (\prod(Q_0, a)) \cdot (\prod(Q_1, a))$ 
      using gen_prod_append semigr_assoc gen_product_rem_point
      by simp }
  moreover
  { assume  $\langle Q_0 - \{n\}, Q_1 \rangle \in \text{Bisections}(A)$  and  $n \in Q_0$ 
    then have  $A \neq 0$  using bisec_props by simp
    with A1 A2 '  $A \in \text{FinPow}(X)$  ' '  $n \in X - A$  ' I II III T
      '  $\langle Q_0 - \{n\}, Q_1 \rangle \in \text{Bisections}(A)$  ' '  $\prod(Q_0 - \{n\}, a) \in G$  '
      '  $\prod(Q_1, a) \in G$  ' '  $Q_0 \in \text{FinPow}(X)$  ' '  $n \in Q_0$  ' '  $Q_0 - \{n\} \neq 0$  '
    have  $\prod(A \cup \{n\}, a) = (\prod(Q_0, a)) \cdot (\prod(Q_1, a))$ 
      using gen_prod_append rearr3elems gen_product_rem_point
      by simp }
  ultimately have
     $\prod(A \cup \{n\}, a) = (\prod(Q_0, a)) \cdot (\prod(Q_1, a))$ 
    by auto }
    ultimately have  $\prod(A \cup \{n\}, a) = (\prod(Q_0, a)) \cdot (\prod(Q_1, a))$ 
  by auto
  } thus thesis by simp
qed
} thus thesis by simp
  qed
} thus thesis by simp
qed
moreover note A2
ultimately show thesis by (rule fin_ind_add_max)
qed

```

A better looking reformulation of prod\_bisect.

```

theorem (in semigr1) prod_disjoint: assumes
  A1:  $f$  {is commutative on}  $G$  and
  A2:  $A \in \text{FinPow}(X)$   $A \neq 0$  and
  A3:  $B \in \text{FinPow}(X)$   $B \neq 0$  and
  A4:  $A \cap B = 0$ 
shows  $\prod(A \cup B, a) = (\prod(A, a)) \cdot (\prod(B, a))$ 
proof -
  from A2 A3 A4 have  $\langle A, B \rangle \in \text{Bisections}(A \cup B)$ 
    using is_bisec by simp
  with A1 A2 A3 show thesis
    using a_is_fun union_finpow prod_bisect by simp
qed

```

A generalization of prod\_disjoint.

```

lemma (in semigr1) prod_list_of_lists: assumes
  A1:  $f$  {is commutative on}  $G$  and A2:  $n \in \text{nat}$ 
shows  $\forall M \in \text{succ}(n) \rightarrow \text{FinPow}(X)$ .
   $M$  {is partition}  $\longrightarrow$ 
   $(\prod \{i, \prod(M(i), a)\}. i \in \text{succ}(n)\}) =$ 

```

```

( $\prod(\bigcup i \in \text{succ}(n). M(i), a)$ )
proof -
  note A2
  moreover have  $\forall M \in \text{succ}(0) \rightarrow \text{FinPow}(X).$ 
    M {is partition}  $\rightarrow$ 
    ( $\prod \{ \langle i, \prod(M(i), a) \rangle. i \in \text{succ}(0) \}$ ) = ( $\prod(\bigcup i \in \text{succ}(0). M(i), a)$ )
    using a_is_fun func1_1_L1 Partition_def apply_funtype setprod_type
      list_len1_singleton prod_of_1elem
    by simp
  moreover have  $\forall k \in \text{nat}.$ 
    ( $\forall M \in \text{succ}(k) \rightarrow \text{FinPow}(X).$ 
      M {is partition}  $\rightarrow$ 
      ( $\prod \{ \langle i, \prod(M(i), a) \rangle. i \in \text{succ}(k) \}$ ) =
      ( $\prod(\bigcup i \in \text{succ}(k). M(i), a)$ )  $\rightarrow$ 
      ( $\forall M \in \text{succ}(\text{succ}(k)) \rightarrow \text{FinPow}(X).$ 
        M {is partition}  $\rightarrow$ 
        ( $\prod \{ \langle i, \prod(M(i), a) \rangle. i \in \text{succ}(\text{succ}(k)) \}$ ) =
        ( $\prod(\bigcup i \in \text{succ}(\text{succ}(k)). M(i), a)$ )
      )
    )
  proof -
    { fix k assume k  $\in$  nat
      assume A3:  $\forall M \in \text{succ}(k) \rightarrow \text{FinPow}(X).$ 
      M {is partition}  $\rightarrow$ 
      ( $\prod \{ \langle i, \prod(M(i), a) \rangle. i \in \text{succ}(k) \}$ ) =
      ( $\prod(\bigcup i \in \text{succ}(k). M(i), a)$ )
      have ( $\forall N \in \text{succ}(\text{succ}(k)) \rightarrow \text{FinPow}(X).$ 
        N {is partition}  $\rightarrow$ 
        ( $\prod \{ \langle i, \prod(N(i), a) \rangle. i \in \text{succ}(\text{succ}(k)) \}$ ) =
        ( $\prod(\bigcup i \in \text{succ}(\text{succ}(k)). N(i), a)$ )
      )
      proof -
        { fix N assume A4:  $N : \text{succ}(\text{succ}(k)) \rightarrow \text{FinPow}(X)$ 
          assume A5: N {is partition}
          with A4 have I:  $\forall i \in \text{succ}(\text{succ}(k)). N(i) \neq 0$ 
            using func1_1_L1 Partition_def by simp
          let b =  $\{ \langle i, \prod(N(i), a) \rangle. i \in \text{succ}(\text{succ}(k)) \}$ 
          let c =  $\{ \langle i, \prod(N(i), a) \rangle. i \in \text{succ}(k) \}$ 
          have II:  $\forall i \in \text{succ}(\text{succ}(k)). \prod(N(i), a) \in G$ 
            proof
              fix i assume i  $\in$   $\text{succ}(\text{succ}(k))$ 
              with A4 I have  $N(i) \in \text{FinPow}(X)$  and  $N(i) \neq 0$ 
                using apply_funtype by auto
              then show  $\prod(N(i), a) \in G$  using setprod_type
                by simp
            qed
          hence  $\forall i \in \text{succ}(k). \prod(N(i), a) \in G$  by auto
          then have c :  $\text{succ}(k) \rightarrow G$  by (rule ZF_fun_from_total)
          have b =  $\{ \langle i, \prod(N(i), a) \rangle. i \in \text{succ}(\text{succ}(k)) \}$ 
            by simp
          with II have b =  $\text{Append}(c, \prod(N(\text{succ}(k)), a))$ 
            by (rule set_list_append)
        }
      }
    }

```

```

with II 'k ∈ nat' 'c : succ(k) → G'
have (∏ b) = (∏ c) · (∏ (N(succ(k)), a))
  using prod_append by simp
also have
  ... = (∏ (∪ i ∈ succ(k). N(i), a)) · (∏ (N(succ(k)), a))
proof -
  let M = restrict(N, succ(k))
  have succ(k) ⊆ succ(succ(k)) by auto
  with 'N : succ(succ(k)) → FinPow(X)'
  have M : succ(k) → FinPow(X) and
    III: ∀ i ∈ succ(k). M(i) = N(i)
    using restrict_type2 restrict apply_funtype
    by auto
  with A5 'M : succ(k) → FinPow(X)' have M {is partition}
    using func1_1_L1 Partition_def by simp
  with A3 'M : succ(k) → FinPow(X)' have
    (∏ {⟨i, ∏ (M(i), a)⟩. i ∈ succ(k)}) =
    (∏ (∪ i ∈ succ(k). M(i), a))
    by blast
  with III show thesis by simp
qed
also have ... = (∏ (∪ i ∈ succ(succ(k)). N(i), a))
proof -
  let A = ∪ i ∈ succ(k). N(i)
  let B = N(succ(k))
  from A4 'k ∈ nat' have succ(k) ∈ nat and
    ∀ i ∈ succ(k). N(i) ∈ FinPow(X)
    using apply_funtype by auto
  then have A ∈ FinPow(X) by (rule union_fin_list_fin)
  moreover from I have A ≠ 0 by auto
  moreover from A4 I have
    N(succ(k)) ∈ FinPow(X) and N(succ(k)) ≠ 0
    using apply_funtype by auto
  moreover from 'succ(k) ∈ nat' A4 A5 have A ∩ B = 0
    by (rule list_partition)
  moreover note A1
  ultimately have ∏ (A ∪ B, a) = (∏ (A, a)) · (∏ (B, a))
    using prod_disjoint by simp
  moreover have A ∪ B = (∪ i ∈ succ(succ(k)). N(i))
    by auto
  ultimately show thesis by simp
qed
finally have (∏ {⟨i, ∏ (N(i), a)⟩. i ∈ succ(succ(k))}) =
  (∏ (∪ i ∈ succ(succ(k)). N(i), a))
  by simp
} thus thesis by auto
qed
} thus thesis by simp
qed

```

ultimately show thesis by (rule ind\_on\_nat)  
qed

A more convenient reformulation of prod\_list\_of\_lists.

```
theorem (in semigr1) prod_list_of_sets:
  assumes A1: f {is commutative on} G and
  A2: n ∈ nat n ≠ 0 and
  A3: M : n → FinPow(X) M {is partition}
  shows
    (∏ {⟨i, ∏(M(i), a)⟩. i ∈ n}) = (∏(∪ i ∈ n. M(i), a))
proof -
  from A2 obtain k where k ∈ nat and n = succ(k)
  using Nat_ZF_1_L3 by auto
  with A1 A3 show thesis using prod_list_of_lists
  by simp
qed
```

The definition of the product  $\prod(A, a) \equiv \text{SetFold}(f, a, A, r)$  of a some (finite) set of semigroup elements requires that  $r$  is a linear order on the set of indices  $A$ . This is necessary so that we know in which order we are multiplying the elements. The product over  $A$  is defined so that we have  $\prod_A a = \prod a \circ \sigma(A)$  where  $\sigma : |A| \rightarrow A$  is the enumeration of  $A$  (the only order isomorphism between the number of elements in  $A$  and  $A$ ), see lemma `setproddef`. However, if the operation is commutative, the order is irrelevant. The next theorem formalizes that fact stating that we can replace the enumeration  $\sigma(A)$  by any bijection between  $|A|$  and  $A$ . In a way this is a generalization of `setproddef`. The proof is based on application of `prod_list_of_sets` to the finite collection of singletons that comprise  $A$ .

```
theorem (in semigr1) prod_order_irr:
  assumes A1: f {is commutative on} G and
  A2: A ∈ FinPow(X) A ≠ 0 and
  A3: b ∈ bij(|A|, A)
  shows (∏ (a 0 b)) = ∏(A, a)
proof -
  let n = |A|
  let M = {⟨k, {b(k)}⟩. k ∈ n}
  have (∏ (a 0 b)) = (∏ {⟨i, ∏(M(i), a)⟩. i ∈ n})
proof -
  have ∀ i ∈ n. ∏(M(i), a) = (a 0 b)(i)
proof
  fix i assume i ∈ n
  with A2 A3 'i ∈ n' have b(i) ∈ X
using bij_def inj_def apply_funtype FinPow_def
by auto
  then have ∏({b(i)}, a) = a(b(i))
using gen_prod_singleton by simp
  with A3 'i ∈ n' have ∏({b(i)}, a) = (a 0 b)(i)
using bij_def inj_def comp_fun_apply by auto
```



```

    with 'i ∈ n' A3 show  $\prod (M(i), a) = (a \ 0 \ b)(i)$ 
using bij_def inj_partition by auto
qed
    hence  $\{(i, \prod (M(i), a)) \mid i \in n\} = \{(i, (a \ 0 \ b)(i)) \mid i \in n\}$ 
    by simp
    moreover have  $\{(i, (a \ 0 \ b)(i)) \mid i \in n\} = a \ 0 \ b$ 
    proof -
      from A3 have  $b : n \rightarrow A$  using bij_def inj_def by simp
      moreover from A2 have  $A \subseteq X$  using FinPow_def by simp
      ultimately have  $b : n \rightarrow X$  by (rule func1_1_L1B)
      then have  $a \ 0 \ b : n \rightarrow G$  using a_is_fun comp_fun
    by simp
      then show  $\{(i, (a \ 0 \ b)(i)) \mid i \in n\} = a \ 0 \ b$ 
using fun_is_set_of_pairs by simp
qed
    ultimately show thesis by simp
qed
    also have  $\dots = (\prod (\bigcup i \in n. M(i), a))$ 
    proof -
      note A1
      moreover from A2 have  $n \in \text{nat}$  and  $n \neq 0$ 
      using card_fin_is_nat card_non_empty_non_zero by auto
      moreover have  $M : n \rightarrow \text{FinPow}(X)$  and  $M \{\text{is partition}\}$ 
    proof -
      from A2 A3 have  $\forall k \in n. \{b(k)\} \in \text{FinPow}(X)$ 
using bij_def inj_def apply_funtype FinPow_def
    singleton_in_finpow by auto
      then show  $M : n \rightarrow \text{FinPow}(X)$  using ZF_fun_from_total
    by simp
      from A3 show  $M \{\text{is partition}\}$  using bij_def inj_partition
    by auto
    qed
      ultimately show
         $(\prod \{(i, \prod (M(i), a)) \mid i \in n\}) = (\prod (\bigcup i \in n. M(i), a))$ 
        by (rule prod_list_of_sets)
    qed
    also from A3 have  $(\prod (\bigcup i \in n. M(i), a)) = \prod (A, a)$ 
      using bij_def inj_partition surj_singleton_image
    by auto
    finally show thesis by simp
qed

```

Another way of expressing the fact that the product does not depend on the order.

```

corollary (in semigr1) prod_bij_same:
  assumes f {is commutative on} G and
  A ∈ FinPow(X) A ≠ 0 and
  b ∈ bij(|A|, A) c ∈ bij(|A|, A)
  shows  $(\prod (a \ 0 \ b)) = (\prod (a \ 0 \ c))$ 

```

```
using assms prod_order_irr by simp
end
```

## 18 Semigroup\_ZF.thy

```
theory CommutativeSemigroup_ZF imports Semigroup_ZF
```

```
begin
```

In the `Semigroup` theory we introduced a notion of `SetFold(f,a, $\Lambda$ ,r)` that represents the sum of values of some function  $a$  valued in a semigroup where the arguments of that function vary over some set  $\Lambda$ . Using the additive notation something like this would be expressed as  $\sum_{x \in \Lambda} f(x)$  in informal mathematics. This theory considers an alternative to that notion that is more specific to commutative semigroups.

### 18.1 Sum of a function over a set

The  $r$  parameter in the definition of `SetFold(f,a, $\Lambda$ ,r)` (from `Semigroup_ZF`) represents a linear order relation on  $\Lambda$  that is needed to indicate in what order we are summing the values  $f(x)$ . If the semigroup operation is commutative the order does not matter and the relation  $r$  is not needed. In this section we define a notion of summing up values of some function  $a : X \rightarrow G$  over a finite set of indices  $\Gamma \subseteq X$ , without using any order relation on  $X$ .

We define the sum of values of a function  $a : X \rightarrow G$  over a set  $\Lambda$  as the only element of the set of sums of lists that are bijections between the number of values in  $\Lambda$  (which is a natural number  $n = \{0, 1, \dots, n-1\}$  if  $\Lambda$  is finite) and  $\Lambda$ . The notion of `Fold1(f,c)` is defined in `Semigroup_ZF` as the fold (sum) of the list  $c$  starting from the first element of that list. The intention is to use the fact that since the result of summing up a list does not depend on the order, the set  $\{\text{Fold1}(f,a \circ b) \mid b \in \text{bij}(|\Lambda|, \Lambda)\}$  is a singleton and we can extract its only value by taking its union.

**definition**

$$\text{CommSetFold}(f,a,\Lambda) = \bigcup \{\text{Fold1}(f,a \circ b) \mid b \in \text{bij}(|\Lambda|, \Lambda)\}$$

the next locale sets up notation for writing about summation in commutative semigroups. We define two kinds of sums. One is the sum of elements of a list (which are just functions defined on a natural number) and the second one represents a more general notion the sum of values of a semigroup valued function over some set of arguments. Since those two types of sums are different notions they are represented by different symbols. However in the presentations they are both intended to be printed as  $\sum$ .

```
locale commsemigr =
```

```
  fixes G f
```

```
  assumes csgassoc: f {is associative on} G
```

```

assumes csgcomm: f {is commutative on} G

fixes csgsum (infixl + 69)
defines csgsum_def[simp]: x + y  $\equiv$  f⟨x,y⟩

fixes X a
assumes csgaisfun: a : X  $\rightarrow$  G

fixes csglistsum ( $\sum$  _ 70)
defines csglistsum_def[simp]:  $\sum$  k  $\equiv$  Foldl(f,k)

fixes csgsetsum ( $\sum$ )
defines csgsetsum_def[simp]:  $\sum$ (A,h)  $\equiv$  CommSetFold(f,h,A)

```

Definition of a sum of function over a set in notation defined in the `commsemigr` locale.

```

lemma (in commsemigr) CommSetFolddef:
  shows ( $\sum$ (A,a)) = ( $\bigcup$ { $\sum$ (a 0 b). b  $\in$  bij(|A|, A)})
  using CommSetFold_def by simp

```

The next lemma states that the result of a sum does not depend on the order we calculate it. This is similar to lemma `prod_order_irr` in the `Semigroup` theory, except that the `semigr1` locale assumes that the domain of the function we sum up is linearly ordered, while in `commsemigr` we don't have this assumption.

```

lemma (in commsemigr) sum_over_set_bij:
  assumes A1: A  $\in$  FinPow(X) A  $\neq$  0 and A2: b  $\in$  bij(|A|,A)
  shows ( $\sum$ (A,a)) = ( $\sum$  (a 0 b))
proof -
  have
     $\forall c \in \text{bij}(|A|,A). \forall d \in \text{bij}(|A|,A). (\sum (a \ 0 \ c)) = (\sum (a \ 0 \ d))$ 
  proof -
    { fix c assume c  $\in$  bij(|A|,A)
      fix d assume d  $\in$  bij(|A|,A)
      let r = InducedRelation(converse(c), Le)
      have semigr1(G,f,A,r,restrict(a, A))
      proof -
        have semigr0(G,f) using csgassoc semigr0_def by simp
        moreover from A1 'c  $\in$  bij(|A|,A)' have IsLinOrder(A,r)
          using bij_converse_bij card_fin_is_nat
            natord_lin_on_each_nat ind_rel_pres_lin by simp
        moreover from A1 have restrict(a, A) : A  $\rightarrow$  G
          using FinPow_def csgaisfun restrict_fun by simp
        ultimately show thesis using semigr1_axioms.intro semigr1_def
          by simp
      }
    qed
  moreover have f {is commutative on} G using csgcomm
by simp

```

```

    moreover from A1 have A ∈ FinPow(A) A ≠ 0
using FinPow_def by auto
    moreover note 'c ∈ bij(|A|,A)' 'd ∈ bij(|A|,A)'
    ultimately have
Fold1(f,restrict(a,A) 0 c) = Fold1(f,restrict(a,A) 0 d)
by (rule semigr1.prod_bij_same)
    hence (∑ (restrict(a,A) 0 c)) = (∑ (restrict(a,A) 0 d))
by simp
    moreover from A1 'c ∈ bij(|A|,A)' 'd ∈ bij(|A|,A)'
    have
restrict(a,A) 0 c = a 0 c and restrict(a,A) 0 d = a 0 d
using bij_def surj_def csgaisfun FinPow_def comp_restrict
by auto
    ultimately have (∑ (a 0 c)) = (∑ (a 0 d)) by simp
    } thus thesis by blast
qed
with A2 have (⋃ {∑ (a 0 b). b ∈ bij(|A|, A)}) = (∑ (a 0 b))
by (rule singleton_comprehension)
then show thesis using CommSetFolddef by simp
qed

```

The result of a sum is in the semigroup. Also, as the second assertion we show that every semigroup valued function generates a homomorphism between the finite subsets of a semigroup and the semigroup. Adding an element to a set corresponds to adding a value.

**lemma** (in commsemigr) sum\_over\_set\_add\_point:

```

assumes A1: A ∈ FinPow(X) A ≠ 0
shows ∑(A,a) ∈ G and
∀x ∈ X-A. ∑(A ∪ {x},a) = (∑(A,a)) + a(x)

```

**proof** -

```

from A1 obtain b where b ∈ bij(|A|,A)
using fin_bij_card by auto
with A1 have ∑(A,a) = (∑ (a 0 b))
using sum_over_set_bij by simp
from A1 have |A| ∈ nat using card_fin_is_nat by simp
have semigr0(G,f) using csgassoc semigr0_def by simp
moreover
from A1 obtain n where n ∈ nat and |A| = succ(n)
using card_non_empty_succ by auto
with A1 'b ∈ bij(|A|,A)' have
n ∈ nat and a 0 b : succ(n) → G
using bij_def inj_def FinPow_def comp_fun_subset csgaisfun
by auto
ultimately have Fold1(f,a 0 b) ∈ G by (rule semigr0.prod_type)
with '∑(A,a) = (∑ (a 0 b))' show ∑(A,a) ∈ G
by simp
{ fix x assume x ∈ X-A
with A1 have (A ∪ {x}) ∈ FinPow(X) and A ∪ {x} ≠ 0
using singleton_in_finpow union_finpow by auto

```

```

    moreover have Append(b,x) ∈ bij(|A ∪ {x}|, A ∪ {x})
  proof -
    note ' |A| ∈ nat ' ' b ∈ bij(|A|,A) '
    moreover from ' x ∈ X-A ' have x ∉ A by simp
    ultimately have Append(b,x) ∈ bij(succ(|A|), A ∪ {x})
  by (rule bij_append_point)
    with A1 ' x ∈ X-A ' show thesis
using card_fin_add_one by auto
  qed
  ultimately have (∑(A ∪ {x},a)) = (∑ (a 0 Append(b,x)))
    using sum_over_set_bij by simp
  also have ... = (∑ Append(a 0 b, a(x)))
  proof -
    note ' |A| ∈ nat '
    moreover
    from A1 ' b ∈ bij(|A|, A) ' have
b : |A| → A and A ⊆ X
using bij_def inj_def using FinPow_def by auto
    then have b : |A| → X by (rule func1_1_L1B)
    moreover from ' x ∈ X-A ' have x ∈ X and a : X → G
using csgaisfun by auto
    ultimately show thesis using list_compose_append
  by simp
  qed
  also have ... = (∑(A,a)) + a(x)
  proof -
    note ' semigr0(G,f) ' ' n ∈ nat ' ' a 0 b : succ(n) → G '
    moreover from ' x ∈ X-A ' have a(x) ∈ G
using csgaisfun apply_funtype by simp
    ultimately have
Fold1(f,Append(a 0 b, a(x))) = f(Fold1(f,a 0 b),a(x))
  by (rule semigr0.prod_append)
    with A1 ' b ∈ bij(|A|,A) ' show thesis
using sum_over_set_bij by simp
  qed
  finally have (∑(A ∪ {x},a)) = (∑(A,a)) + a(x)
    by simp
} thus ∀ x ∈ X-A. ∑(A ∪ {x},a) = (∑(A,a)) + a(x)
  by simp
qed
end

```

## 19 Monoid\_ZF.thy

```
theory Monoid_ZF imports func_ZF
```

```
begin
```

This theory provides basic facts about monoids.

### 19.1 Definition and basic properties

In this section we talk about monoids. The notion of a monoid is similar to the notion of a semigroup except that we require the existence of a neutral element. It is also similar to the notion of group except that we don't require existence of the inverse.

Monoid is a set  $G$  with an associative operation and a neutral element. The operation is a function on  $G \times G$  with values in  $G$ . In the context of ZF set theory this means that it is a set of pairs  $\langle x, y \rangle$ , where  $x \in G \times G$  and  $y \in G$ . In other words the operation is a certain subset of  $(G \times G) \times G$ . We express all this by defining a predicate  $\text{IsAmonoid}(G, f)$ . Here  $G$  is the "carrier" of the group and  $f$  is the binary operation on it.

**definition**

```
IsAmonoid(G,f)  $\equiv$ 
f {is associative on} G  $\wedge$ 
( $\exists e \in G. (\forall g \in G. (f(\langle e, g \rangle) = g) \wedge (f(\langle g, e \rangle) = g)))$ 
```

The next locale called "monoid0" defines a context for theorems that concern monoids. In this context we assume that the pair  $(G, f)$  is a monoid. We will use the  $\oplus$  symbol to denote the monoid operation (for no particular reason).

```
locale monoid0 =
```

```
  fixes G
  fixes f
  assumes monoidAsssum: IsAmonoid(G,f)

  fixes monoper (infixl  $\oplus$  70)
  defines monoper_def [simp]:  $a \oplus b \equiv f(\langle a, b \rangle)$ 
```

The result of the monoid operation is in the monoid (carrier).

```
lemma (in monoid0) group0_1_L1:
  assumes  $a \in G \quad b \in G$  shows  $a \oplus b \in G$ 
  using assms monoidAsssum IsAmonoid_def IsAssociative_def apply_funtype
  by auto
```

There is only one neutral element in a monoid.

```
lemma (in monoid0) group0_1_L2: shows
   $\exists ! e. e \in G \wedge (\forall g \in G. (e \oplus g = g) \wedge g \oplus e = g)$ 
proof
```

```

fix e y
assume e ∈ G ∧ (∀ g ∈ G. e ⊕ g = g ∧ g ⊕ e = g)
  and y ∈ G ∧ (∀ g ∈ G. y ⊕ g = g ∧ g ⊕ y = g)
then have y ⊕ e = y y ⊕ e = e by auto
thus e = y by simp
next from monoidAsssum show
  ∃ e. e ∈ G ∧ (∀ g ∈ G. e ⊕ g = g ∧ g ⊕ e = g)
  using IsAmonoid_def by auto
qed

```

We could put the definition of neutral element anywhere, but it is only usable in conjunction with the above lemma.

**definition**

```

TheNeutralElement(G,f) ≡
  ( THE e. e ∈ G ∧ (∀ g ∈ G. f⟨e,g⟩ = g ∧ f⟨g,e⟩ = g) )

```

The neutral element is neutral.

```

lemma (in monoid0) unit_is_neutral:
  assumes A1: e = TheNeutralElement(G,f)
  shows e ∈ G ∧ (∀ g ∈ G. e ⊕ g = g ∧ g ⊕ e = g)
proof -
  let n = THE b. b ∈ G ∧ (∀ g ∈ G. b ⊕ g = g ∧ g ⊕ b = g)
  have ∃! b. b ∈ G ∧ (∀ g ∈ G. b ⊕ g = g ∧ g ⊕ b = g)
    using group0_1_L2 by simp
  then have n ∈ G ∧ (∀ g ∈ G. n ⊕ g = g ∧ g ⊕ n = g)
    by (rule theI)
  with A1 show thesis
    using TheNeutralElement_def by simp
qed

```

The monoid carrier is not empty.

```

lemma (in monoid0) group0_1_L3A: shows G ≠ 0
proof -
  have TheNeutralElement(G,f) ∈ G using unit_is_neutral
    by simp
  thus thesis by auto
qed

```

The range of the monoid operation is the whole monoid carrier.

```

lemma (in monoid0) group0_1_L3B: shows range(f) = G
proof
  from monoidAsssum have f : G × G → G
    using IsAmonoid_def IsAssociative_def by simp
  then show range(f) ⊆ G
    using func1_1_L5B by simp
  show G ⊆ range(f)
  proof
    fix g assume A1: g ∈ G

```



```

    let e = TheNeutralElement(G,f)
    from A1 have ⟨e,g⟩ ∈ G×G g = f⟨e,g⟩
      using unit_is_neutral by auto
    with 'f : G×G→G' show g ∈ range(f)
      using func1_1_L5A by blast
  qed
qed

```

Another way to state that the range of the monoid operation is the whole monoid carrier.

```

lemma (in monoid0) range_carr: shows f(G×G) = G
  using monoidAsssum IsAmonoid_def IsAssociative_def
  group0_1_L3B range_image_domain by auto

```

In a monoid any neutral element is the neutral element.

```

lemma (in monoid0) group0_1_L4:
  assumes A1: e ∈ G ∧ (∀g∈G. e ⊕ g = g ∧ g ⊕ e = g)
  shows e = TheNeutralElement(G,f)
proof -
  let n = THE b. b ∈ G ∧ (∀ g∈G. b⊕g = g ∧ g⊕b = g)
  have ∃!b. b ∈ G ∧ (∀ g∈G. b⊕g = g ∧ g⊕b = g)
    using group0_1_L2 by simp
  moreover note A1
  ultimately have n = e by (rule the_equality2)
  then show thesis using TheNeutralElement_def by simp
qed

```

The next lemma shows that if the if we restrict the monoid operation to a subset of  $G$  that contains the neutral element, then the neutral element of the monoid operation is also neutral with the restricted operation.

```

lemma (in monoid0) group0_1_L5:
  assumes A1: ∀x∈H.∀y∈H. x⊕y ∈ H
  and A2: H⊆G
  and A3: e = TheNeutralElement(G,f)
  and A4: g = restrict(f,H×H)
  and A5: e∈H
  and A6: h∈H
  shows g⟨e,h⟩ = h ∧ g⟨h,e⟩ = h
proof -
  from A4 A6 A5 have
    g⟨e,h⟩ = e⊕h ∧ g⟨h,e⟩ = h⊕e
    using restrict_if by simp
  with A3 A4 A6 A2 show
    g⟨e,h⟩ = h ∧ g⟨h,e⟩ = h
    using unit_is_neutral by auto
qed

```

The next theorem shows that if the monoid operation is closed on a subset

of  $G$  then this set is a (sub)monoid (although we do not define this notion). This fact will be useful when we study subgroups.

```

theorem (in monoid0) group0_1_T1:
  assumes A1: H {is closed under} f
  and A2:  $H \subseteq G$ 
  and A3: TheNeutralElement( $G, f$ )  $\in H$ 
  shows IsAmonoid( $H, \text{restrict}(f, H \times H)$ )
proof -
  let  $g = \text{restrict}(f, H \times H)$ 
  let  $e = \text{TheNeutralElement}(G, f)$ 
  from monoidAsssum have  $f \in G \times G \rightarrow G$ 
    using IsAmonoid_def IsAssociative_def by simp
  moreover from A2 have  $H \times H \subseteq G \times G$  by auto
  moreover from A1 have  $\forall p \in H \times H. f(p) \in H$ 
    using IsOpClosed_def by auto
  ultimately have  $g \in H \times H \rightarrow H$ 
    using func1_2_L4 by simp
  moreover have  $\forall x \in H. \forall y \in H. \forall z \in H. g\langle g\langle x, y \rangle, z \rangle = g\langle x, g\langle y, z \rangle \rangle$ 
  proof -
    from A1 have  $\forall x \in H. \forall y \in H. \forall z \in H. g\langle g\langle x, y \rangle, z \rangle = x \oplus y \oplus z$ 
      using IsOpClosed_def restrict_if by simp
    moreover have  $\forall x \in H. \forall y \in H. \forall z \in H. x \oplus y \oplus z = x \oplus (y \oplus z)$ 
    proof -
      from monoidAsssum have
 $\forall x \in G. \forall y \in G. \forall z \in G. x \oplus y \oplus z = x \oplus (y \oplus z)$ 
      using IsAmonoid_def IsAssociative_def
      by simp
      with A2 show thesis by auto
    qed
    moreover from A1 have
 $\forall x \in H. \forall y \in H. \forall z \in H. x \oplus (y \oplus z) = g\langle x, g\langle y, z \rangle \rangle$ 
      using IsOpClosed_def restrict_if by simp
    ultimately show thesis by simp
  qed
  moreover have
 $\exists n \in H. (\forall h \in H. g\langle n, h \rangle = h \wedge g\langle h, n \rangle = h)$ 
  proof -
    from A1 have  $\forall x \in H. \forall y \in H. x \oplus y \in H$ 
      using IsOpClosed_def by simp
    with A2 A3 have
 $\forall h \in H. g\langle e, h \rangle = h \wedge g\langle h, e \rangle = h$ 
      using group0_1_L5 by blast
    with A3 show thesis by auto
  qed
  ultimately show thesis using IsAmonoid_def IsAssociative_def
  by simp
qed

```

Under the assumptions of `group0_1_T1` the neutral element of a submonoid is the same as that of the monoid.

```

lemma group0_1_L6:
  assumes A1: IsAmonoid(G,f)
  and A2: H {is closed under} f
  and A3: H⊆G
  and A4: TheNeutralElement(G,f) ∈ H
  shows TheNeutralElement(H,restrict(f,H×H)) = TheNeutralElement(G,f)
proof -
  let e = TheNeutralElement(G,f)
  let g = restrict(f,H×H)
  from assms have monoid0(H,g)
    using monoid0_def monoid0.group0_1_T1
    by simp
  moreover have
    e ∈ H ∧ (∀h∈H. g⟨e,h⟩ = h ∧ g⟨h,e⟩ = h)
  proof -
    { fix h assume h ∈ H
      with assms have
monoid0(G,f)  ∀x∈H.∀y∈H. f⟨x,y⟩ ∈ H
H⊆G  e = TheNeutralElement(G,f)  g = restrict(f,H×H)
e ∈ H  h ∈ H
using monoid0_def IsOpClosed_def by auto
      then have g⟨e,h⟩ = h ∧ g⟨h,e⟩ = h
    by (rule monoid0.group0_1_L5)
    } hence ∀h∈H. g⟨e,h⟩ = h ∧ g⟨h,e⟩ = h by simp
    with A4 show thesis by simp
  qed
  ultimately have e = TheNeutralElement(H,g)
    by (rule monoid0.group0_1_L4)
  thus thesis by simp
qed

```

If a sum of two elements is not zero, then at least one has to be nonzero.

```

lemma (in monoid0) sum_nonzero_elmnt_nonzero:
  assumes a ⊕ b ≠ TheNeutralElement(G,f)
  shows a ≠ TheNeutralElement(G,f) ∨ b ≠ TheNeutralElement(G,f)
  using assms unit_is_neutral by auto

end

```

## 20 Group\_ZF.thy

**theory** Group\_ZF **imports** Monoid\_ZF

**begin**

This theory file covers basics of group theory.

### 20.1 Definition and basic properties of groups

In this section we define the notion of a group and set up the notation for discussing groups. We prove some basic theorems about groups.

To define a group we take a monoid and add a requirement that the right inverse needs to exist for every element of the group.

**definition**

$\text{IsAgroup}(G, f) \equiv$   
 $(\text{IsAmonoid}(G, f) \wedge (\forall g \in G. \exists b \in G. f\langle g, b \rangle = \text{TheNeutralElement}(G, f)))$

We define the group inverse as the set  $\{\langle x, y \rangle \in G \times G : x \cdot y = e\}$ , where  $e$  is the neutral element of the group. This set (which can be written as  $(\cdot)^{-1}\{e\}$ ) is a certain relation on the group (carrier). Since, as we show later, for every  $x \in G$  there is exactly one  $y \in G$  such that  $x \cdot y = e$  this relation is in fact a function from  $G$  to  $G$ .

**definition**

$\text{GroupInv}(G, f) \equiv \{\langle x, y \rangle \in G \times G. f\langle x, y \rangle = \text{TheNeutralElement}(G, f)\}$

We will use the multiplicative notation for groups. The neutral element is denoted 1.

**locale** group0 =

**fixes** G

**fixes** P

**assumes** groupAssum: IsAgroup(G, P)

**fixes** neut (1)

**defines** neut\_def[simp]:  $1 \equiv \text{TheNeutralElement}(G, P)$

**fixes** proper (infixl  $\cdot$  70)

**defines** proper\_def[simp]:  $a \cdot b \equiv P\langle a, b \rangle$

**fixes** inv ( $_^{-1}$  [90] 91)

**defines** inv\_def[simp]:  $x^{-1} \equiv \text{GroupInv}(G, P)(x)$

First we show a lemma that says that we can use theorems proven in the monoid0 context (locale).

**lemma** (in group0) group0\_2\_L1: **shows** monoid0(G, P)

**using** groupAssum IsAgroup\_def monoid0\_def **by** simp

In some strange cases Isabelle has difficulties with applying the definition of a group. The next lemma defines a rule to be applied in such cases.

```
lemma definition_of_group: assumes IsAmonoid(G,f)
  and  $\forall g \in G. \exists b \in G. f\langle g, b \rangle = \text{TheNeutralElement}(G, f)$ 
  shows IsAgroup(G,f)
  using assms IsAgroup_def by simp
```

A technical lemma that allows to use 1 as the neutral element of the group without referencing a list of lemmas and definitions.

```
lemma (in group0) group0_2_L2:
  shows  $1 \in G \wedge (\forall g \in G. (1 \cdot g = g \wedge g \cdot 1 = g))$ 
  using group0_2_L1 monoid0.unit_is_neutral by simp
```

The group is closed under the group operation. Used all the time, useful to have handy.

```
lemma (in group0) group_op_closed: assumes a ∈ G b ∈ G
  shows a · b ∈ G using assms group0_2_L1 monoid0.group0_1_L1
  by simp
```

The group operation is associative. This is another technical lemma that allows to shorten the list of referenced lemmas in some proofs.

```
lemma (in group0) group_oper_assoc:
  assumes a ∈ G b ∈ G c ∈ G shows a · (b · c) = a · b · c
  using groupAssum assms IsAgroup_def IsAmonoid_def
  IsAssociative_def group_op_closed by simp
```

The group operation maps  $G \times G$  into  $G$ . It is convenient to have this fact easily accessible in the group0 context.

```
lemma (in group0) group_oper_assocA: shows P :  $G \times G \rightarrow G$ 
  using groupAssum IsAgroup_def IsAmonoid_def IsAssociative_def
  by simp
```

The definition of a group requires the existence of the right inverse. We show that this is also the left inverse.

```
theorem (in group0) group0_2_T1:
  assumes A1:  $g \in G$  and A2:  $b \in G$  and A3:  $g \cdot b = 1$ 
  shows  $b \cdot g = 1$ 
proof -
  from A2 groupAssum obtain c where I:  $c \in G \wedge b \cdot c = 1$ 
  using IsAgroup_def by auto
  then have c ∈ G by simp
  have  $1 \in G$  using group0_2_L2 by simp
  with A1 A2 I have  $b \cdot g = b \cdot (g \cdot (b \cdot c))$ 
  using group_op_closed group0_2_L2 group_oper_assoc
  by simp
  also from A1 A2 'c ∈ G' have  $b \cdot (g \cdot (b \cdot c)) = b \cdot (g \cdot b \cdot c)$ 
  using group_oper_assoc by simp
```

```

    also from A3 A2 I have  $b \cdot (g \cdot b \cdot c) = 1$  using group0_2_L2 by simp
    finally show  $b \cdot g = 1$  by simp
qed

```

For every element of a group there is only one inverse.

```

lemma (in group0) group0_2_L4:
  assumes A1:  $x \in G$  shows  $\exists! y. y \in G \wedge x \cdot y = 1$ 
proof
  from A1 groupAssum show  $\exists y. y \in G \wedge x \cdot y = 1$ 
    using IsAgroup_def by auto
  fix y n
  assume A2:  $y \in G \wedge x \cdot y = 1$  and A3:  $n \in G \wedge x \cdot n = 1$  show  $y = n$ 
  proof -
    from A1 A2 have T1:  $y \cdot x = 1$ 
      using group0_2_T1 by simp
    from A2 A3 have  $y = y \cdot (x \cdot n)$ 
      using group0_2_L2 by simp
    also from A1 A2 A3 have  $\dots = (y \cdot x) \cdot n$ 
      using group_oper_assoc by blast
    also from T1 A3 have  $\dots = n$ 
      using group0_2_L2 by simp
    finally show  $y = n$  by simp
  qed
qed

```

The group inverse is a function that maps  $G$  into  $G$ .

```

theorem group0_2_T2:
  assumes A1: IsAgroup(G,f) shows GroupInv(G,f) :  $G \rightarrow G$ 
proof -
  have  $\text{GroupInv}(G,f) \subseteq G \times G$  using GroupInv_def by auto
  moreover from A1 have
     $\forall x \in G. \exists! y. y \in G \wedge \langle x, y \rangle \in \text{GroupInv}(G,f)$ 
    using group0_def group0.group0_2_L4 GroupInv_def by simp
  ultimately show thesis using func1_1_L11 by simp
qed

```

We can think about the group inverse (the function) as the inverse image of the neutral element. Recall that in Isabelle  $f^{-1}(A)$  denotes the inverse image of the set  $A$ .

```

theorem (in group0) group0_2_T3: shows  $P^{-1}\{1\} = \text{GroupInv}(G,P)$ 
proof -
  from groupAssum have  $P : G \times G \rightarrow G$ 
    using IsAgroup_def IsAmonoid_def IsAssociative_def
    by simp
  then show  $P^{-1}\{1\} = \text{GroupInv}(G,P)$ 
    using func1_1_L14 GroupInv_def by auto
qed

```

The inverse is in the group.

```

lemma (in group0) inverse_in_group: assumes A1:  $x \in G$  shows  $x^{-1} \in G$ 
proof -
  from groupAssum have GroupInv(G,P) :  $G \rightarrow G$  using group0_2_T2 by simp
  with A1 show thesis using apply_type by simp
qed

```

The notation for the inverse means what it is supposed to mean.

```

lemma (in group0) group0_2_L6:
  assumes A1:  $x \in G$  shows  $x \cdot x^{-1} = 1 \wedge x^{-1} \cdot x = 1$ 
proof
  from groupAssum have GroupInv(G,P) :  $G \rightarrow G$ 
    using group0_2_T2 by simp
  with A1 have  $\langle x, x^{-1} \rangle \in \text{GroupInv}(G,P)$ 
    using apply_Pair by simp
  then show  $x \cdot x^{-1} = 1$  using GroupInv_def by simp
  with A1 show  $x^{-1} \cdot x = 1$  using inverse_in_group group0_2_T1
    by blast
qed

```

The next two lemmas state that unless we multiply by the neutral element, the result is always different than any of the operands.

```

lemma (in group0) group0_2_L7:
  assumes A1:  $a \in G$  and A2:  $b \in G$  and A3:  $a \cdot b = a$ 
  shows  $b = 1$ 
proof -
  from A3 have  $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot a$  by simp
  with A1 A2 show thesis using
    inverse_in_group group_oper_assoc group0_2_L6 group0_2_L2
    by simp
qed

```

See the comment to group0\_2\_L7.

```

lemma (in group0) group0_2_L8:
  assumes A1:  $a \in G$  and A2:  $b \in G$  and A3:  $a \cdot b = b$ 
  shows  $a = 1$ 
proof -
  from A3 have  $(a \cdot b) \cdot b^{-1} = b \cdot b^{-1}$  by simp
  with A1 A2 have  $a \cdot (b \cdot b^{-1}) = b \cdot b^{-1}$  using
    inverse_in_group group_oper_assoc by simp
  with A1 A2 show thesis
    using group0_2_L6 group0_2_L2 by simp
qed

```

The inverse of the neutral element is the neutral element.

```

lemma (in group0) group_inv_of_one: shows  $1^{-1} = 1$ 
  using group0_2_L2 inverse_in_group group0_2_L6 group0_2_L7 by blast

```

if  $a^{-1} = 1$ , then  $a = 1$ .

```

lemma (in group0) group0_2_L8A:
  assumes A1:  $a \in G$  and A2:  $a^{-1} = 1$ 
  shows  $a = 1$ 
proof -
  from A1 have  $a \cdot a^{-1} = 1$  using group0_2_L6 by simp
  with A1 A2 show  $a = 1$  using group0_2_L2 by simp
qed

```

If  $a$  is not a unit, then its inverse is not a unit either.

```

lemma (in group0) group0_2_L8B:
  assumes  $a \in G$  and  $a \neq 1$ 
  shows  $a^{-1} \neq 1$  using assms group0_2_L8A by auto

```

If  $a^{-1}$  is not a unit, then  $a$  is not a unit either.

```

lemma (in group0) group0_2_L8C:
  assumes  $a \in G$  and  $a^{-1} \neq 1$ 
  shows  $a \neq 1$ 
  using assms group0_2_L8A group_inv_of_one by auto

```

If a product of two elements of a group is equal to the neutral element then they are inverses of each other.

```

lemma (in group0) group0_2_L9:
  assumes A1:  $a \in G$  and A2:  $b \in G$  and A3:  $a \cdot b = 1$ 
  shows  $a = b^{-1}$  and  $b = a^{-1}$ 
proof -
  from A3 have  $a \cdot b \cdot b^{-1} = 1 \cdot b^{-1}$  by simp
  with A1 A2 have  $a \cdot (b \cdot b^{-1}) = 1 \cdot b^{-1}$  using
    inverse_in_group group_oper_assoc by simp
  with A1 A2 show  $a = b^{-1}$  using
    group0_2_L6 inverse_in_group group0_2_L2 by simp
  from A3 have  $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 1$  by simp
  with A1 A2 show  $b = a^{-1}$  using
    inverse_in_group group_oper_assoc group0_2_L6 group0_2_L2
    by simp
qed

```

It happens quite often that we know what is (have a meta-function for) the right inverse in a group. The next lemma shows that the value of the group inverse (function) is equal to the right inverse (meta-function).

```

lemma (in group0) group0_2_L9A:
  assumes A1:  $\forall g \in G. b(g) \in G \wedge g \cdot b(g) = 1$ 
  shows  $\forall g \in G. b(g) = g^{-1}$ 
proof
  fix g assume  $g \in G$ 
  moreover from A1 ' $g \in G$ ' have  $b(g) \in G$  by simp
  moreover from A1 ' $g \in G$ ' have  $g \cdot b(g) = 1$  by simp
  ultimately show  $b(g) = g^{-1}$  by (rule group0_2_L9)
qed

```



What is the inverse of a product?

```

lemma (in group0) group_inv_of_two:
  assumes A1: a∈G and A2: b∈G
  shows  $b^{-1} \cdot a^{-1} = (a \cdot b)^{-1}$ 
proof -
  from A1 A2 have
     $b^{-1} \in G$   $a^{-1} \in G$   $a \cdot b \in G$   $b^{-1} \cdot a^{-1} \in G$ 
    using inverse_in_group group_op_closed
    by auto
  from A1 A2 ' $b^{-1} \cdot a^{-1} \in G$ ' have  $a \cdot b \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot (b^{-1} \cdot a^{-1}))$ 
    using group_oper_assoc by simp
  moreover from A2 ' $b^{-1} \in G$ ' ' $a^{-1} \in G$ ' have  $b \cdot (b^{-1} \cdot a^{-1}) = b \cdot b^{-1} \cdot a^{-1}$ 
    using group_oper_assoc by simp
  moreover from A2 ' $a^{-1} \in G$ ' have  $b \cdot b^{-1} \cdot a^{-1} = a^{-1}$ 
    using group0_2_L6 group0_2_L2 by simp
  ultimately have  $a \cdot b \cdot (b^{-1} \cdot a^{-1}) = a \cdot a^{-1}$ 
    by simp
  with A1 have  $a \cdot b \cdot (b^{-1} \cdot a^{-1}) = 1$ 
    using group0_2_L6 by simp
  with ' $a \cdot b \in G$ ' ' $b^{-1} \cdot a^{-1} \in G$ ' show  $b^{-1} \cdot a^{-1} = (a \cdot b)^{-1}$ 
    using group0_2_L9 by simp
qed

```

What is the inverse of a product of three elements?

```

lemma (in group0) group_inv_of_three:
  assumes A1: a∈G b∈G c∈G
  shows
     $(a \cdot b \cdot c)^{-1} = c^{-1} \cdot (a \cdot b)^{-1}$ 
     $(a \cdot b \cdot c)^{-1} = c^{-1} \cdot (b^{-1} \cdot a^{-1})$ 
     $(a \cdot b \cdot c)^{-1} = c^{-1} \cdot b^{-1} \cdot a^{-1}$ 
proof -
  from A1 have T:
     $a \cdot b \in G$   $a^{-1} \in G$   $b^{-1} \in G$   $c^{-1} \in G$ 
    using group_op_closed inverse_in_group by auto
  with A1 show
     $(a \cdot b \cdot c)^{-1} = c^{-1} \cdot (a \cdot b)^{-1}$  and  $(a \cdot b \cdot c)^{-1} = c^{-1} \cdot (b^{-1} \cdot a^{-1})$ 
    using group_inv_of_two by auto
  with T show  $(a \cdot b \cdot c)^{-1} = c^{-1} \cdot b^{-1} \cdot a^{-1}$  using group_oper_assoc
    by simp
qed

```

The inverse of the inverse is the element.

```

lemma (in group0) group_inv_of_inv:
  assumes a∈G shows  $a = (a^{-1})^{-1}$ 
  using assms inverse_in_group group0_2_L6 group0_2_L9
  by simp

```

Group inverse is nilpotent, therefore a bijection and involution.

```

lemma (in group0) group_inv_bij:

```

```

    shows GroupInv(G,P) 0 GroupInv(G,P) = id(G) and GroupInv(G,P) ∈ bij(G,G)
and
  GroupInv(G,P) = converse(GroupInv(G,P))
proof -
  have I: GroupInv(G,P): G→G using groupAssum group0_2_T2 by simp
  then have GroupInv(G,P) 0 GroupInv(G,P): G→G and id(G):G→G
    using comp_fun id_type by auto
  moreover
  { fix g assume g∈G
    with I have (GroupInv(G,P) 0 GroupInv(G,P))(g) = id(G)(g)
      using comp_fun_apply group_inv_of_inv id_conv by simp
  } hence ∀g∈G. (GroupInv(G,P) 0 GroupInv(G,P))(g) = id(G)(g) by simp
  ultimately show GroupInv(G,P) 0 GroupInv(G,P) = id(G)
    by (rule func_eq)
  with I show GroupInv(G,P) ∈ bij(G,G) using nilpotent_imp_bijective
    by simp
  with 'GroupInv(G,P) 0 GroupInv(G,P) = id(G)' show
    GroupInv(G,P) = converse(GroupInv(G,P)) using comp_id_conv by simp
qed

```

For the group inverse the image is the same as inverse image.

```

lemma (in group0) inv_image_vimage: shows GroupInv(G,P)(V) = GroupInv(G,P)-(V)
  using group_inv_bij vimage_converse by simp

```

If the unit is in a set then it is in the inverse of that set.

```

lemma (in group0) neut_inv_neut: assumes A⊆G and 1∈A
  shows 1 ∈ GroupInv(G,P)(A)
proof -
  have GroupInv(G,P):G→G using groupAssum group0_2_T2 by simp
  with assms have 1-1 ∈ GroupInv(G,P)(A) using func_imagedef by auto
  then show thesis using group_inv_of_one by simp
qed

```

The group inverse is onto.

```

lemma (in group0) group_inv_surj: shows GroupInv(G,P)(G) = G
  using group_inv_bij bij_def surj_range_image_domain by auto

```

If  $a^{-1} \cdot b = 1$ , then  $a = b$ .

```

lemma (in group0) group0_2_L11:
  assumes A1: a∈G b∈G and A2: a-1·b = 1
  shows a=b
proof -
  from A1 A2 have a-1 ∈ G b∈G a-1·b = 1
    using inverse_in_group by auto
  then have b = (a-1)-1 by (rule group0_2_L9)
  with A1 show a=b using group_inv_of_inv by simp
qed

```

If  $a \cdot b^{-1} = 1$ , then  $a = b$ .

```

lemma (in group0) group0_2_L11A:
  assumes A1:  $a \in G$   $b \in G$  and A2:  $a \cdot b^{-1} = 1$ 
  shows  $a = b$ 
proof -
  from A1 A2 have  $a \in G$   $b^{-1} \in G$   $a \cdot b^{-1} = 1$ 
  using inverse_in_group by auto
  then have  $a = (b^{-1})^{-1}$  by (rule group0_2_L9)
  with A1 show  $a = b$  using group_inv_of_inv by simp
qed

```

If the inverse of  $b$  is different than  $a$ , then the inverse of  $a$  is different than  $b$ .

```

lemma (in group0) group0_2_L11B:
  assumes A1:  $a \in G$  and A2:  $b^{-1} \neq a$ 
  shows  $a^{-1} \neq b$ 
proof -
  { assume  $a^{-1} = b$ 
    then have  $(a^{-1})^{-1} = b^{-1}$  by simp
    with A1 A2 have False using group_inv_of_inv
    by simp
  } then show  $a^{-1} \neq b$  by auto
qed

```

What is the inverse of  $ab^{-1}$  ?

```

lemma (in group0) group0_2_L12:
  assumes A1:  $a \in G$   $b \in G$ 
  shows
     $(a \cdot b^{-1})^{-1} = b \cdot a^{-1}$ 
     $(a^{-1} \cdot b)^{-1} = b^{-1} \cdot a$ 
proof -
  from A1 have
     $(a \cdot b^{-1})^{-1} = (b^{-1})^{-1} \cdot a^{-1}$  and  $(a^{-1} \cdot b)^{-1} = b^{-1} \cdot (a^{-1})^{-1}$ 
    using inverse_in_group group_inv_of_two by auto
  with A1 show  $(a \cdot b^{-1})^{-1} = b \cdot a^{-1}$   $(a^{-1} \cdot b)^{-1} = b^{-1} \cdot a$ 
    using group_inv_of_inv by auto
qed

```

A couple useful rearrangements with three elements: we can insert a  $b \cdot b^{-1}$  between two group elements (another version) and one about a product of an element and inverse of a product, and two others.

```

lemma (in group0) group0_2_L14A:
  assumes A1:  $a \in G$   $b \in G$   $c \in G$ 
  shows
     $a \cdot c^{-1} = (a \cdot b^{-1}) \cdot (b \cdot c^{-1})$ 
     $a^{-1} \cdot c = (a^{-1} \cdot b) \cdot (b^{-1} \cdot c)$ 
     $a \cdot (b \cdot c)^{-1} = a \cdot c^{-1} \cdot b^{-1}$ 
     $a \cdot (b \cdot c^{-1}) = a \cdot b \cdot c^{-1}$ 
     $(a \cdot b^{-1} \cdot c^{-1})^{-1} = c \cdot b \cdot a^{-1}$ 

```

```

a·b·c-1·(c·b-1) = a
a·(b·c)·c-1 = a·b
proof -
  from A1 have T:
    a-1 ∈ G  b-1 ∈ G  c-1 ∈ G
    a-1·b ∈ G  a·b-1 ∈ G  a·b ∈ G
    c·b-1 ∈ G  b·c ∈ G
  using inverse_in_group group_op_closed
  by auto
  from A1 T have
    a·c-1 = a·(b-1·b)·c-1
    a-1·c = a-1·(b·b-1)·c
  using group0_2_L2 group0_2_L6 by auto
  with A1 T show
    a·c-1 = (a·b-1)·(b·c-1)
    a-1·c = (a-1·b)·(b-1·c)
  using group_oper_assoc by auto
  from A1 have a·(b·c)-1 = a·(c-1·b-1)
  using group_inv_of_two by simp
  with A1 T show a·(b·c)-1 = a·c-1·b-1
  using group_oper_assoc by simp
  from A1 T show a·(b·c-1) = a·b·c-1
  using group_oper_assoc by simp
  from A1 T show (a·b-1·c-1)-1 = c·b·a-1
  using group_inv_of_three group_inv_of_inv
  by simp
  from T have a·b·c-1·(c·b-1) = a·b·(c-1·(c·b-1))
  using group_oper_assoc by simp
  also from A1 T have ... = a·b·b-1
  using group_oper_assoc group0_2_L6 group0_2_L2
  by simp
  also from A1 T have ... = a·(b·b-1)
  using group_oper_assoc by simp
  also from A1 have ... = a
  using group0_2_L6 group0_2_L2 by simp
  finally show a·b·c-1·(c·b-1) = a by simp
  from A1 T have a·(b·c)·c-1 = a·(b·(c·c-1))
  using group_oper_assoc by simp
  also from A1 T have ... = a·b
  using group0_2_L6 group0_2_L2 by simp
  finally show a·(b·c)·c-1 = a·b
  by simp
qed

```

Another lemma about rearranging a product of four group elements.

```

lemma (in group0) group0_2_L15:
  assumes A1: a ∈ G  b ∈ G  c ∈ G  d ∈ G
  shows (a·b)·(c·d)-1 = a·(b·d-1)·a-1·(a·c-1)
proof -

```

```

from A1 have T1:
   $d^{-1} \in G \quad c^{-1} \in G \quad a \cdot b \in G \quad a \cdot (b \cdot d^{-1}) \in G$ 
  using inverse_in_group group_op_closed
  by auto
with A1 have  $(a \cdot b) \cdot (c \cdot d)^{-1} = (a \cdot b) \cdot (d^{-1} \cdot c^{-1})$ 
  using group_inv_of_two by simp
also from A1 T1 have  $\dots = a \cdot (b \cdot d^{-1}) \cdot c^{-1}$ 
  using group_oper_assoc by simp
also from A1 T1 have  $\dots = a \cdot (b \cdot d^{-1}) \cdot a^{-1} \cdot (a \cdot c^{-1})$ 
  using group0_2_L14A by blast
finally show thesis by simp
qed

```

We can cancel an element with its inverse that is written next to it.

```

lemma (in group0) inv_cancel_two:
  assumes A1:  $a \in G \quad b \in G$ 
  shows
     $a \cdot b^{-1} \cdot b = a$ 
     $a \cdot b \cdot b^{-1} = a$ 
     $a^{-1} \cdot (a \cdot b) = b$ 
     $a \cdot (a^{-1} \cdot b) = b$ 
  proof -
    from A1 have
       $a \cdot b^{-1} \cdot b = a \cdot (b^{-1} \cdot b)$ 
       $a \cdot b \cdot b^{-1} = a \cdot (b \cdot b^{-1})$ 
       $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot a \cdot b$ 
       $a \cdot (a^{-1} \cdot b) = a \cdot a^{-1} \cdot b$ 
      using inverse_in_group group_oper_assoc by auto
    with A1 show
       $a \cdot b^{-1} \cdot b = a$ 
       $a \cdot b \cdot b^{-1} = a$ 
       $a^{-1} \cdot (a \cdot b) = b$ 
       $a \cdot (a^{-1} \cdot b) = b$ 
      using group0_2_L6 group0_2_L2 by auto
  qed

```

Another lemma about cancelling with two group elements.

```

lemma (in group0) group0_2_L16A:
  assumes A1:  $a \in G \quad b \in G$ 
  shows  $a \cdot (b \cdot a)^{-1} = b^{-1}$ 
  proof -
    from A1 have  $(b \cdot a)^{-1} = a^{-1} \cdot b^{-1} \quad b^{-1} \in G$ 
      using group_inv_of_two inverse_in_group by auto
    with A1 show  $a \cdot (b \cdot a)^{-1} = b^{-1}$  using inv_cancel_two
      by simp
  qed

```

Adding a neutral element to a set that is closed under the group operation results in a set that is closed under the group operation.

```

lemma (in group0) group0_2_L17:
  assumes  $H \subseteq G$ 

```

```

and H {is closed under} P
shows (H  $\cup$  {1}) {is closed under} P
using assms IsOpClosed_def group0_2_L2 by auto

```

We can put an element on the other side of an equation.

```

lemma (in group0) group0_2_L18:
  assumes A1: a $\in$ G b $\in$ G c $\in$ G
  and A2: c = a $\cdot$ b
  shows c $\cdot$ b-1 = a a-1 $\cdot$ c = b
proof-
  from A2 A1 have c $\cdot$ b-1 = a $\cdot$ (b $\cdot$ b-1) a-1 $\cdot$ c = (a-1 $\cdot$ a) $\cdot$ b
  using inverse_in_group group_oper_assoc by auto
  moreover from A1 have a $\cdot$ (b $\cdot$ b-1) = a (a-1 $\cdot$ a) $\cdot$ b = b
  using group0_2_L6 group0_2_L2 by auto
  ultimately show c $\cdot$ b-1 = a a-1 $\cdot$ c = b
  by auto
qed

```

Multiplying different group elements by the same factor results in different group elements.

```

lemma (in group0) group0_2_L19:
  assumes A1: a $\in$ G b $\in$ G c $\in$ G and A2: a $\neq$ b
  shows a $\cdot$ c  $\neq$  b $\cdot$ c and c $\cdot$ a  $\neq$  c $\cdot$ b
proof -
  { assume a $\cdot$ c = b $\cdot$ c  $\vee$  c $\cdot$ a = c $\cdot$ b
    then have a $\cdot$ c $\cdot$ c-1 = b $\cdot$ c $\cdot$ c-1  $\vee$  c-1 $\cdot$ (c $\cdot$ a) = c-1 $\cdot$ (c $\cdot$ b)
    by auto
    with A1 A2 have False using inv_cancel_two by simp
  } then show a $\cdot$ c  $\neq$  b $\cdot$ c and c $\cdot$ a  $\neq$  c $\cdot$ b by auto
qed

```

## 20.2 Subgroups

There are two common ways to define subgroups. One requires that the group operation is closed in the subgroup. The second one defines subgroup as a subset of a group which is itself a group under the group operations. We use the second approach because it results in shorter definition.

The rest of this section is devoted to proving the equivalence of these two definitions of the notion of a subgroup.

A pair  $(H, P)$  is a subgroup if  $H$  forms a group with the operation  $P$  restricted to  $H \times H$ . It may be surprising that we don't require  $H$  to be a subset of  $G$ . This however can be inferred from the definition if the pair  $(G, P)$  is a group, see lemma group0\_3\_L2.

**definition**

```

IsAsubgroup(H,P)  $\equiv$  IsAgroup(H, restrict(P,H $\times$ H))

```

Formally the group operation in a subgroup is different than in the group as they have different domains. Of course we want to use the original operation with the associated notation in the subgroup. The next couple of lemmas will allow for that.

The next lemma states that the neutral element of a subgroup is in the subgroup and it is both right and left neutral there. The notation is very ugly because we don't want to introduce a separate notation for the subgroup operation.

```

lemma group0_3_L1:
  assumes A1: IsAsubgroup(H,f)
  and A2: n = TheNeutralElement(H,restrict(f,H×H))
  shows n ∈ H
  ∀h∈H. restrict(f,H×H)⟨n,h⟩ = h
  ∀h∈H. restrict(f,H×H)⟨h,n⟩ = h
proof -
  let b = restrict(f,H×H)
  let e = TheNeutralElement(H,restrict(f,H×H))
  from A1 have group0(H,b)
    using IsAsubgroup_def group0_def by simp
  then have I:
    e ∈ H ∧ (∀h∈H. (b⟨e,h⟩ = h ∧ b⟨h,e⟩ = h))
    by (rule group0.group0_2_L2)
  with A2 show n ∈ H by simp
  from A2 I show ∀h∈H. b⟨n,h⟩ = h and ∀h∈H. b⟨h,n⟩ = h
    by auto
qed

```

A subgroup is contained in the group.

```

lemma (in group0) group0_3_L2:
  assumes A1: IsAsubgroup(H,P)
  shows H ⊆ G
proof
  fix h assume h∈H
  let b = restrict(P,H×H)
  let n = TheNeutralElement(H,restrict(P,H×H))
  from A1 have b ∈ H×H→H
    using IsAsubgroup_def IsAgroup_def
    IsAmonoid_def IsAssociative_def by simp
  moreover from A1 'h∈H' have ⟨n,h⟩ ∈ H×H
    using group0_3_L1 by simp
  moreover from A1 'h∈H' have h = b⟨n,h⟩
    using group0_3_L1 by simp
  ultimately have ⟨⟨n,h⟩,h⟩ ∈ b
    using func1_1_L5A by blast
  then have ⟨⟨n,h⟩,h⟩ ∈ P using restrict_subset by auto
  moreover from groupAssum have P:G×G→G
    using IsAgroup_def IsAmonoid_def IsAssociative_def
    by simp

```

```

ultimately show h ∈ G using func1_1_L5
  by blast
qed

```

The group's neutral element (denoted 1 in the group0 context) is a neutral element for the subgroup with respect to the group action.

```

lemma (in group0) group0_3_L3:
  assumes IsAsubgroup(H,P)
  shows  $\forall h \in H. 1 \cdot h = h \wedge h \cdot 1 = h$ 
  using assms groupAssum group0_3_L2 group0_2_L2
  by auto

```

The neutral element of a subgroup is the same as that of the group.

```

lemma (in group0) group0_3_L4: assumes A1: IsAsubgroup(H,P)
  shows TheNeutralElement(H,restrict(P,H×H)) = 1
proof -
  let n = TheNeutralElement(H,restrict(P,H×H))
  from A1 have n ∈ H using group0_3_L1 by simp
  with groupAssum A1 have n ∈ G using group0_3_L2 by auto
  with A1 'n ∈ H' show thesis using
    group0_3_L1 restrict_if group0_2_L7 by simp
qed

```

The neutral element of the group (denoted 1 in the group0 context) belongs to every subgroup.

```

lemma (in group0) group0_3_L5: assumes A1: IsAsubgroup(H,P)
  shows 1 ∈ H
proof -
  from A1 show 1 ∈ H using group0_3_L1 group0_3_L4
    by fast
qed

```

Subgroups are closed with respect to the group operation.

```

lemma (in group0) group0_3_L6: assumes A1: IsAsubgroup(H,P)
  and A2: a ∈ H b ∈ H
  shows a · b ∈ H
proof -
  let f = restrict(P,H×H)
  from A1 have monoid0(H,f) using
    IsAsubgroup_def IsAgroup_def monoid0_def by simp
  with A2 have f ((a,b)) ∈ H using monoid0.group0_1_L1
    by blast
  with A2 show a · b ∈ H using restrict_if by simp
qed

```

A preliminary lemma that we need to show that taking the inverse in the subgroup is the same as taking the inverse in the group.

```

lemma group0_3_L7A:

```



```

assumes A1: IsAgroup(G,f)
and A2: IsAsubgroup(H,f) and A3: g = restrict(f,H×H)
shows GroupInv(G,f) ∩ H×H = GroupInv(H,g)
proof -
  let e = TheNeutralElement(G,f)
  let e1 = TheNeutralElement(H,g)
  from A1 have group0(G,f) using group0_def by simp
  from A2 A3 have group0(H,g)
    using IsAsubgroup_def group0_def by simp
  from 'group0(G,f)' A2 A3 have GroupInv(G,f) = f- $\{e_1\}$ 
    using group0.group0_3_L4 group0.group0_2_T3
    by simp
  moreover have g- $\{e_1\}$  = f- $\{e_1\}$  ∩ H×H
proof -
  from A1 have f ∈ G×G→G
    using IsAgroup_def IsAmonoid_def IsAssociative_def
    by simp
  moreover from A2 'group0(G,f)' have H×H ⊆ G×G
    using group0.group0_3_L2 by auto
  ultimately show g- $\{e_1\}$  = f- $\{e_1\}$  ∩ H×H
    using A3 func1_2_L1 by simp
qed
moreover from A3 'group0(H,g)' have GroupInv(H,g) = g- $\{e_1\}$ 
  using group0.group0_2_T3 by simp
ultimately show thesis by simp
qed

```

Using the lemma above we can show the actual statement: taking the inverse in the subgroup is the same as taking the inverse in the group.

```

theorem (in group0) group0_3_T1:
  assumes A1: IsAsubgroup(H,P)
  and A2: g = restrict(P,H×H)
  shows GroupInv(H,g) = restrict(GroupInv(G,P),H)
proof -
  from groupAssum have GroupInv(G,P) : G→G
    using group0_2_T2 by simp
  moreover from A1 A2 have GroupInv(H,g) : H→H
    using IsAsubgroup_def group0_2_T2 by simp
  moreover from A1 have H ⊆ G
    using group0_3_L2 by simp
  moreover from groupAssum A1 A2 have
    GroupInv(G,P) ∩ H×H = GroupInv(H,g)
    using group0_3_L7A by simp
  ultimately show thesis
    using func1_2_L3 by simp
qed

```

A slightly weaker, but more convenient in applications, reformulation of the above theorem.

```

theorem (in group0) group0_3_T2:
  assumes IsAsubgroup(H,P)
  and g = restrict(P,H×H)
  shows  $\forall h \in H. \text{GroupInv}(H,g)(h) = h^{-1}$ 
  using assms group0_3_T1 restrict_if by simp

```

Subgroups are closed with respect to taking the group inverse.

```

theorem (in group0) group0_3_T3A:
  assumes A1: IsAsubgroup(H,P) and A2:  $h \in H$ 
  shows  $h^{-1} \in H$ 
proof -
  let g = restrict(P,H×H)
  from A1 have GroupInv(H,g)  $\in H \rightarrow H$ 
    using IsAsubgroup_def group0_2_T2 by simp
  with A2 have GroupInv(H,g)(h)  $\in H$ 
    using apply_type by simp
  with A1 A2 show  $h^{-1} \in H$  using group0_3_T2 by simp
qed

```

The next theorem states that a nonempty subset of a group  $G$  that is closed under the group operation and taking the inverse is a subgroup of the group.

```

theorem (in group0) group0_3_T3:
  assumes A1:  $H \neq 0$ 
  and A2:  $H \subseteq G$ 
  and A3:  $H$  {is closed under}  $P$ 
  and A4:  $\forall x \in H. x^{-1} \in H$ 
  shows IsAsubgroup(H,P)
proof -
  let g = restrict(P,H×H)
  let n = TheNeutralElement(H,g)
  from A3 have I:  $\forall x \in H. \forall y \in H. x \cdot y \in H$ 
    using IsOpClosed_def by simp
  from A1 obtain x where  $x \in H$  by auto
  with A4 I A2 have  $1 \in H$ 
    using group0_2_L6 by blast
  with A3 A2 have T2: IsAmonoid(H,g)
    using group0_2_L1 monoid0.group0_1_T1
    by simp
  moreover have  $\forall h \in H. \exists b \in H. g(h,b) = n$ 
proof
  fix h assume  $h \in H$ 
  with A4 A2 have  $h \cdot h^{-1} = 1$ 
    using group0_2_L6 by auto
  moreover from groupAssum A2 A3 ' $1 \in H$ ' have  $1 = n$ 
    using IsAgroup_def group0_1_L6 by auto
  moreover from A4 ' $h \in H$ ' have  $g(h,h^{-1}) = h \cdot h^{-1}$ 
    using restrict_if by simp
  ultimately have  $g(h,h^{-1}) = n$  by simp
  with A4 ' $h \in H$ ' show  $\exists b \in H. g(h,b) = n$  by auto

```

```

qed
ultimately show IsAsubgroup(H,P) using
  IsAsubgroup_def IsAgroup_def by simp
qed

```

Intersection of subgroups is a subgroup.

```

lemma group0_3_L7:
  assumes A1: IsAgroup(G,f)
  and A2: IsAsubgroup(H1,f)
  and A3: IsAsubgroup(H2,f)
  shows IsAsubgroup(H1∩H2,restrict(f,H1×H1))
proof -
  let e = TheNeutralElement(G,f)
  let g = restrict(f,H1×H1)
  from A1 have I: group0(G,f)
    using group0_def by simp
  from A2 have group0(H1,g)
    using IsAsubgroup_def group0_def by simp
  moreover have H1∩H2 ≠ 0
  proof -
    from A1 A2 A3 have e ∈ H1∩H2
      using group0_def group0.group0_3_L5 by simp
    thus thesis by auto
  qed
  moreover have H1∩H2 ⊆ H1 by auto
  moreover from A2 A3 I 'H1∩H2 ⊆ H1' have
    H1∩H2 {is closed under} g
    using group0.group0_3_L6 IsOpClosed_def
      func_ZF_4_L7 func_ZF_4_L5 by simp
  moreover from A2 A3 I have
    ∀x ∈ H1∩H2. GroupInv(H1,g)(x) ∈ H1∩H2
    using group0.group0_3_T2 group0.group0_3_T3A
      by simp
  ultimately show thesis
    using group0.group0_3_T3 by simp
qed

```

The range of the subgroup operation is the whole subgroup.

```

lemma image_subgr_op: assumes A1: IsAsubgroup(H,P)
  shows restrict(P,H×H)(H×H) = H
proof -
  from A1 have monoid0(H,restrict(P,H×H))
    using IsAsubgroup_def IsAgroup_def monoid0_def
      by simp
  then show thesis by (rule monoid0.range_carr)
qed

```

If we restrict the inverse to a subgroup, then the restricted inverse is onto the subgroup.

```

lemma (in group0) restr_inv_onto: assumes A1: IsAsubgroup(H,P)
  shows restrict(GroupInv(G,P),H)(H) = H
proof -
  from A1 have GroupInv(H,restrict(P,H×H))(H) = H
    using IsAsubgroup_def group0_def group0.group_inv_surj
    by simp
  with A1 show thesis using group0_3_T1 by simp
qed
end

```

## 21 Group\_ZF\_1.thy

**theory** Group\_ZF\_1 **imports** Group\_ZF

**begin**

In this theory we consider right and left translations and odd functions.

### 21.1 Translations

In this section we consider translations. Translations are maps  $T : G \rightarrow G$  of the form  $T_g(a) = g \cdot a$  or  $T_g(a) = a \cdot g$ . We also consider two-dimensional translations  $T_g : G \times G \rightarrow G \times G$ , where  $T_g(a, b) = (a \cdot g, b \cdot g)$  or  $T_g(a, b) = (g \cdot a, g \cdot b)$ .

For an element  $a \in G$  the right translation is defined a function (set of pairs) such that its value (the second element of a pair) is the value of the group operation on the first element of the pair and  $g$ . This looks a bit strange in the raw set notation, when we write a function explicitly as a set of pairs and value of the group operation on the pair  $\langle a, b \rangle$  as  $P\langle a, b \rangle$  instead of the usual infix  $a \cdot b$  or  $a + b$ .

**definition**

$$\text{RightTranslation}(G, P, g) \equiv \{ \langle a, b \rangle \in G \times G. P\langle a, g \rangle = b \}$$

A similar definition of the left translation.

**definition**

$$\text{LeftTranslation}(G, P, g) \equiv \{ \langle a, b \rangle \in G \times G. P\langle g, a \rangle = b \}$$

Translations map  $G$  into  $G$ . Two dimensional translations map  $G \times G$  into itself.

**lemma** (in group0) group0\_5\_L1: **assumes** A1:  $g \in G$

**shows**  $\text{RightTranslation}(G, P, g) : G \rightarrow G$  **and**  $\text{LeftTranslation}(G, P, g) : G \rightarrow G$

**proof** -

**from** A1 **have**  $\forall a \in G. a \cdot g \in G$  **and**  $\forall a \in G. g \cdot a \in G$

**using** group\_oper\_assocA **apply** funtype **by** auto

**then show**

$\text{RightTranslation}(G, P, g) : G \rightarrow G$

$\text{LeftTranslation}(G, P, g) : G \rightarrow G$

**using** RightTranslation\_def LeftTranslation\_def func1\_1\_L11A

**by** auto

**qed**

The values of the translations are what we expect.

**lemma** (in group0) group0\_5\_L2: **assumes**  $g \in G$   $a \in G$

**shows**

$$\text{RightTranslation}(G, P, g)(a) = a \cdot g$$

```

LeftTranslation(G,P,g)(a) = g·a
using assms group0_5_L1 RightTranslation_def LeftTranslation_def
func1_1_L11B by auto

```

Composition of left translations is a left translation by the product.

```

lemma (in group0) group0_5_L4: assumes A1: g∈G h∈G a∈G and
  A2: Tg = LeftTranslation(G,P,g) Th = LeftTranslation(G,P,h)
  shows
    Tg(Th(a)) = g·h·a
    Tg(Th(a)) = LeftTranslation(G,P,g·h)(a)
proof -
  from A1 have I: h·a∈G g·h∈G
    using group_oper_assocA apply_funtype by auto
  with A1 A2 show Tg(Th(a)) = g·h·a
    using group0_5_L2 group_oper_assoc by simp
  with A1 A2 I show
    Tg(Th(a)) = LeftTranslation(G,P,g·h)(a)
    using group0_5_L2 group_oper_assoc by simp
qed

```

Composition of right translations is a right translation by the product.

```

lemma (in group0) group0_5_L5: assumes A1: g∈G h∈G a∈G and
  A2: Tg = RightTranslation(G,P,g) Th = RightTranslation(G,P,h)
  shows
    Tg(Th(a)) = a·h·g
    Tg(Th(a)) = RightTranslation(G,P,h·g)(a)
proof -
  from A1 have I: a·h∈G h·g ∈G
    using group_oper_assocA apply_funtype by auto
  with A1 A2 show Tg(Th(a)) = a·h·g
    using group0_5_L2 group_oper_assoc by simp
  with A1 A2 I show
    Tg(Th(a)) = RightTranslation(G,P,h·g)(a)
    using group0_5_L2 group_oper_assoc by simp
qed

```

Point free version of group0\_5\_L4 and group0\_5\_L5.

```

lemma (in group0) trans_comp: assumes g∈G h∈G shows
  RightTranslation(G,P,g) 0 RightTranslation(G,P,h) = RightTranslation(G,P,h·g)
  LeftTranslation(G,P,g) 0 LeftTranslation(G,P,h) = LeftTranslation(G,P,g·h)
proof -
  let Tg = RightTranslation(G,P,g)
  let Th = RightTranslation(G,P,h)
  from assms have Tg:G→G and Th:G→G
    using group0_5_L1 by auto
  then have Tg 0 Th:G→G using comp_fun by simp
  moreover from assms have RightTranslation(G,P,h·g):G→G
    using group_op_closed group0_5_L1 by simp
  moreover from assms 'Th:G→G' have

```

```

    ∀ a ∈ G. (Tg ∘ Th)(a) = RightTranslation(G,P,h·g)(a)
    using comp_fun_apply group0_5_L5 by simp
    ultimately show Tg ∘ Th = RightTranslation(G,P,h·g)
    by (rule func_eq)
next
  let Tg = LeftTranslation(G,P,g)
  let Th = LeftTranslation(G,P,h)
  from assms have Tg:G→G and Th:G→G
    using group0_5_L1 by auto
  then have Tg ∘ Th:G→G using comp_fun by simp
  moreover from assms have LeftTranslation(G,P,g·h):G→G
    using group_op_closed group0_5_L1 by simp
  moreover from assms 'Th:G→G' have
    ∀ a ∈ G. (Tg ∘ Th)(a) = LeftTranslation(G,P,g·h)(a)
    using comp_fun_apply group0_5_L4 by simp
  ultimately show Tg ∘ Th = LeftTranslation(G,P,g·h)
  by (rule func_eq)
qed

```

The image of a set under a composition of translations is the same as the image under translation by a product.

```

lemma (in group0) trans_comp_image: assumes A1: g ∈ G h ∈ G and
  A2: Tg = LeftTranslation(G,P,g) Th = LeftTranslation(G,P,h)
shows Tg(Th(A)) = LeftTranslation(G,P,g·h)(A)
proof -
  from A2 have Tg(Th(A)) = (Tg ∘ Th)(A)
    using image_comp by simp
  with assms show thesis using trans_comp by simp
qed

```

Another form of the image of a set under a composition of translations

```

lemma (in group0) group0_5_L6:
  assumes A1: g ∈ G h ∈ G and A2: A ⊆ G and
  A3: Tg = RightTranslation(G,P,g) Th = RightTranslation(G,P,h)
shows Tg(Th(A)) = {a·h·g. a ∈ A}
proof -
  from A2 have ∀ a ∈ A. a ∈ G by auto
  from A1 A3 have Tg : G→G Th : G→G
    using group0_5_L1 by auto
  with assms '∀ a ∈ A. a ∈ G' show
    Tg(Th(A)) = {a·h·g. a ∈ A}
    using func1_1_L15C group0_5_L5 by auto
qed

```

The translation by neutral element is the identity on group.

```

lemma (in group0) trans_neutral: shows
  RightTranslation(G,P,1) = id(G) and LeftTranslation(G,P,1) = id(G)
proof -

```

```

    have RightTranslation(G,P,1):G→G and ∀a∈G. RightTranslation(G,P,1)(a)
= a
    using group0_2_L2 group0_5_L1 group0_5_L2 by auto
    then show RightTranslation(G,P,1) = id(G) by (rule identity_fun)
    have LeftTranslation(G,P,1):G→G and ∀a∈G. LeftTranslation(G,P,1)(a)
= a
    using group0_2_L2 group0_5_L1 group0_5_L2 by auto
    then show LeftTranslation(G,P,1) = id(G) by (rule identity_fun)
qed

```

Composition of translations by an element and its inverse is identity.

```

lemma (in group0) trans_comp_id: assumes g∈G shows
  RightTranslation(G,P,g) ∘ RightTranslation(G,P,g-1) = id(G) and
  RightTranslation(G,P,g-1) ∘ RightTranslation(G,P,g) = id(G) and
  LeftTranslation(G,P,g) ∘ LeftTranslation(G,P,g-1) = id(G) and
  LeftTranslation(G,P,g-1) ∘ LeftTranslation(G,P,g) = id(G)
  using assms inverse_in_group trans_comp group0_2_L6 trans_neutral by
auto

```

Translations are bijective.

```

lemma (in group0) trans_bij: assumes g∈G shows
  RightTranslation(G,P,g) ∈ bij(G,G) and LeftTranslation(G,P,g) ∈ bij(G,G)
proof-
  from assms have
    RightTranslation(G,P,g):G→G and
    RightTranslation(G,P,g-1):G→G and
    RightTranslation(G,P,g) ∘ RightTranslation(G,P,g-1) = id(G)
    RightTranslation(G,P,g-1) ∘ RightTranslation(G,P,g) = id(G)
  using inverse_in_group group0_5_L1 trans_comp_id by auto
  then show RightTranslation(G,P,g) ∈ bij(G,G) using fg_imp_bijective
by simp
  from assms have
    LeftTranslation(G,P,g):G→G and
    LeftTranslation(G,P,g-1):G→G and
    LeftTranslation(G,P,g) ∘ LeftTranslation(G,P,g-1) = id(G)
    LeftTranslation(G,P,g-1) ∘ LeftTranslation(G,P,g) = id(G)
  using inverse_in_group group0_5_L1 trans_comp_id by auto
  then show LeftTranslation(G,P,g) ∈ bij(G,G) using fg_imp_bijective
by simp
qed

```

Converse of a translation is translation by the inverse.

```

lemma (in group0) trans_conv_inv: assumes g∈G shows
  converse(RightTranslation(G,P,g)) = RightTranslation(G,P,g-1) and
  converse(LeftTranslation(G,P,g)) = LeftTranslation(G,P,g-1) and
  LeftTranslation(G,P,g) = converse(LeftTranslation(G,P,g-1)) and
  RightTranslation(G,P,g) = converse(RightTranslation(G,P,g-1))
proof -
  from assms have

```



```

    RightTranslation(G,P,g) ∈ bij(G,G)  RightTranslation(G,P,g-1) ∈ bij(G,G)
and
    LeftTranslation(G,P,g) ∈ bij(G,G)  LeftTranslation(G,P,g-1) ∈ bij(G,G)
    using trans_bij inverse_in_group by auto
moreover from assms have
    RightTranslation(G,P,g-1) ∘ RightTranslation(G,P,g) = id(G) and
    LeftTranslation(G,P,g-1) ∘ LeftTranslation(G,P,g) = id(G) and
    LeftTranslation(G,P,g) ∘ LeftTranslation(G,P,g-1) = id(G) and
    LeftTranslation(G,P,g-1) ∘ LeftTranslation(G,P,g) = id(G)
    using trans_comp_id by auto
ultimately show
    converse(RightTranslation(G,P,g)) = RightTranslation(G,P,g-1) and
    converse(LeftTranslation(G,P,g)) = LeftTranslation(G,P,g-1) and
    LeftTranslation(G,P,g) = converse(LeftTranslation(G,P,g-1)) and
    RightTranslation(G,P,g) = converse(RightTranslation(G,P,g-1))
    using comp_id_conv by auto
qed

```

The image of a set by translation is the same as the inverse image by the inverse element translation.

```

lemma (in group0) trans_image_vimage: assumes g∈G shows
    LeftTranslation(G,P,g)(A) = LeftTranslation(G,P,g-1)-(A) and
    RightTranslation(G,P,g)(A) = RightTranslation(G,P,g-1)-(A)
    using assms trans_conv_inv vimage_converse by auto

```

Another way of looking at translations is that they are sections of the group operation.

```

lemma (in group0) trans_eq_section: assumes g∈G shows
    RightTranslation(G,P,g) = Fix2ndVar(P,g) and
    LeftTranslation(G,P,g) = Fix1stVar(P,g)
proof -
    let T = RightTranslation(G,P,g)
    let F = Fix2ndVar(P,g)
    from assms have T: G→G and F: G→G
    using group0_5_L1 group_oper_assocA fix_2nd_var_fun by auto
    moreover from assms have ∀a∈G. T(a) = F(a)
    using group0_5_L2 group_oper_assocA fix_var_val by simp
    ultimately show T = F by (rule func_eq)
next
    let T = LeftTranslation(G,P,g)
    let F = Fix1stVar(P,g)
    from assms have T: G→G and F: G→G
    using group0_5_L1 group_oper_assocA fix_1st_var_fun by auto
    moreover from assms have ∀a∈G. T(a) = F(a)
    using group0_5_L2 group_oper_assocA fix_var_val by simp
    ultimately show T = F by (rule func_eq)
qed

```

A lemma about translating sets.

```

lemma (in group0) ltrans_image: assumes A1:  $V \subseteq G$  and A2:  $x \in G$ 
  shows  $\text{LeftTranslation}(G, P, x)(V) = \{x \cdot v. v \in V\}$ 
proof -
  from assms have  $\text{LeftTranslation}(G, P, x)(V) = \{\text{LeftTranslation}(G, P, x)(v). v \in V\}$ 
  using group0_5_L1 func_imagedef by blast
  moreover from assms have  $\forall v \in V. \text{LeftTranslation}(G, P, x)(v) = x \cdot v$ 
  using group0_5_L2 by auto
  ultimately show thesis by auto
qed

```

A technical lemma about solving equations with translations.

```

lemma (in group0) ltrans_inv_in: assumes A1:  $V \subseteq G$  and A2:  $y \in G$  and
  A3:  $x \in \text{LeftTranslation}(G, P, y)(\text{GroupInv}(G, P)(V))$ 
  shows  $y \in \text{LeftTranslation}(G, P, x)(V)$ 
proof -
  have  $x \in G$ 
  proof -
    from A2 have  $\text{LeftTranslation}(G, P, y): G \rightarrow G$  using group0_5_L1 by simp
    then have  $\text{LeftTranslation}(G, P, y)(\text{GroupInv}(G, P)(V)) \subseteq G$ 
    using func1_1_L6 by simp
    with A3 show  $x \in G$  by auto
  qed
  have  $\exists v \in V. x = y \cdot v^{-1}$ 
  proof -
    have  $\text{GroupInv}(G, P): G \rightarrow G$  using groupAssum group0_2_T2
    by simp
    with assms obtain z where  $z \in \text{GroupInv}(G, P)(V)$  and  $x = y \cdot z$ 
    using func1_1_L6 ltrans_image by auto
    with A1 ' $\text{GroupInv}(G, P): G \rightarrow G$ ' show thesis using func_imagedef by
  auto
  qed
  then obtain v where  $v \in V$  and  $x = y \cdot v^{-1}$  by auto
  with A1 A2 have  $y = x \cdot v$  using inv_cancel_two by auto
  with assms ' $x \in G$ ' ' $v \in V$ ' show thesis using ltrans_image by auto
qed

```

We can look at the result of interval arithmetic operation as union of translated sets.

```

lemma (in group0) image_ltrans_union: assumes  $A \subseteq G$   $B \subseteq G$  shows
   $(P \text{ {lifted to subsets of} } G) \langle A, B \rangle = (\bigcup a \in A. \text{LeftTranslation}(G, P, a)(B))$ 
proof
  from assms have I:  $(P \text{ {lifted to subsets of} } G) \langle A, B \rangle = \{a \cdot b. \langle a, b \rangle \in A \times B\}$ 
  using group_oper_assocA lift_subsets_explained by simp
  { fix c assume  $c \in (P \text{ {lifted to subsets of} } G) \langle A, B \rangle$ 
    with I obtain a b where  $c = a \cdot b$  and  $a \in A$   $b \in B$  by auto
    hence  $c \in \{a \cdot b. b \in B\}$  by auto
    moreover from assms ' $a \in A$ ' have

```

```

      LeftTranslation(G,P,a)(B) = {a.b. b∈B} using ltrans_image by auto
      ultimately have c ∈ LeftTranslation(G,P,a)(B) by simp
      with 'a∈A' have c ∈ (⋃ a∈A. LeftTranslation(G,P,a)(B)) by auto
    } thus (P {lifted to subsets of} G)⟨A,B⟩ ⊆ (⋃ a∈A. LeftTranslation(G,P,a)(B))
      by auto
    { fix c assume c ∈ (⋃ a∈A. LeftTranslation(G,P,a)(B))
      then obtain a where a∈A and c ∈ LeftTranslation(G,P,a)(B)
        by auto
      moreover from assms 'a∈A' have LeftTranslation(G,P,a)(B) = {a.b.
b∈B}
        using ltrans_image by auto
      ultimately obtain b where b∈B and c = a.b by auto
      with I 'a∈A' have c ∈ (P {lifted to subsets of} G)⟨A,B⟩ by auto
    } thus (⋃ a∈A. LeftTranslation(G,P,a)(B)) ⊆ (P {lifted to subsets of}
G)⟨A,B⟩
      by auto
qed

```

If the neutral element belongs to a set, then an element of group belongs the translation of that set.

```

lemma (in group0) neut_trans_elem:
  assumes A1: A⊆G and A2: 1∈A
  shows g ∈ LeftTranslation(G,P,g)(A)
proof -
  from assms have g.1 ∈ LeftTranslation(G,P,g)(A)
    using ltrans_image by auto
  with A1 show thesis using group0_2_L2 by simp
qed

```

The neutral element belongs to the translation of a set by the inverse of an element that belongs to it.

```

lemma (in group0) elem_trans_neut: assumes A1: A⊆G and A2: g∈A
  shows 1 ∈ LeftTranslation(G,P,g-1)(A)
proof -
  from assms have g-1 ∈ G using inverse_in_group by auto
  with assms have g-1.g ∈ LeftTranslation(G,P,g-1)(A)
    using ltrans_image by auto
  moreover from assms have g-1.g = 1 using group0_2_L6 by auto
  ultimately show thesis by simp
qed

```

## 21.2 Odd functions

This section is about odd functions.

Odd functions are those that commute with the group inverse:  $f(a^{-1}) = (f(a))^{-1}$ .

**definition**

$$\text{IsOdd}(G, P, f) \equiv (\forall a \in G. f(\text{GroupInv}(G, P)(a)) = \text{GroupInv}(G, P)(f(a)) )$$

Let's see the definition of an odd function in a more readable notation.

```
lemma (in group0) group0_6_L1:
  shows IsOdd(G,P,p)  $\longleftrightarrow$  (  $\forall a \in G. p(a^{-1}) = (p(a))^{-1}$  )
  using IsOdd_def by simp
```

We can express the definition of an odd function in two ways.

```
lemma (in group0) group0_6_L2:
  assumes A1: p : G  $\rightarrow$  G
  shows
    ( $\forall a \in G. p(a^{-1}) = (p(a))^{-1}$ )  $\longleftrightarrow$  ( $\forall a \in G. (p(a^{-1}))^{-1} = p(a)$ )
proof
  assume  $\forall a \in G. p(a^{-1}) = (p(a))^{-1}$ 
  with A1 show  $\forall a \in G. (p(a^{-1}))^{-1} = p(a)$ 
    using apply_funtype group_inv_of_inv by simp
next assume A2:  $\forall a \in G. (p(a^{-1}))^{-1} = p(a)$ 
  { fix a assume a  $\in$  G
    with A1 A2 have
      p(a-1)  $\in$  G and ((p(a-1))-1)-1 = (p(a))-1
      using apply_funtype inverse_in_group by auto
    then have p(a-1) = (p(a))-1
      using group_inv_of_inv by simp
  } then show  $\forall a \in G. p(a^{-1}) = (p(a))^{-1}$  by simp
qed

end
```

## 22 Group\_ZF\_1b.thy

**theory** Group\_ZF\_1b **imports** Group\_ZF

**begin**

In a typical textbook a group is defined as a set  $G$  with an associative operation such that two conditions hold:

A: there is an element  $e \in G$  such that for all  $g \in G$  we have  $e \cdot g = g$  and  $g \cdot e = g$ . We call this element a "unit" or a "neutral element" of the group.

B: for every  $a \in G$  there exists a  $b \in G$  such that  $a \cdot b = e$ , where  $e$  is the element of  $G$  whose existence is guaranteed by A.

The validity of this definition is rather dubious to me, as condition A does not define any specific element  $e$  that can be referred to in condition B - it merely states that a set of such units  $e$  is not empty. Of course it does work in the end as we can prove that the set of such neutral elements has exactly one element, but still the definition by itself is not valid. You just can't reference a variable bound by a quantifier outside of the scope of that quantifier.

One way around this is to first use condition A to define the notion of a monoid, then prove the uniqueness of  $e$  and then use the condition B to define groups.

Another way is to write conditions A and B together as follows:

$$\exists e \in G (\forall g \in G e \cdot g = g \wedge g \cdot e = g) \wedge (\forall a \in G \exists b \in G a \cdot b = e).$$

This is rather ugly.

What I want to talk about is an amusing way to define groups directly without any reference to the neutral elements. Namely, we can define a group as a non-empty set  $G$  with an associative operation " $\cdot$ " such that

C: for every  $a, b \in G$  the equations  $a \cdot x = b$  and  $y \cdot a = b$  can be solved in  $G$ .

This theory file aims at proving the equivalence of this alternative definition with the usual definition of the group, as formulated in `Group_ZF.thy`. The informal proofs come from an Aug. 14, 2005 post by buli on the [matematyka.org](http://matematyka.org) forum.

### 22.1 An alternative definition of group

First we will define notation for writing about groups.

We will use the multiplicative notation for the group operation. To do this, we define a context (locale) that tells Isabelle to interpret  $a \cdot b$  as the value of function  $P$  on the pair  $\langle a, b \rangle$ .

```
locale group2 =  
  fixes P
```

```

fixes dot (infixl · 70)
defines dot_def [simp]: a · b ≡ P⟨a,b⟩

```

The next theorem states that a set  $G$  with an associative operation that satisfies condition C is a group, as defined in IsarMathLib Group\_ZF theory.

```

theorem (in group2) altgroup_is_group:
  assumes A1:  $G \neq 0$  and A2:  $P \text{ \{is associative on\} } G$ 
  and A3:  $\forall a \in G. \forall b \in G. \exists x \in G. a \cdot x = b$ 
  and A4:  $\forall a \in G. \forall b \in G. \exists y \in G. y \cdot a = b$ 
  shows IsAgroup( $G, P$ )
proof -
  from A1 obtain a where  $a \in G$  by auto
  with A3 obtain x where  $x \in G$  and  $a \cdot x = a$ 
    by auto
  from A4 ' $a \in G$ ' obtain y where  $y \in G$  and  $y \cdot a = a$ 
    by auto
  have I:  $\forall b \in G. b = b \cdot x \wedge b = y \cdot b$ 
  proof
    fix b assume  $b \in G$ 
    with A4 ' $a \in G$ ' obtain  $y_b$  where  $y_b \in G$ 
      and  $y_b \cdot a = b$  by auto
    from A3 ' $a \in G$ ' ' $b \in G$ ' obtain  $x_b$  where  $x_b \in G$ 
      and  $a \cdot x_b = b$  by auto
    from ' $a \cdot x = a$ ' ' $y \cdot a = a$ ' ' $y_b \cdot a = b$ ' ' $a \cdot x_b = b$ '
    have  $b = y_b \cdot (a \cdot x)$  and  $b = (y \cdot a) \cdot x_b$ 
      by auto
    moreover from A2 ' $a \in G$ ' ' $x \in G$ ' ' $y \in G$ ' ' $x_b \in G$ ' ' $y_b \in G$ ' have
       $(y \cdot a) \cdot x_b = y \cdot (a \cdot x_b)$   $y_b \cdot (a \cdot x) = (y_b \cdot a) \cdot x$ 
      using IsAssociative_def by auto
    moreover from ' $y_b \cdot a = b$ ' ' $a \cdot x_b = b$ ' have
       $(y_b \cdot a) \cdot x = b \cdot x$   $y \cdot (a \cdot x_b) = y \cdot b$ 
      by auto
    ultimately show  $b = b \cdot x \wedge b = y \cdot b$  by simp
  qed
  moreover have  $x = y$ 
  proof -
    from ' $x \in G$ ' I have  $x = y \cdot x$  by simp
    also from ' $y \in G$ ' I have  $y \cdot x = y$  by simp
    finally show  $x = y$  by simp
  qed
  ultimately have  $\forall b \in G. b \cdot x = b \wedge x \cdot b = b$  by simp
  with A2 ' $x \in G$ ' have IsAmonoid( $G, P$ ) using IsAmonoid_def by auto
  with A3 show IsAgroup( $G, P$ )
    using monoid0_def monoid0.unit_is_neutral IsAgroup_def
    by simp
qed

```

The converse of altgroup\_is\_group: in every (classically defined) group condition C holds. In informal mathematics we can say "Obviously condition C

holds in any group.” In formalized mathematics the word ”obviously” is not in the language. The next theorem is proven in the context called `group0` defined in the theory `Group_ZF.thy`. Similarly to the `group2` that context defines  $a \cdot b$  as  $P\langle a, b \rangle$ . It also defines notation related to the group inverse and adds an assumption that the pair  $(G, P)$  is a group to all its theorems. This is why in the next theorem we don’t explicitly assume that  $(G, P)$  is a group - this assumption is implicit in the context.

```

theorem (in group0) group_is_altgroup: shows
   $\forall a \in G. \forall b \in G. \exists x \in G. a \cdot x = b$  and  $\forall a \in G. \forall b \in G. \exists y \in G. y \cdot a = b$ 
proof -
  { fix a b assume a ∈ G b ∈ G
    let x = a-1 · b
    let y = b · a-1
    from ‘a ∈ G’ ‘b ∈ G’ have
      x ∈ G y ∈ G and a · x = b y · a = b
      using inverse_in_group group_op_closed inv_cancel_two
      by auto
    hence  $\exists x \in G. a \cdot x = b$  and  $\exists y \in G. y \cdot a = b$  by auto
  } thus
     $\forall a \in G. \forall b \in G. \exists x \in G. a \cdot x = b$  and
     $\forall a \in G. \forall b \in G. \exists y \in G. y \cdot a = b$ 
    by auto
qed

end

```

## 23 AbelianGroup\_ZF.thy

**theory** AbelianGroup\_ZF **imports** Group\_ZF

**begin**

A group is called “abelian“ if its operation is commutative, i.e.  $P\langle a, b \rangle = P\langle b, a \rangle$  for all group elements  $a, b$ , where  $P$  is the group operation. It is customary to use the additive notation for abelian groups, so this condition is typically written as  $a + b = b + a$ . We will be using multiplicative notation though (in which the commutativity condition of the operation is written as  $a \cdot b = b \cdot a$ ), just to avoid the hassle of changing the notation we used for general groups.

### 23.1 Rearrangement formulae

This section is not interesting and should not be read. Here we will prove formulas in which right hand side uses the same factors as the left hand side, just in different order. These facts are obvious in informal math sense, but Isabelle prover is not able to derive them automatically, so we have to prove them by hand.

Proving the facts about associative and commutative operations is quite tedious in formalized mathematics. To a human the thing is simple: we can arrange the elements in any order and put parentheses wherever we want, it is all the same. However, formalizing this statement would be rather difficult (I think). The next lemma attempts a quasi-algorithmic approach to this type of problem. To prove that two expressions are equal, we first strip one from parentheses, then rearrange the elements in proper order, then put the parentheses where we want them to be. The algorithm for rearrangement is easy to describe: we keep putting the first element (from the right) that is in the wrong place at the left-most position until we get the proper arrangement. As far removing parentheses is concerned Isabelle does its job automatically.

```
lemma (in group0) group0_4_L2:
  assumes A1:P {is commutative on} G
  and A2:a∈G b∈G c∈G d∈G E∈G F∈G
  shows (a·b)·(c·d)·(E·F) = (a·(d·F))·(b·(c·E))
proof -
  from A2 have (a·b)·(c·d)·(E·F) = a·b·c·d·E·F
    using group_op_closed group_oper_assoc
    by simp
  also have a·b·c·d·E·F = a·d·F·b·c·E
  proof -
    from A1 A2 have a·b·c·d·E·F = F·(a·b·c·d·E)
      using IsCommutative_def group_op_closed
```



```

    by simp
  also from A2 have  $F \cdot (a \cdot b \cdot c \cdot d \cdot E) = F \cdot a \cdot b \cdot c \cdot d \cdot E$ 
    using group_op_closed group_oper_assoc
    by simp
  also from A1 A2 have  $F \cdot a \cdot b \cdot c \cdot d \cdot E = d \cdot (F \cdot a \cdot b \cdot c) \cdot E$ 
    using IsCommutative_def group_op_closed
    by simp
  also from A2 have  $d \cdot (F \cdot a \cdot b \cdot c) \cdot E = d \cdot F \cdot a \cdot b \cdot c \cdot E$ 
    using group_op_closed group_oper_assoc
    by simp
  also from A1 A2 have  $d \cdot F \cdot a \cdot b \cdot c \cdot E = a \cdot (d \cdot F) \cdot b \cdot c \cdot E$ 
    using IsCommutative_def group_op_closed
    by simp
  also from A2 have  $a \cdot (d \cdot F) \cdot b \cdot c \cdot E = a \cdot d \cdot F \cdot b \cdot c \cdot E$ 
    using group_op_closed group_oper_assoc
    by simp
  finally show thesis by simp
qed
also from A2 have  $a \cdot d \cdot F \cdot b \cdot c \cdot E = (a \cdot (d \cdot F)) \cdot (b \cdot (c \cdot E))$ 
  using group_op_closed group_oper_assoc
  by simp
  finally show thesis by simp
qed

```

Another useful rearrangement.

```

lemma (in group0) group0_4_L3:
  assumes A1: P {is commutative on} G
  and A2:  $a \in G \quad b \in G$  and A3:  $c \in G \quad d \in G \quad E \in G \quad F \in G$ 
  shows  $a \cdot b \cdot ((c \cdot d)^{-1} \cdot (E \cdot F)^{-1}) = (a \cdot (E \cdot c)^{-1}) \cdot (b \cdot (F \cdot d)^{-1})$ 
proof -
  from A3 have T1:
     $c^{-1} \in G \quad d^{-1} \in G \quad E^{-1} \in G \quad F^{-1} \in G \quad (c \cdot d)^{-1} \in G \quad (E \cdot F)^{-1} \in G$ 
    using inverse_in_group group_op_closed
    by auto
  from A2 T1 have
     $a \cdot b \cdot ((c \cdot d)^{-1} \cdot (E \cdot F)^{-1}) = a \cdot b \cdot (c \cdot d)^{-1} \cdot (E \cdot F)^{-1}$ 
    using group_op_closed group_oper_assoc
    by simp
  also from A2 A3 have
     $a \cdot b \cdot (c \cdot d)^{-1} \cdot (E \cdot F)^{-1} = (a \cdot b) \cdot (d^{-1} \cdot c^{-1}) \cdot (F^{-1} \cdot E^{-1})$ 
    using group_inv_of_two by simp
  also from A1 A2 T1 have
     $(a \cdot b) \cdot (d^{-1} \cdot c^{-1}) \cdot (F^{-1} \cdot E^{-1}) = (a \cdot (c^{-1} \cdot E^{-1})) \cdot (b \cdot (d^{-1} \cdot F^{-1}))$ 
    using group0_4_L2 by simp
  also from A2 A3 have
     $(a \cdot (c^{-1} \cdot E^{-1})) \cdot (b \cdot (d^{-1} \cdot F^{-1})) = (a \cdot (E \cdot c)^{-1}) \cdot (b \cdot (F \cdot d)^{-1})$ 
    using group_inv_of_two by simp
  finally show thesis by simp
qed

```

Some useful rearrangements for two elements of a group.

```

lemma (in group0) group0_4_L4:
  assumes A1:P {is commutative on} G
  and A2: a∈G b∈G
  shows
     $b^{-1} \cdot a^{-1} = a^{-1} \cdot b^{-1}$ 
     $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$ 
     $(a \cdot b^{-1})^{-1} = a^{-1} \cdot b$ 
  proof -
    from A2 have T1:  $b^{-1} \in G$   $a^{-1} \in G$  using inverse_in_group by auto
    with A1 show  $b^{-1} \cdot a^{-1} = a^{-1} \cdot b^{-1}$  using IsCommutative_def by simp
    with A2 show  $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$  using group_inv_of_two by simp
    from A2 T1 have  $(a \cdot b^{-1})^{-1} = (b^{-1})^{-1} \cdot a^{-1}$  using group_inv_of_two by simp
    with A1 A2 T1 show  $(a \cdot b^{-1})^{-1} = a^{-1} \cdot b$ 
      using group_inv_of_inv IsCommutative_def by simp
  qed

```

Another bunch of useful rearrangements with three elements.

```

lemma (in group0) group0_4_L4A:
  assumes A1: P {is commutative on} G
  and A2: a∈G b∈G c∈G
  shows
     $a \cdot b \cdot c = c \cdot a \cdot b$ 
     $a^{-1} \cdot (b^{-1} \cdot c^{-1})^{-1} = (a \cdot (b \cdot c)^{-1})^{-1}$ 
     $a \cdot (b \cdot c)^{-1} = a \cdot b^{-1} \cdot c^{-1}$ 
     $a \cdot (b \cdot c^{-1})^{-1} = a \cdot b^{-1} \cdot c$ 
     $a \cdot b^{-1} \cdot c^{-1} = a \cdot c^{-1} \cdot b^{-1}$ 
  proof -
    from A1 A2 have  $a \cdot b \cdot c = c \cdot (a \cdot b)$ 
      using IsCommutative_def group_op_closed
      by simp
    with A2 show  $a \cdot b \cdot c = c \cdot a \cdot b$  using
      group_op_closed group_oper_assoc
      by simp
    from A2 have T:
       $b^{-1} \in G$   $c^{-1} \in G$   $b^{-1} \cdot c^{-1} \in G$   $a \cdot b \in G$ 
      using inverse_in_group group_op_closed
      by auto
    with A1 A2 show  $a^{-1} \cdot (b^{-1} \cdot c^{-1})^{-1} = (a \cdot (b \cdot c)^{-1})^{-1}$ 
      using group_inv_of_two IsCommutative_def
      by simp
    from A1 A2 T have  $a \cdot (b \cdot c)^{-1} = a \cdot (b^{-1} \cdot c^{-1})$ 
      using group_inv_of_two IsCommutative_def by simp
    with A2 T show  $a \cdot (b \cdot c)^{-1} = a \cdot b^{-1} \cdot c^{-1}$ 
      using group_oper_assoc by simp
    from A1 A2 T have  $a \cdot (b \cdot c^{-1})^{-1} = a \cdot (b^{-1} \cdot (c^{-1})^{-1})$ 
      using group_inv_of_two IsCommutative_def by simp
    with A2 T show  $a \cdot (b \cdot c^{-1})^{-1} = a \cdot b^{-1} \cdot c$ 
      using group_oper_assoc group_inv_of_inv by simp
  qed

```

```

from A1 A2 T have a·b-1·c-1 = a·(c-1·b-1)
  using group_oper_assoc IsCommutative_def by simp
with A2 T show a·b-1·c-1 = a·c-1·b-1
  using group_oper_assoc by simp
qed

```

Another useful rearrangement.

```

lemma (in group0) group0_4_L4B:
  assumes P {is commutative on} G
  and a∈G b∈G c∈G
  shows a·b-1·(b·c-1) = a·c-1
  using assms inverse_in_group group_op_closed
    group0_4_L4 group_oper_assoc inv_cancel_two by simp

```

A couple of permutations of order for three elements.

```

lemma (in group0) group0_4_L4C:
  assumes A1: P {is commutative on} G
  and A2: a∈G b∈G c∈G
  shows
    a·b·c = c·a·b
    a·b·c = a·(c·b)
    a·b·c = c·(a·b)
    a·b·c = c·b·a
proof -
  from A1 A2 show I: a·b·c = c·a·b
    using group0_4_L4A by simp
  also from A1 A2 have c·a·b = a·c·b
    using IsCommutative_def by simp
  also from A2 have a·c·b = a·(c·b)
    using group_oper_assoc by simp
  finally show a·b·c = a·(c·b) by simp
  from A2 I show a·b·c = c·(a·b)
    using group_oper_assoc by simp
  also from A1 A2 have c·(a·b) = c·(b·a)
    using IsCommutative_def by simp
  also from A2 have c·(b·a) = c·b·a
    using group_oper_assoc by simp
  finally show a·b·c = c·b·a by simp
qed

```

Some rearrangement with three elements and inverse.

```

lemma (in group0) group0_4_L4D:
  assumes A1: P {is commutative on} G
  and A2: a∈G b∈G c∈G
  shows
    a-1·b-1·c = c·a-1·b-1
    b-1·a-1·c = c·a-1·b-1
    (a-1·b·c)-1 = a·b-1·c-1
proof -

```

```

from A2 have T:
  a-1 ∈ G  b-1 ∈ G  c-1 ∈ G
  using inverse_in_group by auto
with A1 A2 show
  a-1.b-1.c = c.a-1.b-1
  b-1.a-1.c = c.a-1.b-1
  using group0_4_L4A by auto
from A1 A2 T show (a-1.b.c)-1 = a.b-1.c-1
  using group_inv_of_three group_inv_of_inv group0_4_L4C
  by simp
qed

```

Another rearrangement lemma with three elements and equation.

```

lemma (in group0) group0_4_L5: assumes A1:P {is commutative on} G
  and A2: a ∈ G  b ∈ G  c ∈ G
  and A3: c = a.b-1
  shows a = b.c
proof -
  from A2 A3 have c.(b-1)-1 = a
    using inverse_in_group group0_2_L18
    by simp
  with A1 A2 show thesis using
    group_inv_of_inv IsCommutative_def by simp
qed

```

In abelian groups we can cancel an element with its inverse even if separated by another element.

```

lemma (in group0) group0_4_L6A: assumes A1: P {is commutative on} G
  and A2: a ∈ G  b ∈ G
  shows
    a.b.a-1 = b
    a-1.b.a = b
    a-1.(b.a) = b
    a.(b.a-1) = b
proof -
  from A1 A2 have
    a.b.a-1 = a-1.a.b
    using inverse_in_group group0_4_L4A by blast
  also from A2 have ... = b
    using group0_2_L6 group0_2_L2 by simp
  finally show a.b.a-1 = b by simp
  from A1 A2 have
    a-1.b.a = a.a-1.b
    using inverse_in_group group0_4_L4A by blast
  also from A2 have ... = b
    using group0_2_L6 group0_2_L2 by simp
  finally show a-1.b.a = b by simp
  moreover from A2 have a-1.b.a = a-1.(b.a)
    using inverse_in_group group_oper_assoc by simp

```

```

ultimately show  $a^{-1} \cdot (b \cdot a) = b$  by simp
from A1 A2 show  $a \cdot (b \cdot a^{-1}) = b$ 
  using inverse_in_group IsCommutative_def inv_cancel_two
  by simp
qed

```

Another lemma about cancelling with two elements.

```

lemma (in group0) group0_4_L6AA:
  assumes A1: P {is commutative on} G and A2:  $a \in G \quad b \in G$ 
  shows  $a \cdot b^{-1} \cdot a^{-1} = b^{-1}$ 
  using assms inverse_in_group group0_4_L6A
  by auto

```

Another lemma about cancelling with two elements.

```

lemma (in group0) group0_4_L6AB:
  assumes A1: P {is commutative on} G and A2:  $a \in G \quad b \in G$ 
  shows
     $a \cdot (a \cdot b)^{-1} = b^{-1}$ 
     $a \cdot (b \cdot a^{-1}) = b$ 
proof -
  from A2 have  $a \cdot (a \cdot b)^{-1} = a \cdot (b^{-1} \cdot a^{-1})$ 
    using group_inv_of_two by simp
  also from A2 have  $\dots = a \cdot b^{-1} \cdot a^{-1}$ 
    using inverse_in_group group_oper_assoc by simp
  also from A1 A2 have  $\dots = b^{-1}$ 
    using group0_4_L6AA by simp
  finally show  $a \cdot (a \cdot b)^{-1} = b^{-1}$  by simp
  from A1 A2 have  $a \cdot (b \cdot a^{-1}) = a \cdot (a^{-1} \cdot b)$ 
    using inverse_in_group IsCommutative_def by simp
  also from A2 have  $\dots = b$ 
    using inverse_in_group group_oper_assoc group0_2_L6 group0_2_L2
    by simp
  finally show  $a \cdot (b \cdot a^{-1}) = b$  by simp
qed

```

Another lemma about cancelling with two elements.

```

lemma (in group0) group0_4_L6AC:
  assumes P {is commutative on} G and  $a \in G \quad b \in G$ 
  shows  $a \cdot (a \cdot b^{-1})^{-1} = b$ 
  using assms inverse_in_group group0_4_L6AB group_inv_of_inv
  by simp

```

In abelian groups we can cancel an element with its inverse even if separated by two other elements.

```

lemma (in group0) group0_4_L6B: assumes A1: P {is commutative on} G
  and A2:  $a \in G \quad b \in G \quad c \in G$ 
  shows
     $a \cdot b \cdot c \cdot a^{-1} = b \cdot c$ 

```

```

a⁻¹·b·c·a = b·c
proof -
  from A2 have
    a·b·c·a⁻¹ = a·(b·c)·a⁻¹
    a⁻¹·b·c·a = a⁻¹·(b·c)·a
  using group_op_closed group_oper_assoc inverse_in_group
  by auto
with A1 A2 show
  a·b·c·a⁻¹ = b·c
  a⁻¹·b·c·a = b·c
  using group_op_closed group0_4_L6A
  by auto
qed

```

In abelian groups we can cancel an element with its inverse even if separated by three other elements.

```

lemma (in group0) group0_4_L6C: assumes A1: P {is commutative on} G
  and A2: a∈G b∈G c∈G d∈G
  shows a·b·c·d·a⁻¹ = b·c·d
proof -
  from A2 have a·b·c·d·a⁻¹ = a·(b·c·d)·a⁻¹
    using group_op_closed group_oper_assoc
    by simp
  with A1 A2 show thesis
    using group_op_closed group0_4_L6A
    by simp
qed

```

Another couple of useful rearrangements of three elements and cancelling.

```

lemma (in group0) group0_4_L6D:
  assumes A1: P {is commutative on} G
  and A2: a∈G b∈G c∈G
  shows
    a·b⁻¹·(a·c⁻¹)⁻¹ = c·b⁻¹
    (a·c)⁻¹·(b·c) = a⁻¹·b
    a·(b·(c·a⁻¹·b⁻¹)) = c
    a·b·c⁻¹·(c·a⁻¹) = b
proof -
  from A2 have T:
    a⁻¹ ∈ G b⁻¹ ∈ G c⁻¹ ∈ G
    a·b ∈ G a·b⁻¹ ∈ G c⁻¹·a⁻¹ ∈ G c·a⁻¹ ∈ G
  using inverse_in_group group_op_closed by auto
with A1 A2 show a·b⁻¹·(a·c⁻¹)⁻¹ = c·b⁻¹
  using group0_2_L12 group_oper_assoc group0_4_L6B
  IsCommutative_def by simp
from A2 T have (a·c)⁻¹·(b·c) = c⁻¹·a⁻¹·b·c
  using group_inv_of_two group_oper_assoc by simp
also from A1 A2 T have ... = a⁻¹·b
  using group0_4_L6B by simp

```

```

finally show  $(a \cdot c)^{-1} \cdot (b \cdot c) = a^{-1} \cdot b$ 
  by simp
from A1 A2 T show  $a \cdot (b \cdot (c \cdot a^{-1} \cdot b^{-1})) = c$ 
  using group_oper_assoc group0_4_L6B group0_4_L6A
  by simp
from T have  $a \cdot b \cdot c^{-1} \cdot (c \cdot a^{-1}) = a \cdot b \cdot (c^{-1} \cdot (c \cdot a^{-1}))$ 
  using group_oper_assoc by simp
also from A1 A2 T have  $\dots = b$ 
  using group_oper_assoc group0_2_L6 group0_2_L2 group0_4_L6A
  by simp
finally show  $a \cdot b \cdot c^{-1} \cdot (c \cdot a^{-1}) = b$  by simp
qed

```

Another useful rearrangement of three elements and cancelling.

```

lemma (in group0) group0_4_L6E:
  assumes A1: P {is commutative on} G
  and A2:  $a \in G \quad b \in G \quad c \in G$ 
  shows
     $a \cdot b \cdot (a \cdot c)^{-1} = b \cdot c^{-1}$ 
proof -
  from A2 have T:  $b^{-1} \in G \quad c^{-1} \in G$ 
    using inverse_in_group by auto
  with A1 A2 have
     $a \cdot (b^{-1})^{-1} \cdot (a \cdot (c^{-1})^{-1})^{-1} = c^{-1} \cdot (b^{-1})^{-1}$ 
    using group0_4_L6D by simp
  with A1 A2 T show  $a \cdot b \cdot (a \cdot c)^{-1} = b \cdot c^{-1}$ 
    using group_inv_of_inv IsCommutative_def
    by simp
qed

```

A rearrangement with two elements and cancelling, special case of group0\_4\_L6D when  $c = b^{-1}$ .

```

lemma (in group0) group0_4_L6F:
  assumes A1: P {is commutative on} G
  and A2:  $a \in G \quad b \in G$ 
  shows  $a \cdot b^{-1} \cdot (a \cdot b)^{-1} = b^{-1} \cdot b^{-1}$ 
proof -
  from A2 have  $b^{-1} \in G$ 
    using inverse_in_group by simp
  with A1 A2 have  $a \cdot b^{-1} \cdot (a \cdot (b^{-1})^{-1})^{-1} = b^{-1} \cdot b^{-1}$ 
    using group0_4_L6D by simp
  with A2 show  $a \cdot b^{-1} \cdot (a \cdot b)^{-1} = b^{-1} \cdot b^{-1}$ 
    using group_inv_of_inv by simp
qed

```

Some other rearrangements with four elements. The algorithm for proof as in group0\_4\_L2 works very well here.

```

lemma (in group0) rearr_ab_gr_4_elemA:

```

```

assumes A1: P {is commutative on} G
and A2: a∈G b∈G c∈G d∈G
shows
a·b·c·d = a·d·b·c
a·b·c·d = a·c·(b·d)
proof -
  from A1 A2 have a·b·c·d = d·(a·b·c)
    using IsCommutative_def group_op_closed
    by simp
  also from A2 have ... = d·a·b·c
    using group_op_closed group_oper_assoc
    by simp
  also from A1 A2 have ... = a·d·b·c
    using IsCommutative_def group_op_closed
    by simp
  finally show a·b·c·d = a·d·b·c
    by simp
  from A1 A2 have a·b·c·d = c·(a·b)·d
    using IsCommutative_def group_op_closed
    by simp
  also from A2 have ... = c·a·b·d
    using group_op_closed group_oper_assoc
    by simp
  also from A1 A2 have ... = a·c·b·d
    using IsCommutative_def group_op_closed
    by simp
  also from A2 have ... = a·c·(b·d)
    using group_op_closed group_oper_assoc
    by simp
  finally show a·b·c·d = a·c·(b·d)
    by simp
qed

```

Some rearrangements with four elements and inverse that are applications of rearr\_ab\_gr\_4\_elem

```

lemma (in group0) rearr_ab_gr_4_elemB:
  assumes A1: P {is commutative on} G
  and A2: a∈G b∈G c∈G d∈G
  shows
    a·b-1·c-1·d-1 = a·d-1·b-1·c-1
    a·b·c·d-1 = a·d-1·b·c
    a·b·c-1·d-1 = a·c-1·(b·d-1)
  proof -
    from A2 have T: b-1 ∈ G c-1 ∈ G d-1 ∈ G
      using inverse_in_group by auto
    with A1 A2 show
      a·b-1·c-1·d-1 = a·d-1·b-1·c-1
      a·b·c·d-1 = a·d-1·b·c
      a·b·c-1·d-1 = a·c-1·(b·d-1)

```



```

    using rearr_ab_gr_4_elemA by auto
qed

```

Some rearrangement lemmas with four elements.

```

lemma (in group0) group0_4_L7:
  assumes A1: P {is commutative on} G
  and A2: a∈G b∈G c∈G d∈G
  shows
    a·b·c·d-1 = a·d-1·b·c
    a·d·(b·d·(c·d))-1 = a·(b·c)-1·d-1
    a·(b·c)·d = a·b·d·c
  proof -
    from A2 have T:
      b·c ∈ G d-1 ∈ G b-1∈G c-1∈G
      d-1·b ∈ G c-1·d ∈ G (b·c)-1 ∈ G
      b·d ∈ G b·d·c ∈ G (b·d·c)-1 ∈ G
      a·d ∈ G b·c ∈ G
    using group_op_closed inverse_in_group
    by auto
    with A1 A2 have a·b·c·d-1 = a·(d-1·b·c)
    using group_oper_assoc group0_4_L4A by simp
    also from A2 T have a·(d-1·b·c) = a·d-1·b·c
    using group_oper_assoc by simp
    finally show a·b·c·d-1 = a·d-1·b·c by simp
    from A2 T have a·d·(b·d·(c·d))-1 = a·d·(d-1·(b·d·c)-1)
    using group_oper_assoc group_inv_of_two by simp
    also from A2 T have ... = a·(b·d·c)-1
    using group_oper_assoc inv_cancel_two by simp
    also from A1 A2 have ... = a·(d·(b·c))-1
    using IsCommutative_def group_oper_assoc by simp
    also from A2 T have ... = a·((b·c)-1·d-1)
    using group_inv_of_two by simp
    also from A2 T have ... = a·(b·c)-1·d-1
    using group_oper_assoc by simp
    finally show a·d·(b·d·(c·d))-1 = a·(b·c)-1·d-1
    by simp
    from A2 have a·(b·c)·d = a·(b·(c·d))
    using group_op_closed group_oper_assoc by simp
    also from A1 A2 have ... = a·(b·(d·c))
    using IsCommutative_def group_op_closed by simp
    also from A2 have ... = a·b·d·c
    using group_op_closed group_oper_assoc by simp
    finally show a·(b·c)·d = a·b·d·c by simp
  qed

```

Some other rearrangements with four elements.

```

lemma (in group0) group0_4_L8:
  assumes A1: P {is commutative on} G
  and A2: a∈G b∈G c∈G d∈G

```

shows

$$a \cdot (b \cdot c)^{-1} = (a \cdot d^{-1} \cdot c^{-1}) \cdot (d \cdot b^{-1})$$

$$a \cdot b \cdot (c \cdot d) = c \cdot a \cdot (b \cdot d)$$

$$a \cdot b \cdot (c \cdot d) = a \cdot c \cdot (b \cdot d)$$

$$a \cdot (b \cdot c^{-1}) \cdot d = a \cdot b \cdot d \cdot c^{-1}$$

$$(a \cdot b) \cdot (c \cdot d)^{-1} \cdot (b \cdot d^{-1})^{-1} = a \cdot c^{-1}$$

proof -

from A2 have T:

$$b \cdot c \in G \quad a \cdot b \in G \quad d^{-1} \in G \quad b^{-1} \in G \quad c^{-1} \in G$$

$$d^{-1} \cdot b \in G \quad c^{-1} \cdot d \in G \quad (b \cdot c)^{-1} \in G$$

$$a \cdot b \in G \quad (c \cdot d)^{-1} \in G \quad (b \cdot d^{-1})^{-1} \in G \quad d \cdot b^{-1} \in G$$

using group\_op\_closed inverse\_in\_group

by auto

from A2 have  $a \cdot (b \cdot c)^{-1} = a \cdot c^{-1} \cdot b^{-1}$  using group0\_2\_L14A by blast

moreover from A2 have  $a \cdot c^{-1} = (a \cdot d^{-1}) \cdot (d \cdot c^{-1})$  using group0\_2\_L14A

by blast

ultimately have  $a \cdot (b \cdot c)^{-1} = (a \cdot d^{-1}) \cdot (d \cdot c^{-1}) \cdot b^{-1}$  by simp

with A1 A2 T have  $a \cdot (b \cdot c)^{-1} = a \cdot d^{-1} \cdot (c^{-1} \cdot d) \cdot b^{-1}$

using IsCommutative\_def by simp

with A2 T show  $a \cdot (b \cdot c)^{-1} = (a \cdot d^{-1} \cdot c^{-1}) \cdot (d \cdot b^{-1})$

using group\_op\_closed group\_oper\_assoc by simp

from A2 T have  $a \cdot b \cdot (c \cdot d) = a \cdot b \cdot c \cdot d$

using group\_oper\_assoc by simp

also have  $a \cdot b \cdot c \cdot d = c \cdot a \cdot b \cdot d$

proof -

from A1 A2 have  $a \cdot b \cdot c \cdot d = c \cdot (a \cdot b) \cdot d$

using IsCommutative\_def group\_op\_closed

by simp

also from A2 have  $\dots = c \cdot a \cdot b \cdot d$

using group\_op\_closed group\_oper\_assoc

by simp

finally show thesis by simp

qed

also from A2 have  $c \cdot a \cdot b \cdot d = c \cdot a \cdot (b \cdot d)$

using group\_op\_closed group\_oper\_assoc

by simp

finally show  $a \cdot b \cdot (c \cdot d) = c \cdot a \cdot (b \cdot d)$  by simp

with A1 A2 show  $a \cdot b \cdot (c \cdot d) = a \cdot c \cdot (b \cdot d)$

using IsCommutative\_def by simp

from A1 A2 T show  $a \cdot (b \cdot c^{-1}) \cdot d = a \cdot b \cdot d \cdot c^{-1}$

using group0\_4\_L7 by simp

from T have  $(a \cdot b) \cdot (c \cdot d)^{-1} \cdot (b \cdot d^{-1})^{-1} = (a \cdot b) \cdot ((c \cdot d)^{-1} \cdot (b \cdot d^{-1})^{-1})$

using group\_oper\_assoc by simp

also from A1 A2 T have  $\dots = (a \cdot b) \cdot (c^{-1} \cdot d^{-1} \cdot (d \cdot b^{-1}))$

using group\_inv\_of\_two group0\_2\_L12 IsCommutative\_def

by simp

also from T have  $\dots = (a \cdot b) \cdot (c^{-1} \cdot (d^{-1} \cdot (d \cdot b^{-1})))$

using group\_oper\_assoc by simp

also from A1 A2 T have  $\dots = a \cdot c^{-1}$

```

    using group_oper_assoc group0_2_L6 group0_2_L2 IsCommutative_def
    inv_cancel_two by simp
    finally show (a·b)·(c·d)-1·(b·d-1)-1 = a·c-1
    by simp
qed

```

Some other rearrangements with four elements.

```

lemma (in group0) group0_4_L8A:
  assumes A1: P {is commutative on} G
  and A2: a∈G b∈G c∈G d∈G
  shows
    a·b-1·(c·d-1) = a·c·(b-1·d-1)
    a·b-1·(c·d-1) = a·c·b-1·d-1
proof -
  from A2 have
    T: a∈G b-1 ∈ G c∈G d-1 ∈ G
    using inverse_in_group by auto
  with A1 show a·b-1·(c·d-1) = a·c·(b-1·d-1)
    by (rule group0_4_L8)
  with A2 T show a·b-1·(c·d-1) = a·c·b-1·d-1
    using group_op_closed group_oper_assoc
    by simp
qed

```

Some rearrangements with an equation.

```

lemma (in group0) group0_4_L9:
  assumes A1: P {is commutative on} G
  and A2: a∈G b∈G c∈G d∈G
  and A3: a = b·c-1·d-1
  shows
    d = b·a-1·c-1
    d = a-1·b·c-1
    b = a·d·c
proof -
  from A2 have T:
    a-1 ∈ G c-1 ∈ G d-1 ∈ G b·c-1 ∈ G
    using group_op_closed inverse_in_group
    by auto
  with A2 A3 have a·(d-1)-1 = b·c-1
    using group0_2_L18 by simp
  with A2 have b·c-1 = a·d
    using group_inv_of_inv by simp
  with A2 T have I: a-1·(b·c-1) = d
    using group0_2_L18 by simp
  with A1 A2 T show
    d = b·a-1·c-1
    d = a-1·b·c-1
    using group_oper_assoc IsCommutative_def by auto
  from A3 have a·d·c = (b·c-1·d-1)·d·c by simp

```

```

also from A2 T have ... = b·c-1·(d-1·d)·c
  using group_oper_assoc by simp
also from A2 T have ... = b·c-1·c
  using group0_2_L6 group0_2_L2 by simp
also from A2 T have ... = b·(c-1·c)
  using group_oper_assoc by simp
also from A2 have ... = b
  using group0_2_L6 group0_2_L2 by simp
finally have a·d·c = b by simp
thus b = a·d·c by simp
qed

end

```

## 24 Group\_ZF\_2.thy

```
theory Group_ZF_2 imports AbelianGroup_ZF func_ZF EquivClass1
```

```
begin
```

This theory continues Group\_ZF.thy and considers lifting the group structure to function spaces and projecting the group structure to quotient spaces, in particular the quotient group.

### 24.1 Lifting groups to function spaces

If we have a monoid (group)  $G$  than we get a monoid (group) structure on a space of functions valued in  $G$  by defining  $(f \cdot g)(x) := f(x) \cdot g(x)$ . We call this process "lifting the monoid (group) to function space". This section formalizes this lifting.

The lifted operation is an operation on the function space.

```
lemma (in monoid0) Group_ZF_2_1_L0A:
  assumes A1: F = f {lifted to function space over} X
  shows F : (X→G)×(X→G)→(X→G)
proof -
  from monoidAsssum have f : G×G→G
    using IsAmonoid_def IsAssociative_def by simp
  with A1 show thesis
    using func_ZF_1_L3 group0_1_L3B by auto
qed
```

The result of the lifted operation is in the function space.

```
lemma (in monoid0) Group_ZF_2_1_L0:
  assumes A1:F = f {lifted to function space over} X
  and A2:s:X→G r:X→G
  shows F⟨ s,r⟩ : X→G
proof -
  from A1 have F : (X→G)×(X→G)→(X→G)
    using Group_ZF_2_1_L0A
    by simp
  with A2 show thesis using apply_funtype
    by simp
qed
```

The lifted monoid operation has a neutral element, namely the constant function with the neutral element as the value.

```
lemma (in monoid0) Group_ZF_2_1_L1:
  assumes A1: F = f {lifted to function space over} X
  and A2: E = ConstantFunction(X,TheNeutralElement(G,f))
  shows E : X→G ∧ (∀s∈X→G. F⟨ E,s⟩ = s ∧ F⟨ s,E⟩ = s)
proof
```

```

from A2 show T1:E : X→G
  using unit_is_neutral func1_3_L1 by simp
show  $\forall s \in X \rightarrow G. F\langle E, s \rangle = s \wedge F\langle s, E \rangle = s$ 
proof
  fix s assume A3:s:X→G
  from monoidAsssum have T2:f : G×G→G
    using IsAmonoid_def IsAssociative_def by simp
  from A3 A1 T1 have
     $F\langle E, s \rangle : X \rightarrow G$   $F\langle s, E \rangle : X \rightarrow G$   $s : X \rightarrow G$ 
    using Group_ZF_2_1_L0 by auto
  moreover from T2 A1 T1 A2 A3 have
     $\forall x \in X. (F\langle E, s \rangle)(x) = s(x)$ 
     $\forall x \in X. (F\langle s, E \rangle)(x) = s(x)$ 
    using func_ZF_1_L4 group0_1_L3B func1_3_L2
  apply_type unit_is_neutral by auto
  ultimately show
     $F\langle E, s \rangle = s \wedge F\langle s, E \rangle = s$ 
    using fun_extension_iff by auto
qed
qed

```

Monoids can be lifted to a function space.

```

lemma (in monoid0) Group_ZF_2_1_T1:
  assumes A1: F = f {lifted to function space over} X
  shows IsAmonoid(X→G,F)
proof -
  from monoidAsssum A1 have
    F {is associative on} (X→G)
    using IsAmonoid_def func_ZF_2_L4 group0_1_L3B
    by auto
  moreover from A1 have
     $\exists E \in X \rightarrow G. \forall s \in X \rightarrow G. F\langle E, s \rangle = s \wedge F\langle s, E \rangle = s$ 
    using Group_ZF_2_1_L1 by blast
  ultimately show thesis using IsAmonoid_def
    by simp
qed

```

The constant function with the neutral element as the value is the neutral element of the lifted monoid.

```

lemma Group_ZF_2_1_L2:
  assumes A1: IsAmonoid(G,f)
  and A2: F = f {lifted to function space over} X
  and A3: E = ConstantFunction(X,TheNeutralElement(G,f))
  shows E = TheNeutralElement(X→G,F)
proof -
  from A1 A2 have
    T1:monoid0(G,f) and T2:monoid0(X→G,F)
    using monoid0_def monoid0.Group_ZF_2_1_T1
    by auto

```

```

from T1 A2 A3 have
  E : X→G ∧ (∀ s∈X→G. F⟨ E,s⟩ = s ∧ F⟨ s,E⟩ = s)
  using monoid0.Group_ZF_2_1_L1 by simp
with T2 show thesis
  using monoid0.group0_1_L4 by auto
qed

```

The lifted operation acts on the functions in a natural way defined by the monoid operation.

```

lemma (in monoid0) lifted_val:
  assumes F = f {lifted to function space over} X
  and s:X→G r:X→G
  and x∈X
  shows (F⟨s,r⟩)(x) = s(x) ⊕ r(x)
  using monoidAsssum assms IsAmonoid_def IsAssociative_def
  group0_1_L3B func_ZF_1_L4
  by auto

```

The lifted operation acts on the functions in a natural way defined by the group operation. This is the same as `lifted_val`, but in the `group0` context.

```

lemma (in group0) Group_ZF_2_1_L3:
  assumes F = P {lifted to function space over} X
  and s:X→G r:X→G
  and x∈X
  shows (F⟨s,r⟩)(x) = s(x)·r(x)
  using assms group0_2_L1 monoid0.lifted_val by simp

```

In the `group0` context we can apply theorems proven in `monoid0` context to the lifted monoid.

```

lemma (in group0) Group_ZF_2_1_L4:
  assumes A1: F = P {lifted to function space over} X
  shows monoid0(X→G,F)
proof -
  from A1 show thesis
    using group0_2_L1 monoid0.Group_ZF_2_1_T1 monoid0_def
    by simp
qed

```

The composition of a function  $f : X \rightarrow G$  with the group inverse is a right inverse for the lifted group.

```

lemma (in group0) Group_ZF_2_1_L5:
  assumes A1: F = P {lifted to function space over} X
  and A2: s : X→G
  and A3: i = GroupInv(G,P) 0 s
  shows i: X→G and F⟨ s,i⟩ = TheNeutralElement(X→G,F)
proof -
  let E = ConstantFunction(X,1)
  have E : X→G

```

```

    using group0_2_L2 func1_3_L1 by simp
  moreover from groupAssum A2 A3 A1 have
    F⟨ s,i ⟩ : X→G using group0_2_T2 comp_fun
      Group_ZF_2_1_L4 monoid0.group0_1_L1
    by simp
  moreover from groupAssum A2 A3 A1 have
    ∀x∈X. (F⟨ s,i ⟩)(x) = E(x)
    using group0_2_T2 comp_fun Group_ZF_2_1_L3
      comp_fun_apply apply_funtype group0_2_L6 func1_3_L2
    by simp
  moreover from groupAssum A1 have
    E = TheNeutralElement(X→G,F)
    using IsAgroup_def Group_ZF_2_1_L2 by simp
  ultimately show F⟨ s,i ⟩ = TheNeutralElement(X→G,F)
    using fun_extension_iff IsAgroup_def Group_ZF_2_1_L2
    by simp
  from groupAssum A2 A3 show i: X→G
    using group0_2_T2 comp_fun by simp
qed

```

Groups can be lifted to the function space.

```

theorem (in group0) Group_ZF_2_1_T2:
  assumes A1: F = P {lifted to function space over} X
  shows IsAgroup(X→G,F)
proof -
  from A1 have IsAmonoid(X→G,F)
    using group0_2_L1 monoid0.Group_ZF_2_1_T1
    by simp
  moreover have
    ∀s∈X→G. ∃i∈X→G. F⟨ s,i ⟩ = TheNeutralElement(X→G,F)
  proof
    fix s assume A2: s : X→G
    let i = GroupInv(G,P) 0 s
    from groupAssum A2 have i:X→G
      using group0_2_T2 comp_fun by simp
    moreover from A1 A2 have
      F⟨ s,i ⟩ = TheNeutralElement(X→G,F)
      using Group_ZF_2_1_L5 by fast
    ultimately show ∃i∈X→G. F⟨ s,i ⟩ = TheNeutralElement(X→G,F)
      by auto
  qed
  ultimately show thesis using IsAgroup_def
    by simp
qed

```

What is the group inverse for the lifted group?

```

lemma (in group0) Group_ZF_2_1_L6:
  assumes A1: F = P {lifted to function space over} X
  shows ∀s∈(X→G). GroupInv(X→G,F)(s) = GroupInv(G,P) 0 s

```



```

proof -
  from A1 have group0( $X \rightarrow G, F$ )
    using group0_def Group_ZF_2_1_T2
    by simp
  moreover from A1 have  $\forall s \in X \rightarrow G. \text{GroupInv}(G, P) \ 0 \ s : X \rightarrow G \wedge$ 
     $F \langle s, \text{GroupInv}(G, P) \ 0 \ s \rangle = \text{TheNeutralElement}(X \rightarrow G, F)$ 
    using Group_ZF_2_1_L5 by simp
  ultimately have
     $\forall s \in (X \rightarrow G). \text{GroupInv}(G, P) \ 0 \ s = \text{GroupInv}(X \rightarrow G, F)(s)$ 
    by (rule group0.group0_2_L9A)
  thus thesis by simp
qed

```

What is the value of the group inverse for the lifted group?

```

corollary (in group0) lift_gr_inv_val:
  assumes  $F = P \ \{\text{lifted to function space over}\} \ X$  and
     $s : X \rightarrow G$  and  $x \in X$ 
  shows  $(\text{GroupInv}(X \rightarrow G, F)(s))(x) = (s(x))^{-1}$ 
  using groupAssum assms Group_ZF_2_1_L6 group0_2_T2 comp_fun_apply
  by simp

```

What is the group inverse in a subgroup of the lifted group?

```

lemma (in group0) Group_ZF_2_1_L6A:
  assumes A1:  $F = P \ \{\text{lifted to function space over}\} \ X$ 
    and A2:  $\text{IsSubgroup}(H, F)$ 
    and A3:  $g = \text{restrict}(F, H \times H)$ 
    and A4:  $s \in H$ 
  shows  $\text{GroupInv}(H, g)(s) = \text{GroupInv}(G, P) \ 0 \ s$ 
proof -
  from A1 have T1: group0( $X \rightarrow G, F$ )
    using group0_def Group_ZF_2_1_T2
    by simp
  with A2 A3 A4 have  $\text{GroupInv}(H, g)(s) = \text{GroupInv}(X \rightarrow G, F)(s)$ 
    using group0.group0_3_T1 restrict by simp
  moreover from T1 A1 A2 A4 have
     $\text{GroupInv}(X \rightarrow G, F)(s) = \text{GroupInv}(G, P) \ 0 \ s$ 
    using group0.group0_3_L2 Group_ZF_2_1_L6 by blast
  ultimately show thesis by simp
qed

```

If a group is abelian, then its lift to a function space is also abelian.

```

lemma (in group0) Group_ZF_2_1_L7:
  assumes A1:  $F = P \ \{\text{lifted to function space over}\} \ X$ 
    and A2:  $P \ \{\text{is commutative on}\} \ G$ 
  shows  $F \ \{\text{is commutative on}\} \ (X \rightarrow G)$ 
proof-
  from A1 A2 have
     $F \ \{\text{is commutative on}\} \ (X \rightarrow \text{range}(P))$ 
    using group_oper_assocA func_ZF_2_L2

```

```

    by simp
  moreover from groupAssum have range(P) = G
    using group0_2_L1 monoid0.group0_1_L3B
    by simp
  ultimately show thesis by simp
qed

```

## 24.2 Equivalence relations on groups

The goal of this section is to establish that (under some conditions) given an equivalence relation on a group or (monoid) we can project the group (monoid) structure on the quotient and obtain another group.

The neutral element class is neutral in the projection.

```

lemma (in monoid0) Group_ZF_2_2_L1:
  assumes A1: equiv(G,r) and A2: Congruent2(r,f)
  and A3: F = ProjFun2(G,r,f)
  and A4: e = TheNeutralElement(G,f)
  shows r{e} ∈ G//r ∧
    (∀ c ∈ G//r. F⟨ r{e},c ⟩ = c ∧ F⟨ c,r{e} ⟩ = c)
proof
  from A4 show T1: r{e} ∈ G//r
    using unit_is_neutral quotientI
    by simp
  show
    ∀ c ∈ G//r. F⟨ r{e},c ⟩ = c ∧ F⟨ c,r{e} ⟩ = c
  proof
    fix c assume A5: c ∈ G//r
    then obtain g where D1: g ∈ G c = r{g}
      using quotient_def by auto
    with A1 A2 A3 A4 D1 show
      F⟨ r{e},c ⟩ = c ∧ F⟨ c,r{e} ⟩ = c
      using unit_is_neutral EquivClass_1_L10
      by simp
  qed
qed

```

The projected structure is a monoid.

```

theorem (in monoid0) Group_ZF_2_2_T1:
  assumes A1: equiv(G,r) and A2: Congruent2(r,f)
  and A3: F = ProjFun2(G,r,f)
  shows IsAmonoid(G//r,F)
proof -
  let E = r{TheNeutralElement(G,f)}
  from A1 A2 A3 have
    E ∈ G//r ∧ (∀ c ∈ G//r. F⟨ E,c ⟩ = c ∧ F⟨ c,E ⟩ = c)
    using Group_ZF_2_2_L1 by simp
  hence
    ∃ E ∈ G//r. ∀ c ∈ G//r. F⟨ E,c ⟩ = c ∧ F⟨ c,E ⟩ = c

```

```

    by auto
  with monoidAsssum A1 A2 A3 show thesis
    using IsAmonoid_def EquivClass_2_T2
    by simp
qed

```

The class of the neutral element is the neutral element of the projected monoid.

```

lemma Group_ZF_2_2_L1:
  assumes A1: IsAmonoid(G,f)
  and A2: equiv(G,r) and A3: Congruent2(r,f)
  and A4: F = ProjFun2(G,r,f)
  and A5: e = TheNeutralElement(G,f)
  shows r{e} = TheNeutralElement(G//r,F)
proof -
  from A1 A2 A3 A4 have
    T1:monoid0(G,f) and T2:monoid0(G//r,F)
    using monoid0_def monoid0.Group_ZF_2_2_T1 by auto
  from T1 A2 A3 A4 A5 have r{e} ∈ G//r ∧
    (∀ c ∈ G//r. F⟨ r{e},c ⟩ = c ∧ F⟨ c,r{e} ⟩ = c)
    using monoid0.Group_ZF_2_2_L1 by simp
  with T2 show thesis using monoid0.group0_1_L4
    by auto
qed

```

The projected operation can be defined in terms of the group operation on representants in a natural way.

```

lemma (in group0) Group_ZF_2_2_L2:
  assumes A1: equiv(G,r) and A2: Congruent2(r,P)
  and A3: F = ProjFun2(G,r,P)
  and A4: a∈G b∈G
  shows F⟨ r{a},r{b} ⟩ = r{a·b}
proof -
  from A1 A2 A3 A4 show thesis
    using EquivClass_1_L10 by simp
qed

```

The class of the inverse is a right inverse of the class.

```

lemma (in group0) Group_ZF_2_2_L3:
  assumes A1: equiv(G,r) and A2: Congruent2(r,P)
  and A3: F = ProjFun2(G,r,P)
  and A4: a∈G
  shows F⟨ r{a},r{a-1} ⟩ = TheNeutralElement(G//r,F)
proof -
  from A1 A2 A3 A4 have
    F⟨ r{a},r{a-1} ⟩ = r{1}
    using inverse_in_group Group_ZF_2_2_L2 group0_2_L6
    by simp

```

```

with groupAssum A1 A2 A3 show thesis
using IsAgroup_def Group_ZF_2_2_L1 by simp
qed

```

The group structure can be projected to the quotient space.

```

theorem (in group0) Group_ZF_3_T2:
  assumes A1: equiv(G,r) and A2: Congruent2(r,P)
  shows IsAgroup(G//r,ProjFun2(G,r,P))
proof -
  let F = ProjFun2(G,r,P)
  let E = TheNeutralElement(G//r,F)
  from groupAssum A1 A2 have IsAmonoid(G//r,F)
    using IsAgroup_def monoid0_def monoid0.Group_ZF_2_2_T1
    by simp
  moreover have
     $\forall c \in G//r. \exists b \in G//r. F\langle c, b \rangle = E$ 
  proof
    fix c assume A3:  $c \in G//r$ 
    then obtain g where D1:  $g \in G$   $c = r\{g\}$ 
      using quotient_def by auto
    let b =  $r\{g^{-1}\}$ 
    from D1 have  $b \in G//r$ 
      using inverse_in_group quotientI
      by simp
    moreover from A1 A2 D1 have
       $F\langle c, b \rangle = E$ 
      using Group_ZF_2_2_L3 by simp
    ultimately show  $\exists b \in G//r. F\langle c, b \rangle = E$ 
      by auto
  qed
  ultimately show thesis
    using IsAgroup_def by simp
qed

```

The group inverse (in the projected group) of a class is the class of the inverse.

```

lemma (in group0) Group_ZF_2_2_L4:
  assumes A1: equiv(G,r) and
  A2: Congruent2(r,P) and
  A3: F = ProjFun2(G,r,P) and
  A4:  $a \in G$ 
  shows  $r\{a^{-1}\} = \text{GroupInv}(G//r,F)(r\{a\})$ 
proof -
  from A1 A2 A3 have group0(G//r,F)
    using Group_ZF_3_T2 group0_def by simp
  moreover from A4 have
     $r\{a\} \in G//r$   $r\{a^{-1}\} \in G//r$ 
    using inverse_in_group quotientI by auto
  moreover from A1 A2 A3 A4 have

```

```

      F⟨r{a},r{a-1}⟩ = TheNeutralElement(G//r,F)
    using Group_ZF_2_2_L3 by simp
  ultimately show thesis
    by (rule group0.group0_2_L9)
qed

```

### 24.3 Normal subgroups and quotient groups

If  $H$  is a subgroup of  $G$ , then for every  $a \in G$  we can consider the sets  $\{a \cdot h \mid h \in H\}$  and  $\{h \cdot a \mid h \in H\}$  (called a left and right "coset of  $H$ ", resp.) These sets sometimes form a group, called the "quotient group". This section discusses the notion of quotient groups.

A normal subgroup  $N$  of a group  $G$  is such that  $aba^{-1}$  belongs to  $N$  if  $a \in G, b \in N$ .

**definition**

$$\text{IsAnormalSubgroup}(G,P,N) \equiv \text{IsASubgroup}(N,P) \wedge$$

$$(\forall n \in N. \forall g \in G. P(\langle g, n \rangle, \text{GroupInv}(G,P)(g)) \in N)$$

Having a group and a normal subgroup  $N$  we can create another group consisting of equivalence classes of the relation  $a \sim b \equiv a \cdot b^{-1} \in N$ . We will refer to this relation as the quotient group relation. The classes of this relation are in fact cosets of subgroup  $H$ .

**definition**

$$\text{QuotientGroupRel}(G,P,H) \equiv$$

$$\{ \langle a, b \rangle \in G \times G. P(\langle a, \text{GroupInv}(G,P)(b) \rangle \in H) \}$$

Next we define the operation in the quotient group as the projection of the group operation on the classes of the quotient group relation.

**definition**

$$\text{QuotientGroupOp}(G,P,H) \equiv \text{ProjFun2}(G, \text{QuotientGroupRel}(G,P,H), P)$$

Definition of a normal subgroup in a more readable notation.

```

lemma (in group0) Group_ZF_2_4_L0:
  assumes IsAnormalSubgroup(G,P,H)
  and g∈G n∈H
  shows g·n·g-1 ∈ H
  using assms IsAnormalSubgroup_def by simp

```

The quotient group relation is reflexive.

```

lemma (in group0) Group_ZF_2_4_L1:
  assumes IsASubgroup(H,P)
  shows refl(G, QuotientGroupRel(G,P,H))
  using assms group0_2_L6 group0_3_L5
  QuotientGroupRel_def refl_def by simp

```

The quotient group relation is symmetric.

```

lemma (in group0) Group_ZF_2_4_L2:
  assumes A1:IsAsubgroup(H,P)
  shows sym(QuotientGroupRel(G,P,H))
proof -
  {
    fix a b assume A2:  $\langle a, b \rangle \in \text{QuotientGroupRel}(G, P, H)$ 
    with A1 have  $(a \cdot b^{-1})^{-1} \in H$ 
      using QuotientGroupRel_def group0_3_T3A
      by simp
    moreover from A2 have  $(a \cdot b^{-1})^{-1} = b \cdot a^{-1}$ 
      using QuotientGroupRel_def group0_2_L12
      by simp
    ultimately have  $b \cdot a^{-1} \in H$  by simp
    with A2 have  $\langle b, a \rangle \in \text{QuotientGroupRel}(G, P, H)$ 
      using QuotientGroupRel_def by simp
  }
  then show thesis using symI by simp
qed

```

The quotient group relation is transitive.

```

lemma (in group0) Group_ZF_2_4_L3A:
  assumes A1: IsAsubgroup(H,P) and
  A2:  $\langle a, b \rangle \in \text{QuotientGroupRel}(G, P, H)$  and
  A3:  $\langle b, c \rangle \in \text{QuotientGroupRel}(G, P, H)$ 
  shows  $\langle a, c \rangle \in \text{QuotientGroupRel}(G, P, H)$ 
proof -
  let r = QuotientGroupRel(G,P,H)
  from A2 A3 have T1:a∈G b∈G c∈G
    using QuotientGroupRel_def by auto
  from A1 A2 A3 have  $(a \cdot b^{-1}) \cdot (b \cdot c^{-1}) \in H$ 
    using QuotientGroupRel_def group0_3_L6
    by simp
  moreover from T1 have
     $a \cdot c^{-1} = (a \cdot b^{-1}) \cdot (b \cdot c^{-1})$ 
    using group0_2_L14A by blast
  ultimately have  $a \cdot c^{-1} \in H$ 
    by simp
  with T1 show thesis using QuotientGroupRel_def
    by simp
qed

```

The quotient group relation is an equivalence relation. Note we do not need the subgroup to be normal for this to be true.

```

lemma (in group0) Group_ZF_2_4_L3: assumes A1:IsAsubgroup(H,P)
  shows equiv(G,QuotientGroupRel(G,P,H))
proof -
  let r = QuotientGroupRel(G,P,H)
  from A1 have
     $\forall a \ b \ c. (\langle a, b \rangle \in r \ \wedge \ \langle b, c \rangle \in r \longrightarrow \langle a, c \rangle \in r)$ 

```

```

    using Group_ZF_2_4_L3A by blast
  then have trans(r)
    using Fol1_L2 by blast
  with A1 show thesis
    using Group_ZF_2_4_L1 Group_ZF_2_4_L2
      QuotientGroupRel_def equiv_def
    by auto
qed

```

The next lemma states the essential condition for congruency of the group operation with respect to the quotient group relation.

```

lemma (in group0) Group_ZF_2_4_L4:
  assumes A1: IsAnormalSubgroup(G,P,H)
  and A2:  $\langle a1, a2 \rangle \in \text{QuotientGroupRel}(G,P,H)$ 
  and A3:  $\langle b1, b2 \rangle \in \text{QuotientGroupRel}(G,P,H)$ 
  shows  $\langle a1 \cdot b1, a2 \cdot b2 \rangle \in \text{QuotientGroupRel}(G,P,H)$ 
proof -
  from A2 A3 have T1:
     $a1 \in G \ a2 \in G \ b1 \in G \ b2 \in G$ 
     $a1 \cdot b1 \in G \ a2 \cdot b2 \in G$ 
     $b1 \cdot b2^{-1} \in H \ a1 \cdot a2^{-1} \in H$ 
  using QuotientGroupRel_def group0_2_L1 monoid0.group0_1_L1
  by auto
  with A1 show thesis using
    IsAnormalSubgroup_def group0_3_L6 group0_2_L15
    QuotientGroupRel_def by simp
qed

```

If the subgroup is normal, the group operation is congruent with respect to the quotient group relation.

```

lemma Group_ZF_2_4_L5A:
  assumes IsAgroup(G,P)
  and IsAnormalSubgroup(G,P,H)
  shows Congruent2(QuotientGroupRel(G,P,H),P)
  using assms group0_def group0.Group_ZF_2_4_L4 Congruent2_def
  by simp

```

The quotient group is indeed a group.

```

theorem Group_ZF_2_4_T1:
  assumes IsAgroup(G,P) and IsAnormalSubgroup(G,P,H)
  shows
    IsAgroup(G//QuotientGroupRel(G,P,H),QuotientGroupOp(G,P,H))
  using assms group0_def group0.Group_ZF_2_4_L3 IsAnormalSubgroup_def
    Group_ZF_2_4_L5A group0.Group_ZF_3_T2 QuotientGroupOp_def
  by simp

```

The class (coset) of the neutral element is the neutral element of the quotient group.

```

lemma Group_ZF_2_4_L5B:
  assumes IsAgroup(G,P) and IsAnormalSubgroup(G,P,H)
  and r = QuotientGroupRel(G,P,H)
  and e = TheNeutralElement(G,P)
  shows r{e} = TheNeutralElement(G//r,QuotientGroupOp(G,P,H))
  using assms IsAnormalSubgroup_def group0_def
    IsAgroup_def group0.Group_ZF_2_4_L3 Group_ZF_2_4_L5A
    QuotientGroupOp_def Group_ZF_2_2_L1
  by simp

```

A group element is equivalent to the neutral element iff it is in the subgroup we divide the group by.

```

lemma (in group0) Group_ZF_2_4_L5C: assumes a∈G
  shows ⟨a,1⟩ ∈ QuotientGroupRel(G,P,H) ⟷ a∈H
  using assms QuotientGroupRel_def group_inv_of_one group0_2_L2
  by auto

```

A group element is in  $H$  iff its class is the neutral element of  $G/H$ .

```

lemma (in group0) Group_ZF_2_4_L5D:
  assumes A1: IsAnormalSubgroup(G,P,H) and
  A2: a∈G and
  A3: r = QuotientGroupRel(G,P,H) and
  A4: TheNeutralElement(G//r,QuotientGroupOp(G,P,H)) = e
  shows r{a} = e ⟷ ⟨a,1⟩ ∈ r

```

**proof**

```

  assume r{a} = e
  with groupAssum assms have
    r{1} = r{a} and I: equiv(G,r)
    using Group_ZF_2_4_L5B IsAnormalSubgroup_def Group_ZF_2_4_L3
    by auto
  with A2 have ⟨1,a⟩ ∈ r using eq_equiv_class
    by simp
  with I show ⟨a,1⟩ ∈ r by (rule equiv_is_sym)
next assume ⟨a,1⟩ ∈ r
  moreover from A1 A3 have equiv(G,r)
    using IsAnormalSubgroup_def Group_ZF_2_4_L3
    by simp
  ultimately have r{a} = r{1}
    using equiv_class_eq by simp
  with groupAssum A1 A3 A4 show r{a} = e
    using Group_ZF_2_4_L5B by simp

```

**qed**

The class of  $a \in G$  is the neutral element of the quotient  $G/H$  iff  $a \in H$ .

```

lemma (in group0) Group_ZF_2_4_L5E:
  assumes IsAnormalSubgroup(G,P,H) and
  a∈G and r = QuotientGroupRel(G,P,H) and
  TheNeutralElement(G//r,QuotientGroupOp(G,P,H)) = e
  shows r{a} = e ⟷ a∈H

```



```

using assms Group_ZF_2_4_L5C Group_ZF_2_4_L5D
by simp

```

Essential condition to show that every subgroup of an abelian group is normal.

```

lemma (in group0) Group_ZF_2_4_L5:
  assumes A1: P {is commutative on} G
  and A2: IsSubgroup(H,P)
  and A3:  $g \in G \quad h \in H$ 
  shows  $g \cdot h \cdot g^{-1} \in H$ 
proof -
  from A2 A3 have T1:  $h \in G \quad g^{-1} \in G$ 
  using group0_3_L2 inverse_in_group by auto
  with A3 A1 have  $g \cdot h \cdot g^{-1} = g^{-1} \cdot g \cdot h$ 
  using group0_4_L4A by simp
  with A3 T1 show thesis using
    group0_2_L6 group0_2_L2
  by simp

```

qed

Every subgroup of an abelian group is normal. Moreover, the quotient group is also abelian.

```

lemma Group_ZF_2_4_L6:
  assumes A1: IsAGroup(G,P)
  and A2: P {is commutative on} G
  and A3: IsSubgroup(H,P)
  shows IsAnormalSubgroup(G,P,H)
  QuotientGroupOp(G,P,H) {is commutative on} (G//QuotientGroupRel(G,P,H))
proof -
  from A1 A2 A3 show T1: IsAnormalSubgroup(G,P,H) using
    group0_def IsAnormalSubgroup_def group0.Group_ZF_2_4_L5
  by simp
  let r = QuotientGroupRel(G,P,H)
  from A1 A3 T1 have equiv(G,r) Congruent2(r,P)
  using group0_def group0.Group_ZF_2_4_L3 Group_ZF_2_4_L5A
  by auto
  with A2 show
    QuotientGroupOp(G,P,H) {is commutative on} (G//QuotientGroupRel(G,P,H))
  using EquivClass_2_T1 QuotientGroupOp_def
  by simp

```

qed

The group inverse (in the quotient group) of a class (coset) is the class of the inverse.

```

lemma (in group0) Group_ZF_2_4_L7:
  assumes IsAnormalSubgroup(G,P,H)
  and  $a \in G$  and  $r = \text{QuotientGroupRel}(G,P,H)$ 
  and  $F = \text{QuotientGroupOp}(G,P,H)$ 

```

```

shows r{a-1} = GroupInv(G//r,F)(r{a})
using groupAssum assms IsAnormalSubgroup_def Group_ZF_2_4_L3
    Group_ZF_2_4_L5A QuotientGroupOp_def Group_ZF_2_2_L4
by simp

```

## 24.4 Function spaces as monoids

On every space of functions  $\{f : X \rightarrow X\}$  we can define a natural monoid structure with composition as the operation. This section explores this fact.

The next lemma states that composition has a neutral element, namely the identity function on  $X$  (the one that maps  $x \in X$  into itself).

```

lemma Group_ZF_2_5_L1: assumes A1: F = Composition(X)
  shows  $\exists I \in (X \rightarrow X). \forall f \in (X \rightarrow X). F\langle I, f \rangle = f \wedge F\langle f, I \rangle = f$ 
proof-
  let I = id(X)
  from A1 have
     $I \in X \rightarrow X \wedge (\forall f \in (X \rightarrow X). F\langle I, f \rangle = f \wedge F\langle f, I \rangle = f)$ 
    using id_type func_ZF_6_L1A by simp
  thus thesis by auto
qed

```

The space of functions that map a set  $X$  into itself is a monoid with composition as operation and the identity function as the neutral element.

```

lemma Group_ZF_2_5_L2: shows
  IsAmonoid( $X \rightarrow X$ , Composition(X))
  id(X) = TheNeutralElement( $X \rightarrow X$ , Composition(X))
proof -
  let I = id(X)
  let F = Composition(X)
  show IsAmonoid( $X \rightarrow X$ , Composition(X))
    using func_ZF_5_L5 Group_ZF_2_5_L1 IsAmonoid_def
    by auto
  then have monoid0( $X \rightarrow X$ , F)
    using monoid0_def by simp
  moreover have
     $I \in X \rightarrow X \wedge (\forall f \in (X \rightarrow X). F\langle I, f \rangle = f \wedge F\langle f, I \rangle = f)$ 
    using id_type func_ZF_6_L1A by simp
  ultimately show I = TheNeutralElement( $X \rightarrow X$ , F)
    using monoid0.group0_1_L4 by auto
qed
end

```

## 25 Group\_ZF\_3.thy

```
theory Group_ZF_3 imports Group_ZF_2 Finite1
```

```
begin
```

In this theory we consider notions in group theory that are useful for the construction of real numbers in the `Real_ZF_x` series of theories.

### 25.1 Group valued finite range functions

In this section show that the group valued functions  $f : X \rightarrow G$ , with the property that  $f(X)$  is a finite subset of  $G$ , is a group. Such functions play an important role in the construction of real numbers in the `Real_ZF` series.

The following proves the essential condition to show that the set of finite range functions is closed with respect to the lifted group operation.

```
lemma (in group0) Group_ZF_3_1_L1:
  assumes A1: F = P {lifted to function space over} X
  and
  A2: s ∈ FinRangeFunctions(X,G)  r ∈ FinRangeFunctions(X,G)
  shows F⟨ s,r⟩ ∈ FinRangeFunctions(X,G)
proof -
  let q = F⟨ s,r⟩
  from A2 have T1:s:X→G r:X→G
    using FinRangeFunctions_def by auto
  with A1 have T2:q : X→G
    using group0_2_L1 monoid0.Group_ZF_2_1_L0
    by simp
  moreover have q(X) ∈ Fin(G)
  proof -
    from A2 have
      {s(x). x∈X} ∈ Fin(G)
      {r(x). x∈X} ∈ Fin(G)
    using Finite1_L18 by auto
  with A1 T1 T2 show thesis using
    group_oper_assocA Finite1_L15 Group_ZF_2_1_L3 func_imagedef
    by simp
qed
ultimately show thesis using FinRangeFunctions_def
  by simp
qed
```

The set of group valued finite range functions is closed with respect to the lifted group operation.

```
lemma (in group0) Group_ZF_3_1_L2:
  assumes A1: F = P {lifted to function space over} X
  shows FinRangeFunctions(X,G) {is closed under} F
```

```

proof -
  let A = FinRangeFunctions(X,G)
  from A1 have  $\forall x \in A. \forall y \in A. F\langle x,y \rangle \in A$ 
    using Group_ZF_3_1_L1 by simp
  then show thesis using IsOpClosed_def by simp
qed

```

A composition of a finite range function with the group inverse is a finite range function.

```

lemma (in group0) Group_ZF_3_1_L3:
  assumes A1:  $s \in \text{FinRangeFunctions}(X,G)$ 
  shows GroupInv(G,P) 0  $s \in \text{FinRangeFunctions}(X,G)$ 
  using groupAssum assms group0_2_T2 Finite1_L20 by simp

```

The set of finite range functions is a subgroup of the lifted group.

```

theorem Group_ZF_3_1_T1:
  assumes A1: IsAgroup(G,P)
  and A2:  $F = P \text{ \{lifted to function space over\} } X$ 
  and A3:  $X \neq 0$ 
  shows IsASubgroup(FinRangeFunctions(X,G),F)

```

```

proof -
  let e = TheNeutralElement(G,P)
  let S = FinRangeFunctions(X,G)
  from A1 have T1: group0(G,P) using group0_def
    by simp
  with A1 A2 have T2: group0( $X \rightarrow G, F$ )
    using group0.Group_ZF_2_1_T2 group0_def
    by simp
  moreover have  $S \neq 0$ 
  proof -
    from T1 A3 have
      ConstantFunction(X,e)  $\in S$ 
      using group0.group0_2_L1 monoid0.unit_is_neutral
      Finite1_L17 by simp
    thus thesis by auto
  qed
  moreover have  $S \subseteq X \rightarrow G$ 
    using FinRangeFunctions_def by auto
  moreover from A2 T1 have
    S {is closed under} F
    using group0.Group_ZF_3_1_L2
    by simp
  moreover from A1 A2 T1 have
     $\forall s \in S. \text{GroupInv}(X \rightarrow G, F)(s) \in S$ 
    using FinRangeFunctions_def group0.Group_ZF_2_1_L6
    group0.Group_ZF_3_1_L3 by simp
  ultimately show thesis
    using group0.group0_3_T3 by simp
qed

```

## 25.2 Almost homomorphisms

An almost homomorphism is a group valued function defined on a monoid  $M$  with the property that the set  $\{f(m+n) - f(m) - f(n)\}_{m,n \in M}$  is finite. This term is used by R. D. Arthan in "The Eudoxus Real Numbers". We use this term in the general group context and use the A'Campo's term "slopes" (see his "A natural construction for the real numbers") to mean an almost homomorphism mapping interegers into themselves. We consider almost homomorphisms because we use slopes to define real numbers in the `Real_ZF_x` series.

`HomDiff` is an acronym for "homomorphism difference". This is the expression  $s(mn)(s(m)s(n))^{-1}$ , or  $s(m+n) - s(m) - s(n)$  in the additive notation. It is equal to the neutral element of the group if  $s$  is a homomorphism.

**definition**

```
HomDiff(G,f,s,x) ≡
  f⟨s(f⟨fst(x),snd(x))⟩,
  (GroupInv(G,f)(f⟨s(fst(x)),s(snd(x)))⟩)⟩
```

Almost homomorphisms are defined as those maps  $s : G \rightarrow G$  such that the homomorphism difference takes only finite number of values on  $G \times G$ .

**definition**

```
AlmostHoms(G,f) ≡
  {s ∈ G→G. {HomDiff(G,f,s,x). x ∈ G×G } ∈ Fin(G)}
```

$\text{AlHomOp1}(G, f)$  is the group operation on almost homomorphisms defined in a natural way by  $(s \cdot r)(n) = s(n) \cdot r(n)$ . In the terminology defined in `func1.thy` this is the group operation  $f$  (on  $G$ ) lifted to the function space  $G \rightarrow G$  and restricted to the set  $\text{AlmostHoms}(G, f)$ .

**definition**

```
AlHomOp1(G,f) ≡
  restrict(f {lifted to function space over} G,
  AlmostHoms(G,f)×AlmostHoms(G,f))
```

We also define a composition (binary) operator on almost homomorphisms in a natural way. We call that operator `AlHomOp2` - the second operation on almost homomorphisms. Composition of almost homomorphisms is used to define multiplication of real numbers in `Real_ZF` series.

**definition**

```
AlHomOp2(G,f) ≡
  restrict(Composition(G),AlmostHoms(G,f)×AlmostHoms(G,f))
```

This lemma provides more readable notation for the `HomDiff` definition. Not really intended to be used in proofs, but just to see the definition in the notation defined in the `group0` locale.

**lemma** (in `group0`) `HomDiff_notation`:

```

shows HomDiff(G,P,s,< m,n>) = s(m·n)·(s(m)·s(n))-1
using HomDiff_def by simp

```

The next lemma shows the set from the definition of almost homomorphism in a different form.

```

lemma (in group0) Group_ZF_3_2_L1A: shows
  {HomDiff(G,P,s,x). x ∈ G×G} = {s(m·n)·(s(m)·s(n))-1. < m,n> ∈ G×G}
proof -
  have ∀m∈G.∀n∈G. HomDiff(G,P,s,< m,n>) = s(m·n)·(s(m)·s(n))-1
    using HomDiff_notation by simp
  then show thesis by (rule ZF1_1_L4A)
qed

```

Let's define some notation. We inherit the notation and assumptions from the group0 context (locale) and add some. We will use AH to denote the set of almost homomorphisms.  $\sim$  is the inverse (negative if the group is the group of integers) of almost homomorphisms,  $(\sim p)(n) = p(n)^{-1}$ .  $\delta$  will denote the homomorphism difference specific for the group  $(\text{HomDiff}(G, f))$ . The notation  $s \approx r$  will mean that  $s, r$  are almost equal, that is they are in the equivalence relation defined by the group of finite range functions (that is a normal subgroup of almost homomorphisms, if the group is abelian). We show that this is equivalent to the set  $\{s(n) \cdot r(n)^{-1} : n \in G\}$  being finite. We also add an assumption that the  $G$  is abelian as many needed properties do not hold without that.

```

locale group1 = group0 +
  assumes isAbelian: P {is commutative on} G

  fixes AH
  defines AH_def [simp]: AH ≡ AlmostHoms(G,P)

  fixes Op1
  defines Op1_def [simp]: Op1 ≡ AlHomOp1(G,P)

  fixes Op2
  defines Op2_def [simp]: Op2 ≡ AlHomOp2(G,P)

  fixes FR
  defines FR_def [simp]: FR ≡ FinRangeFunctions(G,G)

  fixes neg (~_ [90] 91)
  defines neg_def [simp]: ~s ≡ GroupInv(G,P) 0 s

  fixes δ
  defines δ_def [simp]: δ(s,x) ≡ HomDiff(G,P,s,x)

  fixes AHprod (infix · 69)
  defines AHprod_def [simp]: s · r ≡ AlHomOp1(G,P)<s,r>

```

```

fixes AHcomp (infix  $\circ$  70)
defines AHcomp_def [simp]:  $s \circ r \equiv \text{AlHomOp2}(G,P)\langle s,r \rangle$ 

fixes AlEq (infix  $\approx$  68)
defines AlEq_def [simp]:
 $s \approx r \equiv \langle s,r \rangle \in \text{QuotientGroupRel}(\text{AH},\text{Op1},\text{FR})$ 

```

HomDiff is a homomorphism on the lifted group structure.

```

lemma (in group1) Group_ZF_3_2_L1:
  assumes A1:  $s:G \rightarrow G \quad r:G \rightarrow G$ 
  and A2:  $x \in G \times G$ 
  and A3:  $F = P \text{ \{lifted to function space over\} } G$ 
  shows  $\delta(F\langle s,r \rangle, x) = \delta(s,x) \cdot \delta(r,x)$ 
proof -
  let p =  $F\langle s,r \rangle$ 
  from A2 obtain m n where
    D1:  $x = \langle m,n \rangle \quad m \in G \quad n \in G$ 
  by auto
  then have T1:  $m \cdot n \in G$ 
  using group0_2_L1 monoid0.group0_1_L1 by simp
  with A1 D1 have T2:
     $s(m) \in G \quad s(n) \in G \quad r(m) \in G$ 
     $r(n) \in G \quad s(m \cdot n) \in G \quad r(m \cdot n) \in G$ 
  using apply_funtype by auto
  from A3 A1 have T3:  $p : G \rightarrow G$ 
  using group0_2_L1 monoid0.Group_ZF_2_1_L0
  by simp
  from D1 T3 have
     $\delta(p,x) = p(m \cdot n) \cdot ((p(n))^{-1} \cdot (p(m))^{-1})$ 
  using HomDiff_notation apply_funtype group_inv_of_two
  by simp
  also from A3 A1 D1 T1 isAbelian T2 have
     $\dots = \delta(s,x) \cdot \delta(r,x)$ 
  using Group_ZF_2_1_L3 group0_4_L3 HomDiff_notation
  by simp
  finally show thesis by simp
qed

```

The group operation lifted to the function space over  $G$  preserves almost homomorphisms.

```

lemma (in group1) Group_ZF_3_2_L2: assumes A1:  $s \in \text{AH} \quad r \in \text{AH}$ 
  and A2:  $F = P \text{ \{lifted to function space over\} } G$ 
  shows  $F\langle s,r \rangle \in \text{AH}$ 
proof -
  let p =  $F\langle s,r \rangle$ 
  from A1 A2 have p :  $G \rightarrow G$ 
  using AlmostHoms_def group0_2_L1 monoid0.Group_ZF_2_1_L0
  by simp
  moreover have

```

```

      { $\delta(p,x).$   $x \in G \times G$ }  $\in \text{Fin}(G)$ 
    proof -
      from A1 have
        { $\delta(s,x).$   $x \in G \times G$ }  $\in \text{Fin}(G)$ 
        { $\delta(r,x).$   $x \in G \times G$ }  $\in \text{Fin}(G)$ 
        using AlmostHoms_def by auto
      with groupAssum A1 A2 show thesis
        using IsAgroup_def IsAmonoid_def IsAssociative_def
        Finite1_L15 AlmostHoms_def Group_ZF_3_2_L1
        by auto
    qed
    ultimately show thesis using AlmostHoms_def
    by simp
  qed

```

The set of almost homomorphisms is closed under the lifted group operation.

```

lemma (in group1) Group_ZF_3_2_L3:
  assumes  $F = P$  {lifted to function space over}  $G$ 
  shows  $AH$  {is closed under}  $F$ 
  using assms IsOpClosed_def Group_ZF_3_2_L2 by simp

```

The terms in the homomorphism difference for a function are in the group.

```

lemma (in group1) Group_ZF_3_2_L4:
  assumes  $s:G \rightarrow G$  and  $m \in G$   $n \in G$ 
  shows
     $m \cdot n \in G$ 
     $s(m \cdot n) \in G$ 
     $s(m) \in G$   $s(n) \in G$ 
     $\delta(s, \langle m, n \rangle) \in G$ 
     $s(m) \cdot s(n) \in G$ 
  using assms group_op_closed inverse_in_group
  apply_funtype HomDiff_def by auto

```

It is handy to have a version of Group\_ZF\_3\_2\_L4 specifically for almost homomorphisms.

```

corollary (in group1) Group_ZF_3_2_L4A:
  assumes  $s \in AH$  and  $m \in G$   $n \in G$ 
  shows  $m \cdot n \in G$ 
     $s(m \cdot n) \in G$ 
     $s(m) \in G$   $s(n) \in G$ 
     $\delta(s, \langle m, n \rangle) \in G$ 
     $s(m) \cdot s(n) \in G$ 
  using assms AlmostHoms_def Group_ZF_3_2_L4
  by auto

```

The terms in the homomorphism difference are in the group, a different form.

```

lemma (in group1) Group_ZF_3_2_L4B:

```



```

    assumes A1:s ∈ AH and A2:x∈G×G
    shows fst(x)·snd(x) ∈ G
    s(fst(x)·snd(x)) ∈ G
    s(fst(x)) ∈ G s(snd(x)) ∈ G
    δ(s,x) ∈ G
    s(fst(x))·s(snd(x)) ∈ G
  proof -
    let m = fst(x)
    let n = snd(x)
    from A1 A2 show
      m·n ∈ G s(m·n) ∈ G
      s(m) ∈ G s(n) ∈ G
      s(m)·s(n) ∈ G
    using Group_ZF_3_2_L4A
    by auto
    from A1 A2 have δ(s,⟨ m,n⟩) ∈ G using Group_ZF_3_2_L4A
    by simp
    moreover from A2 have ⟨ m,n⟩ = x by auto
    ultimately show δ(s,x) ∈ G by simp
  qed

```

What are the values of the inverse of an almost homomorphism?

```

lemma (in group1) Group_ZF_3_2_L5:
  assumes s ∈ AH and n∈G
  shows (∼s)(n) = (s(n))-1
  using assms AlmostHoms_def comp_fun_apply by auto

```

Homomorphism difference commutes with the inverse for almost homomorphisms.

```

lemma (in group1) Group_ZF_3_2_L6:
  assumes A1:s ∈ AH and A2:x∈G×G
  shows δ(∼s,x) = (δ(s,x))-1
  proof -
    let m = fst(x)
    let n = snd(x)
    have δ(∼s,x) = (∼s)(m·n)·((∼s)(m)·(∼s)(n))-1
    using HomDiff_def by simp
    from A1 A2 isAbelian show thesis
    using Group_ZF_3_2_L4B HomDiff_def
      Group_ZF_3_2_L5 group0_4_L4A
    by simp
  qed

```

The inverse of an almost homomorphism maps the group into itself.

```

lemma (in group1) Group_ZF_3_2_L7:
  assumes s ∈ AH
  shows ∼s : G→G
  using groupAssum assms AlmostHoms_def group0_2_T2 comp_fun by auto

```

The inverse of an almost homomorphism is an almost homomorphism.

```

lemma (in group1) Group_ZF_3_2_L8:
  assumes A1: F = P {lifted to function space over} G
  and A2: s ∈ AH
  shows GroupInv(G→G,F)(s) ∈ AH
proof -
  from A2 have {δ(s,x). x ∈ G×G} ∈ Fin(G)
    using AlmostHoms_def by simp
  with groupAssum have
    GroupInv(G,P){δ(s,x). x ∈ G×G} ∈ Fin(G)
    using group0_2_T2 Finite1_L6A by blast
  moreover have
    GroupInv(G,P){δ(s,x). x ∈ G×G} =
    {(δ(s,x))-1. x ∈ G×G}
  proof -
    from groupAssum have
      GroupInv(G,P) : G→G
      using group0_2_T2 by simp
    moreover from A2 have
      ∀x∈G×G. δ(s,x)∈G
      using Group_ZF_3_2_L4B by simp
    ultimately show thesis
      using func1_1_L17 by simp
  qed
  ultimately have {(δ(s,x))-1. x ∈ G×G} ∈ Fin(G)
    by simp
  moreover from A2 have
    {(δ(s,x))-1. x ∈ G×G} = {δ(∼s,x). x ∈ G×G}
    using Group_ZF_3_2_L6 by simp
  ultimately have {δ(∼s,x). x ∈ G×G} ∈ Fin(G)
    by simp
  with A2 groupAssum A1 show thesis
    using Group_ZF_3_2_L7 AlmostHoms_def Group_ZF_2_1_L6
    by simp
qed

```

The function that assigns the neutral element everywhere is an almost homomorphism.

```

lemma (in group1) Group_ZF_3_2_L9: shows
  ConstantFunction(G,1) ∈ AH and AH≠0
proof -
  let z = ConstantFunction(G,1)
  have G×G≠0 using group0_2_L1 monoid0.group0_1_L3A
    by blast
  moreover have ∀x∈G×G. δ(z,x) = 1
  proof
    fix x assume A1:x ∈ G × G
    then obtain m n where x = ⟨ m,n⟩ m∈G n∈G
      by auto

```

```

    then show  $\delta(z,x) = 1$ 
      using group0_2_L1 monoid0.group0_1_L1
func1_3_L2 HomDiff_def group0_2_L2
group_inv_of_one by simp
qed
ultimately have  $\{\delta(z,x). x \in G \times G\} = \{1\}$  by (rule ZF1_1_L5)
then show  $z \in AH$  using group0_2_L2 Finite1_L16
  func1_3_L1 group0_2_L2 AlmostHoms_def by simp
then show  $AH \neq 0$  by auto
qed

```

If the group is abelian, then almost homomorphisms form a subgroup of the lifted group.

```

lemma Group_ZF_3_2_L10:
  assumes A1: IsAgroup(G,P)
  and A2: P {is commutative on} G
  and A3: F = P {lifted to function space over} G
  shows IsSubgroup(AlmostHoms(G,P),F)
proof -
  let AH = AlmostHoms(G,P)
  from A2 A1 have T1: group1(G,P)
    using group1_axioms.intro group0_def group1_def
    by simp
  from A1 A3 have group0(G→G,F)
    using group0_def group0.Group_ZF_2_1_T2 by simp
  moreover from T1 have AH≠0
    using group1.Group_ZF_3_2_L9 by simp
  moreover have T2: AH ⊆ G→G
    using AlmostHoms_def by auto
  moreover from T1 A3 have
    AH {is closed under} F
    using group1.Group_ZF_3_2_L3 by simp
  moreover from T1 A3 have
    ∀s∈AH. GroupInv(G→G,F)(s) ∈ AH
    using group1.Group_ZF_3_2_L8 by simp
  ultimately show IsSubgroup(AlmostHoms(G,P),F)
    using group0.group0_3_T3 by simp
qed

```

If the group is abelian, then almost homomorphisms form a group with the first operation, hence we can use theorems proven in group0 context applied to this group.

```

lemma (in group1) Group_ZF_3_2_L10A:
  shows IsAgroup(AH,Op1) group0(AH,Op1)
    using groupAssum isAbelian Group_ZF_3_2_L10 IsSubgroup_def
    AlHomOp1_def group0_def by auto

```

The group of almost homomorphisms is abelian

```

lemma Group_ZF_3_2_L11: assumes A1: IsAgroup(G,f)

```

```

and A2: f {is commutative on} G
shows
  IsAgroup(AlmostHoms(G,f),AlHomOp1(G,f))
  AlHomOp1(G,f) {is commutative on} AlmostHoms(G,f)
proof-
  let AH = AlmostHoms(G,f)
  let F = f {lifted to function space over} G
  from A1 A2 have IsAsubgroup(AH,F)
    using Group_ZF_3_2_L10 by simp
  then show IsAgroup(AH,AlHomOp1(G,f))
    using IsAsubgroup_def AlHomOp1_def by simp
  from A1 have F : (G→G)×(G→G)→(G→G)
    using IsAgroup_def monoid0_def monoid0.Group_ZF_2_1_L0A
    by simp
  moreover have AH ⊆ G→G
    using AlmostHoms_def by auto
  moreover from A1 A2 have
    F {is commutative on} (G→G)
    using group0_def group0.Group_ZF_2_1_L7
    by simp
  ultimately show
    AlHomOp1(G,f){is commutative on} AH
    using func_ZF_4_L1 AlHomOp1_def by simp
qed

```

The first operation on homomorphisms acts in a natural way on its operands.

```

lemma (in group1) Group_ZF_3_2_L12:
  assumes s∈AH r∈AH and n∈G
  shows (s·r)(n) = s(n)·r(n)
  using assms AlHomOp1_def restrict AlmostHoms_def Group_ZF_2_1_L3
  by simp

```

What is the group inverse in the group of almost homomorphisms?

```

lemma (in group1) Group_ZF_3_2_L13:
  assumes A1: s∈AH
  shows
    GroupInv(AH,Op1)(s) = GroupInv(G,P) 0 s
    GroupInv(AH,Op1)(s) ∈ AH
    GroupInv(G,P) 0 s ∈ AH
proof -
  let F = P {lifted to function space over} G
  from groupAssum isAbelian have IsAsubgroup(AH,F)
    using Group_ZF_3_2_L10 by simp
  with A1 show I: GroupInv(AH,Op1)(s) = GroupInv(G,P) 0 s
    using AlHomOp1_def Group_ZF_2_1_L6A by simp
  from A1 show GroupInv(AH,Op1)(s) ∈ AH
    using Group_ZF_3_2_L10A group0.inverse_in_group by simp
  with I show GroupInv(G,P) 0 s ∈ AH by simp
qed

```

The group inverse in the group of almost homomorphisms acts in a natural way on its operand.

```
lemma (in group1) Group_ZF_3_2_L14:
  assumes s∈AH and n∈G
  shows (GroupInv(AH,Op1)(s))(n) = (s(n))-1
  using isAbelian assms Group_ZF_3_2_L13 AlmostHoms_def comp_fun_apply
  by auto
```

The next lemma states that if  $s, r$  are almost homomorphisms, then  $s \cdot r^{-1}$  is also an almost homomorphism.

```
lemma Group_ZF_3_2_L15: assumes IsAgroup(G,f)
  and f {is commutative on} G
  and AH = AlmostHoms(G,f) Op1 = AlHomOp1(G,f)
  and s ∈ AH r ∈ AH
  shows
    Op1⟨ s,r ⟩ ∈ AH
    GroupInv(AH,Op1)(r) ∈ AH
    Op1⟨ s,GroupInv(AH,Op1)(r) ⟩ ∈ AH
  using assms group0_def group1_axioms.intro group1_def
    group1.Group_ZF_3_2_L10A group0.group0_2_L1
    monoid0.group0_1_L1 group0.inverse_in_group by auto
```

A version of Group\_ZF\_3\_2\_L15 formulated in notation used in group1 context. States that the product of almost homomorphisms is an almost homomorphism and the the product of an almost homomorphism with a (point-wise) inverse of an almost homomorphism is an almost homomorphism.

```
corollary (in group1) Group_ZF_3_2_L16: assumes s ∈ AH r ∈ AH
  shows s·r ∈ AH s·(∼r) ∈ AH
  using assms isAbelian group0_def group1_axioms group1_def
    Group_ZF_3_2_L15 Group_ZF_3_2_L13 by auto
```

### 25.3 The classes of almost homomorphisms

In the Real\_ZF series we define real numbers as a quotient of the group of integer almost homomorphisms by the integer finite range functions. In this section we setup the background for that in the general group context.

Finite range functions are almost homomorphisms.

```
lemma (in group1) Group_ZF_3_3_L1: shows FR ⊆ AH
proof
  fix s assume A1:s ∈ FR
  then have T1:{s(n). n ∈ G} ∈ Fin(G)
    {s(fst(x)). x∈G×G} ∈ Fin(G)
    {s(snd(x)). x∈G×G} ∈ Fin(G)
    using Finite1_L18 Finite1_L6B by auto
  have {s(fst(x)·snd(x)). x ∈ G×G} ∈ Fin(G)
proof -
```

```

    have  $\forall x \in G \times G. \text{fst}(x) \cdot \text{snd}(x) \in G$ 
      using group0_2_L1 monoid0.group0_1_L1 by simp
    moreover from T1 have  $\{s(n). n \in G\} \in \text{Fin}(G)$  by simp
    ultimately show thesis by (rule Finite1_L6B)
  qed
  moreover have
     $\{(s(\text{fst}(x)) \cdot s(\text{snd}(x)))^{-1}. x \in G \times G\} \in \text{Fin}(G)$ 
  proof -
    have  $\forall g \in G. g^{-1} \in G$  using inverse_in_group
      by simp
    moreover from T1 have
       $\{s(\text{fst}(x)) \cdot s(\text{snd}(x)). x \in G \times G\} \in \text{Fin}(G)$ 
      using group_oper_assocA Finite1_L15 by simp
    ultimately show thesis
      by (rule Finite1_L6C)
  qed
  ultimately have  $\{\delta(s,x). x \in G \times G\} \in \text{Fin}(G)$ 
    using HomDiff_def Finite1_L15 group_oper_assocA
    by simp
  with A1 show  $s \in \text{AH}$ 
    using FinRangeFunctions_def AlmostHoms_def
    by simp
qed

```

Finite range functions valued in an abelian group form a normal subgroup of almost homomorphisms.

```

lemma Group_ZF_3_3_L2: assumes A1:IsAgroup(G,f)
  and A2:f {is commutative on} G
  shows
    IsASubgroup(FinRangeFunctions(G,G),AlHomOp1(G,f))
    IsANormalSubgroup(AlmostHoms(G,f),AlHomOp1(G,f),
      FinRangeFunctions(G,G))
  proof -
    let H1 = AlmostHoms(G,f)
    let H2 = FinRangeFunctions(G,G)
    let F = f {lifted to function space over} G
    from A1 A2 have T1:group0(G,f)
      monoid0(G,f) group1(G,f)
      using group0_def group0.group0_2_L1
      group1_axioms.intro group1_def
      by auto
    with A1 A2 have IsAgroup(G→G,F)
      IsASubgroup(H1,F) IsASubgroup(H2,F)
      using group0.Group_ZF_2_1_T2 Group_ZF_3_2_L10
      monoid0.group0_1_L3A Group_ZF_3_1_T1
      by auto
    then have
      IsASubgroup(H1∩H2,restrict(F,H1×H1))
      using group0_3_L7 by simp
  qed

```

```

moreover from T1 have H1∩H2 = H2
  using group1.Group_ZF_3_3_L1 by auto
ultimately show IsAsubgroup(H2,AlHomOp1(G,f))
  using AlHomOp1_def by simp
with A1 A2 show IsAnormalSubgroup(AlmostHoms(G,f),AlHomOp1(G,f),
  FinRangeFunctions(G,G))
  using Group_ZF_3_2_L11 Group_ZF_2_4_L6
  by simp
qed

```

The group of almost homomorphisms divided by the subgroup of finite range functions is an abelian group.

```

theorem (in group1) Group_ZF_3_3_T1:
  shows
    IsAgroup(AH//QuotientGroupRel(AH,Op1,FR),QuotientGroupOp(AH,Op1,FR))
  and
    QuotientGroupOp(AH,Op1,FR) {is commutative on}
    (AH//QuotientGroupRel(AH,Op1,FR))
  using groupAssum isAbelian Group_ZF_3_3_L2 Group_ZF_3_2_L10A
    Group_ZF_2_4_T1 Group_ZF_3_2_L10A Group_ZF_3_2_L11
    Group_ZF_3_3_L2 IsAnormalSubgroup_def Group_ZF_2_4_L6 by auto

```

It is useful to have a direct statement that the quotient group relation is an equivalence relation for the group of AH and subgroup FR.

```

lemma (in group1) Group_ZF_3_3_L3: shows
  QuotientGroupRel(AH,Op1,FR) ⊆ AH × AH and
  equiv(AH,QuotientGroupRel(AH,Op1,FR))
  using groupAssum isAbelian QuotientGroupRel_def
    Group_ZF_3_3_L2 Group_ZF_3_2_L10A group0.Group_ZF_2_4_L3
  by auto

```

The "almost equal" relation is symmetric.

```

lemma (in group1) Group_ZF_3_3_L3A: assumes A1: s≈r
  shows r≈s
proof -
  let R = QuotientGroupRel(AH,Op1,FR)
  from A1 have equiv(AH,R) and ⟨s,r⟩ ∈ R
    using Group_ZF_3_3_L3 by auto
  then have ⟨r,s⟩ ∈ R by (rule equiv_is_sym)
  then show r≈s by simp
qed

```

Although we have bypassed this fact when proving that group of almost homomorphisms divided by the subgroup of finite range functions is a group, it is still useful to know directly that the first group operation on AH is congruent with respect to the quotient group relation.

```

lemma (in group1) Group_ZF_3_3_L4:
  shows Congruent2(QuotientGroupRel(AH,Op1,FR),Op1)

```

```

using groupAssum isAbelian Group_ZF_3_2_L10A Group_ZF_3_3_L2
Group_ZF_2_4_L5A by simp

```

The class of an almost homomorphism  $s$  is the neutral element of the quotient group of almost homomorphisms iff  $s$  is a finite range function.

```

lemma (in group1) Group_ZF_3_3_L5: assumes s ∈ AH and
  r = QuotientGroupRel(AH,Op1,FR) and
  TheNeutralElement(AH//r,QuotientGroupOp(AH,Op1,FR)) = e
shows r{s} = e ⟷ s ∈ FR
using groupAssum isAbelian assms Group_ZF_3_2_L11
group0_def Group_ZF_3_3_L2 group0.Group_ZF_2_4_L5E
by simp

```

The group inverse of a class of an almost homomorphism  $f$  is the class of the inverse of  $f$ .

```

lemma (in group1) Group_ZF_3_3_L6:
  assumes A1: s ∈ AH and
  r = QuotientGroupRel(AH,Op1,FR) and
  F = ProjFun2(AH,r,Op1)
shows r{~s} = GroupInv(AH//r,F)(r{s})
proof -
  from groupAssum isAbelian assms have
    r{GroupInv(AH, Op1)(s)} = GroupInv(AH//r,F)(r {s})
  using Group_ZF_3_2_L10A Group_ZF_3_3_L2 QuotientGroupOp_def
  group0.Group_ZF_2_4_L7 by simp
  with A1 show thesis using Group_ZF_3_2_L13
  by simp
qed

```

## 25.4 Compositions of almost homomorphisms

The goal of this section is to establish some facts about composition of almost homomorphisms. needed for the real numbers construction in `Real_ZF_x` series. In particular we show that the set of almost homomorphisms is closed under composition and that composition is congruent with respect to the equivalence relation defined by the group of finite range functions (a normal subgroup of almost homomorphisms).

The next formula restates the definition of the homomorphism difference to express the value an almost homomorphism on a product.

```

lemma (in group1) Group_ZF_3_4_L1:
  assumes s∈AH and m∈G n∈G
  shows s(m·n) = s(m)·s(n)·δ(s,⟨ m,n⟩)
using isAbelian assms Group_ZF_3_2_L4A HomDiff_def group0_4_L5
by simp

```

What is the value of a composition of almost homomorphisms?



```

lemma (in group1) Group_ZF_3_4_L2:
  assumes s∈AH r∈AH and m∈G
  shows (s∘r)(m) = s(r(m)) s(r(m)) ∈ G
  using assms AlmostHoms_def func_ZF_5_L3 restrict AlHomOp2_def
  apply_funtype by auto

```

What is the homomorphism difference of a composition?

```

lemma (in group1) Group_ZF_3_4_L3:
  assumes A1: s∈AH r∈AH and A2: m∈G n∈G
  shows δ(s∘r,⟨ m,n⟩) =
    δ(s,⟨ r(m),r(n)⟩)·s(δ(r,⟨ m,n⟩))·δ(s,⟨ r(m)·r(n),δ(r,⟨ m,n⟩)⟩)
proof -
  from A1 A2 have T1:
    s(r(m))·s(r(n)) ∈ G
    δ(s,⟨ r(m),r(n)⟩)∈ G s(δ(r,⟨ m,n⟩)) ∈ G
    δ(s,⟨ (r(m)·r(n)),δ(r,⟨ m,n⟩)⟩) ∈ G
  using Group_ZF_3_4_L2 AlmostHoms_def apply_funtype
    Group_ZF_3_2_L4A group0_2_L1 monoid0.group0_1_L1
  by auto
  from A1 A2 have δ(s∘r,⟨ m,n⟩) =
    s(r(m)·r(n)·δ(r,⟨ m,n⟩))·(s((r(m)))·s(r(n)))-1
  using HomDiff_def group0_2_L1 monoid0.group0_1_L1 Group_ZF_3_4_L2
    Group_ZF_3_4_L1 by simp
  moreover from A1 A2 have
    s(r(m)·r(n)·δ(r,⟨ m,n⟩)) =
    s(r(m)·r(n))·s(δ(r,⟨ m,n⟩))·δ(s,⟨ (r(m)·r(n)),δ(r,⟨ m,n⟩)⟩)
    s(r(m)·r(n)) = s(r(m))·s(r(n))·δ(s,⟨ r(m),r(n)⟩)
  using Group_ZF_3_2_L4A Group_ZF_3_4_L1 by auto
  moreover from T1 isAbelian have
    s(r(m))·s(r(n))·δ(s,⟨ r(m),r(n)⟩)·
    s(δ(r,⟨ m,n⟩))·δ(s,⟨ (r(m)·r(n)),δ(r,⟨ m,n⟩)⟩)·
    (s((r(m)))·s(r(n)))-1 =
    δ(s,⟨ r(m),r(n)⟩)·s(δ(r,⟨ m,n⟩))·δ(s,⟨ (r(m)·r(n)),δ(r,⟨ m,n⟩)⟩)
  using group0_4_L6C by simp
  ultimately show thesis by simp
qed

```

What is the homomorphism difference of a composition (another form)?  
 Here we split the homomorphism difference of a composition into a product of three factors. This will help us in proving that the range of homomorphism difference for the composition is finite, as each factor has finite range.

```

lemma (in group1) Group_ZF_3_4_L4:
  assumes A1: s∈AH r∈AH and A2: x ∈ G×G
  and A3:
    A = δ(s,⟨ r(fst(x)),r(snd(x))⟩)
    B = s(δ(r,x))
    C = δ(s,⟨ (r(fst(x))·r(snd(x))),δ(r,x)⟩)
  shows δ(s∘r,x) = A·B·C
proof -

```

```

let m = fst(x)
let n = snd(x)
note A1
moreover from A2 have m ∈ G n ∈ G
  by auto
ultimately have
   $\delta(s \circ r, \langle m, n \rangle) =$ 
   $\delta(s, \langle r(m), r(n) \rangle) \cdot s(\delta(r, \langle m, n \rangle)) \cdot$ 
   $\delta(s, \langle (r(m) \cdot r(n)), \delta(r, \langle m, n \rangle) \rangle)$ 
  by (rule Group_ZF_3_4_L3)
with A1 A2 A3 show thesis
  by auto
qed

```

The range of the homomorphism difference of a composition of two almost homomorphisms is finite. This is the essential condition to show that a composition of almost homomorphisms is an almost homomorphism.

```

lemma (in group1) Group_ZF_3_4_L5:
  assumes A1: s ∈ AH r ∈ AH
  shows { $\delta(\text{Composition}(G) \langle s, r \rangle, x)$ .  $x \in G \times G$ } ∈ Fin(G)
proof -
  from A1 have
     $\forall x \in G \times G. \langle r(\text{fst}(x)), r(\text{snd}(x)) \rangle \in G \times G$ 
    using Group_ZF_3_2_L4B by simp
  moreover from A1 have
    { $\delta(s, x)$ .  $x \in G \times G$ } ∈ Fin(G)
    using AlmostHoms_def by simp
  ultimately have
    { $\delta(s, \langle r(\text{fst}(x)), r(\text{snd}(x)) \rangle)$ .  $x \in G \times G$ } ∈ Fin(G)
    by (rule Finite1_L6B)
  moreover have { $s(\delta(r, x))$ .  $x \in G \times G$ } ∈ Fin(G)
  proof -
    from A1 have  $\forall m \in G. s(m) \in G$ 
      using AlmostHoms_def apply_funtype by auto
    moreover from A1 have { $\delta(r, x)$ .  $x \in G \times G$ } ∈ Fin(G)
      using AlmostHoms_def by simp
    ultimately show thesis
      by (rule Finite1_L6C)
  qed
  ultimately have
    { $\delta(s, \langle r(\text{fst}(x)), r(\text{snd}(x)) \rangle) \cdot s(\delta(r, x))$ .  $x \in G \times G$ } ∈ Fin(G)
    using group_oper_assocA Finite1_L15 by simp
  moreover have
    { $\delta(s, \langle (r(\text{fst}(x)) \cdot r(\text{snd}(x))), \delta(r, x) \rangle)$ .  $x \in G \times G$ } ∈ Fin(G)
  proof -
    from A1 have
       $\forall x \in G \times G. \langle (r(\text{fst}(x)) \cdot r(\text{snd}(x))), \delta(r, x) \rangle \in G \times G$ 
      using Group_ZF_3_2_L4B by simp
    moreover from A1 have

```

```

      { $\delta(s, x) \cdot x \in G \times G$ }  $\in \text{Fin}(G)$ 
      using AlmostHoms_def by simp
      ultimately show thesis by (rule Finite1_L6B)
    qed
  ultimately have
    { $\delta(s, \langle r(\text{fst}(x)), r(\text{snd}(x)) \rangle) \cdot s(\delta(r, x)) \cdot$ 
 $\delta(s, \langle r(\text{fst}(x)) \cdot r(\text{snd}(x)), \delta(r, x) \rangle) \cdot x \in G \times G$ }  $\in \text{Fin}(G)$ 
    using group_oper_assocA Finite1_L15 by simp
  moreover from A1 have { $\delta(s \circ r, x) \cdot x \in G \times G$ } =
    { $\delta(s, \langle r(\text{fst}(x)), r(\text{snd}(x)) \rangle) \cdot s(\delta(r, x)) \cdot$ 
 $\delta(s, \langle r(\text{fst}(x)) \cdot r(\text{snd}(x)), \delta(r, x) \rangle) \cdot x \in G \times G$ }
    using Group_ZF_3_4_L4 by simp
  ultimately have { $\delta(s \circ r, x) \cdot x \in G \times G$ }  $\in \text{Fin}(G)$  by simp
  with A1 show thesis using restrict AlHomOp2_def
    by simp
qed

```

Composition of almost homomorphisms is an almost homomorphism.

```

theorem (in group1) Group_ZF_3_4_T1:
  assumes A1:  $s \in \text{AH}$   $r \in \text{AH}$ 
  shows  $\text{Composition}(G) \langle s, r \rangle \in \text{AH}$   $s \circ r \in \text{AH}$ 
proof -
  from A1 have  $\langle s, r \rangle \in (G \rightarrow G) \times (G \rightarrow G)$ 
    using AlmostHoms_def by simp
  then have  $\text{Composition}(G) \langle s, r \rangle : G \rightarrow G$ 
    using func_ZF_5_L1 apply_funtype by blast
  with A1 show  $\text{Composition}(G) \langle s, r \rangle \in \text{AH}$ 
    using Group_ZF_3_4_L5 AlmostHoms_def
    by simp
  with A1 show  $s \circ r \in \text{AH}$  using AlHomOp2_def restrict
    by simp
qed

```

The set of almost homomorphisms is closed under composition. The second operation on almost homomorphisms is associative.

```

lemma (in group1) Group_ZF_3_4_L6: shows
   $\text{AH}$  {is closed under}  $\text{Composition}(G)$ 
   $\text{AlHomOp2}(G, P)$  {is associative on}  $\text{AH}$ 
proof -
  show  $\text{AH}$  {is closed under}  $\text{Composition}(G)$ 
    using Group_ZF_3_4_T1 IsOpClosed_def by simp
  moreover have  $\text{AH} \subseteq G \rightarrow G$  using AlmostHoms_def
    by auto
  moreover have
     $\text{Composition}(G)$  {is associative on}  $(G \rightarrow G)$ 
    using func_ZF_5_L5 by simp
  ultimately show  $\text{AlHomOp2}(G, P)$  {is associative on}  $\text{AH}$ 
    using func_ZF_4_L3 AlHomOp2_def by simp
qed

```

Type information related to the situation of two almost homomorphisms.

```

lemma (in group1) Group_ZF_3_4_L7:
  assumes A1: s∈AH r∈AH and A2: n∈G
  shows
    s(n) ∈ G (r(n))-1 ∈ G
    s(n)·(r(n))-1 ∈ G    s(r(n)) ∈ G
proof -
  from A1 A2 show
    s(n) ∈ G
    (r(n))-1 ∈ G
    s(r(n)) ∈ G
    s(n)·(r(n))-1 ∈ G
  using AlmostHoms_def apply_type
    group0_2_L1 monoid0.group0_1_L1 inverse_in_group
  by auto
qed

```

Type information related to the situation of three almost homomorphisms.

```

lemma (in group1) Group_ZF_3_4_L8:
  assumes A1: s∈AH r∈AH q∈AH and A2: n∈G
  shows
    q(n)∈G
    s(r(n)) ∈ G
    r(n)·(q(n))-1 ∈ G
    s(r(n)·(q(n))-1) ∈ G
    δ(s,⟨ q(n),r(n)·(q(n))-1⟩) ∈ G
proof -
  from A1 A2 show
    q(n)∈ G    s(r(n)) ∈ G    r(n)·(q(n))-1 ∈ G
  using AlmostHoms_def apply_type
    group0_2_L1 monoid0.group0_1_L1 inverse_in_group
  by auto
  with A1 A2 show s(r(n)·(q(n))-1) ∈ G
    δ(s,⟨ q(n),r(n)·(q(n))-1⟩) ∈ G
  using AlmostHoms_def apply_type Group_ZF_3_2_L4A
  by auto
qed

```

A formula useful in showing that the composition of almost homomorphisms is congruent with respect to the quotient group relation.

```

lemma (in group1) Group_ZF_3_4_L9:
  assumes A1: s1 ∈ AH r1 ∈ AH s2 ∈ AH r2 ∈ AH
  and A2: n∈G
  shows (s1or1)(n)·((s2or2)(n))-1 =
    s1(r2(n))·(s2(r2(n)))-1·s1(r1(n)·(r2(n))-1)·
    δ(s1,⟨ r2(n),r1(n)·(r2(n))-1⟩)
proof -
  from A1 A2 isAbelian have

```

```

      (s1or1)(n)·((s2or2)(n))-1 =
      s1(r2(n)·(r1(n)·(r2(n))-1))·(s2(r2(n)))-1
      using Group_ZF_3_4_L2 Group_ZF_3_4_L7 group0_4_L6A
      group_oper_assoc by simp
    with A1 A2 have (s1or1)(n)·((s2or2)(n))-1 = s1(r2(n))·
      s1(r1(n)·(r2(n))-1)·δ(s1,⟨ r2(n),r1(n)·(r2(n))-1⟩)·
      (s2(r2(n)))-1
      using Group_ZF_3_4_L8 Group_ZF_3_4_L1 by simp
    with A1 A2 isAbelian show thesis using
      Group_ZF_3_4_L8 group0_4_L7 by simp
  qed

```

The next lemma shows a formula that translates an expression in terms of the first group operation on almost homomorphisms and the group inverse in the group of almost homomorphisms to an expression using only the underlying group operations.

```

lemma (in group1) Group_ZF_3_4_L10: assumes A1: s ∈ AH  r ∈ AH
  and A2: n ∈ G
  shows (s·(GroupInv(AH,Op1)(r)))(n) = s(n)·(r(n))-1
proof -
  from A1 A2 show thesis
    using isAbelian Group_ZF_3_2_L13 Group_ZF_3_2_L12 Group_ZF_3_2_L14
    by simp
qed

```

A necessary condition for two a. h. to be almost equal.

```

lemma (in group1) Group_ZF_3_4_L11:
  assumes A1: s≈r
  shows {s(n)·(r(n))-1. n∈G} ∈ Fin(G)
proof -
  from A1 have s∈AH r∈AH
    using QuotientGroupRel_def by auto
  moreover from A1 have
    {(s·(GroupInv(AH,Op1)(r)))(n). n∈G} ∈ Fin(G)
    using QuotientGroupRel_def Finite1_L18 by simp
  ultimately show thesis
    using Group_ZF_3_4_L10 by simp
qed

```

A sufficient condition for two a. h. to be almost equal.

```

lemma (in group1) Group_ZF_3_4_L12: assumes A1: s∈AH  r∈AH
  and A2: {s(n)·(r(n))-1. n∈G} ∈ Fin(G)
  shows s≈r
proof -
  from groupAssum isAbelian A1 A2 show thesis
    using Group_ZF_3_2_L15 AlmostHoms_def
    Group_ZF_3_4_L10 Finite1_L19 QuotientGroupRel_def
    by simp

```

qed

Another sufficient condition for two a.h. to be almost equal. It is actually just an expansion of the definition of the quotient group relation.

```
lemma (in group1) Group_ZF_3_4_L12A: assumes s∈AH r∈AH
  and s·(GroupInv(AH,Op1)(r)) ∈ FR
  shows s≈r r≈s
```

```
proof -
  from assms show s≈r using assms QuotientGroupRel_def
    by simp
  then show r≈s by (rule Group_ZF_3_3_L3A)
```

qed

Another necessary condition for two a.h. to be almost equal. It is actually just an expansion of the definition of the quotient group relation.

```
lemma (in group1) Group_ZF_3_4_L12B: assumes s≈r
  shows s·(GroupInv(AH,Op1)(r)) ∈ FR
  using assms QuotientGroupRel_def by simp
```

The next lemma states the essential condition for the composition of a. h. to be congruent with respect to the quotient group relation for the subgroup of finite range functions.

```
lemma (in group1) Group_ZF_3_4_L13:
  assumes A1: s1≈s2 r1≈r2
  shows (s1◦r1) ≈ (s2◦r2)
proof -
  have {s1(r2(n))· (s2(r2(n)))-1. n∈G} ∈ Fin(G)
  proof -
    from A1 have ∀n∈G. r2(n) ∈ G
      using QuotientGroupRel_def AlmostHoms_def apply_funtype
      by auto
    moreover from A1 have {s1(n)·(s2(n))-1. n∈G} ∈ Fin(G)
      using Group_ZF_3_4_L11 by simp
    ultimately show thesis by (rule Finite1_L6B)
```

qed

```
moreover have {s1(r1(n)·(r2(n)))-1. n ∈ G} ∈ Fin(G)
```

```
proof -
  from A1 have ∀n∈G. s1(n)∈G
    using QuotientGroupRel_def AlmostHoms_def apply_funtype
    by auto
  moreover from A1 have {r1(n)·(r2(n))-1. n∈G} ∈ Fin(G)
    using Group_ZF_3_4_L11 by simp
  ultimately show thesis by (rule Finite1_L6C)
```

qed

ultimately have

```
{s1(r2(n))· (s2(r2(n)))-1·s1(r1(n)·(r2(n)))-1.
n∈G} ∈ Fin(G)
using group_oper_assocA Finite1_L15 by simp
```

```

moreover have
  { $\delta(s1, \langle r2(n), r1(n) \cdot (r2(n))^{-1} \rangle) \cdot n \in G\} \in \text{Fin}(G)$ 
proof -
  from A1 have  $\forall n \in G. \langle r2(n), r1(n) \cdot (r2(n))^{-1} \rangle \in G \times G$ 
    using QuotientGroupRel_def Group_ZF_3_4_L7 by auto
  moreover from A1 have  $\{\delta(s1, x) \cdot x \in G \times G\} \in \text{Fin}(G)$ 
    using QuotientGroupRel_def AlmostHoms_def by simp
  ultimately show thesis by (rule Finite1_L6B)
qed
ultimately have
  { $s1(r2(n)) \cdot (s2(r2(n)))^{-1} \cdot s1(r1(n) \cdot (r2(n))^{-1}) \cdot$ 
 $\delta(s1, \langle r2(n), r1(n) \cdot (r2(n))^{-1} \rangle) \cdot n \in G\} \in \text{Fin}(G)$ 
    using group_oper_assocA Finite1_L15 by simp
with A1 show thesis using
  QuotientGroupRel_def Group_ZF_3_4_L9
  Group_ZF_3_4_T1 Group_ZF_3_4_L12 by simp
qed

```

Composition of a. h. to is congruent with respect to the quotient group relation for the subgroup of finite range functions. Recall that if an operation say "o" on  $X$  is congruent with respect to an equivalence relation  $R$  then we can define the operation on the quotient space  $X/R$  by  $[s]_R \circ [r]_R := [s \circ r]_R$  and this definition will be correct i.e. it will not depend on the choice of representants for the classes  $[x]$  and  $[y]$ . This is why we want it here.

```

lemma (in group1) Group_ZF_3_4_L13A: shows
  Congruent2(QuotientGroupRel(AH, Op1, FR), Op2)
proof -
  show thesis using Group_ZF_3_4_L13 Congruent2_def
    by simp
qed

```

The homomorphism difference for the identity function is equal to the neutral element of the group (denoted  $e$  in the group1 context).

```

lemma (in group1) Group_ZF_3_4_L14: assumes A1:  $x \in G \times G$ 
shows  $\delta(\text{id}(G), x) = 1$ 
proof -
  from A1 show thesis using
    group0_2_L1 monoid0.group0_1_L1 HomDiff_def id_conv group0_2_L6
    by simp
qed

```

The identity function ( $I(x) = x$ ) on  $G$  is an almost homomorphism.

```

lemma (in group1) Group_ZF_3_4_L15: shows  $\text{id}(G) \in \text{AH}$ 
proof -
  have  $G \times G \neq 0$  using group0_2_L1 monoid0.group0_1_L3A
    by blast
  then show thesis using Group_ZF_3_4_L14 group0_2_L2
    id_type AlmostHoms_def by simp

```

qed

Almost homomorphisms form a monoid with composition. The identity function on the group is the neutral element there.

```

lemma (in group1) Group_ZF_3_4_L16:
  shows
    IsAmonoid(AH,Op2)
    monoid0(AH,Op2)
    id(G) = TheNeutralElement(AH,Op2)
proof-
  let i = TheNeutralElement(G→G,Composition(G))
  have
    IsAmonoid(G→G,Composition(G))
    monoid0(G→G,Composition(G))
    using monoid0_def Group_ZF_2_5_L2 by auto
  moreover have AH {is closed under} Composition(G)
    using Group_ZF_3_4_L6 by simp
  moreover have AH ⊆ G→G
    using AlmostHoms_def by auto
  moreover have i ∈ AH
    using Group_ZF_2_5_L2 Group_ZF_3_4_L15 by simp
  moreover have id(G) = i
    using Group_ZF_2_5_L2 by simp
  ultimately show
    IsAmonoid(AH,Op2)
    monoid0(AH,Op2)
    id(G) = TheNeutralElement(AH,Op2)
    using monoid0.group0_1_T1 group0_1_L6 AlHomOp2_def monoid0_def
    by auto

```

qed

We can project the monoid of almost homomorphisms with composition to the group of almost homomorphisms divided by the subgroup of finite range functions. The class of the identity function is the neutral element of the quotient (monoid).

```

theorem (in group1) Group_ZF_3_4_T2:
  assumes A1: R = QuotientGroupRel(AH,Op1,FR)
  shows
    IsAmonoid(AH//R,ProjFun2(AH,R,Op2))
    R{id(G)} = TheNeutralElement(AH//R,ProjFun2(AH,R,Op2))
proof -
  have group0(AH,Op1) using Group_ZF_3_2_L10A group0_def
    by simp
  with A1 groupAssum isAbelian show
    IsAmonoid(AH//R,ProjFun2(AH,R,Op2))
    R{id(G)} = TheNeutralElement(AH//R,ProjFun2(AH,R,Op2))
    using Group_ZF_3_3_L2 group0.Group_ZF_2_4_L3 Group_ZF_3_4_L13A
    Group_ZF_3_4_L16 monoid0.Group_ZF_2_2_T1 Group_ZF_2_2_L1
    by auto

```



qed

## 25.5 Shifting almost homomorphisms

In this section we consider what happens if we multiply an almost homomorphism by a group element. We show that the resulting function is also an a. h., and almost equal to the original one. This is used only for slopes (integer a.h.) in Int\_ZF\_2 where we need to correct a positive slopes by adding a constant, so that it is at least 2 on positive integers.

If  $s$  is an almost homomorphism and  $c$  is some constant from the group, then  $s \cdot c$  is an almost homomorphism.

```

lemma (in group1) Group_ZF_3_5_L1:
  assumes A1:  $s \in \text{AH}$  and A2:  $c \in G$  and
  A3:  $r = \{ \langle x, s(x) \cdot c \rangle. x \in G \}$ 
  shows
   $\forall x \in G. r(x) = s(x) \cdot c$ 
   $r \in \text{AH}$ 
   $s \approx r$ 
proof -
  from A1 A2 A3 have I:  $r: G \rightarrow G$ 
    using AlmostHoms_def apply_funtype group_op_closed
    ZF_fun_from_total by auto
  with A3 show II:  $\forall x \in G. r(x) = s(x) \cdot c$ 
    using ZF_fun_from_tot_val by simp
  with isAbelian A1 A2 have III:
     $\forall p \in G \times G. \delta(r, p) = \delta(s, p) \cdot c^{-1}$ 
    using group_op_closed AlmostHoms_def apply_funtype
    HomDiff_def group0_4_L7 by auto
  have  $\{ \delta(r, p). p \in G \times G \} \in \text{Fin}(G)$ 
  proof -
    from A1 A2 have
       $\{ \delta(s, p). p \in G \times G \} \in \text{Fin}(G)$   $c^{-1} \in G$ 
      using AlmostHoms_def inverse_in_group by auto
    then have  $\{ \delta(s, p) \cdot c^{-1}. p \in G \times G \} \in \text{Fin}(G)$ 
      using group_oper_assocA Finite1_L16AA
      by simp
    moreover from III have
       $\{ \delta(r, p). p \in G \times G \} = \{ \delta(s, p) \cdot c^{-1}. p \in G \times G \}$ 
      by (rule ZF1_1_L4B)
    ultimately show thesis by simp
  qed
  with I show IV:  $r \in \text{AH}$  using AlmostHoms_def
    by simp
  from isAbelian A1 A2 I II have
     $\forall n \in G. s(n) \cdot (r(n))^{-1} = c^{-1}$ 
    using AlmostHoms_def apply_funtype group0_4_L6AB
    by auto

```

```

then have {s(n)·(r(n))-1. n∈G} = {c-1. n∈G}
  by (rule ZF1_1_L4B)
with A1 A2 IV show s ≈ r
  using group0_2_L1 monoid0.group0_1_L3A
    inverse_in_group Group_ZF_3_4_L12 by simp
qed
end

```

## 26 DirectProduct\_ZF.thy

**theory** DirectProduct\_ZF **imports** func\_ZF

**begin**

This theory considers the direct product of binary operations. Contributed by Seo Sanghyeon.

### 26.1 Definition

In group theory the notion of direct product provides a natural way of creating a new group from two given groups.

Given  $(G, \cdot)$  and  $(H, \circ)$  a new operation  $(G \times H, \times)$  is defined as  $(g, h) \times (g', h') = (g \cdot g', h \circ h')$ .

**definition**

```
DirectProduct(P,Q,G,H)  $\equiv$ 
  { $\langle x, \langle P(\text{fst}(\text{fst}(x)), \text{fst}(\text{snd}(x))) \rangle$  ,  $Q(\text{snd}(\text{fst}(x)), \text{snd}(\text{snd}(x))) \rangle \rangle$  .
   $x \in (G \times H) \times (G \times H)$ }
```

We define a context called `direct0` which holds an assumption that  $P, Q$  are binary operations on  $G, H$ , resp. and denotes  $R$  as the direct product of  $(G, P)$  and  $(H, Q)$ .

```
locale direct0 =
  fixes P Q G H
  assumes Pfun: P : G  $\times$  G  $\rightarrow$  G
  assumes Qfun: Q : H  $\times$  H  $\rightarrow$  H
  fixes R
  defines Rdef [simp]: R  $\equiv$  DirectProduct(P,Q,G,H)
```

The direct product of binary operations is a binary operation.

```
lemma (in direct0) DirectProduct_ZF_1_L1:
  shows R : (G  $\times$  H)  $\times$  (G  $\times$  H)  $\rightarrow$  G  $\times$  H
proof -
  from Pfun Qfun have  $\forall x \in (G \times H) \times (G \times H).$ 
     $\langle P(\text{fst}(\text{fst}(x)), \text{fst}(\text{snd}(x))), Q(\text{snd}(\text{fst}(x)), \text{snd}(\text{snd}(x))) \rangle \in G \times H$ 
  by auto
  then show thesis using ZF_fun_from_total DirectProduct_def
  by simp
qed
```

And it has the intended value.

```
lemma (in direct0) DirectProduct_ZF_1_L2:
  shows  $\forall x \in (G \times H). \forall y \in (G \times H).$ 
     $R\langle x, y \rangle = \langle P(\text{fst}(x), \text{fst}(y)), Q(\text{snd}(x), \text{snd}(y)) \rangle$ 
  using DirectProduct_def DirectProduct_ZF_1_L1 ZF_fun_from_tot_val
```

by simp

And the value belongs to the set the operation is defined on.

```
lemma (in direct0) DirectProduct_ZF_1_L3:
  shows  $\forall x \in (G \times H). \forall y \in (G \times H). R\langle x, y \rangle \in G \times H$ 
  using DirectProduct_ZF_1_L1 by simp
```

## 26.2 Associative and commutative operations

If  $P$  and  $Q$  are both associative or commutative operations, the direct product of  $P$  and  $Q$  has the same property.

Direct product of commutative operations is commutative.

```
lemma (in direct0) DirectProduct_ZF_2_L1:
  assumes  $P \text{ \{is commutative on\} } G$  and  $Q \text{ \{is commutative on\} } H$ 
  shows  $R \text{ \{is commutative on\} } G \times H$ 
proof -
  from assms have  $\forall x \in (G \times H). \forall y \in (G \times H). R\langle x, y \rangle = R\langle y, x \rangle$ 
    using DirectProduct_ZF_1_L2 IsCommutative_def by simp
  then show thesis using IsCommutative_def by simp
qed
```

Direct product of associative operations is associative.

```
lemma (in direct0) DirectProduct_ZF_2_L2:
  assumes  $P \text{ \{is associative on\} } G$  and  $Q \text{ \{is associative on\} } H$ 
  shows  $R \text{ \{is associative on\} } G \times H$ 
proof -
  have  $\forall x \in G \times H. \forall y \in G \times H. \forall z \in G \times H. R\langle R\langle x, y \rangle, z \rangle =$ 
     $\langle P\langle P\langle \text{fst}(x), \text{fst}(y) \rangle, \text{fst}(z) \rangle, Q\langle Q\langle \text{snd}(x), \text{snd}(y) \rangle, \text{snd}(z) \rangle \rangle$ 
    using DirectProduct_ZF_1_L2 DirectProduct_ZF_1_L3
    by auto
  moreover have  $\forall x \in G \times H. \forall y \in G \times H. \forall z \in G \times H. R\langle x, R\langle y, z \rangle \rangle =$ 
     $\langle P\langle \text{fst}(x), P\langle \text{fst}(y), \text{fst}(z) \rangle \rangle, Q\langle \text{snd}(x), Q\langle \text{snd}(y), \text{snd}(z) \rangle \rangle$ 
    using DirectProduct_ZF_1_L2 DirectProduct_ZF_1_L3 by auto
  ultimately have  $\forall x \in G \times H. \forall y \in G \times H. \forall z \in G \times H. R\langle R\langle x, y \rangle, z \rangle = R\langle x, R\langle y, z \rangle \rangle$ 
    using assms IsAssociative_def by simp
  then show thesis
    using DirectProduct_ZF_1_L1 IsAssociative_def by simp
qed

end
```

## 27 OrderedGroup\_ZF.thy

**theory** OrderedGroup\_ZF **imports** Group\_ZF\_1 AbelianGroup\_ZF Order\_ZF Finite\_ZF\_1

**begin**

This theory file defines and shows the basic properties of (partially or linearly) ordered groups. We define the set of nonnegative elements and the absolute value function. We show that in linearly ordered groups finite sets are bounded and provide a sufficient condition for bounded sets to be finite. This allows to show in Int\_ZF\_IML.thy that subsets of integers are bounded iff they are finite.

### 27.1 Ordered groups

This section defines ordered groups and various related notions.

An ordered group is a group equipped with a partial order that is "translation invariant", that is if  $a \leq b$  then  $a \cdot g \leq b \cdot g$  and  $g \cdot a \leq g \cdot b$ .

**definition**

$$\begin{aligned} \text{IsAnOrdGroup}(G, P, r) \equiv & \\ & (\text{IsAGroup}(G, P) \wedge r \subseteq G \times G \wedge \text{IsPartOrder}(G, r) \wedge (\forall g \in G. \forall a \ b. \\ & \langle a, b \rangle \in r \longrightarrow \langle P\langle a, g \rangle, P\langle b, g \rangle \rangle \in r \wedge \langle P\langle g, a \rangle, P\langle g, b \rangle \rangle \in r) ) \end{aligned}$$

We define the set of nonnegative elements in the obvious way as  $G^+ = \{x \in G : 1 \leq x\}$ .

**definition**

$$\text{Nonnegative}(G, P, r) \equiv \{x \in G. \langle \text{TheNeutralElement}(G, P), x \rangle \in r\}$$

The  $\text{PositiveSet}(G, P, r)$  is a set similar to  $\text{Nonnegative}(G, P, r)$ , but without the unit.

**definition**

$$\begin{aligned} \text{PositiveSet}(G, P, r) \equiv & \\ \{x \in G. \langle \text{TheNeutralElement}(G, P), x \rangle \in r \wedge \text{TheNeutralElement}(G, P) \neq x\} & \end{aligned}$$

We also define the absolute value as a ZF-function that is the identity on  $G^+$  and the group inverse on the rest of the group.

**definition**

$$\begin{aligned} \text{AbsoluteValue}(G, P, r) \equiv & \text{id}(\text{Nonnegative}(G, P, r)) \cup \\ & \text{restrict}(\text{GroupInv}(G, P), G - \text{Nonnegative}(G, P, r)) \end{aligned}$$

The odd functions are defined as those having property  $f(a^{-1}) = (f(a))^{-1}$ . This looks a bit strange in the multiplicative notation, I have to admit. For linearly ordered groups a function  $f$  defined on the set of positive elements uniquely defines an odd function of the whole group. This function is called an odd extension of  $f$

**definition**

```

OddExtension(G,P,r,f) ≡
(f ∪ {⟨a, GroupInv(G,P)(f(GroupInv(G,P)(a)))⟩}.
a ∈ GroupInv(G,P)(PositiveSet(G,P,r))} ∪
{⟨TheNeutralElement(G,P),TheNeutralElement(G,P)⟩})

```

We will use a similar notation for ordered groups as for the generic groups.  $G^+$  denotes the set of nonnegative elements (that satisfy  $1 \leq a$ ) and  $G_+$  is the set of (strictly) positive elements.  $-A$  is the set inverses of elements from  $A$ . I hope that using additive notation for this notion is not too shocking here. The symbol  $f^\circ$  denotes the odd extension of  $f$ . For a function defined on  $G_+$  this is the unique odd function on  $G$  that is equal to  $f$  on  $G_+$ .

**locale group3 =**

**fixes G and P and r**

**assumes** ordGroupAssum: IsAnOrdGroup(G,P,r)

**fixes** unit (1)

**defines** unit\_def [simp]: 1 ≡ TheNeutralElement(G,P)

**fixes** proper (infixl · 70)

**defines** proper\_def [simp]:  $a \cdot b \equiv P\langle a, b \rangle$

**fixes** inv ( $_^{-1}$  [90] 91)

**defines** inv\_def [simp]:  $x^{-1} \equiv \text{GroupInv}(G,P)(x)$

**fixes** lesseq (infix  $\leq$  68)

**defines** lesseq\_def [simp]:  $a \leq b \equiv \langle a, b \rangle \in r$

**fixes** sless (infix < 68)

**defines** sless\_def [simp]:  $a < b \equiv a \leq b \wedge a \neq b$

**fixes** nonnegative ( $G^+$ )

**defines** nonnegative\_def [simp]:  $G^+ \equiv \text{Nonnegative}(G,P,r)$

**fixes** positive ( $G_+$ )

**defines** positive\_def [simp]:  $G_+ \equiv \text{PositiveSet}(G,P,r)$

**fixes** setinv ( $-$  \_ 72)

**defines** setninv\_def [simp]:  $-A \equiv \text{GroupInv}(G,P)(A)$

**fixes** abs ( $|$  \_  $|$ )

**defines** abs\_def [simp]:  $|a| \equiv \text{AbsoluteValue}(G,P,r)(a)$

**fixes** oddext ( $_^\circ$ )

**defines** oddext\_def [simp]:  $f^\circ \equiv \text{OddExtension}(G,P,r,f)$

In group3 context we can use the theorems proven in the group0 context.

```
lemma (in group3) OrderedGroup_ZF_1_L1: shows group0(G,P)
  using ordGroupAssum IsAnOrdGroup_def group0_def by simp
```

Ordered group (carrier) is not empty. This is a property of monoids, but it is good to have it handy in the group3 context.

```
lemma (in group3) OrderedGroup_ZF_1_L1A: shows  $G \neq 0$ 
  using OrderedGroup_ZF_1_L1 group0.group0_2_L1 monoid0.group0_1_L3A
  by blast
```

The next lemma is just to see the definition of the nonnegative set in our notation.

```
lemma (in group3) OrderedGroup_ZF_1_L2:
  shows  $g \in G^+ \longleftrightarrow 1 \leq g$ 
  using ordGroupAssum IsAnOrdGroup_def Nonnegative_def
  by auto
```

The next lemma is just to see the definition of the positive set in our notation.

```
lemma (in group3) OrderedGroup_ZF_1_L2A:
  shows  $g \in G_+ \longleftrightarrow (1 \leq g \wedge g \neq 1)$ 
  using ordGroupAssum IsAnOrdGroup_def PositiveSet_def
  by auto
```

For total order if  $g$  is not in  $G^+$ , then it has to be less or equal the unit.

```
lemma (in group3) OrderedGroup_ZF_1_L2B:
  assumes A1:  $r \text{ {is total on} } G$  and A2:  $a \in G - G^+$ 
  shows  $a \leq 1$ 
proof -
  from A2 have  $a \in G \quad 1 \in G \quad \neg(1 \leq a)$ 
  using OrderedGroup_ZF_1_L1 group0.group0_2_L2 OrderedGroup_ZF_1_L2
  by auto
  with A1 show thesis using IsTotal_def by auto
qed
```

The group order is reflexive.

```
lemma (in group3) OrderedGroup_ZF_1_L3: assumes  $g \in G$ 
  shows  $g \leq g$ 
  using ordGroupAssum assms IsAnOrdGroup_def IsPartOrder_def refl_def
  by simp
```

1 is nonnegative.

```
lemma (in group3) OrderedGroup_ZF_1_L3A: shows  $1 \in G^+$ 
  using OrderedGroup_ZF_1_L2 OrderedGroup_ZF_1_L3
  OrderedGroup_ZF_1_L1 group0.group0_2_L2 by simp
```

In this context  $a \leq b$  implies that both  $a$  and  $b$  belong to  $G$ .

```
lemma (in group3) OrderedGroup_ZF_1_L4:
```

```

assumes  $a \leq b$  shows  $a \in G \ b \in G$ 
using ordGroupAssum assms IsAnOrdGroup_def by auto

```

It is good to have transitivity handy.

```

lemma (in group3) Group_order_transitive:
  assumes A1:  $a \leq b \ b \leq c$  shows  $a \leq c$ 
proof -
  from ordGroupAssum have trans(r)
    using IsAnOrdGroup_def IsPartOrder_def
    by simp
  moreover from A1 have  $\langle a, b \rangle \in r \wedge \langle b, c \rangle \in r$  by simp
  ultimately have  $\langle a, c \rangle \in r$  by (rule Fol1_L3)
  thus thesis by simp
qed

```

The order in an ordered group is antisymmetric.

```

lemma (in group3) group_order_antisym:
  assumes A1:  $a \leq b \ b \leq a$  shows  $a = b$ 
proof -
  from ordGroupAssum A1 have
    antisym(r)  $\langle a, b \rangle \in r \ \langle b, a \rangle \in r$ 
    using IsAnOrdGroup_def IsPartOrder_def by auto
  then show  $a = b$  by (rule Fol1_L4)
qed

```

Transitivity for the strict order: if  $a < b$  and  $b \leq c$ , then  $a < c$ .

```

lemma (in group3) OrderedGroup_ZF_1_L4A:
  assumes A1:  $a < b$  and A2:  $b \leq c$ 
  shows  $a < c$ 
proof -
  from A1 A2 have  $a \leq b \ b \leq c$  by auto
  then have  $a \leq c$  by (rule Group_order_transitive)
  moreover from A1 A2 have  $a \neq c$  using group_order_antisym by auto
  ultimately show  $a < c$  by simp
qed

```

Another version of transitivity for the strict order: if  $a \leq b$  and  $b < c$ , then  $a < c$ .

```

lemma (in group3) group_strict_ord_transit:
  assumes A1:  $a \leq b$  and A2:  $b < c$ 
  shows  $a < c$ 
proof -
  from A1 A2 have  $a \leq b \ b \leq c$  by auto
  then have  $a \leq c$  by (rule Group_order_transitive)
  moreover from A1 A2 have  $a \neq c$  using group_order_antisym by auto
  ultimately show  $a < c$  by simp
qed

```

Strict order is preserved by translations.



```

lemma (in group3) group_strict_ord_transl_inv:
  assumes a<b and c∈G
  shows
    a·c < b·c
    c·a < c·b
  using ordGroupAssum assms IsAnOrdGroup_def
    OrderedGroup_ZF_1_L4 OrderedGroup_ZF_1_L1 group0.group0_2_L19
  by auto

```

If the group order is total, then the group is ordered linearly.

```

lemma (in group3) group_ord_total_is_lin:
  assumes r {is total on} G
  shows IsLinOrder(G,r)
  using assms ordGroupAssum IsAnOrdGroup_def Order_ZF_1_L3
  by simp

```

For linearly ordered groups elements in the nonnegative set are greater than those in the complement.

```

lemma (in group3) OrderedGroup_ZF_1_L4B:
  assumes r {is total on} G
  and a∈G+ and b ∈ G-G+
  shows b≤a
proof -
  from assms have b≤1 1≤a
    using OrderedGroup_ZF_1_L2 OrderedGroup_ZF_1_L2B by auto
  then show thesis by (rule Group_order_transitive)
qed

```

If  $a \leq 1$  and  $a \neq 1$ , then  $a \in G \setminus G^+$ .

```

lemma (in group3) OrderedGroup_ZF_1_L4C:
  assumes A1: a≤1 and A2: a≠1
  shows a ∈ G-G+
proof -
  { assume a ∉ G-G+
    with ordGroupAssum A1 A2 have False
      using OrderedGroup_ZF_1_L4 OrderedGroup_ZF_1_L2
    OrderedGroup_ZF_1_L4 IsAnOrdGroup_def IsPartOrder_def antisym_def
    by auto
  } thus thesis by auto
qed

```

An element smaller than an element in  $G \setminus G^+$  is in  $G \setminus G^+$ .

```

lemma (in group3) OrderedGroup_ZF_1_L4D:
  assumes A1: a∈G-G+ and A2: b≤a
  shows b∈G-G+
proof -
  { assume b ∉ G - G+
    with A2 have 1≤b b≤a

```

```

    using OrderedGroup_ZF_1_L4 OrderedGroup_ZF_1_L2 by auto
    then have  $1 \leq a$  by (rule Group_order_transitive)
    with A1 have False using OrderedGroup_ZF_1_L2 by simp
  } thus thesis by auto
qed

```

The nonnegative set is contained in the group.

```

lemma (in group3) OrderedGroup_ZF_1_L4E: shows  $G^+ \subseteq G$ 
  using OrderedGroup_ZF_1_L2 OrderedGroup_ZF_1_L4 by auto

```

Taking the inverse on both sides reverses the inequality.

```

lemma (in group3) OrderedGroup_ZF_1_L5:
  assumes A1:  $a \leq b$  shows  $b^{-1} \leq a^{-1}$ 
proof -
  from A1 have T1:  $a \in G$   $b \in G$   $a^{-1} \in G$   $b^{-1} \in G$ 
    using OrderedGroup_ZF_1_L4 OrderedGroup_ZF_1_L1
    group0.inverse_in_group by auto
  with A1 ordGroupAssum have  $a \cdot a^{-1} \leq b \cdot a^{-1}$  using IsAnOrdGroup_def
    by simp
  with T1 ordGroupAssum have  $b^{-1} \cdot 1 \leq b^{-1} \cdot (b \cdot a^{-1})$ 
    using OrderedGroup_ZF_1_L1 group0.group0_2_L6 IsAnOrdGroup_def
    by simp
  with T1 show thesis using
    OrderedGroup_ZF_1_L1 group0.group0_2_L2 group0.group_oper_assoc
    group0.group0_2_L6 by simp
qed

```

If an element is smaller than the unit, then its inverse is greater.

```

lemma (in group3) OrderedGroup_ZF_1_L5A:
  assumes A1:  $a \leq 1$  shows  $1 \leq a^{-1}$ 
proof -
  from A1 have  $1^{-1} \leq a^{-1}$  using OrderedGroup_ZF_1_L5
    by simp
  then show thesis using OrderedGroup_ZF_1_L1 group0.group_inv_of_one

    by simp
qed

```

If an the inverse of an element is greater than the unit, then the element is smaller.

```

lemma (in group3) OrderedGroup_ZF_1_L5AA:
  assumes A1:  $a \in G$  and A2:  $1 \leq a^{-1}$ 
  shows  $a \leq 1$ 
proof -
  from A2 have  $(a^{-1})^{-1} \leq 1^{-1}$  using OrderedGroup_ZF_1_L5
    by simp
  with A1 show  $a \leq 1$ 
    using OrderedGroup_ZF_1_L1 group0.group_inv_of_inv group0.group_inv_of_one

```

by simp  
qed

If an element is nonnegative, then the inverse is not greater than the unit.  
Also shows that nonnegative elements cannot be negative

```
lemma (in group3) OrderedGroup_ZF_1_L5AB:
  assumes A1:  $1 \leq a$  shows  $a^{-1} \leq 1$  and  $\neg(a \leq 1 \wedge a \neq 1)$ 
proof -
  from A1 have  $a^{-1} \leq 1^{-1}$ 
  using OrderedGroup_ZF_1_L5 by simp
  then show  $a^{-1} \leq 1$  using OrderedGroup_ZF_1_L1 group0.group_inv_of_one
  by simp
  { assume  $a \leq 1$  and  $a \neq 1$ 
    with A1 have False using group_order_antisym
    by blast
  } then show  $\neg(a \leq 1 \wedge a \neq 1)$  by auto
qed
```

If two elements are greater or equal than the unit, then the inverse of one is not greater than the other.

```
lemma (in group3) OrderedGroup_ZF_1_L5AC:
  assumes A1:  $1 \leq a$   $1 \leq b$ 
  shows  $a^{-1} \leq b$ 
proof -
  from A1 have  $a^{-1} \leq 1$   $1 \leq b$ 
  using OrderedGroup_ZF_1_L5AB by auto
  then show  $a^{-1} \leq b$  by (rule Group_order_transitive)
qed
```

## 27.2 Inequalities

This section develops some simple tools to deal with inequalities.

Taking negative on both sides reverses the inequality, case with an inverse on one side.

```
lemma (in group3) OrderedGroup_ZF_1_L5AD:
  assumes A1:  $b \in G$  and A2:  $a \leq b^{-1}$ 
  shows  $b \leq a^{-1}$ 
proof -
  from A2 have  $(b^{-1})^{-1} \leq a^{-1}$ 
  using OrderedGroup_ZF_1_L5 by simp
  with A1 show  $b \leq a^{-1}$ 
  using OrderedGroup_ZF_1_L1 group0.group_inv_of_inv
  by simp
qed
```

We can cancel the same element on both sides of an inequality.

```
lemma (in group3) OrderedGroup_ZF_1_L5AE:
```

```

    assumes A1: a ∈ G  b ∈ G  c ∈ G and A2: a · b ≤ a · c
    shows b ≤ c
  proof -
    from ordGroupAssum A1 A2 have a-1 · (a · b) ≤ a-1 · (a · c)
      using OrderedGroup_ZF_1_L1 group0.inverse_in_group
      IsAnOrdGroup_def by simp
    with A1 show b ≤ c
      using OrderedGroup_ZF_1_L1 group0.inv_cancel_two
      by simp
  qed

```

We can cancel the same element on both sides of an inequality, a version with an inverse on both sides.

```

lemma (in group3) OrderedGroup_ZF_1_L5AF:
  assumes A1: a ∈ G  b ∈ G  c ∈ G and A2: a · b-1 ≤ a · c-1
  shows c ≤ b
proof -
  from A1 A2 have (c-1)-1 ≤ (b-1)-1
    using OrderedGroup_ZF_1_L1 group0.inverse_in_group
    OrderedGroup_ZF_1_L5AE OrderedGroup_ZF_1_L5 by simp
  with A1 show c ≤ b
    using OrderedGroup_ZF_1_L1 group0.group_inv_of_inv by simp
qed

```

Taking negative on both sides reverses the inequality, another case with an inverse on one side.

```

lemma (in group3) OrderedGroup_ZF_1_L5AG:
  assumes A1: a ∈ G and A2: a-1 ≤ b
  shows b-1 ≤ a
proof -
  from A2 have b-1 ≤ (a-1)-1
    using OrderedGroup_ZF_1_L5 by simp
  with A1 show b-1 ≤ a
    using OrderedGroup_ZF_1_L1 group0.group_inv_of_inv
    by simp
qed

```

We can multiply the sides of two inequalities.

```

lemma (in group3) OrderedGroup_ZF_1_L5B:
  assumes A1: a ≤ b and A2: c ≤ d
  shows a · c ≤ b · d
proof -
  from A1 A2 have c ∈ G b ∈ G using OrderedGroup_ZF_1_L4 by auto
  with A1 A2 ordGroupAssum have a · c ≤ b · c b · c ≤ b · d
    using IsAnOrdGroup_def by auto
  then show a · c ≤ b · d by (rule Group_order_transitive)
qed

```

We can replace first of the factors on one side of an inequality with a greater

one.

```
lemma (in group3) OrderedGroup_ZF_1_L5C:
  assumes A1:  $c \in G$  and A2:  $a \leq b \cdot c$  and A3:  $b \leq b_1$ 
  shows  $a \leq b_1 \cdot c$ 
proof -
  from A1 A3 have  $b \cdot c \leq b_1 \cdot c$ 
    using OrderedGroup_ZF_1_L3 OrderedGroup_ZF_1_L5B by simp
  with A2 show  $a \leq b_1 \cdot c$  by (rule Group_order_transitive)
qed
```

We can replace second of the factors on one side of an inequality with a greater one.

```
lemma (in group3) OrderedGroup_ZF_1_L5D:
  assumes A1:  $b \in G$  and A2:  $a \leq b \cdot c$  and A3:  $c \leq b_1$ 
  shows  $a \leq b \cdot b_1$ 
proof -
  from A1 A3 have  $b \cdot c \leq b \cdot b_1$ 
    using OrderedGroup_ZF_1_L3 OrderedGroup_ZF_1_L5B by auto
  with A2 show  $a \leq b \cdot b_1$  by (rule Group_order_transitive)
qed
```

We can replace factors on one side of an inequality with greater ones.

```
lemma (in group3) OrderedGroup_ZF_1_L5E:
  assumes A1:  $a \leq b \cdot c$  and A2:  $b \leq b_1$   $c \leq c_1$ 
  shows  $a \leq b_1 \cdot c_1$ 
proof -
  from A2 have  $b \cdot c \leq b_1 \cdot c_1$  using OrderedGroup_ZF_1_L5B
    by simp
  with A1 show  $a \leq b_1 \cdot c_1$  by (rule Group_order_transitive)
qed
```

We don't decrease an element of the group by multiplying by one that is nonnegative.

```
lemma (in group3) OrderedGroup_ZF_1_L5F:
  assumes A1:  $1 \leq a$  and A2:  $b \in G$ 
  shows  $b \leq a \cdot b$   $b \leq b \cdot a$ 
proof -
  from ordGroupAssum A1 A2 have
     $1 \cdot b \leq a \cdot b$   $b \cdot 1 \leq b \cdot a$ 
    using IsAnOrdGroup_def by auto
  with A2 show  $b \leq a \cdot b$   $b \leq b \cdot a$ 
    using OrderedGroup_ZF_1_L1 group0.group0_2_L2
    by auto
qed
```

We can multiply the right hand side of an inequality by a nonnegative element.

```
lemma (in group3) OrderedGroup_ZF_1_L5G: assumes A1:  $a \leq b$ 
```

```

    and A2:  $1 \leq c$  shows  $a \leq b \cdot c$   $a \leq c \cdot b$ 
  proof -
    from A1 A2 have I:  $b \leq b \cdot c$  and II:  $b \leq c \cdot b$ 
    using OrderedGroup_ZF_1_L4 OrderedGroup_ZF_1_L5F by auto
    from A1 I show  $a \leq b \cdot c$  by (rule Group_order_transitive)
    from A1 II show  $a \leq c \cdot b$  by (rule Group_order_transitive)
  qed

```

We can put two elements on the other side of inequality, changing their sign.

```

lemma (in group3) OrderedGroup_ZF_1_L5H:
  assumes A1:  $a \in G$   $b \in G$  and A2:  $a \cdot b^{-1} \leq c$ 
  shows
     $a \leq c \cdot b$ 
     $c^{-1} \cdot a \leq b$ 
  proof -
    from A2 have T:  $c \in G$   $c^{-1} \in G$ 
    using OrderedGroup_ZF_1_L4 OrderedGroup_ZF_1_L1
    group0.inverse_in_group by auto
    from ordGroupAssum A1 A2 have  $a \cdot b^{-1} \cdot b \leq c \cdot b$ 
    using IsAnOrdGroup_def by simp
    with A1 show  $a \leq c \cdot b$ 
    using OrderedGroup_ZF_1_L1 group0.inv_cancel_two
    by simp
    with ordGroupAssum A2 T have  $c^{-1} \cdot a \leq c^{-1} \cdot (c \cdot b)$ 
    using IsAnOrdGroup_def by simp
    with A1 T show  $c^{-1} \cdot a \leq b$ 
    using OrderedGroup_ZF_1_L1 group0.inv_cancel_two
    by simp
  qed

```

We can multiply the sides of one inequality by inverse of another.

```

lemma (in group3) OrderedGroup_ZF_1_L5I:
  assumes  $a \leq b$  and  $c \leq d$ 
  shows  $a \cdot d^{-1} \leq b \cdot c^{-1}$ 
  using assms OrderedGroup_ZF_1_L5 OrderedGroup_ZF_1_L5B
  by simp

```

We can put an element on the other side of an inequality changing its sign, version with the inverse.

```

lemma (in group3) OrderedGroup_ZF_1_L5J:
  assumes A1:  $a \in G$   $b \in G$  and A2:  $c \leq a \cdot b^{-1}$ 
  shows  $c \cdot b \leq a$ 
  proof -
    from ordGroupAssum A1 A2 have  $c \cdot b \leq a \cdot b^{-1} \cdot b$ 
    using IsAnOrdGroup_def by simp
    with A1 show  $c \cdot b \leq a$ 
    using OrderedGroup_ZF_1_L1 group0.inv_cancel_two
    by simp
  qed

```

We can put an element on the other side of an inequality changing its sign, version with the inverse.

```
lemma (in group3) OrderedGroup_ZF_1_L5JA:
  assumes A1:  $a \in G$   $b \in G$  and A2:  $c \leq a^{-1} \cdot b$ 
  shows  $a \cdot c \leq b$ 
proof -
  from ordGroupAssum A1 A2 have  $a \cdot c \leq a \cdot (a^{-1} \cdot b)$ 
    using IsAnOrdGroup_def by simp
  with A1 show  $a \cdot c \leq b$ 
    using OrderedGroup_ZF_1_L1 group0.inv_cancel_two
    by simp
qed
```

A special case of OrderedGroup\_ZF\_1\_L5J where  $c = 1$ .

```
corollary (in group3) OrderedGroup_ZF_1_L5K:
  assumes A1:  $a \in G$   $b \in G$  and A2:  $1 \leq a \cdot b^{-1}$ 
  shows  $b \leq a$ 
proof -
  from A1 A2 have  $1 \cdot b \leq a$ 
    using OrderedGroup_ZF_1_L5J by simp
  with A1 show  $b \leq a$ 
    using OrderedGroup_ZF_1_L1 group0.group0_2_L2
    by simp
qed
```

A special case of OrderedGroup\_ZF\_1\_L5JA where  $c = 1$ .

```
corollary (in group3) OrderedGroup_ZF_1_L5KA:
  assumes A1:  $a \in G$   $b \in G$  and A2:  $1 \leq a^{-1} \cdot b$ 
  shows  $a \leq b$ 
proof -
  from A1 A2 have  $a \cdot 1 \leq b$ 
    using OrderedGroup_ZF_1_L5JA by simp
  with A1 show  $a \leq b$ 
    using OrderedGroup_ZF_1_L1 group0.group0_2_L2
    by simp
qed
```

If the order is total, the elements that do not belong to the positive set are negative. We also show here that the group inverse of an element that does not belong to the nonnegative set does belong to the nonnegative set.

```
lemma (in group3) OrderedGroup_ZF_1_L6:
  assumes A1:  $r$  {is total on}  $G$  and A2:  $a \in G - G^+$ 
  shows  $a \leq 1$   $a^{-1} \in G^+$  restrict(GroupInv( $G, P$ ),  $G - G^+$ )( $a$ )  $\in G^+$ 
proof -
  from A2 have T1:  $a \in G$   $a \notin G^+$   $1 \in G$ 
    using OrderedGroup_ZF_1_L1 group0.group0_2_L2 by auto
  with A1 show  $a \leq 1$  using OrderedGroup_ZF_1_L2 IsTotal_def
    by auto
```

```

then show  $a^{-1} \in G^+$  using OrderedGroup_ZF_1_L5A OrderedGroup_ZF_1_L2
  by simp
with A2 show  $\text{restrict}(\text{GroupInv}(G,P), G-G^+)(a) \in G^+$ 
  using restrict by simp
qed

```

If a property is invariant with respect to taking the inverse and it is true on the nonnegative set, then it is true on the whole group.

```

lemma (in group3) OrderedGroup_ZF_1_L7:
  assumes A1:  $r$  {is total on}  $G$ 
  and A2:  $\forall a \in G^+. \forall b \in G^+. Q(a,b)$ 
  and A3:  $\forall a \in G. \forall b \in G. Q(a,b) \longrightarrow Q(a^{-1}, b)$ 
  and A4:  $\forall a \in G. \forall b \in G. Q(a,b) \longrightarrow Q(a, b^{-1})$ 
  and A5:  $a \in G \implies b \in G$ 
  shows  $Q(a,b)$ 
proof -
  { assume A6:  $a \in G^+$  have  $Q(a,b)$ 
    proof -
      { assume  $b \in G^+$ 
with A6 A2 have  $Q(a,b)$  by simp }
      moreover
      { assume  $b \notin G^+$ 
with A1 A2 A4 A5 A6 have  $Q(a, (b^{-1})^{-1})$ 
  using OrderedGroup_ZF_1_L6 OrderedGroup_ZF_1_L1 group0.inverse_in_group
  by simp
with A5 have  $Q(a,b)$  using OrderedGroup_ZF_1_L1 group0.group_inv_of_inv
  by simp }
      ultimately show  $Q(a,b)$  by auto
    qed }
  moreover
  { assume  $a \notin G^+$ 
with A1 A5 have T1:  $a^{-1} \in G^+$  using OrderedGroup_ZF_1_L6 by simp
  have  $Q(a,b)$ 
  proof -
    { assume  $b \in G^+$ 
with A2 A3 A5 T1 have  $Q((a^{-1})^{-1}, b)$ 
  using OrderedGroup_ZF_1_L1 group0.inverse_in_group by simp
with A5 have  $Q(a,b)$  using OrderedGroup_ZF_1_L1 group0.group_inv_of_inv
  by simp }
    moreover
    { assume  $b \notin G^+$ 
with A1 A2 A3 A4 A5 T1 have  $Q((a^{-1})^{-1}, (b^{-1})^{-1})$ 
  using OrderedGroup_ZF_1_L6 OrderedGroup_ZF_1_L1 group0.inverse_in_group
  by simp
with A5 have  $Q(a,b)$  using OrderedGroup_ZF_1_L1 group0.group_inv_of_inv
  by simp }
    ultimately show  $Q(a,b)$  by auto
  qed }
  ultimately show  $Q(a,b)$  by auto

```



qed

A lemma about splitting the ordered group "plane" into 6 subsets. Useful for proofs by cases.

```
lemma (in group3) OrdGroup_6cases: assumes A1: r {is total on} G
  and A2: a ∈ G b ∈ G
  shows
     $1 \leq a \wedge 1 \leq b \vee a \leq 1 \wedge b \leq 1 \vee$ 
 $a \leq 1 \wedge 1 \leq b \wedge 1 \leq a \cdot b \vee a \leq 1 \wedge 1 \leq b \wedge a \cdot b \leq 1 \vee$ 
 $1 \leq a \wedge b \leq 1 \wedge 1 \leq a \cdot b \vee 1 \leq a \wedge b \leq 1 \wedge a \cdot b \leq 1$ 
  proof -
    from A1 A2 have
       $1 \leq a \vee a \leq 1$ 
       $1 \leq b \vee b \leq 1$ 
       $1 \leq a \cdot b \vee a \cdot b \leq 1$ 
    using OrderedGroup_ZF_1_L1 group0.group_op_closed group0.group0_2_L2
      IsTotal_def by auto
    then show thesis by auto
  qed
```

The next lemma shows what happens when one element of a totally ordered group is not greater or equal than another.

```
lemma (in group3) OrderedGroup_ZF_1_L8:
  assumes A1: r {is total on} G
  and A2: a ∈ G b ∈ G
  and A3:  $\neg(a \leq b)$ 
  shows  $b \leq a \wedge a^{-1} \leq b^{-1} \wedge a \neq b \wedge b < a$ 
  proof -
    from A1 A2 A3 show I:  $b \leq a$  using IsTotal_def
      by auto
    then show  $a^{-1} \leq b^{-1}$  using OrderedGroup_ZF_1_L5 by simp
    from A2 have  $a \leq a$  using OrderedGroup_ZF_1_L3 by simp
    with I A3 show  $a \neq b \wedge b < a$  by auto
  qed
```

If one element is greater or equal and not equal to another, then it is not smaller or equal.

```
lemma (in group3) OrderedGroup_ZF_1_L8AA:
  assumes A1:  $a \leq b$  and A2:  $a \neq b$ 
  shows  $\neg(b \leq a)$ 
  proof -
    { note A1
      moreover assume  $b \leq a$ 
      ultimately have  $a = b$  by (rule group_order_antisym)
      with A2 have False by simp
    } thus  $\neg(b \leq a)$  by auto
  qed
```

A special case of OrderedGroup\_ZF\_1\_L8 when one of the elements is the unit.

```

corollary (in group3) OrderedGroup_ZF_1_L8A:
  assumes A1: r {is total on} G
  and A2: a ∈ G and A3: ¬(1 ≤ a)
  shows 1 ≤ a-1 1 ≠ a a ≤ 1
proof -
  from A1 A2 A3 have I:
    r {is total on} G
    1 ∈ G a ∈ G
    ¬(1 ≤ a)
  using OrderedGroup_ZF_1_L1 group0.group0_2_L2
  by auto
  then have 1-1 ≤ a-1
    by (rule OrderedGroup_ZF_1_L8)
  then show 1 ≤ a-1
    using OrderedGroup_ZF_1_L1 group0.group_inv_of_one by simp
  from I show 1 ≠ a by (rule OrderedGroup_ZF_1_L8)
  from A1 I show a ≤ 1 using IsTotal_def
    by auto
qed

```

A negative element can not be nonnegative.

```

lemma (in group3) OrderedGroup_ZF_1_L8B:
  assumes A1: a ≤ 1 and A2: a ≠ 1 shows ¬(1 ≤ a)
proof -
  { assume 1 ≤ a
    with A1 have a = 1 using group_order_antisym
      by auto
    with A2 have False by simp
  } thus thesis by auto
qed

```

An element is greater or equal than another iff the difference is nonpositive.

```

lemma (in group3) OrderedGroup_ZF_1_L9:
  assumes A1: a ∈ G b ∈ G
  shows a ≤ b ↔ a · b-1 ≤ 1
proof
  assume a ≤ b
  with ordGroupAssum A1 have a · b-1 ≤ b · b-1
    using OrderedGroup_ZF_1_L1 group0.inverse_in_group
    IsAnOrdGroup_def by simp
  with A1 show a · b-1 ≤ 1
    using OrderedGroup_ZF_1_L1 group0.group0_2_L6
    by simp
next assume A2: a · b-1 ≤ 1
  with ordGroupAssum A1 have a · b-1 · b ≤ 1 · b
    using IsAnOrdGroup_def by simp
  with A1 show a ≤ b
    using OrderedGroup_ZF_1_L1

```

```

      group0.inv_cancel_two group0.group0_2_L2
    by simp
qed

```

We can move an element to the other side of an inequality.

```

lemma (in group3) OrderedGroup_ZF_1_L9A:
  assumes A1:  $a \in G$   $b \in G$   $c \in G$ 
  shows  $a \cdot b \leq c \iff a \leq c \cdot b^{-1}$ 
proof
  assume  $a \cdot b \leq c$ 
  with ordGroupAssum A1 have  $a \cdot b \cdot b^{-1} \leq c \cdot b^{-1}$ 
    using OrderedGroup_ZF_1_L1 group0.inverse_in_group IsAnOrdGroup_def
    by simp
  with A1 show  $a \leq c \cdot b^{-1}$ 
    using OrderedGroup_ZF_1_L1 group0.inv_cancel_two by simp
next assume  $a \leq c \cdot b^{-1}$ 
  with ordGroupAssum A1 have  $a \cdot b \leq c \cdot b^{-1} \cdot b$ 
    using OrderedGroup_ZF_1_L1 group0.inverse_in_group IsAnOrdGroup_def
    by simp
  with A1 show  $a \cdot b \leq c$ 
    using OrderedGroup_ZF_1_L1 group0.inv_cancel_two by simp
qed

```

A one side version of the previous lemma with weaker assumptions.

```

lemma (in group3) OrderedGroup_ZF_1_L9B:
  assumes A1:  $a \in G$   $b \in G$  and A2:  $a \cdot b^{-1} \leq c$ 
  shows  $a \leq c \cdot b$ 
proof -
  from A1 A2 have  $a \in G$   $b^{-1} \in G$   $c \in G$ 
    using OrderedGroup_ZF_1_L1 group0.inverse_in_group
    OrderedGroup_ZF_1_L4 by auto
  with A1 A2 show  $a \leq c \cdot b$ 
    using OrderedGroup_ZF_1_L9A OrderedGroup_ZF_1_L1
    group0.group_inv_of_inv by simp
qed

```

We can put an element on the other side of inequality, changing its sign.

```

lemma (in group3) OrderedGroup_ZF_1_L9C:
  assumes A1:  $a \in G$   $b \in G$  and A2:  $c \leq a \cdot b$ 
  shows
     $c \cdot b^{-1} \leq a$ 
     $a^{-1} \cdot c \leq b$ 
proof -
  from ordGroupAssum A1 A2 have
     $c \cdot b^{-1} \leq a \cdot b \cdot b^{-1}$ 
     $a^{-1} \cdot c \leq a^{-1} \cdot (a \cdot b)$ 
    using OrderedGroup_ZF_1_L1 group0.inverse_in_group IsAnOrdGroup_def
    by auto
  with A1 show

```

```

      c·b-1 ≤ a
      a-1·c ≤ b
      using OrderedGroup_ZF_1_L1 group0.inv_cancel_two
      by auto
qed

```

If an element is greater or equal than another then the difference is nonnegative.

```

lemma (in group3) OrderedGroup_ZF_1_L9D: assumes A1: a ≤ b
  shows 1 ≤ b·a-1
proof -
  from A1 have T: a ∈ G  b ∈ G  a-1 ∈ G
  using OrderedGroup_ZF_1_L4 OrderedGroup_ZF_1_L1
  group0.inverse_in_group by auto
  with ordGroupAssum A1 have a·a-1 ≤ b·a-1
  using IsAnOrdGroup_def by simp
  with T show 1 ≤ b·a-1
  using OrderedGroup_ZF_1_L1 group0.group0_2_L6
  by simp
qed

```

If an element is greater than another then the difference is positive.

```

lemma (in group3) OrderedGroup_ZF_1_L9E:
  assumes A1: a ≤ b  a ≠ b
  shows 1 ≤ b·a-1  1 ≠ b·a-1  b·a-1 ∈ G+
proof -
  from A1 have T: a ∈ G  b ∈ G using OrderedGroup_ZF_1_L4
  by auto
  from A1 show I: 1 ≤ b·a-1 using OrderedGroup_ZF_1_L9D
  by simp
  { assume b·a-1 = 1
    with T have a=b
      using OrderedGroup_ZF_1_L1 group0.group0_2_L11A
      by auto
    with A1 have False by simp
  } then show 1 ≠ b·a-1 by auto
  then have b·a-1 ≠ 1 by auto
  with I show b·a-1 ∈ G+ using OrderedGroup_ZF_1_L2A
  by simp
qed

```

If the difference is nonnegative, then  $a \leq b$ .

```

lemma (in group3) OrderedGroup_ZF_1_L9F:
  assumes A1: a ∈ G  b ∈ G and A2: 1 ≤ b·a-1
  shows a ≤ b
proof -
  from A1 A2 have 1·a ≤ b
  using OrderedGroup_ZF_1_L4 OrderedGroup_ZF_1_L9A
  by simp

```

```

with A1 show  $a \leq b$ 
  using OrderedGroup_ZF_1_L1 group0.group0_2_L2
  by simp
qed

```

If we increase the middle term in a product, the whole product increases.

```

lemma (in group3) OrderedGroup_ZF_1_L10:
  assumes  $a \in G$   $b \in G$  and  $c \leq d$ 
  shows  $a \cdot c \cdot b \leq a \cdot d \cdot b$ 
  using ordGroupAssum assms IsAnOrdGroup_def by simp

```

A product of (strictly) positive elements is not the unit.

```

lemma (in group3) OrderedGroup_ZF_1_L11:
  assumes A1:  $1 \leq a$   $1 \leq b$ 
  and A2:  $1 \neq a$   $1 \neq b$ 
  shows  $1 \neq a \cdot b$ 
proof -
  from A1 have T1:  $a \in G$   $b \in G$ 
  using OrderedGroup_ZF_1_L4 by auto
  { assume  $1 = a \cdot b$ 
    with A1 T1 have  $a \leq 1$   $1 \leq a$ 
    using OrderedGroup_ZF_1_L1 group0.group0_2_L9 OrderedGroup_ZF_1_L5AA
    by auto
    then have  $a = 1$  by (rule group_order_antisym)
    with A2 have False by simp
  } then show  $1 \neq a \cdot b$  by auto
qed

```

A product of nonnegative elements is nonnegative.

```

lemma (in group3) OrderedGroup_ZF_1_L12:
  assumes A1:  $1 \leq a$   $1 \leq b$ 
  shows  $1 \leq a \cdot b$ 
proof -
  from A1 have  $1 \cdot 1 \leq a \cdot b$ 
  using OrderedGroup_ZF_1_L5B by simp
  then show  $1 \leq a \cdot b$ 
  using OrderedGroup_ZF_1_L1 group0.group0_2_L2
  by simp
qed

```

If  $a$  is not greater than  $b$ , then  $1$  is not greater than  $b \cdot a^{-1}$ .

```

lemma (in group3) OrderedGroup_ZF_1_L12A:
  assumes A1:  $a \leq b$  shows  $1 \leq b \cdot a^{-1}$ 
proof -
  from A1 have T:  $1 \in G$   $a \in G$   $b \in G$ 
  using OrderedGroup_ZF_1_L4 OrderedGroup_ZF_1_L1 group0.group0_2_L2
  by auto

```

```

with A1 have 1·a ≤ b
  using OrderedGroup_ZF_1_L1 group0.group0_2_L2
  by simp
with T show 1 ≤ b·a-1 using OrderedGroup_ZF_1_L9A
  by simp
qed

```

We can move an element to the other side of a strict inequality.

```

lemma (in group3) OrderedGroup_ZF_1_L12B:
  assumes A1: a∈G b∈G and A2: a·b-1 < c
  shows a < c·b
proof -
  from A1 A2 have a·b-1·b < c·b
    using group_strict_ord_transl_inv by auto
  moreover from A1 have a·b-1·b = a
    using OrderedGroup_ZF_1_L1 group0.inv_cancel_two
    by simp
  ultimately show a < c·b
    by auto
qed

```

We can multiply the sides of two inequalities, first of them strict and we get a strict inequality.

```

lemma (in group3) OrderedGroup_ZF_1_L12C:
  assumes A1: a<b and A2: c≤d
  shows a·c < b·d
proof -
  from A1 A2 have T: a∈G b∈G c∈G d∈G
    using OrderedGroup_ZF_1_L4 by auto
  with ordGroupAssum A2 have a·c ≤ a·d
    using IsAnOrdGroup_def by simp
  moreover from A1 T have a·d < b·d
    using group_strict_ord_transl_inv by simp
  ultimately show a·c < b·d
    by (rule group_strict_ord_transit)
qed

```

We can multiply the sides of two inequalities, second of them strict and we get a strict inequality.

```

lemma (in group3) OrderedGroup_ZF_1_L12D:
  assumes A1: a≤b and A2: c<d
  shows a·c < b·d
proof -
  from A1 A2 have T: a∈G b∈G c∈G d∈G
    using OrderedGroup_ZF_1_L4 by auto
  with A2 have a·c < a·d
    using group_strict_ord_transl_inv by simp
  moreover from ordGroupAssum A1 T have a·d ≤ b·d

```

```

    using IsAnOrdGroup_def by simp
  ultimately show a·c < b·d
    by (rule OrderedGroup_ZF_1_L4A)
qed

```

### 27.3 The set of positive elements

In this section we study  $G_+$  - the set of elements that are (strictly) greater than the unit. The most important result is that every linearly ordered group can be decomposed into  $\{1\}$ ,  $G_+$  and the set of those elements  $a \in G$  such that  $a^{-1} \in G_+$ . Another property of linearly ordered groups that we prove here is that if  $G_+ \neq \emptyset$ , then it is infinite. This allows to show that nontrivial linearly ordered groups are infinite.

The positive set is closed under the group operation.

```

lemma (in group3) OrderedGroup_ZF_1_L13: shows  $G_+$  {is closed under}
P
proof -
  { fix a b assume a ∈  $G_+$   b ∈  $G_+$ 
    then have T1:  $1 \leq a \cdot b$   and  $1 \neq a \cdot b$ 
      using PositiveSet_def OrderedGroup_ZF_1_L11 OrderedGroup_ZF_1_L12
      by auto
    moreover from T1 have a·b ∈ G
      using OrderedGroup_ZF_1_L4 by simp
    ultimately have a·b ∈  $G_+$  using PositiveSet_def by simp
  } then show  $G_+$  {is closed under} P using IsOpClosed_def
  by simp
qed

```

For totally ordered groups every nonunit element is positive or its inverse is positive.

```

lemma (in group3) OrderedGroup_ZF_1_L14:
  assumes A1: r {is total on} G and A2: a ∈ G
  shows a=1 ∨ a ∈  $G_+$  ∨ a-1 ∈  $G_+$ 
proof -
  { assume A3: a ≠ 1
    moreover from A1 A2 have a ≤ 1 ∨ 1 ≤ a
      using IsTotal_def OrderedGroup_ZF_1_L1 group0.group0_2_L2
      by simp
    moreover from A3 A2 have T1: a-1 ≠ 1
      using OrderedGroup_ZF_1_L1 group0.group0_2_L8B
      by simp
    ultimately have a-1 ∈  $G_+$  ∨ a ∈  $G_+$ 
      using OrderedGroup_ZF_1_L5A OrderedGroup_ZF_1_L2A
      by auto
  } thus a=1 ∨ a ∈  $G_+$  ∨ a-1 ∈  $G_+$  by auto
qed

```

If an element belongs to the positive set, then it is not the unit and its inverse does not belong to the positive set.

```
lemma (in group3) OrderedGroup_ZF_1_L15:
  assumes A1:  $a \in G_+$  shows  $a \neq 1$   $a^{-1} \notin G_+$ 
proof -
  from A1 show T1:  $a \neq 1$  using PositiveSet_def by auto
  { assume  $a^{-1} \in G_+$ 
    with A1 have  $a \leq 1$   $1 \leq a$ 
      using OrderedGroup_ZF_1_L5AA PositiveSet_def by auto
    then have  $a = 1$  by (rule group_order_antisym)
    with T1 have False by simp
  } then show  $a^{-1} \notin G_+$  by auto
qed
```

If  $a^{-1}$  is positive, then  $a$  can not be positive or the unit.

```
lemma (in group3) OrderedGroup_ZF_1_L16:
  assumes A1:  $a \in G$  and A2:  $a^{-1} \in G_+$  shows  $a \neq 1$   $a \notin G_+$ 
proof -
  from A2 have  $a^{-1} \neq 1$   $(a^{-1})^{-1} \notin G_+$ 
    using OrderedGroup_ZF_1_L15 by auto
  with A1 show  $a \neq 1$   $a \notin G_+$ 
    using OrderedGroup_ZF_1_L1 group0.group0_2_L8C group0.group_inv_of_inv
    by auto
qed
```

For linearly ordered groups each element is either the unit, positive or its inverse is positive.

```
lemma (in group3) OrdGroup_decomp:
  assumes A1:  $r$  {is total on}  $G$  and A2:  $a \in G$ 
  shows Exactly_1_of_3_holds ( $a = 1, a \in G_+, a^{-1} \in G_+$ )
proof -
  from A1 A2 have  $a = 1 \vee a \in G_+ \vee a^{-1} \in G_+$ 
    using OrderedGroup_ZF_1_L14 by simp
  moreover from A2 have  $a = 1 \longrightarrow (a \notin G_+ \wedge a^{-1} \notin G_+)$ 
    using OrderedGroup_ZF_1_L1 group0.group_inv_of_one
    PositiveSet_def by simp
  moreover from A2 have  $a \in G_+ \longrightarrow (a \neq 1 \wedge a^{-1} \notin G_+)$ 
    using OrderedGroup_ZF_1_L15 by simp
  moreover from A2 have  $a^{-1} \in G_+ \longrightarrow (a \neq 1 \wedge a \notin G_+)$ 
    using OrderedGroup_ZF_1_L16 by simp
  ultimately show Exactly_1_of_3_holds ( $a = 1, a \in G_+, a^{-1} \in G_+$ )
    by (rule Fol1_L5)
qed
```

A if  $a$  is a nonunit element that is not positive, then  $a^{-1}$  is positive. This is useful for some proofs by cases.

```
lemma (in group3) OrdGroup_cases:
```



```

    assumes A1: r {is total on} G and A2: a ∈ G
    and A3: a ≠ 1  a ∉ G+
    shows a-1 ∈ G+
  proof -
    from A1 A2 have a=1 ∨ a ∈ G+ ∨ a-1 ∈ G+
      using OrderedGroup_ZF_1_L14 by simp
    with A3 show a-1 ∈ G+ by auto
  qed

```

Elements from  $G \setminus G_+$  are not greater than the unit.

```

lemma (in group3) OrderedGroup_ZF_1_L17:
  assumes A1: r {is total on} G and A2: a ∈ G-G+
  shows a ≤ 1
proof -
  { assume a=1
    with A2 have a ≤ 1 using OrderedGroup_ZF_1_L3 by simp }
  moreover
  { assume a ≠ 1
    with A1 A2 have a ≤ 1
      using PositiveSet_def OrderedGroup_ZF_1_L8A
      by auto }
  ultimately show a ≤ 1 by auto
qed

```

The next lemma allows to split proofs that something holds for all  $a \in G$  into cases  $a = 1$ ,  $a \in G_+$ ,  $-a \in G_+$ .

```

lemma (in group3) OrderedGroup_ZF_1_L18:
  assumes A1: r {is total on} G and A2: b ∈ G
  and A3: Q(1) and A4: ∀ a ∈ G+. Q(a) and A5: ∀ a ∈ G+. Q(a-1)
  shows Q(b)
proof -
  from A1 A2 A3 A4 A5 have Q(b) ∨ Q((b-1)-1)
    using OrderedGroup_ZF_1_L14 by auto
  with A2 show Q(b) using OrderedGroup_ZF_1_L1 group0.group_inv_of_inv
    by simp
qed

```

All elements greater or equal than an element of  $G_+$  belong to  $G_+$ .

```

lemma (in group3) OrderedGroup_ZF_1_L19:
  assumes A1: a ∈ G+ and A2: a ≤ b
  shows b ∈ G+
proof -
  from A1 have I: 1 ≤ a  and II: a ≠ 1
    using OrderedGroup_ZF_1_L2A by auto
  from I A2 have 1 ≤ b by (rule Group_order_transitive)
  moreover have b ≠ 1
  proof -
    { assume b=1
      with I A2 have 1 ≤ a  a ≤ 1

```

```

by auto
  then have 1=a by (rule group_order_antisym)
  with II have False by simp
} then show b≠1 by auto
qed
ultimately show b ∈ G+
using OrderedGroup_ZF_1_L2A by simp
qed

```

The inverse of an element of  $G_+$  cannot be in  $G_+$ .

```

lemma (in group3) OrderedGroup_ZF_1_L20:
  assumes A1: r {is total on} G and A2: a ∈ G+
  shows a-1 ∉ G+
proof -
  from A2 have a∈G using PositiveSet_def
  by simp
  with A1 have Exactly_1_of_3_holds (a=1,a∈G+,a-1∈G+)
  using OrdGroup_decomp by simp
  with A2 show a-1 ∉ G+ by (rule Fol1_L7)
qed

```

The set of positive elements of a nontrivial linearly ordered group is not empty.

```

lemma (in group3) OrderedGroup_ZF_1_L21:
  assumes A1: r {is total on} G and A2: G ≠ {1}
  shows G+ ≠ 0
proof -
  have 1 ∈ G using OrderedGroup_ZF_1_L1 group0.group0_2_L2
  by simp
  with A2 obtain a where a∈G a≠1 by auto
  with A1 have a∈G+ ∨ a-1∈G+
  using OrderedGroup_ZF_1_L14 by auto
  then show G+ ≠ 0 by auto
qed

```

If  $b \in G_+$ , then  $a < a \cdot b$ . Multiplying  $a$  by a positive element increases  $a$ .

```

lemma (in group3) OrderedGroup_ZF_1_L22:
  assumes A1: a∈G b∈G+
  shows a≤a·b a ≠ a·b a·b ∈ G
proof -
  from ordGroupAssum A1 have a·1 ≤ a·b
  using OrderedGroup_ZF_1_L2A IsAnOrdGroup_def
  by simp
  with A1 show a≤a·b
  using OrderedGroup_ZF_1_L1 group0.group0_2_L2
  by simp
  then show a·b ∈ G
  using OrderedGroup_ZF_1_L4 by simp
{ from A1 have a∈G b∈G

```

```

    using PositiveSet_def by auto
  moreover assume a = a·b
  ultimately have b = 1
    using OrderedGroup_ZF_1_L1 group0.group0_2_L7
    by simp
  with A1 have False using PositiveSet_def
    by simp
} then show a ≠ a·b by auto
qed

```

If  $G$  is a nontrivial linearly ordered group, then for every element of  $G$  we can find one in  $G_+$  that is greater or equal.

```

lemma (in group3) OrderedGroup_ZF_1_L23:
  assumes A1: r {is total on} G and A2:  $G \neq \{1\}$ 
  and A3:  $a \in G$ 
  shows  $\exists b \in G_+. a \leq b$ 
proof -
  { assume A4:  $a \in G_+$  then have  $a \leq a$ 
    using PositiveSet_def OrderedGroup_ZF_1_L3
    by simp
    with A4 have  $\exists b \in G_+. a \leq b$  by auto }
  moreover
  { assume  $a \notin G_+$ 
    with A1 A3 have I:  $a \leq 1$  using OrderedGroup_ZF_1_L17
    by simp
    from A1 A2 obtain b where II:  $b \in G_+$ 
    using OrderedGroup_ZF_1_L21 by auto
    then have  $1 \leq b$  using PositiveSet_def by simp
    with I have  $a \leq b$  by (rule Group_order_transitive)
    with II have  $\exists b \in G_+. a \leq b$  by auto }
  ultimately show thesis by auto
qed

```

The  $G^+$  is  $G_+$  plus the unit.

```

lemma (in group3) OrderedGroup_ZF_1_L24: shows  $G^+ = G_+ \cup \{1\}$ 
  using OrderedGroup_ZF_1_L2 OrderedGroup_ZF_1_L2A OrderedGroup_ZF_1_L3A
  by auto

```

What is  $-G_+$ , really?

```

lemma (in group3) OrderedGroup_ZF_1_L25: shows
   $(-G_+) = \{a^{-1}. a \in G_+\}$ 
   $(-G_+) \subseteq G$ 
proof -
  from ordGroupAssum have I: GroupInv(G,P) :  $G \rightarrow G$ 
    using IsAnOrdGroup_def group0_2_T2 by simp
  moreover have  $G_+ \subseteq G$  using PositiveSet_def by auto
  ultimately show
     $(-G_+) = \{a^{-1}. a \in G_+\}$ 
     $(-G_+) \subseteq G$ 

```

```

    using func_imagedef func1_1_L6 by auto
qed

```

If the inverse of  $a$  is in  $G_+$ , then  $a$  is in the inverse of  $G_+$ .

```

lemma (in group3) OrderedGroup_ZF_1_L26:
  assumes A1:  $a \in G$  and A2:  $a^{-1} \in G_+$ 
  shows  $a \in (-G_+)$ 
proof -
  from A1 have  $a^{-1} \in G$   $a = (a^{-1})^{-1}$  using OrderedGroup_ZF_1_L1
  group0.inverse_in_group group0.group_inv_of_inv
  by auto
  with A2 show  $a \in (-G_+)$  using OrderedGroup_ZF_1_L25
  by auto
qed

```

If  $a$  is in the inverse of  $G_+$ , then its inverse is in  $G_+$ .

```

lemma (in group3) OrderedGroup_ZF_1_L27:
  assumes  $a \in (-G_+)$ 
  shows  $a^{-1} \in G_+$ 
using assms OrderedGroup_ZF_1_L25 PositiveSet_def
OrderedGroup_ZF_1_L1 group0.group_inv_of_inv
by auto

```

A linearly ordered group can be decomposed into  $G_+$ ,  $\{1\}$  and  $-G_+$

```

lemma (in group3) OrdGroup_decomp2:
  assumes A1:  $r$  {is total on}  $G$ 
  shows
     $G = G_+ \cup (-G_+) \cup \{1\}$ 
     $G_+ \cap (-G_+) = 0$ 
     $1 \notin G_+ \cup (-G_+)$ 
proof -
  { fix a assume A2:  $a \in G$ 
    with A1 have  $a \in G_+ \vee a^{-1} \in G_+ \vee a=1$ 
      using OrderedGroup_ZF_1_L14 by auto
    with A2 have  $a \in G_+ \vee a \in (-G_+) \vee a=1$ 
      using OrderedGroup_ZF_1_L26 by auto
    then have  $a \in (G_+ \cup (-G_+) \cup \{1\})$ 
      by auto
  } then have  $G \subseteq G_+ \cup (-G_+) \cup \{1\}$ 
    by auto
  moreover have  $G_+ \cup (-G_+) \cup \{1\} \subseteq G$ 
    using OrderedGroup_ZF_1_L25 PositiveSet_def
    OrderedGroup_ZF_1_L1 group0.group0_2_L2
    by auto
  ultimately show  $G = G_+ \cup (-G_+) \cup \{1\}$  by auto
  { let A =  $G_+ \cap (-G_+)$ 
    assume  $G_+ \cap (-G_+) \neq 0$ 
    then have  $A \neq 0$  by simp
    then obtain a where  $a \in A$  by blast
  }

```

```

    then have False using OrderedGroup_ZF_1_L15 OrderedGroup_ZF_1_L27
    by auto
  } then show  $G_+ \cap (-G_+) = 0$  by auto
show  $1 \notin G_+ \cup (-G_+)$ 
  using OrderedGroup_ZF_1_L27
  OrderedGroup_ZF_1_L1 group0.group_inv_of_one
  OrderedGroup_ZF_1_L2A by auto
qed

```

If  $a \cdot b^{-1}$  is nonnegative, then  $b \leq a$ . This maybe used to recover the order from the set of nonnegative elements and serve as a way to define order by prescibing that set (see the "Alternative definitions" section).

```

lemma (in group3) OrderedGroup_ZF_1_L28:
  assumes A1:  $a \in G$   $b \in G$  and A2:  $a \cdot b^{-1} \in G_+$ 
  shows  $b \leq a$ 
proof -
  from A2 have  $1 \leq a \cdot b^{-1}$  using OrderedGroup_ZF_1_L2
  by simp
  with A1 show  $b \leq a$  using OrderedGroup_ZF_1_L5K
  by simp
qed

```

A special case of OrderedGroup\_ZF\_1\_L28 when  $a \cdot b^{-1}$  is positive.

```

corollary (in group3) OrderedGroup_ZF_1_L29:
  assumes A1:  $a \in G$   $b \in G$  and A2:  $a \cdot b^{-1} \in G_+$ 
  shows  $b \leq a$   $b \neq a$ 
proof -
  from A2 have  $1 \leq a \cdot b^{-1}$  and I:  $a \cdot b^{-1} \neq 1$ 
  using OrderedGroup_ZF_1_L2A by auto
  with A1 show  $b \leq a$  using OrderedGroup_ZF_1_L5K
  by simp
  from A1 I show  $b \neq a$ 
  using OrderedGroup_ZF_1_L1 group0.group0_2_L6
  by auto
qed

```

A bit stronger that OrderedGroup\_ZF\_1\_L29, adds case when two elements are equal.

```

lemma (in group3) OrderedGroup_ZF_1_L30:
  assumes  $a \in G$   $b \in G$  and  $a=b \vee b \cdot a^{-1} \in G_+$ 
  shows  $a \leq b$ 
  using assms OrderedGroup_ZF_1_L3 OrderedGroup_ZF_1_L29
  by auto

```

A different take on decomposition: we can have  $a = b$  or  $a < b$  or  $b < a$ .

```

lemma (in group3) OrderedGroup_ZF_1_L31:
  assumes A1:  $r$  {is total on}  $G$  and A2:  $a \in G$   $b \in G$ 
  shows  $a=b \vee (a \leq b \wedge a \neq b) \vee (b \leq a \wedge b \neq a)$ 

```

```

proof -
  from A2 have  $a \cdot b^{-1} \in G$  using OrderedGroup_ZF_1_L1
    group0.inverse_in_group group0.group_op_closed
  by simp
  with A1 have  $a \cdot b^{-1} = 1 \vee a \cdot b^{-1} \in G_+ \vee (a \cdot b^{-1})^{-1} \in G_+$ 
    using OrderedGroup_ZF_1_L14 by simp
  moreover
  { assume  $a \cdot b^{-1} = 1$ 
    then have  $a \cdot b^{-1} \cdot b = 1 \cdot b$  by simp
    with A2 have  $a=b \vee (a \leq b \wedge a \neq b) \vee (b \leq a \wedge b \neq a)$ 
      using OrderedGroup_ZF_1_L1
    group0.inv_cancel_two group0.group0_2_L2 by auto }
  moreover
  { assume  $a \cdot b^{-1} \in G_+$ 
    with A2 have  $a=b \vee (a \leq b \wedge a \neq b) \vee (b \leq a \wedge b \neq a)$ 
      using OrderedGroup_ZF_1_L29 by auto }
  moreover
  { assume  $(a \cdot b^{-1})^{-1} \in G_+$ 
    with A2 have  $b \cdot a^{-1} \in G_+$  using OrderedGroup_ZF_1_L1
      group0.group0_2_L12 by simp
    with A2 have  $a=b \vee (a \leq b \wedge a \neq b) \vee (b \leq a \wedge b \neq a)$ 
      using OrderedGroup_ZF_1_L29 by auto }
  ultimately show  $a=b \vee (a \leq b \wedge a \neq b) \vee (b \leq a \wedge b \neq a)$ 
    by auto
qed

```

## 27.4 Intervals and bounded sets

Intervals here are the closed intervals of the form  $\{x \in G. a \leq x \leq b\}$ .

A bounded set can be translated to put it in  $G^+$  and then it is still bounded above.

**lemma** (in group3) OrderedGroup\_ZF\_2\_L1:

```

  assumes A1:  $\forall g \in A. L \leq g \wedge g \leq M$ 
  and A2:  $S = \text{RightTranslation}(G, P, L^{-1})$ 
  and A3:  $a \in S(A)$ 
  shows  $a \leq M \cdot L^{-1} \quad 1 \leq a$ 

```

```

proof -
  from A3 have  $A \neq 0$  using func1_1_L13A by fast
  then obtain g where  $g \in A$  by auto
  with A1 have T1:  $L \in G \ M \in G \ L^{-1} \in G$ 
    using OrderedGroup_ZF_1_L4 OrderedGroup_ZF_1_L1
    group0.inverse_in_group by auto
  with A2 have  $S : G \rightarrow G$  using OrderedGroup_ZF_1_L1 group0.group0_5_L1
    by simp
  moreover from A1 have T2:  $A \subseteq G$  using OrderedGroup_ZF_1_L4 by auto
  ultimately have  $S(A) = \{S(b). b \in A\}$  using func_imagedef
    by simp
  with A3 obtain b where T3:  $b \in A \ a = S(b)$  by auto

```

```

with A1 ordGroupAssum T1 have  $b \cdot L^{-1} \leq M \cdot L^{-1}$   $L \cdot L^{-1} \leq b \cdot L^{-1}$ 
  using IsAnOrdGroup_def by auto
with T3 A2 T1 T2 show  $a \leq M \cdot L^{-1}$   $1 \leq a$ 
  using OrderedGroup_ZF_1_L1 group0.group0_5_L2 group0.group0_2_L6
  by auto
qed

Every bounded set is an image of a subset of an interval that starts at 1.

lemma (in group3) OrderedGroup_ZF_2_L2:
  assumes A1: IsBounded(A,r)
  shows  $\exists B. \exists g \in G^+. \exists T \in G \rightarrow G. A = T(B) \wedge B \subseteq \text{Interval}(r,1,g)$ 
proof -
  { assume A2: A=0
    let B = 0
    let g = 1
    let T = ConstantFunction(G,1)
    have  $g \in G^+$  using OrderedGroup_ZF_1_L3A by simp
    moreover have T :  $G \rightarrow G$ 
      using func1_3_L1 OrderedGroup_ZF_1_L1 group0.group0_2_L2 by simp
    moreover from A2 have A = T(B) by simp
    moreover have  $B \subseteq \text{Interval}(r,1,g)$  by simp
    ultimately have
       $\exists B. \exists g \in G^+. \exists T \in G \rightarrow G. A = T(B) \wedge B \subseteq \text{Interval}(r,1,g)$ 
      by auto }
  moreover
  { assume A3: A $\neq$ 0
    with A1 have  $\exists L. \forall x \in A. L \leq x$  and  $\exists U. \forall x \in A. x \leq U$ 
      using IsBounded_def IsBoundedBelow_def IsBoundedAbove_def
      by auto
    then obtain L U where D1:  $\forall x \in A. L \leq x \wedge x \leq U$ 
      by auto
    with A3 have T1:  $A \subseteq G$  using OrderedGroup_ZF_1_L4 by auto
    from A3 obtain a where  $a \in A$  by auto
    with D1 have T2:  $L \leq a \leq U$  by auto
    then have T3:  $L \in G \ L^{-1} \in G \ U \in G$ 
      using OrderedGroup_ZF_1_L4 OrderedGroup_ZF_1_L1
      group0.inverse_in_group by auto
    let T = RightTranslation(G,P,L)
    let B = RightTranslation(G,P,L $^{-1}$ )(A)
    let g =  $U \cdot L^{-1}$ 
    have  $g \in G^+$ 
    proof -
      from T2 have  $L \leq U$  using Group_order_transitive by fast
      with ordGroupAssum T3 have  $L \cdot L^{-1} \leq g$ 
    using IsAnOrdGroup_def by simp
    with T3 show thesis using OrderedGroup_ZF_1_L1 group0.group0_2_L6
    OrderedGroup_ZF_1_L2 by simp
    qed
    moreover from T3 have T :  $G \rightarrow G$ 

```

```

    using OrderedGroup_ZF_1_L1 group0.group0_5_L1
    by simp
    moreover have A = T(B)
    proof -
      from T3 T1 have T(B) = {a·L-1·L. a∈A}
    using OrderedGroup_ZF_1_L1 group0.group0_5_L6
    by simp
      moreover from T3 T1 have ∀a∈A. a·L-1·L = a·(L-1·L)
    using OrderedGroup_ZF_1_L1 group0.group_oper_assoc by auto
      ultimately have T(B) = {a·(L-1·L). a∈A} by simp
      with T3 have T(B) = {a·1. a∈A}
    using OrderedGroup_ZF_1_L1 group0.group0_2_L6 by simp
      moreover from T1 have ∀a∈A. a·1=a
    using OrderedGroup_ZF_1_L1 group0.group0_2_L2 by auto
      ultimately show thesis by simp
    qed
    moreover have B ⊆ Interval(r,1,g)
    proof
      fix y assume A4: y ∈ B
      let S = RightTranslation(G,P,L-1)
      from D1 have T4: ∀x∈A. L≤x ∧ x≤U by simp
      moreover have T5: S = RightTranslation(G,P,L-1)
    by simp
      moreover from A4 have T6: y ∈ S(A) by simp
      ultimately have y≤U·L-1 using OrderedGroup_ZF_2_L1
    by blast
      moreover from T4 T5 T6 have 1≤y by (rule OrderedGroup_ZF_2_L1)
      ultimately show y ∈ Interval(r,1,g) using Interval_def by auto
    qed
    ultimately have
      ∃B.∃g∈G+.∃T∈G→G. A = T(B) ∧ B ⊆ Interval(r,1,g)
    by auto }
    ultimately show thesis by auto
  qed

```

If every interval starting at 1 is finite, then every bounded set is finite. I find it interesting that this does not require the group to be linearly ordered (the order to be total).

```

theorem (in group3) OrderedGroup_ZF_2_T1:
  assumes A1: ∀g∈G+. Interval(r,1,g) ∈ Fin(G)
  and A2: IsBounded(A,r)
  shows A ∈ Fin(G)
proof -
  from A2 have
    ∃B.∃g∈G+.∃T∈G→G. A = T(B) ∧ B ⊆ Interval(r,1,g)
  using OrderedGroup_ZF_2_L2 by simp
  then obtain B g T where D1: g∈G+ B ⊆ Interval(r,1,g)
  and D2: T : G→G A = T(B) by auto
  from D1 A1 have B∈Fin(G) using Fin_subset_lemma by blast

```



```

    with D2 show thesis using Finite1_L6A by simp
qed

```

In linearly ordered groups finite sets are bounded.

```

theorem (in group3) ord_group_fin_bounded:
  assumes r {is total on} G and B∈Fin(G)
  shows IsBounded(B,r)
  using ordGroupAssum assms IsAnOrdGroup_def IsPartOrder_def Finite_ZF_1_T1
  by simp

```

For nontrivial linearly ordered groups if for every element  $G$  we can find one in  $A$  that is greater or equal (not necessarily strictly greater), then  $A$  can neither be finite nor bounded above.

```

lemma (in group3) OrderedGroup_ZF_2_L2A:
  assumes A1: r {is total on} G and A2:  $G \neq \{1\}$ 
  and A3:  $\forall a \in G. \exists b \in A. a \leq b$ 
  shows
     $\forall a \in G. \exists b \in A. a \neq b \wedge a \leq b$ 
     $\neg \text{IsBoundedAbove}(A,r)$ 
     $A \notin \text{Fin}(G)$ 
proof -
  { fix a
    from A1 A2 obtain c where  $c \in G_+$ 
      using OrderedGroup_ZF_1_L21 by auto
    moreover assume  $a \in G$ 
    ultimately have
       $a \cdot c \in G$  and I:  $a < a \cdot c$ 
      using OrderedGroup_ZF_1_L22 by auto
    with A3 obtain b where II:  $b \in A$  and III:  $a \cdot c \leq b$ 
      by auto
    moreover from I III have  $a < b$  by (rule OrderedGroup_ZF_1_L4A)
    ultimately have  $\exists b \in A. a \neq b \wedge a \leq b$  by auto
  } thus  $\forall a \in G. \exists b \in A. a \neq b \wedge a \leq b$  by simp
with ordGroupAssum A1 show
   $\neg \text{IsBoundedAbove}(A,r)$ 
   $A \notin \text{Fin}(G)$ 
  using IsAnOrdGroup_def IsPartOrder_def
  OrderedGroup_ZF_1_L1A Order_ZF_3_L14 Finite_ZF_1_1_L3
  by auto
qed

```

Nontrivial linearly ordered groups are infinite. Recall that  $\text{Fin}(A)$  is the collection of finite subsets of  $A$ . In this lemma we show that  $G \notin \text{Fin}(G)$ , that is that  $G$  is not a finite subset of itself. This is a way of saying that  $G$  is infinite. We also show that for nontrivial linearly ordered groups  $G_+$  is infinite.

```

theorem (in group3) Linord_group_infinite:
  assumes A1: r {is total on} G and A2:  $G \neq \{1\}$ 

```

```

shows
 $G_+ \notin \text{Fin}(G)$ 
 $G \notin \text{Fin}(G)$ 
proof -
  from A1 A2 show I:  $G_+ \notin \text{Fin}(G)$ 
    using OrderedGroup_ZF_1_L23 OrderedGroup_ZF_2_L2A
    by simp
  { assume  $G \in \text{Fin}(G)$ 
    moreover have  $G_+ \subseteq G$  using PositiveSet_def by auto
    ultimately have  $G_+ \in \text{Fin}(G)$  using Fin_subset_lemma
    by blast
    with I have False by simp
  } then show  $G \notin \text{Fin}(G)$  by auto
qed

```

A property of nonempty subsets of linearly ordered groups that don't have a maximum: for any element in such subset we can find one that is strictly greater.

```

lemma (in group3) OrderedGroup_ZF_2_L2B:
  assumes A1:  $r$  {is total on}  $G$  and A2:  $A \subseteq G$  and
  A3:  $\neg \text{HasAmaximum}(r, A)$  and A4:  $x \in A$ 
  shows  $\exists y \in A. x < y$ 
proof -
  from ordGroupAssum assms have
    antisym( $r$ )
     $r$  {is total on}  $G$ 
     $A \subseteq G$   $\neg \text{HasAmaximum}(r, A)$   $x \in A$ 
    using IsAnOrdGroup_def IsPartOrder_def
    by auto
  then have  $\exists y \in A. \langle x, y \rangle \in r \wedge y \neq x$ 
    using Order_ZF_4_L16 by simp
  then show  $\exists y \in A. x < y$  by auto
qed

```

In linearly ordered groups  $G \setminus G_+$  is bounded above.

```

lemma (in group3) OrderedGroup_ZF_2_L3:
  assumes A1:  $r$  {is total on}  $G$  shows IsBoundedAbove( $G \setminus G_+, r$ )
proof -
  from A1 have  $\forall a \in G \setminus G_+. a \leq 1$ 
    using OrderedGroup_ZF_1_L17 by simp
  then show IsBoundedAbove( $G \setminus G_+, r$ )
    using IsBoundedAbove_def by auto
qed

```

In linearly ordered groups if  $A \cap G_+$  is finite, then  $A$  is bounded above.

```

lemma (in group3) OrderedGroup_ZF_2_L4:
  assumes A1:  $r$  {is total on}  $G$  and A2:  $A \subseteq G$ 
  and A3:  $A \cap G_+ \in \text{Fin}(G)$ 

```

```

shows IsBoundedAbove(A,r)
proof -
  have  $A \cap (G-G_+) \subseteq G-G_+$  by auto
  with A1 have IsBoundedAbove( $A \cap (G-G_+)$ ,r)
    using OrderedGroup_ZF_2_L3 Order_ZF_3_L13
    by blast
  moreover from A1 A3 have IsBoundedAbove( $A \cap G_+$ ,r)
    using ord_group_fin_bounded IsBounded_def
    by simp
  moreover from A1 ordGroupAssum have
    r {is total on} G trans(r)  $r \subseteq G \times G$ 
    using IsAnOrdGroup_def IsPartOrder_def by auto
  ultimately have IsBoundedAbove( $A \cap (G-G_+) \cup A \cap G_+$ ,r)
    using Order_ZF_3_L3 by simp
  moreover from A2 have  $A = A \cap (G-G_+) \cup A \cap G_+$ 
    by auto
  ultimately show IsBoundedAbove(A,r) by simp
qed

```

If a set  $-A \subseteq G$  is bounded above, then  $A$  is bounded below.

```

lemma (in group3) OrderedGroup_ZF_2_L5:
  assumes A1:  $A \subseteq G$  and A2: IsBoundedAbove( $-A$ ,r)
  shows IsBoundedBelow(A,r)
proof -
  { assume A = 0 then have IsBoundedBelow(A,r)
    using IsBoundedBelow_def by auto }
  moreover
  { assume A3:  $A \neq 0$ 
    from ordGroupAssum have I: GroupInv(G,P) :  $G \rightarrow G$ 
      using IsAnOrdGroup_def group0_2_T2 by simp
    with A1 A2 A3 obtain u where D:  $\forall a \in (-A). a \leq u$ 
      using func1_1_L15A IsBoundedAbove_def by auto
    { fix b assume  $b \in A$ 
      with A1 I D have  $b^{-1} \leq u$  and T:  $b \in G$ 
    }
    using func_imagedef by auto
    then have  $u^{-1} \leq (b^{-1})^{-1}$  using OrderedGroup_ZF_1_L5
  } by simp
  with T have  $u^{-1} \leq b$ 
  using OrderedGroup_ZF_1_L1 group0.group_inv_of_inv
  by simp
  } then have  $\forall b \in A. \langle u^{-1}, b \rangle \in r$  by simp
  then have IsBoundedBelow(A,r)
    using Order_ZF_3_L9 by blast }
  ultimately show thesis by auto
qed

```

If  $a \leq b$ , then the image of the interval  $a..b$  by any function is nonempty.

```

lemma (in group3) OrderedGroup_ZF_2_L6:
  assumes  $a \leq b$  and  $f: G \rightarrow G$ 

```

```

shows f(Interval(r,a,b))  $\neq$  0
using ordGroupAssum assms OrderedGroup_ZF_1_L4
    Order_ZF_2_L6 Order_ZF_2_L2A
    IsAnOrdGroup_def IsPartOrder_def func1_1_L15A
by auto
end

```

## 28 OrderedGroup\_ZF\_1.thy

theory OrderedGroup\_ZF\_1 imports OrderedGroup\_ZF

begin

In this theory we continue the OrderedGroup\_ZF theory development.

### 28.1 Absolute value and the triangle inequality

The goal of this section is to prove the triangle inequality for ordered groups.

Absolute value maps  $G$  into  $G$ .

```
lemma (in group3) OrderedGroup_ZF_3_L1:
  shows AbsoluteValue(G,P,r) : G→G
proof -
  let f = id(G+)
  let g = restrict(GroupInv(G,P),G-G+)
  have f : G+→G+ using id_type by simp
  then have f : G+→G using OrderedGroup_ZF_1_L4E fun_weaken_type
    by blast
  moreover have g : G-G+→G
proof -
  from ordGroupAssum have GroupInv(G,P) : G→G
    using IsAnOrdGroup_def group0_2_T2 by simp
  moreover have G-G+ ⊆ G by auto
  ultimately show thesis using restrict_type2 by simp
qed
moreover have G+∩(G-G+) = 0 by blast
ultimately have f ∪ g : G+∪(G-G+)→G∪G
  by (rule fun_disjoint_Un)
moreover have G+∪(G-G+) = G using OrderedGroup_ZF_1_L4E
  by auto
ultimately show AbsoluteValue(G,P,r) : G→G
  using AbsoluteValue_def by simp
qed
```

If  $a \in G^+$ , then  $|a| = a$ .

```
lemma (in group3) OrderedGroup_ZF_3_L2:
  assumes A1: a∈G+ shows |a| = a
proof -
  from ordGroupAssum have GroupInv(G,P) : G→G
    using IsAnOrdGroup_def group0_2_T2 by simp
  with A1 show thesis using
    func1_1_L1 OrderedGroup_ZF_1_L4E fun_disjoint_apply1
    AbsoluteValue_def id_conv by simp
qed
```

The absolute value of the unit is the unit. In the additive totation that would be  $|0| = 0$ .

```
lemma (in group3) OrderedGroup_ZF_3_L2A:
  shows |1| = 1 using OrderedGroup_ZF_1_L3A OrderedGroup_ZF_3_L2
  by simp
```

If  $a$  is positive, then  $|a| = a$ .

```
lemma (in group3) OrderedGroup_ZF_3_L2B:
  assumes a ∈ G+ shows |a| = a
  using assms PositiveSet_def Nonnegative_def OrderedGroup_ZF_3_L2
  by auto
```

If  $a \in G \setminus G^+$ , then  $|a| = a^{-1}$ .

```
lemma (in group3) OrderedGroup_ZF_3_L3:
  assumes A1: a ∈ G-G+ shows |a| = a-1
proof -
  have domain(id(G+)) = G+
  using id_type func1_1_L1 by auto
  with A1 show thesis using fun_disjoint_apply2 AbsoluteValue_def
  restrict by simp
qed
```

For elements that not greater than the unit, the absolute value is the inverse.

```
lemma (in group3) OrderedGroup_ZF_3_L3A:
  assumes A1: a ≤ 1
  shows |a| = a-1
proof -
  { assume a=1 then have |a| = a-1
    using OrderedGroup_ZF_3_L2A OrderedGroup_ZF_1_L1 group0.group_inv_of_one
    by simp }
  moreover
  { assume a ≠ 1
    with A1 have |a| = a-1 using OrderedGroup_ZF_1_L4C OrderedGroup_ZF_3_L3
    by simp }
  ultimately show |a| = a-1 by blast
qed
```

In linearly ordered groups the absolute value of any element is in  $G^+$ .

```
lemma (in group3) OrderedGroup_ZF_3_L3B:
  assumes A1: r {is total on} G and A2: a ∈ G
  shows |a| ∈ G+
proof -
  { assume a ∈ G+ then have |a| ∈ G+
    using OrderedGroup_ZF_3_L2 by simp }
  moreover
  { assume a ∉ G+
    with A1 A2 have |a| ∈ G+ using OrderedGroup_ZF_3_L3
    OrderedGroup_ZF_1_L6 by simp }
qed
```

ultimately show  $|a| \in G^+$  by blast  
qed

For linearly ordered groups (where the order is total), the absolute value maps the group into the positive set.

```
lemma (in group3) OrderedGroup_ZF_3_L3C:
  assumes A1: r {is total on} G
  shows AbsoluteValue(G,P,r) :  $G \rightarrow G^+$ 
proof-
  have AbsoluteValue(G,P,r) :  $G \rightarrow G$  using OrderedGroup_ZF_3_L1
  by simp
  moreover from A1 have T2:
     $\forall g \in G. \text{AbsoluteValue}(G,P,r)(g) \in G^+$ 
  using OrderedGroup_ZF_3_L3B by simp
  ultimately show thesis by (rule func1_1_L1A)
qed
```

If the absolute value is the unit, then the element is the unit.

```
lemma (in group3) OrderedGroup_ZF_3_L3D:
  assumes A1:  $a \in G$  and A2:  $|a| = 1$ 
  shows  $a = 1$ 
proof -
  { assume  $a \in G^+$ 
    with A2 have  $a = 1$  using OrderedGroup_ZF_3_L2 by simp }
  moreover
  { assume  $a \notin G^+$ 
    with A1 A2 have  $a = 1$  using
      OrderedGroup_ZF_3_L3 OrderedGroup_ZF_1_L1 group0.group0_2_L8A
      by auto }
  ultimately show  $a = 1$  by blast
qed
```

In linearly ordered groups the unit is not greater than the absolute value of any element.

```
lemma (in group3) OrderedGroup_ZF_3_L3E:
  assumes r {is total on} G and  $a \in G$ 
  shows  $1 \leq |a|$ 
  using assms OrderedGroup_ZF_3_L3B OrderedGroup_ZF_1_L2 by simp
```

If  $b$  is greater than both  $a$  and  $a^{-1}$ , then  $b$  is greater than  $|a|$ .

```
lemma (in group3) OrderedGroup_ZF_3_L4:
  assumes A1:  $a \leq b$  and A2:  $a^{-1} \leq b$ 
  shows  $|a| \leq b$ 
proof -
  { assume  $a \in G^+$ 
    with A1 have  $|a| \leq b$  using OrderedGroup_ZF_3_L2 by simp }
  moreover
  { assume  $a \notin G^+$ 
```

```

    with A1 A2 have  $|a| \leq b$ 
      using OrderedGroup_ZF_1_L4 OrderedGroup_ZF_3_L3 by simp }
    ultimately show  $|a| \leq b$  by blast
qed

```

In linearly ordered groups  $a \leq |a|$ .

```

lemma (in group3) OrderedGroup_ZF_3_L5:
  assumes A1:  $r$  {is total on}  $G$  and A2:  $a \in G$ 
  shows  $a \leq |a|$ 
proof -
  { assume  $a \in G^+$ 
    with A2 have  $a \leq |a|$ 
      using OrderedGroup_ZF_3_L2 OrderedGroup_ZF_1_L3 by simp }
  moreover
  { assume  $a \notin G^+$ 
    with A1 A2 have  $a \leq |a|$ 
      using OrderedGroup_ZF_3_L3B OrderedGroup_ZF_1_L4B by simp }
  ultimately show  $a \leq |a|$  by blast
qed

```

$a^{-1} \leq |a|$  (in additive notation it would be  $-a \leq |a|$ ).

```

lemma (in group3) OrderedGroup_ZF_3_L6:
  assumes A1:  $a \in G$  shows  $a^{-1} \leq |a|$ 
proof -
  { assume  $a \in G^+$ 
    then have T1:  $1 \leq a$  and T2:  $|a| = a$  using OrderedGroup_ZF_1_L2
      OrderedGroup_ZF_3_L2 by auto
    then have  $a^{-1} \leq 1^{-1}$  using OrderedGroup_ZF_1_L5 by simp
    then have T3:  $a^{-1} \leq 1$ 
      using OrderedGroup_ZF_1_L1 group0.group_inv_of_one by simp
    from T3 T1 have  $a^{-1} \leq a$  by (rule Group_order_transitive)
    with T2 have  $a^{-1} \leq |a|$  by simp }
  moreover
  { assume A2:  $a \notin G^+$ 
    from A1 have  $|a| \in G$ 
      using OrderedGroup_ZF_3_L1 apply_funtype by auto
    with ordGroupAssum have  $|a| \leq |a|$ 
      using IsAnOrdGroup_def IsPartOrder_def refl_def by simp
    with A1 A2 have  $a^{-1} \leq |a|$  using OrderedGroup_ZF_3_L3 by simp }
  ultimately show  $a^{-1} \leq |a|$  by blast
qed

```

Some inequalities about the product of two elements of a linearly ordered group and its absolute value.

```

lemma (in group3) OrderedGroup_ZF_3_L6A:
  assumes  $r$  {is total on}  $G$  and  $a \in G$   $b \in G$ 
  shows
     $a \cdot b \leq |a| \cdot |b|$ 
     $a \cdot b^{-1} \leq |a| \cdot |b|$ 

```



```

a⁻¹·b ≤ |a|·|b|
a⁻¹·b⁻¹ ≤ |a|·|b|
using assms OrderedGroup_ZF_3_L5 OrderedGroup_ZF_3_L6
  OrderedGroup_ZF_1_L5B by auto

|a⁻¹| ≤ |a|.

lemma (in group3) OrderedGroup_ZF_3_L7:
  assumes r {is total on} G and a∈G
  shows |a⁻¹| ≤ |a|
  using assms OrderedGroup_ZF_3_L5 OrderedGroup_ZF_1_L1 group0.group_inv_of_inv
    OrderedGroup_ZF_3_L6 OrderedGroup_ZF_3_L4 by simp

|a⁻¹| = |a|.

lemma (in group3) OrderedGroup_ZF_3_L7A:
  assumes A1: r {is total on} G and A2: a∈G
  shows |a⁻¹| = |a|
proof -
  from A2 have a⁻¹∈G using OrderedGroup_ZF_1_L1 group0.inverse_in_group
    by simp
  with A1 have |(a⁻¹)⁻¹| ≤ |a⁻¹| using OrderedGroup_ZF_3_L7 by simp
  with A1 A2 have |a⁻¹| ≤ |a| |a| ≤ |a⁻¹|
    using OrderedGroup_ZF_1_L1 group0.group_inv_of_inv OrderedGroup_ZF_3_L7
    by auto
  then show thesis by (rule group_order_antisym)
qed

|a · b⁻¹| = |b · a⁻¹|. It doesn't look so strange in the additive notation:
|a - b| = |b - a|.

lemma (in group3) OrderedGroup_ZF_3_L7B:
  assumes A1: r {is total on} G and A2: a∈G b∈G
  shows |a·b⁻¹| = |b·a⁻¹|
proof -
  from A1 A2 have |(a·b⁻¹)⁻¹| = |a·b⁻¹| using
    OrderedGroup_ZF_1_L1 group0.inverse_in_group group0.group0_2_L1
    monoid0.group0_1_L1 OrderedGroup_ZF_3_L7A by simp
  moreover from A2 have (a·b⁻¹)⁻¹ = b·a⁻¹
    using OrderedGroup_ZF_1_L1 group0.group0_2_L12 by simp
  ultimately show thesis by simp
qed

Triangle inequality for linearly ordered abelian groups. It would be nice to
drop commutativity or give an example that shows we can't do that.

theorem (in group3) OrdGroup_triangle_ineq:
  assumes A1: P {is commutative on} G
  and A2: r {is total on} G and A3: a∈G b∈G
  shows |a·b| ≤ |a|·|b|
proof -
  from A1 A2 A3 have

```

```

    a ≤ |a| b ≤ |b| a-1 ≤ |a| b-1 ≤ |b|
    using OrderedGroup_ZF_3_L5 OrderedGroup_ZF_3_L6 by auto
  then have a·b ≤ |a|·|b| a-1·b-1 ≤ |a|·|b|
    using OrderedGroup_ZF_1_L5B by auto
  with A1 A3 show |a·b| ≤ |a|·|b|
    using OrderedGroup_ZF_1_L1 group0.group_inv_of_two IsCommutative_def

  OrderedGroup_ZF_3_L4 by simp
qed

```

We can multiply the sides of an inequality with absolute value.

```

lemma (in group3) OrderedGroup_ZF_3_L7C:
  assumes A1: P {is commutative on} G
  and A2: r {is total on} G and A3: a∈G b∈G
  and A4: |a| ≤ c |b| ≤ d
  shows |a·b| ≤ c·d
proof -
  from A1 A2 A3 A4 have |a·b| ≤ |a|·|b|
    using OrderedGroup_ZF_1_L4 OrdGroup_triangle_ineq
    by simp
  moreover from A4 have |a|·|b| ≤ c·d
    using OrderedGroup_ZF_1_L5B by simp
  ultimately show thesis by (rule Group_order_transitive)
qed

```

A version of the OrderedGroup\_ZF\_3\_L7C but with multiplying by the inverse.

```

lemma (in group3) OrderedGroup_ZF_3_L7CA:
  assumes P {is commutative on} G
  and r {is total on} G and a∈G b∈G
  and |a| ≤ c |b| ≤ d
  shows |a·b-1| ≤ c·d
  using assms OrderedGroup_ZF_1_L1 group0.inverse_in_group
  OrderedGroup_ZF_3_L7A OrderedGroup_ZF_3_L7C by simp

```

Triangle inequality with three integers.

```

lemma (in group3) OrdGroup_triangle_ineq3:
  assumes A1: P {is commutative on} G
  and A2: r {is total on} G and A3: a∈G b∈G c∈G
  shows |a·b·c| ≤ |a|·|b|·|c|
proof -
  from A3 have T: a·b ∈ G |c| ∈ G
    using OrderedGroup_ZF_1_L1 group0.group_op_closed
    OrderedGroup_ZF_3_L1 apply_funtype by auto
  with A1 A2 A3 have |a·b·c| ≤ |a·b|·|c|
    using OrdGroup_triangle_ineq by simp
  moreover from ordGroupAssum A1 A2 A3 T have
    |a·b|·|c| ≤ |a|·|b|·|c|
    using OrdGroup_triangle_ineq IsAnOrdGroup_def by simp
  ultimately show |a·b·c| ≤ |a|·|b|·|c|

```

by (rule Group\_order\_transitive)  
qed

Some variants of the triangle inequality.

```
lemma (in group3) OrderedGroup_ZF_3_L7D:
  assumes A1: P {is commutative on} G
  and A2: r {is total on} G and A3: a ∈ G b ∈ G
  and A4: |a·b-1| ≤ c
  shows
    |a| ≤ c·|b|
    |a| ≤ |b|·c
    c-1·a ≤ b
    a·c-1 ≤ b
    a ≤ b·c
proof -
  from A3 A4 have
    T: a·b-1 ∈ G |b| ∈ G c ∈ G c-1 ∈ G
  using OrderedGroup_ZF_1_L1
    group0.inverse_in_group group0.group0_2_L1 monoid0.group0_1_L1
    OrderedGroup_ZF_3_L1 apply_funtype OrderedGroup_ZF_1_L4
  by auto
  from A3 have |a| = |a·b-1·b|
  using OrderedGroup_ZF_1_L1 group0.inv_cancel_two
  by simp
  with A1 A2 A3 T have |a| ≤ |a·b-1|·|b|
  using OrdGroup_triangle_ineq by simp
  with T A4 show |a| ≤ c·|b| using OrderedGroup_ZF_1_L5C
  by blast
  with T A1 show |a| ≤ |b|·c
  using IsCommutative_def by simp
  from A2 T have a·b-1 ≤ |a·b-1|
  using OrderedGroup_ZF_3_L5 by simp
  moreover note A4
  ultimately have I: a·b-1 ≤ c
  by (rule Group_order_transitive)
  with A3 show c-1·a ≤ b
  using OrderedGroup_ZF_1_L5H by simp
  with A1 A3 T show a·c-1 ≤ b
  using IsCommutative_def by simp
  from A1 A3 T I show a ≤ b·c
  using OrderedGroup_ZF_1_L5H IsCommutative_def
  by auto
qed
```

Some more variants of the triangle inequality.

```
lemma (in group3) OrderedGroup_ZF_3_L7E:
  assumes A1: P {is commutative on} G
  and A2: r {is total on} G and A3: a ∈ G b ∈ G
  and A4: |a·b-1| ≤ c
```

```

shows  $b \cdot c^{-1} \leq a$ 
proof -
  from A3 have  $a \cdot b^{-1} \in G$ 
    using OrderedGroup_ZF_1_L1
    group0.inverse_in_group group0.group_op_closed
  by auto
with A2 have  $|(a \cdot b^{-1})^{-1}| = |a \cdot b^{-1}|$ 
  using OrderedGroup_ZF_3_L7A by simp
moreover from A3 have  $(a \cdot b^{-1})^{-1} = b \cdot a^{-1}$ 
  using OrderedGroup_ZF_1_L1 group0.group0_2_L12
  by simp
ultimately have  $|b \cdot a^{-1}| = |a \cdot b^{-1}|$ 
  by simp
with A1 A2 A3 A4 show  $b \cdot c^{-1} \leq a$ 
  using OrderedGroup_ZF_3_L7D by simp
qed

```

An application of the triangle inequality with four group elements.

```

lemma (in group3) OrderedGroup_ZF_3_L7F:
  assumes A1:  $P \text{ \{is commutative on\} } G$ 
  and A2:  $r \text{ \{is total on\} } G$  and
  A3:  $a \in G \ b \in G \ c \in G \ d \in G$ 
  shows  $|a \cdot c^{-1}| \leq |a \cdot b| \cdot |c \cdot d| \cdot |b \cdot d^{-1}|$ 
proof -
  from A3 have T:
     $a \cdot c^{-1} \in G \ a \cdot b \in G \ c \cdot d \in G \ b \cdot d^{-1} \in G$ 
     $(c \cdot d)^{-1} \in G \ (b \cdot d^{-1})^{-1} \in G$ 
  using OrderedGroup_ZF_1_L1
  group0.inverse_in_group group0.group_op_closed
  by auto
with A1 A2 have  $|(a \cdot b) \cdot (c \cdot d)^{-1} \cdot (b \cdot d^{-1})^{-1}| \leq |a \cdot b| \cdot |(c \cdot d)^{-1}| \cdot |(b \cdot d^{-1})^{-1}|$ 
  using OrdGroup_triangle_ineq3 by simp
moreover from A2 T have  $|(c \cdot d)^{-1}| = |c \cdot d|$  and  $|(b \cdot d^{-1})^{-1}| = |b \cdot d^{-1}|$ 
  using OrderedGroup_ZF_3_L7A by auto
moreover from A1 A3 have  $(a \cdot b) \cdot (c \cdot d)^{-1} \cdot (b \cdot d^{-1})^{-1} = a \cdot c^{-1}$ 
  using OrderedGroup_ZF_1_L1 group0.group0_4_L8
  by simp
ultimately show  $|a \cdot c^{-1}| \leq |a \cdot b| \cdot |c \cdot d| \cdot |b \cdot d^{-1}|$ 
  by simp
qed

```

$|a| \leq L$  implies  $L^{-1} \leq a$  (it would be  $-L \leq a$  in the additive notation).

```

lemma (in group3) OrderedGroup_ZF_3_L8:
  assumes A1:  $a \in G$  and A2:  $|a| \leq L$ 
  shows
     $L^{-1} \leq a$ 
proof -
  from A1 have I:  $a^{-1} \leq |a|$  using OrderedGroup_ZF_3_L6 by simp
  from I A2 have  $a^{-1} \leq L$  by (rule Group_order_transitive)

```

```

    then have  $L^{-1} \leq (a^{-1})^{-1}$  using OrderedGroup_ZF_1_L5 by simp
    with A1 show  $L^{-1} \leq a$  using OrderedGroup_ZF_1_L1 group0.group_inv_of_inv
    by simp
qed

```

In linearly ordered groups  $|a| \leq L$  implies  $a \leq L$  (it would be  $a \leq L$  in the additive notation).

```

lemma (in group3) OrderedGroup_ZF_3_L8A:
  assumes A1: r {is total on} G
  and A2:  $a \in G$  and A3:  $|a| \leq L$ 
  shows
     $a \leq L$ 
     $1 \leq L$ 
proof -
  from A1 A2 have I:  $a \leq |a|$  using OrderedGroup_ZF_3_L5 by simp
  from I A3 show  $a \leq L$  by (rule Group_order_transitive)
  from A1 A2 A3 have  $1 \leq |a|$   $|a| \leq L$ 
    using OrderedGroup_ZF_3_L3B OrderedGroup_ZF_1_L2 by auto
  then show  $1 \leq L$  by (rule Group_order_transitive)
qed

```

A somewhat generalized version of the above lemma.

```

lemma (in group3) OrderedGroup_ZF_3_L8B:
  assumes A1:  $a \in G$  and A2:  $|a| \leq L$  and A3:  $1 \leq c$ 
  shows  $(L \cdot c)^{-1} \leq a$ 
proof -
  from A1 A2 A3 have  $c^{-1} \cdot L^{-1} \leq 1 \cdot a$ 
    using OrderedGroup_ZF_3_L8 OrderedGroup_ZF_1_L5AB
    OrderedGroup_ZF_1_L5B by simp
  with A1 A2 A3 show  $(L \cdot c)^{-1} \leq a$ 
    using OrderedGroup_ZF_1_L4 OrderedGroup_ZF_1_L1
    group0.group_inv_of_two group0.group0_2_L2
    by simp
qed

```

If  $b$  is between  $a$  and  $a \cdot c$ , then  $b \cdot a^{-1} \leq c$ .

```

lemma (in group3) OrderedGroup_ZF_3_L8C:
  assumes A1:  $a \leq b$  and A2:  $c \in G$  and A3:  $b \leq c \cdot a$ 
  shows  $|b \cdot a^{-1}| \leq c$ 
proof -
  from A1 A2 A3 have  $b \cdot a^{-1} \leq c$ 
    using OrderedGroup_ZF_1_L9C OrderedGroup_ZF_1_L4
    by simp
  moreover have  $(b \cdot a^{-1})^{-1} \leq c$ 
proof -
  from A1 have T:  $a \in G$   $b \in G$ 
    using OrderedGroup_ZF_1_L4 by auto
  with A1 have  $a \cdot b^{-1} \leq 1$ 
    using OrderedGroup_ZF_1_L9 by blast

```

```

    moreover
    from A1 A3 have  $a \leq c \cdot a$ 
      by (rule Group_order_transitive)
    with ordGroupAssum T have  $a \cdot a^{-1} \leq c \cdot a \cdot a^{-1}$ 
      using OrderedGroup_ZF_1_L1 group0.inverse_in_group
      IsAnOrdGroup_def by simp
    with T A2 have  $1 \leq c$ 
      using OrderedGroup_ZF_1_L1
group0.group0_2_L6 group0.inv_cancel_two
      by simp
    ultimately have  $a \cdot b^{-1} \leq c$ 
      by (rule Group_order_transitive)
    with T show  $(b \cdot a^{-1})^{-1} \leq c$ 
      using OrderedGroup_ZF_1_L1 group0.group0_2_L12
      by simp
  qed
  ultimately show  $|b \cdot a^{-1}| \leq c$ 
    using OrderedGroup_ZF_3_L4 by simp
qed

```

For linearly ordered groups if the absolute values of elements in a set are bounded, then the set is bounded.

```

lemma (in group3) OrderedGroup_ZF_3_L9:
  assumes A1: r {is total on} G
  and A2:  $A \subseteq G$  and A3:  $\forall a \in A. |a| \leq L$ 
  shows IsBounded(A,r)
proof -
  from A1 A2 A3 have
     $\forall a \in A. a \leq L \ \forall a \in A. L^{-1} \leq a$ 
    using OrderedGroup_ZF_3_L8 OrderedGroup_ZF_3_L8A by auto
  then show IsBounded(A,r) using
    IsBoundedAbove_def IsBoundedBelow_def IsBounded_def
    by auto
qed

```

A slightly more general version of the previous lemma, stating the same fact for a set defined by separation.

```

lemma (in group3) OrderedGroup_ZF_3_L9A:
  assumes A1: r {is total on} G
  and A2:  $\forall x \in X. b(x) \in G \wedge |b(x)| \leq L$ 
  shows IsBounded( $\{b(x). x \in X\}$ ,r)
proof -
  from A2 have  $\{b(x). x \in X\} \subseteq G \ \forall a \in \{b(x). x \in X\}. |a| \leq L$ 
    by auto
  with A1 show thesis using OrderedGroup_ZF_3_L9 by blast
qed

```

A special form of the previous lemma stating a similar fact for an image of a set by a function with values in a linearly ordered group.

```

lemma (in group3) OrderedGroup_ZF_3_L9B:
  assumes A1: r {is total on} G
  and A2: f:X→G and A3: A⊆X
  and A4: ∀x∈A. |f(x)| ≤ L
  shows IsBounded(f(A),r)
proof -
  from A2 A3 A4 have ∀x∈A. f(x) ∈ G ∧ |f(x)| ≤ L
    using apply_funtype by auto
  with A1 have IsBounded({f(x). x∈A},r)
    by (rule OrderedGroup_ZF_3_L9A)
  with A2 A3 show IsBounded(f(A),r)
    using func_imagedef by simp
qed

```

For linearly ordered groups if  $l \leq a \leq u$  then  $|a|$  is smaller than the greater of  $|l|, |u|$ .

```

lemma (in group3) OrderedGroup_ZF_3_L10:
  assumes A1: r {is total on} G
  and A2: 1≤a a≤u
  shows
    |a| ≤ GreaterOf(r, |l|, |u|)
proof -
  from A2 have T1: |l| ∈ G |a| ∈ G |u| ∈ G
    using OrderedGroup_ZF_1_L4 OrderedGroup_ZF_3_L1 apply_funtype
    by auto
  { assume A3: a∈G+
    with A2 have 1≤a a≤u
      using OrderedGroup_ZF_1_L2 by auto
    then have 1≤u by (rule Group_order_transitive)
    with A2 A3 have |a|≤|u|
      using OrderedGroup_ZF_1_L2 OrderedGroup_ZF_3_L2 by simp
    moreover from A1 T1 have |u| ≤ GreaterOf(r, |l|, |u|)
      using Order_ZF_3_L2 by simp
    ultimately have |a| ≤ GreaterOf(r, |l|, |u|)
      by (rule Group_order_transitive) }
  moreover
  { assume A4: a∉G+
    with A2 have T2:
      1∈G |l| ∈ G |a| ∈ G |u| ∈ G a ∈ G-G+
      using OrderedGroup_ZF_1_L4 OrderedGroup_ZF_3_L1 apply_funtype
      by auto
    with A2 have 1 ∈ G-G+ using OrderedGroup_ZF_1_L4D by fast
    with T2 A2 have |a| ≤ |l|
      using OrderedGroup_ZF_3_L3 OrderedGroup_ZF_1_L5
      by simp
    moreover from A1 T2 have |l| ≤ GreaterOf(r, |l|, |u|)
      using Order_ZF_3_L2 by simp
    ultimately have |a| ≤ GreaterOf(r, |l|, |u|)
      by (rule Group_order_transitive) }

```

ultimately show thesis by blast  
qed

For linearly ordered groups if a set is bounded then the absolute values are bounded.

```
lemma (in group3) OrderedGroup_ZF_3_L10A:
  assumes A1: r {is total on} G
  and A2: IsBounded(A,r)
  shows  $\exists L. \forall a \in A. |a| \leq L$ 
proof -
  { assume A = 0 then have thesis by auto }
  moreover
  { assume A3: A  $\neq$  0
    with A2 have  $\exists u. \forall g \in A. g \leq u$  and  $\exists l. \forall g \in A. l \leq g$ 
      using IsBounded_def IsBoundedAbove_def IsBoundedBelow_def
      by auto
    then obtain u l where  $\forall g \in A. l \leq g \wedge g \leq u$ 
      by auto
    with A1 have  $\forall a \in A. |a| \leq \text{GreaterOf}(r, |l|, |u|)$ 
      using OrderedGroup_ZF_3_L10 by simp
    then have thesis by auto }
  ultimately show thesis by blast
qed
```

A slightly more general version of the previous lemma, stating the same fact for a set defined by separation.

```
lemma (in group3) OrderedGroup_ZF_3_L11:
  assumes r {is total on} G
  and IsBounded({b(x). x  $\in$  X}, r)
  shows  $\exists L. \forall x \in X. |b(x)| \leq L$ 
  using assms OrderedGroup_ZF_3_L10A by blast
```

Absolute values of elements of a finite image of a nonempty set are bounded by an element of the group.

```
lemma (in group3) OrderedGroup_ZF_3_L11A:
  assumes A1: r {is total on} G
  and A2: X  $\neq$  0 and A3: {b(x). x  $\in$  X}  $\in$  Fin(G)
  shows  $\exists L \in G. \forall x \in X. |b(x)| \leq L$ 
proof -
  from A1 A3 have  $\exists L. \forall x \in X. |b(x)| \leq L$ 
    using ord_group_fin_bounded OrderedGroup_ZF_3_L11
    by simp
  then obtain L where I:  $\forall x \in X. |b(x)| \leq L$ 
    using OrderedGroup_ZF_3_L11 by auto
  from A2 obtain x where x  $\in$  X by auto
  with I show thesis using OrderedGroup_ZF_1_L4
    by blast
qed
```



In totally ordered groups the absolute value of a nonunit element is in  $G_+$ .

```

lemma (in group3) OrderedGroup_ZF_3_L12:
  assumes A1: r {is total on} G
  and A2: a ∈ G  and A3: a ≠ 1
  shows |a| ∈ G+
proof -
  from A1 A2 have |a| ∈ G  1 ≤ |a|
    using OrderedGroup_ZF_3_L1 apply_funtype
    OrderedGroup_ZF_3_L3B OrderedGroup_ZF_1_L2
  by auto
  moreover from A2 A3 have |a| ≠ 1
    using OrderedGroup_ZF_3_L3D by auto
  ultimately show |a| ∈ G+
    using PositiveSet_def by auto
qed

```

## 28.2 Maximum absolute value of a set

Quite often when considering inequalities we prefer to talk about the absolute values instead of raw elements of a set. This section formalizes some material that is useful for that.

If a set has a maximum and minimum, then the greater of the absolute value of the maximum and minimum belongs to the image of the set by the absolute value function.

```

lemma (in group3) OrderedGroup_ZF_4_L1:
  assumes A ⊆ G
  and HasAmaximum(r,A) HasAminimum(r,A)
  and M = GreaterOf(r, |Minimum(r,A)|, |Maximum(r,A)|)
  shows M ∈ AbsoluteValue(G,P,r)(A)
  using ordGroupAssum assms IsAnOrdGroup_def IsPartOrder_def
  Order_ZF_4_L3 Order_ZF_4_L4 OrderedGroup_ZF_3_L1
  func_imagedef GreaterOf_def by auto

```

If a set has a maximum and minimum, then the greater of the absolute value of the maximum and minimum bounds absolute values of all elements of the set.

```

lemma (in group3) OrderedGroup_ZF_4_L2:
  assumes A1: r {is total on} G
  and A2: HasAmaximum(r,A) HasAminimum(r,A)
  and A3: a ∈ A
  shows |a| ≤ GreaterOf(r, |Minimum(r,A)|, |Maximum(r,A)|)
proof -
  from ordGroupAssum A2 A3 have
    Minimum(r,A) ≤ a ≤ Maximum(r,A)
  using IsAnOrdGroup_def IsPartOrder_def Order_ZF_4_L3 Order_ZF_4_L4
  by auto

```

```

    with A1 show thesis by (rule OrderedGroup_ZF_3_L10)
qed

```

If a set has a maximum and minimum, then the greater of the absolute value of the maximum and minimum bounds absolute values of all elements of the set. In this lemma the absolute values of elements of a set are represented as the elements of the image of the set by the absolute value function.

```

lemma (in group3) OrderedGroup_ZF_4_L3:
  assumes r {is total on} G and A  $\subseteq$  G
  and HasAmaximum(r,A) HasAminimum(r,A)
  and b  $\in$  AbsoluteValue(G,P,r)(A)
  shows b  $\leq$  GreaterOf(r,|Minimum(r,A)|,|Maximum(r,A)|)
  using assms OrderedGroup_ZF_3_L1 func_imagedef OrderedGroup_ZF_4_L2
  by auto

```

If a set has a maximum and minimum, then the set of absolute values also has a maximum.

```

lemma (in group3) OrderedGroup_ZF_4_L4:
  assumes A1: r {is total on} G and A2: A  $\subseteq$  G
  and A3: HasAmaximum(r,A) HasAminimum(r,A)
  shows HasAmaximum(r,AbsoluteValue(G,P,r)(A))
proof -
  let M = GreaterOf(r,|Minimum(r,A)|,|Maximum(r,A)|)
  from A2 A3 have M  $\in$  AbsoluteValue(G,P,r)(A)
    using OrderedGroup_ZF_4_L1 by simp
  moreover from A1 A2 A3 have
     $\forall b \in \text{AbsoluteValue}(G,P,r)(A). b \leq M$ 
    using OrderedGroup_ZF_4_L3 by simp
  ultimately show thesis using HasAmaximum_def by auto
qed

```

If a set has a maximum and a minimum, then all absolute values are bounded by the maximum of the set of absolute values.

```

lemma (in group3) OrderedGroup_ZF_4_L5:
  assumes A1: r {is total on} G and A2: A  $\subseteq$  G
  and A3: HasAmaximum(r,A) HasAminimum(r,A)
  and A4: a  $\in$  A
  shows |a|  $\leq$  Maximum(r,AbsoluteValue(G,P,r)(A))
proof -
  from A2 A4 have |a|  $\in$  AbsoluteValue(G,P,r)(A)
    using OrderedGroup_ZF_3_L1 func_imagedef by auto
  with ordGroupAssum A1 A2 A3 show thesis using
    IsAnOrdGroup_def IsPartOrder_def OrderedGroup_ZF_4_L4
    Order_ZF_4_L3 by simp
qed

```

### 28.3 Alternative definitions

Sometimes it is useful to define the order by prescribing the set of positive or nonnegative elements. This section deals with two such definitions. One takes a subset  $H$  of  $G$  that is closed under the group operation,  $1 \notin H$  and for every  $a \in H$  we have either  $a \in H$  or  $a^{-1} \in H$ . Then the order is defined as  $a \leq b$  iff  $a = b$  or  $a^{-1}b \in H$ . For abelian groups this makes a linearly ordered group. We will refer to order defined this way in the comments as the order defined by a positive set. The context used in this section is the `group0` context defined in `Group_ZF` theory. Recall that `f` in that context denotes the group operation (unlike in the previous sections where the group operation was denoted `P`).

The order defined by a positive set is the same as the order defined by a nonnegative set.

```
lemma (in group0) OrderedGroup_ZF_5_L1:
  assumes A1:  $r = \{p \in G \times G. \text{fst}(p) = \text{snd}(p) \vee \text{fst}(p)^{-1} \cdot \text{snd}(p) \in H\}$ 
  shows  $\langle a, b \rangle \in r \iff a \in G \wedge b \in G \wedge a^{-1} \cdot b \in H \cup \{1\}$ 
proof
  assume  $\langle a, b \rangle \in r$ 
  with A1 show  $a \in G \wedge b \in G \wedge a^{-1} \cdot b \in H \cup \{1\}$ 
    using group0_2_L6 by auto
next assume  $a \in G \wedge b \in G \wedge a^{-1} \cdot b \in H \cup \{1\}$ 
  then have  $a \in G \wedge b \in G \wedge b = (a^{-1})^{-1} \vee a \in G \wedge b \in G \wedge a^{-1} \cdot b \in H$ 
    using inverse_in_group group0_2_L9 by auto
  with A1 show  $\langle a, b \rangle \in r$  using group_inv_of_inv
    by auto
qed
```

The relation defined by a positive set is antisymmetric.

```
lemma (in group0) OrderedGroup_ZF_5_L2:
  assumes A1:  $r = \{p \in G \times G. \text{fst}(p) = \text{snd}(p) \vee \text{fst}(p)^{-1} \cdot \text{snd}(p) \in H\}$ 
  and A2:  $\forall a \in G. a \neq 1 \implies (a \in H) \text{ Xor } (a^{-1} \in H)$ 
  shows antisym(r)
proof -
  { fix a b assume A3:  $\langle a, b \rangle \in r \ \langle b, a \rangle \in r$ 
    with A1 have T:  $a \in G \ b \in G$  by auto
    { assume A4:  $a \neq b$ 
      with A1 A3 have  $a^{-1} \cdot b \in G \ a^{-1} \cdot b \in H \ (a^{-1} \cdot b)^{-1} \in H$ 
    using inverse_in_group group0_2_L1 monoid0.group0_1_L1 group0_2_L12
    by auto
      with A2 have  $a^{-1} \cdot b = 1$  using Xor_def by auto
      with T A4 have False using group0_2_L11 by auto
    } then have  $a = b$  by auto
  } then show antisym(r) by (rule antisymI)
qed
```

The relation defined by a positive set is transitive.

```

lemma (in group0) OrderedGroup_ZF_5_L3:
  assumes A1:  $r = \{p \in G \times G. \text{fst}(p) = \text{snd}(p) \vee \text{fst}(p)^{-1} \cdot \text{snd}(p) \in H\}$ 
  and A2:  $H \subseteq G$   $H$  {is closed under}  $P$ 
  shows  $\text{trans}(r)$ 
proof -
  { fix a b c assume  $\langle a, b \rangle \in r$   $\langle b, c \rangle \in r$ 
    with A1 have
       $a \in G \wedge b \in G \wedge a^{-1} \cdot b \in H \cup \{1\}$ 
       $b \in G \wedge c \in G \wedge b^{-1} \cdot c \in H \cup \{1\}$ 
      using OrderedGroup_ZF_5_L1 by auto
    with A2 have
      I:  $a \in G$   $b \in G$   $c \in G$ 
      and  $(a^{-1} \cdot b) \cdot (b^{-1} \cdot c) \in H \cup \{1\}$ 
      using inverse_in_group group0_2_L17 IsOpClosed_def
      by auto
    moreover from I have  $a^{-1} \cdot c = (a^{-1} \cdot b) \cdot (b^{-1} \cdot c)$ 
      by (rule group0_2_L14A)
    ultimately have  $\langle a, c \rangle \in G \times G$   $a^{-1} \cdot c \in H \cup \{1\}$ 
      by auto
    with A1 have  $\langle a, c \rangle \in r$  using OrderedGroup_ZF_5_L1
      by auto
  } then have  $\forall a b c. \langle a, b \rangle \in r \wedge \langle b, c \rangle \in r \longrightarrow \langle a, c \rangle \in r$ 
    by blast
  then show  $\text{trans}(r)$  by (rule Fol1_L2)
qed

```

The relation defined by a positive set is translation invariant. With our definition this step requires the group to be abelian.

```

lemma (in group0) OrderedGroup_ZF_5_L4:
  assumes A1:  $r = \{p \in G \times G. \text{fst}(p) = \text{snd}(p) \vee \text{fst}(p)^{-1} \cdot \text{snd}(p) \in H\}$ 
  and A2:  $P$  {is commutative on}  $G$ 
  and A3:  $\langle a, b \rangle \in r$  and A4:  $c \in G$ 
  shows  $\langle a \cdot c, b \cdot c \rangle \in r \wedge \langle c \cdot a, c \cdot b \rangle \in r$ 
proof
  from A1 A3 A4 have
    I:  $a \in G$   $b \in G$   $a \cdot c \in G$   $b \cdot c \in G$ 
    and II:  $a^{-1} \cdot b \in H \cup \{1\}$ 
    using OrderedGroup_ZF_5_L1 group_op_closed
    by auto
  with A2 A4 have  $(a \cdot c)^{-1} \cdot (b \cdot c) \in H \cup \{1\}$ 
    using group0_4_L6D by simp
  with A1 I show  $\langle a \cdot c, b \cdot c \rangle \in r$  using OrderedGroup_ZF_5_L1
    by auto
  with A2 A4 I show  $\langle c \cdot a, c \cdot b \rangle \in r$ 
    using IsCommutative_def by simp
qed

```

If  $H \subseteq G$  is closed under the group operation  $1 \notin H$  and for every  $a \in H$  we have either  $a \in H$  or  $a^{-1} \in H$ , then the relation " $\leq$ " defined by  $a \leq b \Leftrightarrow$

$a^{-1}b \in H$  orders the group  $G$ . In such order  $H$  may be the set of positive or nonnegative elements.

```

lemma (in group0) OrderedGroup_ZF_5_L5:
  assumes A1: P {is commutative on} G
  and A2:  $H \subseteq G$   $H$  {is closed under} P
  and A3:  $\forall a \in G. a \neq 1 \longrightarrow (a \in H) \text{ Xor } (a^{-1} \in H)$ 
  and A4:  $r = \{p \in G \times G. \text{fst}(p) = \text{snd}(p) \vee \text{fst}(p)^{-1} \cdot \text{snd}(p) \in H\}$ 
  shows
    IsAnOrdGroup(G,P,r)
  r {is total on} G
  Nonnegative(G,P,r) = PositiveSet(G,P,r)  $\cup \{1\}$ 
proof -
  from groupAssum A2 A3 A4 have
    IsAgroup(G,P)  $r \subseteq G \times G$  IsPartOrder(G,r)
    using refl_def OrderedGroup_ZF_5_L2 OrderedGroup_ZF_5_L3
    IsPartOrder_def by auto
  moreover from A1 A4 have
     $\forall g \in G. \forall a b. \langle a, b \rangle \in r \longrightarrow \langle a \cdot g, b \cdot g \rangle \in r \wedge \langle g \cdot a, g \cdot b \rangle \in r$ 
    using OrderedGroup_ZF_5_L4 by blast
  ultimately show IsAnOrdGroup(G,P,r)
    using IsAnOrdGroup_def by simp
  then show Nonnegative(G,P,r) = PositiveSet(G,P,r)  $\cup \{1\}$ 
    using group3_def group3.OrderedGroup_ZF_1_L24
    by simp
  { fix a b
    assume T:  $a \in G \ b \in G$ 
    then have T1:  $a^{-1} \cdot b \in G$ 
      using inverse_in_group group_op_closed by simp
    { assume  $\langle a, b \rangle \notin r$ 
      with A4 T have I:  $a \neq b$  and II:  $a^{-1} \cdot b \notin H$ 
    }
  } by auto
  from A3 T T1 I have  $(a^{-1} \cdot b \in H) \text{ Xor } ((a^{-1} \cdot b)^{-1} \in H)$ 
  using group0_2_L11 by auto
  with A4 T II have  $\langle b, a \rangle \in r$ 
  using Xor_def group0_2_L12 by simp
  } then have  $\langle a, b \rangle \in r \vee \langle b, a \rangle \in r$  by auto
  } then show r {is total on} G using IsTotal_def
  by simp
qed

```

If the set defined as in OrderedGroup\_ZF\_5\_L4 does not contain the neutral element, then it is the positive set for the resulting order.

```

lemma (in group0) OrderedGroup_ZF_5_L6:
  assumes P {is commutative on} G
  and  $H \subseteq G$  and  $1 \notin H$ 
  and  $r = \{p \in G \times G. \text{fst}(p) = \text{snd}(p) \vee \text{fst}(p)^{-1} \cdot \text{snd}(p) \in H\}$ 
  shows PositiveSet(G,P,r) = H
  using assms group_inv_of_one group0_2_L2 PositiveSet_def
  by auto

```

The next definition describes how we construct an order relation from the prescribed set of positive elements.

**definition**

```
OrderFromPosSet(G,P,H) ≡
  {p ∈ G×G. fst(p) = snd(p) ∨ P(GroupInv(G,P)(fst(p)),snd(p)) ∈ H }
```

The next theorem rephrases lemmas `OrderedGroup_ZF_5_L5` and `OrderedGroup_ZF_5_L6` using the definition of the order from the positive set `OrderFromPosSet`. To summarize, this is what it says: Suppose that  $H \subseteq G$  is a set closed under that group operation such that  $1 \notin H$  and for every nonunit group element  $a$  either  $a \in H$  or  $a^{-1} \in H$ . Define the order as  $a \leq b$  iff  $a = b$  or  $a^{-1} \cdot b \in H$ . Then this order makes  $G$  into a linearly ordered group such  $H$  is the set of positive elements (and then of course  $H \cup \{1\}$  is the set of nonnegative elements).

**theorem** (in `group0`) `Group_ord_by_positive_set`:

```
  assumes P {is commutative on} G
  and H⊆G   H {is closed under} P   1 ∉ H
  and ∀a∈G. a≠1 ⟶ (a∈H) Xor (a-1∈H)
  shows
    IsAnOrdGroup(G,P,OrderFromPosSet(G,P,H))
    OrderFromPosSet(G,P,H) {is total on} G
    PositiveSet(G,P,OrderFromPosSet(G,P,H)) = H
    Nonnegative(G,P,OrderFromPosSet(G,P,H)) = H ∪ {1}
  using assms OrderFromPosSet_def OrderedGroup_ZF_5_L5 OrderedGroup_ZF_5_L6
  by auto
```

## 28.4 Odd Extensions

In this section we verify properties of odd extensions of functions defined on  $G_+$ . An odd extension of a function  $f : G_+ \rightarrow G$  is a function  $f^\circ : G \rightarrow G$  defined by  $f^\circ(x) = f(x)$  if  $x \in G_+$ ,  $f(1) = 1$  and  $f^\circ(x) = (f(x^{-1}))^{-1}$  for  $x < 1$ . Such function is the unique odd function that is equal to  $f$  when restricted to  $G_+$ .

The next lemma is just to see the definition of the odd extension in the notation used in the `group1` context.

**lemma** (in `group3`) `OrderedGroup_ZF_6_L1`:

```
  shows f° = f ∪ {⟨a, (f(a-1))-1⟩. a ∈ -G+} ∪ {⟨1,1⟩}
  using OddExtension_def by simp
```

A technical lemma that states that from a function defined on  $G_+$  with values in  $G$  we have  $(f(a^{-1}))^{-1} \in G$ .

**lemma** (in `group3`) `OrderedGroup_ZF_6_L2`:

```
  assumes f: G+→G and a∈-G+
  shows
    f(a-1) ∈ G
```

```

(f(a-1))-1 ∈ G
using assms OrderedGroup_ZF_1_L27 apply_funtype
  OrderedGroup_ZF_1_L1 group0.inverse_in_group
by auto

```

The main theorem about odd extensions. It basically says that the odd extension of a function is what we want to to be.

```

lemma (in group3) odd_ext_props:
  assumes A1: r {is total on} G and A2: f: G+→G
  shows
    f° : G → G
    ∀a∈G+. (f°)(a) = f(a)
    ∀a∈(-G+). (f°)(a) = (f(a-1))-1
    (f°)(1) = 1
proof -
  from A1 A2 have I:
    f: G+→G
    ∀a∈-G+. (f(a-1))-1 ∈ G
    G+ ∩ (-G+) = 0
    1 ∉ G+ ∪ (-G+)
    f° = f ∪ {⟨a, (f(a-1))-1}. a ∈ -G+} ∪ {⟨1,1⟩}
    using OrderedGroup_ZF_6_L2 OrdGroup_decomp2 OrderedGroup_ZF_6_L1
    by auto
  then have f°: G+ ∪ (-G+) ∪ {1} → G ∪ G ∪ {1}
    by (rule func1_1_L11E)
  moreover from A1 have
    G+ ∪ (-G+) ∪ {1} = G
    G ∪ G ∪ {1} = G
    using OrdGroup_decomp2 OrderedGroup_ZF_1_L1 group0.group0_2_L2
    by auto
  ultimately show f° : G → G by simp
  from I show ∀a∈G+. (f°)(a) = f(a)
    by (rule func1_1_L11E)
  from I show ∀a∈(-G+). (f°)(a) = (f(a-1))-1
    by (rule func1_1_L11E)
  from I show (f°)(1) = 1
    by (rule func1_1_L11E)
qed

```

Odd extensions are odd, of course.

```

lemma (in group3) oddext_is_odd:
  assumes A1: r {is total on} G and A2: f: G+→G
  and A3: a∈G
  shows (f°)(a-1) = ((f°)(a))-1
proof -
  from A1 A3 have a∈G+ ∨ a ∈ (-G+) ∨ a=1
    using OrdGroup_decomp2 by blast
  moreover
  { assume a∈G+

```

```

with A1 A2 have  $a^{-1} \in -G_+$  and  $(f^\circ)(a) = f(a)$ 
  using OrderedGroup_ZF_1_L25 odd_ext_props by auto
with A1 A2 have
   $(f^\circ)(a^{-1}) = (f((a^{-1})^{-1}))^{-1}$  and  $(f(a))^{-1} = ((f^\circ)(a))^{-1}$ 
  using odd_ext_props by auto
with A3 have  $(f^\circ)(a^{-1}) = ((f^\circ)(a))^{-1}$ 
  using OrderedGroup_ZF_1_L1 group0.group_inv_of_inv
  by simp }
moreover
{ assume A4:  $a \in -G_+$ 
  with A1 A2 have  $a^{-1} \in G_+$  and  $(f^\circ)(a) = (f(a^{-1}))^{-1}$ 
    using OrderedGroup_ZF_1_L27 odd_ext_props
    by auto
  with A1 A2 A4 have  $(f^\circ)(a^{-1}) = ((f^\circ)(a))^{-1}$ 
    using odd_ext_props OrderedGroup_ZF_6_L2
    OrderedGroup_ZF_1_L1 group0.group_inv_of_inv
    by simp }
moreover
{ assume a = 1
  with A1 A2 have  $(f^\circ)(a^{-1}) = ((f^\circ)(a))^{-1}$ 
    using OrderedGroup_ZF_1_L1 group0.group_inv_of_one
    odd_ext_props by simp
  }
ultimately show  $(f^\circ)(a^{-1}) = ((f^\circ)(a))^{-1}$ 
  by auto
qed

```

Another way of saying that odd extensions are odd.

```

lemma (in group3) oddext_is_odd_alt:
  assumes A1:  $r \text{ \{is total on\} } G$  and A2:  $f: G_+ \rightarrow G$ 
  and A3:  $a \in G$ 
  shows  $((f^\circ)(a^{-1}))^{-1} = (f^\circ)(a)$ 
proof -
  from A1 A2 have
     $f^\circ : G \rightarrow G$ 
     $\forall a \in G. (f^\circ)(a^{-1}) = ((f^\circ)(a))^{-1}$ 
    using odd_ext_props oddext_is_odd by auto
  then have  $\forall a \in G. ((f^\circ)(a^{-1}))^{-1} = (f^\circ)(a)$ 
    using OrderedGroup_ZF_1_L1 group0.group0_6_L2 by simp
  with A3 show  $((f^\circ)(a^{-1}))^{-1} = (f^\circ)(a)$  by simp
qed

```

## 28.5 Functions with infinite limits

In this section we consider functions  $f : G \rightarrow G$  with the property that for  $f(x)$  is arbitrarily large for large enough  $x$ . More precisely, for every  $a \in G$  there exist  $b \in G_+$  such that for every  $x \geq b$  we have  $f(x) \geq a$ . In a sense this means that  $\lim_{x \rightarrow \infty} f(x) = \infty$ , hence the title of this section. We also prove dual statements for functions such that  $\lim_{x \rightarrow -\infty} f(x) = -\infty$ .



If an image of a set by a function with infinite positive limit is bounded above, then the set itself is bounded above.

```

lemma (in group3) OrderedGroup_ZF_7_L1:
  assumes A1: r {is total on} G and A2:  $G \neq \{1\}$  and
  A3:  $f:G \rightarrow G$  and
  A4:  $\forall a \in G. \exists b \in G_+. \forall x. b \leq x \longrightarrow a \leq f(x)$  and
  A5:  $A \subseteq G$  and
  A6: IsBoundedAbove( $f(A)$ ,r)
  shows IsBoundedAbove(A,r)
proof -
  { assume  $\neg$ IsBoundedAbove(A,r)
    then have I:  $\forall u. \exists x \in A. \neg(x \leq u)$ 
      using IsBoundedAbove_def by auto
    have  $\forall a \in G. \exists y \in f(A). a \leq y$ 
      proof -
      { fix a assume  $a \in G$ 
        with A4 obtain b where
          II:  $b \in G_+$  and III:  $\forall x. b \leq x \longrightarrow a \leq f(x)$ 
          by auto
        from I obtain x where IV:  $x \in A$  and  $\neg(x \leq b)$ 
          by auto
        with A1 A5 II have
          r {is total on} G
           $x \in G$   $b \in G$   $\neg(x \leq b)$ 
          using PositiveSet_def by auto
        with III have  $a \leq f(x)$ 
          using OrderedGroup_ZF_1_L8 by blast
        with A3 A5 IV have  $\exists y \in f(A). a \leq y$ 
          using func_imagedef by auto
        } thus thesis by simp
      } qed
    with A1 A2 A6 have False using OrderedGroup_ZF_2_L2A
      by simp
  } thus thesis by auto
qed

```

If an image of a set defined by separation by a function with infinite positive limit is bounded above, then the set itself is bounded above.

```

lemma (in group3) OrderedGroup_ZF_7_L2:
  assumes A1: r {is total on} G and A2:  $G \neq \{1\}$  and
  A3:  $X \neq 0$  and A4:  $f:G \rightarrow G$  and
  A5:  $\forall a \in G. \exists b \in G_+. \forall y. b \leq y \longrightarrow a \leq f(y)$  and
  A6:  $\forall x \in X. b(x) \in G \wedge f(b(x)) \leq U$ 
  shows  $\exists u. \forall x \in X. b(x) \leq u$ 
proof -
  let A = { $b(x). x \in X$ }
  from A6 have I:  $A \subseteq G$  by auto
  moreover note assms
  moreover have IsBoundedAbove( $f(A)$ ,r)

```

```

proof -
  from A4 A6 I have  $\forall z \in f(A). \langle z, U \rangle \in r$ 
    using func_imagedef by simp
  then show IsBoundedAbove(f(A),r)
    by (rule Order_ZF_3_L10)
qed
ultimately have IsBoundedAbove(A,r) using OrderedGroup_ZF_7_L1
  by simp
with A3 have  $\exists u. \forall y \in A. y \leq u$ 
  using IsBoundedAbove_def by simp
then show  $\exists u. \forall x \in X. b(x) \leq u$  by auto
qed

```

If the image of a set defined by separation by a function with infinite negative limit is bounded below, then the set itself is bounded above. This is dual to OrderedGroup\_ZF\_7\_L2.

```

lemma (in group3) OrderedGroup_ZF_7_L3:
  assumes A1: r {is total on} G and A2:  $G \neq \{1\}$  and
  A3:  $X \neq 0$  and A4:  $f: G \rightarrow G$  and
  A5:  $\forall a \in G. \exists b \in G_+. \forall y. b \leq y \longrightarrow f(y^{-1}) \leq a$  and
  A6:  $\forall x \in X. b(x) \in G \wedge L \leq f(b(x))$ 
  shows  $\exists 1. \forall x \in X. 1 \leq b(x)$ 

```

```

proof -
  let g = GroupInv(G,P) 0 f 0 GroupInv(G,P)
  from ordGroupAssum have I: GroupInv(G,P) :  $G \rightarrow G$ 
    using IsAnOrdGroup_def group0_2_T2 by simp
  with A4 have II:  $\forall x \in G. g(x) = (f(x^{-1}))^{-1}$ 
    using func1_1_L18 by simp
  note A1 A2 A3
  moreover from A4 I have  $g : G \rightarrow G$ 
    using comp_fun by blast
  moreover have  $\forall a \in G. \exists b \in G_+. \forall y. b \leq y \longrightarrow a \leq g(y)$ 
  proof -
    { fix a assume A7:  $a \in G$ 
      then have  $a^{-1} \in G$ 
        using OrderedGroup_ZF_1_L1 group0.inverse_in_group
        by simp
      with A5 obtain b where
        III:  $b \in G_+$  and  $\forall y. b \leq y \longrightarrow f(y^{-1}) \leq a^{-1}$ 
        by auto
      with II A7 have  $\forall y. b \leq y \longrightarrow a \leq g(y)$ 
        using OrderedGroup_ZF_1_L5AD OrderedGroup_ZF_1_L4
        by simp
      with III have  $\exists b \in G_+. \forall y. b \leq y \longrightarrow a \leq g(y)$ 
        by auto
    } then show  $\forall a \in G. \exists b \in G_+. \forall y. b \leq y \longrightarrow a \leq g(y)$ 
      by simp
  qed
  moreover have  $\forall x \in X. b(x)^{-1} \in G \wedge g(b(x)^{-1}) \leq L^{-1}$ 

```

```

proof-
  { fix x assume x∈X
    with A6 have
T:  $b(x) \in G \wedge b(x)^{-1} \in G$  and  $L \leq f(b(x))$ 
using OrderedGroup_ZF_1_L1 group0.inverse_in_group
by auto
    then have  $(f(b(x)))^{-1} \leq L^{-1}$ 
using OrderedGroup_ZF_1_L5 by simp
    moreover from II T have  $(f(b(x)))^{-1} = g(b(x)^{-1})$ 
using OrderedGroup_ZF_1_L1 group0.group_inv_of_inv
by simp
    ultimately have  $g(b(x)^{-1}) \leq L^{-1}$  by simp
    with T have  $b(x)^{-1} \in G \wedge g(b(x)^{-1}) \leq L^{-1}$ 
by simp
  } then show  $\forall x \in X. b(x)^{-1} \in G \wedge g(b(x)^{-1}) \leq L^{-1}$ 
    by simp
qed
ultimately have  $\exists u. \forall x \in X. (b(x))^{-1} \leq u$ 
  by (rule OrderedGroup_ZF_7_L2)
then have  $\exists u. \forall x \in X. u^{-1} \leq (b(x)^{-1})^{-1}$ 
  using OrderedGroup_ZF_1_L5 by auto
with A6 show  $\exists 1. \forall x \in X. 1 \leq b(x)$ 
  using OrderedGroup_ZF_1_L1 group0.group_inv_of_inv
  by auto
qed

```

The next lemma combines OrderedGroup\_ZF\_7\_L2 and OrderedGroup\_ZF\_7\_L3 to show that if an image of a set defined by separation by a function with infinite limits is bounded, then the set itself is bounded.

```

lemma (in group3) OrderedGroup_ZF_7_L4:
  assumes A1:  $r$  {is total on}  $G$  and A2:  $G \neq \{1\}$  and
  A3:  $X \neq \emptyset$  and A4:  $f: G \rightarrow G$  and
  A5:  $\forall a \in G. \exists b \in G_+. \forall y. b \leq y \longrightarrow a \leq f(y)$  and
  A6:  $\forall a \in G. \exists b \in G_+. \forall y. b \leq y \longrightarrow f(y^{-1}) \leq a$  and
  A7:  $\forall x \in X. b(x) \in G \wedge L \leq f(b(x)) \wedge f(b(x)) \leq U$ 
shows  $\exists M. \forall x \in X. |b(x)| \leq M$ 
proof -
  from A7 have
    I:  $\forall x \in X. b(x) \in G \wedge f(b(x)) \leq U$  and
    II:  $\forall x \in X. b(x) \in G \wedge L \leq f(b(x))$ 
  by auto
  from A1 A2 A3 A4 A5 I have  $\exists u. \forall x \in X. b(x) \leq u$ 
    by (rule OrderedGroup_ZF_7_L2)
  moreover from A1 A2 A3 A4 A6 II have  $\exists 1. \forall x \in X. 1 \leq b(x)$ 
    by (rule OrderedGroup_ZF_7_L3)
  ultimately have  $\exists u 1. \forall x \in X. 1 \leq b(x) \wedge b(x) \leq u$ 
    by auto
  with A1 have  $\exists u 1. \forall x \in X. |b(x)| \leq \text{GreaterOf}(r, |1|, |u|)$ 
    using OrderedGroup_ZF_3_L10 by blast

```

```
    then show  $\exists M. \forall x \in X. |b(x)| \leq M$ 
      by auto
qed
end
```

## 29 Ring\_ZF.thy

```
theory Ring_ZF imports AbelianGroup_ZF
```

```
begin
```

This theory file covers basic facts about rings.

### 29.1 Definition and basic properties

In this section we define what is a ring and list the basic properties of rings.

We say that three sets  $(R, A, M)$  form a ring if  $(R, A)$  is an abelian group,  $(R, M)$  is a monoid and  $A$  is distributive with respect to  $M$  on  $R$ .  $A$  represents the additive operation on  $R$ . As such it is a subset of  $(R \times R) \times R$  (recall that in ZF set theory functions are sets). Similarly  $M$  represents the multiplicative operation on  $R$  and is also a subset of  $(R \times R) \times R$ . We don't require the multiplicative operation to be commutative in the definition of a ring.

**definition**

```
IsAring(R,A,M)  $\equiv$  IsAgroup(R,A)  $\wedge$  (A {is commutative on} R)  $\wedge$   
IsAmonoid(R,M)  $\wedge$  IsDistributive(R,A,M)
```

We also define the notion of having no zero divisors. In standard notation the ring has no zero divisors if for all  $a, b \in R$  we have  $a \cdot b = 0$  implies  $a = 0$  or  $b = 0$ .

**definition**

```
HasNoZeroDivs(R,A,M)  $\equiv$  ( $\forall a \in R. \forall b \in R.$   
M( $\langle a, b \rangle$ ) = TheNeutralElement(R,A)  $\longrightarrow$   
a = TheNeutralElement(R,A)  $\vee$  b = TheNeutralElement(R,A))
```

Next we define a locale that will be used when considering rings.

```
locale ring0 =
```

```
  fixes R and A and M
```

```
  assumes ringAssum: IsAring(R,A,M)
```

```
  fixes ringa (infixl + 90)
```

```
  defines ringa_def [simp]: a+b  $\equiv$  A( $\langle a, b \rangle$ )
```

```
  fixes ringminus (- _ 89)
```

```
  defines ringminus_def [simp]: (-a)  $\equiv$  GroupInv(R,A)(a)
```

```
  fixes ringsub (infixl - 90)
```

```
  defines ringsub_def [simp]: a-b  $\equiv$  a+(-b)
```

```

fixes ringm (infixl · 95)
defines ringm_def [simp]: a·b ≡ M⟨ a,b⟩

fixes ringzero (0)
defines ringzero_def [simp]: 0 ≡ TheNeutralElement(R,A)

fixes ringone (1)
defines ringone_def [simp]: 1 ≡ TheNeutralElement(R,M)

fixes ringtwo (2)
defines ringtwo_def [simp]: 2 ≡ 1+1

fixes ringsq (_^2 [96] 97)
defines ringsq_def [simp]: a^2 ≡ a·a

```

In the ring0 context we can use theorems proven in some other contexts.

```

lemma (in ring0) Ring_ZF_1_L1: shows
  monoid0(R,M)
  group0(R,A)
  A {is commutative on} R
  using ringAssum IsAring_def group0_def monoid0_def by auto

```

The additive operation in a ring is distributive with respect to the multiplicative operation.

```

lemma (in ring0) ring_oper_distr: assumes A1: a∈R b∈R c∈R
  shows
    a·(b+c) = a·b + a·c
    (b+c)·a = b·a + c·a
  using ringAssum assms IsAring_def IsDistributive_def by auto

```

Zero and one of the ring are elements of the ring. The negative of zero is zero.

```

lemma (in ring0) Ring_ZF_1_L2:
  shows 0∈R 1∈R (-0) = 0
  using Ring_ZF_1_L1 group0.group0_2_L2 monoid0.unit_is_neutral
    group0.group_inv_of_one by auto

```

The next lemma lists some properties of a ring that require one element of a ring.

```

lemma (in ring0) Ring_ZF_1_L3: assumes a∈R
  shows
    (-a) ∈ R
    -(-a) = a
    a+0 = a
    0+a = a
    a·1 = a
    1·a = a
    a-a = 0

```

```

a-0 = a
2·a = a+a
(-a)+a = 0
using assms Ring_ZF_1_L1 group0.inverse_in_group group0.group_inv_of_inv

    group0.group0_2_L6 group0.group0_2_L2 monoid0.unit_is_neutral
    Ring_ZF_1_L2 ring_oper_distr
by auto

```

Properties that require two elements of a ring.

```

lemma (in ring0) Ring_ZF_1_L4: assumes A1: a∈R b∈R
  shows
    a+b ∈ R
    a-b ∈ R
    a·b ∈ R
    a+b = b+a
  using ringAssum assms Ring_ZF_1_L1 Ring_ZF_1_L3
    group0.group0_2_L1 monoid0.group0_1_L1
    IsAring_def IsCommutative_def
  by auto

```

Cancellation of an element on both sides of equality. This is a property of groups, written in the (additive) notation we use for the additive operation in rings.

```

lemma (in ring0) ring_cancel_add:
  assumes A1: a∈R b∈R and A2: a + b = a
  shows b = 0
  using assms Ring_ZF_1_L1 group0.group0_2_L7 by simp

```

Any element of a ring multiplied by zero is zero.

```

lemma (in ring0) Ring_ZF_1_L6:
  assumes A1: x∈R shows 0·x = 0    x·0 = 0
proof -
  let a = x·1
  let b = x·0
  let c = 1·x
  let d = 0·x
  from A1 have
    a + b = x·(1 + 0)    c + d = (1 + 0)·x
    using Ring_ZF_1_L2 ring_oper_distr by auto
  moreover have x·(1 + 0) = a (1 + 0)·x = c
    using Ring_ZF_1_L2 Ring_ZF_1_L3 by auto
  ultimately have a + b = a and T1: c + d = c
    by auto
  moreover from A1 have
    a ∈ R    b ∈ R and T2: c ∈ R    d ∈ R
    using Ring_ZF_1_L2 Ring_ZF_1_L4 by auto
  ultimately have b = 0 using ring_cancel_add

```

```

    by blast
  moreover from T2 T1 have d = 0 using ring_cancel_add
    by blast
  ultimately show x·0 = 0  0·x = 0 by auto
qed

```

Negative can be pulled out of a product.

```

lemma (in ring0) Ring_ZF_1_L7:
  assumes A1: a∈R  b∈R
  shows
    (-a)·b = -(a·b)
    a·(-b) = -(a·b)
    (-a)·b = a·(-b)
proof -
  from A1 have I:
    a·b ∈ R  (-a) ∈ R  ((-a)·b) ∈ R
    (-b) ∈ R  a·(-b) ∈ R
    using Ring_ZF_1_L3 Ring_ZF_1_L4 by auto
  moreover have (-a)·b + a·b = 0
    and II: a·(-b) + a·b = 0
  proof -
    from A1 I have
      (-a)·b + a·b = ((-a)+ a)·b
      a·(-b) + a·b = a·((-b)+b)
      using ring_oper_distr by auto
    moreover from A1 have
      ((-a)+ a)·b = 0
      a·((-b)+b) = 0
      using Ring_ZF_1_L1 group0.group0_2_L6 Ring_ZF_1_L6
      by auto
    ultimately show
      (-a)·b + a·b = 0
      a·(-b) + a·b = 0
      by auto
  qed
  ultimately show (-a)·b = -(a·b)
    using Ring_ZF_1_L1 group0.group0_2_L9 by simp
  moreover from I II show a·(-b) = -(a·b)
    using Ring_ZF_1_L1 group0.group0_2_L9 by simp
  ultimately show (-a)·b = a·(-b) by simp
qed

```

Minus times minus is plus.

```

lemma (in ring0) Ring_ZF_1_L7A: assumes a∈R  b∈R
  shows (-a)·(-b) = a·b
  using asms Ring_ZF_1_L3 Ring_ZF_1_L7 Ring_ZF_1_L4
  by simp

```

Subtraction is distributive with respect to multiplication.



```

lemma (in ring0) Ring_ZF_1_L8: assumes a∈R  b∈R  c∈R
  shows
    a·(b-c) = a·b - a·c
    (b-c)·a = b·a - c·a
  using assms Ring_ZF_1_L3 ring_oper_distr Ring_ZF_1_L7 Ring_ZF_1_L4
  by auto

```

Other basic properties involving two elements of a ring.

```

lemma (in ring0) Ring_ZF_1_L9: assumes a∈R  b∈R
  shows
    (-b)-a = (-a)-b
    -(a+b) = (-a)-b
    -(a-b) = ((-a)+b)
    a-(-b) = a+b
  using assms ringAssum IsAring_def
    Ring_ZF_1_L1 group0.group0_4_L4  group0.group_inv_of_inv
  by auto

```

If the difference of two element is zero, then those elements are equal.

```

lemma (in ring0) Ring_ZF_1_L9A:
  assumes A1: a∈R  b∈R and A2: a-b = 0
  shows a=b
proof -
  from A1 A2 have
    group0(R,A)
    a∈R  b∈R
    A⟨a,GroupInv(R,A)(b)⟩ = TheNeutralElement(R,A)
  using Ring_ZF_1_L1 by auto
  then show a=b by (rule group0.group0_2_L11A)
qed

```

Other basic properties involving three elements of a ring.

```

lemma (in ring0) Ring_ZF_1_L10:
  assumes a∈R  b∈R  c∈R
  shows
    a+(b+c) = a+b+c

    a-(b+c) = a-b-c
    a-(b-c) = a-b+c
  using assms ringAssum Ring_ZF_1_L1 group0.group_oper_assoc
    IsAring_def group0.group0_4_L4A by auto

```

Another property with three elements.

```

lemma (in ring0) Ring_ZF_1_L10A:
  assumes A1: a∈R  b∈R  c∈R
  shows a+(b-c) = a+b-c
  using assms Ring_ZF_1_L3 Ring_ZF_1_L10 by simp

```

Associativity of addition and multiplication.

```

lemma (in ring0) Ring_ZF_1_L11:
  assumes a∈R b∈R c∈R
  shows
    a+b+c = a+(b+c)
    a·b·c = a·(b·c)
  using assms ringAssum Ring_ZF_1_L1 group0.group_oper_assoc
    IsAring_def IsAmonoid_def IsAssociative_def
  by auto

```

An interpretation of what it means that a ring has no zero divisors.

```

lemma (in ring0) Ring_ZF_1_L12:
  assumes HasNoZeroDivs(R,A,M)
  and a∈R a≠0 b∈R b≠0
  shows a·b≠0
  using assms HasNoZeroDivs_def by auto

```

In rings with no zero divisors we can cancel nonzero factors.

```

lemma (in ring0) Ring_ZF_1_L12A:
  assumes A1: HasNoZeroDivs(R,A,M) and A2: a∈R b∈R c∈R
  and A3: a·c = b·c and A4: c≠0
  shows a=b
proof -
  from A2 have T: a·c ∈ R a·b ∈ R
    using Ring_ZF_1_L4 by auto
  with A1 A2 A3 have a·b = 0 ∨ c=0
    using Ring_ZF_1_L3 Ring_ZF_1_L8 HasNoZeroDivs_def
    by simp
  with A2 A4 have a∈R b∈R a·b = 0
    by auto
  then show a=b by (rule Ring_ZF_1_L9A)
qed

```

In rings with no zero divisors if two elements are different, then after multiplying by a nonzero element they are still different.

```

lemma (in ring0) Ring_ZF_1_L12B:
  assumes A1: HasNoZeroDivs(R,A,M)
  a∈R b∈R c∈R a≠b c≠0
  shows a·c ≠ b·c
  using A1 Ring_ZF_1_L12A by auto

```

In rings with no zero divisors multiplying a nonzero element by a nonzero element changes the value.

```

lemma (in ring0) Ring_ZF_1_L12C:
  assumes A1: HasNoZeroDivs(R,A,M) and
  A2: a∈R b∈R and A3: 0≠a 1≠b
  shows a ≠ a·b
proof -
  { assume a = a·b

```

```

    with A1 A2 have a = 0 ∨ b-1 = 0
      using Ring_ZF_1_L3 Ring_ZF_1_L2 Ring_ZF_1_L8
Ring_ZF_1_L3 Ring_ZF_1_L2 Ring_ZF_1_L4 HasNoZeroDivs_def
    by simp
    with A2 A3 have False
      using Ring_ZF_1_L2 Ring_ZF_1_L9A by auto
  } then show a ≠ a·b by auto
qed

```

If a square is nonzero, then the element is nonzero.

```

lemma (in ring0) Ring_ZF_1_L13:
  assumes a∈R and a2 ≠ 0
  shows a≠0
  using assms Ring_ZF_1_L2 Ring_ZF_1_L6 by auto

```

Square of an element and its opposite are the same.

```

lemma (in ring0) Ring_ZF_1_L14:
  assumes a∈R shows (-a)2 = ((a)2)
  using assms Ring_ZF_1_L7A by simp

```

Adding zero to a set that is closed under addition results in a set that is also closed under addition. This is a property of groups.

```

lemma (in ring0) Ring_ZF_1_L15:
  assumes H ⊆ R and H {is closed under} A
  shows (H ∪ {0}) {is closed under} A
  using assms Ring_ZF_1_L1 group0.group0_2_L17 by simp

```

Adding zero to a set that is closed under multiplication results in a set that is also closed under multiplication.

```

lemma (in ring0) Ring_ZF_1_L16:
  assumes A1: H ⊆ R and A2: H {is closed under} M
  shows (H ∪ {0}) {is closed under} M
  using assms Ring_ZF_1_L2 Ring_ZF_1_L6 IsOpClosed_def
  by auto

```

The ring is trivial iff  $0 = 1$ .

```

lemma (in ring0) Ring_ZF_1_L17: shows R = {0} ⟷ 0=1
proof
  assume R = {0}
  then show 0=1 using Ring_ZF_1_L2
    by blast
next assume A1: 0 = 1
  then have R ⊆ {0}
    using Ring_ZF_1_L3 Ring_ZF_1_L6 by auto
  moreover have {0} ⊆ R using Ring_ZF_1_L2 by auto
  ultimately show R = {0} by auto
qed

```

The sets  $\{m \cdot x.x \in R\}$  and  $\{-m \cdot x.x \in R\}$  are the same.

**lemma** (in ring0) Ring\_ZF\_1\_L18: assumes A1:  $m \in R$

shows  $\{m \cdot x. x \in R\} = \{(-m) \cdot x. x \in R\}$

**proof**

```
{ fix a assume a ∈ {m·x. x∈R}
  then obtain x where x∈R and a = m·x
    by auto
  with A1 have (-x) ∈ R and a = (-m)·(-x)
    using Ring_ZF_1_L3 Ring_ZF_1_L7A by auto
  then have a ∈ {(-m)·x. x∈R}
    by auto
} then show {m·x. x∈R} ⊆ {(-m)·x. x∈R}
  by auto
```

**next**

```
{ fix a assume a ∈ {(-m)·x. x∈R}
  then obtain x where x∈R and a = (-m)·x
    by auto
  with A1 have (-x) ∈ R and a = m·(-x)
    using Ring_ZF_1_L3 Ring_ZF_1_L7 by auto
  then have a ∈ {m·x. x∈R} by auto
} then show {(-m)·x. x∈R} ⊆ {m·x. x∈R}
  by auto
```

**qed**

## 29.2 Rearrangement lemmas

It happens quite often that we want to show a fact like  $(a + b)c + d = (ac + d - e) + (bc + e)$  in rings. This is trivial in romantic math and probably there is a way to make it trivial in formalized math. However, I don't know any other way than to tediously prove each such rearrangement when it is needed. This section collects facts of this type.

Rearrangements with two elements of a ring.

**lemma** (in ring0) Ring\_ZF\_2\_L1: assumes  $a \in R$   $b \in R$

shows  $a + b \cdot a = (b + 1) \cdot a$

using assms Ring\_ZF\_1\_L2 ring\_oper\_distr Ring\_ZF\_1\_L3 Ring\_ZF\_1\_L4

by simp

Rearrangements with two elements and cancelling.

**lemma** (in ring0) Ring\_ZF\_2\_L1A: assumes  $a \in R$   $b \in R$

shows

$a - b + b = a$

$a + b - a = b$

$(-a) + b + a = b$

$(-a) + (b + a) = b$

$a + (b - a) = b$

using assms Ring\_ZF\_1\_L1 group0.inv\_cancel\_two group0.group0\_4\_L6A

by auto

In commutative rings  $a - (b+1)c = (a-d-c) + (d-bc)$ . For unknown reasons we have to use the raw set notation in the proof, otherwise all methods fail.

```
lemma (in ring0) Ring_ZF_2_L2:
  assumes A1: a∈R b∈R c∈R d∈R
  shows a-(b+1)·c = (a-d-c)+(d-b·c)
proof -
  let B = b·c
  from ringAssum have A {is commutative on} R
    using IsAring_def by simp
  moreover from A1 have a∈R B ∈ R c∈R d∈R
    using Ring_ZF_1_L4 by auto
  ultimately have A⟨a, GroupInv(R,A)(A⟨B, c⟩)⟩ =
    A⟨A⟨a, GroupInv(R, A)(d)⟩, GroupInv(R, A)(c)⟩,
    A⟨d, GroupInv(R, A)(B)⟩⟩
    using Ring_ZF_1_L1 group0.group0_4_L8 by blast
  with A1 show thesis
    using Ring_ZF_1_L2 ring_oper_distr Ring_ZF_1_L3 by simp
qed
```

Rearrangement about adding linear functions.

```
lemma (in ring0) Ring_ZF_2_L3:
  assumes A1: a∈R b∈R c∈R d∈R x∈R
  shows (a·x + b) + (c·x + d) = (a+c)·x + (b+d)
proof -
  from A1 have
    group0(R,A)
    A {is commutative on} R
    a·x ∈ R b∈R c·x ∈ R d∈R
    using Ring_ZF_1_L1 Ring_ZF_1_L4 by auto
  then have A⟨A⟨a·x,b⟩,A⟨c·x,d⟩⟩ = A⟨A⟨a·x,c·x⟩,A⟨b,d⟩⟩
    by (rule group0.group0_4_L8)
  with A1 show
    (a·x + b) + (c·x + d) = (a+c)·x + (b+d)
    using ring_oper_distr by simp
qed
```

Rearrangement with three elements

```
lemma (in ring0) Ring_ZF_2_L4:
  assumes M {is commutative on} R
  and a∈R b∈R c∈R
  shows a·(b·c) = a·c·b
  using assms IsCommutative_def Ring_ZF_1_L11
  by simp
```

Some other rearrangements with three elements.

```
lemma (in ring0) ring_rearr_3_elemA:
  assumes A1: M {is commutative on} R and
  A2: a∈R b∈R c∈R
```

```

shows
a·(a·c) - b·(-b·c) = (a·a + b·b)·c
a·(-b·c) + b·(a·c) = 0
proof -
  from A2 have T:
    b·c ∈ R  a·a ∈ R  b·b ∈ R
    b·(b·c) ∈ R  a·(b·c) ∈ R
    using Ring_ZF_1_L4 by auto
  with A2 show
    a·(a·c) - b·(-b·c) = (a·a + b·b)·c
    using Ring_ZF_1_L7 Ring_ZF_1_L3 Ring_ZF_1_L11
    ring_oper_distr by simp
  from A2 T have
    a·(-b·c) + b·(a·c) = (-a·(b·c)) + b·a·c
    using Ring_ZF_1_L7 Ring_ZF_1_L11 by simp
  also from A1 A2 T have ... = 0
    using IsCommutative_def Ring_ZF_1_L11 Ring_ZF_1_L3
    by simp
  finally show a·(-b·c) + b·(a·c) = 0
    by simp
qed

```

Some rearrangements with four elements. Properties of abelian groups.

```

lemma (in ring0) Ring_ZF_2_L5:
  assumes a∈R  b∈R  c∈R  d∈R
  shows
    a - b - c - d = a - d - b - c
    a + b + c - d = a - d + b + c
    a + b - c - d = a - c + (b - d)
    a + b + c + d = a + c + (b + d)
  using assms Ring_ZF_1_L1 group0.rearr_ab_gr_4_elemB
  group0.rearr_ab_gr_4_elemA by auto

```

Two big rearrangements with six elements, useful for proving properties of complex addition and multiplication.

```

lemma (in ring0) Ring_ZF_2_L6:
  assumes A1: a∈R  b∈R  c∈R  d∈R  e∈R  f∈R
  shows
    a·(c·e - d·f) - b·(c·f + d·e) =
      (a·c - b·d)·e - (a·d + b·c)·f
    a·(c·f + d·e) + b·(c·e - d·f) =
      (a·c - b·d)·f + (a·d + b·c)·e
    a·(c+e) - b·(d+f) = a·c - b·d + (a·e - b·f)
    a·(d+f) + b·(c+e) = a·d + b·c + (a·f + b·e)
  proof -
    from A1 have T:
      c·e ∈ R  d·f ∈ R  c·f ∈ R  d·e ∈ R
      a·c ∈ R  b·d ∈ R  a·d ∈ R  b·c ∈ R
      b·f ∈ R  a·e ∈ R  b·e ∈ R  a·f ∈ R

```

```

a·c·e ∈ R  a·d·f ∈ R
b·c·f ∈ R  b·d·e ∈ R
b·c·e ∈ R  b·d·f ∈ R
a·c·f ∈ R  a·d·e ∈ R
a·c·e - a·d·f ∈ R
a·c·e - b·d·e ∈ R
a·c·f + a·d·e ∈ R
a·c·f - b·d·f ∈ R
a·c + a·e ∈ R
a·d + a·f ∈ R
using Ring_ZF_1_L4 by auto
with A1 show a·(c·e - d·f) - b·(c·f + d·e) =
  (a·c - b·d)·e - (a·d + b·c)·f
  using Ring_ZF_1_L8 ring_oper_distr Ring_ZF_1_L11
    Ring_ZF_1_L10 Ring_ZF_2_L5 by simp
from A1 T show
  a·(c·f + d·e) + b·(c·e - d·f) =
  (a·c - b·d)·f + (a·d + b·c)·e
  using Ring_ZF_1_L8 ring_oper_distr Ring_ZF_1_L11
    Ring_ZF_1_L10A Ring_ZF_2_L5 Ring_ZF_1_L10
  by simp
from A1 T show
  a·(c+e) - b·(d+f) = a·c - b·d + (a·e - b·f)
  a·(d+f) + b·(c+e) = a·d + b·c + (a·f + b·e)
  using ring_oper_distr Ring_ZF_1_L10 Ring_ZF_2_L5
  by auto
qed
end

```

## 30 Ring\_ZF\_1.thy

**theory** Ring\_ZF\_1 **imports** Ring\_ZF Group\_ZF\_3

**begin**

This theory is devoted to the part of ring theory specific the construction of real numbers in the `Real_ZF_x` series of theories. The goal is to show that classes of almost homomorphisms form a ring.

### 30.1 The ring of classes of almost homomorphisms

Almost homomorphisms do not form a ring as the regular homomorphisms do because the lifted group operation is not distributive with respect to composition – we have  $s \circ (r \cdot q) \neq s \circ r \cdot s \circ q$  in general. However, we do have  $s \circ (r \cdot q) \approx s \circ r \cdot s \circ q$  in the sense of the equivalence relation defined by the group of finite range functions (that is a normal subgroup of almost homomorphisms, if the group is abelian). This allows to define a natural ring structure on the classes of almost homomorphisms.

The next lemma provides a formula useful for proving that two sides of the distributive law equation for almost homomorphisms are almost equal.

**lemma** (in group1) Ring\_ZF\_1\_1\_L1:  
**assumes** A1:  $s \in \text{AH}$   $r \in \text{AH}$   $q \in \text{AH}$  **and** A2:  $n \in G$   
**shows**  
 $((s \circ (r \cdot q))(n)) \cdot (((s \circ r) \cdot (s \circ q))(n))^{-1} = \delta(s, \langle r(n), q(n) \rangle)$   
 $((r \cdot q) \circ s)(n) = ((r \circ s) \cdot (q \circ s))(n)$   
**proof** -  
**from** groupAssum isAbelian A1 **have** T1:  
 $r \cdot q \in \text{AH}$   $s \circ r \in \text{AH}$   $s \circ q \in \text{AH}$   $(s \circ r) \cdot (s \circ q) \in \text{AH}$   
 $r \circ s \in \text{AH}$   $q \circ s \in \text{AH}$   $(r \circ s) \cdot (q \circ s) \in \text{AH}$   
**using** Group\_ZF\_3\_2\_L15 Group\_ZF\_3\_4\_T1 **by** auto  
**from** A1 A2 **have** T2:  $r(n) \in G$   $q(n) \in G$   $s(n) \in G$   
 $s(r(n)) \in G$   $s(q(n)) \in G$   $\delta(s, \langle r(n), q(n) \rangle) \in G$   
 $s(r(n)) \cdot s(q(n)) \in G$   $r(s(n)) \in G$   $q(s(n)) \in G$   
 $r(s(n)) \cdot q(s(n)) \in G$   
**using** AlmostHoms\_def apply\_funtype Group\_ZF\_3\_2\_L4B  
group0\_2\_L1 monoid0.group0\_1\_L1 **by** auto  
**with** T1 A1 A2 isAbelian **show**  
 $((s \circ (r \cdot q))(n)) \cdot (((s \circ r) \cdot (s \circ q))(n))^{-1} = \delta(s, \langle r(n), q(n) \rangle)$   
 $((r \cdot q) \circ s)(n) = ((r \circ s) \cdot (q \circ s))(n)$   
**using** Group\_ZF\_3\_2\_L12 Group\_ZF\_3\_4\_L2 Group\_ZF\_3\_4\_L1 group0\_4\_L6A  
**by** auto  
**qed**

The sides of the distributive law equations for almost homomorphisms are almost equal.

**lemma** (in group1) Ring\_ZF\_1\_1\_L2:



```

assumes A1: s∈AH r∈AH q∈AH
shows
so(r·q) ≈ (sor)·(soq)
(r·q)os = (ros)·(qos)
proof -
from A1 have ∀n∈G. ⟨ r(n),q(n)⟩ ∈ G×G
  using AlmostHoms_def apply_funtype by auto
moreover from A1 have {δ(s,x). x ∈ G×G} ∈ Fin(G)
  using AlmostHoms_def by simp
ultimately have {δ(s,⟨ r(n),q(n)⟩). n∈G} ∈ Fin(G)
  by (rule Finite1_L6B)
with A1 have
  {((so(r·q))(n))·(((sor)·(soq))(n))-1. n ∈ G} ∈ Fin(G)
  using Ring_ZF_1_1_L1 by simp
moreover from groupAssum isAbelian A1 A1 have
  so(r·q) ∈ AH (sor)·(soq) ∈ AH
  using Group_ZF_3_2_L15 Group_ZF_3_4_T1 by auto
ultimately show so(r·q) ≈ (sor)·(soq)
  using Group_ZF_3_4_L12 by simp
from groupAssum isAbelian A1 have
  (r·q)os : G→G (ros)·(qos) : G→G
  using Group_ZF_3_2_L15 Group_ZF_3_4_T1 AlmostHoms_def
  by auto
moreover from A1 have
  ∀n∈G. ((r·q)os)(n) = ((ros)·(qos))(n)
  using Ring_ZF_1_1_L1 by simp
ultimately show (r·q)os = (ros)·(qos)
  using fun_extension_iff by simp
qed

```

The essential condition to show the distributivity for the operations defined on classes of almost homomorphisms.

```

lemma (in group1) Ring_ZF_1_1_L3:
  assumes A1: R = QuotientGroupRel(AH,Op1,FR)
  and A2: a ∈ AH//R b ∈ AH//R c ∈ AH//R
  and A3: A = ProjFun2(AH,R,Op1) M = ProjFun2(AH,R,Op2)
  shows M⟨a,A⟨ b,c⟩⟩ = A⟨M⟨ a,b⟩,M⟨ a,c⟩⟩ ∧
  M⟨A⟨ b,c⟩,a⟩ = A⟨M⟨ b,a⟩,M⟨ c,a⟩⟩
proof
from A2 obtain s q r where D1: s∈AH r∈AH q∈AH
  a = R{s} b = R{q} c = R{r}
  using quotient_def by auto
from A1 have T1:equiv(AH,R)
  using Group_ZF_3_3_L3 by simp
with A1 A3 D1 groupAssum isAbelian have
  M⟨ a,A⟨ b,c⟩⟩ = R{so(q·r)}
  using Group_ZF_3_3_L4 EquivClass_1_L10
  Group_ZF_3_2_L15 Group_ZF_3_4_L13A by simp
also have R{so(q·r)} = R{(soq)·(sor)}

```

```

proof -
  from T1 D1 have equiv(AH,R) so(q.r)≈(soq).(sor)
    using Ring_ZF_1_1_L2 by auto
  with A1 show thesis using equiv_class_eq by simp
qed
also from A1 T1 D1 A3 have
  R{(soq).(sor)} = A⟨M⟨ a,b⟩,M⟨ a,c⟩⟩
    using Group_ZF_3_3_L4 Group_ZF_3_4_T1 EquivClass_1_L10
    Group_ZF_3_3_L3 Group_ZF_3_4_L13A EquivClass_1_L10 Group_ZF_3_4_T1
    by simp
finally show M⟨a,A⟨ b,c⟩⟩ = A⟨M⟨ a,b⟩,M⟨ a,c⟩⟩ by simp
from A1 A3 T1 D1 groupAssum isAbelian show
  M⟨A⟨ b,c⟩,a⟩ = A⟨M⟨ b,a⟩,M⟨ c,a⟩⟩
    using Group_ZF_3_3_L4 EquivClass_1_L10 Group_ZF_3_4_L13A
    Group_ZF_3_2_L15 Ring_ZF_1_1_L2 Group_ZF_3_4_T1 by simp
qed

```

The projection of the first group operation on almost homomorphisms is distributive with respect to the second group operation.

```

lemma (in group1) Ring_ZF_1_1_L4:
  assumes A1: R = QuotientGroupRel(AH,Op1,FR)
  and A2: A = ProjFun2(AH,R,Op1) M = ProjFun2(AH,R,Op2)
  shows IsDistributive(AH//R,A,M)
proof -
  from A1 A2 have  $\forall a \in (AH//R). \forall b \in (AH//R). \forall c \in (AH//R).$ 
  M⟨a,A⟨ b,c⟩⟩ = A⟨M⟨ a,b⟩, M⟨ a,c⟩⟩  $\wedge$ 
  M⟨A⟨ b,c⟩, a⟩ = A⟨M⟨ b,a⟩,M⟨ c,a⟩⟩
    using Ring_ZF_1_1_L3 by simp
  then show thesis using IsDistributive_def by simp
qed

```

The classes of almost homomorphisms form a ring.

```

theorem (in group1) Ring_ZF_1_1_T1:
  assumes R = QuotientGroupRel(AH,Op1,FR)
  and A = ProjFun2(AH,R,Op1) M = ProjFun2(AH,R,Op2)
  shows IsAring(AH//R,A,M)
  using assms QuotientGroupOp_def Group_ZF_3_3_T1 Group_ZF_3_4_T2
  Ring_ZF_1_1_L4 IsAring_def by simp

```

**end**

## 31 OrderedRing\_ZF.thy

**theory** OrderedRing\_ZF **imports** Ring\_ZF OrderedGroup\_ZF\_1

**begin**

In this theory file we consider ordered rings.

### 31.1 Definition and notation

This section defines ordered rings and sets up appropriate notation.

We define ordered ring as a commutative ring with linear order that is preserved by translations and such that the set of nonnegative elements is closed under multiplication. Note that this definition does not guarantee that there are no zero divisors in the ring.

**definition**

```
IsAnOrdRing(R,A,M,r)  $\equiv$   
( IsARing(R,A,M)  $\wedge$  (M {is commutative on} R)  $\wedge$   
r $\subseteq$ R $\times$ R  $\wedge$  IsLinOrder(R,r)  $\wedge$   
( $\forall$  a b.  $\forall$  c $\in$ R.  $\langle$  a,b $\rangle \in$  r  $\longrightarrow$   $\langle$  A $\langle$  a,c $\rangle$ ,A $\langle$  b,c $\rangle$  $\rangle \in$  r)  $\wedge$   
(Nonnegative(R,A,r) {is closed under} M))
```

The next context (locale) defines notation used for ordered rings. We do that by extending the notation defined in the `ring0` locale and adding some assumptions to make sure we are talking about ordered rings in this context.

**locale** ring1 = ring0 +

```
assumes mult_commut: M {is commutative on} R
```

```
fixes r
```

```
assumes ordincl: r  $\subseteq$  R $\times$ R
```

```
assumes linord: IsLinOrder(R,r)
```

```
fixes lesseq (infix  $\leq$  68)
```

```
defines lesseq_def [simp]: a  $\leq$  b  $\equiv$   $\langle$  a,b $\rangle \in$  r
```

```
fixes sless (infix  $<$  68)
```

```
defines sless_def [simp]: a  $<$  b  $\equiv$  a $\leq$ b  $\wedge$  a $\neq$ b
```

```
assumes ordgroup:  $\forall$  a b.  $\forall$  c $\in$ R. a $\leq$ b  $\longrightarrow$  a+c  $\leq$  b+c
```

```
assumes pos_mult_closed: Nonnegative(R,A,r) {is closed under} M
```

```
fixes abs (| _ |)
```

```
defines abs_def [simp]: |a|  $\equiv$  AbsoluteValue(R,A,r)(a)
```

```

fixes positiveset (R+)
defines positiveset_def [simp]: R+ ≡ PositiveSet(R,A,r)

```

The next lemma assures us that we are talking about ordered rings in the ring1 context.

```

lemma (in ring1) OrdRing_ZF_1_L1: shows IsAnOrdRing(R,A,M,r)
  using ring0_def ringAssum mult_commut ordincl linord ordgroup
  pos_mult_closed IsAnOrdRing_def by simp

```

We can use theorems proven in the ring1 context whenever we talk about an ordered ring.

```

lemma OrdRing_ZF_1_L2: assumes IsAnOrdRing(R,A,M,r)
  shows ring1(R,A,M,r)
  using assms IsAnOrdRing_def ring1_axioms.intro ring0_def ring1_def
  by simp

```

In the ring1 context  $a \leq b$  implies that  $a, b$  are elements of the ring.

```

lemma (in ring1) OrdRing_ZF_1_L3: assumes a ≤ b
  shows a ∈ R  b ∈ R
  using assms ordincl by auto

```

Ordered ring is an ordered group, hence we can use theorems proven in the group3 context.

```

lemma (in ring1) OrdRing_ZF_1_L4: shows
  IsAnOrdGroup(R,A,r)
  r {is total on} R
  A {is commutative on} R
  group3(R,A,r)
proof -
  { fix a b g assume A1: g ∈ R and A2: a ≤ b
    with ordgroup have a+g ≤ b+g
      by simp
    moreover from ringAssum A1 A2 have
      a+g = g+a  b+g = g+b
      using OrdRing_ZF_1_L3 IsAring_def IsCommutative_def by auto
    ultimately have
      a+g ≤ b+g  g+a ≤ g+b
      by auto
  } hence
    ∀ g ∈ R. ∀ a b. a ≤ b ⟶ a+g ≤ b+g ∧ g+a ≤ g+b
    by simp
with ringAssum ordincl linord show
  IsAnOrdGroup(R,A,r)
  group3(R,A,r)
  r {is total on} R
  A {is commutative on} R
  using IsAring_def Order_ZF_1_L2 IsAnOrdGroup_def group3_def IsLinOrder_def

```

by auto  
qed

The order relation in rings is transitive.

```
lemma (in ring1) ring_ord_transitive: assumes A1:  $a \leq b$   $b \leq c$ 
  shows  $a \leq c$ 
proof -
  from A1 have
    group3(R,A,r)  $\langle a,b \rangle \in r$   $\langle b,c \rangle \in r$ 
    using OrdRing_ZF_1_L4 by auto
  then have  $\langle a,c \rangle \in r$  by (rule group3.Group_order_transitive)
  then show  $a \leq c$  by simp
qed
```

Transitivity for the strict order: if  $a < b$  and  $b \leq c$ , then  $a < c$ . Property of ordered groups.

```
lemma (in ring1) ring_strict_ord_trans:
  assumes A1:  $a < b$  and A2:  $b \leq c$ 
  shows  $a < c$ 
proof -
  from A1 A2 have
    group3(R,A,r)
     $\langle a,b \rangle \in r \wedge a \neq b$   $\langle b,c \rangle \in r$ 
    using OrdRing_ZF_1_L4 by auto
  then have  $\langle a,c \rangle \in r \wedge a \neq c$  by (rule group3.OrderedGroup_ZF_1_L4A)
  then show  $a < c$  by simp
qed
```

Another version of transitivity for the strict order: if  $a \leq b$  and  $b < c$ , then  $a < c$ . Property of ordered groups.

```
lemma (in ring1) ring_strict_ord_transit:
  assumes A1:  $a \leq b$  and A2:  $b < c$ 
  shows  $a < c$ 
proof -
  from A1 A2 have
    group3(R,A,r)
     $\langle a,b \rangle \in r$   $\langle b,c \rangle \in r \wedge b \neq c$ 
    using OrdRing_ZF_1_L4 by auto
  then have  $\langle a,c \rangle \in r \wedge a \neq c$  by (rule group3.group_strict_ord_transit)
  then show  $a < c$  by simp
qed
```

The next lemma shows what happens when one element of an ordered ring is not greater or equal than another.

```
lemma (in ring1) OrdRing_ZF_1_L4A: assumes A1:  $a \in R$   $b \in R$ 
  and A2:  $\neg(a \leq b)$ 
  shows  $b \leq a$   $(-a) \leq (-b)$   $a \neq b$ 
proof -
```

```

from A1 A2 have I:
  group3(R,A,r)
  r {is total on} R
  a ∈ R b ∈ R ⟨a, b⟩ ∉ r
  using OrdRing_ZF_1_L4 by auto
then have ⟨b,a⟩ ∈ r by (rule group3.OrderedGroup_ZF_1_L8)
then show b ≤ a by simp
from I have ⟨GroupInv(R,A)(a),GroupInv(R,A)(b)⟩ ∈ r
  by (rule group3.OrderedGroup_ZF_1_L8)
then show (-a) ≤ (-b) by simp
from I show a≠b by (rule group3.OrderedGroup_ZF_1_L8)
qed

```

A special case of OrdRing\_ZF\_1\_L4A when one of the constants is 0. This is useful for many proofs by cases.

```

corollary (in ring1) ord_ring_split2: assumes A1: a∈R
  shows a≤0 ∨ (0≤a ∧ a≠0)
proof -
  { from A1 have I: a∈R 0∈R
    using Ring_ZF_1_L2 by auto
    moreover assume A2: ¬(a≤0)
    ultimately have 0≤a by (rule OrdRing_ZF_1_L4A)
    moreover from I A2 have a≠0 by (rule OrdRing_ZF_1_L4A)
    ultimately have 0≤a ∧ a≠0 by simp}
  then show thesis by auto
qed

```

Taking minus on both sides reverses an inequality.

```

lemma (in ring1) OrdRing_ZF_1_L4B: assumes a≤b
  shows (-b) ≤ (-a)
  using assms OrdRing_ZF_1_L4 group3.OrderedGroup_ZF_1_L5
  by simp

```

The next lemma just expands the condition that requires the set of non-negative elements to be closed with respect to multiplication. These are properties of totally ordered groups.

```

lemma (in ring1) OrdRing_ZF_1_L5:
  assumes 0≤a 0≤b
  shows 0 ≤ a·b
  using pos_mult_closed assms OrdRing_ZF_1_L4 group3.OrderedGroup_ZF_1_L2
  IsOpClosed_def by simp

```

Double nonnegative is nonnegative.

```

lemma (in ring1) OrdRing_ZF_1_L5A: assumes A1: 0≤a
  shows 0≤2·a
  using assms OrdRing_ZF_1_L4 group3.OrderedGroup_ZF_1_L5G
  OrdRing_ZF_1_L3 Ring_ZF_1_L3 by simp

```

A sufficient (somewhat redundant) condition for a structure to be an ordered ring. It says that a commutative ring that is a totally ordered group with respect to the additive operation such that set of nonnegative elements is closed under multiplication, is an ordered ring.

```
lemma OrdRing_ZF_1_L6:
  assumes
    IsAring(R,A,M)
    M {is commutative on} R
    Nonnegative(R,A,r) {is closed under} M
    IsAnOrdGroup(R,A,r)
    r {is total on} R
  shows IsAnOrdRing(R,A,M,r)
  using assms IsAnOrdGroup_def Order_ZF_1_L3 IsAnOrdRing_def
  by simp
```

$a \leq b$  iff  $a - b \leq 0$ . This is a fact from `OrderedGroup.thy`, where it is stated in multiplicative notation.

```
lemma (in ring1) OrdRing_ZF_1_L7:
  assumes a∈R b∈R
  shows a≤b ⟷ a-b ≤ 0
  using assms OrdRing_ZF_1_L4 group3.OrderedGroup_ZF_1_L9
  by simp
```

Negative times positive is negative.

```
lemma (in ring1) OrdRing_ZF_1_L8:
  assumes A1: a≤0 and A2: 0≤b
  shows a·b ≤ 0
proof -
  from A1 A2 have T1: a∈R b∈R a·b ∈ R
    using OrdRing_ZF_1_L3 Ring_ZF_1_L4 by auto
  from A1 A2 have 0≤(-a)·b
    using OrdRing_ZF_1_L4 group3.OrderedGroup_ZF_1_L5A OrdRing_ZF_1_L5
    by simp
  with T1 show a·b ≤ 0
    using Ring_ZF_1_L7 OrdRing_ZF_1_L4 group3.OrderedGroup_ZF_1_L5AA
    by simp
qed
```

We can multiply both sides of an inequality by a nonnegative ring element. This property is sometimes (not here) used to define ordered rings.

```
lemma (in ring1) OrdRing_ZF_1_L9:
  assumes A1: a≤b and A2: 0≤c
  shows
    a·c ≤ b·c
    c·a ≤ c·b
proof -
  from A1 A2 have T1:
    a∈R b∈R c∈R a·c ∈ R b·c ∈ R
```

```

    using OrdRing_ZF_1_L3 Ring_ZF_1_L4 by auto
  with A1 A2 have  $(a-b) \cdot c \leq 0$ 
    using OrdRing_ZF_1_L7 OrdRing_ZF_1_L8 by simp
  with T1 show  $a \cdot c \leq b \cdot c$ 
    using Ring_ZF_1_L8 OrdRing_ZF_1_L7 by simp
  with mult_commut T1 show  $c \cdot a \leq c \cdot b$ 
    using IsCommutative_def by simp
qed

```

A special case of OrdRing\_ZF\_1\_L9: we can multiply an inequality by a positive ring element.

```

lemma (in ring1) OrdRing_ZF_1_L9A:
  assumes A1:  $a \leq b$  and A2:  $c \in \mathbb{R}_+$ 
  shows
     $a \cdot c \leq b \cdot c$ 
     $c \cdot a \leq c \cdot b$ 
proof -
  from A2 have  $0 \leq c$  using PositiveSet_def
  by simp
  with A1 show  $a \cdot c \leq b \cdot c$   $c \cdot a \leq c \cdot b$ 
    using OrdRing_ZF_1_L9 by auto
qed

```

A square is nonnegative.

```

lemma (in ring1) OrdRing_ZF_1_L10:
  assumes A1:  $a \in \mathbb{R}$  shows  $0 \leq (a^2)$ 
proof -
  { assume  $0 \leq a$ 
    then have  $0 \leq (a^2)$  using OrdRing_ZF_1_L5 by simp }
  moreover
  { assume  $\neg(0 \leq a)$ 
    with A1 have  $0 \leq ((-a)^2)$ 
      using OrdRing_ZF_1_L4 group3.OrderedGroup_ZF_1_L8A
      OrdRing_ZF_1_L5 by simp
    with A1 have  $0 \leq (a^2)$  using Ring_ZF_1_L14 by simp }
  ultimately show thesis by blast
qed

```

1 is nonnegative.

```

corollary (in ring1) ordring_one_is_nonneg: shows  $0 \leq 1$ 
proof -
  have  $0 \leq (1^2)$  using Ring_ZF_1_L2 OrdRing_ZF_1_L10
  by simp
  then show  $0 \leq 1$  using Ring_ZF_1_L2 Ring_ZF_1_L3
  by simp
qed

```

In nontrivial rings one is positive.

```

lemma (in ring1) ordring_one_is_pos: assumes  $0 \neq 1$ 

```



```

shows  $1 \in R_+$ 
using assms Ring_ZF_1_L2 ordring_one_is_nonneg PositiveSet_def
by auto

```

Nonnegative is not negative. Property of ordered groups.

```

lemma (in ring1) OrdRing_ZF_1_L11: assumes  $0 \leq a$ 
  shows  $\neg(a \leq 0 \wedge a \neq 0)$ 
  using assms OrdRing_ZF_1_L4 group3.OrderedGroup_ZF_1_L5AB
  by simp

```

A negative element cannot be a square.

```

lemma (in ring1) OrdRing_ZF_1_L12:
  assumes A1:  $a \leq 0 \wedge a \neq 0$ 
  shows  $\neg(\exists b \in R. a = (b^2))$ 
proof -
  { assume  $\exists b \in R. a = (b^2)$ 
    with A1 have False using OrdRing_ZF_1_L10 OrdRing_ZF_1_L11
    by auto
  } then show thesis by auto
qed

```

If  $a \leq b$ , then  $0 \leq b - a$ .

```

lemma (in ring1) OrdRing_ZF_1_L13: assumes  $a \leq b$ 
  shows  $0 \leq b - a$ 
  using assms OrdRing_ZF_1_L4 group3.OrderedGroup_ZF_1_L9D
  by simp

```

If  $a < b$ , then  $0 < b - a$ .

```

lemma (in ring1) OrdRing_ZF_1_L14: assumes  $a \leq b \wedge a \neq b$ 
  shows
     $0 \leq b - a \wedge 0 \neq b - a$ 
     $b - a \in R_+$ 
  using assms OrdRing_ZF_1_L4 group3.OrderedGroup_ZF_1_L9E
  by auto

```

If the difference is nonnegative, then  $a \leq b$ .

```

lemma (in ring1) OrdRing_ZF_1_L15:
  assumes  $a \in R \wedge b \in R \wedge 0 \leq b - a$ 
  shows  $a \leq b$ 
  using assms OrdRing_ZF_1_L4 group3.OrderedGroup_ZF_1_L9F
  by simp

```

A nonnegative number is does not decrease when multiplied by a number greater or equal 1.

```

lemma (in ring1) OrdRing_ZF_1_L16:
  assumes A1:  $0 \leq a$  and A2:  $1 \leq b$ 
  shows  $a \leq a \cdot b$ 
proof -

```

```

from A1 A2 have T: a∈R b∈R a·b ∈ R
  using OrdRing_ZF_1_L3 Ring_ZF_1_L4 by auto
from A1 A2 have 0 ≤ a·(b-1)
  using OrdRing_ZF_1_L13 OrdRing_ZF_1_L5 by simp
with T show a≤a·b
  using Ring_ZF_1_L8 Ring_ZF_1_L2 Ring_ZF_1_L3 OrdRing_ZF_1_L15
  by simp
qed

```

We can multiply the right hand side of an inequality between nonnegative ring elements by an element greater or equal 1.

```

lemma (in ring1) OrdRing_ZF_1_L17:
  assumes A1: 0≤a and A2: a≤b and A3: 1≤c
  shows a≤b·c
proof -
  from A1 A2 have 0≤b by (rule ring_ord_transitive)
  with A3 have b≤b·c using OrdRing_ZF_1_L16
    by simp
  with A2 show a≤b·c by (rule ring_ord_transitive)
qed

```

Strict order is preserved by translations.

```

lemma (in ring1) ring_strict_ord_trans_inv:
  assumes a<b and c∈R
  shows
    a+c < b+c
    c+a < c+b
  using assms OrdRing_ZF_1_L4 group3.group_strict_ord_transl_inv
  by auto

```

We can put an element on the other side of a strict inequality, changing its sign.

```

lemma (in ring1) OrdRing_ZF_1_L18:
  assumes a∈R b∈R and a-b < c
  shows a < c+b
  using assms OrdRing_ZF_1_L4 group3.OrderedGroup_ZF_1_L12B
  by simp

```

We can add the sides of two inequalities, the first of them strict, and we get a strict inequality. Property of ordered groups.

```

lemma (in ring1) OrdRing_ZF_1_L19:
  assumes a<b and c≤d
  shows a+c < b+d
  using assms OrdRing_ZF_1_L4 group3.OrderedGroup_ZF_1_L12C
  by simp

```

We can add the sides of two inequalities, the second of them strict and we get a strict inequality. Property of ordered groups.

```

lemma (in ring1) OrdRing_ZF_1_L20:
  assumes  $a \leq b$  and  $c < d$ 
  shows  $a + c < b + d$ 
  using assms OrdRing_ZF_1_L4 group3.OrderedGroup_ZF_1_L12D
  by simp

```

## 31.2 Absolute value for ordered rings

Absolute value is defined for ordered groups as a function that is the identity on the nonnegative set and the negative of the element (the inverse in the multiplicative notation) on the rest. In this section we consider properties of absolute value related to multiplication in ordered rings.

Absolute value of a product is the product of absolute values: the case when both elements of the ring are nonnegative.

```

lemma (in ring1) OrdRing_ZF_2_L1:
  assumes  $0 \leq a$   $0 \leq b$ 
  shows  $|a \cdot b| = |a| \cdot |b|$ 
  using assms OrdRing_ZF_1_L5 OrdRing_ZF_1_L4
  group3.OrderedGroup_ZF_1_L2 group3.OrderedGroup_ZF_3_L2
  by simp

```

The absolute value of an element and its negative are the same.

```

lemma (in ring1) OrdRing_ZF_2_L2: assumes  $a \in R$ 
  shows  $|-a| = |a|$ 
  using assms OrdRing_ZF_1_L4 group3.OrderedGroup_ZF_3_L7A by simp

```

The next lemma states that  $|a \cdot (-b)| = |(-a) \cdot b| = |(-a) \cdot (-b)| = |a \cdot b|$ .

```

lemma (in ring1) OrdRing_ZF_2_L3:
  assumes  $a \in R$   $b \in R$ 
  shows
     $|(-a) \cdot b| = |a \cdot b|$ 
     $|a \cdot (-b)| = |a \cdot b|$ 
     $|(-a) \cdot (-b)| = |a \cdot b|$ 
  using assms Ring_ZF_1_L4 Ring_ZF_1_L7 Ring_ZF_1_L7A
  OrdRing_ZF_2_L2 by auto

```

This lemma allows to prove theorems for the case of positive and negative elements of the ring separately.

```

lemma (in ring1) OrdRing_ZF_2_L4: assumes  $a \in R$  and  $\neg(0 \leq a)$ 
  shows  $0 \leq (-a)$   $0 \neq a$ 
  using assms OrdRing_ZF_1_L4 group3.OrderedGroup_ZF_1_L8A
  by auto

```

Absolute value of a product is the product of absolute values.

```

lemma (in ring1) OrdRing_ZF_2_L5:
  assumes A1:  $a \in R$   $b \in R$ 

```

```

    shows  $|a \cdot b| = |a| \cdot |b|$ 
  proof -
    { assume A2:  $0 \leq a$  have  $|a \cdot b| = |a| \cdot |b|$ 
      proof -
        { assume  $0 \leq b$ 
          with A2 have  $|a \cdot b| = |a| \cdot |b|$ 
            using OrdRing_ZF_2_L1 by simp }
        moreover
        { assume  $\neg(0 \leq b)$ 
          with A1 A2 have  $|a \cdot (-b)| = |a| \cdot |-b|$ 
            using OrdRing_ZF_2_L4 OrdRing_ZF_2_L1 by simp
          with A1 have  $|a \cdot b| = |a| \cdot |b|$ 
            using OrdRing_ZF_2_L2 OrdRing_ZF_2_L3 by simp }
          ultimately show thesis by blast
        qed }
      moreover
      { assume  $\neg(0 \leq a)$ 
        with A1 have A3:  $0 \leq (-a)$ 
          using OrdRing_ZF_2_L4 by simp
        have  $|a \cdot b| = |-a| \cdot |b|$ 
          proof -
            { assume  $0 \leq b$ 
              with A3 have  $|(-a) \cdot b| = |-a| \cdot |b|$ 
                using OrdRing_ZF_2_L1 by simp
              with A1 have  $|a \cdot b| = |-a| \cdot |b|$ 
                using OrdRing_ZF_2_L2 OrdRing_ZF_2_L3 by simp }
              moreover
              { assume  $\neg(0 \leq b)$ 
                with A1 A3 have  $|(-a) \cdot (-b)| = |-a| \cdot |-b|$ 
                  using OrdRing_ZF_2_L4 OrdRing_ZF_2_L1 by simp
                with A1 have  $|a \cdot b| = |-a| \cdot |b|$ 
                  using OrdRing_ZF_2_L2 OrdRing_ZF_2_L3 by simp }
                  ultimately show thesis by blast
                qed }
            ultimately show thesis by blast
          qed
        }
      ultimately show thesis by blast
    qed
  qed

```

Triangle inequality. Property of linearly ordered abelian groups.

```

lemma (in ring1) ord_ring_triangle_ineq: assumes  $a \in \mathbb{R}$   $b \in \mathbb{R}$ 
  shows  $|a+b| \leq |a|+|b|$ 
  using assms OrdRing_ZF_1_L4 group3.OrdGroup_triangle_ineq
  by simp

```

If  $a \leq c$  and  $b \leq c$ , then  $a + b \leq 2 \cdot c$ .

```

lemma (in ring1) OrdRing_ZF_2_L6:
  assumes  $a \leq c$   $b \leq c$  shows  $a+b \leq 2 \cdot c$ 
  using assms OrdRing_ZF_1_L4 group3.OrderedGroup_ZF_1_L5B
  OrdRing_ZF_1_L3 Ring_ZF_1_L3 by simp

```

### 31.3 Positivity in ordered rings

This section is about properties of the set of positive elements  $R_+$ .

The set of positive elements is closed under ring addition. This is a property of ordered groups, we just reference a theorem from `OrderedGroup_ZF` theory in the proof.

```
lemma (in ring1) OrdRing_ZF_3_L1: shows  $R_+$  {is closed under} A
  using OrdRing_ZF_1_L4 group3.OrderedGroup_ZF_1_L13
  by simp
```

Every element of a ring can be either in the positive set, equal to zero or its opposite (the additive inverse) is in the positive set. This is a property of ordered groups, we just reference a theorem from `OrderedGroup_ZF` theory.

```
lemma (in ring1) OrdRing_ZF_3_L2: assumes  $a \in R$ 
  shows Exactly_1_of_3_holds ( $a=0$ ,  $a \in R_+$ ,  $(-a) \in R_+$ )
  using assms OrdRing_ZF_1_L4 group3.OrdGroup_decomp
  by simp
```

If a ring element  $a \neq 0$ , and it is not positive, then  $-a$  is positive.

```
lemma (in ring1) OrdRing_ZF_3_L2A: assumes  $a \in R$   $a \neq 0$   $a \notin R_+$ 
  shows  $(-a) \in R_+$ 
  using assms OrdRing_ZF_1_L4 group3.OrdGroup_cases
  by simp
```

$R_+$  is closed under multiplication iff the ring has no zero divisors.

```
lemma (in ring1) OrdRing_ZF_3_L3:
  shows  $(R_+ \text{ {is closed under} } M) \longleftrightarrow \text{HasNoZeroDivs}(R, A, M)$ 
proof
  assume A1: HasNoZeroDivs(R, A, M)
  { fix a b assume  $a \in R_+$   $b \in R_+$ 
    then have  $0 \leq a$   $a \neq 0$   $0 \leq b$   $b \neq 0$ 
      using PositiveSet_def by auto
    with A1 have  $a \cdot b \in R_+$ 
      using OrdRing_ZF_1_L5 Ring_ZF_1_L2 OrdRing_ZF_1_L3 Ring_ZF_1_L12
      OrdRing_ZF_1_L4 group3.OrderedGroup_ZF_1_L2A
      by simp
  } then show  $R_+ \text{ {is closed under} } M$  using IsOpClosed_def
  by simp
next assume A2:  $R_+ \text{ {is closed under} } M$ 
  { fix a b assume A3:  $a \in R$   $b \in R$  and  $a \neq 0$   $b \neq 0$ 
    with A2 have  $|a \cdot b| \in R_+$ 
      using OrdRing_ZF_1_L4 group3.OrderedGroup_ZF_3_L12 IsOpClosed_def
      OrdRing_ZF_2_L5 by simp
    with A3 have  $a \cdot b \neq 0$ 
      using PositiveSet_def Ring_ZF_1_L4
      OrdRing_ZF_1_L4 group3.OrderedGroup_ZF_3_L2A
      by auto
```

```

    } then show HasNoZeroDivs(R,A,M) using HasNoZeroDivs_def
    by auto
qed

```

Another (in addition to OrdRing\_ZF\_1\_L6 sufficient condition that defines order in an ordered ring starting from the positive set.

```

theorem (in ring0) ring_ord_by_positive_set:
  assumes
    A1: M {is commutative on} R and
    A2:  $P \subseteq R$   $P$  {is closed under} A  $0 \notin P$  and
    A3:  $\forall a \in R. a \neq 0 \longrightarrow (a \in P) \text{ Xor } ((-a) \in P)$  and
    A4: P {is closed under} M and
    A5: r = OrderFromPosSet(R,A,P)
  shows
    IsAnOrdGroup(R,A,r)
    IsAnOrdRing(R,A,M,r)
    r {is total on} R
    PositiveSet(R,A,r) = P
    Nonnegative(R,A,r) =  $P \cup \{0\}$ 
    HasNoZeroDivs(R,A,M)
proof -
  from A2 A3 A5 show
    I: IsAnOrdGroup(R,A,r) r {is total on} R and
    II: PositiveSet(R,A,r) = P and
    III: Nonnegative(R,A,r) =  $P \cup \{0\}$ 
  using Ring_ZF_1_L1 group0.Group_ord_by_positive_set
  by auto
  from A2 A4 III have Nonnegative(R,A,r) {is closed under} M
  using Ring_ZF_1_L16 by simp
  with ringAssum A1 I show IsAnOrdRing(R,A,M,r)
  using OrdRing_ZF_1_L6 by simp
  with A4 II show HasNoZeroDivs(R,A,M)
  using OrdRing_ZF_1_L2 ring1.OrdRing_ZF_3_L3
  by auto
qed

```

Nontrivial ordered rings are infinite. More precisely we assume that the neutral element of the additive operation is not equal to the multiplicative neutral element and show that the the set of positive elements of the ring is not a finite subset of the ring and the ring is not a finite subset of itself.

```

theorem (in ring1) ord_ring_infinite: assumes  $0 \neq 1$ 
  shows
     $R_+ \notin \text{Fin}(R)$ 
     $R \notin \text{Fin}(R)$ 
  using assms Ring_ZF_1_L17 OrdRing_ZF_1_L4 group3.Linord_group_infinite
  by auto

```

If every element of a nontrivial ordered ring can be dominated by an element from  $B$ , then we  $B$  is not bounded and not finite.

```

lemma (in ring1) OrdRing_ZF_3_L4:
  assumes  $0 \neq 1$  and  $\forall a \in R. \exists b \in B. a \leq b$ 
  shows
     $\neg \text{IsBoundedAbove}(B, r)$ 
     $B \notin \text{Fin}(R)$ 
  using assms Ring_ZF_1_L17 OrdRing_ZF_1_L4 group3.OrderedGroup_ZF_2_L2A
  by auto

```

If  $m$  is greater or equal the multiplicative unit, then the set  $\{m \cdot n : n \in R\}$  is infinite (unless the ring is trivial).

```

lemma (in ring1) OrdRing_ZF_3_L5: assumes A1:  $0 \neq 1$  and A2:  $1 \leq m$ 
  shows
     $\{m \cdot x. x \in R_+\} \notin \text{Fin}(R)$ 
     $\{m \cdot x. x \in R\} \notin \text{Fin}(R)$ 
     $\{(-m) \cdot x. x \in R\} \notin \text{Fin}(R)$ 
  proof -
    from A2 have T:  $m \in R$  using OrdRing_ZF_1_L3 by simp
    from A2 have  $0 \leq 1$   $1 \leq m$ 
      using ordring_one_is_nonneg by auto
    then have I:  $0 \leq m$  by (rule ring_ord_transitive)
    let B =  $\{m \cdot x. x \in R_+\}$ 
    { fix a assume A3:  $a \in R$ 
      then have  $a \leq 0 \vee (0 \leq a \wedge a \neq 0)$ 
        using ord_ring_split2 by simp
      moreover
      { assume A4:  $a \leq 0$ 
        from A1 have  $m \cdot 1 \in B$  using ordring_one_is_pos
      }
    } by auto
    with T have  $m \in B$  using Ring_ZF_1_L3 by simp
    moreover from A4 I have  $a \leq m$  by (rule ring_ord_transitive)
    ultimately have  $\exists b \in B. a \leq b$  by blast }
    moreover
    { assume A4:  $0 \leq a \wedge a \neq 0$ 
      with A3 have  $m \cdot a \in B$  using PositiveSet_def
    } by auto
    moreover
    from A2 A4 have  $1 \cdot a \leq m \cdot a$  using OrdRing_ZF_1_L9
  by simp
  with A3 have  $a \leq m \cdot a$  using Ring_ZF_1_L3
  by simp
  ultimately have  $\exists b \in B. a \leq b$  by auto }
  ultimately have  $\exists b \in B. a \leq b$  by auto
} then have  $\forall a \in R. \exists b \in B. a \leq b$ 
  by simp
with A1 show  $B \notin \text{Fin}(R)$  using OrdRing_ZF_3_L4
  by simp
moreover have  $B \subseteq \{m \cdot x. x \in R\}$ 
  using PositiveSet_def by auto
ultimately show  $\{m \cdot x. x \in R\} \notin \text{Fin}(R)$  using Fin_subset

```

```

    by auto
  with T show  $\{(-m) \cdot x. x \in R\} \notin \text{Fin}(R)$  using Ring_ZF_1_L18
  by simp
qed

```

If  $m$  is less or equal than the negative of multiplicative unit, then the set  $\{m \cdot n : n \in R\}$  is infinite (unless the ring is trivial).

```

lemma (in ring1) OrdRing_ZF_3_L6: assumes A1:  $0 \neq 1$  and A2:  $m \leq -1$ 
  shows  $\{m \cdot x. x \in R\} \notin \text{Fin}(R)$ 
proof -
  from A2 have  $(-(-1)) \leq -m$ 
  using OrdRing_ZF_1_L4B by simp
  with A1 have  $\{(-m) \cdot x. x \in R\} \notin \text{Fin}(R)$ 
  using Ring_ZF_1_L2 Ring_ZF_1_L3 OrdRing_ZF_3_L5
  by simp
  with A2 show  $\{m \cdot x. x \in R\} \notin \text{Fin}(R)$ 
  using OrdRing_ZF_1_L3 Ring_ZF_1_L18 by simp
qed

```

All elements greater or equal than an element of  $R_+$  belong to  $R_+$ . Property of ordered groups.

```

lemma (in ring1) OrdRing_ZF_3_L7: assumes A1:  $a \in R_+$  and A2:  $a \leq b$ 
  shows  $b \in R_+$ 
proof -
  from A1 A2 have
    group3(R,A,r)
     $a \in \text{PositiveSet}(R,A,r)$ 
     $\langle a, b \rangle \in r$ 
  using OrdRing_ZF_1_L4 by auto
  then have  $b \in \text{PositiveSet}(R,A,r)$ 
  by (rule group3.OrderedGroup_ZF_1_L19)
  then show  $b \in R_+$  by simp
qed

```

A special case of OrdRing\_ZF\_3\_L7: a ring element greater or equal than 1 is positive.

```

corollary (in ring1) OrdRing_ZF_3_L8: assumes A1:  $0 \neq 1$  and A2:  $1 \leq a$ 
  shows  $a \in R_+$ 
proof -
  from A1 A2 have  $1 \in R_+$   $1 \leq a$ 
  using ordring_one_is_pos by auto
  then show  $a \in R_+$  by (rule OrdRing_ZF_3_L7)
qed

```

Adding a positive element to  $a$  strictly increases  $a$ . Property of ordered groups.

```

lemma (in ring1) OrdRing_ZF_3_L9: assumes A1:  $a \in R$   $b \in R_+$ 
  shows  $a \leq a+b$   $a \neq a+b$ 

```



```

using assms OrdRing_ZF_1_L4 group3.OrderedGroup_ZF_1_L22
by auto

```

A special case of OrdRing\_ZF\_3\_L9: in nontrivial rings adding one to  $a$  increases  $a$ .

```

corollary (in ring1) OrdRing_ZF_3_L10: assumes A1:  $0 \neq 1$  and A2:  $a \in R$ 
  shows  $a \leq a+1$   $a \neq a+1$ 
  using assms ordning_one_is_pos OrdRing_ZF_3_L9
  by auto

```

If  $a$  is not greater than  $b$ , then it is strictly less than  $b + 1$ .

```

lemma (in ring1) OrdRing_ZF_3_L11: assumes A1:  $0 \neq 1$  and A2:  $a \leq b$ 
  shows  $a < b+1$ 
proof -
  from A1 A2 have I:  $b < b+1$ 
  using OrdRing_ZF_1_L3 OrdRing_ZF_3_L10 by auto
  with A2 show  $a < b+1$  by (rule ring_strict_ord_transit)
qed

```

For any ring element  $a$  the greater of  $a$  and 1 is a positive element that is greater or equal than  $m$ . If we add 1 to it we get a positive element that is strictly greater than  $m$ . This holds in nontrivial rings.

```

lemma (in ring1) OrdRing_ZF_3_L12: assumes A1:  $0 \neq 1$  and A2:  $a \in R$ 
  shows
     $a \leq \text{GreaterOf}(r, 1, a)$ 
     $\text{GreaterOf}(r, 1, a) \in R_+$ 
     $\text{GreaterOf}(r, 1, a) + 1 \in R_+$ 
     $a \leq \text{GreaterOf}(r, 1, a) + 1$   $a \neq \text{GreaterOf}(r, 1, a) + 1$ 
proof -
  from linord have r {is total on} R using IsLinOrder_def
  by simp
  moreover from A2 have  $1 \in R$   $a \in R$ 
  using Ring_ZF_1_L2 by auto
  ultimately have
     $1 \leq \text{GreaterOf}(r, 1, a)$  and
    I:  $a \leq \text{GreaterOf}(r, 1, a)$ 
  using Order_ZF_3_L2 by auto
  with A1 show
     $a \leq \text{GreaterOf}(r, 1, a)$  and
     $\text{GreaterOf}(r, 1, a) \in R_+$ 
  using OrdRing_ZF_3_L8 by auto
  with A1 show  $\text{GreaterOf}(r, 1, a) + 1 \in R_+$ 
  using ordning_one_is_pos OrdRing_ZF_3_L1 IsOpClosed_def
  by simp
  from A1 I show
     $a \leq \text{GreaterOf}(r, 1, a) + 1$   $a \neq \text{GreaterOf}(r, 1, a) + 1$ 
  using OrdRing_ZF_3_L11 by auto
qed

```

We can multiply strict inequality by a positive element.

```

lemma (in ring1) OrdRing_ZF_3_L13:
  assumes A1: HasNoZeroDivs(R,A,M) and
  A2:  $a < b$  and A3:  $c \in R_+$ 
  shows
   $a \cdot c < b \cdot c$ 
   $c \cdot a < c \cdot b$ 
proof -
  from A2 A3 have T:  $a \in R$   $b \in R$   $c \in R$   $c \neq 0$ 
  using OrdRing_ZF_1_L3 PositiveSet_def by auto
  from A2 A3 have  $a \cdot c \leq b \cdot c$  using OrdRing_ZF_1_L9A
  by simp
  moreover from A1 A2 T have  $a \cdot c \neq b \cdot c$ 
  using Ring_ZF_1_L12A by auto
  ultimately show  $a \cdot c < b \cdot c$  by simp
  moreover from mult_commut T have  $a \cdot c = c \cdot a$  and  $b \cdot c = c \cdot b$ 
  using IsCommutative_def by auto
  ultimately show  $c \cdot a < c \cdot b$  by simp
qed

```

A sufficient condition for an element to be in the set of positive ring elements.

```

lemma (in ring1) OrdRing_ZF_3_L14: assumes  $0 \leq a$  and  $a \neq 0$ 
  shows  $a \in R_+$ 
  using assms OrdRing_ZF_1_L3 PositiveSet_def
  by auto

```

If a ring has no zero divisors, the square of a nonzero element is positive.

```

lemma (in ring1) OrdRing_ZF_3_L15:
  assumes HasNoZeroDivs(R,A,M) and  $a \in R$   $a \neq 0$ 
  shows  $0 \leq a^2$   $a^2 \neq 0$   $a^2 \in R_+$ 
  using assms OrdRing_ZF_1_L10 Ring_ZF_1_L12 OrdRing_ZF_3_L14
  by auto

```

In rings with no zero divisors we can (strictly) increase a positive element by multiplying it by an element that is greater than 1.

```

lemma (in ring1) OrdRing_ZF_3_L16:
  assumes HasNoZeroDivs(R,A,M) and  $a \in R_+$  and  $1 \leq b$   $1 \neq b$ 
  shows  $a \leq a \cdot b$   $a \neq a \cdot b$ 
  using assms PositiveSet_def OrdRing_ZF_1_L16 OrdRing_ZF_1_L3
  Ring_ZF_1_L12C by auto

```

If the right hand side of an inequality is positive we can multiply it by a number that is greater than one.

```

lemma (in ring1) OrdRing_ZF_3_L17:
  assumes A1: HasNoZeroDivs(R,A,M) and A2:  $b \in R_+$  and
  A3:  $a \leq b$  and A4:  $1 < c$ 
  shows  $a < b \cdot c$ 
proof -

```

```

from A1 A2 A4 have b < b·c
  using OrdRing_ZF_3_L16 by auto
with A3 show a<b·c by (rule ring_strict_ord_transit)
qed

```

We can multiply a right hand side of an inequality between positive numbers by a number that is greater than one.

```

lemma (in ring1) OrdRing_ZF_3_L18:
  assumes A1: HasNoZeroDivs(R,A,M) and A2: a ∈ R+ and
  A3: a ≤ b and A4: 1 < c
  shows a < b·c
proof -
  from A2 A3 have b ∈ R+ using OrdRing_ZF_3_L7
  by blast
  with A1 A3 A4 show a < b·c
  using OrdRing_ZF_3_L17 by simp
qed

```

In ordered rings with no zero divisors if at least one of  $a, b$  is not zero, then  $0 < a^2 + b^2$ , in particular  $a^2 + b^2 \neq 0$ .

```

lemma (in ring1) OrdRing_ZF_3_L19:
  assumes A1: HasNoZeroDivs(R,A,M) and A2: a ∈ R  b ∈ R and
  A3: a ≠ 0 ∨ b ≠ 0
  shows 0 < a2 + b2
proof -
  { assume a ≠ 0
    with A1 A2 have 0 ≤ a2  a2 ≠ 0
      using OrdRing_ZF_3_L15 by auto
    then have 0 < a2 by auto
    moreover from A2 have 0 ≤ b2
      using OrdRing_ZF_1_L10 by simp
    ultimately have 0 + 0 < a2 + b2
      using OrdRing_ZF_1_L19 by simp
    then have 0 < a2 + b2
      using Ring_ZF_1_L2 Ring_ZF_1_L3 by simp }
  moreover
  { assume A4: a = 0
    then have a2 + b2 = 0 + b2
      using Ring_ZF_1_L2 Ring_ZF_1_L6 by simp
    also from A2 have ... = b2
      using Ring_ZF_1_L4 Ring_ZF_1_L3 by simp
    finally have a2 + b2 = b2 by simp
    moreover
    from A3 A4 have b ≠ 0 by simp
    with A1 A2 have 0 ≤ b2 and b2 ≠ 0
      using OrdRing_ZF_3_L15 by auto
    hence 0 < b2 by auto
    ultimately have 0 < a2 + b2 by simp }
  ultimately show 0 < a2 + b2

```

by auto  
qed

end

## 32 Field\_ZF.thy

**theory** Field\_ZF **imports** Ring\_ZF

**begin**

This theory covers basic facts about fields.

### 32.1 Definition and basic properties

In this section we define what is a field and list the basic properties of fields.

Field is a nontrivial commutative ring such that all non-zero elements have an inverse. We define the notion of being a field as a statement about three sets. The first set, denoted  $K$  is the carrier of the field. The second set, denoted  $A$  represents the additive operation on  $K$  (recall that in ZF set theory functions are sets). The third set  $M$  represents the multiplicative operation on  $K$ .

**definition**

```
IsAfield(K,A,M)  $\equiv$   
(IsAring(K,A,M)  $\wedge$  (M {is commutative on} K)  $\wedge$   
TheNeutralElement(K,A)  $\neq$  TheNeutralElement(K,M)  $\wedge$   
( $\forall a \in K. a \neq \text{TheNeutralElement}(K,A) \longrightarrow$   
( $\exists b \in K. M(a,b) = \text{TheNeutralElement}(K,M)$ )))
```

The `field0` context extends the `ring0` context adding field-related assumptions and notation related to the multiplicative inverse.

```
locale field0 = ring0 K A M for K A M +  
  assumes mult_commute: M {is commutative on} K  
  
  assumes not_triv: 0  $\neq$  1  
  
  assumes inv_exists:  $\forall a \in K. a \neq 0 \longrightarrow (\exists b \in K. a \cdot b = 1)$   
  
  fixes non_zero (K0)  
  defines non_zero_def[simp]: K0  $\equiv$  K - {0}  
  
  fixes inv ( $_^{-1}$  [96] 97)  
  defines inv_def[simp]:  $a^{-1} \equiv \text{GroupInv}(K_0, \text{restrict}(M, K_0 \times K_0))(a)$ 
```

The next lemma assures us that we are talking fields in the `field0` context.

```
lemma (in field0) Field_ZF_1_L1: shows IsAfield(K,A,M)  
  using ringAssum mult_commute not_triv inv_exists IsAfield_def  
  by simp
```

We can use theorems proven in the `field0` context whenever we talk about a field.

```
lemma field_field0: assumes IsAfield(K,A,M)
```

```

shows field0(K,A,M)
using assms IsAfield_def field0_axioms.intro ring0_def field0_def
by simp

```

Let's have an explicit statement that the multiplication in fields is commutative.

```

lemma (in field0) field_mult_comm: assumes a∈K b∈K
  shows a·b = b·a
  using mult_commute assms IsCommutative_def by simp

```

Fields do not have zero divisors.

```

lemma (in field0) field_has_no_zero_divs: shows HasNoZeroDivs(K,A,M)
proof -
  { fix a b assume A1: a∈K b∈K and A2: a·b = 0 and A3: b≠0
    from inv_exists A1 A3 obtain c where I: c∈K and II: b·c = 1
      by auto
    from A2 have a·b·c = 0·c by simp
    with A1 I have a·(b·c) = 0
      using Ring_ZF_1_L11 Ring_ZF_1_L6 by simp
    with A1 II have a=0 using Ring_ZF_1_L3 by simp }
  then have ∀a∈K.∀b∈K. a·b = 0 ⟶ a=0 ∨ b=0 by auto
  then show thesis using HasNoZeroDivs_def by auto
qed

```

$K_0$  (the set of nonzero field elements is closed with respect to multiplication.

```

lemma (in field0) Field_ZF_1_L2:
  shows  $K_0$  {is closed under} M
  using Ring_ZF_1_L4 field_has_no_zero_divs Ring_ZF_1_L12
  IsOpClosed_def by auto

```

Any nonzero element has a right inverse that is nonzero.

```

lemma (in field0) Field_ZF_1_L3: assumes A1: a∈ $K_0$ 
  shows ∃b∈ $K_0$ . a·b = 1
proof -
  from inv_exists A1 obtain b where b∈K and a·b = 1
    by auto
  with not_triv A1 show ∃b∈ $K_0$ . a·b = 1
    using Ring_ZF_1_L6 by auto
qed

```

If we remove zero, the field with multiplication becomes a group and we can use all theorems proven in `group0` context.

```

theorem (in field0) Field_ZF_1_L4: shows
  IsAgroup( $K_0$ , restrict(M,  $K_0 \times K_0$ ))
  group0( $K_0$ , restrict(M,  $K_0 \times K_0$ ))
  1 = TheNeutralElement( $K_0$ , restrict(M,  $K_0 \times K_0$ ))
proof-
  let f = restrict(M,  $K_0 \times K_0$ )

```

```

have
  M {is associative on} K
  K0 ⊆ K K0 {is closed under} M
  using Field_ZF_1_L1 IsAfield_def IsAring_def IsAgroup_def
  IsAmonoid_def Field_ZF_1_L2 by auto
then have f {is associative on} K0
  using func_ZF_4_L3 by simp
moreover
from not_triv have
  I: 1 ∈ K0 ∧ (∀ a ∈ K0. f⟨1, a⟩ = a ∧ f⟨a, 1⟩ = a)
  using Ring_ZF_1_L2 Ring_ZF_1_L3 by auto
then have ∃ n ∈ K0. ∀ a ∈ K0. f⟨n, a⟩ = a ∧ f⟨a, n⟩ = a
  by blast
ultimately have II: IsAmonoid(K0, f) using IsAmonoid_def
  by simp
then have monoid0(K0, f) using monoid0_def by simp
moreover note I
ultimately show 1 = TheNeutralElement(K0, f)
  by (rule monoid0.group0_1_L4)
then have ∀ a ∈ K0. ∃ b ∈ K0. f⟨a, b⟩ = TheNeutralElement(K0, f)
  using Field_ZF_1_L3 by auto
with II show IsAgroup(K0, f) by (rule definition_of_group)
then show group0(K0, f) using group0_def by simp
qed

```

The inverse of a nonzero field element is nonzero.

```

lemma (in field0) Field_ZF_1_L5: assumes A1: a ∈ K a ≠ 0
  shows a-1 ∈ K0 (a-1)2 ∈ K0 a-1 ∈ K a-1 ≠ 0
proof -
  from A1 have a ∈ K0 by simp
  then show a-1 ∈ K0 using Field_ZF_1_L4 group0.inverse_in_group
  by auto
  then show (a-1)2 ∈ K0 a-1 ∈ K a-1 ≠ 0
  using Field_ZF_1_L2 IsOpClosed_def by auto
qed

```

The inverse is really the inverse.

```

lemma (in field0) Field_ZF_1_L6: assumes A1: a ∈ K a ≠ 0
  shows a · a-1 = 1 a-1 · a = 1
proof -
  let f = restrict(M, K0 × K0)
  from A1 have
    group0(K0, f)
    a ∈ K0
    using Field_ZF_1_L4 by auto
  then have
    f⟨a, GroupInv(K0, f)(a)⟩ = TheNeutralElement(K0, f) ∧
    f⟨GroupInv(K0, f)(a), a⟩ = TheNeutralElement(K0, f)
    by (rule group0.group0_2_L6)

```

```

with A1 show  $a \cdot a^{-1} = 1$   $a^{-1} \cdot a = 1$ 
  using Field_ZF_1_L5 Field_ZF_1_L4 by auto
qed

```

A lemma with two field elements and cancelling.

```

lemma (in field0) Field_ZF_1_L7: assumes  $a \in K$   $b \in K$   $b \neq 0$ 
  shows
     $a \cdot b \cdot b^{-1} = a$ 
     $a \cdot b^{-1} \cdot b = a$ 
  using assms Field_ZF_1_L5 Ring_ZF_1_L11 Field_ZF_1_L6 Ring_ZF_1_L3
  by auto

```

## 32.2 Equations and identities

This section deals with more specialized identities that are true in fields.

$$a/(a^2) = a.$$

```

lemma (in field0) Field_ZF_2_L1: assumes A1:  $a \in K$   $a \neq 0$ 
  shows  $a \cdot (a^{-1})^2 = a^{-1}$ 
proof -
  have  $a \cdot (a^{-1})^2 = a \cdot (a^{-1} \cdot a^{-1})$  by simp
  also from A1 have ... =  $(a \cdot a^{-1}) \cdot a^{-1}$ 
    using Field_ZF_1_L5 Ring_ZF_1_L11
    by simp
  also from A1 have ... =  $a^{-1}$ 
    using Field_ZF_1_L6 Field_ZF_1_L5 Ring_ZF_1_L3
    by simp
  finally show  $a \cdot (a^{-1})^2 = a^{-1}$  by simp
qed

```

If we multiply two different numbers by a nonzero number, the results will be different.

```

lemma (in field0) Field_ZF_2_L2:
  assumes  $a \in K$   $b \in K$   $c \in K$   $a \neq b$   $c \neq 0$ 
  shows  $a \cdot c^{-1} \neq b \cdot c^{-1}$ 
  using assms field_has_no_zero_divs Field_ZF_1_L5 Ring_ZF_1_L12B
  by simp

```

We can put a nonzero factor on the other side of non-identity (is this the best way to call it?) changing it to the inverse.

```

lemma (in field0) Field_ZF_2_L3:
  assumes A1:  $a \in K$   $b \in K$   $b \neq 0$   $c \in K$  and A2:  $a \cdot b \neq c$ 
  shows  $a \neq c \cdot b^{-1}$ 
proof -
  from A1 A2 have  $a \cdot b \cdot b^{-1} \neq c \cdot b^{-1}$ 
    using Ring_ZF_1_L4 Field_ZF_2_L2 by simp
  with A1 show  $a \neq c \cdot b^{-1}$  using Field_ZF_1_L7
    by simp

```



qed

If if the inverse of  $b$  is different than  $a$ , then the inverse of  $a$  is different than  $b$ .

```
lemma (in field0) Field_ZF_2_L4:
  assumes a∈K  a≠0 and b-1 ≠ a
  shows a-1 ≠ b
  using assms Field_ZF_1_L4 group0.group0_2_L11B
  by simp
```

An identity with two field elements, one and an inverse.

```
lemma (in field0) Field_ZF_2_L5:
  assumes a∈K  b∈K b≠0
  shows (1 + a·b)·b-1 = a + b-1
  using assms Ring_ZF_1_L4 Field_ZF_1_L5 Ring_ZF_1_L2 ring_oper_distr
    Field_ZF_1_L7 Ring_ZF_1_L3 by simp
```

An identity with three field elements, inverse and cancelling.

```
lemma (in field0) Field_ZF_2_L6: assumes A1: a∈K  b∈K  b≠0  c∈K
  shows a·b·(c·b-1) = a·c
proof -
  from A1 have T: a·b ∈ K  b-1 ∈ K
    using Ring_ZF_1_L4 Field_ZF_1_L5 by auto
  with mult_commute A1 have a·b·(c·b-1) = a·b·(b-1·c)
    using IsCommutative_def by simp
  moreover
  from A1 T have a·b ∈ K  b-1 ∈ K  c∈K
    by auto
  then have a·b·b-1·c = a·b·(b-1·c)
    by (rule Ring_ZF_1_L11)
  ultimately have a·b·(c·b-1) = a·b·b-1·c by simp
  with A1 show a·b·(c·b-1) = a·c
    using Field_ZF_1_L7 by simp
qed
```

### 32.3 1/0=0

In ZF if  $f : X \rightarrow Y$  and  $x \notin X$  we have  $f(x) = \emptyset$ . Since  $\emptyset$  (the empty set) in ZF is the same as zero of natural numbers we can claim that  $1/0 = 0$  in certain sense. In this section we prove a theorem that makes makes it explicit.

The next locale extends the `field0` locale to introduce notation for division operation.

```
locale fieldd = field0 +
  fixes division
  defines division_def[simp]: division ≡ {⟨p, fst(p)·snd(p)-1⟩. p∈K×K0}
```

```

fixes fdiv (infixl / 95)
defines fdiv_def[simp]: x/y  $\equiv$  division(x,y)

```

Division is a function on  $K \times K_0$  with values in  $K$ .

```

lemma (in fieldd) div_fun: shows division:  $K \times K_0 \rightarrow K$ 
proof -
  have  $\forall p \in K \times K_0. \text{fst}(p) \cdot \text{snd}(p)^{-1} \in K$ 
  proof
    fix p assume p  $\in K \times K_0$ 
    hence  $\text{fst}(p) \in K$  and  $\text{snd}(p) \in K_0$  by auto
    then show  $\text{fst}(p) \cdot \text{snd}(p)^{-1} \in K$  using Ring_ZF_1_L4 Field_ZF_1_L5 by
  auto
  qed
  then have  $\{(p, \text{fst}(p) \cdot \text{snd}(p)^{-1}). p \in K \times K_0\}: K \times K_0 \rightarrow K$ 
    by (rule ZF_fun_from_total)
  thus thesis by simp
qed

```

So, really  $1/0 = 0$ . The essential lemma is `apply_0` from standard Isabelle's `func.thy`.

```

theorem (in fieldd) one_over_zero: shows 1/0 = 0
proof-
  have domain(division) =  $K \times K_0$  using div_fun func1_1_L1
    by simp
  hence  $\langle 1, 0 \rangle \notin \text{domain}(\text{division})$  by auto
  then show thesis using apply_0 by simp
qed

end

```

### 33 OrderedField\_ZF.thy

```
theory OrderedField_ZF imports OrderedRing_ZF Field_ZF
```

```
begin
```

This theory covers basic facts about ordered fields.

#### 33.1 Definition and basic properties

Here we define ordered fields and prove their basic properties.

Ordered field is a nontrivial ordered ring such that all non-zero elements have an inverse. We define the notion of being a ordered field as a statement about four sets. The first set, denoted  $K$  is the carrier of the field. The second set, denoted  $A$  represents the additive operation on  $K$  (recall that in ZF set theory functions are sets). The third set  $M$  represents the multiplicative operation on  $K$ . The fourth set  $r$  is the order relation on  $K$ .

**definition**

$$\begin{aligned} \text{IsAnOrdField}(K, A, M, r) \equiv & (\text{IsAnOrdRing}(K, A, M, r) \wedge \\ & (M \text{ \{is commutative on\} } K) \wedge \\ & \text{TheNeutralElement}(K, A) \neq \text{TheNeutralElement}(K, M) \wedge \\ & (\forall a \in K. a \neq \text{TheNeutralElement}(K, A) \longrightarrow \\ & (\exists b \in K. M(a, b) = \text{TheNeutralElement}(K, M)))) \end{aligned}$$

The next context (locale) defines notation used for ordered fields. We do that by extending the notation defined in the `ring1` context that is used for ordered rings and adding some assumptions to make sure we are talking about ordered fields in this context. We should rename the carrier from  $R$  used in the `ring1` context to  $K$ , more appropriate for fields. Theoretically the Isar locale facility supports such renaming, but we experienced difficulties using some lemmas from `ring1` locale after renaming.

```
locale field1 = ring1 +
```

```
  assumes mult_commute: M {is commutative on} R
```

```
  assumes not_triv: 0 ≠ 1
```

```
  assumes inv_exists: ∀ a ∈ R. a ≠ 0 ⟶ (∃ b ∈ R. a · b = 1)
```

```
  fixes non_zero (R0)
```

```
  defines non_zero_def[simp]: R0 ≡ R - {0}
```

```
  fixes inv (_-1 [96] 97)
```

```
  defines inv_def[simp]: a-1 ≡ GroupInv(R0, restrict(M, R0 × R0))(a)
```

The next lemma assures us that we are talking fields in the `field1` context.

```

lemma (in field1) OrdField_ZF_1_L1: shows IsAnOrdField(R,A,M,r)
  using OrdRing_ZF_1_L1 mult_commute not_triv inv_exists IsAnOrdField_def
  by simp

```

Ordered field is a field, of course.

```

lemma OrdField_ZF_1_L1A: assumes IsAnOrdField(K,A,M,r)
  shows IsAfield(K,A,M)
  using assms IsAnOrdField_def IsAnOrdRing_def IsAfield_def
  by simp

```

Theorems proven in field0 (about fields) context are valid in the field1 context (about ordered fields).

```

lemma (in field1) OrdField_ZF_1_L1B: shows field0(R,A,M)
  using OrdField_ZF_1_L1 OrdField_ZF_1_L1A field_field0
  by simp

```

We can use theorems proven in the field1 context whenever we talk about an ordered field.

```

lemma OrdField_ZF_1_L2: assumes IsAnOrdField(K,A,M,r)
  shows field1(K,A,M,r)
  using assms IsAnOrdField_def OrdRing_ZF_1_L2 ring1_def
    IsAnOrdField_def field1_axioms_def field1_def
  by auto

```

In ordered rings the existence of a right inverse for all positive elements implies the existence of an inverse for all non zero elements.

```

lemma (in ring1) OrdField_ZF_1_L3:
  assumes A1:  $\forall a \in R_+. \exists b \in R. a \cdot b = 1$  and A2:  $c \in R \quad c \neq 0$ 
  shows  $\exists b \in R. c \cdot b = 1$ 

```

```

proof -
  { assume  $c \in R_+$ 
    with A1 have  $\exists b \in R. c \cdot b = 1$  by simp }
  moreover
  { assume  $c \notin R_+$ 
    with A2 have  $(-c) \in R_+$ 
      using OrdRing_ZF_3_L2A by simp
    with A1 obtain b where  $b \in R$  and  $(-c) \cdot b = 1$ 
      by auto
    with A2 have  $(-b) \in R \quad c \cdot (-b) = 1$ 
      using Ring_ZF_1_L3 Ring_ZF_1_L7 by auto
    then have  $\exists b \in R. c \cdot b = 1$  by auto }
  ultimately show thesis by blast
qed

```

Ordered fields are easier to deal with, because it is sufficient to show the existence of an inverse for the set of positive elements.

```

lemma (in ring1) OrdField_ZF_1_L4:
  assumes  $0 \neq 1$  and M {is commutative on} R

```

```

and  $\forall a \in R_+. \exists b \in R. a \cdot b = 1$ 
shows IsAnOrdField(R,A,M,r)
using assms OrdRing_ZF_1_L1 OrdField_ZF_1_L3 IsAnOrdField_def
by simp

```

The set of positive field elements is closed under multiplication.

```

lemma (in field1) OrdField_ZF_1_L5: shows  $R_+$  {is closed under} M
  using OrdField_ZF_1_L1B field0.field_has_no_zero_divs OrdRing_ZF_3_L3
  by simp

```

The set of positive field elements is closed under multiplication: the explicit version.

```

lemma (in field1) pos_mul_closed:
  assumes A1:  $0 < a$   $0 < b$ 
  shows  $0 < a \cdot b$ 
proof -
  from A1 have  $a \in R_+$  and  $b \in R_+$ 
  using OrdRing_ZF_3_L14 by auto
  then show  $0 < a \cdot b$ 
  using OrdField_ZF_1_L5 IsOpClosed_def PositiveSet_def
  by simp
qed

```

In fields square of a nonzero element is positive.

```

lemma (in field1) OrdField_ZF_1_L6: assumes  $a \in R$   $a \neq 0$ 
  shows  $a^2 \in R_+$ 
  using assms OrdField_ZF_1_L1B field0.field_has_no_zero_divs
  OrdRing_ZF_3_L15 by simp

```

The next lemma restates the fact Field\_ZF that out notation for the field inverse means what it is supposed to mean.

```

lemma (in field1) OrdField_ZF_1_L7: assumes  $a \in R$   $a \neq 0$ 
  shows  $a \cdot (a^{-1}) = 1$   $(a^{-1}) \cdot a = 1$ 
  using assms OrdField_ZF_1_L1B field0.Field_ZF_1_L6
  by auto

```

A simple lemma about multiplication and cancelling of a positive field element.

```

lemma (in field1) OrdField_ZF_1_L7A:
  assumes A1:  $a \in R$   $b \in R_+$ 
  shows
     $a \cdot b \cdot b^{-1} = a$ 
     $a \cdot b^{-1} \cdot b = a$ 
proof -
  from A1 have  $b \in R$   $b \neq 0$  using PositiveSet_def
  by auto
  with A1 show  $a \cdot b \cdot b^{-1} = a$  and  $a \cdot b^{-1} \cdot b = a$ 
  using OrdField_ZF_1_L1B field0.Field_ZF_1_L7

```

by auto  
qed

Some properties of the inverse of a positive element.

```
lemma (in field1) OrdField_ZF_1_L8: assumes A1: a ∈ R+
  shows a-1 ∈ R+  a·(a-1) = 1  (a-1)·a = 1
proof -
  from A1 have I: a ∈ R  a ≠ 0 using PositiveSet_def
  by auto
  with A1 have a·(a-1)2 ∈ R+
  using OrdField_ZF_1_L1B field0.Field_ZF_1_L5 OrdField_ZF_1_L6
  OrdField_ZF_1_L5 IsOpClosed_def by simp
  with I show a-1 ∈ R+
  using OrdField_ZF_1_L1B field0.Field_ZF_2_L1
  by simp
  from I show a·(a-1) = 1  (a-1)·a = 1
  using OrdField_ZF_1_L7 by auto
qed
```

If  $a < b$ , then  $(b - a)^{-1}$  is positive.

```
lemma (in field1) OrdField_ZF_1_L9: assumes a < b
  shows (b-a)-1 ∈ R+
  using assms OrdRing_ZF_1_L14 OrdField_ZF_1_L8
  by simp
```

In ordered fields if at least one of  $a, b$  is not zero, then  $a^2 + b^2 > 0$ , in particular  $a^2 + b^2 \neq 0$  and exists the (multiplicative) inverse of  $a^2 + b^2$ .

```
lemma (in field1) OrdField_ZF_1_L10:
  assumes A1: a ∈ R  b ∈ R and A2: a ≠ 0 ∨ b ≠ 0
  shows 0 < a2 + b2 and ∃ c ∈ R. (a2 + b2)·c = 1
proof -
  from A1 A2 show 0 < a2 + b2
  using OrdField_ZF_1_L1B field0.field_has_no_zero_divs
  OrdRing_ZF_3_L19 by simp
  then have
    (a2 + b2)-1 ∈ R and (a2 + b2)·(a2 + b2)-1 = 1
  using OrdRing_ZF_1_L3 PositiveSet_def OrdField_ZF_1_L8
  by auto
  then show ∃ c ∈ R. (a2 + b2)·c = 1 by auto
qed
```

### 33.2 Inequalities

In this section we develop tools to deal inequalities in fields.

We can multiply strict inequality by a positive element.

```
lemma (in field1) OrdField_ZF_2_L1:
  assumes a < b and c ∈ R+
```

```

shows a·c < b·c
using assms OrdField_ZF_1_L1B field0.field_has_no_zero_divs
    OrdRing_ZF_3_L13
by simp

```

A special case of OrdField\_ZF\_2\_L1 when we multiply an inverse by an element.

```

lemma (in field1) OrdField_ZF_2_L2:
  assumes A1: a∈R+ and A2: a-1 < b
  shows 1 < b·a
proof -
  from A1 A2 have (a-1)·a < b·a
    using OrdField_ZF_2_L1 by simp
  with A1 show 1 < b·a
    using OrdField_ZF_1_L8 by simp
qed

```

We can multiply an inequality by the inverse of a positive element.

```

lemma (in field1) OrdField_ZF_2_L3:
  assumes a≤b and c∈R+ shows a·(c-1) ≤ b·(c-1)
  using assms OrdField_ZF_1_L8 OrdRing_ZF_1_L9A
  by simp

```

We can multiply a strict inequality by a positive element or its inverse.

```

lemma (in field1) OrdField_ZF_2_L4:
  assumes a<b and c∈R+
  shows
    a·c < b·c
    c·a < c·b
    a·c-1 < b·c-1
  using assms OrdField_ZF_1_L1B field0.field_has_no_zero_divs
    OrdField_ZF_1_L8 OrdRing_ZF_3_L13 by auto

```

We can put a positive factor on the other side of an inequality, changing it to its inverse.

```

lemma (in field1) OrdField_ZF_2_L5:
  assumes A1: a∈R b∈R+ and A2: a·b ≤ c
  shows a ≤ c·b-1
proof -
  from A1 A2 have a·b·b-1 ≤ c·b-1
    using OrdField_ZF_2_L3 by simp
  with A1 show a ≤ c·b-1 using OrdField_ZF_1_L7A
    by simp
qed

```

We can put a positive factor on the other side of an inequality, changing it to its inverse, version with a product initially on the right hand side.

```

lemma (in field1) OrdField_ZF_2_L5A:

```

```

    assumes A1:  $b \in \mathbb{R}$   $c \in \mathbb{R}_+$  and A2:  $a \leq b \cdot c$ 
    shows  $a \cdot c^{-1} \leq b$ 
  proof -
    from A1 A2 have  $a \cdot c^{-1} \leq b \cdot c \cdot c^{-1}$ 
      using OrdField_ZF_2_L3 by simp
    with A1 show  $a \cdot c^{-1} \leq b$  using OrdField_ZF_1_L7A
      by simp
  qed

```

We can put a positive factor on the other side of a strict inequality, changing it to its inverse, version with a product initially on the left hand side.

```

lemma (in field1) OrdField_ZF_2_L6:
  assumes A1:  $a \in \mathbb{R}$   $b \in \mathbb{R}_+$  and A2:  $a \cdot b < c$ 
  shows  $a < c \cdot b^{-1}$ 
proof -
  from A1 A2 have  $a \cdot b \cdot b^{-1} < c \cdot b^{-1}$ 
    using OrdField_ZF_2_L4 by simp
  with A1 show  $a < c \cdot b^{-1}$  using OrdField_ZF_1_L7A
    by simp
qed

```

We can put a positive factor on the other side of a strict inequality, changing it to its inverse, version with a product initially on the right hand side.

```

lemma (in field1) OrdField_ZF_2_L6A:
  assumes A1:  $b \in \mathbb{R}$   $c \in \mathbb{R}_+$  and A2:  $a < b \cdot c$ 
  shows  $a \cdot c^{-1} < b$ 
proof -
  from A1 A2 have  $a \cdot c^{-1} < b \cdot c \cdot c^{-1}$ 
    using OrdField_ZF_2_L4 by simp
  with A1 show  $a \cdot c^{-1} < b$  using OrdField_ZF_1_L7A
    by simp
qed

```

Sometimes we can reverse an inequality by taking inverse on both sides.

```

lemma (in field1) OrdField_ZF_2_L7:
  assumes A1:  $a \in \mathbb{R}_+$  and A2:  $a^{-1} \leq b$ 
  shows  $b^{-1} \leq a$ 
proof -
  from A1 have  $a^{-1} \in \mathbb{R}_+$  using OrdField_ZF_1_L8
    by simp
  with A2 have  $b \in \mathbb{R}_+$  using OrdRing_ZF_3_L7
    by blast
  then have T:  $b \in \mathbb{R}_+$   $b^{-1} \in \mathbb{R}_+$  using OrdField_ZF_1_L8
    by auto
  with A1 A2 have  $b^{-1} \cdot a^{-1} \cdot a \leq b^{-1} \cdot b \cdot a$ 
    using OrdRing_ZF_1_L9A by simp
  moreover
  from A1 A2 T have

```



```

    b-1 ∈ R  a ∈ R  a ≠ 0  b ∈ R  b ≠ 0
    using PositiveSet_def OrdRing_ZF_1_L3 by auto
  then have b-1 · a-1 · a = b-1 and b-1 · b · a = a
    using OrdField_ZF_1_L1B field0.Field_ZF_1_L7
      field0.Field_ZF_1_L6 Ring_ZF_1_L3
    by auto
  ultimately show b-1 ≤ a by simp
qed

```

Sometimes we can reverse a strict inequality by taking inverse on both sides.

```

lemma (in field1) OrdField_ZF_2_L8:
  assumes A1: a ∈ R+ and A2: a-1 < b
  shows b-1 < a
proof -
  from A1 A2 have a-1 ∈ R+ a-1 ≤ b
    using OrdField_ZF_1_L8 by auto
  then have b ∈ R+ using OrdRing_ZF_3_L7
    by blast
  then have b ∈ R  b ≠ 0 using PositiveSet_def by auto
  with A2 have b-1 ≠ a
    using OrdField_ZF_1_L1B field0.Field_ZF_2_L4
    by simp
  with A1 A2 show b-1 < a
    using OrdField_ZF_2_L7 by simp
qed

```

A technical lemma about solving a strict inequality with three field elements and inverse of a difference.

```

lemma (in field1) OrdField_ZF_2_L9:
  assumes A1: a < b and A2: (b-a)-1 < c
  shows 1 + a · c < b · c
proof -
  from A1 A2 have (b-a)-1 ∈ R+ (b-a)-1 ≤ c
    using OrdField_ZF_1_L9 by auto
  then have T1: c ∈ R+ using OrdRing_ZF_3_L7 by blast
  with A1 A2 have T2:
    a ∈ R  b ∈ R  c ∈ R  c ≠ 0  c-1 ∈ R
    using OrdRing_ZF_1_L3 OrdField_ZF_1_L8 PositiveSet_def
    by auto
  with A1 A2 have c-1 + a < b-a + a
    using OrdRing_ZF_1_L14 OrdField_ZF_2_L8 ring_strict_ord_trans_inv
    by simp
  with T1 T2 have (c-1 + a) · c < b · c
    using Ring_ZF_2_L1A OrdField_ZF_2_L1 by simp
  with T1 T2 show 1 + a · c < b · c
    using ring_oper_distr OrdField_ZF_1_L8
    by simp
qed

```

### 33.3 Definition of real numbers

The only purpose of this section is to define what does it mean to be a model of real numbers.

We define model of real numbers as any quadruple of sets  $(K, A, M, r)$  such that  $(K, A, M, r)$  is an ordered field and the order relation  $r$  is complete, that is every set that is nonempty and bounded above in this relation has a supremum.

**definition**

`IsAmodelOfReals(K,A,M,r)  $\equiv$  IsAnOrdField(K,A,M,r)  $\wedge$  (r {is complete})`

**end**

## 34 Int\_ZF.thy

```
theory Int_ZF_IML imports OrderedGroup_ZF_1 Finite_ZF_1 Int_ZF Nat_ZF_IML
```

```
begin
```

This theory file is an interface between the old-style Isabelle (ZF logic) material on integers and the IsarMathLib project. Here we redefine the meta-level operations on integers (addition and multiplication) to convert them to ZF-functions and show that integers form a commutative group with respect to addition and commutative monoid with respect to multiplication. Similarly, we redefine the order on integers as a relation, that is a subset of  $Z \times Z$ . We show that a subset of integers is bounded iff it is finite. As we are forced to use standard Isabelle notation with all these dollar signs, sharps etc. to denote "type coercions" (?) the notation is often ugly and difficult to read.

### 34.1 Addition and multiplication as ZF-functions.

In this section we provide definitions of addition and multiplication as subsets of  $(Z \times Z) \times Z$ . We use the (higher order) relation defined in the standard `Int` theory to define a subset of  $Z \times Z$  that constitutes the ZF order relation corresponding to it. We define the set of positive integers using the notion of positive set from the `OrderedGroup_ZF` theory.

Definition of addition of integers as a binary operation on `int`. Recall that in standard Isabelle/ZF `int` is the set of integers and the sum of integers is denoted by prepending  $+$  with a dollar sign.

**definition**

$$\text{IntegerAddition} \equiv \{ \langle x, c \rangle \in (\text{int} \times \text{int}) \times \text{int}. \text{fst}(x) \$+ \text{snd}(x) = c \}$$

Definition of multiplication of integers as a binary operation on `int`. In standard Isabelle/ZF product of integers is denoted by prepending the dollar sign to  $\times$ .

**definition**

$$\begin{aligned} \text{IntegerMultiplication} \equiv \\ \{ \langle x, c \rangle \in (\text{int} \times \text{int}) \times \text{int}. \text{fst}(x) \$\times \text{snd}(x) = c \} \end{aligned}$$

Definition of natural order on integers as a relation on `int`. In the standard Isabelle/ZF the inequality relation on integers is denoted  $\leq$  prepended with the dollar sign.

**definition**

$$\text{IntegerOrder} \equiv \{ p \in \text{int} \times \text{int}. \text{fst}(p) \$\leq \text{snd}(p) \}$$

This defines the set of positive integers.

**definition**

```

PositiveIntegers  $\equiv$  PositiveSet(int,IntegerAddition,IntegerOrder)

IntegerAddition and IntegerMultiplication are functions on  $\text{int} \times \text{int}$ .

lemma Int_ZF_1_L1: shows
  IntegerAddition :  $\text{int} \times \text{int} \rightarrow \text{int}$ 
  IntegerMultiplication :  $\text{int} \times \text{int} \rightarrow \text{int}$ 
proof -
  have
    { $\langle x, c \rangle \in (\text{int} \times \text{int}) \times \text{int}. \text{fst}(x) \$+ \text{snd}(x) = c$ }  $\in \text{int} \times \text{int} \rightarrow \text{int}$ 
    { $\langle x, c \rangle \in (\text{int} \times \text{int}) \times \text{int}. \text{fst}(x) \$\times \text{snd}(x) = c$ }  $\in \text{int} \times \text{int} \rightarrow \text{int}$ 
    using func1_1_L11A by auto
  then show IntegerAddition :  $\text{int} \times \text{int} \rightarrow \text{int}$ 
    IntegerMultiplication :  $\text{int} \times \text{int} \rightarrow \text{int}$ 
    using IntegerAddition_def IntegerMultiplication_def by auto
qed

```

The next context (locale) defines notation used for integers. We define **0** to denote the neutral element of addition, **1** as the unit of the multiplicative monoid. We introduce notation  $m \leq n$  for integers and write  $m..n$  to denote the integer interval with endpoints in  $m$  and  $n$ .  $\text{abs}(m)$  means the absolute value of  $m$ . This is a function defined in `OrderedGroup` that assigns  $x$  to itself if  $x$  is positive and assigns the opposite of  $x$  if  $x \leq 0$ . Unfortunately we cannot use the  $|\cdot|$  notation as in the `OrderedGroup` theory as this notation has been hogged by the standard Isabelle's `Int` theory. The notation  $-A$  where  $A$  is a subset of integers means the set  $\{-m : m \in A\}$ . The symbol  $\text{maxf}(f, M)$  denotes the maximum of function  $f$  over the set  $A$ . We also introduce a similar notation for the minimum.

```

locale int0 =

  fixes ints ( $\mathbb{Z}$ )
  defines ints_def [simp]:  $\mathbb{Z} \equiv \text{int}$ 

  fixes ia (infixl + 69)
  defines ia_def [simp]:  $a+b \equiv \text{IntegerAddition}(\langle a, b \rangle)$ 

  fixes iminus (- _ 72)
  defines rminus_def [simp]:  $-a \equiv \text{GroupInv}(\mathbb{Z}, \text{IntegerAddition})(a)$ 

  fixes isub (infixl - 69)
  defines isub_def [simp]:  $a-b \equiv a+(-b)$ 

  fixes imult (infixl  $\cdot$  70)
  defines imult_def [simp]:  $a \cdot b \equiv \text{IntegerMultiplication}(\langle a, b \rangle)$ 

  fixes setneg (- _ 72)
  defines setneg_def [simp]:  $-A \equiv \text{GroupInv}(\mathbb{Z}, \text{IntegerAddition})(A)$ 

  fixes izero (0)

```

```

defines izero_def [simp]: 0  $\equiv$  TheNeutralElement( $\mathbb{Z}$ ,IntegerAddition)

fixes ione (1)
defines ione_def [simp]: 1  $\equiv$  TheNeutralElement( $\mathbb{Z}$ ,IntegerMultiplication)

fixes itwo (2)
defines itwo_def [simp]: 2  $\equiv$  1+1

fixes ithree (3)
defines ithree_def [simp]: 3  $\equiv$  2+1

fixes nonnegative ( $\mathbb{Z}^+$ )
defines nonnegative_def [simp]:
 $\mathbb{Z}^+ \equiv$  Nonnegative( $\mathbb{Z}$ ,IntegerAddition,IntegerOrder)

fixes positive ( $\mathbb{Z}_+$ )
defines positive_def [simp]:
 $\mathbb{Z}_+ \equiv$  PositiveSet( $\mathbb{Z}$ ,IntegerAddition,IntegerOrder)

fixes abs
defines abs_def [simp]:
abs(m)  $\equiv$  AbsoluteValue( $\mathbb{Z}$ ,IntegerAddition,IntegerOrder)(m)

fixes lesseq (infix  $\leq$  60)
defines lesseq_def [simp]:  $m \leq n \equiv \langle m,n \rangle \in$  IntegerOrder

fixes interval (infix  $\dots$  70)
defines interval_def [simp]:  $m..n \equiv$  Interval(IntegerOrder,m,n)

fixes maxf
defines maxf_def [simp]: maxf(f,A)  $\equiv$  Maximum(IntegerOrder,f(A))

fixes minf
defines minf_def [simp]: minf(f,A)  $\equiv$  Minimum(IntegerOrder,f(A))

```

IntegerAddition adds integers and IntegerMultiplication multiplies integers. This states that the ZF functions IntegerAddition and IntegerMultiplication give the same results as the higher-order equivalents defined in the standard Int theory.

```

lemma (in int0) Int_ZF_1_L2: assumes A1:  $a \in \mathbb{Z} \quad b \in \mathbb{Z}$ 
shows
   $a+b = a \ \$+ \ b$ 
   $a \cdot b = a \ \$\times \ b$ 
proof -
  let x =  $\langle a,b \rangle$ 
  let c =  $a \ \$+ \ b$ 
  let d =  $a \ \$\times \ b$ 
  from A1 have
     $\langle x,c \rangle \in \{ \langle x,c \rangle \in (\mathbb{Z} \times \mathbb{Z}) \times \mathbb{Z}. \text{fst}(x) \ \$+ \ \text{snd}(x) = c \}$ 

```

```

    ⟨ x,d⟩ ∈ {⟨ x,d⟩ ∈ (ℤ×ℤ)×ℤ. fst(x) $× snd(x) = d}
  by auto
then show a+b = a $+ b  a·b = a $× b
  using IntegerAddition_def IntegerMultiplication_def
  Int_ZF_1_L1 apply_iff by auto
qed

```

Integer addition and multiplication are associative.

```

lemma (in int0) Int_ZF_1_L3:
  assumes x∈ℤ  y∈ℤ  z∈ℤ
  shows x+y+z = x+(y+z)  x·y·z = x·(y·z)
  using assms Int_ZF_1_L2 zadd_assoc zmult_assoc by auto

```

Integer addition and multiplication are commutative.

```

lemma (in int0) Int_ZF_1_L4:
  assumes x∈ℤ  y∈ℤ
  shows x+y = y+x  x·y = y·x
  using assms Int_ZF_1_L2 zadd_commute zmult_commute
  by auto

```

Zero is neutral for addition and one for multiplication.

```

lemma (in int0) Int_ZF_1_L5: assumes A1:x∈ℤ
  shows ($# 0) + x = x ∧ x + ($# 0) = x
  ($# 1)·x = x ∧ x·($# 1) = x
proof -
  from A1 show ($# 0) + x = x ∧ x + ($# 0) = x
    using Int_ZF_1_L2 zadd_int0 Int_ZF_1_L4 by simp
  from A1 have ($# 1)·x = x
    using Int_ZF_1_L2 zmult_int1 by simp
  with A1 show ($# 1)·x = x ∧ x·($# 1) = x
    using Int_ZF_1_L4 by simp
qed

```

Zero is neutral for addition and one for multiplication.

```

lemma (in int0) Int_ZF_1_L6: shows ($# 0)∈ℤ ∧
  (∀x∈ℤ. ($# 0)+x = x ∧ x+($# 0) = x)
  ($# 1)∈ℤ ∧
  (∀x∈ℤ. ($# 1)·x = x ∧ x·($# 1) = x)
  using Int_ZF_1_L5 by auto

```

Integers with addition and integers with multiplication form monoids.

```

theorem (in int0) Int_ZF_1_T1: shows
  IsAmonoid(ℤ,IntegerAddition)
  IsAmonoid(ℤ,IntegerMultiplication)
proof -
  have
    ∃e∈ℤ. ∀x∈ℤ. e+x = x ∧ x+e = x
    ∃e∈ℤ. ∀x∈ℤ. e·x = x ∧ x·e = x

```

```

    using int0.Int_ZF_1_L6 by auto
  then show IsAmonoid( $\mathbb{Z}$ , IntegerAddition)
    IsAmonoid( $\mathbb{Z}$ , IntegerMultiplication) using
    IsAmonoid_def IsAssociative_def Int_ZF_1_L1 Int_ZF_1_L3
  by auto
qed

```

Zero is the neutral element of the integers with addition and one is the neutral element of the integers with multiplication.

```

lemma (in int0) Int_ZF_1_L8: shows ( $\#$  0) = 0  ( $\#$  1) = 1
proof -
  have monoid0( $\mathbb{Z}$ , IntegerAddition)
    using Int_ZF_1_T1 monoid0_def by simp
  moreover have
    ( $\#$  0)  $\in \mathbb{Z}$   $\wedge$ 
    ( $\forall x \in \mathbb{Z}. \text{IntegerAddition}(\# 0, x) = x \wedge$ 
    IntegerAddition( $x, \# 0$ ) =  $x$ )
    using Int_ZF_1_L6 by auto
  ultimately have ( $\#$  0) = TheNeutralElement( $\mathbb{Z}$ , IntegerAddition)
    by (rule monoid0.group0_1_L4)
  then show ( $\#$  0) = 0 by simp
  have monoid0(int, IntegerMultiplication)
    using Int_ZF_1_T1 monoid0_def by simp
  moreover have ( $\#$  1)  $\in$  int  $\wedge$ 
    ( $\forall x \in$  int. IntegerMultiplication( $\#$  1,  $x$ ) =  $x \wedge$ 
    IntegerMultiplication( $x, \# 1$ ) =  $x$ )
    using Int_ZF_1_L6 by auto
  ultimately have
    ( $\#$  1) = TheNeutralElement(int, IntegerMultiplication)
    by (rule monoid0.group0_1_L4)
  then show ( $\#$  1) = 1 by simp
qed

```

0 and 1, as defined in int0 context, are integers.

```

lemma (in int0) Int_ZF_1_L8A: shows 0  $\in \mathbb{Z}$  1  $\in \mathbb{Z}$ 
proof -
  have ( $\#$  0)  $\in \mathbb{Z}$   ( $\#$  1)  $\in \mathbb{Z}$  by auto
  then show 0  $\in \mathbb{Z}$  1  $\in \mathbb{Z}$  using Int_ZF_1_L8 by auto
qed

```

Zero is not one.

```

lemma (in int0) int_zero_not_one: shows 0  $\neq$  1
proof -
  have ( $\#$  0)  $\neq$  ( $\#$  1) by simp
  then show 0  $\neq$  1 using Int_ZF_1_L8 by simp
qed

```

The set of integers is not empty, of course.

```

lemma (in int0) int_not_empty: shows  $\mathbb{Z} \neq \emptyset$ 

```

```
using Int_ZF_1_L8A by auto
```

The set of integers has more than just zero in it.

```
lemma (in int0) int_not_trivial: shows  $\mathbb{Z} \neq \{0\}$ 
  using Int_ZF_1_L8A int_zero_not_one by blast
```

Each integer has an inverse (in the addition sense).

```
lemma (in int0) Int_ZF_1_L9: assumes A1:  $g \in \mathbb{Z}$ 
  shows  $\exists b \in \mathbb{Z}. g+b = 0$ 
proof -
  from A1 have  $g+(-g) = 0$ 
    using Int_ZF_1_L2 Int_ZF_1_L8 by simp
  thus thesis by auto
qed
```

Integers with addition form an abelian group. This also shows that we can apply all theorems proven in the proof contexts (locales) that require the assumption that some pair of sets form a group like locale `group0`.

```
theorem Int_ZF_1_T2: shows
  IsAgroup(int,IntegerAddition)
  IntegerAddition {is commutative on} int
  group0(int,IntegerAddition)
  using int0.Int_ZF_1_T1 int0.Int_ZF_1_L9 IsAgroup_def
  group0_def int0.Int_ZF_1_L4 IsCommutative_def by auto
```

What is the additive group inverse in the group of integers?

```
lemma (in int0) Int_ZF_1_L9A: assumes A1:  $m \in \mathbb{Z}$ 
  shows  $-m = -m$ 
proof -
  from A1 have  $m \in \text{int}$   $-m \in \text{int}$  IntegerAddition< $m, -m$ > =
    TheNeutralElement(int,IntegerAddition)
  using zminus_type Int_ZF_1_L2 Int_ZF_1_L8 by auto
  then have  $-m = \text{GroupInv}(\text{int}, \text{IntegerAddition})(m)$ 
    using Int_ZF_1_T2 group0.group0_2_L9 by blast
  then show thesis by simp
qed
```

Subtracting integers corresponds to adding the negative.

```
lemma (in int0) Int_ZF_1_L10: assumes A1:  $m \in \mathbb{Z} \quad n \in \mathbb{Z}$ 
  shows  $m-n = m + (-n)$ 
  using assms Int_ZF_1_T2 group0.inverse_in_group Int_ZF_1_L9A Int_ZF_1_L2
  by simp
```

Negative of zero is zero.

```
lemma (in int0) Int_ZF_1_L11: shows  $(-0) = 0$ 
  using Int_ZF_1_T2 group0.group_inv_of_one by simp
```

A trivial calculation lemma that allows to subtract and add one.



```

lemma Int_ZF_1_L12:
  assumes m ∈ int shows m $- $#1 $+ $#1 = m
  using assms eq_zdiff_iff by auto

```

A trivial calculation lemma that allows to subtract and add one, version with ZF-operation.

```

lemma (in int0) Int_ZF_1_L13: assumes m ∈ ℤ
  shows (m $- $#1) + 1 = m
  using assms Int_ZF_1_L8A Int_ZF_1_L2 Int_ZF_1_L8 Int_ZF_1_L12
  by simp

```

Adding or subtracing one changes integers.

```

lemma (in int0) Int_ZF_1_L14: assumes A1: m ∈ ℤ
  shows
    m+1 ≠ m
    m-1 ≠ m
  proof -
    { assume m+1 = m
      with A1 have
        group0(ℤ,IntegerAddition)
        m ∈ ℤ 1 ∈ ℤ
        IntegerAddition⟨m,1⟩ = m
        using Int_ZF_1_T2 Int_ZF_1_L8A by auto
      then have 1 = TheNeutralElement(ℤ,IntegerAddition)
        by (rule group0.group0_2_L7)
      then have False using int_zero_not_one by simp
    } then show I: m+1 ≠ m by auto
    { from A1 have m - 1 + 1 = m
      using Int_ZF_1_L8A Int_ZF_1_T2 group0.inv_cancel_two
      by simp
      moreover assume m-1 = m
      ultimately have m + 1 = m by simp
      with I have False by simp
    } then show m-1 ≠ m by auto
  qed

```

If the difference is zero, the integers are equal.

```

lemma (in int0) Int_ZF_1_L15:
  assumes A1: m ∈ ℤ n ∈ ℤ and A2: m-n = 0
  shows m=n
  proof -
    let G = ℤ
    let f = IntegerAddition
    from A1 A2 have
      group0(G, f)
      m ∈ G n ∈ G
      f⟨m, GroupInv(G, f)(n)⟩ = TheNeutralElement(G, f)
      using Int_ZF_1_T2 by auto
    then show m=n by (rule group0.group0_2_L11A)
  qed

```

qed

## 34.2 Integers as an ordered group

In this section we define order on integers as a relation, that is a subset of  $\mathbb{Z} \times \mathbb{Z}$  and show that integers form an ordered group.

The next lemma interprets the order definition one way.

```
lemma (in int0) Int_ZF_2_L1:
  assumes A1:  $m \in \mathbb{Z}$   $n \in \mathbb{Z}$  and A2:  $m \leq n$ 
  shows  $m \leq n$ 
proof -
  from A1 A2 have  $\langle m, n \rangle \in \{x \in \mathbb{Z} \times \mathbb{Z}. \text{fst}(x) \leq \text{snd}(x)\}$ 
  by simp
  then show thesis using IntegerOrder_def by simp
qed
```

The next lemma interprets the definition the other way.

```
lemma (in int0) Int_ZF_2_L1A: assumes A1:  $m \leq n$ 
  shows  $m \leq n$   $m \in \mathbb{Z}$   $n \in \mathbb{Z}$ 
proof -
  from A1 have  $\langle m, n \rangle \in \{p \in \mathbb{Z} \times \mathbb{Z}. \text{fst}(p) \leq \text{snd}(p)\}$ 
  using IntegerOrder_def by simp
  thus  $m \leq n$   $m \in \mathbb{Z}$   $n \in \mathbb{Z}$  by auto
qed
```

Integer order is a relation on integers.

```
lemma Int_ZF_2_L1B: shows IntegerOrder  $\subseteq$   $\text{int} \times \text{int}$ 
proof
  fix x assume  $x \in \text{IntegerOrder}$ 
  then have  $x \in \{p \in \text{int} \times \text{int}. \text{fst}(p) \leq \text{snd}(p)\}$ 
  using IntegerOrder_def by simp
  then show  $x \in \text{int} \times \text{int}$  by simp
qed
```

The way we define the notion of being bounded below, its sufficient for the relation to be on integers for all bounded below sets to be subsets of integers.

```
lemma (in int0) Int_ZF_2_L1C:
  assumes A1: IsBoundedBelow(A, IntegerOrder)
  shows  $A \subseteq \mathbb{Z}$ 
proof -
  from A1 have
    IntegerOrder  $\subseteq \mathbb{Z} \times \mathbb{Z}$ 
    IsBoundedBelow(A, IntegerOrder)
  using Int_ZF_2_L1B by auto
  then show  $A \subseteq \mathbb{Z}$  by (rule Order_ZF_3_L1B)
qed
```

The order on integers is reflexive.

```
lemma (in int0) int_ord_is_refl: shows refl( $\mathbb{Z}$ , IntegerOrder)
  using Int_ZF_2_L1 zle_refl refl_def by auto
```

The essential condition to show antisymmetry of the order on integers.

```
lemma (in int0) Int_ZF_2_L3:
  assumes A1:  $m \leq n \quad n \leq m$ 
  shows  $m=n$ 
proof -
  from A1 have  $m \leq n \quad n \leq m \quad m \in \mathbb{Z} \quad n \in \mathbb{Z}$ 
    using Int_ZF_2_L1A by auto
  then show  $m=n$  using zle_anti_sym by auto
qed
```

The order on integers is antisymmetric.

```
lemma (in int0) Int_ZF_2_L4: shows antisym(IntegerOrder)
proof -
  have  $\forall m \ n. m \leq n \ \wedge \ n \leq m \longrightarrow m=n$ 
    using Int_ZF_2_L3 by auto
  then show thesis using imp_conj antisym_def by simp
qed
```

The essential condition to show that the order on integers is transitive.

```
lemma Int_ZF_2_L5:
  assumes A1:  $\langle m, n \rangle \in \text{IntegerOrder} \quad \langle n, k \rangle \in \text{IntegerOrder}$ 
  shows  $\langle m, k \rangle \in \text{IntegerOrder}$ 
proof -
  from A1 have T1:  $m \leq n \quad n \leq k$  and T2:  $m \in \text{int} \quad k \in \text{int}$ 
    using int0.Int_ZF_2_L1A by auto
  from T1 have  $m \leq k$  by (rule zle_trans)
  with T2 show thesis using int0.Int_ZF_2_L1 by simp
qed
```

The order on integers is transitive. This version is stated in the int0 context using notation for integers.

```
lemma (in int0) Int_order_transitive:
  assumes A1:  $m \leq n \quad n \leq k$ 
  shows  $m \leq k$ 
proof -
  from A1 have  $\langle m, n \rangle \in \text{IntegerOrder} \quad \langle n, k \rangle \in \text{IntegerOrder}$ 
    by auto
  then have  $\langle m, k \rangle \in \text{IntegerOrder}$  by (rule Int_ZF_2_L5)
  then show  $m \leq k$  by simp
qed
```

The order on integers is transitive.

```
lemma Int_ZF_2_L6: shows trans(IntegerOrder)
```

```

proof -
  have  $\forall m n k.$ 
     $\langle m, n \rangle \in \text{IntegerOrder} \wedge \langle n, k \rangle \in \text{IntegerOrder} \longrightarrow$ 
     $\langle m, k \rangle \in \text{IntegerOrder}$ 
    using Int_ZF_2_L5 by blast
  then show thesis by (rule Fol1_L2)
qed

```

The order on integers is a partial order.

```

lemma Int_ZF_2_L7: shows IsPartOrder(int,IntegerOrder)
  using int0.int_ord_is_refl int0.Int_ZF_2_L4
  Int_ZF_2_L6 IsPartOrder_def by simp

```

The essential condition to show that the order on integers is preserved by translations.

```

lemma (in int0) int_ord_transl_inv:
  assumes A1:  $k \in \mathbb{Z}$  and A2:  $m \leq n$ 
  shows  $m+k \leq n+k \quad k+m \leq k+n$ 
proof -
  from A2 have  $m \leq n$  and  $m \in \mathbb{Z} \ n \in \mathbb{Z}$ 
  using Int_ZF_2_L1A by auto
  with A1 show  $m+k \leq n+k \quad k+m \leq k+n$ 
  using zadd_right_cancel_zle zadd_left_cancel_zle
  Int_ZF_1_L2 Int_ZF_1_L1 apply_funtype
  Int_ZF_1_L2 Int_ZF_2_L1 Int_ZF_1_L2 by auto
qed

```

Integers form a linearly ordered group. We can apply all theorems proven in group3 context to integers.

```

theorem (in int0) Int_ZF_2_T1: shows
  IsAnOrdGroup( $\mathbb{Z}$ ,IntegerAddition,IntegerOrder)
  IntegerOrder {is total on}  $\mathbb{Z}$ 
  group3( $\mathbb{Z}$ ,IntegerAddition,IntegerOrder)
  IsLinOrder( $\mathbb{Z}$ ,IntegerOrder)
proof -
  have  $\forall k \in \mathbb{Z}. \forall m n. m \leq n \longrightarrow$ 
     $m+k \leq n+k \wedge k+m \leq k+n$ 
    using int_ord_transl_inv by simp
  then show T1: IsAnOrdGroup( $\mathbb{Z}$ ,IntegerAddition,IntegerOrder) using
    Int_ZF_1_T2 Int_ZF_2_L1B Int_ZF_2_L7 IsAnOrdGroup_def
    by simp
  then show group3( $\mathbb{Z}$ ,IntegerAddition,IntegerOrder)
    using group3_def by simp
  have  $\forall n \in \mathbb{Z}. \forall m \in \mathbb{Z}. n \leq m \vee m \leq n$ 
    using zle_linear Int_ZF_2_L1 by auto
  then show IntegerOrder {is total on}  $\mathbb{Z}$ 
    using IsTotal_def by simp
  with T1 show IsLinOrder( $\mathbb{Z}$ ,IntegerOrder)

```

```

    using IsAnOrdGroup_def IsPartOrder_def IsLinOrder_def by simp
qed

```

If a pair  $(i, m)$  belongs to the order relation on integers and  $i \neq m$ , then  $i < m$  in the sense of defined in the standard Isabelle's Int.thy.

```

lemma (in int0) Int_ZF_2_L9: assumes A1:  $i \leq m$  and A2:  $i \neq m$ 
  shows  $i < m$ 
proof -
  from A1 have  $i \leq m$   $i \in \mathbb{Z}$   $m \in \mathbb{Z}$ 
    using Int_ZF_2_L1A by auto
  with A2 show  $i < m$  using zle_def by simp
qed

```

This shows how Isabelle's  $<$  operator translates to IsarMathLib notation.

```

lemma (in int0) Int_ZF_2_L9AA: assumes A1:  $m \in \mathbb{Z}$   $n \in \mathbb{Z}$ 
  and A2:  $m < n$ 
  shows  $m \leq n$   $m \neq n$ 
  using assms zle_def Int_ZF_2_L1 by auto

```

A small technical lemma about putting one on the other side of an inequality.

```

lemma (in int0) Int_ZF_2_L9A:
  assumes A1:  $k \in \mathbb{Z}$  and A2:  $m \leq k - (\# 1)$ 
  shows  $m+1 \leq k$ 
proof -
  from A2 have  $m+1 \leq (k - (\# 1)) + 1$ 
    using Int_ZF_1_L8A int_ord_transl_inv by simp
  with A1 show  $m+1 \leq k$ 
    using Int_ZF_1_L13 by simp
qed

```

We can put any integer on the other side of an inequality reversing its sign.

```

lemma (in int0) Int_ZF_2_L9B: assumes  $i \in \mathbb{Z}$   $m \in \mathbb{Z}$   $k \in \mathbb{Z}$ 
  shows  $i+m \leq k \iff i \leq k-m$ 
  using assms Int_ZF_2_T1 group3.OrderedGroup_ZF_1_L9A
  by simp

```

A special case of Int\_ZF\_2\_L9B with weaker assumptions.

```

lemma (in int0) Int_ZF_2_L9C:
  assumes  $i \in \mathbb{Z}$   $m \in \mathbb{Z}$  and  $i-m \leq k$ 
  shows  $i \leq k+m$ 
  using assms Int_ZF_2_T1 group3.OrderedGroup_ZF_1_L9B
  by simp

```

Taking (higher order) minus on both sides of inequality reverses it.

```

lemma (in int0) Int_ZF_2_L10: assumes  $k \leq i$ 
  shows
     $(-i) \leq (-k)$ 
     $\neg i \leq \neg k$ 

```

```

using assms Int_ZF_2_L1A Int_ZF_1_L9A Int_ZF_2_T1
group3.OrderedGroup_ZF_1_L5 by auto

```

Taking minus on both sides of inequality reverses it, version with a negative on one side.

```

lemma (in int0) Int_ZF_2_L10AA: assumes  $n \in \mathbb{Z}$   $m \leq (-n)$ 
shows  $n \leq (-m)$ 
using assms Int_ZF_2_T1 group3.OrderedGroup_ZF_1_L5AD
by simp

```

We can cancel the same element on on both sides of an inequality, a version with minus on both sides.

```

lemma (in int0) Int_ZF_2_L10AB:
assumes  $m \in \mathbb{Z}$   $n \in \mathbb{Z}$   $k \in \mathbb{Z}$  and  $m - n \leq m - k$ 
shows  $k \leq n$ 
using assms Int_ZF_2_T1 group3.OrderedGroup_ZF_1_L5AF
by simp

```

If an integer is nonpositive, then its opposite is nonnegative.

```

lemma (in int0) Int_ZF_2_L10A: assumes  $k \leq 0$ 
shows  $0 \leq (-k)$ 
using assms Int_ZF_2_T1 group3.OrderedGroup_ZF_1_L5A by simp

```

If the opposite of an integers is nonnegative, then the integer is nonpositive.

```

lemma (in int0) Int_ZF_2_L10B:
assumes  $k \in \mathbb{Z}$  and  $0 \leq (-k)$ 
shows  $k \leq 0$ 
using assms Int_ZF_2_T1 group3.OrderedGroup_ZF_1_L5AA by simp

```

Adding one to an integer corresponds to taking a successor for a natural number.

```

lemma (in int0) Int_ZF_2_L11:
shows  $i \ \$+ \ \$\# \ n \ \$+ \ (\$ \# \ 1) = i \ \$+ \ \$\# \ succ(n)$ 
proof -
have  $\$ \# \ succ(n) = \$ \# \ 1 \ \$+ \ \$\# \ n$  using int_succ_int_1 by blast
then have  $i \ \$+ \ \$\# \ succ(n) = i \ \$+ \ (\$ \# \ n \ \$+ \ \$ \# \ 1)$ 
using zadd_commute by simp
then show thesis using zadd_assoc by simp
qed

```

Adding a natural number increases integers.

```

lemma (in int0) Int_ZF_2_L12: assumes A1:  $i \in \mathbb{Z}$  and A2:  $n \in \text{nat}$ 
shows  $i \leq i \ \$+ \ \$\# \ n$ 
proof -
{ assume  $n = 0$ 
with A1 have  $i \leq i \ \$+ \ \$\# \ n$  using zadd_int0 int_ord_is_refl refl_def
by simp }

```

```

moreover
{ assume n≠0
  with A2 obtain k where k∈nat n = succ(k)
    using Nat_ZF_1_L3 by auto
  with A1 have i ≤ i $+ $#n
    using zless_succ_zadd zless_imp_zle Int_ZF_2_L1 by simp }
ultimately show thesis by blast
qed

```

Adding one increases integers.

```

lemma (in int0) Int_ZF_2_L12A: assumes A1: j≤k
  shows j ≤ k $+ $#1  j ≤ k+1
proof -
  from A1 have T1:j∈ℤ k∈ℤ j ≤ k
    using Int_ZF_2_L1A by auto
  moreover from T1 have k ≤ k $+ $#1 using Int_ZF_2_L12 Int_ZF_2_L1A
    by simp
  ultimately have j ≤ k $+ $#1 using zle_trans by fast
  with T1 show j ≤ k $+ $#1 using Int_ZF_2_L1 by simp
  with T1 have j ≤ k+$#1
    using Int_ZF_1_L2 by simp
  then show j ≤ k+1 using Int_ZF_1_L8 by simp
qed

```

Adding one increases integers, yet one more version.

```

lemma (in int0) Int_ZF_2_L12B: assumes A1: m∈ℤ shows m ≤ m+1
  using assms int_ord_is_refl refl_def Int_ZF_2_L12A by simp

```

If  $k + 1 = m + n$ , where  $n$  is a non-zero natural number, then  $m \leq k$ .

```

lemma (in int0) Int_ZF_2_L13:
  assumes A1: k∈ℤ m∈ℤ and A2: n∈nat
  and A3: k $+ ($# 1) = m $+ $# succ(n)
  shows m ≤ k
proof -
  from A1 have k∈ℤ m $+ $# n ∈ ℤ by auto
  moreover from assms have k $+ $# 1 = m $+ $# n $+ $#1
    using Int_ZF_2_L11 by simp
  ultimately have k = m $+ $# n using zadd_right_cancel by simp
  with A1 A2 show thesis using Int_ZF_2_L12 by simp
qed

```

The absolute value of an integer is an integer.

```

lemma (in int0) Int_ZF_2_L14: assumes A1: m∈ℤ
  shows abs(m) ∈ ℤ
proof -
  have AbsoluteValue(ℤ,IntegerAddition,IntegerOrder) : ℤ→ℤ
    using Int_ZF_2_T1 group3.OrderedGroup_ZF_3_L1 by simp
  with A1 show thesis using apply_funtype by simp

```

qed

If two integers are nonnegative, then the opposite of one is less or equal than the other and the sum is also nonnegative.

```
lemma (in int0) Int_ZF_2_L14A:
  assumes  $0 \leq m$   $0 \leq n$ 
  shows
     $(-m) \leq n$ 
     $0 \leq m + n$ 
  using assms Int_ZF_2_T1
    group3.OrderedGroup_ZF_1_L5AC group3.OrderedGroup_ZF_1_L12
  by auto
```

We can increase components in an estimate.

```
lemma (in int0) Int_ZF_2_L15:
  assumes  $b \leq b_1$   $c \leq c_1$  and  $a \leq b+c$ 
  shows  $a \leq b_1+c_1$ 
proof -
  from assms have group3( $\mathbb{Z}$ , IntegerAddition, IntegerOrder)
     $\langle a, \text{IntegerAddition}(b, c) \rangle \in \text{IntegerOrder}$ 
     $\langle b, b_1 \rangle \in \text{IntegerOrder}$   $\langle c, c_1 \rangle \in \text{IntegerOrder}$ 
  using Int_ZF_2_T1 by auto
  then have  $\langle a, \text{IntegerAddition}(b_1, c_1) \rangle \in \text{IntegerOrder}$ 
    by (rule group3.OrderedGroup_ZF_1_L5E)
  thus thesis by simp
qed
```

We can add or subtract the sides of two inequalities.

```
lemma (in int0) int_ineq_add_sides:
  assumes  $a \leq b$  and  $c \leq d$ 
  shows
     $a+c \leq b+d$ 
     $a-d \leq b-c$ 
  using assms Int_ZF_2_T1
    group3.OrderedGroup_ZF_1_L5B group3.OrderedGroup_ZF_1_L5I
  by auto
```

We can increase the second component in an estimate.

```
lemma (in int0) Int_ZF_2_L15A:
  assumes  $b \in \mathbb{Z}$  and  $a \leq b+c$  and A3:  $c \leq c_1$ 
  shows  $a \leq b+c_1$ 
proof -
  from assms have
    group3( $\mathbb{Z}$ , IntegerAddition, IntegerOrder)
     $b \in \mathbb{Z}$ 
     $\langle a, \text{IntegerAddition}(b, c) \rangle \in \text{IntegerOrder}$ 
     $\langle c, c_1 \rangle \in \text{IntegerOrder}$ 
  using Int_ZF_2_T1 by auto
```



```

    then have ⟨a,IntegerAddition( b,c₁)⟩ ∈ IntegerOrder
      by (rule group3.OrderedGroup_ZF_1_L5D)
    thus thesis by simp
qed

```

If we increase the second component in a sum of three integers, the whole sum inceases.

```

lemma (in int0) Int_ZF_2_L15C:
  assumes A1:  $m \in \mathbb{Z}$   $n \in \mathbb{Z}$  and A2:  $k \leq L$ 
  shows  $m+k+n \leq m+L+n$ 
proof -
  let P = IntegerAddition
  from assms have
    group3(int,P,IntegerOrder)
     $m \in \text{int}$   $n \in \text{int}$ 
     $\langle k,L \rangle \in \text{IntegerOrder}$ 
  using Int_ZF_2_T1 by auto
  then have ⟨P⟨P⟨ m,k⟩,n⟩, P⟨P⟨ m,L⟩,n⟩⟩ ∈ IntegerOrder
    by (rule group3.OrderedGroup_ZF_1_L10)
  then show  $m+k+n \leq m+L+n$  by simp
qed

```

We don't decrease an integer by adding a nonnegative one.

```

lemma (in int0) Int_ZF_2_L15D:
  assumes  $0 \leq n$   $m \in \mathbb{Z}$ 
  shows  $m \leq n+m$ 
  using assms Int_ZF_2_T1 group3.OrderedGroup_ZF_1_L5F
  by simp

```

Some inequalities about the sum of two integers and its absolute value.

```

lemma (in int0) Int_ZF_2_L15E:
  assumes  $m \in \mathbb{Z}$   $n \in \mathbb{Z}$ 
  shows
     $m+n \leq \text{abs}(m)+\text{abs}(n)$ 
     $m-n \leq \text{abs}(m)+\text{abs}(n)$ 
     $(-m)+n \leq \text{abs}(m)+\text{abs}(n)$ 
     $(-m)-n \leq \text{abs}(m)+\text{abs}(n)$ 
  using assms Int_ZF_2_T1 group3.OrderedGroup_ZF_3_L6A
  by auto

```

We can add a nonnegative integer to the right hand side of an inequality.

```

lemma (in int0) Int_ZF_2_L15F:  assumes  $m \leq k$  and  $0 \leq n$ 
  shows  $m \leq k+n$   $m \leq n+k$ 
  using assms Int_ZF_2_T1 group3.OrderedGroup_ZF_1_L5G
  by auto

```

Triangle inequality for integers.

```

lemma (in int0) Int_triangle_ineq:

```

```

assumes  $m \in \mathbb{Z}$   $n \in \mathbb{Z}$ 
shows  $\text{abs}(m+n) \leq \text{abs}(m) + \text{abs}(n)$ 
using assms Int_ZF_1_T2 Int_ZF_2_T1 group3.OrdGroup_triangle_ineq
by simp

```

Taking absolute value does not change nonnegative integers.

```

lemma (in int0) Int_ZF_2_L16:
  assumes  $0 \leq m$  shows  $m \in \mathbb{Z}^+$  and  $\text{abs}(m) = m$ 
  using assms Int_ZF_2_T1 group3.OrderedGroup_ZF_1_L2
    group3.OrderedGroup_ZF_3_L2 by auto

```

$0 \leq 1$ , so  $|1| = 1$ .

```

lemma (in int0) Int_ZF_2_L16A: shows  $0 \leq 1$  and  $\text{abs}(1) = 1$ 
proof -
  have  $(\# 0) \in \mathbb{Z}$   $(\# 1) \in \mathbb{Z}$  by auto
  then have  $0 \leq 0$  and T1:  $1 \in \mathbb{Z}$ 
    using Int_ZF_1_L8 int_ord_is_refl refl_def by auto
  then have  $0 \leq 0+1$  using Int_ZF_2_L12A by simp
  with T1 show  $0 \leq 1$  using Int_ZF_1_T2 group0.group0_2_L2
    by simp
  then show  $\text{abs}(1) = 1$  using Int_ZF_2_L16 by simp
qed

```

$1 \leq 2$ .

```

lemma (in int0) Int_ZF_2_L16B: shows  $1 \leq 2$ 
proof -
  have  $(\# 1) \in \mathbb{Z}$  by simp
  then show  $1 \leq 2$ 
    using Int_ZF_1_L8 int_ord_is_refl refl_def Int_ZF_2_L12A
    by simp
qed

```

Integers greater or equal one are greater or equal zero.

```

lemma (in int0) Int_ZF_2_L16C:
  assumes A1:  $1 \leq a$  shows
     $0 \leq a$   $a \neq 0$ 
     $2 \leq a+1$ 
     $1 \leq a+1$ 
     $0 \leq a+1$ 
proof -
  from A1 have  $0 \leq 1$  and  $1 \leq a$ 
    using Int_ZF_2_L16A by auto
  then show  $0 \leq a$  by (rule Int_order_transitive)
  have I:  $0 \leq 1$  using Int_ZF_2_L16A by simp
  have  $1 \leq 2$  using Int_ZF_2_L16B by simp
  moreover from A1 show  $2 \leq a+1$ 
    using Int_ZF_1_L8A int_ord_transl_inv by simp
  ultimately show  $1 \leq a+1$  by (rule Int_order_transitive)

```

```

with I show  $0 \leq a+1$  by (rule Int_order_transitive)
from A1 show  $a \neq 0$  using
  Int_ZF_2_L16A Int_ZF_2_L3 int_zero_not_one by auto
qed

```

Absolute value is the same for an integer and its opposite.

```

lemma (in int0) Int_ZF_2_L17:
  assumes  $m \in \mathbb{Z}$  shows  $\text{abs}(-m) = \text{abs}(m)$ 
  using assms Int_ZF_2_T1 group3.OrderedGroup_ZF_3_L7A by simp

```

The absolute value of zero is zero.

```

lemma (in int0) Int_ZF_2_L18: shows  $\text{abs}(0) = 0$ 
  using Int_ZF_2_T1 group3.OrderedGroup_ZF_3_L2A by simp

```

A different version of the triangle inequality.

```

lemma (in int0) Int_triangle_ineq1:
  assumes A1:  $m \in \mathbb{Z} \quad n \in \mathbb{Z}$ 
  shows
     $\text{abs}(m-n) \leq \text{abs}(n)+\text{abs}(m)$ 
     $\text{abs}(m-n) \leq \text{abs}(m)+\text{abs}(n)$ 
proof -
  have  $-n \in \mathbb{Z}$  by simp
  with A1 have  $\text{abs}(m-n) \leq \text{abs}(m)+\text{abs}(-n)$ 
    using Int_ZF_1_L9A Int_triangle_ineq by simp
  with A1 show
     $\text{abs}(m-n) \leq \text{abs}(n)+\text{abs}(m)$ 
     $\text{abs}(m-n) \leq \text{abs}(m)+\text{abs}(n)$ 
    using Int_ZF_2_L17 Int_ZF_2_L14 Int_ZF_1_T2 IsCommutative_def
    by auto
qed

```

Another version of the triangle inequality.

```

lemma (in int0) Int_triangle_ineq2:
  assumes  $m \in \mathbb{Z} \quad n \in \mathbb{Z}$ 
  and  $\text{abs}(m-n) \leq k$ 
  shows
     $\text{abs}(m) \leq \text{abs}(n)+k$ 
     $m-k \leq n$ 
     $m \leq n+k$ 
     $n-k \leq m$ 
  using assms Int_ZF_1_T2 Int_ZF_2_T1
    group3.OrderedGroup_ZF_3_L7D group3.OrderedGroup_ZF_3_L7E
  by auto

```

Triangle inequality with three integers. We could use `OrdGroup_triangle_ineq3`, but since `simp` cannot translate the notation directly, it is simpler to reprove it for integers.

```

lemma (in int0) Int_triangle_ineq3:

```

```

    assumes A1:  $m \in \mathbb{Z}$   $n \in \mathbb{Z}$   $k \in \mathbb{Z}$ 
    shows  $\text{abs}(m+n+k) \leq \text{abs}(m) + \text{abs}(n) + \text{abs}(k)$ 
  proof -
    from A1 have T:  $m+n \in \mathbb{Z}$   $\text{abs}(k) \in \mathbb{Z}$ 
      using Int_ZF_1_T2 group0.group_op_closed Int_ZF_2_L14
      by auto
    with A1 have  $\text{abs}(m+n+k) \leq \text{abs}(m+n) + \text{abs}(k)$ 
      using Int_triangle_ineq by simp
    moreover from A1 T have
       $\text{abs}(m+n) + \text{abs}(k) \leq \text{abs}(m) + \text{abs}(n) + \text{abs}(k)$ 
      using Int_triangle_ineq int_ord_transl_inv by simp
    ultimately show thesis by (rule Int_order_transitive)
  qed

```

The next lemma shows what happens when one integers is not greater or equal than another.

```

lemma (in int0) Int_ZF_2_L19:
  assumes A1:  $m \in \mathbb{Z}$   $n \in \mathbb{Z}$  and A2:  $\neg(n \leq m)$ 
  shows  $m \leq n \implies (-n) \leq (-m)$   $m \neq n$ 
proof -
  from A1 A2 show  $m \leq n$  using Int_ZF_2_T1 IsTotal_def
    by auto
  then show  $(-n) \leq (-m)$  using Int_ZF_2_L10
    by simp
  from A1 have  $n \leq n$  using int_ord_is_refl refl_def
    by simp
  with A2 show  $m \neq n$  by auto
qed

```

If one integer is greater or equal and not equal to another, then it is not smaller or equal.

```

lemma (in int0) Int_ZF_2_L19AA: assumes A1:  $m \leq n$  and A2:  $m \neq n$ 
  shows  $\neg(n \leq m)$ 
proof -
  from A1 A2 have
     $\text{group3}(\mathbb{Z}, \text{IntegerAddition}, \text{IntegerOrder})$ 
     $\langle m, n \rangle \in \text{IntegerOrder}$ 
     $m \neq n$ 
    using Int_ZF_2_T1 by auto
  then have  $\langle n, m \rangle \notin \text{IntegerOrder}$ 
    by (rule group3.OrderedGroup_ZF_1_L8AA)
  thus  $\neg(n \leq m)$  by simp
qed

```

The next lemma allows to prove theorems for the case of positive and negative integers separately.

```

lemma (in int0) Int_ZF_2_L19A: assumes A1:  $m \in \mathbb{Z}$  and A2:  $\neg(0 \leq m)$ 
  shows  $m \leq 0$   $0 \leq (-m)$   $m \neq 0$ 

```

```

proof -
  from A1 have T:  $0 \in \mathbb{Z}$ 
    using Int_ZF_1_T2 group0.group0_2_L2 by auto
  with A1 A2 show  $m \leq 0$  using Int_ZF_2_L19 by blast
  from A1 T A2 show  $m \neq 0$  by (rule Int_ZF_2_L19)
  from A1 T A2 have  $(-0) \leq (-m)$  by (rule Int_ZF_2_L19)
  then show  $0 \leq (-m)$ 
    using Int_ZF_1_T2 group0.group_inv_of_one by simp
qed

```

We can prove a theorem about integers by proving that it holds for  $m = 0$ ,  $m \in \mathbb{Z}_+$  and  $-m \in \mathbb{Z}_+$ .

```

lemma (in int0) Int_ZF_2_L19B:
  assumes  $m \in \mathbb{Z}$  and  $Q(0)$  and  $\forall n \in \mathbb{Z}_+. Q(n)$  and  $\forall n \in \mathbb{Z}_+. Q(-n)$ 
  shows  $Q(m)$ 
proof -
  let  $G = \mathbb{Z}$ 
  let  $P = \text{IntegerAddition}$ 
  let  $r = \text{IntegerOrder}$ 
  let  $b = m$ 
  from assms have
    group3( $G, P, r$ )
     $r \text{ \{is total on\} } G$ 
     $b \in G$ 
     $Q(\text{TheNeutralElement}(G, P))$ 
     $\forall a \in \text{PositiveSet}(G, P, r). Q(a)$ 
     $\forall a \in \text{PositiveSet}(G, P, r). Q(\text{GroupInv}(G, P)(a))$ 
    using Int_ZF_2_T1 by auto
  then show  $Q(b)$  by (rule group3.OrderedGroup_ZF_1_L18)
qed

```

An integer is not greater than its absolute value.

```

lemma (in int0) Int_ZF_2_L19C: assumes A1:  $m \in \mathbb{Z}$ 
  shows
     $m \leq \text{abs}(m)$ 
     $(-m) \leq \text{abs}(m)$ 
  using assms Int_ZF_2_T1
    group3.OrderedGroup_ZF_3_L5 group3.OrderedGroup_ZF_3_L6
  by auto

```

$$|m - n| = |n - m|.$$

```

lemma (in int0) Int_ZF_2_L20: assumes  $m \in \mathbb{Z}$   $n \in \mathbb{Z}$ 
  shows  $\text{abs}(m - n) = \text{abs}(n - m)$ 
  using assms Int_ZF_2_T1 group3.OrderedGroup_ZF_3_L7B by simp

```

We can add the sides of inequalities with absolute values.

```

lemma (in int0) Int_ZF_2_L21:
  assumes A1:  $m \in \mathbb{Z}$   $n \in \mathbb{Z}$ 

```

```

and A2: abs(m) ≤ k abs(n) ≤ 1
shows
abs(m+n) ≤ k + 1
abs(m-n) ≤ k + 1
using assms Int_ZF_1_T2 Int_ZF_2_T1
group3.OrderedGroup_ZF_3_L7C group3.OrderedGroup_ZF_3_L7CA
by auto

```

Absolute value is nonnegative.

```

lemma (in int0) int_abs_nonneg: assumes A1: m ∈ ℤ
shows abs(m) ∈ ℤ+ 0 ≤ abs(m)
proof -
have AbsoluteValue(ℤ,IntegerAddition,IntegerOrder) : ℤ → ℤ+
using Int_ZF_2_T1 group3.OrderedGroup_ZF_3_L3C by simp
with A1 show abs(m) ∈ ℤ+ using apply_funtype
by simp
then show 0 ≤ abs(m)
using Int_ZF_2_T1 group3.OrderedGroup_ZF_1_L2 by simp
qed

```

If an nonnegative integer is less or equal than another, then so is its absolute value.

```

lemma (in int0) Int_ZF_2_L23:
assumes 0 ≤ m m ≤ k
shows abs(m) ≤ k
using assms Int_ZF_2_L16 by simp

```

### 34.3 Induction on integers.

In this section we show some induction lemmas for integers. The basic tools are the induction on natural numbers and the fact that integers can be written as a sum of a smaller integer and a natural number.

An integer can be written as a sum of a smaller integer and a natural number.

```

lemma (in int0) Int_ZF_3_L2: assumes A1: i ≤ m
shows ∃ n ∈ nat. m = i + n
proof -
let n = 0
{ assume A2: i = m
from A1 A2 have n ∈ nat m = i + n
using Int_ZF_2_L1A zadd_int0_right by auto
hence ∃ n ∈ nat. m = i + n by blast }
moreover
{ assume A3: i ≠ m
with A1 have i < m i ∈ ℤ m ∈ ℤ
using Int_ZF_2_L9 Int_ZF_2_L1A by auto
then obtain k where D1: k ∈ nat m = i + succ(k)
using zless_imp_succ_zadd_lemma by auto
}

```

```

    let n = succ(k)
    from D1 have n∈nat m = i $+ $# n by auto
    hence ∃n∈nat. m = i $+ $# n by simp }
  ultimately show thesis by blast
qed

```

Induction for integers, the induction step.

```

lemma (in int0) Int_ZF_3_L6: assumes A1: i∈ℤ
  and A2: ∀m. i≤m ∧ Q(m) ⟶ Q(m $+ ($# 1))
  shows ∀k∈nat. Q(i $+ ($# k)) ⟶ Q(i $+ ($# succ(k)))
proof
  fix k assume A3: k∈nat show Q(i $+ $# k) ⟶ Q(i $+ $# succ(k))
  proof
    assume A4: Q(i $+ $# k)
    from A1 A3 have i≤ i $+ ($# k) using Int_ZF_2_L12
    by simp
    with A4 A2 have Q(i $+ ($# k) $+ ($# 1)) by simp
    then show Q(i $+ ($# succ(k))) using Int_ZF_2_L11 by simp
  qed
qed

```

Induction on integers, version with higher-order increment function.

```

lemma (in int0) Int_ZF_3_L7:
  assumes A1: i≤k and A2: Q(i)
  and A3: ∀m. i≤m ∧ Q(m) ⟶ Q(m $+ ($# 1))
  shows Q(k)
proof -
  from A1 obtain n where D1: n∈nat and D2: k = i $+ $# n
  using Int_ZF_3_L2 by auto
  from A1 have T1: i∈ℤ using Int_ZF_2_L1A by simp
  note 'n∈nat'
  moreover from A1 A2 have Q(i $+ $#0)
  using Int_ZF_2_L1A zadd_int0 by simp
  moreover from T1 A3 have
    ∀k∈nat. Q(i $+ ($# k)) ⟶ Q(i $+ ($# succ(k)))
  by (rule Int_ZF_3_L6)
  ultimately have Q(i $+ ($# n)) by (rule ind_on_nat)
  with D2 show Q(k) by simp
qed

```

Induction on integer, implication between two forms of the induction step.

```

lemma (in int0) Int_ZF_3_L7A: assumes
  A1: ∀m. i≤m ∧ Q(m) ⟶ Q(m+1)
  shows ∀m. i≤m ∧ Q(m) ⟶ Q(m $+ ($# 1))
proof -
  { fix m assume i≤m ∧ Q(m)
    with A1 have T1: m∈ℤ Q(m+1) using Int_ZF_2_L1A by auto
    then have m+1 = m+($# 1) using Int_ZF_1_L8 by simp
    with T1 have Q(m $+ ($# 1)) using Int_ZF_1_L2

```

```

    by simp
  } then show thesis by simp
qed

```

Induction on integers, version with ZF increment function.

```

theorem (in int0) Induction_on_int:
  assumes A1:  $i \leq k$  and A2:  $Q(i)$ 
  and A3:  $\forall m. i \leq m \wedge Q(m) \longrightarrow Q(m+1)$ 
  shows  $Q(k)$ 
proof -
  from A3 have  $\forall m. i \leq m \wedge Q(m) \longrightarrow Q(m \$+ (\$ \# 1))$ 
  by (rule Int_ZF_3_L7A)
  with A1 A2 show thesis by (rule Int_ZF_3_L7)
qed

```

Another form of induction on integers. This rewrites the basic theorem Int\_ZF\_3\_L7 substituting  $P(-k)$  for  $Q(k)$ .

```

lemma (in int0) Int_ZF_3_L7B: assumes A1:  $i \leq k$  and A2:  $P(\$-i)$ 
  and A3:  $\forall m. i \leq m \wedge P(\$-m) \longrightarrow P(\$-(m \$+ (\$ \# 1)))$ 
  shows  $P(\$-k)$ 
proof -
  from A1 A2 A3 show  $P(\$-k)$  by (rule Int_ZF_3_L7)
qed

```

Another induction on integers. This rewrites Int\_ZF\_3\_L7 substituting  $-k$  for  $k$  and  $-i$  for  $i$ .

```

lemma (in int0) Int_ZF_3_L8: assumes A1:  $k \leq i$  and A2:  $P(i)$ 
  and A3:  $\forall m. \$-i \leq m \wedge P(\$-m) \longrightarrow P(\$-(m \$+ (\$ \# 1)))$ 
  shows  $P(k)$ 
proof -
  from A1 have  $T1: \$-i \leq \$-k$  using Int_ZF_2_L10 by simp
  from A1 A2 have  $T2: P(\$- \$- i)$  using Int_ZF_2_L1A zminus_zminus
  by simp
  from T1 T2 A3 have  $P(\$-(\$-k))$  by (rule Int_ZF_3_L7)
  with A1 show  $P(k)$  using Int_ZF_2_L1A zminus_zminus by simp
qed

```

An implication between two forms of induction steps.

```

lemma (in int0) Int_ZF_3_L9: assumes A1:  $i \in \mathbb{Z}$ 
  and A2:  $\forall n. n \leq i \wedge P(n) \longrightarrow P(n \$+ \$- (\$ \# 1))$ 
  shows  $\forall m. \$-i \leq m \wedge P(\$-m) \longrightarrow P(\$-(m \$+ (\$ \# 1)))$ 
proof
  fix m show  $\$-i \leq m \wedge P(\$-m) \longrightarrow P(\$-(m \$+ (\$ \# 1)))$ 
  proof
    assume A3:  $\$-i \leq m \wedge P(\$-m)$ 
    then have  $\$-i \leq m$  by simp
    then have  $\$-m \leq \$- (\$- i)$  by (rule Int_ZF_2_L10)
    with A1 A2 A3 show  $P(\$-(m \$+ (\$ \# 1)))$ 

```



```

      using zminus_zminus zminus_zadd_distrib by simp
    qed
  qed

```

Backwards induction on integers, version with higher-order decrement function.

```

lemma (in int0) Int_ZF_3_L9A: assumes A1:  $k \leq i$  and A2:  $P(i)$ 
  and A3:  $\forall n. n \leq i \wedge P(n) \longrightarrow P(n \ \$+ \ \$-(\#1))$ 
  shows  $P(k)$ 
proof -
  from A1 have T1:  $i \in \mathbb{Z}$  using Int_ZF_2_L1A by simp
  from T1 A3 have T2:  $\forall m. \ \$-i \leq m \wedge P(\$-m) \longrightarrow P(\$-(m \ \$+ (\# \ 1)))$ 
    by (rule Int_ZF_3_L9)
  from A1 A2 T2 show  $P(k)$  by (rule Int_ZF_3_L8)
qed

```

Induction on integers, implication between two forms of the induction step.

```

lemma (in int0) Int_ZF_3_L10: assumes
  A1:  $\forall n. n \leq i \wedge P(n) \longrightarrow P(n-1)$ 
  shows  $\forall n. n \leq i \wedge P(n) \longrightarrow P(n \ \$+ \ \$-(\#1))$ 
proof -
  { fix n assume  $n \leq i \wedge P(n)$ 
    with A1 have T1:  $n \in \mathbb{Z} \ P(n-1)$  using Int_ZF_2_L1A by auto
    then have  $n-1 = n - (\# \ 1)$  using Int_ZF_1_L8 by simp
    with T1 have  $P(n \ \$+ \ \$-(\#1))$  using Int_ZF_1_L10 by simp
  } then show thesis by simp
qed

```

Backwards induction on integers.

```

theorem (in int0) Back_induct_on_int:
  assumes A1:  $k \leq i$  and A2:  $P(i)$ 
  and A3:  $\forall n. n \leq i \wedge P(n) \longrightarrow P(n-1)$ 
  shows  $P(k)$ 
proof -
  from A3 have  $\forall n. n \leq i \wedge P(n) \longrightarrow P(n \ \$+ \ \$-(\#1))$ 
    by (rule Int_ZF_3_L10)
  with A1 A2 show  $P(k)$  by (rule Int_ZF_3_L9A)
qed

```

### 34.4 Bounded vs. finite subsets of integers

The goal of this section is to establish that a subset of integers is bounded is and only if it is finite. The fact that all finite sets are bounded is already shown for all linearly ordered groups in `OrderedGroups_ZF.thy`. To show the other implication we show that all intervals starting at 0 are finite and then use a result from `OrderedGroups_ZF.thy`.

There are no integers between  $k$  and  $k + 1$ .

```

lemma (in int0) Int_ZF_4_L1:
  assumes A1:  $k \in \mathbb{Z}$   $m \in \mathbb{Z}$   $n \in \text{nat}$  and A2:  $k + \#1 = m + \#n$ 
  shows  $m = k + \#1 \vee m \leq k$ 
proof -
  { assume n=0
    with A1 A2 have  $m = k + \#1 \vee m \leq k$ 
    using zadd_int0 by simp }
  moreover
  { assume n $\neq$ 0
    with A1 obtain j where D1:  $j \in \text{nat}$   $n = \text{succ}(j)$ 
    using Nat_ZF_1_L3 by auto
    with A1 A2 D1 have  $m = k + \#1 \vee m \leq k$ 
    using Int_ZF_2_L13 by simp }
  ultimately show thesis by blast
qed

```

A trivial calculation lemma that allows to subtract and add one.

```

lemma Int_ZF_4_L1A:
  assumes  $m \in \text{int}$  shows  $m - \#1 + \#1 = m$ 
  using assms eq_zdiff_iff by auto

```

There are no integers between  $k$  and  $k + 1$ , another formulation.

```

lemma (in int0) Int_ZF_4_L1B: assumes A1:  $m \leq L$ 
  shows
     $m = L \vee m + 1 \leq L$ 
     $m = L \vee m \leq L - 1$ 
proof -
  let  $k = L - \#1$ 
  from A1 have T1:  $m \in \mathbb{Z}$   $L \in \mathbb{Z}$   $L = k + \#1$ 
  using Int_ZF_2_L1A Int_ZF_4_L1A by auto
  moreover from A1 obtain n where D1:  $n \in \text{nat}$   $L = m + \#n$ 
  using Int_ZF_3_L2 by auto
  ultimately have  $m = L \vee m \leq k$ 
  using Int_ZF_4_L1 by simp
  with T1 show  $m = L \vee m + 1 \leq L$ 
  using Int_ZF_2_L9A by auto
  with T1 show  $m = L \vee m \leq L - 1$ 
  using Int_ZF_1_L8A Int_ZF_2_L9B by simp
qed

```

If  $j \in m..k + 1$ , then  $j \in m..n$  or  $j = k + 1$ .

```

lemma (in int0) Int_ZF_4_L2: assumes A1:  $k \in \mathbb{Z}$ 
  and A2:  $j \in m..(k + \#1)$ 
  shows  $j \in m..k \vee j \in \{k + \#1\}$ 
proof -
  from A2 have T1:  $m \leq j \leq (k + \#1)$  using Order_ZF_2_L1A
  by auto
  then have T2:  $m \in \mathbb{Z}$   $j \in \mathbb{Z}$  using Int_ZF_2_L1A by auto
  from T1 obtain n where  $n \in \text{nat}$   $k + \#1 = j + \#n$ 

```

```

    using Int_ZF_3_L2 by auto
  with A1 T1 T2 have (m ≤ j ∧ j ≤ k) ∨ j ∈ {k $+ $#1}
    using Int_ZF_4_L1 by auto
  then show thesis using Order_ZF_2_L1B by auto
qed

```

Extending an integer interval by one is the same as adding the new endpoint.

```

lemma (in int0) Int_ZF_4_L3: assumes A1: m ≤ k
  shows m..(k $+ $#1) = m..k ∪ {k $+ $#1}
proof
  from A1 have T1: m ∈ ℤ k ∈ ℤ using Int_ZF_2_L1A by auto
  then show m..(k $+ $#1) ⊆ m..k ∪ {k $+ $#1}
    using Int_ZF_4_L2 by auto
  from T1 have m ≤ m using Int_ZF_2_T1 group3.OrderedGroup_ZF_1_L3
    by simp
  with T1 A1 have m..k ⊆ m..(k $+ $#1)
    using Int_ZF_2_L12 Int_ZF_2_L6 Order_ZF_2_L3 by simp
  with T1 A1 show m..k ∪ {k $+ $#1} ⊆ m..(k $+ $#1)
    using Int_ZF_2_L12A int_ord_is_refl Order_ZF_2_L2 by auto
qed

```

Integer intervals are finite - induction step.

```

lemma (in int0) Int_ZF_4_L4:
  assumes A1: i ≤ m and A2: i..m ∈ Fin(ℤ)
  shows i..(m $+ $#1) ∈ Fin(ℤ)
  using assms Int_ZF_4_L3 by simp

```

Integer intervals are finite.

```

lemma (in int0) Int_ZF_4_L5: assumes A1: i ∈ ℤ k ∈ ℤ
  shows i..k ∈ Fin(ℤ)
proof -
  { assume A2: i ≤ k
    moreover from A1 have i..i ∈ Fin(ℤ)
      using int_ord_is_refl Int_ZF_2_L4 Order_ZF_2_L4 by simp
    moreover from A2 have
      ∀m. i ≤ m ∧ i..m ∈ Fin(ℤ) ⟶ i..(m $+ $#1) ∈ Fin(ℤ)
      using Int_ZF_4_L4 by simp
    ultimately have i..k ∈ Fin(ℤ) by (rule Int_ZF_3_L7) }
  moreover
  { assume ¬ i ≤ k
    then have i..k ∈ Fin(ℤ) using Int_ZF_2_L6 Order_ZF_2_L5
      by simp }
  ultimately show thesis by blast
qed

```

Bounded integer sets are finite.

```

lemma (in int0) Int_ZF_4_L6: assumes A1: IsBounded(A,IntegerOrder)
  shows A ∈ Fin(ℤ)

```

```

proof -
  have T1:  $\forall m \in \text{Nonnegative}(\mathbb{Z}, \text{IntegerAddition}, \text{IntegerOrder}).$ 
     $\#0..m \in \text{Fin}(\mathbb{Z})$ 
  proof
    fix m assume m  $\in \text{Nonnegative}(\mathbb{Z}, \text{IntegerAddition}, \text{IntegerOrder})$ 
    then have  $m \in \mathbb{Z}$  using Int_ZF_2_T1 group3.OrderedGroup_ZF_1_L4E
    by auto
    then show  $\#0..m \in \text{Fin}(\mathbb{Z})$  using Int_ZF_4_L5 by simp
  qed
  have group3( $\mathbb{Z}$ , IntegerAddition, IntegerOrder)
    using Int_ZF_2_T1 by simp
  moreover from T1 have  $\forall m \in \text{Nonnegative}(\mathbb{Z}, \text{IntegerAddition}, \text{IntegerOrder}).$ 
    Interval(IntegerOrder, TheNeutralElement( $\mathbb{Z}$ , IntegerAddition), m)
     $\in \text{Fin}(\mathbb{Z})$  using Int_ZF_1_L8 by simp
  moreover note A1
  ultimately show  $A \in \text{Fin}(\mathbb{Z})$  by (rule group3.OrderedGroup_ZF_2_T1)
qed

```

A subset of integers is bounded iff it is finite.

```

theorem (in int0) Int_bounded_iff_fin:
  shows IsBounded(A, IntegerOrder)  $\longleftrightarrow$   $A \in \text{Fin}(\mathbb{Z})$ 
  using Int_ZF_4_L6 Int_ZF_2_T1 group3.ord_group_fin_bounded
  by blast

```

The image of an interval by any integer function is finite, hence bounded.

```

lemma (in int0) Int_ZF_4_L8:
  assumes A1:  $i \in \mathbb{Z} \quad k \in \mathbb{Z}$  and A2:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$ 
  shows
     $f(i..k) \in \text{Fin}(\mathbb{Z})$ 
    IsBounded( $f(i..k)$ , IntegerOrder)
  using assms Int_ZF_4_L5 Finite1_L6A Int_bounded_iff_fin
  by auto

```

If for every integer we can find one in  $A$  that is greater or equal, then  $A$  is not bounded above, hence infinite.

```

lemma (in int0) Int_ZF_4_L9: assumes A1:  $\forall m \in \mathbb{Z}. \exists k \in A. m \leq k$ 
  shows
     $\neg \text{IsBoundedAbove}(A, \text{IntegerOrder})$ 
     $A \notin \text{Fin}(\mathbb{Z})$ 
  proof -
    have  $\mathbb{Z} \neq \{0\}$ 
      using Int_ZF_1_L8A int_zero_not_one by blast
    with A1 show
       $\neg \text{IsBoundedAbove}(A, \text{IntegerOrder})$ 
       $A \notin \text{Fin}(\mathbb{Z})$ 
      using Int_ZF_2_T1 group3.OrderedGroup_ZF_2_L2A
      by auto
  qed

```

end

## 35 Int\_ZF\_1.thy

```
theory Int_ZF_1 imports Int_ZF_IML OrderedRing_ZF
```

```
begin
```

This theory file considers the set of integers as an ordered ring.

### 35.1 Integers as a ring

In this section we show that integers form a commutative ring.

The next lemma provides the condition to show that addition is distributive with respect to multiplication.

```
lemma (in int0) Int_ZF_1_1_L1: assumes A1:  $a \in \mathbb{Z}$   $b \in \mathbb{Z}$   $c \in \mathbb{Z}$ 
  shows
     $a \cdot (b+c) = a \cdot b + a \cdot c$ 
     $(b+c) \cdot a = b \cdot a + c \cdot a$ 
  using assms Int_ZF_1_L2 zadd_zmult_distrib zadd_zmult_distrib2
  by auto
```

Integers form a commutative ring, hence we can use theorems proven in ring0 context (locale).

```
lemma (in int0) Int_ZF_1_1_L2: shows
  IsAring( $\mathbb{Z}$ , IntegerAddition, IntegerMultiplication)
  IntegerMultiplication {is commutative on}  $\mathbb{Z}$ 
  ring0( $\mathbb{Z}$ , IntegerAddition, IntegerMultiplication)
proof -
  have  $\forall a \in \mathbb{Z}. \forall b \in \mathbb{Z}. \forall c \in \mathbb{Z}.
    a \cdot (b+c) = a \cdot b + a \cdot c \wedge (b+c) \cdot a = b \cdot a + c \cdot a$ 
  using Int_ZF_1_1_L1 by simp
  then have IsDistributive( $\mathbb{Z}$ , IntegerAddition, IntegerMultiplication)
  using IsDistributive_def by simp
  then show IsAring( $\mathbb{Z}$ , IntegerAddition, IntegerMultiplication)
  ring0( $\mathbb{Z}$ , IntegerAddition, IntegerMultiplication)
  using Int_ZF_1_T1 Int_ZF_1_T2 IsAring_def ring0_def
  by auto
  have  $\forall a \in \mathbb{Z}. \forall b \in \mathbb{Z}. a \cdot b = b \cdot a$  using Int_ZF_1_L4 by simp
  then show IntegerMultiplication {is commutative on}  $\mathbb{Z}$ 
  using IsCommutative_def by simp
qed
```

Zero and one are integers.

```
lemma (in int0) int_zero_one_are_int: shows  $0 \in \mathbb{Z}$   $1 \in \mathbb{Z}$ 
  using Int_ZF_1_1_L2 ring0.Ring_ZF_1_L2 by auto
```

Negative of zero is zero.

```
lemma (in int0) int_zero_one_are_intA: shows  $(-0) = 0$ 
```

using Int\_ZF\_1\_T2 group0.group\_inv\_of\_one by simp

Properties with one integer.

```
lemma (in int0) Int_ZF_1_1_L4: assumes A1:  $a \in \mathbb{Z}$ 
  shows
     $a+0 = a$ 
     $0+a = a$ 
     $a \cdot 1 = a$      $1 \cdot a = a$ 
     $0 \cdot a = 0$      $a \cdot 0 = 0$ 
     $(-a) \in \mathbb{Z}$      $-(-a) = a$ 
     $a-a = 0$      $a-0 = a$      $2 \cdot a = a+a$ 
proof -
  from A1 show
     $a+0 = a$      $0+a = a$      $a \cdot 1 = a$ 
     $1 \cdot a = a$      $a-a = 0$      $a-0 = a$ 
     $(-a) \in \mathbb{Z}$      $2 \cdot a = a+a$      $-(-a) = a$ 
  using Int_ZF_1_1_L2 ring0.Ring_ZF_1_L3 by auto
  from A1 show  $0 \cdot a = 0$      $a \cdot 0 = 0$ 
  using Int_ZF_1_1_L2 ring0.Ring_ZF_1_L6 by auto
qed
```

Properties that require two integers.

```
lemma (in int0) Int_ZF_1_1_L5: assumes  $a \in \mathbb{Z}$      $b \in \mathbb{Z}$ 
  shows
     $a+b \in \mathbb{Z}$ 
     $a-b \in \mathbb{Z}$ 
     $a \cdot b \in \mathbb{Z}$ 
     $a+b = b+a$ 
     $a \cdot b = b \cdot a$ 
     $(-b)-a = (-a)-b$ 
     $-(a+b) = (-a)-b$ 
     $-(a-b) = ((-a)+b)$ 
     $(-a) \cdot b = -(a \cdot b)$ 
     $a \cdot (-b) = -(a \cdot b)$ 
     $(-a) \cdot (-b) = a \cdot b$ 
  using assms Int_ZF_1_1_L2 ring0.Ring_ZF_1_L4 ring0.Ring_ZF_1_L9
    ring0.Ring_ZF_1_L7 ring0.Ring_ZF_1_L7A Int_ZF_1_L4 by auto
```

2 and 3 are integers.

```
lemma (in int0) int_two_three_are_int: shows  $2 \in \mathbb{Z}$      $3 \in \mathbb{Z}$ 
  using int_zero_one_are_int Int_ZF_1_1_L5 by auto
```

Another property with two integers.

```
lemma (in int0) Int_ZF_1_1_L5B:
  assumes  $a \in \mathbb{Z}$      $b \in \mathbb{Z}$ 
  shows  $a-(-b) = a+b$ 
  using assms Int_ZF_1_1_L2 ring0.Ring_ZF_1_L9
  by simp
```

Properties that require three integers.

```
lemma (in int0) Int_ZF_1_1_L6: assumes a $\in\mathbb{Z}$  b $\in\mathbb{Z}$  c $\in\mathbb{Z}$ 
  shows
    a-(b+c) = a-b-c
    a-(b-c) = a-b+c
    a·(b-c) = a·b - a·c
    (b-c)·a = b·a - c·a
  using assms Int_ZF_1_1_L2 ring0.Ring_ZF_1_L10 ring0.Ring_ZF_1_L8
  by auto
```

One more property with three integers.

```
lemma (in int0) Int_ZF_1_1_L6A: assumes a $\in\mathbb{Z}$  b $\in\mathbb{Z}$  c $\in\mathbb{Z}$ 
  shows a+(b-c) = a+b-c
  using assms Int_ZF_1_1_L2 ring0.Ring_ZF_1_L10A by simp
```

Associativity of addition and multiplication.

```
lemma (in int0) Int_ZF_1_1_L7: assumes a $\in\mathbb{Z}$  b $\in\mathbb{Z}$  c $\in\mathbb{Z}$ 
  shows
    a+b+c = a+(b+c)
    a·b·c = a·(b·c)
  using assms Int_ZF_1_1_L2 ring0.Ring_ZF_1_L11 by auto
```

## 35.2 Rearrangement lemmas

In this section we collect lemmas about identities related to rearranging the terms in expressions

A formula with a positive integer.

```
lemma (in int0) Int_ZF_1_2_L1: assumes 0 $\leq$ a
  shows abs(a)+1 = abs(a+1)
  using assms Int_ZF_2_L16 Int_ZF_2_L12A by simp
```

A formula with two integers, one positive.

```
lemma (in int0) Int_ZF_1_2_L2: assumes A1: a $\in\mathbb{Z}$  and A2: 0 $\leq$ b
  shows a+(abs(b)+1)·a = (abs(b+1)+1)·a
proof -
  from A2 have abs(b+1)  $\in\mathbb{Z}$ 
  using Int_ZF_2_L12A Int_ZF_2_L1A Int_ZF_2_L14 by blast
  with A1 A2 show thesis
  using Int_ZF_1_2_L1 Int_ZF_1_1_L2 ring0.Ring_ZF_2_L1
  by simp
qed
```

A couple of formulae about canceling opposite integers.

```
lemma (in int0) Int_ZF_1_2_L3: assumes A1: a $\in\mathbb{Z}$  b $\in\mathbb{Z}$ 
  shows
    a+b-a = b
```



```

a+(b-a) = b
a+b-b = a
a-b+b = a
(-a)+(a+b) = b
a+(b-a) = b
(-b)+(a+b) = a
a-(b+a) = -b
a-(a+b) = -b
a-(a-b) = b
a-b-a = -b
a-b - (a+b) = (-b)-b
using assms Int_ZF_1_T2 group0.group0_4_L6A group0.inv_cancel_two
    group0.group0_2_L16A group0.group0_4_L6AA group0.group0_4_L6AB
    group0.group0_4_L6F group0.group0_4_L6AC by auto

```

Subtracting one does not increase integers. This may be moved to a theory about ordered rings one day.

```

lemma (in int0) Int_ZF_1_2_L3A: assumes A1: a≤b
  shows a-1 ≤ b
proof -
  from A1 have b+1-1 = b
    using Int_ZF_2_L1A int_zero_one_are_int Int_ZF_1_2_L3 by simp
  moreover from A1 have a-1 ≤ b+1-1
    using Int_ZF_2_L12A int_zero_one_are_int Int_ZF_1_1_L4 int_ord_transl_inv
    by simp
  ultimately show a-1 ≤ b by simp
qed

```

Subtracting one does not increase integers, special case.

```

lemma (in int0) Int_ZF_1_2_L3AA:
  assumes A1: a∈ℤ shows
    a-1 ≤a
    a-1 ≠ a
    ¬(a≤a-1)
    ¬(a+1 ≤a)
    ¬(1+a ≤a)
proof -
  from A1 have a≤a using int_ord_is_refl refl_def
    by simp
  then show a-1 ≤a using Int_ZF_1_2_L3A
    by simp
  moreover from A1 show a-1 ≠ a using Int_ZF_1_L14 by simp
  ultimately show I: ¬(a≤a-1) using Int_ZF_2_L19AA
    by blast
  with A1 show ¬(a+1 ≤a)
    using int_zero_one_are_int Int_ZF_2_L9B by simp
  with A1 show ¬(1+a ≤a)
    using int_zero_one_are_int Int_ZF_1_1_L5 by simp
qed

```

A formula with a nonpositive integer.

```
lemma (in int0) Int_ZF_1_2_L4: assumes a≤0
  shows abs(a)+1 = abs(a-1)
  using assms int_zero_one_are_int Int_ZF_1_2_L3A Int_ZF_2_T1
    group3.OrderedGroup_ZF_3_L3A Int_ZF_2_L1A
    int_zero_one_are_int Int_ZF_1_1_L5 by simp
```

A formula with two integers, one negative.

```
lemma (in int0) Int_ZF_1_2_L5: assumes A1: a∈ℤ and A2: b≤0
  shows a+(abs(b)+1)·a = (abs(b-1)+1)·a
proof -
  from A2 have abs(b-1) ∈ ℤ
    using int_zero_one_are_int Int_ZF_1_2_L3A Int_ZF_2_L1A Int_ZF_2_L14

    by blast
  with A1 A2 show thesis
    using Int_ZF_1_2_L4 Int_ZF_1_1_L2 ring0.Ring_ZF_2_L1
    by simp
qed
```

A rearrangement with four integers.

```
lemma (in int0) Int_ZF_1_2_L6:
  assumes A1: a∈ℤ b∈ℤ c∈ℤ d∈ℤ
  shows
    a-(b-1)·c = (d-b·c)-(d-a-c)
proof -
  from A1 have T1:
    (d-b·c) ∈ ℤ d-a ∈ ℤ (-(b·c)) ∈ ℤ
    using Int_ZF_1_1_L5 Int_ZF_1_1_L4 by auto
  with A1 have
    (d-b·c)-(d-a-c) = (-(b·c))+a+c
    using Int_ZF_1_1_L6 Int_ZF_1_2_L3 by simp
  also from A1 T1 have (-(b·c))+a+c = a-(b-1)·c
    using int_zero_one_are_int Int_ZF_1_1_L6 Int_ZF_1_1_L4 Int_ZF_1_1_L5
    by simp
  finally show thesis by simp
qed
```

Some other rearrangements with two integers.

```
lemma (in int0) Int_ZF_1_2_L7: assumes a∈ℤ b∈ℤ
  shows
    a·b = (a-1)·b+b
    a·(b+1) = a·b+a
    (b+1)·a = b·a+a
    (b+1)·a = a+b·a
  using assms Int_ZF_1_1_L1 Int_ZF_1_1_L5 int_zero_one_are_int
    Int_ZF_1_1_L6 Int_ZF_1_1_L4 Int_ZF_1_T2 group0.inv_cancel_two
  by auto
```

Another rearrangement with two integers.

```
lemma (in int0) Int_ZF_1_2_L8:
  assumes A1:  $a \in \mathbb{Z}$   $b \in \mathbb{Z}$ 
  shows  $a+1+(b+1) = b+a+2$ 
  using assms int_zero_one_are_int Int_ZF_1_T2 group0.group0_4_L8
  by simp
```

A couple of rearrangement with three integers.

```
lemma (in int0) Int_ZF_1_2_L9:
  assumes  $a \in \mathbb{Z}$   $b \in \mathbb{Z}$   $c \in \mathbb{Z}$ 
  shows
     $(a-b)+(b-c) = a-c$ 
     $(a-b)-(a-c) = c-b$ 
     $a+(b+(c-a-b)) = c$ 
     $(-a)-b+c = c-a-b$ 
     $(-b)-a+c = c-a-b$ 
     $(-((-a)+b+c)) = a-b-c$ 
     $a+b+c-a = b+c$ 
     $a+b-(a+c) = b-c$ 
  using assms Int_ZF_1_T2
    group0.group0_4_L4B group0.group0_4_L6D group0.group0_4_L4D
    group0.group0_4_L6B group0.group0_4_L6E
  by auto
```

Another couple of rearrangements with three integers.

```
lemma (in int0) Int_ZF_1_2_L9A:
  assumes A1:  $a \in \mathbb{Z}$   $b \in \mathbb{Z}$   $c \in \mathbb{Z}$ 
  shows  $-(a-b-c) = c+b-a$ 
proof -
  from A1 have T:
     $a-b \in \mathbb{Z}$   $- (a-b) \in \mathbb{Z}$   $(-b) \in \mathbb{Z}$  using
    Int_ZF_1_1_L4 Int_ZF_1_1_L5 by auto
  with A1 have  $-(a-b-c) = c - ((-b)+a)$ 
    using Int_ZF_1_1_L5 by simp
  also from A1 T have  $\dots = c+b-a$ 
    using Int_ZF_1_1_L6 Int_ZF_1_1_L5B
    by simp
  finally show  $-(a-b-c) = c+b-a$ 
    by simp
qed
```

Another rearrangement with three integers.

```
lemma (in int0) Int_ZF_1_2_L10:
  assumes A1:  $a \in \mathbb{Z}$   $b \in \mathbb{Z}$   $c \in \mathbb{Z}$ 
  shows  $(a+1) \cdot b + (c+1) \cdot b = (c+a+2) \cdot b$ 
proof -
  from A1 have  $a+1 \in \mathbb{Z}$   $c+1 \in \mathbb{Z}$ 
    using int_zero_one_are_int Int_ZF_1_1_L5 by auto
```

```

with A1 have
  (a+1)·b + (c+1)·b = (a+1+(c+1))·b
  using Int_ZF_1_1_L1 by simp
also from A1 have ... = (c+a+2)·b
  using Int_ZF_1_2_L8 by simp
finally show thesis by simp
qed

```

A technical rearrangement involving inequalities with absolute value.

```

lemma (in int0) Int_ZF_1_2_L10A:
  assumes A1: a∈ℤ b∈ℤ c∈ℤ e∈ℤ
  and A2: abs(a·b-c) ≤ d abs(b·a-e) ≤ f
  shows abs(c-e) ≤ f+d
proof -
  from A1 A2 have T1:
    d∈ℤ f∈ℤ a·b ∈ ℤ a·b-c ∈ ℤ b·a-e ∈ ℤ
    using Int_ZF_2_L1A Int_ZF_1_1_L5 by auto
  with A2 have
    abs((b·a-e)-(a·b-c)) ≤ f +d
    using Int_ZF_2_L21 by simp
  with A1 T1 show abs(c-e) ≤ f+d
    using Int_ZF_1_1_L5 Int_ZF_1_2_L9 by simp
qed

```

Some arithmetics.

```

lemma (in int0) Int_ZF_1_2_L11: assumes A1: a∈ℤ
  shows
    a+1+2 = a+3
    a = 2·a - a
proof -
  from A1 show a+1+2 = a+3
    using int_zero_one_are_int int_two_three_are_int Int_ZF_1_T2 group0.group0_4_L4C
    by simp
  from A1 show a = 2·a - a
    using int_zero_one_are_int Int_ZF_1_1_L1 Int_ZF_1_1_L4 Int_ZF_1_T2
    group0.inv_cancel_two
    by simp
qed

```

A simple rearrangement with three integers.

```

lemma (in int0) Int_ZF_1_2_L12:
  assumes a∈ℤ b∈ℤ c∈ℤ
  shows
    (b-c)·a = a·b - a·c
  using assms Int_ZF_1_1_L6 Int_ZF_1_1_L5 by simp

```

A big rearrangement with five integers.

```

lemma (in int0) Int_ZF_1_2_L13:

```

```

assumes A1: a $\in\mathbb{Z}$  b $\in\mathbb{Z}$  c $\in\mathbb{Z}$  d $\in\mathbb{Z}$  x $\in\mathbb{Z}$ 
shows (x+(a·x+b)+c)·d = d·(a+1)·x + (b·d+c·d)
proof -
  from A1 have T1:
    a·x  $\in\mathbb{Z}$  (a+1)·x  $\in\mathbb{Z}$ 
    (a+1)·x + b  $\in\mathbb{Z}$ 
  using Int_ZF_1_1_L5 int_zero_one_are_int by auto
  with A1 have (x+(a·x+b)+c)·d = ((a+1)·x + b)·d + c·d
  using Int_ZF_1_1_L7 Int_ZF_1_2_L7 Int_ZF_1_1_L1
  by simp
  also from A1 T1 have ... = (a+1)·x·d + b·d + c·d
  using Int_ZF_1_1_L1 by simp
  finally have (x+(a·x+b)+c)·d = (a+1)·x·d + b·d + c·d
  by simp
  moreover from A1 T1 have (a+1)·x·d = d·(a+1)·x
  using int_zero_one_are_int Int_ZF_1_1_L5 Int_ZF_1_1_L7 by simp
  ultimately have (x+(a·x+b)+c)·d = d·(a+1)·x + b·d + c·d
  by simp
  moreover from A1 T1 have
    d·(a+1)·x  $\in\mathbb{Z}$  b·d  $\in\mathbb{Z}$  c·d  $\in\mathbb{Z}$ 
  using int_zero_one_are_int Int_ZF_1_1_L5 by auto
  ultimately show thesis using Int_ZF_1_1_L7 by simp
qed

```

Rerrangement about adding linear functions.

```

lemma (in int0) Int_ZF_1_2_L14:
  assumes a $\in\mathbb{Z}$  b $\in\mathbb{Z}$  c $\in\mathbb{Z}$  d $\in\mathbb{Z}$  x $\in\mathbb{Z}$ 
  shows (a·x + b) + (c·x + d) = (a+c)·x + (b+d)
  using assms Int_ZF_1_1_L2 ring0.Ring_ZF_2_L3 by simp

```

A rearrangement with four integers. Again we have to use the generic set notation to use a theorem proven in different context.

```

lemma (in int0) Int_ZF_1_2_L15: assumes A1: a $\in\mathbb{Z}$  b $\in\mathbb{Z}$  c $\in\mathbb{Z}$  d $\in\mathbb{Z}$ 
  and A2: a = b-c-d
  shows
    d = b-a-c
    d = (-a)+b-c
    b = a+d+c
proof -
  let G = int
  let f = IntegerAddition
  from A1 A2 have I:
    group0(G, f) f {is commutative on} G
    a  $\in G$  b  $\in G$  c  $\in G$  d  $\in G$ 
    a = f⟨f⟨b, GroupInv(G, f)(c)⟩, GroupInv(G, f)(d)⟩
  using Int_ZF_1_T2 by auto
  then have
    d = f⟨f⟨b, GroupInv(G, f)(a)⟩, GroupInv(G, f)(c)⟩
  by (rule group0.group0_4_L9)

```

```

then show d = b-a-c by simp
from I have d = f⟨f⟨GroupInv(G, f)(a), b⟩, GroupInv(G, f)(c)⟩
  by (rule group0.group0_4_L9)
thus d = (-a)+b-c
  by simp
from I have b = f⟨f⟨a, d⟩, c⟩
  by (rule group0.group0_4_L9)
thus b = a+d+c by simp
qed

```

A rearrangement with four integers. Property of groups.

```

lemma (in int0) Int_ZF_1_2_L16:
  assumes a∈ℤ b∈ℤ c∈ℤ d∈ℤ
  shows a+(b-c)+d = a+b+d-c
  using assms Int_ZF_1_T2 group0.group0_4_L8 by simp

```

Some rearrangements with three integers. Properties of groups.

```

lemma (in int0) Int_ZF_1_2_L17:
  assumes A1: a∈ℤ b∈ℤ c∈ℤ
  shows
    a+b-c+(c-b) = a
    a+(b+c)-c = a+b
proof -
  let G = int
  let f = IntegerAddition
  from A1 have I:
    group0(G, f)
    a ∈ G b ∈ G c ∈ G
  using Int_ZF_1_T2 by auto
  then have
    f⟨f⟨f⟨a, b⟩, GroupInv(G, f)(c)⟩, f⟨c, GroupInv(G, f)(b)⟩⟩ = a
  by (rule group0.group0_2_L14A)
  thus a+b-c+(c-b) = a by simp
  from I have
    f⟨f⟨a, f⟨b, c⟩⟩, GroupInv(G, f)(c)⟩ = f⟨a, b⟩
  by (rule group0.group0_2_L14A)
  thus a+(b+c)-c = a+b by simp
qed

```

Another rearrangement with three integers. Property of abelian groups.

```

lemma (in int0) Int_ZF_1_2_L18:
  assumes A1: a∈ℤ b∈ℤ c∈ℤ
  shows a+b-c+(c-a) = b
proof -
  let G = int
  let f = IntegerAddition
  from A1 have
    group0(G, f) f {is commutative on} G
    a ∈ G b ∈ G c ∈ G

```

```

    using Int_ZF_1_T2 by auto
  then have
    f⟨f⟨f⟨a,b⟩,GroupInv(G, f)(c)⟩,f⟨c,GroupInv(G, f)(a)⟩⟩ = b
    by (rule group0.group0_4_L6D)
  thus a+b-c+(c-a) = b by simp
qed

```

### 35.3 Integers as an ordered ring

We already know from Int\_ZF that integers with addition form a linearly ordered group. To show that integers form an ordered ring we need the fact that the set of nonnegative integers is closed under multiplication.

We start with the property that a product of nonnegative integers is nonnegative. The proof is by induction and the next lemma is the induction step.

```

lemma (in int0) Int_ZF_1_3_L1: assumes A1:  $0 \leq a$   $0 \leq b$ 
  and A3:  $0 \leq a \cdot b$ 
  shows  $0 \leq a \cdot (b+1)$ 
proof -
  from A1 A3 have  $0+0 \leq a \cdot b + a$ 
    using int_ineq_add_sides by simp
  with A1 show  $0 \leq a \cdot (b+1)$ 
    using int_zero_one_are_int Int_ZF_1_1_L4 Int_ZF_2_L1A Int_ZF_1_2_L7

    by simp
qed

```

Product of nonnegative integers is nonnegative.

```

lemma (in int0) Int_ZF_1_3_L2: assumes A1:  $0 \leq a$   $0 \leq b$ 
  shows  $0 \leq a \cdot b$ 
proof -
  from A1 have  $0 \leq b$  by simp
  moreover from A1 have  $0 \leq a \cdot 0$  using
    Int_ZF_2_L1A Int_ZF_1_1_L4 int_zero_one_are_int int_ord_is_refl refl_def
    by simp
  moreover from A1 have
     $\forall m. 0 \leq m \wedge 0 \leq a \cdot m \longrightarrow 0 \leq a \cdot (m+1)$ 
    using Int_ZF_1_3_L1 by simp
  ultimately show  $0 \leq a \cdot b$  by (rule Induction_on_int)
qed

```

The set of nonnegative integers is closed under multiplication.

```

lemma (in int0) Int_ZF_1_3_L2A: shows
   $\mathbb{Z}^+$  {is closed under} IntegerMultiplication
proof -
  { fix a b assume  $a \in \mathbb{Z}^+$   $b \in \mathbb{Z}^+$ 
    then have  $a \cdot b \in \mathbb{Z}^+$ 

```

```

        using Int_ZF_1_3_L2 Int_ZF_2_T1 group3.OrderedGroup_ZF_1_L2
        by simp
    } then have  $\forall a \in \mathbb{Z}^+. \forall b \in \mathbb{Z}^+. a \cdot b \in \mathbb{Z}^+$  by simp
    then show thesis using IsOpClosed_def by simp
qed

```

Integers form an ordered ring. All theorems proven in the `ring1` context are valid in `int0` context.

```

theorem (in int0) Int_ZF_1_3_T1: shows
  IsAnOrdRing( $\mathbb{Z}$ , IntegerAddition, IntegerMultiplication, IntegerOrder)
  ring1( $\mathbb{Z}$ , IntegerAddition, IntegerMultiplication, IntegerOrder)
  using Int_ZF_1_1_L2 Int_ZF_2_L1B Int_ZF_1_3_L2A Int_ZF_2_T1
  OrdRing_ZF_1_L6 OrdRing_ZF_1_L2 by auto

```

Product of integers that are greater than one is greater than one. The proof is by induction and the next step is the induction step.

```

lemma (in int0) Int_ZF_1_3_L3_indstep:
  assumes A1:  $1 \leq a$   $1 \leq b$ 
  and A2:  $1 \leq a \cdot b$ 
  shows  $1 \leq a \cdot (b+1)$ 
proof -
  from A1 A2 have  $1 \leq 2$  and  $2 \leq a \cdot (b+1)$ 
  using Int_ZF_2_L1A int_ineq_add_sides Int_ZF_2_L16B Int_ZF_1_2_L7

  by auto
  then show  $1 \leq a \cdot (b+1)$  by (rule Int_order_transitive)
qed

```

Product of integers that are greater than one is greater than one.

```

lemma (in int0) Int_ZF_1_3_L3:
  assumes A1:  $1 \leq a$   $1 \leq b$ 
  shows  $1 \leq a \cdot b$ 
proof -
  from A1 have  $1 \leq b$   $1 \leq a \cdot 1$ 
  using Int_ZF_2_L1A Int_ZF_1_1_L4 by auto
  moreover from A1 have
     $\forall m. 1 \leq m \wedge 1 \leq a \cdot m \longrightarrow 1 \leq a \cdot (m+1)$ 
  using Int_ZF_1_3_L3_indstep by simp
  ultimately show  $1 \leq a \cdot b$  by (rule Induction_on_int)
qed

```

$|a \cdot (-b)| = |(-a) \cdot b| = |(-a) \cdot (-b)| = |a \cdot b|$  This is a property of ordered rings..

```

lemma (in int0) Int_ZF_1_3_L4: assumes  $a \in \mathbb{Z}$   $b \in \mathbb{Z}$ 
  shows
     $\text{abs}((-a) \cdot b) = \text{abs}(a \cdot b)$ 
     $\text{abs}(a \cdot (-b)) = \text{abs}(a \cdot b)$ 
     $\text{abs}((-a) \cdot (-b)) = \text{abs}(a \cdot b)$ 

```



```
using assms Int_ZF_1_1_L5 Int_ZF_2_L17 by auto
```

Absolute value of a product is the product of absolute values. Property of ordered rings.

```
lemma (in int0) Int_ZF_1_3_L5:
  assumes A1:  $a \in \mathbb{Z}$   $b \in \mathbb{Z}$ 
  shows  $\text{abs}(a \cdot b) = \text{abs}(a) \cdot \text{abs}(b)$ 
  using assms Int_ZF_1_3_T1 ring1.OrdRing_ZF_2_L5 by simp
```

Double nonnegative is nonnegative. Property of ordered rings.

```
lemma (in int0) Int_ZF_1_3_L5A: assumes  $0 \leq a$ 
  shows  $0 \leq 2 \cdot a$ 
  using assms Int_ZF_1_3_T1 ring1.OrdRing_ZF_1_L5A by simp
```

The next lemma shows what happens when one integer is not greater or equal than another.

```
lemma (in int0) Int_ZF_1_3_L6:
  assumes A1:  $a \in \mathbb{Z}$   $b \in \mathbb{Z}$ 
  shows  $\neg(b \leq a) \longleftrightarrow a+1 \leq b$ 
proof
  assume A3:  $\neg(b \leq a)$ 
  with A1 have  $a \leq b$  by (rule Int_ZF_2_L19)
  then have  $a = b \vee a+1 \leq b$ 
    using Int_ZF_4_L1B by simp
  moreover from A1 A3 have  $a \neq b$  by (rule Int_ZF_2_L19)
  ultimately show  $a+1 \leq b$  by simp
next assume A4:  $a+1 \leq b$ 
  { assume  $b \leq a$ 
    with A4 have  $a+1 \leq a$  by (rule Int_order_transitive)
    moreover from A1 have  $a \leq a+1$ 
      using Int_ZF_2_L12B by simp
    ultimately have  $a+1 = a$ 
      by (rule Int_ZF_2_L3)
    with A1 have False using Int_ZF_1_L14 by simp
  } then show  $\neg(b \leq a)$  by auto
qed
```

Another form of stating that there are no integers between integers  $m$  and  $m+1$ .

```
corollary (in int0) no_int_between: assumes A1:  $a \in \mathbb{Z}$   $b \in \mathbb{Z}$ 
  shows  $b \leq a \vee a+1 \leq b$ 
  using A1 Int_ZF_1_3_L6 by auto
```

Another way of saying what it means that one integer is not greater or equal than another.

```
corollary (in int0) Int_ZF_1_3_L6A:
  assumes A1:  $a \in \mathbb{Z}$   $b \in \mathbb{Z}$  and A2:  $\neg(b \leq a)$ 
  shows  $a \leq b-1$ 
```

```

proof -
  from A1 A2 have  $a+1 - 1 \leq b - 1$ 
    using Int_ZF_1_3_L6 int_zero_one_are_int Int_ZF_1_1_L4
      int_ord_transl_inv by simp
  with A1 show  $a \leq b-1$ 
    using int_zero_one_are_int Int_ZF_1_2_L3
      by simp
qed

```

Yet another form of stating that there are no integers between  $m$  and  $m+1$ .

```

lemma (in int0) no_int_between1:
  assumes A1:  $a \leq b$  and A2:  $a \neq b$ 
  shows
     $a+1 \leq b$ 
     $a \leq b-1$ 
proof -
  from A1 have T:  $a \in \mathbb{Z} \quad b \in \mathbb{Z}$  using Int_ZF_2_L1A
  by auto
  { assume  $b \leq a$ 
    with A1 have  $a=b$  by (rule Int_ZF_2_L3)
    with A2 have False by simp }
  then have  $\neg(b \leq a)$  by auto
  with T show
     $a+1 \leq b$ 
     $a \leq b-1$ 
    using no_int_between Int_ZF_1_3_L6A by auto
qed

```

We can decompose proofs into three cases:  $a = b$ ,  $a \leq b - 1$  or  $a \geq b + 1$ .

```

lemma (in int0) Int_ZF_1_3_L6B: assumes A1:  $a \in \mathbb{Z} \quad b \in \mathbb{Z}$ 
  shows  $a=b \vee (a \leq b-1) \vee (b+1 \leq a)$ 
proof -
  from A1 have  $a=b \vee (a \leq b \wedge a \neq b) \vee (b \leq a \wedge b \neq a)$ 
    using Int_ZF_2_T1 group3.OrderedGroup_ZF_1_L31
      by simp
  then show thesis using no_int_between1
    by auto
qed

```

A special case of Int\_ZF\_1\_3\_L6B when  $b = 0$ . This allows to split the proofs in cases  $a \leq -1$ ,  $a = 0$  and  $a \geq 1$ .

```

corollary (in int0) Int_ZF_1_3_L6C: assumes A1:  $a \in \mathbb{Z}$ 
  shows  $a=0 \vee (a \leq -1) \vee (1 \leq a)$ 
proof -
  from A1 have  $a=0 \vee (a \leq 0 -1) \vee (0 +1 \leq a)$ 
    using int_zero_one_are_int Int_ZF_1_3_L6B by simp
  then show thesis using Int_ZF_1_1_L4 int_zero_one_are_int
    by simp
qed

```

An integer is not less or equal zero iff it is greater or equal one.

```
lemma (in int0) Int_ZF_1_3_L7: assumes a $\in\mathbb{Z}$ 
  shows  $\neg(a\leq 0) \longleftrightarrow 1 \leq a$ 
  using assms int_zero_one_are_int Int_ZF_1_3_L6 Int_ZF_1_1_L4
  by simp
```

Product of positive integers is positive.

```
lemma (in int0) Int_ZF_1_3_L8:
  assumes a $\in\mathbb{Z}$  b $\in\mathbb{Z}$ 
  and  $\neg(a\leq 0)$   $\neg(b\leq 0)$ 
  shows  $\neg((a\cdot b) \leq 0)$ 
  using assms Int_ZF_1_3_L7 Int_ZF_1_3_L3 Int_ZF_1_1_L5 Int_ZF_1_3_L7
  by simp
```

If  $a \cdot b$  is nonnegative and  $b$  is positive, then  $a$  is nonnegative. Proof by contradiction.

```
lemma (in int0) Int_ZF_1_3_L9:
  assumes A1: a $\in\mathbb{Z}$  b $\in\mathbb{Z}$ 
  and A2:  $\neg(b\leq 0)$  and A3:  $a\cdot b \leq 0$ 
  shows a $\leq 0$ 
proof -
  { assume  $\neg(a\leq 0)$ 
    with A1 A2 have  $\neg((a\cdot b) \leq 0)$  using Int_ZF_1_3_L8
    by simp
  } with A3 show a $\leq 0$  by auto
qed
```

One integer is less or equal another iff the difference is nonpositive.

```
lemma (in int0) Int_ZF_1_3_L10:
  assumes a $\in\mathbb{Z}$  b $\in\mathbb{Z}$ 
  shows  $a\leq b \longleftrightarrow a-b \leq 0$ 
  using assms Int_ZF_2_T1 group3.OrderedGroup_ZF_1_L9
  by simp
```

Some conclusions from the fact that one integer is less or equal than another.

```
lemma (in int0) Int_ZF_1_3_L10A: assumes a $\leq$ b
  shows  $0 \leq b-a$ 
  using assms Int_ZF_2_T1 group3.OrderedGroup_ZF_1_L12A
  by simp
```

We can simplify out a positive element on both sides of an inequality.

```
lemma (in int0) Int_ineq_simpl_positive:
  assumes A1: a $\in\mathbb{Z}$  b $\in\mathbb{Z}$  c $\in\mathbb{Z}$ 
  and A2:  $a\cdot c \leq b\cdot c$  and A4:  $\neg(c\leq 0)$ 
  shows a  $\leq$  b
proof -
  from A1 A4 have a-b  $\in \mathbb{Z}$  c $\in\mathbb{Z}$   $\neg(c\leq 0)$ 
```

```

    using Int_ZF_1_1_L5 by auto
  moreover from A1 A2 have  $(a-b) \cdot c \leq 0$ 
    using Int_ZF_1_1_L5 Int_ZF_1_3_L10 Int_ZF_1_1_L6
    by simp
  ultimately have  $a-b \leq 0$  by (rule Int_ZF_1_3_L9)
  with A1 show  $a \leq b$  using Int_ZF_1_3_L10 by simp
qed

```

A technical lemma about conclusion from an inequality between absolute values. This is a property of ordered rings.

```

lemma (in int0) Int_ZF_1_3_L11:
  assumes A1:  $a \in \mathbb{Z}$   $b \in \mathbb{Z}$ 
  and A2:  $\neg(\text{abs}(a) \leq \text{abs}(b))$ 
  shows  $\neg(\text{abs}(a) \leq 0)$ 
proof -
  { assume  $\text{abs}(a) \leq 0$ 
    moreover from A1 have  $0 \leq \text{abs}(a)$  using int_abs_nonneg
    by simp
    ultimately have  $\text{abs}(a) = 0$  by (rule Int_ZF_2_L3)
    with A1 A2 have False using int_abs_nonneg by simp
  } then show  $\neg(\text{abs}(a) \leq 0)$  by auto
qed

```

Negative times positive is negative. This a property of ordered rings.

```

lemma (in int0) Int_ZF_1_3_L12:
  assumes  $a \leq 0$  and  $0 \leq b$ 
  shows  $a \cdot b \leq 0$ 
  using assms Int_ZF_1_3_T1 ring1.OrdRing_ZF_1_L8
  by simp

```

We can multiply an inequality by a nonnegative number. This is a property of ordered rings.

```

lemma (in int0) Int_ZF_1_3_L13:
  assumes A1:  $a \leq b$  and A2:  $0 \leq c$ 
  shows
     $a \cdot c \leq b \cdot c$ 
     $c \cdot a \leq c \cdot b$ 
  using assms Int_ZF_1_3_T1 ring1.OrdRing_ZF_1_L9 by auto

```

A technical lemma about decreasing a factor in an inequality.

```

lemma (in int0) Int_ZF_1_3_L13A:
  assumes  $1 \leq a$  and  $b \leq c$  and  $(a+1) \cdot c \leq d$ 
  shows  $(a+1) \cdot b \leq d$ 
proof -
  from assms have
     $(a+1) \cdot b \leq (a+1) \cdot c$ 
     $(a+1) \cdot c \leq d$ 
  using Int_ZF_2_L16C Int_ZF_1_3_L13 by auto

```

```

    then show  $(a+1) \cdot b \leq d$  by (rule Int_order_transitive)
qed

```

We can multiply an inequality by a positive number. This is a property of ordered rings.

```

lemma (in int0) Int_ZF_1_3_L13B:
  assumes A1:  $a \leq b$  and A2:  $c \in \mathbb{Z}_+$ 
  shows
     $a \cdot c \leq b \cdot c$ 
     $c \cdot a \leq c \cdot b$ 
proof -
  let R =  $\mathbb{Z}$ 
  let A = IntegerAddition
  let M = IntegerMultiplication
  let r = IntegerOrder
  from A1 A2 have
    ring1(R, A, M, r)
     $\langle a, b \rangle \in r$ 
     $c \in \text{PositiveSet}(R, A, r)$ 
    using Int_ZF_1_3_T1 by auto
  then show
     $a \cdot c \leq b \cdot c$ 
     $c \cdot a \leq c \cdot b$ 
    using ring1.OrdRing_ZF_1_L9A by auto
qed

```

A rearrangement with four integers and absolute value.

```

lemma (in int0) Int_ZF_1_3_L14:
  assumes A1:  $a \in \mathbb{Z}$   $b \in \mathbb{Z}$   $c \in \mathbb{Z}$   $d \in \mathbb{Z}$ 
  shows  $\text{abs}(a \cdot b) + (\text{abs}(a) + c) \cdot d = (d + \text{abs}(b)) \cdot \text{abs}(a) + c \cdot d$ 
proof -
  from A1 have T1:
     $\text{abs}(a) \in \mathbb{Z}$   $\text{abs}(b) \in \mathbb{Z}$ 
     $\text{abs}(a) \cdot \text{abs}(b) \in \mathbb{Z}$ 
     $\text{abs}(a) \cdot d \in \mathbb{Z}$ 
     $c \cdot d \in \mathbb{Z}$ 
     $\text{abs}(b) + d \in \mathbb{Z}$ 
    using Int_ZF_2_L14 Int_ZF_1_1_L5 by auto
  with A1 have  $\text{abs}(a \cdot b) + (\text{abs}(a) + c) \cdot d = \text{abs}(a) \cdot (\text{abs}(b) + d) + c \cdot d$ 
    using Int_ZF_1_3_L5 Int_ZF_1_1_L1 Int_ZF_1_1_L7 by simp
  with A1 T1 show thesis using Int_ZF_1_1_L5 by simp
qed

```

A technical lemma about what happens when one absolute value is not greater or equal than another.

```

lemma (in int0) Int_ZF_1_3_L15: assumes A1:  $m \in \mathbb{Z}$   $n \in \mathbb{Z}$ 
  and A2:  $\neg(\text{abs}(m) \leq \text{abs}(n))$ 
  shows  $n \leq \text{abs}(m)$   $m \neq 0$ 

```

```

proof -
  from A1 have T1:  $n \leq \text{abs}(n)$ 
    using Int_ZF_2_L19C by simp
  from A1 have  $\text{abs}(n) \in \mathbb{Z}$   $\text{abs}(m) \in \mathbb{Z}$ 
    using Int_ZF_2_L14 by auto
  moreover note A2
  ultimately have  $\text{abs}(n) \leq \text{abs}(m)$ 
    by (rule Int_ZF_2_L19)
  with T1 show  $n \leq \text{abs}(m)$  by (rule Int_order_transitive)
  from A1 A2 show  $m \neq 0$  using Int_ZF_2_L18 int_abs_nonneg by auto
qed

```

Negative of a nonnegative is nonpositive.

```

lemma (in int0) Int_ZF_1_3_L16: assumes A1:  $0 \leq m$ 
  shows  $(-m) \leq 0$ 
proof -
  from A1 have  $(-m) \leq (-0)$ 
    using Int_ZF_2_L10 by simp
  then show  $(-m) \leq 0$  using Int_ZF_1_L11
    by simp
qed

```

Some statements about intervals centered at 0.

```

lemma (in int0) Int_ZF_1_3_L17: assumes A1:  $m \in \mathbb{Z}$ 
  shows
     $(-\text{abs}(m)) \leq \text{abs}(m)$ 
     $(-\text{abs}(m)).. \text{abs}(m) \neq 0$ 
proof -
  from A1 have  $(-\text{abs}(m)) \leq 0$   $0 \leq \text{abs}(m)$ 
    using int_abs_nonneg Int_ZF_1_3_L16 by auto
  then show  $(-\text{abs}(m)) \leq \text{abs}(m)$  by (rule Int_order_transitive)
  then have  $\text{abs}(m) \in (-\text{abs}(m)).. \text{abs}(m)$ 
    using int_ord_is_refl Int_ZF_2_L1A Order_ZF_2_L2 by simp
  thus  $(-\text{abs}(m)).. \text{abs}(m) \neq 0$  by auto
qed

```

The greater of two integers is indeed greater than both, and the smaller one is smaller than both.

```

lemma (in int0) Int_ZF_1_3_L18: assumes A1:  $m \in \mathbb{Z}$   $n \in \mathbb{Z}$ 
  shows
     $m \leq \text{GreaterOf}(\text{IntegerOrder}, m, n)$ 
     $n \leq \text{GreaterOf}(\text{IntegerOrder}, m, n)$ 
     $\text{SmallerOf}(\text{IntegerOrder}, m, n) \leq m$ 
     $\text{SmallerOf}(\text{IntegerOrder}, m, n) \leq n$ 
    using assms Int_ZF_2_T1 Order_ZF_3_L2 by auto

```

If  $|m| \leq n$ , then  $m \in -n..n$ .

```

lemma (in int0) Int_ZF_1_3_L19:

```

```

assumes A1:  $m \in \mathbb{Z}$  and A2:  $\text{abs}(m) \leq n$ 
shows
 $(-n) \leq m \leq n$ 
 $m \in (-n)..n$ 
 $0 \leq n$ 
using assms Int_ZF_2_T1 group3.OrderedGroup_ZF_3_L8
group3.OrderedGroup_ZF_3_L8A Order_ZF_2_L1
by auto

```

A slight generalization of the above lemma.

```

lemma (in int0) Int_ZF_1_3_L19A:
  assumes A1:  $m \in \mathbb{Z}$  and A2:  $\text{abs}(m) \leq n$  and A3:  $0 \leq k$ 
  shows  $-(n+k) \leq m$ 
  using assms Int_ZF_2_T1 group3.OrderedGroup_ZF_3_L8B
  by simp

```

Sets of integers that have absolute value bounded are bounded.

```

lemma (in int0) Int_ZF_1_3_L20:
  assumes A1:  $\forall x \in X. b(x) \in \mathbb{Z} \wedge \text{abs}(b(x)) \leq L$ 
  shows  $\text{IsBounded}(\{b(x). x \in X\}, \text{IntegerOrder})$ 
proof -
  let G =  $\mathbb{Z}$ 
  let P = IntegerAddition
  let r = IntegerOrder
  from A1 have
    group3(G, P, r)
    r {is total on} G
     $\forall x \in X. b(x) \in G \wedge \langle \text{AbsoluteValue}(G, P, r) \ b(x), L \rangle \in r$ 
  using Int_ZF_2_T1 by auto
  then show  $\text{IsBounded}(\{b(x). x \in X\}, \text{IntegerOrder})$ 
    by (rule group3.OrderedGroup_ZF_3_L9A)
qed

```

If a set is bounded, then the absolute values of the elements of that set are bounded.

```

lemma (in int0) Int_ZF_1_3_L20A: assumes  $\text{IsBounded}(A, \text{IntegerOrder})$ 
  shows  $\exists L. \forall a \in A. \text{abs}(a) \leq L$ 
  using assms Int_ZF_2_T1 group3.OrderedGroup_ZF_3_L10A
  by simp

```

Absolute values of integers from a finite image of integers are bounded by an integer.

```

lemma (in int0) Int_ZF_1_3_L20AA:
  assumes A1:  $\{b(x). x \in \mathbb{Z}\} \in \text{Fin}(\mathbb{Z})$ 
  shows  $\exists L \in \mathbb{Z}. \forall x \in \mathbb{Z}. \text{abs}(b(x)) \leq L$ 
  using assms int_not_empty Int_ZF_2_T1 group3.OrderedGroup_ZF_3_L11A
  by simp

```

If absolute values of values of some integer function are bounded, then the image a set from the domain is a bounded set.

```

lemma (in int0) Int_ZF_1_3_L20B:
  assumes f:X→ℤ and A⊆X and ∀x∈A. abs(f(x)) ≤ L
  shows IsBounded(f(A),IntegerOrder)
proof -
  let G = ℤ
  let P = IntegerAddition
  let r = IntegerOrder
  from assms have
    group3(G, P, r)
    r {is total on} G
    f:X→G
    A⊆X
    ∀x∈A. ⟨AbsoluteValue(G, P, r)(f(x)), L⟩ ∈ r
  using Int_ZF_2_T1 by auto
  then show IsBounded(f(A), r)
    by (rule group3.OrderedGroup_ZF_3_L9B)
qed

```

A special case of the previous lemma for a function from integers to integers.

```

corollary (in int0) Int_ZF_1_3_L20C:
  assumes f:ℤ→ℤ and ∀m∈ℤ. abs(f(m)) ≤ L
  shows f(ℤ) ∈ Fin(ℤ)
proof -
  from assms have f:ℤ→ℤ ℤ ⊆ ℤ ∀m∈ℤ. abs(f(m)) ≤ L
  by auto
  then have IsBounded(f(ℤ),IntegerOrder)
  by (rule Int_ZF_1_3_L20B)
  then show f(ℤ) ∈ Fin(ℤ) using Int_bounded_iff_fin
  by simp
qed

```

A triangle inequality with three integers. Property of linearly ordered abelian groups.

```

lemma (in int0) int_triangle_ineq3:
  assumes A1: a∈ℤ b∈ℤ c∈ℤ
  shows abs(a-b-c) ≤ abs(a) + abs(b) + abs(c)
proof -
  from A1 have T: a-b ∈ ℤ abs(c) ∈ ℤ
  using Int_ZF_1_1_L5 Int_ZF_2_L14 by auto
  with A1 have abs(a-b-c) ≤ abs(a-b) + abs(c)
  using Int_triangle_ineq1 by simp
  moreover from A1 T have
    abs(a-b) + abs(c) ≤ abs(a) + abs(b) + abs(c)
  using Int_triangle_ineq1 int_ord_transl_inv by simp
  ultimately show thesis by (rule Int_order_transitive)
qed

```



If  $a \leq c$  and  $b \leq c$ , then  $a + b \leq 2 \cdot c$ . Property of ordered rings.

```
lemma (in int0) Int_ZF_1_3_L21:
  assumes A1: a≤c b≤c shows a+b ≤ 2·c
  using assms Int_ZF_1_3_T1 ring1.OrdRing_ZF_2_L6 by simp
```

If an integer  $a$  is between  $b$  and  $b + c$ , then  $|b - a| \leq c$ . Property of ordered groups.

```
lemma (in int0) Int_ZF_1_3_L22:
  assumes a≤b and c∈ℤ and b≤ c+a
  shows abs(b-a) ≤ c
  using assms Int_ZF_2_T1 group3.OrderedGroup_ZF_3_L8C
  by simp
```

An application of the triangle inequality with four integers. Property of linearly ordered abelian groups.

```
lemma (in int0) Int_ZF_1_3_L22A:
  assumes a∈ℤ b∈ℤ c∈ℤ d∈ℤ
  shows abs(a-c) ≤ abs(a+b) + abs(c+d) + abs(b-d)
  using assms Int_ZF_1_T2 Int_ZF_2_T1 group3.OrderedGroup_ZF_3_L7F
  by simp
```

If an integer  $a$  is between  $b$  and  $b + c$ , then  $|b - a| \leq c$ . Property of ordered groups. A version of Int\_ZF\_1\_3\_L22 with slightly different assumptions.

```
lemma (in int0) Int_ZF_1_3_L23:
  assumes A1: a≤b and A2: c∈ℤ and A3: b≤ a+c
  shows abs(b-a) ≤ c
proof -
  from A1 have a ∈ ℤ
    using Int_ZF_2_L1A by simp
  with A2 A3 have b≤ c+a
    using Int_ZF_1_1_L5 by simp
  with A1 A2 show abs(b-a) ≤ c
    using Int_ZF_1_3_L22 by simp
qed
```

### 35.4 Maximum and minimum of a set of integers

In this section we provide some sufficient conditions for integer subsets to have extrema (maxima and minima).

Finite nonempty subsets of integers attain maxima and minima.

```
theorem (in int0) Int_fin_have_max_min:
  assumes A1: A ∈ Fin(ℤ) and A2: A≠0
  shows
    HasAmaximum(IntegerOrder,A)
    HasAminimum(IntegerOrder,A)
    Maximum(IntegerOrder,A) ∈ A
```

```

Minimum(IntegerOrder,A) ∈ A
∀x∈A. x ≤ Maximum(IntegerOrder,A)
∀x∈A. Minimum(IntegerOrder,A) ≤ x
Maximum(IntegerOrder,A) ∈ ℤ
Minimum(IntegerOrder,A) ∈ ℤ
proof -
  from A1 have
    A=0 ∨ HasAmaximum(IntegerOrder,A) and
    A=0 ∨ HasAminimum(IntegerOrder,A)
  using Int_ZF_2_T1 Int_ZF_2_L6 Finite_ZF_1_1_T1A Finite_ZF_1_1_T1B
  by auto
with A2 show
  HasAmaximum(IntegerOrder,A)
  HasAminimum(IntegerOrder,A)
  by auto
from A1 A2 show
  Maximum(IntegerOrder,A) ∈ A
  Minimum(IntegerOrder,A) ∈ A
  ∀x∈A. x ≤ Maximum(IntegerOrder,A)
  ∀x∈A. Minimum(IntegerOrder,A) ≤ x
  using Int_ZF_2_T1 Finite_ZF_1_T2 by auto
moreover from A1 have A⊆ℤ using FinD by simp
ultimately show
  Maximum(IntegerOrder,A) ∈ ℤ
  Minimum(IntegerOrder,A) ∈ ℤ
  by auto
qed

```

Bounded nonempty integer subsets attain maximum and minimum.

```

theorem (in int0) Int_bounded_have_max_min:
  assumes IsBounded(A,IntegerOrder) and A≠0
  shows
    HasAmaximum(IntegerOrder,A)
    HasAminimum(IntegerOrder,A)
    Maximum(IntegerOrder,A) ∈ A
    Minimum(IntegerOrder,A) ∈ A
    ∀x∈A. x ≤ Maximum(IntegerOrder,A)
    ∀x∈A. Minimum(IntegerOrder,A) ≤ x
    Maximum(IntegerOrder,A) ∈ ℤ
    Minimum(IntegerOrder,A) ∈ ℤ
  using assms Int_fin_have_max_min Int_bounded_iff_fin
  by auto

```

Nonempty set of integers that is bounded below attains its minimum.

```

theorem (in int0) int_bounded_below_has_min:
  assumes A1: IsBoundedBelow(A,IntegerOrder) and A2: A≠0
  shows
    HasAminimum(IntegerOrder,A)
    Minimum(IntegerOrder,A) ∈ A

```

```

 $\forall x \in A. \text{Minimum}(\text{IntegerOrder}, A) \leq x$ 
proof -
  from A1 A2 have
    IntegerOrder {is total on}  $\mathbb{Z}$ 
    trans(IntegerOrder)
    IntegerOrder  $\subseteq \mathbb{Z} \times \mathbb{Z}$ 
     $\forall A. \text{IsBounded}(A, \text{IntegerOrder}) \wedge A \neq 0 \longrightarrow \text{HasAminimum}(\text{IntegerOrder}, A)$ 
     $A \neq 0 \text{ IsBoundedBelow}(A, \text{IntegerOrder})$ 
    using Int_ZF_2_T1 Int_ZF_2_L6 Int_ZF_2_L1B Int_bounded_have_max_min
    by auto
  then show HasAminimum(IntegerOrder, A)
    by (rule Order_ZF_4_L11)
  then show
    Minimum(IntegerOrder, A)  $\in A$ 
     $\forall x \in A. \text{Minimum}(\text{IntegerOrder}, A) \leq x$ 
    using Int_ZF_2_L4 Order_ZF_4_L4 by auto
qed

```

Nonempty set of integers that is bounded above attains its maximum.

```

theorem (in int0) int_bounded_above_has_max:
  assumes A1: IsBoundedAbove(A, IntegerOrder) and A2:  $A \neq 0$ 
  shows
    HasAmaximum(IntegerOrder, A)
    Maximum(IntegerOrder, A)  $\in A$ 
    Maximum(IntegerOrder, A)  $\in \mathbb{Z}$ 
     $\forall x \in A. x \leq \text{Maximum}(\text{IntegerOrder}, A)$ 
proof -
  from A1 A2 have
    IntegerOrder {is total on}  $\mathbb{Z}$ 
    trans(IntegerOrder) and
    I: IntegerOrder  $\subseteq \mathbb{Z} \times \mathbb{Z}$  and
     $\forall A. \text{IsBounded}(A, \text{IntegerOrder}) \wedge A \neq 0 \longrightarrow \text{HasAmaximum}(\text{IntegerOrder}, A)$ 
     $A \neq 0 \text{ IsBoundedAbove}(A, \text{IntegerOrder})$ 
    using Int_ZF_2_T1 Int_ZF_2_L6 Int_ZF_2_L1B Int_bounded_have_max_min
    by auto
  then show HasAmaximum(IntegerOrder, A)
    by (rule Order_ZF_4_L11A)
  then show
    II: Maximum(IntegerOrder, A)  $\in A$  and
     $\forall x \in A. x \leq \text{Maximum}(\text{IntegerOrder}, A)$ 
    using Int_ZF_2_L4 Order_ZF_4_L3 by auto
  from I A1 have  $A \subseteq \mathbb{Z}$  by (rule Order_ZF_3_L1A)
  with II show Maximum(IntegerOrder, A)  $\in \mathbb{Z}$  by auto
qed

```

A set defined by separation over a bounded set attains its maximum and minimum.

```

lemma (in int0) Int_ZF_1_4_L1:

```

```

assumes A1: IsBounded(A,IntegerOrder) and A2: A≠0
and A3:  $\forall q \in \mathbb{Z}. F(q) \in \mathbb{Z}$ 
and A4:  $K = \{F(q). q \in A\}$ 
shows
HasAmaximum(IntegerOrder,K)
HasAminimum(IntegerOrder,K)
Maximum(IntegerOrder,K)  $\in K$ 
Minimum(IntegerOrder,K)  $\in K$ 
Maximum(IntegerOrder,K)  $\in \mathbb{Z}$ 
Minimum(IntegerOrder,K)  $\in \mathbb{Z}$ 
 $\forall q \in A. F(q) \leq \text{Maximum(IntegerOrder,K)}$ 
 $\forall q \in A. \text{Minimum(IntegerOrder,K)} \leq F(q)$ 
IsBounded(K,IntegerOrder)
proof -
  from A1 have A  $\in \text{Fin}(\mathbb{Z})$  using Int_bounded_iff_fin
  by simp
  with A3 have  $\{F(q). q \in A\} \in \text{Fin}(\mathbb{Z})$ 
  by (rule fin_image_fin)
  with A2 A4 have T1:  $K \in \text{Fin}(\mathbb{Z})$   $K \neq 0$  by auto
  then show T2:
    HasAmaximum(IntegerOrder,K)
    HasAminimum(IntegerOrder,K)
    and Maximum(IntegerOrder,K)  $\in K$ 
    Minimum(IntegerOrder,K)  $\in K$ 
    Maximum(IntegerOrder,K)  $\in \mathbb{Z}$ 
    Minimum(IntegerOrder,K)  $\in \mathbb{Z}$ 
    using Int_fin_have_max_min by auto
  { fix q assume  $q \in A$ 
    with A4 have  $F(q) \in K$  by auto
    with T1 have
       $F(q) \leq \text{Maximum(IntegerOrder,K)}$ 
       $\text{Minimum(IntegerOrder,K)} \leq F(q)$ 
      using Int_fin_have_max_min by auto
    } then show
       $\forall q \in A. F(q) \leq \text{Maximum(IntegerOrder,K)}$ 
       $\forall q \in A. \text{Minimum(IntegerOrder,K)} \leq F(q)$ 
    by auto
  from T2 show IsBounded(K,IntegerOrder)
    using Order_ZF_4_L7 Order_ZF_4_L8A IsBounded_def
    by simp
qed

```

A three element set has a maximum and minimum.

```

lemma (in int0) Int_ZF_1_4_L1A: assumes A1:  $a \in \mathbb{Z}$   $b \in \mathbb{Z}$   $c \in \mathbb{Z}$ 
shows
Maximum(IntegerOrder,{a,b,c})  $\in \mathbb{Z}$ 
 $a \leq \text{Maximum(IntegerOrder,{a,b,c})}$ 
 $b \leq \text{Maximum(IntegerOrder,{a,b,c})}$ 
 $c \leq \text{Maximum(IntegerOrder,{a,b,c})}$ 

```

```
using assms Int_ZF_2_T1 Finite_ZF_1_L2A by auto
```

Integer functions attain maxima and minima over intervals.

```
lemma (in int0) Int_ZF_1_4_L2:
  assumes A1:  $f:\mathbb{Z}\rightarrow\mathbb{Z}$  and A2:  $a\leq b$ 
  shows
     $\max f(a..b) \in \mathbb{Z}$ 
     $\forall c \in a..b. f(c) \leq \max f(a..b)$ 
     $\exists c \in a..b. f(c) = \max f(a..b)$ 
     $\min f(a..b) \in \mathbb{Z}$ 
     $\forall c \in a..b. \min f(a..b) \leq f(c)$ 
     $\exists c \in a..b. f(c) = \min f(a..b)$ 
proof -
  from A2 have T:  $a \in \mathbb{Z} \quad b \in \mathbb{Z} \quad a..b \subseteq \mathbb{Z}$ 
  using Int_ZF_2_L1A Int_ZF_2_L1B Order_ZF_2_L6
  by auto
  with A1 A2 have
     $\text{Maximum}(\text{IntegerOrder}, f(a..b)) \in f(a..b)$ 
     $\forall x \in f(a..b). x \leq \text{Maximum}(\text{IntegerOrder}, f(a..b))$ 
     $\text{Maximum}(\text{IntegerOrder}, f(a..b)) \in \mathbb{Z}$ 
     $\text{Minimum}(\text{IntegerOrder}, f(a..b)) \in f(a..b)$ 
     $\forall x \in f(a..b). \text{Minimum}(\text{IntegerOrder}, f(a..b)) \leq x$ 
     $\text{Minimum}(\text{IntegerOrder}, f(a..b)) \in \mathbb{Z}$ 
  using Int_ZF_4_L8 Int_ZF_2_T1 group3.OrderedGroup_ZF_2_L6
  Int_fin_have_max_min by auto
  with A1 T show
     $\max f(a..b) \in \mathbb{Z}$ 
     $\forall c \in a..b. f(c) \leq \max f(a..b)$ 
     $\exists c \in a..b. f(c) = \max f(a..b)$ 
     $\min f(a..b) \in \mathbb{Z}$ 
     $\forall c \in a..b. \min f(a..b) \leq f(c)$ 
     $\exists c \in a..b. f(c) = \min f(a..b)$ 
  using func_imagedef by auto
qed
```

### 35.5 The set of nonnegative integers

The set of nonnegative integers looks like the set of natural numbers. We explore that in this section. We also rephrase some lemmas about the set of positive integers known from the theory of ordered groups.

The set of positive integers is closed under addition.

```
lemma (in int0) pos_int_closed_add:
  shows  $\mathbb{Z}_+$  {is closed under} IntegerAddition
  using Int_ZF_2_T1 group3.OrderedGroup_ZF_1_L13 by simp
```

Text expended version of the fact that the set of positive integers is closed under addition

```

lemma (in int0) pos_int_closed_add_unfolded:
  assumes a $\in\mathbb{Z}_+$  b $\in\mathbb{Z}_+$  shows a+b  $\in\mathbb{Z}_+$ 
  using assms pos_int_closed_add IsOpClosed_def
  by simp

```

$\mathbb{Z}^+$  is bounded below.

```

lemma (in int0) Int_ZF_1_5_L1: shows
  IsBoundedBelow( $\mathbb{Z}^+$ , IntegerOrder)
  IsBoundedBelow( $\mathbb{Z}_+$ , IntegerOrder)
  using Nonnegative_def PositiveSet_def IsBoundedBelow_def by auto

```

Subsets of  $\mathbb{Z}^+$  are bounded below.

```

lemma (in int0) Int_ZF_1_5_L1A: assumes A  $\subseteq\mathbb{Z}^+$ 
  shows IsBoundedBelow(A, IntegerOrder)
  using assms Int_ZF_1_5_L1 Order_ZF_3_L12 by blast

```

Subsets of  $\mathbb{Z}_+$  are bounded below.

```

lemma (in int0) Int_ZF_1_5_L1B: assumes A1: A  $\subseteq\mathbb{Z}_+$ 
  shows IsBoundedBelow(A, IntegerOrder)
  using A1 Int_ZF_1_5_L1 Order_ZF_3_L12 by blast

```

Every nonempty subset of positive integers has a minimum.

```

lemma (in int0) Int_ZF_1_5_L1C: assumes A  $\subseteq\mathbb{Z}_+$  and A  $\neq\emptyset$ 
  shows
    HasAminimum(IntegerOrder, A)
    Minimum(IntegerOrder, A)  $\in A$ 
     $\forall x\in A. \text{Minimum(IntegerOrder, A)} \leq x$ 
  using assms Int_ZF_1_5_L1B int_bounded_below_has_min by auto

```

Infinite subsets of  $\mathbb{Z}^+$  do not have a maximum - If  $A \subseteq \mathbb{Z}^+$  then for every integer we can find one in the set that is not smaller.

```

lemma (in int0) Int_ZF_1_5_L2:
  assumes A1: A  $\subseteq\mathbb{Z}^+$  and A2: A  $\notin \text{Fin}(\mathbb{Z})$  and A3: D $\in\mathbb{Z}$ 
  shows  $\exists n\in A. D\leq n$ 

```

**proof** -

```

{ assume  $\forall n\in A. \neg(D\leq n)$ 
  moreover from A1 A3 have D $\in\mathbb{Z}$   $\forall n\in A. n\in\mathbb{Z}$ 
    using Nonnegative_def by auto
  ultimately have  $\forall n\in A. n\leq D$ 
    using Int_ZF_2_L19 by blast
  hence  $\forall n\in A. \langle n, D \rangle \in \text{IntegerOrder}$  by simp
  then have IsBoundedAbove(A, IntegerOrder)
    by (rule Order_ZF_3_L10)
  with A1 have IsBounded(A, IntegerOrder)
    using Int_ZF_1_5_L1A IsBounded_def by simp
  with A2 have False using Int_bounded_iff_fin by auto
} thus thesis by auto

```

**qed**

Infinite subsets of  $\mathbb{Z}_+$  do not have a maximum - If  $A \subseteq \mathbb{Z}_+$  then for every integer we can find one in the set that is not smaller. This is very similar to Int\_ZF\_1\_5\_L2, except we have  $\mathbb{Z}_+$  instead of  $\mathbb{Z}^+$  here.

```

lemma (in int0) Int_ZF_1_5_L2A:
  assumes A1:  $A \subseteq \mathbb{Z}_+$  and A2:  $A \notin \text{Fin}(\mathbb{Z})$  and A3:  $D \in \mathbb{Z}$ 
  shows  $\exists n \in A. D \leq n$ 
proof -
{ assume  $\forall n \in A. \neg(D \leq n)$ 
  moreover from A1 A3 have  $D \in \mathbb{Z} \quad \forall n \in A. n \in \mathbb{Z}$ 
  using PositiveSet_def by auto
  ultimately have  $\forall n \in A. n \leq D$ 
  using Int_ZF_2_L19 by blast
  hence  $\forall n \in A. \langle n, D \rangle \in \text{IntegerOrder}$  by simp
  then have IsBoundedAbove(A, IntegerOrder)
    by (rule Order_ZF_3_L10)
  with A1 have IsBounded(A, IntegerOrder)
    using Int_ZF_1_5_L1B IsBounded_def by simp
  with A2 have False using Int_bounded_iff_fin by auto
} thus thesis by auto
qed

```

An integer is either positive, zero, or its opposite is positive.

```

lemma (in int0) Int_decomp: assumes  $m \in \mathbb{Z}$ 
  shows Exactly_1_of_3_holds ( $m=0, m \in \mathbb{Z}_+, (-m) \in \mathbb{Z}_+$ )
  using assms Int_ZF_2_T1 group3.OrdGroup_decomp
  by simp

```

An integer is zero, positive, or it's inverse is positive.

```

lemma (in int0) int_decomp_cases: assumes  $m \in \mathbb{Z}$ 
  shows  $m=0 \vee m \in \mathbb{Z}_+ \vee (-m) \in \mathbb{Z}_+$ 
  using assms Int_ZF_2_T1 group3.OrderedGroup_ZF_1_L14
  by simp

```

An integer is in the positive set iff it is greater or equal one.

```

lemma (in int0) Int_ZF_1_5_L3: shows  $m \in \mathbb{Z}_+ \longleftrightarrow 1 \leq m$ 
proof
  assume  $m \in \mathbb{Z}_+$  then have  $0 \leq m \quad m \neq 0$ 
  using PositiveSet_def by auto
  then have  $0+1 \leq m$ 
  using Int_ZF_4_L1B by auto
  then show  $1 \leq m$ 
  using int_zero_one_are_int Int_ZF_1_T2 group0.group0_2_L2
  by simp
next assume  $1 \leq m$ 
  then have  $m \in \mathbb{Z} \quad 0 \leq m \quad m \neq 0$ 
  using Int_ZF_2_L1A Int_ZF_2_L16C by auto
  then show  $m \in \mathbb{Z}_+$  using PositiveSet_def by auto
qed

```

The set of positive integers is closed under multiplication. The unfolded form.

```
lemma (in int0) pos_int_closed_mul_unfold:
  assumes a∈ℤ+ b∈ℤ+
  shows a·b ∈ ℤ+
  using assms Int_ZF_1_5_L3 Int_ZF_1_3_L3 by simp
```

The set of positive integers is closed under multiplication.

```
lemma (in int0) pos_int_closed_mul: shows
  ℤ+ {is closed under} IntegerMultiplication
  using pos_int_closed_mul_unfold IsOpClosed_def
  by simp
```

It is an overkill to prove that the ring of integers has no zero divisors this way, but why not?

```
lemma (in int0) int_has_no_zero_divs:
  shows HasNoZeroDivs(ℤ,IntegerAddition,IntegerMultiplication)
  using pos_int_closed_mul Int_ZF_1_3_T1 ring1.OrdRing_ZF_3_L3
  by simp
```

Nonnegative integers are positive ones plus zero.

```
lemma (in int0) Int_ZF_1_5_L3A: shows ℤ+ = ℤ+ ∪ {0}
  using Int_ZF_2_T1 group3.OrderedGroup_ZF_1_L24 by simp
```

We can make a function smaller than any constant on a given interval of positive integers by adding another constant.

```
lemma (in int0) Int_ZF_1_5_L4:
  assumes A1: f:ℤ→ℤ and A2: K∈ℤ N∈ℤ
  shows ∃C∈ℤ. ∀n∈ℤ+. K ≤ f(n) + C ⟶ N≤n
proof -
  from A2 have N≤1 ∨ 2≤N
    using int_zero_one_are_int no_int_between
    by simp
  moreover
  { assume A3: N≤1
    let C = 0
    have C ∈ ℤ using int_zero_one_are_int
      by simp
    moreover
    { fix n assume n∈ℤ+
      then have 1 ≤ n using Int_ZF_1_5_L3
    }
  } by simp
  with A3 have N≤n by (rule Int_order_transitive)
  } then have ∀n∈ℤ+. K ≤ f(n) + C ⟶ N≤n
    by auto
  ultimately have ∃C∈ℤ. ∀n∈ℤ+. K ≤ f(n) + C ⟶ N≤n
    by auto }
moreover
```



```

{ let C = K - 1 - maxf(f,1..(N-1))
  assume 2 ≤ N
  then have 2-1 ≤ N-1
    using int_zero_one_are_int Int_ZF_1_1_L4 int_ord_transl_inv
    by simp
  then have I: 1 ≤ N-1
    using int_zero_one_are_int Int_ZF_1_2_L3 by simp
  with A1 A2 have T:
    maxf(f,1..(N-1)) ∈ ℤ K-1 ∈ ℤ C ∈ ℤ
    using Int_ZF_1_4_L2 Int_ZF_1_1_L5 int_zero_one_are_int
    by auto
  moreover
  { fix n assume A4: n ∈ ℤ+
    { assume A5: K ≤ f(n) + C and ¬(N ≤ n)
  with A2 A4 have n ≤ N-1
    using PositiveSet_def Int_ZF_1_3_L6A by simp
  with A4 have n ∈ 1..(N-1)
    using Int_ZF_1_5_L3 Interval_def by auto
  with A1 I T have f(n)+C ≤ maxf(f,1..(N-1)) + C
    using Int_ZF_1_4_L2 int_ord_transl_inv by simp
  with T have f(n)+C ≤ K-1
    using Int_ZF_1_2_L3 by simp
  with A5 have K ≤ K-1
    by (rule Int_order_transitive)
  with A2 have False using Int_ZF_1_2_L3AA by simp
    } then have K ≤ f(n) + C → N ≤ n
  by auto
    } then have ∀n ∈ ℤ+. K ≤ f(n) + C → N ≤ n
    by simp
    ultimately have ∃C ∈ ℤ. ∀n ∈ ℤ+. K ≤ f(n) + C → N ≤ n
    by auto }
  ultimately show thesis by auto
qed

```

Absolute value is identity on positive integers.

```

lemma (in int0) Int_ZF_1_5_L4A:
  assumes a ∈ ℤ+ shows abs(a) = a
  using assms Int_ZF_2_T1 group3.OrderedGroup_ZF_3_L2B
  by simp

```

One and two are in  $\mathbb{Z}_+$ .

```

lemma (in int0) int_one_two_are_pos: shows 1 ∈ ℤ+ 2 ∈ ℤ+
  using int_zero_one_are_int int_ord_is_refl refl_def Int_ZF_1_5_L3
  Int_ZF_2_L16B by auto

```

The image of  $\mathbb{Z}_+$  by a function defined on integers is not empty.

```

lemma (in int0) Int_ZF_1_5_L5: assumes A1: f : ℤ → X
  shows f(ℤ+) ≠ 0
proof -

```

```

have  $\mathbb{Z}_+ \subseteq \mathbb{Z}$  using PositiveSet_def by auto
with A1 show  $f(\mathbb{Z}_+) \neq 0$ 
  using int_one_two_are_pos func_imagedef by auto
qed

```

If  $n$  is positive, then  $n - 1$  is nonnegative.

```

lemma (in int0) Int_ZF_1_5_L6: assumes A1:  $n \in \mathbb{Z}_+$ 
  shows
     $0 \leq n-1$ 
     $0 \in 0..(n-1)$ 
     $0..(n-1) \subseteq \mathbb{Z}$ 
proof -
  from A1 have  $1 \leq n$   $(-1) \in \mathbb{Z}$ 
    using Int_ZF_1_5_L3 int_zero_one_are_int Int_ZF_1_1_L4
    by auto
  then have  $1-1 \leq n-1$ 
    using int_ord_transl_inv by simp
  then show  $0 \leq n-1$ 
    using int_zero_one_are_int Int_ZF_1_1_L4 by simp
  then show  $0 \in 0..(n-1)$ 
    using int_zero_one_are_int int_ord_is_refl refl_def Order_ZF_2_L1B
    by simp
  show  $0..(n-1) \subseteq \mathbb{Z}$ 
    using Int_ZF_2_L1B Order_ZF_2_L6 by simp
qed

```

Intgers greater than one in  $\mathbb{Z}_+$  belong to  $\mathbb{Z}_+$ . This is a property of ordered groups and follows from OrderedGroup\_ZF\_1\_L19, but Isabelle's simplifier has problems using that result directly, so we reprove it specifically for integers.

```

lemma (in int0) Int_ZF_1_5_L7: assumes  $a \in \mathbb{Z}_+$  and  $a \leq b$ 
  shows  $b \in \mathbb{Z}_+$ 
proof-
  from assms have  $1 \leq a$   $a \leq b$ 
    using Int_ZF_1_5_L3 by auto
  then have  $1 \leq b$  by (rule Int_order_transitive)
  then show  $b \in \mathbb{Z}_+$  using Int_ZF_1_5_L3 by simp
qed

```

Adding a positive integer increases integers.

```

lemma (in int0) Int_ZF_1_5_L7A: assumes  $a \in \mathbb{Z}$   $b \in \mathbb{Z}_+$ 
  shows  $a \leq a+b$   $a \neq a+b$   $a+b \in \mathbb{Z}$ 
  using assms Int_ZF_2_T1 group3.OrderedGroup_ZF_1_L22
  by auto

```

For any integer  $m$  the greater of  $m$  and 1 is a positive integer that is greater or equal than  $m$ . If we add 1 to it we get a positive integer that is strictly greater than  $m$ .

```

lemma (in int0) Int_ZF_1_5_L7B: assumes  $a \in \mathbb{Z}$ 

```

```

shows
a ≤ GreaterOf(IntegerOrder,1,a)
GreaterOf(IntegerOrder,1,a) ∈ ℤ+
GreaterOf(IntegerOrder,1,a) + 1 ∈ ℤ+
a ≤ GreaterOf(IntegerOrder,1,a) + 1
a ≠ GreaterOf(IntegerOrder,1,a) + 1
using assms int_zero_not_one Int_ZF_1_3_T1 ring1.OrdRing_ZF_3_L12
by auto

```

The opposite of an element of  $\mathbb{Z}_+$  cannot belong to  $\mathbb{Z}_+$ .

```

lemma (in int0) Int_ZF_1_5_L8: assumes a ∈ ℤ+
  shows (-a) ∉ ℤ+
  using assms Int_ZF_2_T1 group3.OrderedGroup_ZF_1_L20
  by simp

```

For every integer there is one in  $\mathbb{Z}_+$  that is greater or equal.

```

lemma (in int0) Int_ZF_1_5_L9: assumes a ∈ ℤ
  shows ∃ b ∈ ℤ+. a ≤ b
  using assms int_not_trivial Int_ZF_2_T1 group3.OrderedGroup_ZF_1_L23
  by simp

```

A theorem about odd extensions. Recall from `OrdereGroup_ZF.thy` that the odd extension of an integer function  $f$  defined on  $\mathbb{Z}_+$  is the odd function on  $\mathbb{Z}$  equal to  $f$  on  $\mathbb{Z}_+$ . First we show that the odd extension is defined on  $\mathbb{Z}$ .

```

lemma (in int0) Int_ZF_1_5_L10: assumes f : ℤ+ → ℤ
  shows OddExtension(ℤ,IntegerAddition,IntegerOrder,f) : ℤ → ℤ
  using assms Int_ZF_2_T1 group3.odd_ext_props by simp

```

On  $\mathbb{Z}_+$ , the odd extension of  $f$  is the same as  $f$ .

```

lemma (in int0) Int_ZF_1_5_L11: assumes f : ℤ+ → ℤ and a ∈ ℤ+ and
  g = OddExtension(ℤ,IntegerAddition,IntegerOrder,f)
  shows g(a) = f(a)
  using assms Int_ZF_2_T1 group3.odd_ext_props by simp

```

On  $-\mathbb{Z}_+$ , the value of the odd extension of  $f$  is the negative of  $f(-a)$ .

```

lemma (in int0) Int_ZF_1_5_L12:
  assumes f : ℤ+ → ℤ and a ∈ (-ℤ+) and
  g = OddExtension(ℤ,IntegerAddition,IntegerOrder,f)
  shows g(a) = -(f(-a))
  using assms Int_ZF_2_T1 group3.odd_ext_props by simp

```

Odd extensions are odd on  $\mathbb{Z}$ .

```

lemma (in int0) int_oddext_is_odd:
  assumes f : ℤ+ → ℤ and a ∈ ℤ and
  g = OddExtension(ℤ,IntegerAddition,IntegerOrder,f)
  shows g(-a) = -(g(a))
  using assms Int_ZF_2_T1 group3.oddext_is_odd by simp

```

Alternative definition of an odd function.

```
lemma (in int0) Int_ZF_1_5_L13: assumes A1:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  shows
   $(\forall a \in \mathbb{Z}. f(-a) = (-f(a))) \longleftrightarrow (\forall a \in \mathbb{Z}. (-f(-a))) = f(a)$ 
  using assms Int_ZF_1_T2 group0.group0_6_L2 by simp
```

Another way of expressing the fact that odd extensions are odd.

```
lemma (in int0) int_oddext_is_odd_alt:
  assumes  $f: \mathbb{Z}_+ \rightarrow \mathbb{Z}$  and  $a \in \mathbb{Z}$  and
   $g = \text{OddExtension}(\mathbb{Z}, \text{IntegerAddition}, \text{IntegerOrder}, f)$ 
  shows  $(-g(-a)) = g(a)$ 
  using assms Int_ZF_2_T1 group3.oddext_is_odd_alt by simp
```

### 35.6 Functions with infinite limits

In this section we consider functions (integer sequences) that have infinite limits. An integer function has infinite positive limit if it is arbitrarily large for large enough arguments. Similarly, a function has infinite negative limit if it is arbitrarily small for small enough arguments. The material in this come mostly from the section in `OrderedGroup_ZF.thy` with the same title. Here we rewrite the theorems from that section in the notation we use for integers and add some results specific for the ordered group of integers.

If an image of a set by a function with infinite positive limit is bounded above, then the set itself is bounded above.

```
lemma (in int0) Int_ZF_1_6_L1: assumes  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  and
   $\forall a \in \mathbb{Z}. \exists b \in \mathbb{Z}_+. \forall x. b \leq x \longrightarrow a \leq f(x)$  and  $A \subseteq \mathbb{Z}$  and
   $\text{IsBoundedAbove}(f(A), \text{IntegerOrder})$ 
  shows  $\text{IsBoundedAbove}(A, \text{IntegerOrder})$ 
  using assms int_not_trivial Int_ZF_2_T1 group3.OrderedGroup_ZF_7_L1
  by simp
```

If an image of a set defined by separation by a function with infinite positive limit is bounded above, then the set itself is bounded above.

```
lemma (in int0) Int_ZF_1_6_L2: assumes A1:  $X \neq 0$  and A2:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  and
```

```
  A3:  $\forall a \in \mathbb{Z}. \exists b \in \mathbb{Z}_+. \forall x. b \leq x \longrightarrow a \leq f(x)$  and
  A4:  $\forall x \in X. b(x) \in \mathbb{Z} \wedge f(b(x)) \leq U$ 
  shows  $\exists u. \forall x \in X. b(x) \leq u$ 
```

**proof** -

```
  let  $G = \mathbb{Z}$ 
  let  $P = \text{IntegerAddition}$ 
  let  $r = \text{IntegerOrder}$ 
  from A1 A2 A3 A4 have
    group3( $G, P, r$ )
     $r \{ \text{is total on} \} G$ 
     $G \neq \{ \text{TheNeutralElement}(G, P) \}$ 
     $X \neq 0 \quad f: G \rightarrow G$ 
```

```

     $\forall a \in G. \exists b \in \text{PositiveSet}(G, P, r). \forall y. \langle b, y \rangle \in r \longrightarrow \langle a, f(y) \rangle \in r$ 
     $\forall x \in X. b(x) \in G \wedge \langle f(b(x)), U \rangle \in r$ 
    using int_not_trivial Int_ZF_2_T1 by auto
    then have  $\exists u. \forall x \in X. \langle b(x), u \rangle \in r$  by (rule group3.OrderedGroup_ZF_7_L2)
    thus thesis by simp
qed

```

If an image of a set defined by separation by a integer function with infinite negative limit is bounded below, then the set itself is bounded above. This is dual to Int\_ZF\_1\_6\_L2.

**lemma** (in int0) Int\_ZF\_1\_6\_L3: assumes A1:  $X \neq 0$  and A2:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  and

```

    A3:  $\forall a \in \mathbb{Z}. \exists b \in \mathbb{Z}_+. \forall y. b \leq y \longrightarrow f(-y) \leq a$  and
    A4:  $\forall x \in X. b(x) \in \mathbb{Z} \wedge L \leq f(b(x))$ 
    shows  $\exists 1. \forall x \in X. 1 \leq b(x)$ 

```

**proof** -

```

    let G =  $\mathbb{Z}$ 
    let P = IntegerAddition
    let r = IntegerOrder
    from A1 A2 A3 A4 have
      group3(G, P, r)
      r {is total on} G
       $G \neq \{\text{TheNeutralElement}(G, P)\}$ 
       $X \neq 0$  f:  $G \rightarrow G$ 
       $\forall a \in G. \exists b \in \text{PositiveSet}(G, P, r). \forall y. \langle b, y \rangle \in r \longrightarrow \langle f(\text{GroupInv}(G, P)(y)), a \rangle \in r$ 
       $\forall x \in X. b(x) \in G \wedge \langle L, f(b(x)) \rangle \in r$ 
      using int_not_trivial Int_ZF_2_T1 by auto
    then have  $\exists 1. \forall x \in X. \langle 1, b(x) \rangle \in r$  by (rule group3.OrderedGroup_ZF_7_L3)
    thus thesis by simp

```

qed

The next lemma combines Int\_ZF\_1\_6\_L2 and Int\_ZF\_1\_6\_L3 to show that if the image of a set defined by separation by a function with infinite limits is bounded, then the set itself is bounded. The proof again uses directly a fact from OrderedGroup\_ZF.

**lemma** (in int0) Int\_ZF\_1\_6\_L4:

```

    assumes A1:  $X \neq 0$  and A2:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  and
    A3:  $\forall a \in \mathbb{Z}. \exists b \in \mathbb{Z}_+. \forall x. b \leq x \longrightarrow a \leq f(x)$  and
    A4:  $\forall a \in \mathbb{Z}. \exists b \in \mathbb{Z}_+. \forall y. b \leq y \longrightarrow f(-y) \leq a$  and
    A5:  $\forall x \in X. b(x) \in \mathbb{Z} \wedge f(b(x)) \leq U \wedge L \leq f(b(x))$ 
    shows  $\exists M. \forall x \in X. \text{abs}(b(x)) \leq M$ 

```

**proof** -

```

    let G =  $\mathbb{Z}$ 
    let P = IntegerAddition
    let r = IntegerOrder
    from A1 A2 A3 A4 A5 have
      group3(G, P, r)

```

```

r {is total on} G
G ≠ {TheNeutralElement(G, P)}
X≠0 f: G→G
∀a∈G. ∃b∈PositiveSet(G, P, r). ∀y. ⟨b, y⟩ ∈ r → ⟨a, f(y)⟩ ∈ r
∀a∈G. ∃b∈PositiveSet(G, P, r). ∀y.
⟨b, y⟩ ∈ r → ⟨f(GroupInv(G, P)(y)), a⟩ ∈ r
∀x∈X. b(x) ∈ G ∧ ⟨L, f(b(x))⟩ ∈ r ∧ ⟨f(b(x)), U⟩ ∈ r
using int_not_trivial Int_ZF_2_T1 by auto
then have ∃M. ∀x∈X. ⟨AbsoluteValue(G, P, r) b(x), M⟩ ∈ r
by (rule group3.OrderedGroup_ZF_7_L4)
thus thesis by simp
qed

```

If a function is larger than some constant for arguments large enough, then the image of a set that is bounded below is bounded below. This is not true for ordered groups in general, but only for those for which bounded sets are finite. This does not require the function to have infinite limit, but such functions do have this property.

```

lemma (in int0) Int_ZF_1_6_L5:
  assumes A1: f: ℤ→ℤ and A2: N∈ℤ and
  A3: ∀m. N≤m → L ≤ f(m) and
  A4: IsBoundedBelow(A, IntegerOrder)
  shows IsBoundedBelow(f(A), IntegerOrder)
proof -
  from A2 A4 have A = {x∈A. x≤N} ∪ {x∈A. N≤x}
    using Int_ZF_2_T1 Int_ZF_2_L1C Order_ZF_1_L5
    by simp
  moreover have
    f({x∈A. x≤N} ∪ {x∈A. N≤x}) =
    f{x∈A. x≤N} ∪ f{x∈A. N≤x}
    by (rule image_Un)
  ultimately have f(A) = f{x∈A. x≤N} ∪ f{x∈A. N≤x}
    by simp
  moreover have IsBoundedBelow(f{x∈A. x≤N}, IntegerOrder)
  proof -
    let B = {x∈A. x≤N}
    from A4 have B ∈ Fin(ℤ)
      using Order_ZF_3_L16 Int_bounded_iff_fin by auto
    with A1 have IsBounded(f(B), IntegerOrder)
      using Finite1_L6A Int_bounded_iff_fin by simp
    then show IsBoundedBelow(f(B), IntegerOrder)
      using IsBounded_def by simp
  qed
  moreover have IsBoundedBelow(f{x∈A. N≤x}, IntegerOrder)
  proof -
    let C = {x∈A. N≤x}
    from A4 have C ⊆ ℤ using Int_ZF_2_L1C by auto
    with A1 A3 have ∀y ∈ f(C). ⟨L, y⟩ ∈ IntegerOrder
      using func_imagedef by simp
  qed

```

```

    then show IsBoundedBelow(f(C),IntegerOrder)
      by (rule Order_ZF_3_L9)
  qed
  ultimately show IsBoundedBelow(f(A),IntegerOrder)
    using Int_ZF_2_T1 Int_ZF_2_L6 Int_ZF_2_L1B Order_ZF_3_L6
    by simp
qed

```

A function that has an infinite limit can be made arbitrarily large on positive integers by adding a constant. This does not actually require the function to have infinite limit, just to be larger than a constant for arguments large enough.

```

lemma (in int0) Int_ZF_1_6_L6: assumes A1:  $N \in \mathbb{Z}$  and
  A2:  $\forall m. N \leq m \longrightarrow L \leq f(m)$  and
  A3:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  and A4:  $K \in \mathbb{Z}$ 
  shows  $\exists c \in \mathbb{Z}. \forall n \in \mathbb{Z}_+. K \leq f(n) + c$ 
proof -
  have IsBoundedBelow( $\mathbb{Z}_+$ ,IntegerOrder)
    using Int_ZF_1_5_L1 by simp
  with A3 A1 A2 have IsBoundedBelow(f( $\mathbb{Z}_+$ ),IntegerOrder)
    by (rule Int_ZF_1_6_L5)
  with A1 obtain I where I:  $\forall y \in f(\mathbb{Z}_+). 1 \leq y$ 
    using Int_ZF_1_5_L5 IsBoundedBelow_def by auto
  let c = K-1
  from A3 have f( $\mathbb{Z}_+$ )  $\neq 0$  using Int_ZF_1_5_L5
    by simp
  then have  $\exists y. y \in f(\mathbb{Z}_+)$  by (rule nonempty_has_element)
  then obtain y where y  $\in f(\mathbb{Z}_+)$  by auto
  with A4 I have T:  $1 \in \mathbb{Z} \quad c \in \mathbb{Z}$ 
    using Int_ZF_2_L1A Int_ZF_1_1_L5 by auto
  { fix n assume A5:  $n \in \mathbb{Z}_+$ 
    have  $\mathbb{Z}_+ \subseteq \mathbb{Z}$  using PositiveSet_def by auto
    with A3 I T A5 have  $1 + c \leq f(n) + c$ 
      using func_imagedef int_ord_transl_inv by auto
    with I T have  $1 + c \leq f(n) + c$ 
      using int_ord_transl_inv by simp
    with A4 T have  $K \leq f(n) + c$ 
      using Int_ZF_1_2_L3 by simp
  } then have  $\forall n \in \mathbb{Z}_+. K \leq f(n) + c$  by simp
  with T show thesis by auto
qed

```

If a function has infinite limit, then we can add such constant such that minimum of those arguments for which the function (plus the constant) is larger than another given constant is greater than a third constant. It is not as complicated as it sounds.

```

lemma (in int0) Int_ZF_1_6_L7:
  assumes A1:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  and A2:  $K \in \mathbb{Z} \quad N \in \mathbb{Z}$  and

```

```

A3:  $\forall a \in \mathbb{Z}. \exists b \in \mathbb{Z}_+. \forall x. b \leq x \longrightarrow a \leq f(x)$ 
shows  $\exists C \in \mathbb{Z}. N \leq \text{Minimum}(\text{IntegerOrder}, \{n \in \mathbb{Z}_+. K \leq f(n) + C\})$ 
proof -
  from A1 A2 have  $\exists C \in \mathbb{Z}. \forall n \in \mathbb{Z}_+. K \leq f(n) + C \longrightarrow N \leq n$ 
    using Int_ZF_1_5_L4 by simp
  then obtain C where I:  $C \in \mathbb{Z}$  and
    II:  $\forall n \in \mathbb{Z}_+. K \leq f(n) + C \longrightarrow N \leq n$ 
    by auto
  have antisym(IntegerOrder) using Int_ZF_2_L4 by simp
  moreover have HasAminimum(IntegerOrder,  $\{n \in \mathbb{Z}_+. K \leq f(n) + C\}$ )
  proof -
    from A2 A3 I have  $\exists n \in \mathbb{Z}_+. \forall x. n \leq x \longrightarrow K - C \leq f(x)$ 
      using Int_ZF_1_1_L5 by simp
    then obtain n where
       $n \in \mathbb{Z}_+$  and  $\forall x. n \leq x \longrightarrow K - C \leq f(x)$ 
      by auto
    with A2 I have
       $\{n \in \mathbb{Z}_+. K \leq f(n) + C\} \neq 0$ 
       $\{n \in \mathbb{Z}_+. K \leq f(n) + C\} \subseteq \mathbb{Z}_+$ 
      using int_ord_is_refl refl_def PositiveSet_def Int_ZF_2_L9C
      by auto
    then show HasAminimum(IntegerOrder,  $\{n \in \mathbb{Z}_+. K \leq f(n) + C\}$ )
      using Int_ZF_1_5_L1C by simp
  qed
  moreover from II have
     $\forall n \in \{n \in \mathbb{Z}_+. K \leq f(n) + C\}. \langle N, n \rangle \in \text{IntegerOrder}$ 
    by auto
  ultimately have
     $\langle N, \text{Minimum}(\text{IntegerOrder}, \{n \in \mathbb{Z}_+. K \leq f(n) + C\}) \rangle \in \text{IntegerOrder}$ 
    by (rule Order_ZF_4_L12)
  with I show thesis by auto
qed

```

For any integer  $m$  the function  $k \mapsto m \cdot k$  has an infinite limit (or negative of that). This is why we put some properties of these functions here, even though they properly belong to a (yet nonexistent) section on homomorphisms. The next lemma shows that the set  $\{a \cdot x : x \in \mathbb{Z}\}$  can finite only if  $a = 0$ .

```

lemma (in int0) Int_ZF_1_6_L8:
  assumes A1:  $a \in \mathbb{Z}$  and A2:  $\{a \cdot x. x \in \mathbb{Z}\} \in \text{Fin}(\mathbb{Z})$ 
  shows  $a = 0$ 
proof -
  from A1 have  $a = 0 \vee (a \leq -1) \vee (1 \leq a)$ 
    using Int_ZF_1_3_L6C by simp
  moreover
  { assume  $a \leq -1$ 
    then have  $\{a \cdot x. x \in \mathbb{Z}\} \notin \text{Fin}(\mathbb{Z})$ 
      using int_zero_not_one Int_ZF_1_3_T1 ring1.OrdRing_ZF_3_L6
      by simp
  }

```



```

    with A2 have False by simp }
moreover
{ assume 1 ≤ a
  then have {a·x. x∈ℤ} ∉ Fin(ℤ)
    using int_zero_not_one Int_ZF_1_3_T1 ring1.OrdRing_ZF_3_L5
    by simp
  with A2 have False by simp }
ultimately show a = 0 by auto
qed

```

### 35.7 Miscelaneous

In this section we put some technical lemmas needed in various other places that are hard to classify.

Suppose we have an integer expression (a meta-function)  $F$  such that  $F(p)|p|$  is bounded by a linear function of  $|p|$ , that is for some integers  $A, B$  we have  $F(p)|p| \leq A|p| + B$ . We show that  $F$  is then bounded. The proof is easy, we just divide both sides by  $|p|$  and take the limit (just kidding).

```

lemma (in int0) Int_ZF_1_7_L1:
  assumes A1:  $\forall q \in \mathbb{Z}. F(q) \in \mathbb{Z}$  and
  A2:  $\forall q \in \mathbb{Z}. F(q) \cdot \text{abs}(q) \leq A \cdot \text{abs}(q) + B$  and
  A3:  $A \in \mathbb{Z} \ B \in \mathbb{Z}$ 
  shows  $\exists L. \forall p \in \mathbb{Z}. F(p) \leq L$ 
proof -
  let I =  $(-\text{abs}(B)).. \text{abs}(B)$ 
  let K =  $\{F(q). q \in I\}$ 
  let M = Maximum(IntegerOrder, K)
  let L = GreaterOf(IntegerOrder, M, A+1)
  from A3 A1 have C1:
    IsBounded(I, IntegerOrder)
    I  $\neq$  0
     $\forall q \in \mathbb{Z}. F(q) \in \mathbb{Z}$ 
    K =  $\{F(q). q \in I\}$ 
    using Order_ZF_3_L11 Int_ZF_1_3_L17 by auto
  then have M  $\in \mathbb{Z}$  by (rule Int_ZF_1_4_L1)
  with A3 have T1:  $M \leq L \ A+1 \leq L$ 
    using int_zero_one_are_int Int_ZF_1_1_L5 Int_ZF_1_3_L18
    by auto
  from C1 have T2:  $\forall q \in I. F(q) \leq M$ 
    by (rule Int_ZF_1_4_L1)
  { fix p assume A4:  $p \in \mathbb{Z}$  have  $F(p) \leq L$ 
    proof -
      { assume  $\text{abs}(p) \leq \text{abs}(B)$ 
        with A4 T1 T2 have  $F(p) \leq M \ M \leq L$ 
          using Int_ZF_1_3_L19 by auto
        then have  $F(p) \leq L$  by (rule Int_order_transitive) }
      moreover
      { assume A5:  $\neg(\text{abs}(p) \leq \text{abs}(B))$ 

```

```

from A3 A2 A4 have
  A·abs(p) ∈ ℤ  F(p)·abs(p) ≤ A·abs(p) + B
  using Int_ZF_2_L14 Int_ZF_1_1_L5 by auto
moreover from A3 A4 A5 have B ≤ abs(p)
  using Int_ZF_1_3_L15 by simp
ultimately have
  F(p)·abs(p) ≤ A·abs(p) + abs(p)
  using Int_ZF_2_L15A by blast
with A3 A4 have F(p)·abs(p) ≤ (A+1)·abs(p)
  using Int_ZF_2_L14 Int_ZF_1_2_L7 by simp
moreover from A3 A1 A4 A5 have
  F(p) ∈ ℤ  A+1 ∈ ℤ  abs(p) ∈ ℤ
  ¬(abs(p) ≤ 0)
  using int_zero_one_are_int Int_ZF_1_1_L5 Int_ZF_2_L14 Int_ZF_1_3_L11
  by auto
ultimately have F(p) ≤ A+1
  using Int_ineq_simpl_positive by simp
moreover from T1 have A+1 ≤ L by simp
ultimately have F(p) ≤ L by (rule Int_order_transitive) }
  ultimately show thesis by blast
qed
} then have ∀p∈ℤ. F(p) ≤ L by simp
thus thesis by auto
qed

```

A lemma about splitting (not really, there is some overlap) the  $\mathbb{Z} \times \mathbb{Z}$  into six subsets (cases). The subsets are as follows: first and third quadrant, and second and fourth quadrant farther split by the  $b = -a$  line.

```

lemma (in int0) int_plane_split_in6: assumes a∈ℤ  b∈ℤ
  shows
    0≤a ∧ 0≤b  ∨  a≤0 ∧ b≤0  ∨
    a≤0 ∧ 0≤b ∧ 0 ≤ a+b  ∨  a≤0 ∧ 0≤b ∧ a+b ≤ 0  ∨
    0≤a ∧ b≤0 ∧ 0 ≤ a+b  ∨  0≤a ∧ b≤0 ∧ a+b ≤ 0
  using assms Int_ZF_2_T1 group3.OrdGroup_6cases by simp
end

```

## 36 IntDiv\_ZF\_IML.thy

**theory** IntDiv\_ZF\_IML **imports** Int\_ZF\_1 IntDiv\_ZF

**begin**

This theory translates some results from the Isabelle's IntDiv.thy theory to the notation used by IsarMathLib.

### 36.1 Quotient and remainder

For any integers  $m, n$ ,  $n > 0$  there are unique integers  $q, p$  such that  $0 \leq p < n$  and  $m = n \cdot q + p$ . Number  $p$  in this decomposition is usually called  $m \bmod n$ . Standard Isabelle denotes numbers  $q, p$  as  $m \text{ zdiv } n$  and  $m \text{ zmod } n$ , resp., and we will use the same notation.

The next lemma is sometimes called the "quotient-remainder theorem".

**lemma** (in int0) IntDiv\_ZF\_1\_L1: **assumes**  $m \in \mathbb{Z}$   $n \in \mathbb{Z}$   
**shows**  $m = n \cdot (m \text{ zdiv } n) + (m \text{ zmod } n)$   
**using** `assms Int_ZF_1_L2 raw_zmod_zdiv_equality`  
**by** `simp`

If  $n$  is greater than 0 then  $m \text{ zmod } n$  is between 0 and  $n - 1$ .

**lemma** (in int0) IntDiv\_ZF\_1\_L2:  
**assumes**  $A1: m \in \mathbb{Z}$  **and**  $A2: 0 \leq n$   $n \neq 0$   
**shows**  
 $0 \leq m \text{ zmod } n$   
 $m \text{ zmod } n \leq n$   $m \text{ zmod } n \neq n$   
 $m \text{ zmod } n \leq n-1$   
**proof** -  
**from**  $A2$  **have**  $T: n \in \mathbb{Z}$   
**using** `Int_ZF_2_L1A` **by** `simp`  
**from**  $A2$  **have**  $0 \leq n$  **using** `Int_ZF_2_L9 Int_ZF_1_L8`  
**by** `auto`  
**with**  $T$  **show**  
 $0 \leq m \text{ zmod } n$   
 $m \text{ zmod } n \leq n$   
 $m \text{ zmod } n \neq n$   
**using** `pos_mod Int_ZF_1_L8 Int_ZF_1_L8A zmod_type`  
`Int_ZF_2_L1 Int_ZF_2_L9AA`  
**by** `auto`  
**then show**  $m \text{ zmod } n \leq n-1$   
**using** `Int_ZF_4_L1B` **by** `auto`  
**qed**

$(m \cdot k) \text{ div } k = m$ .

**lemma** (in int0) IntDiv\_ZF\_1\_L3:  
**assumes**  $m \in \mathbb{Z}$   $k \in \mathbb{Z}$  **and**  $k \neq 0$

```

shows
(m·k) zdiv k = m
(k·m) zdiv k = m
using assms zdiv_zmult_self1 zdiv_zmult_self2
  Int_ZF_1_L8 Int_ZF_1_L2 by auto

```

The next lemma essentially translates `zdiv_mono1` from standard Isabelle to our notation.

```

lemma (in int0) IntDiv_ZF_1_L4:
  assumes A1:  $m \leq k$  and A2:  $0 \leq n$   $n \neq 0$ 
  shows  $m \text{ zdiv } n \leq k \text{ zdiv } n$ 
proof -
  from A2 have  $0 \leq n$   $0 \neq n$ 
    using Int_ZF_1_L8 by auto
  with A1 have
     $m \text{ zdiv } n \leq k \text{ zdiv } n$ 
     $m \text{ zdiv } n \in \mathbb{Z}$   $m \text{ zdiv } k \in \mathbb{Z}$ 
    using Int_ZF_2_L1A Int_ZF_2_L9 zdiv_mono1
    by auto
  then show  $(m \text{ zdiv } n) \leq (k \text{ zdiv } n)$ 
    using Int_ZF_2_L1 by simp
qed

```

A quotient-remainder theorem about integers greater than a given product.

```

lemma (in int0) IntDiv_ZF_1_L5:
  assumes A1:  $n \in \mathbb{Z}_+$  and A2:  $n \leq k$  and A3:  $k \cdot n \leq m$ 
  shows
     $m = n \cdot (m \text{ zdiv } n) + (m \text{ zmod } n)$ 
     $m = (m \text{ zdiv } n) \cdot n + (m \text{ zmod } n)$ 
     $(m \text{ zmod } n) \in 0..(n-1)$ 
     $k \leq (m \text{ zdiv } n)$ 
     $m \text{ zdiv } n \in \mathbb{Z}_+$ 
proof -
  from A2 A3 have T:
     $m \in \mathbb{Z}$   $n \in \mathbb{Z}$   $k \in \mathbb{Z}$   $m \text{ zdiv } n \in \mathbb{Z}$ 
    using Int_ZF_2_L1A by auto
  then show  $m = n \cdot (m \text{ zdiv } n) + (m \text{ zmod } n)$ 
    using IntDiv_ZF_1_L1 by simp
  with T show  $m = (m \text{ zdiv } n) \cdot n + (m \text{ zmod } n)$ 
    using Int_ZF_1_L4 by simp
  from A1 have I:  $0 \leq n$   $n \neq 0$ 
    using PositiveSet_def by auto
  with T show  $(m \text{ zmod } n) \in 0..(n-1)$ 
    using IntDiv_ZF_1_L2 Order_ZF_2_L1
    by simp
  from A3 I have  $(k \cdot n \text{ zdiv } n) \leq (m \text{ zdiv } n)$ 
    using IntDiv_ZF_1_L4 by simp
  with I T show  $k \leq (m \text{ zdiv } n)$ 
    using IntDiv_ZF_1_L3 by simp

```

```

      with A1 A2 show m zdiv n  $\in \mathbb{Z}_+$ 
        using Int_ZF_1_5_L7 by blast
    qed

end

```

## 37 Int\_ZF\_2.thy

`theory Int_ZF_2 imports func_ZF_1 Int_ZF_1 IntDiv_ZF_IML Group_ZF_3`

`begin`

In this theory file we consider the properties of integers that are needed for the real numbers construction in `Real_ZF` series.

### 37.1 Slopes

In this section we study basic properties of slopes - the integer almost homomorphisms. The general definition of an almost homomorphism  $f$  on a group  $G$  written in additive notation requires the set  $\{f(m+n) - f(m) - f(n) : m, n \in G\}$  to be finite. In this section we establish a definition that is equivalent for integers: that for all integer  $m, n$  we have  $|f(m+n) - f(m) - f(n)| \leq L$  for some  $L$ .

First we extend the standard notation for integers with notation related to slopes. We define slopes as almost homomorphisms on the additive group of integers. The set of slopes is denoted  $\mathcal{S}$ . We also define "positive" slopes as those that take infinite number of positive values on positive integers. We write  $\delta(s, m, n)$  to denote the homomorphism difference of  $s$  at  $m, n$  (i.e. the expression  $s(m+n) - s(m) - s(n)$ ). We denote  $\max \delta(s)$  the maximum absolute value of homomorphism difference of  $s$  as  $m, n$  range over integers. If  $s$  is a slope, then the set of homomorphism differences is finite and this maximum exists. In `Group_ZF_3` we define the equivalence relation on almost homomorphisms using the notion of a quotient group relation and use " $\approx$ " to denote it. As here this symbol seems to be hogged by the standard Isabelle, we will use " $\sim$ " instead " $\approx$ ". We show in this section that  $s \sim r$  iff for some  $L$  we have  $|s(m) - r(m)| \leq L$  for all integer  $m$ . The " $+$ " denotes the first operation on almost homomorphisms. For slopes this is addition of functions defined in the natural way. The " $\circ$ " symbol denotes the second operation on almost homomorphisms (see `Group_ZF_3` for definition), defined for the group of integers. In short " $\circ$ " is the composition of slopes. The " $^{-1}$ " symbol acts as an infix operator that assigns the value  $\min\{n \in \mathbb{Z}_+ : p \leq f(n)\}$  to a pair (of sets)  $f$  and  $p$ . In application  $f$  represents a function defined on  $\mathbb{Z}_+$  and  $p$  is a positive integer. We choose this notation because we use it to construct the right inverse in the ring of classes of slopes and show that this ring is in fact a field. To study the homomorphism difference of the function defined by  $p \mapsto f^{-1}(p)$  we introduce the symbol  $\varepsilon$  defined as  $\varepsilon(f, \langle m, n \rangle) = f^{-1}(m+n) - f^{-1}(m) - f^{-1}(n)$ . Of course the intention is to use the fact that  $\varepsilon(f, \langle m, n \rangle)$  is the homomorphism difference of the function  $g$  defined as  $g(m) = f^{-1}(m)$ . We also define  $\gamma(s, m, n)$  as the expression  $\delta(f, m, -n) + s(0) - \delta(f, n, -n)$ . This is useful because of the

identity  $f(m - n) = \gamma(m, n) + f(m) - f(n)$  that allows to obtain bounds on the value of a slope at the difference of two integers. For every integer  $m$  we introduce notation  $m^S$  defined by  $m^E(n) = m \cdot n$ . The mapping  $q \mapsto q^S$  embeds integers into  $\mathcal{S}$  preserving the order, (that is, maps positive integers into  $\mathcal{S}_+$ ).

```

locale int1 = int0 +

  fixes slopes ( $\mathcal{S}$  )
  defines slopes_def[simp]:  $\mathcal{S} \equiv \text{AlmostHoms}(\mathbb{Z}, \text{IntegerAddition})$ 

  fixes posslopes ( $\mathcal{S}_+$ )
  defines posslopes_def[simp]:  $\mathcal{S}_+ \equiv \{s \in \mathcal{S}. s(\mathbb{Z}_+) \cap \mathbb{Z}_+ \notin \text{Fin}(\mathbb{Z})\}$ 

  fixes  $\delta$ 
  defines  $\delta$ _def[simp]:  $\delta(s, m, n) \equiv s(m+n) - s(m) - s(n)$ 

  fixes maxhomdiff ( $\text{max}\delta$  )
  defines maxhomdiff_def[simp]:
   $\text{max}\delta(s) \equiv \text{Maximum}(\text{IntegerOrder}, \{\text{abs}(\delta(s, m, n)). \langle m, n \rangle \in \mathbb{Z} \times \mathbb{Z}\})$ 

  fixes AlEqRel
  defines AlEqRel_def[simp]:
   $\text{AlEqRel} \equiv \text{QuotientGroupRel}(\mathcal{S}, \text{AlHomOp1}(\mathbb{Z}, \text{IntegerAddition}), \text{FinRangeFunctions}(\mathbb{Z}, \mathbb{Z}))$ 

  fixes AlEq (infix  $\sim$  68)
  defines AlEq_def[simp]:  $s \sim r \equiv \langle s, r \rangle \in \text{AlEqRel}$ 

  fixes slope_add (infix  $+$  70)
  defines slope_add_def[simp]:  $s + r \equiv \text{AlHomOp1}(\mathbb{Z}, \text{IntegerAddition}) \langle s, r \rangle$ 

  fixes slope_comp (infix  $\circ$  70)
  defines slope_comp_def[simp]:  $s \circ r \equiv \text{AlHomOp2}(\mathbb{Z}, \text{IntegerAddition}) \langle$ 
 $s, r \rangle$ 

  fixes neg (-_ [90] 91)
  defines neg_def[simp]:  $-s \equiv \text{GroupInv}(\mathbb{Z}, \text{IntegerAddition}) \ 0 \ s$ 

  fixes slope_inv (infix  $^{-1}$  71)
  defines slope_inv_def[simp]:
   $f^{-1}(p) \equiv \text{Minimum}(\text{IntegerOrder}, \{n \in \mathbb{Z}_+. p \leq f(n)\})$ 
  fixes  $\varepsilon$ 
  defines  $\varepsilon$ _def[simp]:
   $\varepsilon(f, p) \equiv f^{-1}(\text{fst}(p) + \text{snd}(p)) - f^{-1}(\text{fst}(p)) - f^{-1}(\text{snd}(p))$ 

  fixes  $\gamma$ 
  defines  $\gamma$ _def[simp]:
   $\gamma(s, m, n) \equiv \delta(s, m, -n) - \delta(s, n, -n) + s(0)$ 

```

```

fixes intembed ( $_S$ )
defines intembed_def[simp]:  $m^S \equiv \{\langle n, m \cdot n \rangle. n \in \mathbb{Z}\}$ 

```

We can use theorems proven in the `group1` context.

```

lemma (in int1) Int_ZF_2_1_L1: shows group1( $\mathbb{Z}$ , IntegerAddition)
  using Int_ZF_1_T2 group1_axioms.intro group1_def by simp

```

Type information related to the homomorphism difference expression.

```

lemma (in int1) Int_ZF_2_1_L2: assumes  $f \in S$  and  $n \in \mathbb{Z}$   $m \in \mathbb{Z}$ 
  shows
     $m + n \in \mathbb{Z}$ 
     $f(m + n) \in \mathbb{Z}$ 
     $f(m) \in \mathbb{Z}$     $f(n) \in \mathbb{Z}$ 
     $f(m) + f(n) \in \mathbb{Z}$ 
     $\text{HomDiff}(\mathbb{Z}, \text{IntegerAddition}, f, \langle m, n \rangle) \in \mathbb{Z}$ 
  using assms Int_ZF_2_1_L1 group1.Group_ZF_3_2_L4A
  by auto

```

Type information related to the homomorphism difference expression.

```

lemma (in int1) Int_ZF_2_1_L2A:
  assumes  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  and  $n \in \mathbb{Z}$     $m \in \mathbb{Z}$ 
  shows
     $m + n \in \mathbb{Z}$ 
     $f(m + n) \in \mathbb{Z}$     $f(m) \in \mathbb{Z}$     $f(n) \in \mathbb{Z}$ 
     $f(m) + f(n) \in \mathbb{Z}$ 
     $\text{HomDiff}(\mathbb{Z}, \text{IntegerAddition}, f, \langle m, n \rangle) \in \mathbb{Z}$ 
  using assms Int_ZF_2_1_L1 group1.Group_ZF_3_2_L4
  by auto

```

Slopes map integers into integers.

```

lemma (in int1) Int_ZF_2_1_L2B:
  assumes A1:  $f \in S$  and A2:  $m \in \mathbb{Z}$ 
  shows  $f(m) \in \mathbb{Z}$ 
proof -
  from A1 have  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  using AlmostHoms_def by simp
  with A2 show  $f(m) \in \mathbb{Z}$  using apply_funtype by simp
qed

```

The homomorphism difference in multiplicative notation is defined as the expression  $s(m \cdot n) \cdot (s(m) \cdot s(n))^{-1}$ . The next lemma shows that in the additive notation used for integers the homomorphism difference is  $f(m + n) - f(m) - f(n)$  which we denote as  $\delta(f, m, n)$ .

```

lemma (in int1) Int_ZF_2_1_L3:
  assumes  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  and  $m \in \mathbb{Z}$     $n \in \mathbb{Z}$ 
  shows  $\text{HomDiff}(\mathbb{Z}, \text{IntegerAddition}, f, \langle m, n \rangle) = \delta(f, m, n)$ 
  using assms Int_ZF_2_1_L2A Int_ZF_1_T2 group0.group0_4_L4A
    HomDiff_def by auto

```



The next formula restates the definition of the homomorphism difference to express the value an almost homomorphism on a sum.

```

lemma (in int1) Int_ZF_2_1_L3A:
  assumes A1:  $f \in S$  and A2:  $m \in \mathbb{Z} \quad n \in \mathbb{Z}$ 
  shows
     $f(m+n) = f(m) + (f(n) + \delta(f, m, n))$ 
proof -
  from A1 A2 have
    T:  $f(m) \in \mathbb{Z} \quad f(n) \in \mathbb{Z} \quad \delta(f, m, n) \in \mathbb{Z}$  and
     $\text{HomDiff}(\mathbb{Z}, \text{IntegerAddition}, f, \langle m, n \rangle) = \delta(f, m, n)$ 
  using Int_ZF_2_1_L2 AlmostHoms_def Int_ZF_2_1_L3 by auto
  with A1 A2 show  $f(m+n) = f(m) + (f(n) + \delta(f, m, n))$ 
  using Int_ZF_2_1_L3 Int_ZF_1_L3
    Int_ZF_2_1_L1 group1.Group_ZF_3_4_L1
  by simp
qed

```

The homomorphism difference of any integer function is integer.

```

lemma (in int1) Int_ZF_2_1_L3B:
  assumes  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  and  $m \in \mathbb{Z} \quad n \in \mathbb{Z}$ 
  shows  $\delta(f, m, n) \in \mathbb{Z}$ 
  using assms Int_ZF_2_1_L2A Int_ZF_2_1_L3 by simp

```

The value of an integer function at a sum expressed in terms of  $\delta$ .

```

lemma (in int1) Int_ZF_2_1_L3C: assumes A1:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  and A2:  $m \in \mathbb{Z} \quad n \in \mathbb{Z}$ 
  shows  $f(m+n) = \delta(f, m, n) + f(n) + f(m)$ 
proof -
  from A1 A2 have T:
     $\delta(f, m, n) \in \mathbb{Z} \quad f(m+n) \in \mathbb{Z} \quad f(m) \in \mathbb{Z} \quad f(n) \in \mathbb{Z}$ 
  using Int_ZF_1_1_L5 apply_funtype by auto
  then show  $f(m+n) = \delta(f, m, n) + f(n) + f(m)$ 
  using Int_ZF_1_2_L15 by simp
qed

```

The next lemma presents two ways the set of homomorphism differences can be written.

```

lemma (in int1) Int_ZF_2_1_L4: assumes A1:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$ 
  shows  $\{\text{abs}(\text{HomDiff}(\mathbb{Z}, \text{IntegerAddition}, f, x)) \mid x \in \mathbb{Z} \times \mathbb{Z}\} =$ 
 $\{\text{abs}(\delta(f, m, n)) \mid \langle m, n \rangle \in \mathbb{Z} \times \mathbb{Z}\}$ 
proof -
  from A1 have  $\forall m \in \mathbb{Z}. \forall n \in \mathbb{Z}.
    \text{abs}(\text{HomDiff}(\mathbb{Z}, \text{IntegerAddition}, f, \langle m, n \rangle)) = \text{abs}(\delta(f, m, n))$ 
  using Int_ZF_2_1_L3 by simp
  then show thesis by (rule ZF1_1_L4A)
qed

```

If  $f$  maps integers into integers and for all  $m, n \in \mathbb{Z}$  we have  $|f(m+n) - f(m) - f(n)| \leq L$  for some  $L$ , then  $f$  is a slope.

```

lemma (in int1) Int_ZF_2_1_L5: assumes A1:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$ 
  and A2:  $\forall m \in \mathbb{Z}. \forall n \in \mathbb{Z}. \text{abs}(\delta(f, m, n)) \leq L$ 
  shows  $f \in \mathcal{S}$ 
proof -
  let Abs = AbsoluteValue( $\mathbb{Z}$ , IntegerAddition, IntegerOrder)
  have group3( $\mathbb{Z}$ , IntegerAddition, IntegerOrder)
    IntegerOrder {is total on}  $\mathbb{Z}$ 
    using Int_ZF_2_T1 by auto
  moreover from A1 A2 have
     $\forall x \in \mathbb{Z} \times \mathbb{Z}. \text{HomDiff}(\mathbb{Z}, \text{IntegerAddition}, f, x) \in \mathbb{Z} \wedge$ 
     $\langle \text{Abs}(\text{HomDiff}(\mathbb{Z}, \text{IntegerAddition}, f, x)), L \rangle \in \text{IntegerOrder}$ 
    using Int_ZF_2_1_L2A Int_ZF_2_1_L3 by auto
  ultimately have
    IsBounded( $\{\text{HomDiff}(\mathbb{Z}, \text{IntegerAddition}, f, x). x \in \mathbb{Z} \times \mathbb{Z}\}$ , IntegerOrder)
    by (rule group3.OrderedGroup_ZF_3_L9A)
  with A1 show  $f \in \mathcal{S}$  using Int_bounded_iff_fin AlmostHoms_def
    by simp
qed

```

The absolute value of homomorphism difference of a slope  $s$  does not exceed  $\max \delta(s)$ .

```

lemma (in int1) Int_ZF_2_1_L7:
  assumes A1:  $s \in \mathcal{S}$  and A2:  $n \in \mathbb{Z} \quad m \in \mathbb{Z}$ 
  shows
     $\text{abs}(\delta(s, m, n)) \leq \max \delta(s)$ 
     $\delta(s, m, n) \in \mathbb{Z} \quad \max \delta(s) \in \mathbb{Z}$ 
     $(-\max \delta(s)) \leq \delta(s, m, n)$ 
proof -
  from A1 A2 show T:  $\delta(s, m, n) \in \mathbb{Z}$ 
    using Int_ZF_2_1_L2 Int_ZF_1_1_L5 by simp
  let A =  $\{\text{abs}(\text{HomDiff}(\mathbb{Z}, \text{IntegerAddition}, s, x)). x \in \mathbb{Z} \times \mathbb{Z}\}$ 
  let B =  $\{\text{abs}(\delta(s, m, n)). \langle m, n \rangle \in \mathbb{Z} \times \mathbb{Z}\}$ 
  let d =  $\text{abs}(\delta(s, m, n))$ 
  have IsLinOrder( $\mathbb{Z}$ , IntegerOrder) using Int_ZF_2_T1
    by simp
  moreover have  $A \in \text{Fin}(\mathbb{Z})$ 
proof -
  have  $\forall k \in \mathbb{Z}. \text{abs}(k) \in \mathbb{Z}$  using Int_ZF_2_L14 by simp
  moreover from A1 have
     $\{\text{HomDiff}(\mathbb{Z}, \text{IntegerAddition}, s, x). x \in \mathbb{Z} \times \mathbb{Z}\} \in \text{Fin}(\mathbb{Z})$ 
    using AlmostHoms_def by simp
  ultimately show  $A \in \text{Fin}(\mathbb{Z})$  by (rule Finite1_L6C)
qed
  moreover have  $A \neq \emptyset$  by auto
  ultimately have  $\forall k \in A. \langle k, \text{Maximum}(\text{IntegerOrder}, A) \rangle \in \text{IntegerOrder}$ 
    by (rule Finite_ZF_1_T2)
  moreover from A1 A2 have  $d \in A$  using AlmostHoms_def Int_ZF_2_1_L4
    by auto
  ultimately have  $d \leq \text{Maximum}(\text{IntegerOrder}, A)$  by auto

```

```

with A1 show  $d \leq \max \delta(s)$   $\max \delta(s) \in \mathbb{Z}$ 
  using AlmostHoms_def Int_ZF_2_1_L4 Int_ZF_2_L1A
  by auto
with T show  $(-\max \delta(s)) \leq \delta(s, m, n)$ 
  using Int_ZF_1_3_L19 by simp
qed

```

A useful estimate for the value of a slope at 0, plus some type information for slopes.

```

lemma (in int1) Int_ZF_2_1_L8: assumes A1:  $s \in \mathcal{S}$ 
  shows
     $\text{abs}(s(0)) \leq \max \delta(s)$ 
     $0 \leq \max \delta(s)$ 
     $\text{abs}(s(0)) \in \mathbb{Z}$   $\max \delta(s) \in \mathbb{Z}$ 
     $\text{abs}(s(0)) + \max \delta(s) \in \mathbb{Z}$ 
  proof -
    from A1 have  $s(0) \in \mathbb{Z}$ 
      using int_zero_one_are_int Int_ZF_2_1_L2B by simp
    then have I:  $0 \leq \text{abs}(s(0))$ 
      and  $\text{abs}(\delta(s, 0, 0)) = \text{abs}(s(0))$ 
      using int_abs_nonneg int_zero_one_are_int Int_ZF_1_1_L4
        Int_ZF_2_L17 by auto
    moreover from A1 have  $\text{abs}(\delta(s, 0, 0)) \leq \max \delta(s)$ 
      using int_zero_one_are_int Int_ZF_2_1_L7 by simp
    ultimately show II:  $\text{abs}(s(0)) \leq \max \delta(s)$ 
      by simp
    with I show  $0 \leq \max \delta(s)$  by (rule Int_order_transitive)
    with II show
       $\max \delta(s) \in \mathbb{Z}$   $\text{abs}(s(0)) \in \mathbb{Z}$ 
       $\text{abs}(s(0)) + \max \delta(s) \in \mathbb{Z}$ 
      using Int_ZF_2_L1A Int_ZF_1_1_L5 by auto
  qed

```

In `Group_ZF_3.thy` we show that finite range functions valued in an abelian group form a normal subgroup of almost homomorphisms. This allows to define the equivalence relation between almost homomorphisms as the relation resulting from dividing by that normal subgroup. Then we show in `Group_ZF_3_4_L12` that if the difference of  $f$  and  $g$  has finite range (actually  $f(n) \cdot g(n)^{-1}$  as we use multiplicative notation in `Group_ZF_3.thy`), then  $f$  and  $g$  are equivalent. The next lemma translates that fact into the notation used in `int1` context.

```

lemma (in int1) Int_ZF_2_1_L9: assumes A1:  $s \in \mathcal{S}$   $r \in \mathcal{S}$ 
  and A2:  $\forall m \in \mathbb{Z}. \text{abs}(s(m) - r(m)) \leq L$ 
  shows  $s \sim r$ 
  proof -
    from A1 A2 have
       $\forall m \in \mathbb{Z}. s(m) - r(m) \in \mathbb{Z} \wedge \text{abs}(s(m) - r(m)) \leq L$ 
      using Int_ZF_2_1_L2B Int_ZF_1_1_L5 by simp
  qed

```

```

then have
  IsBounded({s(n)-r(n). n∈ℤ}, IntegerOrder)
  by (rule Int_ZF_1_3_L20)
with A1 show s ~ r using Int_bounded_iff_fin
  Int_ZF_2_1_L1 group1.Group_ZF_3_4_L12 by simp
qed

```

A necessary condition for two slopes to be almost equal. For slopes the definition postulates the set  $\{f(m) - g(m) : m \in \mathbb{Z}\}$  to be finite. This lemma shows that this implies that  $|f(m) - g(m)|$  is bounded (by some integer) as  $m$  varies over integers. We also mention here that in this context  $s \sim r$  implies that both  $s$  and  $r$  are slopes.

```

lemma (in int1) Int_ZF_2_1_L9A: assumes s ~ r
  shows
    ∃L∈ℤ. ∀m∈ℤ. abs(s(m)-r(m)) ≤ L
  s∈S r∈S
  using assms Int_ZF_2_1_L1 group1.Group_ZF_3_4_L11
    Int_ZF_1_3_L20AA QuotientGroupRel_def by auto

```

Let's recall that the relation of almost equality is an equivalence relation on the set of slopes.

```

lemma (in int1) Int_ZF_2_1_L9B: shows
  A1EqRel ⊆ S×S
  equiv(S,A1EqRel)
  using Int_ZF_2_1_L1 group1.Group_ZF_3_3_L3 by auto

```

Another version of sufficient condition for two slopes to be almost equal: if the difference of two slopes is a finite range function, then they are almost equal.

```

lemma (in int1) Int_ZF_2_1_L9C: assumes s∈S r∈S and
  s + (-r) ∈ FinRangeFunctions(ℤ,ℤ)
  shows
    s ~ r
    r ~ s
  using assms Int_ZF_2_1_L1
    group1.Group_ZF_3_2_L13 group1.Group_ZF_3_4_L12A
  by auto

```

If two slopes are almost equal, then the difference has finite range. This is the inverse of Int\_ZF\_2\_1\_L9C.

```

lemma (in int1) Int_ZF_2_1_L9D: assumes A1: s ~ r
  shows s + (-r) ∈ FinRangeFunctions(ℤ,ℤ)
proof -
  let G = ℤ
  let f = IntegerAddition
  from A1 have A1HomOp1(G, f)⟨s, GroupInv(AlmostHoms(G, f), A1HomOp1(G, f))(r)⟩

```

```

    ∈ FinRangeFunctions(G, G)
    using Int_ZF_2_1_L1 group1.Group_ZF_3_4_L12B by auto
with A1 show s + (-r) ∈ FinRangeFunctions( $\mathbb{Z}$ ,  $\mathbb{Z}$ )
    using Int_ZF_2_1_L9A Int_ZF_2_1_L1 group1.Group_ZF_3_2_L13
    by simp
qed

```

What is the value of a composition of slopes?

```

lemma (in int1) Int_ZF_2_1_L10:
  assumes s ∈  $\mathcal{S}$  r ∈  $\mathcal{S}$  and m ∈  $\mathbb{Z}$ 
  shows (s ∘ r)(m) = s(r(m)) s(r(m)) ∈  $\mathbb{Z}$ 
  using assms Int_ZF_2_1_L1 group1.Group_ZF_3_4_L2 by auto

```

Composition of slopes is a slope.

```

lemma (in int1) Int_ZF_2_1_L11:
  assumes s ∈  $\mathcal{S}$  r ∈  $\mathcal{S}$ 
  shows s ∘ r ∈  $\mathcal{S}$ 
  using assms Int_ZF_2_1_L1 group1.Group_ZF_3_4_T1 by simp

```

Negative of a slope is a slope.

```

lemma (in int1) Int_ZF_2_1_L12: assumes s ∈  $\mathcal{S}$  shows -s ∈  $\mathcal{S}$ 
  using assms Int_ZF_1_T2 Int_ZF_2_1_L1 group1.Group_ZF_3_2_L13
  by simp

```

What is the value of a negative of a slope?

```

lemma (in int1) Int_ZF_2_1_L12A:
  assumes s ∈  $\mathcal{S}$  and m ∈  $\mathbb{Z}$  shows (-s)(m) = -(s(m))
  using assms Int_ZF_2_1_L1 group1.Group_ZF_3_2_L5
  by simp

```

What are the values of a sum of slopes?

```

lemma (in int1) Int_ZF_2_1_L12B: assumes s ∈  $\mathcal{S}$  r ∈  $\mathcal{S}$  and m ∈  $\mathbb{Z}$ 
  shows (s+r)(m) = s(m) + r(m)
  using assms Int_ZF_2_1_L1 group1.Group_ZF_3_2_L12
  by simp

```

Sum of slopes is a slope.

```

lemma (in int1) Int_ZF_2_1_L12C: assumes s ∈  $\mathcal{S}$  r ∈  $\mathcal{S}$ 
  shows s+r ∈  $\mathcal{S}$ 
  using assms Int_ZF_2_1_L1 group1.Group_ZF_3_2_L16
  by simp

```

A simple but useful identity.

```

lemma (in int1) Int_ZF_2_1_L13:
  assumes s ∈  $\mathcal{S}$  and n ∈  $\mathbb{Z}$  m ∈  $\mathbb{Z}$ 
  shows s(n·m) + (s(m) +  $\delta$ (s, n·m, m)) = s((n+1)·m)
  using assms Int_ZF_1_1_L5 Int_ZF_2_1_L2B Int_ZF_1_2_L9 Int_ZF_1_2_L7
  by simp

```

Some estimates for the absolute value of a slope at the opposite integer.

```

lemma (in int1) Int_ZF_2_1_L14: assumes A1:  $s \in \mathcal{S}$  and A2:  $m \in \mathbb{Z}$ 
  shows
     $s(-m) = s(0) - \delta(s, m, -m) - s(m)$ 
     $\text{abs}(s(m) + s(-m)) \leq 2 \cdot \max \delta(s)$ 
     $\text{abs}(s(-m)) \leq 2 \cdot \max \delta(s) + \text{abs}(s(m))$ 
     $s(-m) \leq \text{abs}(s(0)) + \max \delta(s) - s(m)$ 
  proof -
    from A1 A2 have T:
       $(-m) \in \mathbb{Z}$   $\text{abs}(s(m)) \in \mathbb{Z}$   $s(0) \in \mathbb{Z}$   $\text{abs}(s(0)) \in \mathbb{Z}$ 
       $\delta(s, m, -m) \in \mathbb{Z}$   $s(m) \in \mathbb{Z}$   $s(-m) \in \mathbb{Z}$ 
       $-(s(m)) \in \mathbb{Z}$   $s(0) - \delta(s, m, -m) \in \mathbb{Z}$ 
      using Int_ZF_1_1_L4 Int_ZF_2_1_L2B Int_ZF_2_L14 Int_ZF_2_1_L2
      Int_ZF_1_1_L5 int_zero_one_are_int by auto
    with A2 show I:  $s(-m) = s(0) - \delta(s, m, -m) - s(m)$ 
      using Int_ZF_1_1_L4 Int_ZF_1_2_L15 by simp
    from T have  $\text{abs}(s(0) - \delta(s, m, -m)) \leq \text{abs}(s(0)) + \text{abs}(\delta(s, m, -m))$ 
      using Int_triangle_ineq1 by simp
    moreover from A1 A2 T have  $\text{abs}(s(0)) + \text{abs}(\delta(s, m, -m)) \leq 2 \cdot \max \delta(s)$ 
      using Int_ZF_2_1_L7 Int_ZF_2_1_L8 Int_ZF_1_3_L21 by simp
    ultimately have  $\text{abs}(s(0) - \delta(s, m, -m)) \leq 2 \cdot \max \delta(s)$ 
      by (rule Int_order_transitive)
    moreover
    from I have  $s(m) + s(-m) = s(m) + (s(0) - \delta(s, m, -m) - s(m))$ 
      by simp
    with T have  $\text{abs}(s(m) + s(-m)) = \text{abs}(s(0) - \delta(s, m, -m))$ 
      using Int_ZF_1_2_L3 by simp
    ultimately show  $\text{abs}(s(m) + s(-m)) \leq 2 \cdot \max \delta(s)$ 
      by simp
    from I have  $\text{abs}(s(-m)) = \text{abs}(s(0) - \delta(s, m, -m) - s(m))$ 
      by simp
    with T have
       $\text{abs}(s(-m)) \leq \text{abs}(s(0)) + \text{abs}(\delta(s, m, -m)) + \text{abs}(s(m))$ 
      using int_triangle_ineq3 by simp
    moreover from A1 A2 T have
       $\text{abs}(s(0)) + \text{abs}(\delta(s, m, -m)) + \text{abs}(s(m)) \leq 2 \cdot \max \delta(s) + \text{abs}(s(m))$ 
      using Int_ZF_2_1_L7 Int_ZF_2_1_L8 Int_ZF_1_3_L21 int_ord_transl_inv
    by simp
    ultimately show  $\text{abs}(s(-m)) \leq 2 \cdot \max \delta(s) + \text{abs}(s(m))$ 
      by (rule Int_order_transitive)
    from T have  $s(0) - \delta(s, m, -m) \leq \text{abs}(s(0)) + \text{abs}(\delta(s, m, -m))$ 
      using Int_ZF_2_L15E by simp
    moreover from A1 A2 T have
       $\text{abs}(s(0)) + \text{abs}(\delta(s, m, -m)) \leq \text{abs}(s(0)) + \max \delta(s)$ 
      using Int_ZF_2_1_L7 int_ord_transl_inv by simp
    ultimately have  $s(0) - \delta(s, m, -m) \leq \text{abs}(s(0)) + \max \delta(s)$ 
      by (rule Int_order_transitive)
    with T have
       $s(0) - \delta(s, m, -m) - s(m) \leq \text{abs}(s(0)) + \max \delta(s) - s(m)$ 

```

```

    using int_ord_transl_inv by simp
  with I show  $s(-m) \leq \text{abs}(s(0)) + \max \delta(s) - s(m)$ 
    by simp
qed

```

An identity that expresses the value of an integer function at the opposite integer in terms of the value of that function at the integer, zero, and the homomorphism difference. We have a similar identity in `Int_ZF_2_1_L14`, but over there we assume that  $f$  is a slope.

```

lemma (in int1) Int_ZF_2_1_L14A: assumes A1:  $f:\mathbb{Z}\rightarrow\mathbb{Z}$  and A2:  $m\in\mathbb{Z}$ 
  shows  $f(-m) = (-\delta(f,m,-m)) + f(0) - f(m)$ 
proof -
  from A1 A2 have T:
     $f(-m) \in \mathbb{Z} \quad \delta(f,m,-m) \in \mathbb{Z} \quad f(0) \in \mathbb{Z} \quad f(m) \in \mathbb{Z}$ 
    using Int_ZF_1_1_L4 Int_ZF_1_1_L5 int_zero_one_are_int apply_funtype

    by auto
  with A2 show  $f(-m) = (-\delta(f,m,-m)) + f(0) - f(m)$ 
    using Int_ZF_1_1_L4 Int_ZF_1_2_L15 by simp
qed

```

The next lemma allows to use the expression  $\max f(f, 0..M-1)$ . Recall that  $\max f(f, A)$  is the maximum of (function)  $f$  on (the set)  $A$ .

```

lemma (in int1) Int_ZF_2_1_L15:
  assumes  $s\in\mathcal{S}$  and  $M \in \mathbb{Z}_+$ 
  shows
     $\max f(s, 0..(M-1)) \in \mathbb{Z}$ 
     $\forall n \in 0..(M-1). s(n) \leq \max f(s, 0..(M-1))$ 
     $\min f(s, 0..(M-1)) \in \mathbb{Z}$ 
     $\forall n \in 0..(M-1). \min f(s, 0..(M-1)) \leq s(n)$ 
  using assms AlmostHoms_def Int_ZF_1_5_L6 Int_ZF_1_4_L2
  by auto

```

A lower estimate for the value of a slope at  $nM + k$ .

```

lemma (in int1) Int_ZF_2_1_L16:
  assumes A1:  $s\in\mathcal{S}$  and A2:  $m\in\mathbb{Z}$  and A3:  $M \in \mathbb{Z}_+$  and A4:  $k \in 0..(M-1)$ 
  shows  $s(m\cdot M) + (\min f(s, 0..(M-1)) - \max \delta(s)) \leq s(m\cdot M + k)$ 
proof -
  from A3 have  $0..(M-1) \subseteq \mathbb{Z}$ 
    using Int_ZF_1_5_L6 by simp
  with A1 A2 A3 A4 have T:  $m\cdot M \in \mathbb{Z} \quad k \in \mathbb{Z} \quad s(m\cdot M) \in \mathbb{Z}$ 
    using PositiveSet_def Int_ZF_1_1_L5 Int_ZF_2_1_L2B
    by auto
  with A1 A3 A4 have
     $s(m\cdot M) + (\min f(s, 0..(M-1)) - \max \delta(s)) \leq s(m\cdot M) + (s(k) + \delta(s, m\cdot M, k))$ 
    using Int_ZF_2_1_L15 Int_ZF_2_1_L7 int_ineq_add_sides int_ord_transl_inv
    by simp
  with A1 T show thesis using Int_ZF_2_1_L3A by simp

```

qed

Identity is a slope.

```
lemma (in int1) Int_ZF_2_1_L17: shows  $\text{id}(\mathbb{Z}) \in \mathcal{S}$ 
  using Int_ZF_2_1_L1 group1.Group_ZF_3_4_L15 by simp
```

Simple identities about (absolute value of) homomorphism differences.

```
lemma (in int1) Int_ZF_2_1_L18:
  assumes A1:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  and A2:  $m \in \mathbb{Z} \quad n \in \mathbb{Z}$ 
  shows
     $\text{abs}(f(n) + f(m) - f(m+n)) = \text{abs}(\delta(f, m, n))$ 
     $\text{abs}(f(m) + f(n) - f(m+n)) = \text{abs}(\delta(f, m, n))$ 
     $(-(f(m))) - f(n) + f(m+n) = \delta(f, m, n)$ 
     $(-(f(n))) - f(m) + f(m+n) = \delta(f, m, n)$ 
     $\text{abs}((-f(m+n)) + f(m) + f(n)) = \text{abs}(\delta(f, m, n))$ 
  proof -
    from A1 A2 have T:
       $f(m+n) \in \mathbb{Z} \quad f(m) \in \mathbb{Z} \quad f(n) \in \mathbb{Z}$ 
       $f(m+n) - f(m) - f(n) \in \mathbb{Z}$ 
       $(-(f(m))) \in \mathbb{Z}$ 
       $(-f(m+n)) + f(m) + f(n) \in \mathbb{Z}$ 
      using apply_funtype Int_ZF_1_1_L4 Int_ZF_1_1_L5 by auto
    then have
       $\text{abs}(-(f(m+n) - f(m) - f(n))) = \text{abs}(f(m+n) - f(m) - f(n))$ 
      using Int_ZF_2_L17 by simp
    moreover from T have
       $(-(f(m+n) - f(m) - f(n))) = f(n) + f(m) - f(m+n)$ 
      using Int_ZF_1_2_L9A by simp
    ultimately show  $\text{abs}(f(n) + f(m) - f(m+n)) = \text{abs}(\delta(f, m, n))$ 
      by simp
    moreover from T have  $f(n) + f(m) = f(m) + f(n)$ 
      using Int_ZF_1_1_L5 by simp
    ultimately show  $\text{abs}(f(m) + f(n) - f(m+n)) = \text{abs}(\delta(f, m, n))$ 
      by simp
    from T show
       $(-(f(m))) - f(n) + f(m+n) = \delta(f, m, n)$ 
       $(-(f(n))) - f(m) + f(m+n) = \delta(f, m, n)$ 
      using Int_ZF_1_2_L9 by auto
    from T have
       $\text{abs}((-f(m+n)) + f(m) + f(n)) =$ 
       $\text{abs}(-((-f(m+n)) + f(m) + f(n)))$ 
      using Int_ZF_2_L17 by simp
    also from T have
       $\text{abs}(-((-f(m+n)) + f(m) + f(n))) = \text{abs}(\delta(f, m, n))$ 
      using Int_ZF_1_2_L9 by simp
    finally show  $\text{abs}((-f(m+n)) + f(m) + f(n)) = \text{abs}(\delta(f, m, n))$ 
      by simp
  qed
```

qed

Some identities about the homomorphism difference of odd functions.



```

lemma (in int1) Int_ZF_2_1_L19:
  assumes A1:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  and A2:  $\forall x \in \mathbb{Z}. (-f(-x)) = f(x)$ 
  and A3:  $m \in \mathbb{Z} \quad n \in \mathbb{Z}$ 
  shows
     $\text{abs}(\delta(f, -m, m+n)) = \text{abs}(\delta(f, m, n))$ 
     $\text{abs}(\delta(f, -n, m+n)) = \text{abs}(\delta(f, m, n))$ 
     $\delta(f, n, -(m+n)) = \delta(f, m, n)$ 
     $\delta(f, m, -(m+n)) = \delta(f, m, n)$ 
     $\text{abs}(\delta(f, -m, -n)) = \text{abs}(\delta(f, m, n))$ 
  proof -
    from A1 A2 A3 show
       $\text{abs}(\delta(f, -m, m+n)) = \text{abs}(\delta(f, m, n))$ 
       $\text{abs}(\delta(f, -n, m+n)) = \text{abs}(\delta(f, m, n))$ 
      using Int_ZF_1_2_L3 Int_ZF_2_1_L18 by auto
    from A3 have T:  $m+n \in \mathbb{Z}$  using Int_ZF_1_1_L5 by simp
    from A1 A2 have I:  $\forall x \in \mathbb{Z}. f(-x) = (-f(x))$ 
      using Int_ZF_1_5_L13 by simp
    with A1 A2 A3 T show
       $\delta(f, n, -(m+n)) = \delta(f, m, n)$ 
       $\delta(f, m, -(m+n)) = \delta(f, m, n)$ 
      using Int_ZF_1_2_L3 Int_ZF_2_1_L18 by auto
    from A3 have
       $\text{abs}(\delta(f, -m, -n)) = \text{abs}(f(-(m+n)) - f(-m) - f(-n))$ 
      using Int_ZF_1_1_L5 by simp
    also from A1 A2 A3 T I have ... =  $\text{abs}(\delta(f, m, n))$ 
      using Int_ZF_2_1_L18 by simp
    finally show  $\text{abs}(\delta(f, -m, -n)) = \text{abs}(\delta(f, m, n))$  by simp
  qed

```

Recall that  $f$  is a slope iff  $f(m+n) - f(m) - f(n)$  is bounded as  $m, n$  ranges over integers. The next lemma is the first step in showing that we only need to check this condition as  $m, n$  ranges over positive integers. Namely we show that if the condition holds for positive integers, then it holds if one integer is positive and the second one is nonnegative.

```

lemma (in int1) Int_ZF_2_1_L20: assumes A1:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  and
  A2:  $\forall a \in \mathbb{Z}_+. \forall b \in \mathbb{Z}_+. \text{abs}(\delta(f, a, b)) \leq L$  and
  A3:  $m \in \mathbb{Z}^+ \quad n \in \mathbb{Z}_+$ 
  shows
     $0 \leq L$ 
     $\text{abs}(\delta(f, m, n)) \leq L + \text{abs}(f(0))$ 
  proof -
    from A1 A2 have
       $\delta(f, 1, 1) \in \mathbb{Z}$  and  $\text{abs}(\delta(f, 1, 1)) \leq L$ 
      using int_one_two_are_pos PositiveSet_def Int_ZF_2_1_L3B
      by auto
    then show I:  $0 \leq L$  using Int_ZF_1_3_L19 by simp
    from A1 A3 have T:
       $n \in \mathbb{Z} \quad f(n) \in \mathbb{Z} \quad f(0) \in \mathbb{Z}$ 
       $\delta(f, m, n) \in \mathbb{Z} \quad \text{abs}(\delta(f, m, n)) \in \mathbb{Z}$ 

```

```

    using PositiveSet_def int_zero_one_are_int apply_funtype
    Nonnegative_def Int_ZF_2_1_L3B Int_ZF_2_L14 by auto
from A3 have m=0  $\vee$   $m \in \mathbb{Z}_+$  using Int_ZF_1_5_L3A by auto
moreover
{ assume m = 0
  with T I have  $\text{abs}(\delta(f,m,n)) \leq L + \text{abs}(f(0))$ 
    using Int_ZF_1_1_L4 Int_ZF_1_2_L3 Int_ZF_2_L17
int_ord_is_refl refl_def Int_ZF_2_L15F by simp }
moreover
{ assume  $m \in \mathbb{Z}_+$ 
  with A2 A3 T have  $\text{abs}(\delta(f,m,n)) \leq L + \text{abs}(f(0))$ 
    using int_abs_nonneg Int_ZF_2_L15F by simp }
ultimately show  $\text{abs}(\delta(f,m,n)) \leq L + \text{abs}(f(0))$ 
  by auto
qed

```

If the slope condition holds for all pairs of integers such that one integer is positive and the second one is nonnegative, then it holds when both integers are nonnegative.

**lemma** (in int1) Int\_ZF\_2\_1\_L21: assumes A1:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  and  
 A2:  $\forall a \in \mathbb{Z}^+. \forall b \in \mathbb{Z}_+. \text{abs}(\delta(f,a,b)) \leq L$  and  
 A3:  $n \in \mathbb{Z}^+ \quad m \in \mathbb{Z}^+$   
 shows  $\text{abs}(\delta(f,m,n)) \leq L + \text{abs}(f(0))$

**proof** -

```

from A1 A2 have
   $\delta(f,1,1) \in \mathbb{Z}$  and  $\text{abs}(\delta(f,1,1)) \leq L$ 
  using int_one_two_are_pos PositiveSet_def Nonnegative_def Int_ZF_2_1_L3B
  by auto
then have I:  $0 \leq L$  using Int_ZF_1_3_L19 by simp
from A1 A3 have T:
   $m \in \mathbb{Z} \quad f(m) \in \mathbb{Z} \quad f(0) \in \mathbb{Z} \quad (-f(0)) \in \mathbb{Z}$ 
   $\delta(f,m,n) \in \mathbb{Z} \quad \text{abs}(\delta(f,m,n)) \in \mathbb{Z}$ 
  using int_zero_one_are_int apply_funtype Nonnegative_def
    Int_ZF_2_1_L3B Int_ZF_2_L14 Int_ZF_1_1_L4 by auto
from A3 have n=0  $\vee$   $n \in \mathbb{Z}_+$  using Int_ZF_1_5_L3A by auto
moreover
{ assume n=0
  with T have  $\delta(f,m,n) = -f(0)$ 
    using Int_ZF_1_1_L4 by simp
  with T have  $\text{abs}(\delta(f,m,n)) = \text{abs}(f(0))$ 
    using Int_ZF_2_L17 by simp
  with T have  $\text{abs}(\delta(f,m,n)) \leq \text{abs}(f(0))$ 
    using int_ord_is_refl refl_def by simp
  with T I have  $\text{abs}(\delta(f,m,n)) \leq L + \text{abs}(f(0))$ 
    using Int_ZF_2_L15F by simp }
moreover
{ assume  $n \in \mathbb{Z}_+$ 
  with A2 A3 T have  $\text{abs}(\delta(f,m,n)) \leq L + \text{abs}(f(0))$ 
    using int_abs_nonneg Int_ZF_2_L15F by simp }

```

ultimately show  $\text{abs}(\delta(f,m,n)) \leq L + \text{abs}(f(0))$   
 by auto  
 qed

If the homomorphism difference is bounded on  $\mathbb{Z}_+ \times \mathbb{Z}_+$ , then it is bounded on  $\mathbb{Z}^+ \times \mathbb{Z}^+$ .

lemma (in int1) Int\_ZF\_2\_1\_L22: assumes A1:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  and  
 A2:  $\forall a \in \mathbb{Z}_+. \forall b \in \mathbb{Z}_+. \text{abs}(\delta(f,a,b)) \leq L$   
 shows  $\exists M. \forall m \in \mathbb{Z}^+. \forall n \in \mathbb{Z}^+. \text{abs}(\delta(f,m,n)) \leq M$   
 proof -  
 from A1 A2 have  
 $\forall m \in \mathbb{Z}^+. \forall n \in \mathbb{Z}^+. \text{abs}(\delta(f,m,n)) \leq L + \text{abs}(f(0)) + \text{abs}(f(0))$   
 using Int\_ZF\_2\_1\_L20 Int\_ZF\_2\_1\_L21 by simp  
 then show thesis by auto  
 qed

For odd functions we can do better than in Int\_ZF\_2\_1\_L22: if the homomorphism difference of  $f$  is bounded on  $\mathbb{Z}^+ \times \mathbb{Z}^+$ , then it is bounded on  $\mathbb{Z} \times \mathbb{Z}$ , hence  $f$  is a slope. Loong prof by splitting the  $\mathbb{Z} \times \mathbb{Z}$  into six subsets.

lemma (in int1) Int\_ZF\_2\_1\_L23: assumes A1:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  and  
 A2:  $\forall a \in \mathbb{Z}_+. \forall b \in \mathbb{Z}_+. \text{abs}(\delta(f,a,b)) \leq L$   
 and A3:  $\forall x \in \mathbb{Z}. (-f(-x)) = f(x)$   
 shows  $f \in \mathcal{S}$   
 proof -  
 from A1 A2 have  
 $\exists M. \forall a \in \mathbb{Z}^+. \forall b \in \mathbb{Z}^+. \text{abs}(\delta(f,a,b)) \leq M$   
 by (rule Int\_ZF\_2\_1\_L22)  
 then obtain M where I:  $\forall m \in \mathbb{Z}^+. \forall n \in \mathbb{Z}^+. \text{abs}(\delta(f,m,n)) \leq M$   
 by auto  
 { fix a b assume A4:  $a \in \mathbb{Z} \quad b \in \mathbb{Z}$   
 then have  
 $0 \leq a \wedge 0 \leq b \vee a \leq 0 \wedge b \leq 0 \vee$   
 $a \leq 0 \wedge 0 \leq b \wedge 0 \leq a+b \vee a \leq 0 \wedge 0 \leq b \wedge a+b \leq 0 \vee$   
 $0 \leq a \wedge b \leq 0 \wedge 0 \leq a+b \vee 0 \leq a \wedge b \leq 0 \wedge a+b \leq 0$   
 using int\_plane\_split\_in6 by simp  
 moreover  
 { assume  $0 \leq a \wedge 0 \leq b$   
 then have  $a \in \mathbb{Z}^+ \quad b \in \mathbb{Z}^+$   
 using Int\_ZF\_2\_L16 by auto  
 with I have  $\text{abs}(\delta(f,a,b)) \leq M$  by simp }  
 moreover  
 { assume  $a \leq 0 \wedge b \leq 0$   
 with I have  $\text{abs}(\delta(f,-a,-b)) \leq M$   
 using Int\_ZF\_2\_L10A Int\_ZF\_2\_L16 by simp  
 with A1 A3 A4 have  $\text{abs}(\delta(f,a,b)) \leq M$   
 using Int\_ZF\_2\_1\_L19 by simp }  
 moreover  
 { assume  $a \leq 0 \wedge 0 \leq b \wedge 0 \leq a+b$   
 with I have  $\text{abs}(\delta(f,-a,a+b)) \leq M$

```

using Int_ZF_2_L10A Int_ZF_2_L16 by simp
  with A1 A3 A4 have  $\text{abs}(\delta(f,a,b)) \leq M$ 
using Int_ZF_2_1_L19 by simp }
  moreover
  { assume  $a \leq 0 \wedge 0 \leq b \wedge a+b \leq 0$ 
    with I have  $\text{abs}(\delta(f,b,-(a+b))) \leq M$ 
using Int_ZF_2_L10A Int_ZF_2_L16 by simp
  with A1 A3 A4 have  $\text{abs}(\delta(f,a,b)) \leq M$ 
using Int_ZF_2_1_L19 by simp }
  moreover
  { assume  $0 \leq a \wedge b \leq 0 \wedge 0 \leq a+b$ 
    with I have  $\text{abs}(\delta(f,-b,a+b)) \leq M$ 
using Int_ZF_2_L10A Int_ZF_2_L16 by simp
  with A1 A3 A4 have  $\text{abs}(\delta(f,a,b)) \leq M$ 
using Int_ZF_2_1_L19 by simp }
  moreover
  { assume  $0 \leq a \wedge b \leq 0 \wedge a+b \leq 0$ 
    with I have  $\text{abs}(\delta(f,a,-(a+b))) \leq M$ 
using Int_ZF_2_L10A Int_ZF_2_L16 by simp
  with A1 A3 A4 have  $\text{abs}(\delta(f,a,b)) \leq M$ 
using Int_ZF_2_1_L19 by simp }
  ultimately have  $\text{abs}(\delta(f,a,b)) \leq M$  by auto }
  then have  $\forall m \in \mathbb{Z}. \forall n \in \mathbb{Z}. \text{abs}(\delta(f,m,n)) \leq M$  by simp
  with A1 show  $f \in \mathcal{S}$  by (rule Int_ZF_2_1_L5)
qed

```

If the homomorphism difference of a function defined on positive integers is bounded, then the odd extension of this function is a slope.

```

lemma (in int1) Int_ZF_2_1_L24:
  assumes A1:  $f: \mathbb{Z}_+ \rightarrow \mathbb{Z}$  and A2:  $\forall a \in \mathbb{Z}_+. \forall b \in \mathbb{Z}_+. \text{abs}(\delta(f,a,b)) \leq L$ 
  shows OddExtension( $\mathbb{Z}$ , IntegerAddition, IntegerOrder, f)  $\in \mathcal{S}$ 
proof -
  let g = OddExtension( $\mathbb{Z}$ , IntegerAddition, IntegerOrder, f)
  from A1 have g :  $\mathbb{Z} \rightarrow \mathbb{Z}$ 
  using Int_ZF_1_5_L10 by simp
  moreover have  $\forall a \in \mathbb{Z}_+. \forall b \in \mathbb{Z}_+. \text{abs}(\delta(g,a,b)) \leq L$ 
  proof -
    { fix a b assume A3:  $a \in \mathbb{Z}_+ \quad b \in \mathbb{Z}_+$ 
      with A1 have  $\text{abs}(\delta(f,a,b)) = \text{abs}(\delta(g,a,b))$ 
using pos_int_closed_add_unfolded Int_ZF_1_5_L11
by simp
      moreover from A2 A3 have  $\text{abs}(\delta(f,a,b)) \leq L$  by simp
      ultimately have  $\text{abs}(\delta(g,a,b)) \leq L$  by simp
    } then show thesis by simp
  qed
  moreover from A1 have  $\forall x \in \mathbb{Z}. (-g(-x)) = g(x)$ 
  using int_oddext_is_odd_alt by simp
  ultimately show  $g \in \mathcal{S}$  by (rule Int_ZF_2_1_L23)
qed

```

Type information related to  $\gamma$ .

```

lemma (in int1) Int_ZF_2_1_L25:
  assumes A1:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  and A2:  $m \in \mathbb{Z} \quad n \in \mathbb{Z}$ 
  shows
     $\delta(f, m, -n) \in \mathbb{Z}$ 
     $\delta(f, n, -n) \in \mathbb{Z}$ 
     $(-\delta(f, n, -n)) \in \mathbb{Z}$ 
     $f(0) \in \mathbb{Z}$ 
     $\gamma(f, m, n) \in \mathbb{Z}$ 
proof -
  from A1 A2 show T1:
     $\delta(f, m, -n) \in \mathbb{Z} \quad f(0) \in \mathbb{Z}$ 
    using Int_ZF_1_1_L4 Int_ZF_2_1_L3B int_zero_one_are_int apply_funtype
    by auto
  from A2 have  $(-n) \in \mathbb{Z}$ 
    using Int_ZF_1_1_L4 by simp
  with A1 A2 show  $\delta(f, n, -n) \in \mathbb{Z}$ 
    using Int_ZF_2_1_L3B by simp
  then show  $(-\delta(f, n, -n)) \in \mathbb{Z}$ 
    using Int_ZF_1_1_L4 by simp
  with T1 show  $\gamma(f, m, n) \in \mathbb{Z}$ 
    using Int_ZF_1_1_L5 by simp
qed

```

A couple of formulae involving  $f(m - n)$  and  $\gamma(f, m, n)$ .

```

lemma (in int1) Int_ZF_2_1_L26:
  assumes A1:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  and A2:  $m \in \mathbb{Z} \quad n \in \mathbb{Z}$ 
  shows
     $f(m-n) = \gamma(f, m, n) + f(m) - f(n)$ 
     $f(m-n) = \gamma(f, m, n) + (f(m) - f(n))$ 
     $f(m-n) + (f(n) - \gamma(f, m, n)) = f(m)$ 
proof -
  from A1 A2 have T:
     $(-n) \in \mathbb{Z} \quad \delta(f, m, -n) \in \mathbb{Z}$ 
     $f(0) \in \mathbb{Z} \quad f(m) \in \mathbb{Z} \quad f(n) \in \mathbb{Z} \quad (-f(n)) \in \mathbb{Z}$ 
     $(-\delta(f, n, -n)) \in \mathbb{Z}$ 
     $(-\delta(f, n, -n)) + f(0) \in \mathbb{Z}$ 
     $\gamma(f, m, n) \in \mathbb{Z}$ 
    using Int_ZF_1_1_L4 Int_ZF_2_1_L25 apply_funtype Int_ZF_1_1_L5
    by auto
  with A1 A2 have  $f(m-n) =$ 
     $\delta(f, m, -n) + ((-\delta(f, n, -n)) + f(0) - f(n)) + f(m)$ 
    using Int_ZF_2_1_L3C Int_ZF_2_1_L14A by simp
  with T have  $f(m-n) =$ 
     $\delta(f, m, -n) + ((-\delta(f, n, -n)) + f(0)) + f(m) - f(n)$ 
    using Int_ZF_1_2_L16 by simp
  moreover from T have
     $\delta(f, m, -n) + ((-\delta(f, n, -n)) + f(0)) = \gamma(f, m, n)$ 
    using Int_ZF_1_1_L7 by simp

```

```

ultimately show I:  $f(m-n) = \gamma(f, m, n) + f(m) - f(n)$ 
  by simp
then have  $f(m-n) + (f(n) - \gamma(f, m, n)) =$ 
   $(\gamma(f, m, n) + f(m) - f(n)) + (f(n) - \gamma(f, m, n))$ 
  by simp
moreover from T have  $\dots = f(m)$  using Int_ZF_1_2_L18
  by simp
ultimately show  $f(m-n) + (f(n) - \gamma(f, m, n)) = f(m)$ 
  by simp
from T have  $\gamma(f, m, n) \in \mathbb{Z} \quad f(m) \in \mathbb{Z} \quad (-f(n)) \in \mathbb{Z}$ 
  by auto
then have
   $\gamma(f, m, n) + f(m) + (-f(n)) = \gamma(f, m, n) + (f(m) + (-f(n)))$ 
  by (rule Int_ZF_1_1_L7)
with I show  $f(m-n) = \gamma(f, m, n) + (f(m) - f(n))$  by simp
qed

```

A formula expressing the difference between  $f(m-n-k)$  and  $f(m) - f(n) - f(k)$  in terms of  $\gamma$ .

```

lemma (in int1) Int_ZF_2_1_L26A:
  assumes A1:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  and A2:  $m \in \mathbb{Z} \quad n \in \mathbb{Z} \quad k \in \mathbb{Z}$ 
  shows
     $f(m-n-k) - (f(m) - f(n) - f(k)) = \gamma(f, m-n, k) + \gamma(f, m, n)$ 
proof -
  from A1 A2 have
    T:  $m-n \in \mathbb{Z} \quad \gamma(f, m-n, k) \in \mathbb{Z} \quad f(m) - f(n) - f(k) \in \mathbb{Z}$  and
    T1:  $\gamma(f, m, n) \in \mathbb{Z} \quad f(m) - f(n) \in \mathbb{Z} \quad (-f(k)) \in \mathbb{Z}$ 
    using Int_ZF_1_1_L4 Int_ZF_1_1_L5 Int_ZF_2_1_L25 apply funtype
    by auto
  from A1 A2 have
     $f(m-n) - f(k) = \gamma(f, m, n) + (f(m) - f(n)) + (-f(k))$ 
    using Int_ZF_2_1_L26 by simp
  also from T1 have  $\dots = \gamma(f, m, n) + (f(m) - f(n) + (-f(k)))$ 
    by (rule Int_ZF_1_1_L7)
  finally have
     $f(m-n) - f(k) = \gamma(f, m, n) + (f(m) - f(n) - f(k))$ 
    by simp
  moreover from A1 A2 T have
     $f(m-n-k) = \gamma(f, m-n, k) + (f(m-n) - f(k))$ 
    using Int_ZF_2_1_L26 by simp
  ultimately have
     $f(m-n-k) - (f(m) - f(n) - f(k)) =$ 
     $\gamma(f, m-n, k) + (\gamma(f, m, n) + (f(m) - f(n) - f(k)))$ 
     $- (f(m) - f(n) - f(k))$ 
    by simp
  with T T1 show thesis
    using Int_ZF_1_2_L17 by simp
qed

```

If  $s$  is a slope, then  $\gamma(s, m, n)$  is uniformly bounded.

```

lemma (in int1) Int_ZF_2_1_L27: assumes A1:  $s \in \mathcal{S}$ 
  shows  $\exists L \in \mathbb{Z}. \forall m \in \mathbb{Z}. \forall n \in \mathbb{Z}. \text{abs}(\gamma(s, m, n)) \leq L$ 
proof -
  let  $L = \max \delta(s) + \max \delta(s) + \text{abs}(s(0))$ 
  from A1 have T:
     $\max \delta(s) \in \mathbb{Z} \quad \text{abs}(s(0)) \in \mathbb{Z} \quad L \in \mathbb{Z}$ 
    using Int_ZF_2_1_L8 int_zero_one_are_int Int_ZF_2_1_L2B
      Int_ZF_2_L14 Int_ZF_1_1_L5 by auto
  moreover
  { fix m
    fix n
    assume A2:  $m \in \mathbb{Z} \quad n \in \mathbb{Z}$ 
    with A1 have T:
       $(-n) \in \mathbb{Z}$ 
       $\delta(s, m, -n) \in \mathbb{Z}$ 
       $\delta(s, n, -n) \in \mathbb{Z}$ 
       $(-\delta(s, n, -n)) \in \mathbb{Z}$ 
       $s(0) \in \mathbb{Z} \quad \text{abs}(s(0)) \in \mathbb{Z}$ 
      using Int_ZF_1_1_L4 AlmostHoms_def Int_ZF_2_1_L25 Int_ZF_2_L14
        by auto
    with T have
       $\text{abs}(\delta(s, m, -n) - \delta(s, n, -n) + s(0)) \leq$ 
       $\text{abs}(\delta(s, m, -n)) + \text{abs}(-\delta(s, n, -n)) + \text{abs}(s(0))$ 
      using Int_triangle_ineq3 by simp
    moreover from A1 A2 T have
       $\text{abs}(\delta(s, m, -n)) + \text{abs}(-\delta(s, n, -n)) + \text{abs}(s(0)) \leq L$ 
      using Int_ZF_2_1_L7 int_ineq_add_sides int_ord_transl_inv Int_ZF_2_L17
        by simp
    ultimately have  $\text{abs}(\delta(s, m, -n) - \delta(s, n, -n) + s(0)) \leq L$ 
      by (rule Int_order_transitive)
    then have  $\text{abs}(\gamma(s, m, n)) \leq L$  by simp }
  ultimately show  $\exists L \in \mathbb{Z}. \forall m \in \mathbb{Z}. \forall n \in \mathbb{Z}. \text{abs}(\gamma(s, m, n)) \leq L$ 
    by auto
qed

```

If  $s$  is a slope, then  $s(m) \leq s(m-1) + M$ , where  $L$  does not depend on  $m$ .

```

lemma (in int1) Int_ZF_2_1_L28: assumes A1:  $s \in \mathcal{S}$ 
  shows  $\exists M \in \mathbb{Z}. \forall m \in \mathbb{Z}. s(m) \leq s(m-1) + M$ 
proof -
  from A1 have
     $\exists L \in \mathbb{Z}. \forall m \in \mathbb{Z}. \forall n \in \mathbb{Z}. \text{abs}(\gamma(s, m, n)) \leq L$ 
    using Int_ZF_2_1_L27 by simp
  then obtain L where T:  $L \in \mathbb{Z}$  and  $\forall m \in \mathbb{Z}. \forall n \in \mathbb{Z}. \text{abs}(\gamma(s, m, n)) \leq L$ 
    using Int_ZF_2_1_L27 by auto
  then have I:  $\forall m \in \mathbb{Z}. \text{abs}(\gamma(s, m, 1)) \leq L$ 
    using int_zero_one_are_int by simp
  let  $M = s(1) + L$ 
  from A1 T have  $M \in \mathbb{Z}$ 

```

```

    using int_zero_one_are_int Int_ZF_2_1_L2B Int_ZF_1_1_L5
  by simp
moreover
{ fix m assume A2: m ∈ ℤ
  with A1 have
    T1: s:ℤ→ℤ m ∈ ℤ 1 ∈ ℤ and
    T2: γ(s,m,1) ∈ ℤ s(1) ∈ ℤ
    using int_zero_one_are_int AlmostHoms_def
Int_ZF_2_1_L25 by auto
  from A2 T1 have T3: s(m-1) ∈ ℤ
    using Int_ZF_1_1_L5 apply_funtype by simp
  from I A2 T2 have
    (-γ(s,m,1)) ≤ abs(γ(s,m,1))
    abs(γ(s,m,1)) ≤ L
    using Int_ZF_2_L19C by auto
  then have (-γ(s,m,1)) ≤ L
    by (rule Int_order_transitive)
  with T2 T3 have
    s(m-1) + (s(1) - γ(s,m,1)) ≤ s(m-1) + M
    using int_ord_transl_inv by simp
  moreover from T1 have
    s(m-1) + (s(1) - γ(s,m,1)) = s(m)
    by (rule Int_ZF_2_1_L26)
  ultimately have s(m) ≤ s(m-1) + M by simp }
ultimately show ∃M ∈ ℤ. ∀m ∈ ℤ. s(m) ≤ s(m-1) + M
  by auto
qed

```

If  $s$  is a slope, then the difference between  $s(m-n-k)$  and  $s(m)-s(n)-s(k)$  is uniformly bounded.

```

lemma (in int1) Int_ZF_2_1_L29: assumes A1: s ∈ S
  shows
    ∃M ∈ ℤ. ∀m ∈ ℤ. ∀n ∈ ℤ. ∀k ∈ ℤ. abs(s(m-n-k) - (s(m)-s(n)-s(k))) ≤ M
proof -
  from A1 have ∃L ∈ ℤ. ∀m ∈ ℤ. ∀n ∈ ℤ. abs(γ(s,m,n)) ≤ L
    using Int_ZF_2_1_L27 by simp
  then obtain L where I: L ∈ ℤ and
    II: ∀m ∈ ℤ. ∀n ∈ ℤ. abs(γ(s,m,n)) ≤ L
    by auto
  from I have L+L ∈ ℤ
    using Int_ZF_1_1_L5 by simp
  moreover
  { fix m n k assume A2: m ∈ ℤ n ∈ ℤ k ∈ ℤ
    with A1 have T:
      m-n ∈ ℤ γ(s,m-n,k) ∈ ℤ γ(s,m,n) ∈ ℤ
      using Int_ZF_1_1_L5 AlmostHoms_def Int_ZF_2_1_L25
      by auto
    then have
      I: abs(γ(s,m-n,k) + γ(s,m,n)) ≤ abs(γ(s,m-n,k)) + abs(γ(s,m,n))

```



```

    using Int_triangle_ineq by simp
  from II A2 T have
    abs( $\gamma(s, m-n, k)$ )  $\leq$  L
    abs( $\gamma(s, m, n)$ )  $\leq$  L
    by auto
  then have abs( $\gamma(s, m-n, k)$ ) + abs( $\gamma(s, m, n)$ )  $\leq$  L+L
    using int_ineq_add_sides by simp
  with I have abs( $\gamma(s, m-n, k)$  +  $\gamma(s, m, n)$ )  $\leq$  L+L
    by (rule Int_order_transitive)
  moreover from A1 A2 have
     $s(m-n-k) - (s(m) - s(n) - s(k)) = \gamma(s, m-n, k) + \gamma(s, m, n)$ 
    using AlmostHoms_def Int_ZF_2_1_L26A by simp
  ultimately have
    abs( $s(m-n-k) - (s(m) - s(n) - s(k))$ )  $\leq$  L+L
    by simp }
  ultimately show thesis by auto
qed

```

If  $s$  is a slope, then we can find integers  $M, K$  such that  $s(m - n - k) \leq s(m) - s(n) - s(k) + M$  and  $s(m) - s(n) - s(k) + K \leq s(m - n - k)$ , for all integer  $m, n, k$ .

**lemma** (in int1) Int\_ZF\_2\_1\_L30: assumes A1:  $s \in \mathcal{S}$

shows

$\exists M \in \mathbb{Z}. \forall m \in \mathbb{Z}. \forall n \in \mathbb{Z}. \forall k \in \mathbb{Z}. s(m-n-k) \leq s(m) - s(n) - s(k) + M$

$\exists K \in \mathbb{Z}. \forall m \in \mathbb{Z}. \forall n \in \mathbb{Z}. \forall k \in \mathbb{Z}. s(m) - s(n) - s(k) + K \leq s(m-n-k)$

**proof** -

from A1 have

$\exists M \in \mathbb{Z}. \forall m \in \mathbb{Z}. \forall n \in \mathbb{Z}. \forall k \in \mathbb{Z}. \text{abs}(s(m-n-k) - (s(m) - s(n) - s(k))) \leq M$

using Int\_ZF\_2\_1\_L29 by simp

then obtain M where I:  $M \in \mathbb{Z}$  and II:

$\forall m \in \mathbb{Z}. \forall n \in \mathbb{Z}. \forall k \in \mathbb{Z}. \text{abs}(s(m-n-k) - (s(m) - s(n) - s(k))) \leq M$

by auto

from I have III:  $(-M) \in \mathbb{Z}$  using Int\_ZF\_1\_1\_L4 by simp

{ fix m n k assume A2:  $m \in \mathbb{Z} \quad n \in \mathbb{Z} \quad k \in \mathbb{Z}$

with A1 have  $s(m-n-k) \in \mathbb{Z}$  and  $s(m) - s(n) - s(k) \in \mathbb{Z}$

using Int\_ZF\_1\_1\_L5 Int\_ZF\_2\_1\_L2B by auto

moreover from II A2 have

abs( $s(m-n-k) - (s(m) - s(n) - s(k))$ )  $\leq$  M

by simp

ultimately have

$s(m-n-k) \leq s(m) - s(n) - s(k) + M \wedge$

$s(m) - s(n) - s(k) - M \leq s(m-n-k)$

using Int\_triangle\_ineq2 by simp

} then have

$\forall m \in \mathbb{Z}. \forall n \in \mathbb{Z}. \forall k \in \mathbb{Z}. s(m-n-k) \leq s(m) - s(n) - s(k) + M$

$\forall m \in \mathbb{Z}. \forall n \in \mathbb{Z}. \forall k \in \mathbb{Z}. s(m) - s(n) - s(k) - M \leq s(m-n-k)$

by auto

with I III show

$\exists M \in \mathbb{Z}. \forall m \in \mathbb{Z}. \forall n \in \mathbb{Z}. \forall k \in \mathbb{Z}. s(m-n-k) \leq s(m) - s(n) - s(k) + M$

$\exists K \in \mathbb{Z}. \forall m \in \mathbb{Z}. \forall n \in \mathbb{Z}. \forall k \in \mathbb{Z}. s(m) - s(n) - s(k) + K \leq s(m - n - k)$   
 by auto

qed

By definition functions  $f, g$  are almost equal if  $f - g^*$  is bounded. In the next lemma we show it is sufficient to check the boundedness on positive integers.

**lemma** (in int1) Int\_ZF\_2\_1\_L31: assumes A1:  $s \in S \quad r \in S$   
 and A2:  $\forall m \in \mathbb{Z}_+. \text{abs}(s(m) - r(m)) \leq L$   
 shows  $s \sim r$

**proof** -

let a =  $\text{abs}(s(0) - r(0))$   
 let c =  $2 \cdot \text{max}\delta(s) + 2 \cdot \text{max}\delta(r) + L$   
 let M =  $\text{Maximum}(\text{IntegerOrder}, \{a, L, c\})$   
 from A2 have  $\text{abs}(s(1) - r(1)) \leq L$   
 using int\_one\_two\_are\_pos by simp  
 then have T:  $L \in \mathbb{Z}$  using Int\_ZF\_2\_L1A by simp  
 moreover from A1 have  $a \in \mathbb{Z}$   
 using int\_zero\_one\_are\_int Int\_ZF\_2\_1\_L2B  
 Int\_ZF\_1\_1\_L5 Int\_ZF\_2\_L14 by simp  
 moreover from A1 T have  $c \in \mathbb{Z}$   
 using Int\_ZF\_2\_1\_L8 int\_two\_three\_are\_int Int\_ZF\_1\_1\_L5  
 by simp  
 ultimately have  
 I:  $a \leq M$  and  
 II:  $L \leq M$  and  
 III:  $c \leq M$   
 using Int\_ZF\_1\_4\_L1A by auto

{ fix m assume A5:  $m \in \mathbb{Z}$   
 with A1 have T:  
 $s(m) \in \mathbb{Z} \quad r(m) \in \mathbb{Z} \quad s(m) - r(m) \in \mathbb{Z}$   
 $s(-m) \in \mathbb{Z} \quad r(-m) \in \mathbb{Z}$   
 using Int\_ZF\_2\_1\_L2B Int\_ZF\_1\_1\_L4 Int\_ZF\_1\_1\_L5  
 by auto

from A5 have  $m=0 \vee m \in \mathbb{Z}_+ \vee (-m) \in \mathbb{Z}_+$   
 using int\_decomp\_cases by simp

moreover  
 { assume  $m=0$   
 with I have  $\text{abs}(s(m) - r(m)) \leq M$

by simp }

moreover

{ assume  $m \in \mathbb{Z}_+$   
 with A2 II have

$\text{abs}(s(m) - r(m)) \leq L$  and  $L \leq M$

by auto

then have  $\text{abs}(s(m) - r(m)) \leq M$

by (rule Int\_order\_transitive) }

moreover

```

      { assume A6:  $(-m) \in \mathbb{Z}_+$ 
        from T have  $\text{abs}(s(m)-r(m)) \leq$ 
 $\text{abs}(s(m)+s(-m)) + \text{abs}(r(m)+r(-m)) + \text{abs}(s(-m)-r(-m))$ 
      using Int_ZF_1_3_L22A by simp
      moreover
      from A1 A2 III A5 A6 have
 $\text{abs}(s(m)+s(-m)) + \text{abs}(r(m)+r(-m)) + \text{abs}(s(-m)-r(-m)) \leq c$ 
 $c \leq M$ 
      using Int_ZF_2_1_L14 int_ineq_add_sides by auto
      then have
 $\text{abs}(s(m)+s(-m)) + \text{abs}(r(m)+r(-m)) + \text{abs}(s(-m)-r(-m)) \leq M$ 
      by (rule Int_order_transitive)
      ultimately have  $\text{abs}(s(m)-r(m)) \leq M$ 
      by (rule Int_order_transitive) }
      ultimately have  $\text{abs}(s(m) - r(m)) \leq M$ 
      by auto
    } then have  $\forall m \in \mathbb{Z}. \text{abs}(s(m)-r(m)) \leq M$ 
      by simp
    with A1 show  $s \sim r$  by (rule Int_ZF_2_1_L9)
  qed

```

A sufficient condition for an odd slope to be almost equal to identity: If for all positive integers the value of the slope at  $m$  is between  $m$  and  $m$  plus some constant independent of  $m$ , then the slope is almost identity.

```

lemma (in int1) Int_ZF_2_1_L32: assumes A1:  $s \in \mathcal{S} \quad M \in \mathbb{Z}$ 
  and A2:  $\forall m \in \mathbb{Z}_+. m \leq s(m) \wedge s(m) \leq m+M$ 
  shows  $s \sim \text{id}(\mathbb{Z})$ 
proof -
  let  $r = \text{id}(\mathbb{Z})$ 
  from A1 have  $s \in \mathcal{S} \quad r \in \mathcal{S}$ 
  using Int_ZF_2_1_L17 by auto
  moreover from A1 A2 have  $\forall m \in \mathbb{Z}_+. \text{abs}(s(m)-r(m)) \leq M$ 
  using Int_ZF_1_3_L23 PositiveSet_def id_conv by simp
  ultimately show  $s \sim \text{id}(\mathbb{Z})$  by (rule Int_ZF_2_1_L31)
qed

```

A lemma about adding a constant to slopes. This is actually proven in Group\_ZF\_3\_5\_L1, in Group\_ZF\_3.thy here we just refer to that lemma to show it in notation used for integers. Unfortunately we have to use raw set notation in the proof.

```

lemma (in int1) Int_ZF_2_1_L33:
  assumes A1:  $s \in \mathcal{S}$  and A2:  $c \in \mathbb{Z}$  and
  A3:  $r = \{ \langle m, s(m)+c \rangle. m \in \mathbb{Z} \}$ 
  shows
 $\forall m \in \mathbb{Z}. r(m) = s(m)+c$ 
 $r \in \mathcal{S}$ 
 $s \sim r$ 
proof -

```

```

let G = ℤ
let f = IntegerAddition
let AH = AlmostHoms(G, f)
from assms have I:
  group1(G, f)
  s ∈ AlmostHoms(G, f)
  c ∈ G
  r = {⟨x, f(s(x), c)⟩. x ∈ G}
  using Int_ZF_2_1_L1 by auto
then have ∀x∈G. r(x) = f(s(x), c)
  by (rule group1.Group_ZF_3_5_L1)
moreover from I have r ∈ AlmostHoms(G, f)
  by (rule group1.Group_ZF_3_5_L1)
moreover from I have
  ⟨s, r⟩ ∈ QuotientGroupRel(AlmostHoms(G, f), AlHomOp1(G, f), FinRangeFunctions(G,
G))
  by (rule group1.Group_ZF_3_5_L1)
ultimately show
  ∀m∈ℤ. r(m) = s(m)+c
  r∈S
  s ∼ r
  by auto
qed

```

### 37.2 Composing slopes

Composition of slopes is not commutative. However, as we show in this section if  $f$  and  $g$  are slopes then the range of  $f \circ g - g \circ f$  is bounded. This allows to show that the multiplication of real numbers is commutative.

Two useful estimates.

```

lemma (in int1) Int_ZF_2_2_L1:
  assumes A1: f:ℤ→ℤ and A2: p∈ℤ q∈ℤ
  shows
    abs(f((p+1)·q)-(p+1)·f(q)) ≤ abs(δ(f,p·q,q))+abs(f(p·q)-p·f(q))
    abs(f((p-1)·q)-(p-1)·f(q)) ≤ abs(δ(f,(p-1)·q,q))+abs(f(p·q)-p·f(q))
proof -
  let R = ℤ
  let A = IntegerAddition
  let M = IntegerMultiplication
  let I = GroupInv(R, A)
  let a = f((p+1)·q)
  let b = p
  let c = f(q)
  let d = f(p·q)
  from A1 A2 have T1:
    ring0(R, A, M) a ∈ R b ∈ R c ∈ R d ∈ R
  using Int_ZF_1_1_L2 int_zero_one_are_int Int_ZF_1_1_L5 apply_funtype

```

```

    by auto
  then have
    A⟨a, I(M⟨A⟨b, TheNeutralElement(R, M)⟩, c)⟩⟩ =
    A⟨A⟨A⟨a, I(d)⟩, I(c)⟩, A⟨d, I(M⟨b, c)⟩⟩⟩
    by (rule ring0.Ring_ZF_2_L2)
  with A2 have
    f((p+1)·q)-(p+1)·f(q) = δ(f,p·q,q)+(f(p·q)-p·f(q))
    using int_zero_one_are_int Int_ZF_1_1_L1 Int_ZF_1_1_L4 by simp
  moreover from A1 A2 T1 have δ(f,p·q,q) ∈ ℤ f(p·q)-p·f(q) ∈ ℤ
    using Int_ZF_1_1_L5 apply_funtype by auto
  ultimately show
    abs(f((p+1)·q)-(p+1)·f(q)) ≤ abs(δ(f,p·q,q))+abs(f(p·q)-p·f(q))
    using Int_triangle_ineq by simp
  from A1 A2 have T1:
    f((p-1)·q) ∈ ℤ p ∈ ℤ f(q) ∈ ℤ f(p·q) ∈ ℤ
    using int_zero_one_are_int Int_ZF_1_1_L5 apply_funtype by auto
  then have
    f((p-1)·q)-(p-1)·f(q) = (f(p·q)-p·f(q))-(f(p·q)-f((p-1)·q)-f(q))
    by (rule Int_ZF_1_2_L6)
  with A2 have f((p-1)·q)-(p-1)·f(q) = (f(p·q)-p·f(q))-δ(f,(p-1)·q,q)
    using Int_ZF_1_2_L7 by simp
  moreover from A1 A2 have
    f(p·q)-p·f(q) ∈ ℤ δ(f,(p-1)·q,q) ∈ ℤ
    using Int_ZF_1_1_L5 int_zero_one_are_int apply_funtype by auto
  ultimately show
    abs(f((p-1)·q)-(p-1)·f(q)) ≤ abs(δ(f,(p-1)·q,q))+abs(f(p·q)-p·f(q))
    using Int_triangle_ineq1 by simp
qed

```

If  $f$  is a slope, then  $|f(p \cdot q) - p \cdot f(q)| \leq (|p| + 1) \cdot \max \delta(f)$ . The proof is by induction on  $p$  and the next lemma is the induction step for the case when  $0 \leq p$ .

```

lemma (in int1) Int_ZF_2_2_L2:
  assumes A1: f ∈ S and A2: 0 ≤ p q ∈ ℤ
  and A3: abs(f(p·q)-p·f(q)) ≤ (abs(p)+1)·maxδ(f)
  shows
    abs(f((p+1)·q)-(p+1)·f(q)) ≤ (abs(p+1)+ 1)·maxδ(f)
proof -
  from A2 have q ∈ ℤ p·q ∈ ℤ
    using Int_ZF_2_L1A Int_ZF_1_1_L5 by auto
  with A1 have I: abs(δ(f,p·q,q)) ≤ maxδ(f) by (rule Int_ZF_2_1_L7)
  moreover note A3
  moreover from A1 A2 have
    abs(f((p+1)·q)-(p+1)·f(q)) ≤ abs(δ(f,p·q,q))+abs(f(p·q)-p·f(q))
    using AlmostHoms_def Int_ZF_2_L1A Int_ZF_2_2_L1 by simp
  ultimately have
    abs(f((p+1)·q)-(p+1)·f(q)) ≤ maxδ(f)+(abs(p)+1)·maxδ(f)
    by (rule Int_ZF_2_L15)
  moreover from I A2 have

```

```

    maxδ(f)+(abs(p)+1)·maxδ(f) = (abs(p+1)+ 1)·maxδ(f)
    using Int_ZF_2_L1A Int_ZF_1_2_L2 by simp
  ultimately show
    abs(f((p+1)·q)-(p+1)·f(q)) ≤ (abs(p+1)+ 1)·maxδ(f)
    by simp
qed

```

If  $f$  is a slope, then  $|f(p \cdot q) - p \cdot f(q)| \leq (|p| + 1) \cdot \max \delta$ . The proof is by induction on  $p$  and the next lemma is the induction step for the case when  $p \leq 0$ .

```

lemma (in int1) Int_ZF_2_2_L3:
  assumes A1: f∈S and A2: p≤0  q∈ℤ
  and A3: abs(f(p·q)-p·f(q)) ≤ (abs(p)+1)·maxδ(f)
  shows  abs(f((p-1)·q)-(p-1)·f(q)) ≤ (abs(p-1)+ 1)·maxδ(f)
proof -
  from A2 have q∈ℤ  (p-1)·q ∈ ℤ
    using Int_ZF_2_L1A int_zero_one_are_int Int_ZF_1_1_L5 by auto
  with A1 have I: abs(δ(f, (p-1)·q, q)) ≤ maxδ(f) by (rule Int_ZF_2_1_L7)
  moreover note A3
  moreover from A1 A2 have
    abs(f((p-1)·q)-(p-1)·f(q)) ≤ abs(δ(f, (p-1)·q, q))+abs(f(p·q)-p·f(q))
    using AlmostHoms_def Int_ZF_2_L1A Int_ZF_2_2_L1 by simp
  ultimately have
    abs(f((p-1)·q)-(p-1)·f(q)) ≤ maxδ(f)+(abs(p)+1)·maxδ(f)
    by (rule Int_ZF_2_L15)
  with I A2 show thesis using Int_ZF_2_L1A Int_ZF_1_2_L5 by simp
qed

```

If  $f$  is a slope, then  $|f(p \cdot q) - p \cdot f(q)| \leq (|p| + 1) \cdot \max \delta(f)$ . Proof by cases on  $0 \leq p$ .

```

lemma (in int1) Int_ZF_2_2_L4:
  assumes A1: f∈S and A2: p∈ℤ q∈ℤ
  shows abs(f(p·q)-p·f(q)) ≤ (abs(p)+1)·maxδ(f)
proof -
  { assume 0≤p
    moreover from A1 A2 have abs(f(0·q)-0·f(q)) ≤ (abs(0)+1)·maxδ(f)
      using int_zero_one_are_int Int_ZF_2_1_L2B Int_ZF_1_1_L4
    Int_ZF_2_1_L8 Int_ZF_2_L18 by simp
    moreover from A1 A2 have
      ∀p. 0≤p ∧ abs(f(p·q)-p·f(q)) ≤ (abs(p)+1)·maxδ(f) ⟶
      abs(f((p+1)·q)-(p+1)·f(q)) ≤ (abs(p+1)+ 1)·maxδ(f)
      using Int_ZF_2_2_L2 by simp
    ultimately have abs(f(p·q)-p·f(q)) ≤ (abs(p)+1)·maxδ(f)
      by (rule Induction_on_int) }
  moreover
  { assume ¬(0≤p)
    with A2 have p≤0 using Int_ZF_2_L19A by simp
    moreover from A1 A2 have abs(f(0·q)-0·f(q)) ≤ (abs(0)+1)·maxδ(f)
      using int_zero_one_are_int Int_ZF_2_1_L2B Int_ZF_1_1_L4

```

```

Int_ZF_2_1_L8 Int_ZF_2_L18 by simp
  moreover from A1 A2 have
     $\forall p. p \leq 0 \wedge \text{abs}(f(p \cdot q) - p \cdot f(q)) \leq (\text{abs}(p) + 1) \cdot \text{max}\delta(f) \longrightarrow$ 
 $\text{abs}(f((p-1) \cdot q) - (p-1) \cdot f(q)) \leq (\text{abs}(p-1) + 1) \cdot \text{max}\delta(f)$ 
    using Int_ZF_2_2_L3 by simp
    ultimately have  $\text{abs}(f(p \cdot q) - p \cdot f(q)) \leq (\text{abs}(p) + 1) \cdot \text{max}\delta(f)$ 
    by (rule Back_induct_on_int) }
  ultimately show thesis by blast
qed

```

The next elegant result is Lemma 7 in the Arthan's paper [2].

```

lemma (in int1) Arthan_Lem_7:
  assumes A1:  $f \in \mathcal{S}$  and A2:  $p \in \mathbb{Z} \quad q \in \mathbb{Z}$ 
  shows  $\text{abs}(q \cdot f(p) - p \cdot f(q)) \leq (\text{abs}(p) + \text{abs}(q) + 2) \cdot \text{max}\delta(f)$ 
proof -
  from A1 A2 have T:
     $q \cdot f(p) - f(p \cdot q) \in \mathbb{Z}$ 
     $f(p \cdot q) - p \cdot f(q) \in \mathbb{Z}$ 
     $f(q \cdot p) \in \mathbb{Z} \quad f(p \cdot q) \in \mathbb{Z}$ 
     $q \cdot f(p) \in \mathbb{Z} \quad p \cdot f(q) \in \mathbb{Z}$ 
     $\text{max}\delta(f) \in \mathbb{Z}$ 
     $\text{abs}(q) \in \mathbb{Z} \quad \text{abs}(p) \in \mathbb{Z}$ 
  using Int_ZF_1_1_L5 Int_ZF_2_1_L2B Int_ZF_2_1_L7 Int_ZF_2_L14 by auto
  moreover have  $\text{abs}(q \cdot f(p) - f(p \cdot q)) \leq (\text{abs}(q) + 1) \cdot \text{max}\delta(f)$ 
proof -
  from A1 A2 have  $\text{abs}(f(q \cdot p) - q \cdot f(p)) \leq (\text{abs}(q) + 1) \cdot \text{max}\delta(f)$ 
  using Int_ZF_2_2_L4 by simp
  with T A2 show thesis
  using Int_ZF_2_L20 Int_ZF_1_1_L5 by simp
qed
moreover from A1 A2 have  $\text{abs}(f(p \cdot q) - p \cdot f(q)) \leq (\text{abs}(p) + 1) \cdot \text{max}\delta(f)$ 
using Int_ZF_2_2_L4 by simp
ultimately have
 $\text{abs}(q \cdot f(p) - f(p \cdot q) + (f(p \cdot q) - p \cdot f(q))) \leq (\text{abs}(q) + 1) \cdot \text{max}\delta(f) + (\text{abs}(p) + 1) \cdot \text{max}\delta(f)$ 
using Int_ZF_2_L21 by simp
with T show thesis using Int_ZF_1_2_L9 int_zero_one_are_int Int_ZF_1_2_L10
by simp
qed

```

This is Lemma 8 in the Arthan's paper.

```

lemma (in int1) Arthan_Lem_8: assumes A1:  $f \in \mathcal{S}$ 
  shows  $\exists A B. A \in \mathbb{Z} \wedge B \in \mathbb{Z} \wedge (\forall p \in \mathbb{Z}. \text{abs}(f(p)) \leq A \cdot \text{abs}(p) + B)$ 
proof -
  let A =  $\text{max}\delta(f) + \text{abs}(f(1))$ 
  let B =  $3 \cdot \text{max}\delta(f)$ 
  from A1 have  $A \in \mathbb{Z} \quad B \in \mathbb{Z}$ 
  using int_zero_one_are_int Int_ZF_1_1_L5 Int_ZF_2_1_L2B
    Int_ZF_2_1_L7 Int_ZF_2_L14 by auto
  moreover have  $\forall p \in \mathbb{Z}. \text{abs}(f(p)) \leq A \cdot \text{abs}(p) + B$ 

```

```

proof
  fix p assume A2: p ∈ ℤ
  with A1 have T:
    f(p) ∈ ℤ abs(p) ∈ ℤ f(1) ∈ ℤ
    p·f(1) ∈ ℤ 3 ∈ ℤ maxδ(f) ∈ ℤ
    using Int_ZF_2_1_L2B Int_ZF_2_L14 int_zero_one_are_int
Int_ZF_1_1_L5 Int_ZF_2_1_L7 by auto
  from A1 A2 have
    abs(1·f(p)-p·f(1)) ≤ (abs(p)+abs(1)+2)·maxδ(f)
    using int_zero_one_are_int Arthan_Lem_7 by simp
  with T have abs(f(p)) ≤ abs(p·f(1))+abs(p)+3)·maxδ(f)
    using Int_ZF_2_L16A Int_ZF_1_1_L4 Int_ZF_1_2_L11
Int_triangle_ineq2 by simp
  with A2 T show abs(f(p)) ≤ A·abs(p)+B
    using Int_ZF_1_3_L14 by simp
qed
ultimately show thesis by auto
qed

```

If  $f$  and  $g$  are slopes, then  $f \circ g$  is equivalent (almost equal) to  $g \circ f$ . This is Theorem 9 in Arthan's paper [2].

**theorem** (in int1) Arthan\_Th\_9: assumes A1:  $f \in S \quad g \in S$   
 shows  $f \circ g \sim g \circ f$

**proof** -

```

  from A1 have
    ∃ A B. A ∈ ℤ ∧ B ∈ ℤ ∧ (∀ p ∈ ℤ. abs(f(p)) ≤ A·abs(p)+B)
    ∃ C D. C ∈ ℤ ∧ D ∈ ℤ ∧ (∀ p ∈ ℤ. abs(g(p)) ≤ C·abs(p)+D)
    using Arthan_Lem_8 by auto
  then obtain A B C D where D1: A ∈ ℤ B ∈ ℤ C ∈ ℤ D ∈ ℤ and D2:
    ∀ p ∈ ℤ. abs(f(p)) ≤ A·abs(p)+B
    ∀ p ∈ ℤ. abs(g(p)) ≤ C·abs(p)+D
    by auto

```

```

  let E = maxδ(g)·(A+1) + maxδ(f)·(C+1)

```

```

  let F = (B·maxδ(g) + 2·maxδ(g)) + (D·maxδ(f) + 2·maxδ(f))

```

```

{ fix p assume A2: p ∈ ℤ

```

```

  with A1 have T1:

```

```

    g(p) ∈ ℤ f(p) ∈ ℤ abs(p) ∈ ℤ 2 ∈ ℤ
    f(g(p)) ∈ ℤ g(f(p)) ∈ ℤ f(g(p)) - g(f(p)) ∈ ℤ
    p·f(g(p)) ∈ ℤ p·g(f(p)) ∈ ℤ
    abs(f(g(p))-g(f(p))) ∈ ℤ

```

```

    using Int_ZF_2_1_L2B Int_ZF_2_1_L10 Int_ZF_1_1_L5 Int_ZF_2_L14 int_two_three_are_int
    by auto

```

```

  with A1 A2 have

```

```

    abs((f(g(p))-g(f(p)))·p) ≤
    (abs(p)+abs(f(p))+2)·maxδ(g) + (abs(p)+abs(g(p))+2)·maxδ(f)
    using Arthan_Lem_7 Int_ZF_1_2_L10A Int_ZF_1_2_L12 by simp

```

```

  moreover have

```

```

    (abs(p)+abs(f(p))+2)·maxδ(g) + (abs(p)+abs(g(p))+2)·maxδ(f) ≤
    ((maxδ(g)·(A+1) + maxδ(f)·(C+1))·abs(p) +

```



```

      ((B·maxδ(g) + 2·maxδ(g)) + (D·maxδ(f) + 2·maxδ(f)))
    proof -
      from D2 A2 T1 have
        abs(p)+abs(f(p))+2 ≤ abs(p)+(A·abs(p)+B)+2
        abs(p)+abs(g(p))+2 ≤ abs(p)+(C·abs(p)+D)+2
      using Int_ZF_2_L15C by auto
      with A1 have
        (abs(p)+abs(f(p))+2)·maxδ(g) ≤ (abs(p)+(A·abs(p)+B)+2)·maxδ(g)
        (abs(p)+abs(g(p))+2)·maxδ(f) ≤ (abs(p)+(C·abs(p)+D)+2)·maxδ(f)
      using Int_ZF_2_1_L8 Int_ZF_1_3_L13 by auto
      moreover from A1 D1 T1 have
        (abs(p)+(A·abs(p)+B)+2)·maxδ(g) =
        maxδ(g)·(A+1)·abs(p) + (B·maxδ(g) + 2·maxδ(g))
        (abs(p)+(C·abs(p)+D)+2)·maxδ(f) =
        maxδ(f)·(C+1)·abs(p) + (D·maxδ(f) + 2·maxδ(f))
      using Int_ZF_2_1_L8 Int_ZF_1_2_L13 by auto
      ultimately have
        (abs(p)+abs(f(p))+2)·maxδ(g) + (abs(p)+abs(g(p))+2)·maxδ(f) ≤
        (maxδ(g)·(A+1)·abs(p) + (B·maxδ(g) + 2·maxδ(g))) +
        (maxδ(f)·(C+1)·abs(p) + (D·maxδ(f) + 2·maxδ(f)))
      using int_ineq_add_sides by simp
      moreover from A1 A2 D1 have abs(p) ∈ ℤ
        maxδ(g)·(A+1) ∈ ℤ B·maxδ(g) + 2·maxδ(g) ∈ ℤ
        maxδ(f)·(C+1) ∈ ℤ D·maxδ(f) + 2·maxδ(f) ∈ ℤ
      using Int_ZF_2_L14 Int_ZF_2_1_L8 int_zero_one_are_int
        Int_ZF_1_1_L5 int_two_three_are_int by auto
      ultimately show thesis using Int_ZF_1_2_L14 by simp
    qed
    ultimately have
      abs((f(g(p))-g(f(p)))·p) ≤ E·abs(p) + F
    by (rule Int_order_transitive)
    with A2 T1 have
      abs(f(g(p))-g(f(p)))·abs(p) ≤ E·abs(p) + F
      abs(f(g(p))-g(f(p))) ∈ ℤ
    using Int_ZF_1_3_L5 by auto
  } then have
    ∀p∈ℤ. abs(f(g(p))-g(f(p))) ∈ ℤ
    ∀p∈ℤ. abs(f(g(p))-g(f(p)))·abs(p) ≤ E·abs(p) + F
  by auto
  moreover from A1 D1 have E ∈ ℤ F ∈ ℤ
    using int_zero_one_are_int int_two_three_are_int Int_ZF_2_1_L8 Int_ZF_1_1_L5
    by auto
  ultimately have
    ∃L. ∀p∈ℤ. abs(f(g(p))-g(f(p))) ≤ L
  by (rule Int_ZF_1_7_L1)
  with A1 obtain L where ∀p∈ℤ. abs((f◦g)(p)-(g◦f)(p)) ≤ L
    using Int_ZF_2_1_L10 by auto
  moreover from A1 have f◦g ∈ S g◦f ∈ S
    using Int_ZF_2_1_L11 by auto

```

```
ultimately show  $f \circ g \sim g \circ f$  using Int_ZF_2_1_L9 by auto
qed
end
```

## 38 Int\_ZF\_3.thy

**theory** Int\_ZF\_3 **imports** Int\_ZF\_2

**begin**

This theory is a continuation of Int\_ZF\_2. We consider here the properties of slopes (almost homomorphisms on integers) that allow to define the order relation and multiplicative inverse on real numbers. We also prove theorems that allow to show completeness of the order relation of real numbers we define in Real\_ZF.

### 38.1 Positive slopes

This section provides background material for defining the order relation on real numbers.

Positive slopes are functions (of course.)

**lemma** (in int1) Int\_ZF\_2\_3\_L1: **assumes** A1:  $f \in \mathcal{S}_+$  **shows**  $f: \mathbb{Z} \rightarrow \mathbb{Z}$   
**using** assms AlmostHoms\_def PositiveSet\_def **by** simp

A small technical lemma to simplify the proof of the next theorem.

**lemma** (in int1) Int\_ZF\_2\_3\_L1A:  
**assumes** A1:  $f \in \mathcal{S}_+$  **and** A2:  $\exists n \in f(\mathbb{Z}_+) \cap \mathbb{Z}_+. a \leq n$   
**shows**  $\exists M \in \mathbb{Z}_+. a \leq f(M)$

**proof** -

**from** A1 **have**  $f: \mathbb{Z} \rightarrow \mathbb{Z} \quad \mathbb{Z}_+ \subseteq \mathbb{Z}$   
**using** AlmostHoms\_def PositiveSet\_def **by** auto  
**with** A2 **show** thesis **using** func\_imagedef **by** auto  
**qed**

The next lemma is Lemma 3 in the Arthan's paper.

**lemma** (in int1) Arthan\_Lem\_3:  
**assumes** A1:  $f \in \mathcal{S}_+$  **and** A2:  $D \in \mathbb{Z}_+$   
**shows**  $\exists M \in \mathbb{Z}_+. \forall m \in \mathbb{Z}_+. (m+1) \cdot D \leq f(m \cdot M)$

**proof** -

**let** E =  $\max \delta(f) + D$   
**let** A =  $f(\mathbb{Z}_+) \cap \mathbb{Z}_+$   
**from** A1 A2 **have** I:  $D \leq E$   
**using** Int\_ZF\_1\_5\_L3 Int\_ZF\_2\_1\_L8 Int\_ZF\_2\_L1A Int\_ZF\_2\_L15D  
**by** simp  
**from** A1 A2 **have**  $A \subseteq \mathbb{Z}_+ \quad A \not\subseteq \text{Fin}(\mathbb{Z}) \quad 2 \cdot E \in \mathbb{Z}$   
**using** int\_two\_three\_are\_int Int\_ZF\_2\_1\_L8 PositiveSet\_def Int\_ZF\_1\_1\_L5  
**by** auto  
**with** A1 **have**  $\exists M \in \mathbb{Z}_+. 2 \cdot E \leq f(M)$   
**using** Int\_ZF\_1\_5\_L2A Int\_ZF\_2\_3\_L1A **by** simp  
**then obtain** M **where** II:  $M \in \mathbb{Z}_+ \quad \text{and} \quad \text{III: } 2 \cdot E \leq f(M)$   
**by** auto

```

{ fix m assume m ∈ ℤ+ then have A4: 1 ≤ m
  using Int_ZF_1_5_L3 by simp
  moreover from II III have (1+1) · E ≤ f(1·M)
  using PositiveSet_def Int_ZF_1_1_L4 by simp
  moreover have ∀k.
    1 ≤ k ∧ (k+1) · E ≤ f(k·M) ⟶ (k+1+1) · E ≤ f((k+1)·M)
  proof -
    { fix k assume A5: 1 ≤ k and A6: (k+1) · E ≤ f(k·M)
  with A1 A2 II have T:
    k ∈ ℤ M ∈ ℤ k+1 ∈ ℤ E ∈ ℤ (k+1) · E ∈ ℤ 2·E ∈ ℤ
    using Int_ZF_2_L1A PositiveSet_def int_zero_one_are_int
      Int_ZF_1_1_L5 Int_ZF_2_1_L8 by auto
  from A1 A2 A5 II have
    δ(f,k·M,M) ∈ ℤ abs(δ(f,k·M,M)) ≤ max δ(f) 0 ≤ D
    using Int_ZF_2_L1A PositiveSet_def Int_ZF_1_1_L5
      Int_ZF_2_1_L7 Int_ZF_2_L16C by auto
  with III A6 have
    (k+1) · E + (2·E - E) ≤ f(k·M) + (f(M) + δ(f,k·M,M))
    using Int_ZF_1_3_L19A int_ineq_add_sides by simp
  with A1 T have (k+1+1) · E ≤ f((k+1)·M)
    using Int_ZF_1_1_L1 int_zero_one_are_int Int_ZF_1_1_L4
      Int_ZF_1_2_L11 Int_ZF_2_1_L13 by simp
    } then show thesis by simp
  qed
  ultimately have (m+1) · E ≤ f(m·M) by (rule Induction_on_int)
  with A4 I have (m+1) · D ≤ f(m·M) using Int_ZF_1_3_L13A
    by simp
} then have ∀m ∈ ℤ+. (m+1) · D ≤ f(m·M) by simp
with II show thesis by auto
qed

```

A special case of Arthan\_Lem\_3 when  $D = 1$ .

```

corollary (in int1) Arthan_L_3_spec: assumes A1: f ∈ S+
  shows ∃M ∈ ℤ+. ∀n ∈ ℤ+. n+1 ≤ f(n·M)
proof -
  have ∀n ∈ ℤ+. n+1 ∈ ℤ
    using PositiveSet_def int_zero_one_are_int Int_ZF_1_1_L5
    by simp
  then have ∀n ∈ ℤ+. (n+1) · 1 = n+1
    using Int_ZF_1_1_L4 by simp
  moreover from A1 have ∃M ∈ ℤ+. ∀n ∈ ℤ+. (n+1) · 1 ≤ f(n·M)
    using int_one_two_are_pos Arthan_Lem_3 by simp
  ultimately show thesis by simp
qed

```

We know from Group\_ZF\_3.thy that finite range functions are almost homomorphisms. Besides reminding that fact for slopes the next lemma shows that finite range functions do not belong to  $S_+$ . This is important, because the projection of the set of finite range functions defines zero in the real

number construction in `Real_ZF_x.thy` series, while the projection of  $S_+$  becomes the set of (strictly) positive reals. We don't want zero to be positive, do we? The next lemma is a part of Lemma 5 in the Arthan's paper [2].

```
lemma (in int1) Int_ZF_2_3_L1B:
  assumes A1:  $f \in \text{FinRangeFunctions}(\mathbb{Z}, \mathbb{Z})$ 
  shows  $f \in S \implies f \notin S_+$ 
proof -
  from A1 show  $f \in S$  using Int_ZF_2_1_L1 group1.Group_ZF_3_3_L1
  by auto
  have  $\mathbb{Z}_+ \subseteq \mathbb{Z}$  using PositiveSet_def by auto
  with A1 have  $f(\mathbb{Z}_+) \in \text{Fin}(\mathbb{Z})$ 
  using Finite1_L21 by simp
  then have  $f(\mathbb{Z}_+) \cap \mathbb{Z}_+ \in \text{Fin}(\mathbb{Z})$ 
  using Fin_subset_lemma by blast
  thus  $f \notin S_+$  by auto
qed
```

We want to show that if  $f$  is a slope and neither  $f$  nor  $-f$  are in  $S_+$ , then  $f$  is bounded. The next lemma is the first step towards that goal and shows that if slope is not in  $S_+$  then  $f(\mathbb{Z}_+)$  is bounded above.

```
lemma (in int1) Int_ZF_2_3_L2: assumes A1:  $f \in S$  and A2:  $f \notin S_+$ 
  shows  $\text{IsBoundedAbove}(f(\mathbb{Z}_+), \text{IntegerOrder})$ 
proof -
  from A1 have  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  using AlmostHoms_def by simp
  then have  $f(\mathbb{Z}_+) \subseteq \mathbb{Z}$  using func1_1_L6 by simp
  moreover from A1 A2 have  $f(\mathbb{Z}_+) \cap \mathbb{Z}_+ \in \text{Fin}(\mathbb{Z})$  by auto
  ultimately show thesis using Int_ZF_2_T1 group3.OrderedGroup_ZF_2_L4
  by simp
qed
```

If  $f$  is a slope and  $-f \notin S_+$ , then  $f(\mathbb{Z}_+)$  is bounded below.

```
lemma (in int1) Int_ZF_2_3_L3: assumes A1:  $f \in S$  and A2:  $-f \notin S_+$ 
  shows  $\text{IsBoundedBelow}(f(\mathbb{Z}_+), \text{IntegerOrder})$ 
proof -
  from A1 have  $T: f: \mathbb{Z} \rightarrow \mathbb{Z}$  using AlmostHoms_def by simp
  then have  $-(f(\mathbb{Z}_+)) = (-f)(\mathbb{Z}_+)$ 
  using Int_ZF_1_T2 group0_2_T2 PositiveSet_def func1_1_L15C
  by auto
  with A1 A2 T show  $\text{IsBoundedBelow}(f(\mathbb{Z}_+), \text{IntegerOrder})$ 
  using Int_ZF_2_1_L12 Int_ZF_2_3_L2 PositiveSet_def func1_1_L6
  Int_ZF_2_T1 group3.OrderedGroup_ZF_2_L5 by simp
qed
```

A slope that is bounded on  $\mathbb{Z}_+$  is bounded everywhere.

```
lemma (in int1) Int_ZF_2_3_L4:
  assumes A1:  $f \in S$  and A2:  $m \in \mathbb{Z}$ 
  and A3:  $\forall n \in \mathbb{Z}_+. \text{abs}(f(n)) \leq L$ 
  shows  $\text{abs}(f(m)) \leq 2 \cdot \max \delta(f) + L$ 
```

```

proof -
  from A1 A3 have
     $0 \leq \text{abs}(f(1)) \quad \text{abs}(f(1)) \leq L$ 
    using int_zero_one_are_int Int_ZF_2_1_L2B int_abs_nonneg int_one_two_are_pos
    by auto
  then have II:  $0 \leq L$  by (rule Int_order_transitive)
  note A2
  moreover have  $\text{abs}(f(0)) \leq 2 \cdot \max \delta(f) + L$ 
  proof -
    from A1 have
       $\text{abs}(f(0)) \leq \max \delta(f) \quad 0 \leq \max \delta(f)$ 
      and T:  $\max \delta(f) \in \mathbb{Z}$ 
      using Int_ZF_2_1_L8 by auto
    with II have  $\text{abs}(f(0)) \leq \max \delta(f) + \max \delta(f) + L$ 
    using Int_ZF_2_L15F by simp
    with T show thesis using Int_ZF_1_1_L4 by simp
  qed
  moreover from A1 A3 II have
     $\forall n \in \mathbb{Z}_+. \text{abs}(f(n)) \leq 2 \cdot \max \delta(f) + L$ 
    using Int_ZF_2_1_L8 Int_ZF_1_3_L5A Int_ZF_2_L15F
    by simp
  moreover have  $\forall n \in \mathbb{Z}_+. \text{abs}(f(-n)) \leq 2 \cdot \max \delta(f) + L$ 
  proof
    fix n assume  $n \in \mathbb{Z}_+$ 
    with A1 A3 have
       $2 \cdot \max \delta(f) \in \mathbb{Z}$ 
       $\text{abs}(f(-n)) \leq 2 \cdot \max \delta(f) + \text{abs}(f(n))$ 
       $\text{abs}(f(n)) \leq L$ 
      using int_two_three_are_int Int_ZF_2_1_L8 Int_ZF_1_1_L5
      PositiveSet_def Int_ZF_2_1_L14 by auto
    then show  $\text{abs}(f(-n)) \leq 2 \cdot \max \delta(f) + L$ 
    using Int_ZF_2_L15A by blast
  qed
  ultimately show thesis by (rule Int_ZF_2_L19B)
qed

```

A slope whose image of the set of positive integers is bounded is a finite range function.

```

lemma (in int1) Int_ZF_2_3_L4A:
  assumes A1:  $f \in S$  and A2:  $\text{IsBounded}(f(\mathbb{Z}_+), \text{IntegerOrder})$ 
  shows  $f \in \text{FinRangeFunctions}(\mathbb{Z}, \mathbb{Z})$ 
proof -
  have T1:  $\mathbb{Z}_+ \subseteq \mathbb{Z}$  using PositiveSet_def by auto
  from A1 have T2:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  using AlmostHoms_def by simp
  from A2 obtain L where  $\forall a \in f(\mathbb{Z}_+). \text{abs}(a) \leq L$ 
  using Int_ZF_1_3_L20A by auto
  with T2 T1 have  $\forall n \in \mathbb{Z}_+. \text{abs}(f(n)) \leq L$ 
  by (rule func1_1_L15B)
  with A1 have  $\forall m \in \mathbb{Z}. \text{abs}(f(m)) \leq 2 \cdot \max \delta(f) + L$ 

```

```

    using Int_ZF_2_3_L4 by simp
  with T2 have  $f(\mathbb{Z}) \in \text{Fin}(\mathbb{Z})$ 
    by (rule Int_ZF_1_3_L20C)
  with T2 show  $f \in \text{FinRangeFunctions}(\mathbb{Z}, \mathbb{Z})$ 
    using FinRangeFunctions_def by simp
qed

```

A slope whose image of the set of positive integers is bounded below is a finite range function or a positive slope.

```

lemma (in int1) Int_ZF_2_3_L4B:
  assumes  $f \in \mathcal{S}$  and  $\text{IsBoundedBelow}(f(\mathbb{Z}_+), \text{IntegerOrder})$ 
  shows  $f \in \text{FinRangeFunctions}(\mathbb{Z}, \mathbb{Z}) \vee f \in \mathcal{S}_+$ 
  using assms Int_ZF_2_3_L2 IsBounded_def Int_ZF_2_3_L4A
  by auto

```

If one slope is not greater than another on positive integers, then they are almost equal or the difference is a positive slope.

```

lemma (in int1) Int_ZF_2_3_L4C: assumes A1:  $f \in \mathcal{S}$   $g \in \mathcal{S}$  and
  A2:  $\forall n \in \mathbb{Z}_+. f(n) \leq g(n)$ 
  shows  $f \sim g \vee g + (-f) \in \mathcal{S}_+$ 
proof -
  let h =  $g + (-f)$ 
  from A1 have  $(-f) \in \mathcal{S}$  using Int_ZF_2_1_L12
    by simp
  with A1 have I:  $h \in \mathcal{S}$  using Int_ZF_2_1_L12C
    by simp
  moreover have  $\text{IsBoundedBelow}(h(\mathbb{Z}_+), \text{IntegerOrder})$ 
  proof -
    from I have
       $h: \mathbb{Z} \rightarrow \mathbb{Z}$  and  $\mathbb{Z}_+ \subseteq \mathbb{Z}$  using AlmostHoms_def PositiveSet_def
      by auto
    moreover from A1 A2 have  $\forall n \in \mathbb{Z}_+. \langle 0, h(n) \rangle \in \text{IntegerOrder}$ 
      using Int_ZF_2_1_L2B PositiveSet_def Int_ZF_1_3_L10A
      Int_ZF_2_1_L12 Int_ZF_2_1_L12B Int_ZF_2_1_L12A
      by simp
    ultimately show  $\text{IsBoundedBelow}(h(\mathbb{Z}_+), \text{IntegerOrder})$ 
      by (rule func_ZF_8_L1)
  qed
  ultimately have  $h \in \text{FinRangeFunctions}(\mathbb{Z}, \mathbb{Z}) \vee h \in \mathcal{S}_+$ 
    using Int_ZF_2_3_L4B by simp
  with A1 show  $f \sim g \vee g + (-f) \in \mathcal{S}_+$ 
    using Int_ZF_2_1_L9C by auto
qed

```

Positive slopes are arbitrarily large for large enough arguments.

```

lemma (in int1) Int_ZF_2_3_L5:
  assumes A1:  $f \in \mathcal{S}_+$  and A2:  $K \in \mathbb{Z}$ 
  shows  $\exists N \in \mathbb{Z}_+. \forall m. N \leq m \longrightarrow K \leq f(m)$ 

```

```

proof -
  from A1 obtain M where I:  $M \in \mathbb{Z}_+$  and II:  $\forall n \in \mathbb{Z}_+. n+1 \leq f(n \cdot M)$ 
    using Arthan_L_3_spec by auto
  let j = GreaterOf(IntegerOrder, M, K - (minf(f, 0..(M-1)) - maxδ(f)) -
1)
  from A1 I have T1:
    minf(f, 0..(M-1)) - maxδ(f)  $\in \mathbb{Z}$   $M \in \mathbb{Z}$ 
    using Int_ZF_2_1_L15 Int_ZF_2_1_L8 Int_ZF_1_1_L5 PositiveSet_def
    by auto
  with A2 I have T2:
    K - (minf(f, 0..(M-1)) - maxδ(f))  $\in \mathbb{Z}$ 
    K - (minf(f, 0..(M-1)) - maxδ(f)) - 1  $\in \mathbb{Z}$ 
    using Int_ZF_1_1_L5 int_zero_one_are_int by auto
  with T1 have III:  $M \leq j$  and
    K - (minf(f, 0..(M-1)) - maxδ(f)) - 1  $\leq j$ 
    using Int_ZF_1_3_L18 by auto
  with A2 T1 T2 have
    IV:  $K \leq j+1 + (\text{minf}(f, 0..(M-1)) - \text{max}\delta(f))$ 
    using int_zero_one_are_int Int_ZF_2_L9C by simp
  let N = GreaterOf(IntegerOrder, 1, j·M)
  from T1 III have T3:  $j \in \mathbb{Z}$   $j \cdot M \in \mathbb{Z}$ 
    using Int_ZF_2_L1A Int_ZF_1_1_L5 by auto
  then have V:  $N \in \mathbb{Z}_+$  and VI:  $j \cdot M \leq N$ 
    using int_zero_one_are_int Int_ZF_1_5_L3 Int_ZF_1_3_L18
    by auto
  { fix m
    let n = m zdiv M
    let k = m zmod M
    assume  $N \leq m$ 
    with VI have  $j \cdot M \leq m$  by (rule Int_order_transitive)
    with I III have
      VII:  $m = n \cdot M + k$ 
       $j \leq n$  and
      VIII:  $n \in \mathbb{Z}_+$   $k \in 0..(M-1)$ 
      using IntDiv_ZF_1_L5 by auto
    with II have
       $j + 1 \leq n + 1$   $n+1 \leq f(n \cdot M)$ 
      using int_zero_one_are_int int_ord_transl_inv by auto
    then have  $j + 1 \leq f(n \cdot M)$ 
      by (rule Int_order_transitive)
    with T1 have
       $j+1 + (\text{minf}(f, 0..(M-1)) - \text{max}\delta(f)) \leq$ 
       $f(n \cdot M) + (\text{minf}(f, 0..(M-1)) - \text{max}\delta(f))$ 
      using int_ord_transl_inv by simp
    with IV have  $K \leq f(n \cdot M) + (\text{minf}(f, 0..(M-1)) - \text{max}\delta(f))$ 
      by (rule Int_order_transitive)
    moreover from A1 I VIII have
       $f(n \cdot M) + (\text{minf}(f, 0..(M-1)) - \text{max}\delta(f)) \leq f(n \cdot M + k)$ 
      using PositiveSet_def Int_ZF_2_1_L16 by simp
  }

```



```

ultimately have  $K \leq f(n \cdot M + k)$ 
  by (rule Int_order_transitive)
with VII have  $K \leq f(m)$  by simp
} then have  $\forall m. N \leq m \longrightarrow K \leq f(m)$ 
  by simp
with V show thesis by auto
qed

```

Positive slopes are arbitrarily small for small enough arguments. Kind of dual to Int\_ZF\_2\_3\_L5.

**lemma** (in int1) Int\_ZF\_2\_3\_L5A: assumes  $A1: f \in S_+$  and  $A2: K \in \mathbb{Z}$   
 shows  $\exists N \in \mathbb{Z}_+. \forall m. N \leq m \longrightarrow f(-m) \leq K$

```

proof -
  from A1 have T1:  $\text{abs}(f(0)) + \max \delta(f) \in \mathbb{Z}$ 
    using Int_ZF_2_1_L8 by auto
  with A2 have  $\text{abs}(f(0)) + \max \delta(f) - K \in \mathbb{Z}$ 
    using Int_ZF_1_1_L5 by simp
  with A1 have
     $\exists N \in \mathbb{Z}_+. \forall m. N \leq m \longrightarrow \text{abs}(f(0)) + \max \delta(f) - K \leq f(m)$ 
    using Int_ZF_2_3_L5 by simp
  then obtain N where I:  $N \in \mathbb{Z}_+$  and II:
     $\forall m. N \leq m \longrightarrow \text{abs}(f(0)) + \max \delta(f) - K \leq f(m)$ 
    by auto
  { fix m assume A3:  $N \leq m$ 
    with A1 have
       $f(-m) \leq \text{abs}(f(0)) + \max \delta(f) - f(m)$ 
      using Int_ZF_2_L1A Int_ZF_2_1_L14 by simp
    moreover
      from II T1 A3 have  $\text{abs}(f(0)) + \max \delta(f) - f(m) \leq$ 
         $(\text{abs}(f(0)) + \max \delta(f)) - (\text{abs}(f(0)) + \max \delta(f) - K)$ 
        using Int_ZF_2_L10 int_ord_transl_inv by simp
      with A2 T1 have  $\text{abs}(f(0)) + \max \delta(f) - f(m) \leq K$ 
        using Int_ZF_1_2_L3 by simp
      ultimately have  $f(-m) \leq K$ 
        by (rule Int_order_transitive)
    } then have  $\forall m. N \leq m \longrightarrow f(-m) \leq K$ 
      by simp
  with I show thesis by auto
qed

```

A special case of Int\_ZF\_2\_3\_L5 where  $K = 1$ .

**corollary** (in int1) Int\_ZF\_2\_3\_L6: assumes  $f \in S_+$   
 shows  $\exists N \in \mathbb{Z}_+. \forall m. N \leq m \longrightarrow f(m) \in \mathbb{Z}_+$   
 using assms int\_zero\_one\_are\_int Int\_ZF\_2\_3\_L5 Int\_ZF\_1\_5\_L3  
 by simp

A special case of Int\_ZF\_2\_3\_L5 where  $m = N$ .

**corollary** (in int1) Int\_ZF\_2\_3\_L6A: assumes  $f \in S_+$  and  $K \in \mathbb{Z}$   
 shows  $\exists N \in \mathbb{Z}_+. K \leq f(N)$

```

proof -
  from assms have  $\exists N \in \mathbb{Z}_+. \forall m. N \leq m \longrightarrow K \leq f(m)$ 
    using Int_ZF_2_3_L5 by simp
  then obtain N where I:  $N \in \mathbb{Z}_+$  and II:  $\forall m. N \leq m \longrightarrow K \leq f(m)$ 
    by auto
  then show thesis using PositiveSet_def int_ord_is_refl refl_def
    by auto
qed

```

If values of a slope are not bounded above, then the slope is positive.

```

lemma (in int1) Int_ZF_2_3_L7: assumes A1:  $f \in \mathcal{S}$ 
  and A2:  $\forall K \in \mathbb{Z}. \exists n \in \mathbb{Z}_+. K \leq f(n)$ 
  shows  $f \in \mathcal{S}_+$ 
proof -
  { fix K assume  $K \in \mathbb{Z}$ 
    with A2 obtain n where  $n \in \mathbb{Z}_+ \quad K \leq f(n)$ 
      by auto
    moreover from A1 have  $\mathbb{Z}_+ \subseteq \mathbb{Z} \quad f: \mathbb{Z} \rightarrow \mathbb{Z}$ 
      using PositiveSet_def AlmostHoms_def by auto
    ultimately have  $\exists m \in f(\mathbb{Z}_+). K \leq m$ 
      using func1_1_L15D by auto
  } then have  $\forall K \in \mathbb{Z}. \exists m \in f(\mathbb{Z}_+). K \leq m$  by simp
  with A1 show  $f \in \mathcal{S}_+$  using Int_ZF_4_L9 Int_ZF_2_3_L2
    by auto
qed

```

For unbounded slope  $f$  either  $f \in \mathcal{S}_+$  or  $-f \in \mathcal{S}_+$ .

```

theorem (in int1) Int_ZF_2_3_L8:
  assumes A1:  $f \in \mathcal{S}$  and A2:  $f \notin \text{FinRangeFunctions}(\mathbb{Z}, \mathbb{Z})$ 
  shows  $(f \in \mathcal{S}_+) \text{ Xor } ((-f) \in \mathcal{S}_+)$ 
proof -
  have T1:  $\mathbb{Z}_+ \subseteq \mathbb{Z}$  using PositiveSet_def by auto
  from A1 have T2:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  using AlmostHoms_def by simp
  then have I:  $f(\mathbb{Z}_+) \subseteq \mathbb{Z}$  using func1_1_L6 by auto
  from A1 A2 have  $f \in \mathcal{S}_+ \vee (-f) \in \mathcal{S}_+$ 
    using Int_ZF_2_3_L2 Int_ZF_2_3_L3 IsBounded_def Int_ZF_2_3_L4A
    by blast
  moreover have  $\neg(f \in \mathcal{S}_+ \wedge (-f) \in \mathcal{S}_+)$ 
  proof -
    { assume A3:  $f \in \mathcal{S}_+$  and A4:  $(-f) \in \mathcal{S}_+$ 
      from A3 obtain N1 where
        I:  $N1 \in \mathbb{Z}_+$  and II:  $\forall m. N1 \leq m \longrightarrow f(m) \in \mathbb{Z}_+$ 
      using Int_ZF_2_3_L6 by auto
      from A4 obtain N2 where
        III:  $N2 \in \mathbb{Z}_+$  and IV:  $\forall m. N2 \leq m \longrightarrow (-f)(m) \in \mathbb{Z}_+$ 
      using Int_ZF_2_3_L6 by auto
      let N = GreaterOf(IntegerOrder, N1, N2)
      from I III have  $N1 \leq N \quad N2 \leq N$ 
      using PositiveSet_def Int_ZF_1_3_L18 by auto
    }
  qed

```

```

      with A1 II IV have
f(N) ∈ ℤ+  (-f)(N) ∈ ℤ+  (-f)(N) = -(f(N))
using Int_ZF_2_L1A PositiveSet_def Int_ZF_2_1_L12A
by auto
      then have False using Int_ZF_1_5_L8 by simp
    } thus thesis by auto
qed
ultimately show (f ∈ S+) Xor ((-f) ∈ S+)
using Xor_def by simp
qed

```

The sum of positive slopes is a positive slope.

```

theorem (in int1) sum_of_pos_sls_is_pos_sl:
  assumes A1: f ∈ S+  g ∈ S+
  shows f+g ∈ S+
proof -
  { fix K assume K∈ℤ
    with A1 have ∃N∈ℤ+. ∀m. N≤m ⟶ K ≤ f(m)
      using Int_ZF_2_3_L5 by simp
    then obtain N where I: N∈ℤ+ and II: ∀m. N≤m ⟶ K ≤ f(m)
      by auto
    from A1 have ∃M∈ℤ+. ∀m. M≤m ⟶ 0 ≤ g(m)
      using int_zero_one_are_int Int_ZF_2_3_L5 by simp
    then obtain M where III: M∈ℤ+ and IV: ∀m. M≤m ⟶ 0 ≤ g(m)
      by auto
    let L = GreaterOf(IntegerOrder,N,M)
    from I III have V: L ∈ ℤ+  ℤ+ ⊆ ℤ
      using GreaterOf_def PositiveSet_def by auto
    moreover from A1 V have (f+g)(L) = f(L) + g(L)
      using Int_ZF_2_1_L12B by auto
    moreover from I II III IV have K ≤ f(L) + g(L)
      using PositiveSet_def Int_ZF_1_3_L18 Int_ZF_2_L15F
      by simp
    ultimately have L ∈ ℤ+  K ≤ (f+g)(L)
      by auto
    then have ∃n ∈ ℤ+. K ≤ (f+g)(n)
      by auto
  } with A1 show f+g ∈ S+
  using Int_ZF_2_1_L12C Int_ZF_2_3_L7 by simp
qed

```

The composition of positive slopes is a positive slope.

```

theorem (in int1) comp_of_pos_sls_is_pos_sl:
  assumes A1: f ∈ S+  g ∈ S+
  shows f◦g ∈ S+
proof -
  { fix K assume K∈ℤ
    with A1 have ∃N∈ℤ+. ∀m. N≤m ⟶ K ≤ f(m)
      using Int_ZF_2_3_L5 by simp

```

```

    then obtain N where  $N \in \mathbb{Z}_+$  and I:  $\forall m. N \leq m \longrightarrow K \leq f(m)$ 
      by auto
    with A1 have  $\exists M \in \mathbb{Z}_+. N \leq g(M)$ 
      using PositiveSet_def Int_ZF_2_3_L6A by simp
    then obtain M where  $M \in \mathbb{Z}_+ \quad N \leq g(M)$ 
      by auto
    with A1 I have  $\exists M \in \mathbb{Z}_+. K \leq (f \circ g)(M)$ 
      using PositiveSet_def Int_ZF_2_1_L10
      by auto
  } with A1 show  $f \circ g \in S_+$ 
    using Int_ZF_2_1_L11 Int_ZF_2_3_L7
    by simp
qed

```

A slope equivalent to a positive one is positive.

```

lemma (in int1) Int_ZF_2_3_L9:
  assumes A1:  $f \in S_+$  and A2:  $\langle f, g \rangle \in \text{AlEqRel}$  shows  $g \in S_+$ 
proof -
  from A2 have T:  $g \in S$  and  $\exists L \in \mathbb{Z}. \forall m \in \mathbb{Z}. \text{abs}(f(m) - g(m)) \leq L$ 
    using Int_ZF_2_1_L9A by auto
  then obtain L where
    I:  $L \in \mathbb{Z}$  and II:  $\forall m \in \mathbb{Z}. \text{abs}(f(m) - g(m)) \leq L$ 
    by auto
  { fix K assume A3:  $K \in \mathbb{Z}$ 
    with I have  $K + L \in \mathbb{Z}$ 
      using Int_ZF_1_1_L5 by simp
    with A1 obtain M where III:  $M \in \mathbb{Z}_+$  and IV:  $K + L \leq f(M)$ 
      using Int_ZF_2_3_L6A by auto
    with A1 A3 I have  $K \leq f(M) - L$ 
      using PositiveSet_def Int_ZF_2_1_L2B Int_ZF_2_L9B
      by simp
    moreover from A1 T II III have
       $f(M) - L \leq g(M)$ 
      using PositiveSet_def Int_ZF_2_1_L2B Int_triangle_ineq2
      by simp
    ultimately have  $K \leq g(M)$ 
      by (rule Int_order_transitive)
    with III have  $\exists n \in \mathbb{Z}_+. K \leq g(n)$ 
      by auto
  } with T show  $g \in S_+$ 
    using Int_ZF_2_3_L7 by simp
qed

```

The set of positive slopes is saturated with respect to the relation of equivalence of slopes.

```

lemma (in int1) pos_slopes_saturated: shows IsSaturated( $\text{AlEqRel}, S_+$ )
proof -
  have
    equiv( $S, \text{AlEqRel}$ )

```

```

    AlEqRel  $\subseteq \mathcal{S} \times \mathcal{S}$ 
    using Int_ZF_2_1_L9B by auto
    moreover have  $\mathcal{S}_+ \subseteq \mathcal{S}$  by auto
    moreover have  $\forall f \in \mathcal{S}_+. \forall g \in \mathcal{S}. \langle f, g \rangle \in \text{AlEqRel} \longrightarrow g \in \mathcal{S}_+$ 
    using Int_ZF_2_3_L9 by blast
    ultimately show IsSaturated(AlEqRel,  $\mathcal{S}_+$ )
    by (rule EquivClass_3_L3)
qed

```

A technical lemma involving a projection of the set of positive slopes and a logical expression with exclusive or.

```

lemma (in int1) Int_ZF_2_3_L10:
  assumes A1:  $f \in \mathcal{S} \quad g \in \mathcal{S}$ 
  and A2:  $R = \{\text{AlEqRel}\{s\}. s \in \mathcal{S}_+\}$ 
  and A3:  $(f \in \mathcal{S}_+) \text{ Xor } (g \in \mathcal{S}_+)$ 
  shows  $(\text{AlEqRel}\{f\} \in R) \text{ Xor } (\text{AlEqRel}\{g\} \in R)$ 
proof -
  from A1 A2 A3 have
    equiv( $\mathcal{S}$ , AlEqRel)
    IsSaturated(AlEqRel,  $\mathcal{S}_+$ )
     $\mathcal{S}_+ \subseteq \mathcal{S}$ 
     $f \in \mathcal{S} \quad g \in \mathcal{S}$ 
     $R = \{\text{AlEqRel}\{s\}. s \in \mathcal{S}_+\}$ 
     $(f \in \mathcal{S}_+) \text{ Xor } (g \in \mathcal{S}_+)$ 
    using pos_slopes_saturated Int_ZF_2_1_L9B by auto
  then show thesis by (rule EquivClass_3_L7)
qed

```

Identity function is a positive slope.

```

lemma (in int1) Int_ZF_2_3_L11: shows  $\text{id}(\mathbb{Z}) \in \mathcal{S}_+$ 
proof -
  let f = id( $\mathbb{Z}$ )
  { fix K assume  $K \in \mathbb{Z}$ 
    then obtain n where T:  $n \in \mathbb{Z}_+$  and  $K \leq n$ 
    using Int_ZF_1_5_L9 by auto
    moreover from T have  $f(n) = n$ 
    using PositiveSet_def by simp
    ultimately have  $n \in \mathbb{Z}_+$  and  $K \leq f(n)$ 
    by auto
    then have  $\exists n \in \mathbb{Z}_+. K \leq f(n)$  by auto
  } then show  $f \in \mathcal{S}_+$ 
  using Int_ZF_2_1_L17 Int_ZF_2_3_L7 by simp
qed

```

The identity function is not almost equal to any bounded function.

```

lemma (in int1) Int_ZF_2_3_L12: assumes A1:  $f \in \text{FinRangeFunctions}(\mathbb{Z}, \mathbb{Z})$ 
  shows  $\neg(\text{id}(\mathbb{Z}) \sim f)$ 
proof -
  { from A1 have  $\text{id}(\mathbb{Z}) \in \mathcal{S}_+$ 

```

```

      using Int_ZF_2_3_L11 by simp
    moreover assume  $\langle \text{id}(\mathbb{Z}), f \rangle \in \text{AlEqRel}$ 
    ultimately have  $f \in S_+$ 
      by (rule Int_ZF_2_3_L9)
    with A1 have False using Int_ZF_2_3_L1B
      by simp
  } then show  $\neg(\text{id}(\mathbb{Z}) \sim f)$  by auto
qed

```

### 38.2 Inverting slopes

Not every slope is a 1:1 function. However, we can still invert slopes in the sense that if  $f$  is a slope, then we can find a slope  $g$  such that  $f \circ g$  is almost equal to the identity function. The goal of this section is to establish this fact for positive slopes.

If  $f$  is a positive slope, then for every positive integer  $p$  the set  $\{n \in \mathbb{Z}_+ : p \leq f(n)\}$  is a nonempty subset of positive integers. Recall that  $f^{-1}(p)$  is the notation for the smallest element of this set.

```

lemma (in int1) Int_ZF_2_4_L1:
  assumes A1:  $f \in S_+$  and A2:  $p \in \mathbb{Z}_+$  and A3:  $A = \{n \in \mathbb{Z}_+ . p \leq f(n)\}$ 
  shows
     $A \subseteq \mathbb{Z}_+$ 
     $A \neq 0$ 
     $f^{-1}(p) \in A$ 
     $\forall m \in A. f^{-1}(p) \leq m$ 
proof -
  from A3 show I:  $A \subseteq \mathbb{Z}_+$  by auto
  from A1 A2 have  $\exists n \in \mathbb{Z}_+ . p \leq f(n)$ 
    using PositiveSet_def Int_ZF_2_3_L6A by simp
  with A3 show II:  $A \neq 0$  by auto
  from A3 I II show
     $f^{-1}(p) \in A$ 
     $\forall m \in A. f^{-1}(p) \leq m$ 
    using Int_ZF_1_5_L1C by auto
qed

```

If  $f$  is a positive slope and  $p$  is a positive integer  $p$ , then  $f^{-1}(p)$  (defined as the minimum of the set  $\{n \in \mathbb{Z}_+ : p \leq f(n)\}$ ) is a (well defined) positive integer.

```

lemma (in int1) Int_ZF_2_4_L2:
  assumes  $f \in S_+$  and  $p \in \mathbb{Z}_+$ 
  shows
     $f^{-1}(p) \in \mathbb{Z}_+$ 
     $p \leq f(f^{-1}(p))$ 
  using assms Int_ZF_2_4_L1 by auto

```

If  $f$  is a positive slope and  $p$  is a positive integer such that  $n \leq f(p)$ , then

$$f^{-1}(n) \leq p.$$

```

lemma (in int1) Int_ZF_2_4_L3:
  assumes f ∈ S+ and m ∈ ℤ+ p ∈ ℤ+ and m ≤ f(p)
  shows f-1(m) ≤ p
  using assms Int_ZF_2_4_L1 by simp

```

An upper bound  $f(f^{-1}(m) - 1)$  for positive slopes.

```

lemma (in int1) Int_ZF_2_4_L4:
  assumes A1: f ∈ S+ and A2: m ∈ ℤ+ and A3: f-1(m)-1 ∈ ℤ+
  shows f(f-1(m)-1) ≤ m   f(f-1(m)-1) ≠ m
proof -
  from A1 A2 have T: f-1(m) ∈ ℤ using Int_ZF_2_4_L2 PositiveSet_def
  by simp
  from A1 A3 have f: ℤ → ℤ and f-1(m)-1 ∈ ℤ
  using Int_ZF_2_3_L1 PositiveSet_def by auto
  with A1 A2 have T1: f(f-1(m)-1) ∈ ℤ m ∈ ℤ
  using apply_funtype PositiveSet_def by auto
  { assume m ≤ f(f-1(m)-1)
    with A1 A2 A3 have f-1(m) ≤ f-1(m)-1
    by (rule Int_ZF_2_4_L3)
    with T have False using Int_ZF_1_2_L3AA
    by simp
  } then have I: ¬(m ≤ f(f-1(m)-1)) by auto
  with T1 show f(f-1(m)-1) ≤ m
  by (rule Int_ZF_2_L19)
  from T1 I show f(f-1(m)-1) ≠ m
  by (rule Int_ZF_2_L19)
qed

```

The (candidate for) the inverse of a positive slope is nondecreasing.

```

lemma (in int1) Int_ZF_2_4_L5:
  assumes A1: f ∈ S+ and A2: m ∈ ℤ+ and A3: m ≤ n
  shows f-1(m) ≤ f-1(n)
proof -
  from A2 A3 have T: n ∈ ℤ+ using Int_ZF_1_5_L7 by blast
  with A1 have n ≤ f(f-1(n)) using Int_ZF_2_4_L2
  by simp
  with A3 have m ≤ f(f-1(n)) by (rule Int_order_transitive)
  with A1 A2 T show f-1(m) ≤ f-1(n)
  using Int_ZF_2_4_L2 Int_ZF_2_4_L3 by simp
qed

```

If  $f^{-1}(m)$  is positive and  $n$  is a positive integer, then, then  $f^{-1}(m + n) - 1$  is positive.

```

lemma (in int1) Int_ZF_2_4_L6:
  assumes A1: f ∈ S+ and A2: m ∈ ℤ+ n ∈ ℤ+ and
  A3: f-1(m)-1 ∈ ℤ+
  shows f-1(m+n)-1 ∈ ℤ+

```

```

proof -
  from A1 A2 have  $f^{-1}(m)-1 \leq f^{-1}(m+n) - 1$ 
    using PositiveSet_def Int_ZF_1_5_L7A Int_ZF_2_4_L2
      Int_ZF_2_4_L5 int_zero_one_are_int Int_ZF_1_1_L4
      int_ord_transl_inv by simp
  with A3 show  $f^{-1}(m+n)-1 \in \mathbb{Z}_+$  using Int_ZF_1_5_L7
    by blast
qed

```

If  $f$  is a slope, then  $f(f^{-1}(m+n) - f^{-1}(m) - f^{-1}(n))$  is uniformly bounded above and below. Will it be the messiest IsarMathLib proof ever? Only time will tell.

```

lemma (in int1) Int_ZF_2_4_L7:  assumes A1:  $f \in \mathcal{S}_+$  and
  A2:  $\forall m \in \mathbb{Z}_+. f^{-1}(m)-1 \in \mathbb{Z}_+$ 
  shows
     $\exists U \in \mathbb{Z}. \forall m \in \mathbb{Z}_+. \forall n \in \mathbb{Z}_+. f(f^{-1}(m+n)-f^{-1}(m)-f^{-1}(n)) \leq U$ 
     $\exists N \in \mathbb{Z}. \forall m \in \mathbb{Z}_+. \forall n \in \mathbb{Z}_+. N \leq f(f^{-1}(m+n)-f^{-1}(m)-f^{-1}(n))$ 

```

```

proof -
  from A1 have  $\exists L \in \mathbb{Z}. \forall r \in \mathbb{Z}. f(r) \leq f(r-1) + L$ 
    using Int_ZF_2_1_L28 by simp
  then obtain L where
    I:  $L \in \mathbb{Z}$  and II:  $\forall r \in \mathbb{Z}. f(r) \leq f(r-1) + L$ 
    by auto
  from A1 have
     $\exists M \in \mathbb{Z}. \forall r \in \mathbb{Z}. \forall p \in \mathbb{Z}. \forall q \in \mathbb{Z}. f(r-p-q) \leq f(r)-f(p)-f(q)+M$ 
     $\exists K \in \mathbb{Z}. \forall r \in \mathbb{Z}. \forall p \in \mathbb{Z}. \forall q \in \mathbb{Z}. f(r)-f(p)-f(q)+K \leq f(r-p-q)$ 
    using Int_ZF_2_1_L30 by auto
  then obtain M K where III:  $M \in \mathbb{Z}$  and
    IV:  $\forall r \in \mathbb{Z}. \forall p \in \mathbb{Z}. \forall q \in \mathbb{Z}. f(r-p-q) \leq f(r)-f(p)-f(q)+M$ 
    and
    V:  $K \in \mathbb{Z}$  and VI:  $\forall r \in \mathbb{Z}. \forall p \in \mathbb{Z}. \forall q \in \mathbb{Z}. f(r)-f(p)-f(q)+K \leq f(r-p-q)$ 
    by auto
  from I III V have
     $L+M \in \mathbb{Z} \quad (-L) - L + K \in \mathbb{Z}$ 
    using Int_ZF_1_1_L4 Int_ZF_1_1_L5 by auto
  moreover
    { fix m n
      assume A3:  $m \in \mathbb{Z}_+ \quad n \in \mathbb{Z}_+$ 
      have  $f(f^{-1}(m+n)-f^{-1}(m)-f^{-1}(n)) \leq L+M \wedge$ 
         $(-L)-L+K \leq f(f^{-1}(m+n)-f^{-1}(m)-f^{-1}(n))$ 
      proof -
        let r =  $f^{-1}(m+n)$ 
        let p =  $f^{-1}(m)$ 
        let q =  $f^{-1}(n)$ 
        from A1 A3 have T1:
           $p \in \mathbb{Z}_+ \quad q \in \mathbb{Z}_+ \quad r \in \mathbb{Z}_+$ 
          using Int_ZF_2_4_L2 pos_int_closed_add_unfolded by auto
        with A3 have T2:
           $m \in \mathbb{Z} \quad n \in \mathbb{Z} \quad p \in \mathbb{Z} \quad q \in \mathbb{Z} \quad r \in \mathbb{Z}$ 

```



```

    using PositiveSet_def by auto
from A2 A3 have T3:
   $r-1 \in \mathbb{Z}_+$   $p-1 \in \mathbb{Z}_+$   $q-1 \in \mathbb{Z}_+$ 
    using pos_int_closed_add_unfolded by auto
from A1 A3 have VII:
   $m+n \leq f(r)$ 
   $m \leq f(p)$ 
   $n \leq f(q)$ 
    using Int_ZF_2_4_L2 pos_int_closed_add_unfolded by auto
from A1 A3 T3 have VIII:
   $f(r-1) \leq m+n$ 
   $f(p-1) \leq m$ 
   $f(q-1) \leq n$ 
    using pos_int_closed_add_unfolded Int_ZF_2_4_L4 by auto
have  $f(r-p-q) \leq L+M$ 
proof -
  from IV T2 have  $f(r-p-q) \leq f(r)-f(p)-f(q)+M$ 
    by simp
  moreover
  from I II T2 VIII have
     $f(r) \leq f(r-1) + L$ 
     $f(r-1) + L \leq m+n+L$ 
    using int_ord_transl_inv by auto
  then have  $f(r) \leq m+n+L$ 
    by (rule Int_order_transitive)
  with VII have  $f(r) - f(p) \leq m+n+L-m$ 
    using int_ineq_add_sides by simp
  with I T2 VII have  $f(r) - f(p) - f(q) \leq n+L-n$ 
    using Int_ZF_1_2_L9 int_ineq_add_sides by simp
  with I III T2 have  $f(r) - f(p) - f(q) + M \leq L+M$ 
    using Int_ZF_1_2_L3 int_ord_transl_inv by simp
  ultimately show  $f(r-p-q) \leq L+M$ 
    by (rule Int_order_transitive)
qed
moreover have  $(-L)-L +K \leq f(r-p-q)$ 
proof -
  from I II T2 VIII have
     $f(p) \leq f(p-1) + L$ 
     $f(p-1) + L \leq m +L$ 
    using int_ord_transl_inv by auto
  then have  $f(p) \leq m +L$ 
    by (rule Int_order_transitive)
  with VII have  $m+n -(m+L) \leq f(r) - f(p)$ 
    using int_ineq_add_sides by simp
  with I T2 have  $n - L \leq f(r) - f(p)$ 
    using Int_ZF_1_2_L9 by simp
  moreover
  from I II T2 VIII have
     $f(q) \leq f(q-1) + L$ 

```

```

      f(q-1) + L ≤ n + L
      using int_ord_transl_inv by auto
    then have f(q) ≤ n + L
      by (rule Int_order_transitive)
    ultimately have
      n - L - (n+L) ≤ f(r) - f(p) - f(q)
      using int_ineq_add_sides by simp
    with I V T2 have
      (-L)-L +K ≤ f(r) - f(p) - f(q) + K
      using Int_ZF_1_2_L3 int_ord_transl_inv by simp
    moreover from VI T2 have
      f(r) - f(p) - f(q) + K ≤ f(r-p-q)
      by simp
    ultimately show (-L)-L +K ≤ f(r-p-q)
      by (rule Int_order_transitive)
  qed
  ultimately show
    f(r-p-q) ≤ L+M ∧
    (-L)-L+K ≤ f(f-1(m+n)-f-1(m)-f-1(n))
    by simp
  qed
}
ultimately show
  ∃U∈ℤ. ∀m∈ℤ+. ∀n∈ℤ+. f(f-1(m+n)-f-1(m)-f-1(n)) ≤ U
  ∃N∈ℤ. ∀m∈ℤ+. ∀n∈ℤ+. N ≤ f(f-1(m+n)-f-1(m)-f-1(n))
  by auto
qed

```

The expression  $f^{-1}(m+n) - f^{-1}(m) - f^{-1}(n)$  is uniformly bounded for all pairs  $\langle m, n \rangle \in \mathbb{Z}_+ \times \mathbb{Z}_+$ . Recall that in the `int1` context  $\varepsilon(f, x)$  is defined so that  $\varepsilon(f, \langle m, n \rangle) = f^{-1}(m+n) - f^{-1}(m) - f^{-1}(n)$ .

**lemma** (in `int1`) `Int_ZF_2_4_L8`: assumes `A1`:  $f \in \mathcal{S}_+$  and  
`A2`:  $\forall m \in \mathbb{Z}_+. f^{-1}(m) - 1 \in \mathbb{Z}_+$   
 shows  $\exists M. \forall x \in \mathbb{Z}_+ \times \mathbb{Z}_+. \text{abs}(\varepsilon(f, x)) \leq M$

**proof** -

from `A1 A2` have

```

  ∃U∈ℤ. ∀m∈ℤ+. ∀n∈ℤ+. f(f-1(m+n)-f-1(m)-f-1(n)) ≤ U
  ∃N∈ℤ. ∀m∈ℤ+. ∀n∈ℤ+. N ≤ f(f-1(m+n)-f-1(m)-f-1(n))
  using Int_ZF_2_4_L7 by auto

```

then obtain `U N` where `I`:

```

  ∀m∈ℤ+. ∀n∈ℤ+. f(f-1(m+n)-f-1(m)-f-1(n)) ≤ U
  ∀m∈ℤ+. ∀n∈ℤ+. N ≤ f(f-1(m+n)-f-1(m)-f-1(n))
  by auto

```

have  $\mathbb{Z}_+ \times \mathbb{Z}_+ \neq 0$  using `int_one_two_are_pos` by auto

moreover from `A1` have  $f: \mathbb{Z} \rightarrow \mathbb{Z}$

using `AlmostHoms_def` by simp

moreover from `A1` have

```

  ∀a∈ℤ. ∃b∈ℤ+. ∀x. b ≤ x ⟶ a ≤ f(x)
  using Int_ZF_2_3_L5 by simp

```

```

moreover from A1 have
   $\forall a \in \mathbb{Z}. \exists b \in \mathbb{Z}_+. \forall y. b \leq y \longrightarrow f(-y) \leq a$ 
  using Int_ZF_2_3_L5A by simp
moreover have
   $\forall x \in \mathbb{Z}_+ \times \mathbb{Z}_+. \varepsilon(f, x) \in \mathbb{Z} \wedge f(\varepsilon(f, x)) \leq U \wedge N \leq f(\varepsilon(f, x))$ 
proof -
  { fix x assume A3:  $x \in \mathbb{Z}_+ \times \mathbb{Z}_+$ 
    let m = fst(x)
    let n = snd(x)
    from A3 have T:  $m \in \mathbb{Z}_+ \quad n \in \mathbb{Z}_+ \quad m+n \in \mathbb{Z}_+$ 
  using pos_int_closed_add_unfolded by auto
  with A1 have
     $f^{-1}(m+n) \in \mathbb{Z} \quad f^{-1}(m) \in \mathbb{Z} \quad f^{-1}(n) \in \mathbb{Z}$ 
  using Int_ZF_2_4_L2 PositiveSet_def by auto
  with I T have
     $\varepsilon(f, x) \in \mathbb{Z} \wedge f(\varepsilon(f, x)) \leq U \wedge N \leq f(\varepsilon(f, x))$ 
  using Int_ZF_1_1_L5 by auto
  } thus thesis by simp
qed
ultimately show  $\exists M. \forall x \in \mathbb{Z}_+ \times \mathbb{Z}_+. \text{abs}(\varepsilon(f, x)) \leq M$ 
by (rule Int_ZF_1_6_L4)
qed

```

The (candidate for) inverse of a positive slope is a (well defined) function on  $\mathbb{Z}_+$ .

```

lemma (in int1) Int_ZF_2_4_L9:
  assumes A1:  $f \in \mathcal{S}_+$  and A2:  $g = \{\langle p, f^{-1}(p) \rangle. p \in \mathbb{Z}_+\}$ 
  shows
     $g : \mathbb{Z}_+ \rightarrow \mathbb{Z}_+$ 
     $g : \mathbb{Z}_+ \rightarrow \mathbb{Z}$ 
proof -
  from A1 have
     $\forall p \in \mathbb{Z}_+. f^{-1}(p) \in \mathbb{Z}_+$ 
     $\forall p \in \mathbb{Z}_+. f^{-1}(p) \in \mathbb{Z}$ 
  using Int_ZF_2_4_L2 PositiveSet_def by auto
  with A2 show
     $g : \mathbb{Z}_+ \rightarrow \mathbb{Z}_+ \quad \text{and} \quad g : \mathbb{Z}_+ \rightarrow \mathbb{Z}$ 
  using ZF_fun_from_total by auto
qed

```

What are the values of the (candidate for) the inverse of a positive slope?

```

lemma (in int1) Int_ZF_2_4_L10:
  assumes A1:  $f \in \mathcal{S}_+$  and A2:  $g = \{\langle p, f^{-1}(p) \rangle. p \in \mathbb{Z}_+\}$  and A3:  $p \in \mathbb{Z}_+$ 
  shows  $g(p) = f^{-1}(p)$ 
proof -
  from A1 A2 have  $g : \mathbb{Z}_+ \rightarrow \mathbb{Z}_+$  using Int_ZF_2_4_L9 by simp
  with A2 A3 show  $g(p) = f^{-1}(p)$  using ZF_fun_from_tot_val by simp
qed

```

The (candidate for) the inverse of a positive slope is a slope.

```

lemma (in int1) Int_ZF_2_4_L11: assumes A1:  $f \in S_+$  and
  A2:  $\forall m \in \mathbb{Z}_+. f^{-1}(m)-1 \in \mathbb{Z}_+$  and
  A3:  $g = \{\langle p, f^{-1}(p) \rangle. p \in \mathbb{Z}_+\}$ 
  shows OddExtension( $\mathbb{Z}$ , IntegerAddition, IntegerOrder,  $g$ )  $\in S$ 
proof -
  from A1 A2 have  $\exists L. \forall x \in \mathbb{Z}_+ \times \mathbb{Z}_+. \text{abs}(\varepsilon(f, x)) \leq L$ 
    using Int_ZF_2_4_L8 by simp
  then obtain L where I:  $\forall x \in \mathbb{Z}_+ \times \mathbb{Z}_+. \text{abs}(\varepsilon(f, x)) \leq L$ 
    by auto
  from A1 A3 have  $g : \mathbb{Z}_+ \rightarrow \mathbb{Z}$  using Int_ZF_2_4_L9
    by simp
  moreover have  $\forall m \in \mathbb{Z}_+. \forall n \in \mathbb{Z}_+. \text{abs}(\delta(g, m, n)) \leq L$ 
  proof-
    { fix m n
      assume A4:  $m \in \mathbb{Z}_+ \quad n \in \mathbb{Z}_+$ 
      then have  $\langle m, n \rangle \in \mathbb{Z}_+ \times \mathbb{Z}_+$  by simp
      with I have  $\text{abs}(\varepsilon(f, \langle m, n \rangle)) \leq L$  by simp
      moreover have  $\varepsilon(f, \langle m, n \rangle) = f^{-1}(m+n) - f^{-1}(m) - f^{-1}(n)$ 
    }
  by simp
  moreover from A1 A3 A4 have
     $f^{-1}(m+n) = g(m+n) \quad f^{-1}(m) = g(m) \quad f^{-1}(n) = g(n)$ 
  using pos_int_closed_add_unfolded Int_ZF_2_4_L10 by auto
  ultimately have  $\text{abs}(\delta(g, m, n)) \leq L$  by simp
} thus  $\forall m \in \mathbb{Z}_+. \forall n \in \mathbb{Z}_+. \text{abs}(\delta(g, m, n)) \leq L$  by simp
qed
ultimately show thesis by (rule Int_ZF_2_1_L24)
qed

```

Every positive slope that is at least 2 on positive integers almost has an inverse.

```

lemma (in int1) Int_ZF_2_4_L12: assumes A1:  $f \in S_+$  and
  A2:  $\forall m \in \mathbb{Z}_+. f^{-1}(m)-1 \in \mathbb{Z}_+$ 
  shows  $\exists h \in S. f \circ h \sim \text{id}(\mathbb{Z})$ 
proof -
  let  $g = \{\langle p, f^{-1}(p) \rangle. p \in \mathbb{Z}_+\}$ 
  let  $h = \text{OddExtension}(\mathbb{Z}, \text{IntegerAddition}, \text{IntegerOrder}, g)$ 
  from A1 have
     $\exists M \in \mathbb{Z}. \forall n \in \mathbb{Z}. f(n) \leq f(n-1) + M$ 
  using Int_ZF_2_1_L28 by simp
  then obtain M where
    I:  $M \in \mathbb{Z}$  and II:  $\forall n \in \mathbb{Z}. f(n) \leq f(n-1) + M$ 
  by auto
  from A1 A2 have T:  $h \in S$ 
    using Int_ZF_2_4_L11 by simp
  moreover have  $f \circ h \sim \text{id}(\mathbb{Z})$ 
  proof -
    from A1 T have  $f \circ h \in S$  using Int_ZF_2_1_L11
    by simp
  qed

```

```

    moreover note I
  moreover
    { fix m assume A3: m ∈ ℤ+
      with A1 have f-1(m) ∈ ℤ
    using Int_ZF_2_4_L2 PositiveSet_def by simp
      with II have f(f-1(m)) ≤ f(f-1(m)-1) + M
    by simp
      moreover from A1 A2 I A3 have f(f-1(m)-1) + M ≤ m+M
    using Int_ZF_2_4_L4 int_ord_transl_inv by simp
      ultimately have f(f-1(m)) ≤ m+M
    by (rule Int_order_transitive)
      moreover from A1 A3 have m ≤ f(f-1(m))
    using Int_ZF_2_4_L2 by simp
      moreover from A1 A2 T A3 have f(f-1(m)) = (f ∘ h)(m)
    using Int_ZF_2_4_L9 Int_ZF_1_5_L11
      Int_ZF_2_4_L10 PositiveSet_def Int_ZF_2_1_L10
    by simp
      ultimately have m ≤ (f ∘ h)(m) ∧ (f ∘ h)(m) ≤ m+M
    by simp }
    ultimately show f ∘ h ∼ id(ℤ) using Int_ZF_2_1_L32
      by simp
  qed
  ultimately show ∃ h ∈ S. f ∘ h ∼ id(ℤ)
    by auto
qed

```

Int\_ZF\_2\_4\_L12 is almost what we need, except that it has an assumption that the values of the slope that we get the inverse for are not smaller than 2 on positive integers. The Arthan's proof of Theorem 11 has a mistake where he says "note that for all but finitely many  $m, n \in N$   $p = g(m)$  and  $q = g(n)$  are both positive". Of course there may be infinitely many pairs  $\langle m, n \rangle$  such that  $p, q$  are not both positive. This is however easy to workaround: we just modify the slope by adding a constant so that the slope is large enough on positive integers and then look for the inverse.

```

theorem (in int1) pos_slope_has_inv: assumes A1: f ∈ S+
  shows ∃ g ∈ S. f ∼ g ∧ (∃ h ∈ S. g ∘ h ∼ id(ℤ))
proof -
  from A1 have f: ℤ → ℤ  1 ∈ ℤ  2 ∈ ℤ
    using AlmostHoms_def int_zero_one_are_int int_two_three_are_int
  by auto
  moreover from A1 have
    ∀ a ∈ ℤ. ∃ b ∈ ℤ+. ∀ x. b ≤ x ⟶ a ≤ f(x)
  using Int_ZF_2_3_L5 by simp
  ultimately have
    ∃ c ∈ ℤ. 2 ≤ Minimum(IntegerOrder, {n ∈ ℤ+. 1 ≤ f(n)+c})
  by (rule Int_ZF_1_6_L7)
  then obtain c where I: c ∈ ℤ and
    II: 2 ≤ Minimum(IntegerOrder, {n ∈ ℤ+. 1 ≤ f(n)+c})

```

```

    by auto
  let g = {⟨m, f(m)+c⟩. m ∈ ℤ}
  from A1 I have III: g ∈ S and IV: f ~ g using Int_ZF_2_1_L33
    by auto
  from IV have ⟨f, g⟩ ∈ A1EqRel by simp
  with A1 have T: g ∈ S+ by (rule Int_ZF_2_3_L9)
  moreover have ∀m ∈ ℤ+. g-1(m)-1 ∈ ℤ+
proof
  fix m assume A2: m ∈ ℤ+
  from A1 I II have V: 2 ≤ g-1(1)
    using Int_ZF_2_1_L33 PositiveSet_def by simp
  moreover from A2 T have g-1(1) ≤ g-1(m)
    using Int_ZF_1_5_L3 int_one_two_are_pos Int_ZF_2_4_L5
    by simp
  ultimately have 2 ≤ g-1(m)
    by (rule Int_order_transitive)
  then have 2-1 ≤ g-1(m)-1
    using int_zero_one_are_int Int_ZF_1_1_L4 int_ord_transl_inv
    by simp
  then show g-1(m)-1 ∈ ℤ+
    using int_zero_one_are_int Int_ZF_1_2_L3 Int_ZF_1_5_L3
    by simp
qed
ultimately have ∃h ∈ S. g ∘ h ~ id(ℤ)
  by (rule Int_ZF_2_4_L12)
with III IV show thesis by auto
qed

```

### 38.3 Completeness

In this section we consider properties of slopes that are needed for the proof of completeness of real numbers constructed in `Real_ZF_1.thy`. In particular we consider properties of embedding of integers into the set of slopes by the mapping  $m \mapsto m^S$ , where  $m^S$  is defined by  $m^S(n) = m \cdot n$ .

If  $m$  is an integer, then  $m^S$  is a slope whose value is  $m \cdot n$  for every integer.

**lemma** (in int1) Int\_ZF\_2\_5\_L1: assumes A1:  $m \in \mathbb{Z}$

shows

$\forall n \in \mathbb{Z}. (m^S)(n) = m \cdot n$

$m^S \in S$

**proof** -

from A1 have I:  $m^S: \mathbb{Z} \rightarrow \mathbb{Z}$

using Int\_ZF\_1\_1\_L5 ZF\_fun\_from\_total by simp

then show II:  $\forall n \in \mathbb{Z}. (m^S)(n) = m \cdot n$  using ZF\_fun\_from\_tot\_val

by simp

{ fix n k

assume A2:  $n \in \mathbb{Z} \quad k \in \mathbb{Z}$

with A1 have T:  $m \cdot n \in \mathbb{Z} \quad m \cdot k \in \mathbb{Z}$

using Int\_ZF\_1\_1\_L5 by auto

```

from A1 A2 II T have  $\delta(m^S, n, k) = m \cdot k - m \cdot k$ 
  using Int_ZF_1_1_L5 Int_ZF_1_1_L1 Int_ZF_1_2_L3
  by simp
also from T have ... = 0 using Int_ZF_1_1_L4
  by simp
finally have  $\delta(m^S, n, k) = 0$  by simp
then have  $\text{abs}(\delta(m^S, n, k)) \leq 0$ 
  using Int_ZF_2_L18 int_zero_one_are_int int_ord_is_refl refl_def
  by simp
} then have  $\forall n \in \mathbb{Z}. \forall k \in \mathbb{Z}. \text{abs}(\delta(m^S, n, k)) \leq 0$ 
  by simp
with I show  $m^S \in \mathcal{S}$  by (rule Int_ZF_2_1_L5)
qed

```

For any slope  $f$  there is an integer  $m$  such that there is some slope  $g$  that is almost equal to  $m^S$  and dominates  $f$  in the sense that  $f \leq g$  on positive integers (which implies that either  $g$  is almost equal to  $f$  or  $g - f$  is a positive slope. This will be used in `Real_ZF_1.thy` to show that for any real number there is an integer that (whose real embedding) is greater or equal.

**lemma** (in int1) Int\_ZF\_2\_5\_L2: **assumes** A1:  $f \in \mathcal{S}$   
**shows**  $\exists m \in \mathbb{Z}. \exists g \in \mathcal{S}. (m^S \sim g \wedge (f \sim g \vee g + (-f) \in \mathcal{S}_+))$

**proof** -

from A1 have

$\exists m \ k. m \in \mathbb{Z} \wedge k \in \mathbb{Z} \wedge (\forall p \in \mathbb{Z}. \text{abs}(f(p)) \leq m \cdot \text{abs}(p) + k)$

using Arthan\_Lem\_8 by simp

then obtain m k where I:  $m \in \mathbb{Z}$  and II:  $k \in \mathbb{Z}$  and

III:  $\forall p \in \mathbb{Z}. \text{abs}(f(p)) \leq m \cdot \text{abs}(p) + k$

by auto

let  $g = \{\langle n, m^S(n) + k \rangle. n \in \mathbb{Z}\}$

from I have IV:  $m^S \in \mathcal{S}$  using Int\_ZF\_2\_5\_L1 by simp

with II have V:  $g \in \mathcal{S}$  and VI:  $m^S \sim g$  using Int\_ZF\_2\_1\_L33

by auto

{ fix n assume A2:  $n \in \mathbb{Z}_+$

with A1 have  $f(n) \in \mathbb{Z}$

using Int\_ZF\_2\_1\_L2B PositiveSet\_def by simp

then have  $f(n) \leq \text{abs}(f(n))$  using Int\_ZF\_2\_L19C

by simp

moreover

from III A2 have  $\text{abs}(f(n)) \leq m \cdot \text{abs}(n) + k$

using PositiveSet\_def by simp

with A2 have  $\text{abs}(f(n)) \leq m \cdot n + k$

using Int\_ZF\_1\_5\_L4A by simp

ultimately have  $f(n) \leq m \cdot n + k$

by (rule Int\_order\_transitive)

moreover

from II IV A2 have  $g(n) = (m^S)(n) + k$

using Int\_ZF\_2\_1\_L33 PositiveSet\_def by simp

with I A2 have  $g(n) = m \cdot n + k$

using Int\_ZF\_2\_5\_L1 PositiveSet\_def by simp

```

ultimately have  $f(n) \leq g(n)$ 
  by simp
} then have  $\forall n \in \mathbb{Z}_+. f(n) \leq g(n)$ 
  by simp
with A1 V have  $f \sim g \vee g + (-f) \in \mathcal{S}_+$ 
  using Int_ZF_2_3_L4C by simp
with I V VI show thesis by auto
qed

```

The negative of an integer embeds in slopes as a negative of the original embedding.

```

lemma (in int1) Int_ZF_2_5_L3: assumes A1:  $m \in \mathbb{Z}$ 
  shows  $(-m)^S = -(m^S)$ 
proof -
  from A1 have  $(-m)^S: \mathbb{Z} \rightarrow \mathbb{Z}$  and  $(-m^S): \mathbb{Z} \rightarrow \mathbb{Z}$ 
    using Int_ZF_1_1_L4 Int_ZF_2_5_L1 AlmostHoms_def Int_ZF_2_1_L12
    by auto
  moreover have  $\forall n \in \mathbb{Z}. ((-m)^S)(n) = (-m^S)(n)$ 
  proof
    fix n assume A2:  $n \in \mathbb{Z}$ 
    with A1 have
       $((-m)^S)(n) = (-m) \cdot n$ 
       $(-m^S)(n) = -(m \cdot n)$ 
      using Int_ZF_1_1_L4 Int_ZF_2_5_L1 Int_ZF_2_1_L12A
      by auto
    with A1 A2 show  $((-m)^S)(n) = (-m^S)(n)$ 
      using Int_ZF_1_1_L5 by simp
  qed
  ultimately show  $(-m)^S = -(m^S)$  using fun_extension_iff
    by simp
qed

```

The sum of embeddings is the embedding of the sum.

```

lemma (in int1) Int_ZF_2_5_L3A: assumes A1:  $m \in \mathbb{Z} \quad k \in \mathbb{Z}$ 
  shows  $(m^S) + (k^S) = (m+k)^S$ 
proof -
  from A1 have T1:  $m+k \in \mathbb{Z}$  using Int_ZF_1_1_L5
  by simp
  with A1 have T2:
     $(m^S) \in \mathcal{S} \quad (k^S) \in \mathcal{S}$ 
     $(m+k)^S \in \mathcal{S}$ 
     $(m^S) + (k^S) \in \mathcal{S}$ 
    using Int_ZF_2_5_L1 Int_ZF_2_1_L12C by auto
  then have
     $(m^S) + (k^S): \mathbb{Z} \rightarrow \mathbb{Z}$ 
     $(m+k)^S: \mathbb{Z} \rightarrow \mathbb{Z}$ 
    using AlmostHoms_def by auto
  moreover have  $\forall n \in \mathbb{Z}. ((m^S) + (k^S))(n) = ((m+k)^S)(n)$ 
  proof

```



```

fix n assume A2: n ∈ ℤ
with A1 T1 T2 have ((mS) + (kS))(n) = (m+k)·n
  using Int_ZF_2_1_L12B Int_ZF_2_5_L1 Int_ZF_1_1_L1
  by simp
also from T1 A2 have ... = ((m+k)S)(n)
  using Int_ZF_2_5_L1 by simp
finally show ((mS) + (kS))(n) = ((m+k)S)(n)
  by simp
qed
ultimately show (mS) + (kS) = ((m+k)S)
  using fun_extension_iff by simp
qed

```

The composition of embeddings is the embedding of the product.

```

lemma (in int1) Int_ZF_2_5_L3B: assumes A1: m ∈ ℤ k ∈ ℤ
  shows (mS) ∘ (kS) = ((m·k)S)
proof -
  from A1 have T1: m·k ∈ ℤ using Int_ZF_1_1_L5
  by simp
  with A1 have T2:
    (mS) ∈ ℳ (kS) ∈ ℳ
    (m·k)S ∈ ℳ
    (mS) ∘ (kS) ∈ ℳ
  using Int_ZF_2_5_L1 Int_ZF_2_1_L11 by auto
  then have
    (mS) ∘ (kS) : ℤ → ℤ
    (m·k)S : ℤ → ℤ
  using AlmostHoms_def by auto
  moreover have ∀ n ∈ ℤ. ((mS) ∘ (kS))(n) = ((m·k)S)(n)
  proof
    fix n assume A2: n ∈ ℤ
    with A1 T2 have
      ((mS) ∘ (kS))(n) = (mS)(k·n)
      using Int_ZF_2_1_L10 Int_ZF_2_5_L1 by simp
    moreover
      from A1 A2 have k·n ∈ ℤ using Int_ZF_1_1_L5
      by simp
    with A1 A2 have (mS)(k·n) = m·k·n
      using Int_ZF_2_5_L1 Int_ZF_1_1_L7 by simp
    ultimately have ((mS) ∘ (kS))(n) = m·k·n
      by simp
    also from T1 A2 have m·k·n = ((m·k)S)(n)
      using Int_ZF_2_5_L1 by simp
    finally show ((mS) ∘ (kS))(n) = ((m·k)S)(n)
      by simp
  qed
  ultimately show (mS) ∘ (kS) = ((m·k)S)
    using fun_extension_iff by simp
qed

```

Embedding integers in slopes preserves order.

```

lemma (in int1) Int_ZF_2_5_L4: assumes A1:  $m \leq n$ 
  shows  $(m^S) \sim (n^S) \vee (n^S) + (-m^S) \in S_+$ 
proof -
  from A1 have  $m^S \in S$  and  $n^S \in S$ 
    using Int_ZF_2_L1A Int_ZF_2_5_L1 by auto
  moreover from A1 have  $\forall k \in \mathbb{Z}_+. (m^S)(k) \leq (n^S)(k)$ 
    using Int_ZF_1_3_L13B Int_ZF_2_L1A PositiveSet_def Int_ZF_2_5_L1
    by simp
  ultimately show thesis using Int_ZF_2_3_L4C
    by simp
qed

```

We aim at showing that  $m \mapsto m^S$  is an injection modulo the relation of almost equality. To do that we first show that if  $m^S$  has finite range, then  $m = 0$ .

```

lemma (in int1) Int_ZF_2_5_L5:
  assumes  $m \in \mathbb{Z}$  and  $m^S \in \text{FinRangeFunctions}(\mathbb{Z}, \mathbb{Z})$ 
  shows  $m = 0$ 
  using assms FinRangeFunctions_def Int_ZF_2_5_L1 AlmostHoms_def
  func_imagedef Int_ZF_1_6_L8 by simp

```

Embeddings of two integers are almost equal only if the integers are equal.

```

lemma (in int1) Int_ZF_2_5_L6:
  assumes A1:  $m \in \mathbb{Z} \quad k \in \mathbb{Z}$  and A2:  $(m^S) \sim (k^S)$ 
  shows  $m = k$ 
proof -
  from A1 have T:  $m - k \in \mathbb{Z}$  using Int_ZF_1_1_L5 by simp
  from A1 have  $(-(k^S)) = ((-k)^S)$ 
    using Int_ZF_2_5_L3 by simp
  then have  $m^S + (-(k^S)) = (m^S) + ((-k)^S)$ 
    by simp
  with A1 have  $m^S + (-(k^S)) = ((m-k)^S)$ 
    using Int_ZF_1_1_L4 Int_ZF_2_5_L3A by simp
  moreover from A1 A2 have  $m^S + (-(k^S)) \in \text{FinRangeFunctions}(\mathbb{Z}, \mathbb{Z})$ 
    using Int_ZF_2_5_L1 Int_ZF_2_1_L9D by simp
  ultimately have  $(m-k)^S \in \text{FinRangeFunctions}(\mathbb{Z}, \mathbb{Z})$ 
    by simp
  with T have  $m - k = 0$  using Int_ZF_2_5_L5
    by simp
  with A1 show  $m = k$  by (rule Int_ZF_1_L15)
qed

```

Embedding of 1 is the identity slope and embedding of zero is a finite range function.

```

lemma (in int1) Int_ZF_2_5_L7: shows
   $1^S = \text{id}(\mathbb{Z})$ 
   $0^S \in \text{FinRangeFunctions}(\mathbb{Z}, \mathbb{Z})$ 

```

```

proof -
  have id( $\mathbb{Z}$ ) =  $\{ \langle x, x \rangle . x \in \mathbb{Z} \}$ 
    using id_def by blast
  then show  $1^S = \text{id}(\mathbb{Z})$  using Int_ZF_1_1_L4 by simp
  have  $\{0^S(n) . n \in \mathbb{Z}\} = \{0 \cdot n . n \in \mathbb{Z}\}$ 
    using int_zero_one_are_int Int_ZF_2_5_L1 by simp
  also have  $\dots = \{0\}$  using Int_ZF_1_1_L4 int_not_empty
    by simp
  finally have  $\{0^S(n) . n \in \mathbb{Z}\} = \{0\}$  by simp
  then have  $\{0^S(n) . n \in \mathbb{Z}\} \in \text{Fin}(\mathbb{Z})$ 
    using int_zero_one_are_int Finite1_L16 by simp
  moreover have  $0^S : \mathbb{Z} \rightarrow \mathbb{Z}$ 
    using int_zero_one_are_int Int_ZF_2_5_L1 AlmostHoms_def
    by simp
  ultimately show  $0^S \in \text{FinRangeFunctions}(\mathbb{Z}, \mathbb{Z})$ 
    using Finite1_L19 by simp
qed

```

A somewhat technical condition for a embedding of an integer to be "less or equal" (in the sense appropriate for slopes) than the composition of a slope and another integer (embedding).

```

lemma (in int1) Int_ZF_2_5_L8:
  assumes A1:  $f \in \mathcal{S}$  and A2:  $N \in \mathbb{Z} \quad M \in \mathbb{Z}$  and
  A3:  $\forall n \in \mathbb{Z}_+ . M \cdot n \leq f(N \cdot n)$ 
  shows  $M^S \sim f \circ (N^S) \vee (f \circ (N^S)) + (- (M^S)) \in \mathcal{S}_+$ 
proof -
  from A1 A2 have  $M^S \in \mathcal{S} \quad f \circ (N^S) \in \mathcal{S}$ 
    using Int_ZF_2_5_L1 Int_ZF_2_1_L11 by auto
  moreover from A1 A2 A3 have  $\forall n \in \mathbb{Z}_+ . (M^S)(n) \leq (f \circ (N^S))(n)$ 
    using Int_ZF_2_5_L1 PositiveSet_def Int_ZF_2_1_L10
    by simp
  ultimately show thesis using Int_ZF_2_3_L4C
    by simp
qed

```

Another technical condition for the composition of a slope and an integer (embedding) to be "less or equal" (in the sense appropriate for slopes) than embedding of another integer.

```

lemma (in int1) Int_ZF_2_5_L9:
  assumes A1:  $f \in \mathcal{S}$  and A2:  $N \in \mathbb{Z} \quad M \in \mathbb{Z}$  and
  A3:  $\forall n \in \mathbb{Z}_+ . f(N \cdot n) \leq M \cdot n$ 
  shows  $f \circ (N^S) \sim (M^S) \vee (M^S) + (- (f \circ (N^S))) \in \mathcal{S}_+$ 
proof -
  from A1 A2 have  $f \circ (N^S) \in \mathcal{S} \quad M^S \in \mathcal{S}$ 
    using Int_ZF_2_5_L1 Int_ZF_2_1_L11 by auto
  moreover from A1 A2 A3 have  $\forall n \in \mathbb{Z}_+ . (f \circ (N^S))(n) \leq (M^S)(n)$ 
    using Int_ZF_2_5_L1 PositiveSet_def Int_ZF_2_1_L10
    by simp
  ultimately show thesis using Int_ZF_2_3_L4C

```

```
      by simp
qed
end
```

## 39 Real\_ZF.thy

```
theory Real_ZF imports Int_ZF_IML Ring_ZF_1
```

```
begin
```

The goal of the `Real_ZF` series of theory files is to provide a construction of the set of real numbers. There are several ways to construct real numbers. Most common start from the rational numbers and use Dedekind cuts or Cauchy sequences. `Real_ZF_x.thy` series formalizes an alternative approach that constructs real numbers directly from the group of integers. Our formalization is mostly based on [2]. Different variants of this construction are also described in [1] and [3]. I recommend to read these papers, but for the impatient here is a short description: we take a set of maps  $s : \mathbb{Z} \rightarrow \mathbb{Z}$  such that the set  $\{s(m+n) - s(m) - s(n)\}_{n,m \in \mathbb{Z}}$  is finite ( $\mathbb{Z}$  means the integers here). We call these maps slopes. Slopes form a group with the natural addition  $(s+r)(n) = s(n) + r(n)$ . The maps such that the set  $s(\mathbb{Z})$  is finite (finite range functions) form a subgroup of slopes. The additive group of real numbers is defined as the quotient group of slopes by the (sub)group of finite range functions. The multiplication is defined as the projection of the composition of slopes into the resulting quotient (coset) space.

### 39.1 The definition of real numbers

This section contains the construction of the ring of real numbers as classes of slopes - integer almost homomorphisms. The real definitions are in `Group_ZF_2` theory, here we just specialize the definitions of almost homomorphisms, their equivalence and operations to the additive group of integers from the general case of abelian groups considered in `Group_ZF_2`.

The set of slopes is defined as the set of almost homomorphisms on the additive group of integers.

**definition**

```
Slopes  $\equiv$  AlmostHoms(int,IntegerAddition)
```

The first operation on slopes (pointwise addition) is a special case of the first operation on almost homomorphisms.

**definition**

```
SlopeOp1  $\equiv$  AlHomOp1(int,IntegerAddition)
```

The second operation on slopes (composition) is a special case of the second operation on almost homomorphisms.

**definition**

```
SlopeOp2  $\equiv$  AlHomOp2(int,IntegerAddition)
```

Bounded integer maps are functions from integers to integers that have finite range. They play a role of zero in the set of real numbers we are constructing.

**definition**

```
BoundedIntMaps ≡ FinRangeFunctions(int,int)
```

Bounded integer maps form a normal subgroup of slopes. The equivalence relation on slopes is the (group) quotient relation defined by this subgroup.

**definition**

```
SlopeEquivalenceRel ≡ QuotientGroupRel(Slopes,SlopeOp1,BoundedIntMaps)
```

The set of real numbers is the set of equivalence classes of slopes.

**definition**

```
RealNumbers ≡ Slopes//SlopeEquivalenceRel
```

The addition on real numbers is defined as the projection of pointwise addition of slopes on the quotient. This means that the additive group of real numbers is the quotient group: the group of slopes (with pointwise addition) defined by the normal subgroup of bounded integer maps.

**definition**

```
RealAddition ≡ ProjFun2(Slopes,SlopeEquivalenceRel,SlopeOp1)
```

Multiplication is defined as the projection of composition of slopes on the quotient. The fact that it works is probably the most surprising part of the construction.

**definition**

```
RealMultiplication ≡ ProjFun2(Slopes,SlopeEquivalenceRel,SlopeOp2)
```

We first show that we can use theorems proven in some proof contexts (locales). The locale `group1` requires assumption that we deal with an abelian group. The next lemma allows to use all theorems proven in the context called `group1`.

**lemma** `Real_ZF_1_L1: shows group1(int,IntegerAddition)`

```
using group1_axioms.intro group1_def Int_ZF_1_T2 by simp
```

Real numbers form a ring. This is a special case of the theorem proven in `Ring_ZF_1.thy`, where we show the same in general for almost homomorphisms rather than slopes.

**theorem** `Real_ZF_1_T1: shows IsAring(RealNumbers,RealAddition,RealMultiplication)`

**proof** -

```
let AH = AlmostHoms(int,IntegerAddition)
let Op1 = AlHomOp1(int,IntegerAddition)
let FR = FinRangeFunctions(int,int)
let Op2 = AlHomOp2(int,IntegerAddition)
let R = QuotientGroupRel(AH,Op1,FR)
let A = ProjFun2(AH,R,Op1)
let M = ProjFun2(AH,R,Op2)
```

```

have IsAring(AH//R,A,M) using Real_ZF_1_L1 group1.Ring_ZF_1_1_T1
  by simp
then show thesis using Slopes_def SlopeOp2_def SlopeOp1_def
  BoundedIntMaps_def SlopeEquivalenceRel_def RealNumbers_def
  RealAddition_def RealMultiplication_def by simp
qed

```

We can use theorems proven in `group0` and `group1` contexts applied to the group of real numbers.

```

lemma Real_ZF_1_L2: shows
  group0(RealNumbers,RealAddition)
  RealAddition {is commutative on} RealNumbers
  group1(RealNumbers,RealAddition)
proof -
  have
    IsAgroup(RealNumbers,RealAddition)
    RealAddition {is commutative on} RealNumbers
    using Real_ZF_1_T1 IsAring_def by auto
  then show
    group0(RealNumbers,RealAddition)
    RealAddition {is commutative on} RealNumbers
    group1(RealNumbers,RealAddition)
    using group1_axioms.intro group0_def group1_def
    by auto
qed

```

Let's define some notation.

```

locale real0 =

  fixes real ( $\mathbb{R}$ )
  defines real_def [simp]:  $\mathbb{R} \equiv \text{RealNumbers}$ 

  fixes ra (infixl + 69)
  defines ra_def [simp]:  $a + b \equiv \text{RealAddition}(a,b)$ 

  fixes rminus (- _ 72)
  defines rminus_def [simp]:  $-a \equiv \text{GroupInv}(\mathbb{R}, \text{RealAddition})(a)$ 

  fixes rsub (infixl - 69)
  defines rsub_def [simp]:  $a - b \equiv a + (-b)$ 

  fixes rm (infixl  $\cdot$  70)
  defines rm_def [simp]:  $a \cdot b \equiv \text{RealMultiplication}(a,b)$ 

  fixes rzero (0)
  defines rzero_def [simp]:
    0  $\equiv \text{TheNeutralElement}(\text{RealNumbers}, \text{RealAddition})$ 

  fixes rone (1)

```

```

defines rone_def [simp]:
1  $\equiv$  TheNeutralElement(RealNumbers,RealMultiplication)

fixes rtwo (2)
defines rtwo_def [simp]: 2  $\equiv$  1+1

fixes non_zero ( $\mathbb{R}_0$ )
defines non_zero_def[simp]:  $\mathbb{R}_0 \equiv \mathbb{R} - \{0\}$ 

fixes inv ( $_{-}^{-1}$  [90] 91)
defines inv_def[simp]:
 $a^{-1} \equiv \text{GroupInv}(\mathbb{R}_0, \text{restrict}(\text{RealMultiplication}, \mathbb{R}_0 \times \mathbb{R}_0))(a)$ 

```

In `real0` context all theorems proven in the `ring0`, context are valid.

```

lemma (in real0) Real_ZF_1_L3: shows
  ring0( $\mathbb{R}$ ,RealAddition,RealMultiplication)
  using Real_ZF_1_T1 ring0_def ring0.Ring_ZF_1_L1
  by auto

```

Lets try out our notation to see that zero and one are real numbers.

```

lemma (in real0) Real_ZF_1_L4: shows  $0 \in \mathbb{R}$   $1 \in \mathbb{R}$ 
  using Real_ZF_1_L3 ring0.Ring_ZF_1_L2 by auto

```

The lemma below lists some properties that require one real number to state.

```

lemma (in real0) Real_ZF_1_L5: assumes A1:  $a \in \mathbb{R}$ 
shows
   $(-a) \in \mathbb{R}$ 
   $(-(-a)) = a$ 
   $a+0 = a$ 
   $0+a = a$ 
   $a \cdot 1 = a$ 
   $1 \cdot a = a$ 
   $a-a = 0$ 
   $a-0 = a$ 
  using assms Real_ZF_1_L3 ring0.Ring_ZF_1_L3 by auto

```

The lemma below lists some properties that require two real numbers to state.

```

lemma (in real0) Real_ZF_1_L6: assumes  $a \in \mathbb{R}$   $b \in \mathbb{R}$ 
shows
   $a+b \in \mathbb{R}$ 
   $a-b \in \mathbb{R}$ 
   $a \cdot b \in \mathbb{R}$ 
   $a+b = b+a$ 
   $(-a) \cdot b = -(a \cdot b)$ 
   $a \cdot (-b) = -(a \cdot b)$ 
  using assms Real_ZF_1_L3 ring0.Ring_ZF_1_L4 ring0.Ring_ZF_1_L7
  by auto

```



Multiplication of reals is associative.

```
lemma (in real0) Real_ZF_1_L6A: assumes a∈ℝ b∈ℝ c∈ℝ
  shows a·(b·c) = (a·b)·c
  using assms Real_ZF_1_L3 ring0.Ring_ZF_1_L11
  by simp
```

Addition is distributive with respect to multiplication.

```
lemma (in real0) Real_ZF_1_L7: assumes a∈ℝ b∈ℝ c∈ℝ
  shows
    a·(b+c) = a·b + a·c
    (b+c)·a = b·a + c·a
    a·(b-c) = a·b - a·c
    (b-c)·a = b·a - c·a
  using assms Real_ZF_1_L3 ring0.ring_oper_distr ring0.Ring_ZF_1_L8
  by auto
```

A simple rearrangement with four real numbers.

```
lemma (in real0) Real_ZF_1_L7A:
  assumes a∈ℝ b∈ℝ c∈ℝ d∈ℝ
  shows a-b + (c-d) = a+c-b-d
  using assms Real_ZF_1_L2 group0.group0_4_L8A by simp
```

RealAddition is defined as the projection of the first operation on slopes (that is, slope addition) on the quotient (slopes divided by the "almost equal" relation). The next lemma plays with definitions to show that this is the same as the operation induced on the appropriate quotient group. The names AH, Op1 and FR are used in group1 context to denote almost homomorphisms, the first operation on AH and finite range functions resp.

```
lemma Real_ZF_1_L8: assumes
  AH = AlmostHoms(int,IntegerAddition) and
  Op1 = AlHomOp1(int,IntegerAddition) and
  FR = FinRangeFunctions(int,int)
  shows RealAddition = QuotientGroupOp(AH,Op1,FR)
  using assms RealAddition_def SlopeEquivalenceRel_def
    QuotientGroupOp_def Slopes_def SlopeOp1_def BoundedIntMaps_def
  by simp
```

The symbol 0 in the real0 context is defined as the neutral element of real addition. The next lemma shows that this is the same as the neutral element of the appropriate quotient group.

```
lemma (in real0) Real_ZF_1_L9: assumes
  AH = AlmostHoms(int,IntegerAddition) and
  Op1 = AlHomOp1(int,IntegerAddition) and
  FR = FinRangeFunctions(int,int) and
  r = QuotientGroupRel(AH,Op1,FR)
  shows
    TheNeutralElement(AH//r,QuotientGroupOp(AH,Op1,FR)) = 0
```

```

SlopeEquivalenceRel = r
using assms Slopes_def Real_ZF_1_L8 RealNumbers_def
  SlopeEquivalenceRel_def SlopeOp1_def BoundedIntMaps_def
by auto

```

Zero is the class of any finite range function.

```

lemma (in real0) Real_ZF_1_L10:
  assumes A1:  $s \in \text{Slopes}$ 
  shows  $\text{SlopeEquivalenceRel}\{s\} = 0 \iff s \in \text{BoundedIntMaps}$ 
proof -
  let AH = AlmostHoms(int,IntegerAddition)
  let Op1 = AlHomOp1(int,IntegerAddition)
  let FR = FinRangeFunctions(int,int)
  let r = QuotientGroupRel(AH,Op1,FR)
  let e = TheNeutralElement(AH//r,QuotientGroupOp(AH,Op1,FR))
  from A1 have
    group1(int,IntegerAddition)
     $s \in \text{AH}$ 
    using Real_ZF_1_L1 Slopes_def
    by auto
  then have  $r\{s\} = e \iff s \in \text{FR}$ 
    using group1.Group_ZF_3_3_L5 by simp
  moreover have
     $r = \text{SlopeEquivalenceRel}$ 
     $e = 0$ 
     $\text{FR} = \text{BoundedIntMaps}$ 
    using SlopeEquivalenceRel_def Slopes_def SlopeOp1_def
    BoundedIntMaps_def Real_ZF_1_L9 by auto
  ultimately show thesis by simp
qed

```

We will need a couple of results from Group\_ZF\_3.thy The first two that state that the definition of addition and multiplication of real numbers are consistent, that is the result does not depend on the choice of the slopes representing the numbers. The second one implies that what we call SlopeEquivalenceRel is actually an equivalence relation on the set of slopes. We also show that the neutral element of the multiplicative operation on reals (in short number 1) is the class of the identity function on integers.

```

lemma Real_ZF_1_L11: shows
  Congruent2(SlopeEquivalenceRel,SlopeOp1)
  Congruent2(SlopeEquivalenceRel,SlopeOp2)
   $\text{SlopeEquivalenceRel} \subseteq \text{Slopes} \times \text{Slopes}$ 
  equiv(Slopes, SlopeEquivalenceRel)
   $\text{SlopeEquivalenceRel}\{\text{id}(\text{int})\} =$ 
  TheNeutralElement(RealNumbers,RealMultiplication)
   $\text{BoundedIntMaps} \subseteq \text{Slopes}$ 
proof -
  let G = int

```

```

let f = IntegerAddition
let AH = AlmostHoms(int,IntegerAddition)
let Op1 = AlHomOp1(int,IntegerAddition)
let Op2 = AlHomOp2(int,IntegerAddition)
let FR = FinRangeFunctions(int,int)
let R = QuotientGroupRel(AH,Op1,FR)
  have
    Congruent2(R,Op1)
    Congruent2(R,Op2)
  using Real_ZF_1_L1 group1.Group_ZF_3_4_L13A group1.Group_ZF_3_3_L4
  by auto
then show
  Congruent2(SlopeEquivalenceRel,SlopeOp1)
  Congruent2(SlopeEquivalenceRel,SlopeOp2)
  using SlopeEquivalenceRel_def SlopeOp1_def Slopes_def
    BoundedIntMaps_def SlopeOp2_def by auto
have equiv(AH,R)
  using Real_ZF_1_L1 group1.Group_ZF_3_3_L3 by simp
then show equiv(Slopes,SlopeEquivalenceRel)
  using BoundedIntMaps_def SlopeEquivalenceRel_def SlopeOp1_def Slopes_def
  by simp
then show SlopeEquivalenceRel  $\subseteq$  Slopes  $\times$  Slopes
  using equiv_type by simp
have R{id(int)} = TheNeutralElement(AH//R,ProjFun2(AH,R,Op2))
  using Real_ZF_1_L1 group1.Group_ZF_3_4_T2 by simp
then show SlopeEquivalenceRel{id(int)} =
  TheNeutralElement(RealNumbers,RealMultiplication)
  using Slopes_def RealNumbers_def
    SlopeEquivalenceRel_def SlopeOp1_def BoundedIntMaps_def
    RealMultiplication_def SlopeOp2_def
  by simp
have FR  $\subseteq$  AH using Real_ZF_1_L1 group1.Group_ZF_3_3_L1
  by simp
then show BoundedIntMaps  $\subseteq$  Slopes
  using BoundedIntMaps_def Slopes_def by simp
qed

```

A one-side implication of the equivalence from Real\_ZF\_1\_L10: the class of a bounded integer map is the real zero.

```

lemma (in real0) Real_ZF_1_L11A: assumes  $s \in \text{BoundedIntMaps}$ 
  shows SlopeEquivalenceRel{s} = 0
  using assms Real_ZF_1_L11 Real_ZF_1_L10 by auto

```

The next lemma is rephrases the result from Group\_ZF\_3.thy that says that the negative (the group inverse with respect to real addition) of the class of a slope is the class of that slope composed with the integer additive group inverse. The result and proof is not very readable as we use mostly generic set theory notation with long names here. Real\_ZF\_1.thy contains the same statement written in a more readable notation:  $[-s] = -[s]$ .

```

lemma (in real0) Real_ZF_1_L12: assumes A1: s ∈ Slopes and
  Dr: r = QuotientGroupRel(Slopes,SlopeOp1,BoundedIntMaps)
  shows r{GroupInv(int,IntegerAddition) 0 s} = -(r{s})
proof -
  let G = int
  let f = IntegerAddition
  let AH = AlmostHoms(int,IntegerAddition)
  let Op1 = AlHomOp1(int,IntegerAddition)
  let FR = FinRangeFunctions(int,int)
  let F = ProjFun2(Slopes,r,SlopeOp1)
  from A1 Dr have
    group1(G, f)
    s ∈ AlmostHoms(G, f)
    r = QuotientGroupRel(
      AlmostHoms(G, f), AlHomOp1(G, f), FinRangeFunctions(G, G))
    and F = ProjFun2(AlmostHoms(G, f), r, AlHomOp1(G, f))
    using Real_ZF_1_L1 Slopes_def SlopeOp1_def BoundedIntMaps_def
    by auto
  then have
    r{GroupInv(G, f) 0 s} =
    GroupInv(AlmostHoms(G, f) // r, F)(r {s})
    using group1.Group_ZF_3_3_L6 by simp
  with Dr show thesis
    using RealNumbers_def Slopes_def SlopeEquivalenceRel_def RealAddition_def
    by simp
qed

```

Two classes are equal iff the slopes that represent them are almost equal.

```

lemma Real_ZF_1_L13: assumes s ∈ Slopes p ∈ Slopes
  and r = SlopeEquivalenceRel
  shows r{s} = r{p}  $\longleftrightarrow$  (s,p) ∈ r
  using assms Real_ZF_1_L11 eq_equiv_class equiv_class_eq
  by blast

```

Identity function on integers is a slope. This lemma concludes the easy part of the construction that follows from the fact that slope equivalence classes form a ring. It is easy to see that multiplication of classes of almost homomorphisms is not commutative in general. The remaining properties of real numbers, like commutativity of multiplication and the existence of multiplicative inverses have to be proven using properties of the group of integers, rather than in general setting of abelian groups.

```

lemma Real_ZF_1_L14: shows id(int) ∈ Slopes
proof -
  have id(int) ∈ AlmostHoms(int,IntegerAddition)
    using Real_ZF_1_L1 group1.Group_ZF_3_4_L15
    by simp
  then show thesis using Slopes_def by simp
qed

```

end

## 40 Real\_ZF\_1.thy

**theory** Real\_ZF\_1 **imports** Real\_ZF Int\_ZF\_3 OrderedField\_ZF

**begin**

In this theory file we continue the construction of real numbers started in Real\_ZF to a succesful conclusion. We put here those parts of the construction that can not be done in the general settings of abelian groups and require integers.

### 40.1 Definitions and notation

In this section we define notions and notation needed for the rest of the construction.

We define positive slopes as those that take an infinite number of positive values on the positive integers (see Int\_ZF\_2 for properties of positive slopes).

**definition**

$\text{PositiveSlopes} \equiv \{s \in \text{Slopes}.$   
 $s(\text{PositiveIntegers}) \cap \text{PositiveIntegers} \notin \text{Fin}(\text{int})\}$

The order on the set of real numbers is constructed by specifying the set of positive reals. This set is defined as the projection of the set of positive slopes.

**definition**

$\text{PositiveReals} \equiv \{\text{SlopeEquivalenceRel}\{s\}. s \in \text{PositiveSlopes}\}$

The order relation on real numbers is constructed from the set of positive elements in a standard way (see section "Alternative definitions" in OrderedGroup\_ZF.)

**definition**

$\text{OrderOnReals} \equiv \text{OrderFromPosSet}(\text{RealNumbers}, \text{RealAddition}, \text{PositiveReals})$

The next locale extends the locale `real0` to define notation specific to the construction of real numbers. The notation follows the one defined in Int\_ZF\_2.thy. If  $m$  is an integer, then the real number which is the class of the slope  $n \mapsto m \cdot n$  is denoted  $m^R$ . For a real number  $a$  notation  $\lfloor a \rfloor$  means the largest integer  $m$  such that the real version of it (that is,  $m^R$ ) is not greater than  $a$ . For an integer  $m$  and a subset of reals  $S$  the expression  $\Gamma(S, m)$  is defined as  $\max\{\lfloor p^R \cdot x \rfloor : x \in S\}$ . This plays a role in the proof of completeness of real numbers. We also reuse some notation defined in the `int0` context, like  $\mathbb{Z}_+$  (the set of positive integers) and  $\text{abs}(m)$  (the absolute value of an integer, and some defined in the `int1` context, like the addition  $(+)$  and composition  $(\circ)$  of slopes.

**locale** `real1` = `real0` +

```

fixes AlEq (infix ~ 68)
defines AlEq_def[simp]:  $s \sim r \equiv \langle s, r \rangle \in \text{SlopeEquivalenceRel}$ 

fixes slope_add (infix + 70)
defines slope_add_def[simp]:
 $s + r \equiv \text{SlopeOp1}\langle s, r \rangle$ 

fixes slope_comp (infix  $\circ$  71)
defines slope_comp_def[simp]:  $s \circ r \equiv \text{SlopeOp2}\langle s, r \rangle$ 

fixes slopes ( $\mathcal{S}$ )
defines slopes_def[simp]:  $\mathcal{S} \equiv \text{AlmostHoms}(\text{int}, \text{IntegerAddition})$ 

fixes posslopes ( $\mathcal{S}_+$ )
defines posslopes_def[simp]:  $\mathcal{S}_+ \equiv \text{PositiveSlopes}$ 

fixes slope_class ([ _ ])
defines slope_class_def[simp]:  $[f] \equiv \text{SlopeEquivalenceRel}\{f\}$ 

fixes slope_neg (-_ [90] 91)
defines slope_neg_def[simp]:  $-s \equiv \text{GroupInv}(\text{int}, \text{IntegerAddition})\ 0\ s$ 

fixes lesseqr (infix  $\leq$  60)
defines lesseqr_def[simp]:  $a \leq b \equiv \langle a, b \rangle \in \text{OrderOnReals}$ 

fixes sless (infix < 60)
defines sless_def[simp]:  $a < b \equiv a \leq b \wedge a \neq b$ 

fixes positivereals ( $\mathbb{R}_+$ )
defines positivereals_def[simp]:  $\mathbb{R}_+ \equiv \text{PositiveSet}(\mathbb{R}, \text{RealAddition}, \text{OrderOnReals})$ 

fixes intembed ( $_^R$  [90] 91)
defines intembed_def[simp]:
 $m^R \equiv [\{\langle n, \text{IntegerMultiplication}\langle m, n \rangle \rangle. n \in \text{int}\}]$ 

fixes floor ([ _ ])
defines floor_def[simp]:
 $\lfloor a \rfloor \equiv \text{Maximum}(\text{IntegerOrder}, \{m \in \text{int}. m^R \leq a\})$ 

fixes  $\Gamma$ 
defines  $\Gamma$ _def[simp]:  $\Gamma(S, p) \equiv \text{Maximum}(\text{IntegerOrder}, \{\lfloor p^R \cdot x \rfloor. x \in S\})$ 

fixes ia (infixl + 69)
defines ia_def[simp]:  $a + b \equiv \text{IntegerAddition}\langle a, b \rangle$ 

fixes iminus (- _ 72)
defines iminus_def[simp]:  $-a \equiv \text{GroupInv}(\text{int}, \text{IntegerAddition})(a)$ 

```

```

fixes isub (infixl - 69)
defines isub_def[simp]: a-b  $\equiv$  a+ (- b)

fixes intpositives ( $\mathbb{Z}_+$ )
defines intpositives_def[simp]:
 $\mathbb{Z}_+ \equiv \text{PositiveSet}(\text{int}, \text{IntegerAddition}, \text{IntegerOrder})$ 

fixes zlesseq (infix  $\leq$  60)
defines lesseq_def[simp]:  $m \leq n \equiv \langle m, n \rangle \in \text{IntegerOrder}$ 

fixes imult (infixl  $\cdot$  70)
defines imult_def[simp]: a\cdotb  $\equiv \text{IntegerMultiplication} \langle a, b \rangle$ 

fixes izero ( $0_{\mathbb{Z}}$ )
defines izero_def[simp]:  $0_{\mathbb{Z}} \equiv \text{TheNeutralElement}(\text{int}, \text{IntegerAddition})$ 

fixes ione ( $1_{\mathbb{Z}}$ )
defines ione_def[simp]:  $1_{\mathbb{Z}} \equiv \text{TheNeutralElement}(\text{int}, \text{IntegerMultiplication})$ 

fixes itwo ( $2_{\mathbb{Z}}$ )
defines itwo_def[simp]:  $2_{\mathbb{Z}} \equiv 1_{\mathbb{Z}} + 1_{\mathbb{Z}}$ 

fixes abs
defines abs_def[simp]:
abs(m)  $\equiv \text{AbsoluteValue}(\text{int}, \text{IntegerAddition}, \text{IntegerOrder})(m)$ 

fixes  $\delta$ 
defines  $\delta$ _def[simp]:  $\delta(s, m, n) \equiv s(m+n) - s(m) - s(n)$ 

```

## 40.2 Multiplication of real numbers

Multiplication of real numbers is defined as a projection of composition of slopes onto the space of equivalence classes of slopes. Thus, the product of the real numbers given as classes of slopes  $s$  and  $r$  is defined as the class of  $s \circ r$ . The goal of this section is to show that multiplication defined this way is commutative.

Let's recall a theorem from `Int_ZF_2.thy` that states that if  $f, g$  are slopes, then  $f \circ g$  is equivalent to  $g \circ f$ . Here we conclude from that that the classes of  $f \circ g$  and  $g \circ f$  are the same.

```

lemma (in real1) Real_ZF_1_1_L2: assumes A1:  $f \in \mathcal{S}$   $g \in \mathcal{S}$ 
  shows  $[f \circ g] = [g \circ f]$ 
proof -
  from A1 have  $f \circ g \sim g \circ f$ 
    using Slopes_def int1.Arthan_Th_9 SlopeOp1_def BoundedIntMaps_def
    SlopeEquivalenceRel_def SlopeOp2_def by simp
  then show thesis using Real_ZF_1_L11 equiv_class_eq

```



by simp  
qed

Classes of slopes are real numbers.

```
lemma (in real1) Real_ZF_1_1_L3: assumes A1:  $f \in \mathcal{S}$ 
  shows  $[f] \in \mathbb{R}$ 
proof -
  from A1 have  $[f] \in \text{Slopes} // \text{SlopeEquivalenceRel}$ 
    using Slopes_def quotientI by simp
  then show  $[f] \in \mathbb{R}$  using RealNumbers_def by simp
qed
```

Each real number is a class of a slope.

```
lemma (in real1) Real_ZF_1_1_L3A: assumes A1:  $a \in \mathbb{R}$ 
  shows  $\exists f \in \mathcal{S} . a = [f]$ 
proof -
  from A1 have  $a \in \mathcal{S} // \text{SlopeEquivalenceRel}$ 
    using RealNumbers_def Slopes_def by simp
  then show thesis using quotient_def
    by simp
qed
```

It is useful to have the definition of addition and multiplication in the `real1` context notation.

```
lemma (in real1) Real_ZF_1_1_L4:
  assumes A1:  $f \in \mathcal{S} \quad g \in \mathcal{S}$ 
  shows
     $[f] + [g] = [f+g]$ 
     $[f] \cdot [g] = [f \circ g]$ 
proof -
  let r = SlopeEquivalenceRel
  have  $[f] \cdot [g] = \text{ProjFun2}(\mathcal{S}, r, \text{SlopeOp2}) \langle [f], [g] \rangle$ 
    using RealMultiplication_def Slopes_def by simp
  also from A1 have  $\dots = [f \circ g]$ 
    using Real_ZF_1_L11 EquivClass_1_L10 Slopes_def
    by simp
  finally show  $[f] \cdot [g] = [f \circ g]$  by simp
  have  $[f] + [g] = \text{ProjFun2}(\mathcal{S}, r, \text{SlopeOp1}) \langle [f], [g] \rangle$ 
    using RealAddition_def Slopes_def by simp
  also from A1 have  $\dots = [f+g]$ 
    using Real_ZF_1_L11 EquivClass_1_L10 Slopes_def
    by simp
  finally show  $[f] + [g] = [f+g]$  by simp
qed
```

The next lemma is essentially the same as `Real_ZF_1_L12`, but written in the notation defined in the `real1` context. It states that if  $f$  is a slope, then  $-[f] = [-f]$ .

```

lemma (in real1) Real_ZF_1_1_L4A: assumes  $f \in \mathcal{S}$ 
  shows  $[-f] = -[f]$ 
  using assms Slopes_def SlopeEquivalenceRel_def Real_ZF_1_L12
  by simp

```

Subtracting real numbers corresponds to adding the opposite slope.

```

lemma (in real1) Real_ZF_1_1_L4B: assumes A1:  $f \in \mathcal{S} \quad g \in \mathcal{S}$ 
  shows  $[f] - [g] = [f+(-g)]$ 
proof -
  from A1 have  $[f+(-g)] = [f] + [-g]$ 
    using Slopes_def BoundedIntMaps_def int1.Int_ZF_2_1_L12
    Real_ZF_1_1_L4 by simp
  with A1 show  $[f] - [g] = [f+(-g)]$ 
    using Real_ZF_1_1_L4A by simp
qed

```

Multiplication of real numbers is commutative.

```

theorem (in real1) real_mult_commute: assumes A1:  $a \in \mathbb{R} \quad b \in \mathbb{R}$ 
  shows  $a \cdot b = b \cdot a$ 
proof -
  from A1 have
     $\exists f \in \mathcal{S} . a = [f]$ 
     $\exists g \in \mathcal{S} . b = [g]$ 
    using Real_ZF_1_1_L3A by auto
  then obtain  $f \ g$  where
     $f \in \mathcal{S} \quad g \in \mathcal{S}$  and  $a = [f] \quad b = [g]$ 
    by auto
  then show  $a \cdot b = b \cdot a$ 
    using Real_ZF_1_1_L4 Real_ZF_1_1_L2 by simp
qed

```

Multiplication is commutative on reals.

```

lemma real_mult_commutative: shows
  RealMultiplication {is commutative on} RealNumbers
  using real1.real_mult_commute IsCommutative_def
  by simp

```

The neutral element of multiplication of reals (denoted as **1** in the `real1` context) is the class of identity function on integers. This is really shown in `Real_ZF_1_L11`, here we only rewrite it in the notation used in the `real1` context.

```

lemma (in real1) real_one_cl_identity: shows  $[id(int)] = 1$ 
  using Real_ZF_1_L11 by simp

```

If  $f$  is bounded, then its class is the neutral element of additive operation on reals (denoted as **0** in the `real1` context).

```

lemma (in real1) real_zero_cl_bounded_map:
  assumes  $f \in \text{BoundedIntMaps}$  shows  $[f] = 0$ 

```

using assms Real\_ZF\_1\_L11A by simp

Two real numbers are equal iff the slopes that represent them are almost equal. This is proven in Real\_ZF\_1\_L13, here we just rewrite it in the notation used in the real1 context.

```
lemma (in real1) Real_ZF_1_1_L5:
  assumes f ∈ S  g ∈ S
  shows [f] = [g] ⟷ f ~ g
  using assms Slopes_def Real_ZF_1_L13 by simp
```

If the pair of function belongs to the slope equivalence relation, then their classes are equal. This is convenient, because we don't need to assume that  $f, g$  are slopes (follows from the fact that  $f \sim g$ ).

```
lemma (in real1) Real_ZF_1_1_L5A: assumes f ~ g
  shows [f] = [g]
  using assms Real_ZF_1_L11 Slopes_def Real_ZF_1_1_L5
  by auto
```

Identity function on integers is a slope. This is proven in Real\_ZF\_1\_L13, here we just rewrite it in the notation used in the real1 context.

```
lemma (in real1) id_on_int_is_slope: shows id(int) ∈ S
  using Real_ZF_1_L14 Slopes_def by simp
```

A result from Int\_ZF\_2.thy: the identity function on integers is not almost equal to any bounded function.

```
lemma (in real1) Real_ZF_1_1_L7:
  assumes A1: f ∈ BoundedIntMaps
  shows ¬(id(int) ~ f)
  using assms Slopes_def SlopeOp1_def BoundedIntMaps_def
    SlopeEquivalenceRel_def BoundedIntMaps_def int1.Int_ZF_2_3_L12
  by simp
```

Zero is not one.

```
lemma (in real1) real_zero_not_one: shows 1 ≠ 0
proof -
  { assume A1: 1 = 0
    have ∃f ∈ S. 0 = [f]
      using Real_ZF_1_L4 Real_ZF_1_1_L3A by simp
    with A1 have
      ∃f ∈ S. [id(int)] = [f] ∧ [f] = 0
      using real_one_cl_identity by auto
    then have False using Real_ZF_1_1_L5 Slopes_def
      Real_ZF_1_L10 Real_ZF_1_1_L7 id_on_int_is_slope
      by auto
  } then show 1 ≠ 0 by auto
qed
```

Negative of a real number is a real number. Property of groups.

```

lemma (in real1) Real_ZF_1_1_L8: assumes a ∈ ℝ shows (-a) ∈ ℝ
  using assms Real_ZF_1_L2 group0.inverse_in_group
  by simp

```

An identity with three real numbers.

```

lemma (in real1) Real_ZF_1_1_L9: assumes a ∈ ℝ b ∈ ℝ c ∈ ℝ
  shows a · (b · c) = a · c · b
  using assms real_mult_commutative Real_ZF_1_L3 ring0.Ring_ZF_2_L4
  by simp

```

### 40.3 The order on reals

In this section we show that the order relation defined by prescribing the set of positive reals as the projection of the set of positive slopes makes the ring of real numbers into an ordered ring. We also collect the facts about ordered groups and rings that we use in the construction.

Positive slopes are slopes and positive reals are real.

```

lemma Real_ZF_1_2_L1: shows
  PositiveSlopes ⊆ Slopes
  PositiveReals ⊆ RealNumbers
proof -
  have PositiveSlopes =
    {s ∈ Slopes. s(PositiveIntegers) ∩ PositiveIntegers ≠ Fin(int)}
  using PositiveSlopes_def by simp
  then show PositiveSlopes ⊆ Slopes by (rule subset_with_property)
  then have
    {SlopeEquivalenceRel{s}. s ∈ PositiveSlopes } ⊆
    Slopes//SlopeEquivalenceRel
  using EquivClass_1_L1A by simp
  then show PositiveReals ⊆ RealNumbers
  using PositiveReals_def RealNumbers_def by simp
qed

```

Positive reals are the same as classes of a positive slopes.

```

lemma (in real1) Real_ZF_1_2_L2:
  shows a ∈ PositiveReals ⟷ (∃ f ∈ S+. a = [f])
proof
  assume a ∈ PositiveReals
  then have a ∈ {[s]}. s ∈ S+ using PositiveReals_def
  by simp
  then show ∃ f ∈ S+. a = [f] by auto
next assume ∃ f ∈ S+. a = [f]
  then have a ∈ {[s]}. s ∈ S+ by auto
  then show a ∈ PositiveReals using PositiveReals_def
  by simp
qed

```

Let's recall from `Int_ZF_2.thy` that the sum and composition of positive slopes is a positive slope.

```
lemma (in real1) Real_ZF_1_2_L3:
  assumes f ∈ S+  g ∈ S+
  shows
    f+g ∈ S+
    f◦g ∈ S+
  using assms Slopes_def PositiveSlopes_def PositiveIntegers_def
    SlopeOp1_def int1.sum_of_pos_sls_is_pos_sl
    SlopeOp2_def int1.comp_of_pos_sls_is_pos_sl
  by auto
```

Bounded integer maps are not positive slopes.

```
lemma (in real1) Real_ZF_1_2_L5:
  assumes f ∈ BoundedIntMaps
  shows f ∉ S+
  using assms BoundedIntMaps_def Slopes_def PositiveSlopes_def
    PositiveIntegers_def int1.Int_ZF_2_3_L1B by simp
```

The set of positive reals is closed under addition and multiplication. Zero (the neutral element of addition) is not a positive number.

```
lemma (in real1) Real_ZF_1_2_L6: shows
  PositiveReals {is closed under} RealAddition
  PositiveReals {is closed under} RealMultiplication
  0 ∉ PositiveReals
proof -
  { fix a fix b
    assume a ∈ PositiveReals and b ∈ PositiveReals
    then obtain f g where
      I: f ∈ S+  g ∈ S+ and
      II: a = [f]  b = [g]
    using Real_ZF_1_2_L2 by auto
    then have f ∈ S  g ∈ S using Real_ZF_1_2_L1 Slopes_def
      by auto
    with I II have
      a+b ∈ PositiveReals ∧ a·b ∈ PositiveReals
      using Real_ZF_1_1_L4 Real_ZF_1_2_L3 Real_ZF_1_2_L2
      by auto
  } then show
    PositiveReals {is closed under} RealAddition
    PositiveReals {is closed under} RealMultiplication
  using IsOpClosed_def
  by auto
{ assume 0 ∈ PositiveReals
  then obtain f where f ∈ S+ and 0 = [f]
  using Real_ZF_1_2_L2 by auto
  then have False
    using Real_ZF_1_2_L1 Slopes_def Real_ZF_1_L10 Real_ZF_1_2_L5
```

```

      by auto
    } then show  $0 \notin \text{PositiveReals}$  by auto
qed

```

If a class of a slope  $f$  is not zero, then either  $f$  is a positive slope or  $-f$  is a positive slope. The real proof is in `Int_ZF_2.thy`.

```

lemma (in real1) Real_ZF_1_2_L7:
  assumes A1:  $f \in \mathcal{S}$  and A2:  $[f] \neq 0$ 
  shows  $(f \in \mathcal{S}_+) \text{ Xor } ((-f) \in \mathcal{S}_+)$ 
  using assms Slopes_def SlopeEquivalenceRel_def BoundedIntMaps_def
    PositiveSlopes_def PositiveIntegers_def
    Real_ZF_1_L10 int1.Int_ZF_2_3_L8 by simp

```

The next lemma rephrases `Int_ZF_2_3_L10` in the notation used in `real1` context.

```

lemma (in real1) Real_ZF_1_2_L8:
  assumes A1:  $f \in \mathcal{S}$   $g \in \mathcal{S}$ 
  and A2:  $(f \in \mathcal{S}_+) \text{ Xor } (g \in \mathcal{S}_+)$ 
  shows  $([f] \in \text{PositiveReals}) \text{ Xor } ([g] \in \text{PositiveReals})$ 
  using assms PositiveReals_def SlopeEquivalenceRel_def Slopes_def
    SlopeOp1_def BoundedIntMaps_def PositiveSlopes_def PositiveIntegers_def
    int1.Int_ZF_2_3_L10 by simp

```

The trichotomy law for the (potential) order on reals: if  $a \neq 0$ , then either  $a$  is positive or  $-a$  is positive.

```

lemma (in real1) Real_ZF_1_2_L9:
  assumes A1:  $a \in \mathbb{R}$  and A2:  $a \neq 0$ 
  shows  $(a \in \text{PositiveReals}) \text{ Xor } ((-a) \in \text{PositiveReals})$ 
proof -
  from A1 obtain f where I:  $f \in \mathcal{S}$   $a = [f]$ 
  using Real_ZF_1_1_L3A by auto
  with A2 have  $([f] \in \text{PositiveReals}) \text{ Xor } ([-f] \in \text{PositiveReals})$ 
  using Slopes_def BoundedIntMaps_def int1.Int_ZF_2_1_L12
    Real_ZF_1_2_L7 Real_ZF_1_2_L8 by simp
  with I show  $(a \in \text{PositiveReals}) \text{ Xor } ((-a) \in \text{PositiveReals})$ 
  using Real_ZF_1_1_L4A by simp
qed

```

Finally we are ready to prove that real numbers form an ordered ring with no zero divisors.

```

theorem reals_are_ord_ring: shows
  IsAnOrdRing(RealNumbers, RealAddition, RealMultiplication, OrderOnReals)
  OrderOnReals {is total on} RealNumbers
  PositiveSet(RealNumbers, RealAddition, OrderOnReals) = PositiveReals
  HasNoZeroDivs(RealNumbers, RealAddition, RealMultiplication)
proof -
  let R = RealNumbers
  let A = RealAddition

```

```

let M = RealMultiplication
let P = PositiveReals
let r = OrderOnReals
let z = TheNeutralElement(R, A)
have I:
  ring0(R, A, M)
  M {is commutative on} R
  P  $\subseteq$  R
  P {is closed under} A
  TheNeutralElement(R, A)  $\notin$  P
   $\forall a \in R. a \neq z \longrightarrow (a \in P) \text{ Xor } (\text{GroupInv}(R, A)(a) \in P)$ 
  P {is closed under} M
  r = OrderFromPosSet(R, A, P)
  using real0.Real_ZF_1_L3 real_mult_commutative Real_ZF_1_2_L1
    real1.Real_ZF_1_2_L6 real1.Real_ZF_1_2_L9 OrderOnReals_def
  by auto
then show IsAnOrdRing(R, A, M, r)
  by (rule ring0.ring_ord_by_positive_set)
from I show r {is total on} R
  by (rule ring0.ring_ord_by_positive_set)
from I show PositiveSet(R,A,r) = P
  by (rule ring0.ring_ord_by_positive_set)
from I show HasNoZeroDivs(R,A,M)
  by (rule ring0.ring_ord_by_positive_set)
qed

```

All theorems proven in the ring1 (about ordered rings), group3 (about ordered groups) and group1 (about groups) contexts are valid as applied to ordered real numbers with addition and (real) order.

```

lemma Real_ZF_1_2_L10: shows
  ring1(RealNumbers,RealAddition,RealMultiplication,OrderOnReals)
  IsAnOrdGroup(RealNumbers,RealAddition,OrderOnReals)
  group3(RealNumbers,RealAddition,OrderOnReals)
  OrderOnReals {is total on} RealNumbers
proof -
  show ring1(RealNumbers,RealAddition,RealMultiplication,OrderOnReals)
    using reals_are_ord_ring OrdRing_ZF_1_L2 by simp
  then show
    IsAnOrdGroup(RealNumbers,RealAddition,OrderOnReals)
    group3(RealNumbers,RealAddition,OrderOnReals)
    OrderOnReals {is total on} RealNumbers
    using ring1.OrdRing_ZF_1_L4 by auto
qed

```

If  $a = b$  or  $b - a$  is positive, then  $a$  is less or equal  $b$ .

```

lemma (in real1) Real_ZF_1_2_L11: assumes A1:  $a \in \mathbb{R}$   $b \in \mathbb{R}$  and
  A3:  $a=b \vee b-a \in \text{PositiveReals}$ 
  shows  $a \leq b$ 
  using assms reals_are_ord_ring Real_ZF_1_2_L10

```

group3.OrderedGroup\_ZF\_1\_L30 by simp

A sufficient condition for two classes to be in the real order.

```

lemma (in real1) Real_ZF_1_2_L12: assumes A1:  $f \in \mathcal{S}$   $g \in \mathcal{S}$  and
  A2:  $f \sim g \vee (g + (-f)) \in \mathcal{S}_+$ 
  shows  $[f] \leq [g]$ 
proof -
  from A1 A2 have  $[f] = [g] \vee [g] - [f] \in \text{PositiveReals}$ 
    using Real_ZF_1_1_L5A Real_ZF_1_2_L2 Real_ZF_1_1_L4B
    by auto
  with A1 show  $[f] \leq [g]$  using Real_ZF_1_1_L3 Real_ZF_1_2_L11
    by simp
qed

```

Taking negative on both sides reverses the inequality, a case with an inverse on one side. Property of ordered groups.

```

lemma (in real1) Real_ZF_1_2_L13:
  assumes A1:  $a \in \mathbb{R}$  and A2:  $(-a) \leq b$ 
  shows  $(-b) \leq a$ 
  using assms Real_ZF_1_2_L10 group3.OrderedGroup_ZF_1_L5AG
  by simp

```

Real order is antisymmetric.

```

lemma (in real1) real_ord_antisym:
  assumes A1:  $a \leq b$   $b \leq a$  shows  $a = b$ 
proof -
  from A1 have
    group3(RealNumbers, RealAddition, OrderOnReals)
     $\langle a, b \rangle \in \text{OrderOnReals}$   $\langle b, a \rangle \in \text{OrderOnReals}$ 
    using Real_ZF_1_2_L10 by auto
  then show  $a = b$  by (rule group3.group_order_antisym)
qed

```

Real order is transitive.

```

lemma (in real1) real_ord_transitive: assumes A1:  $a \leq b$   $b \leq c$ 
  shows  $a \leq c$ 
proof -
  from A1 have
    group3(RealNumbers, RealAddition, OrderOnReals)
     $\langle a, b \rangle \in \text{OrderOnReals}$   $\langle b, c \rangle \in \text{OrderOnReals}$ 
    using Real_ZF_1_2_L10 by auto
  then have  $\langle a, c \rangle \in \text{OrderOnReals}$ 
    by (rule group3.Group_order_transitive)
  then show  $a \leq c$  by simp
qed

```

We can multiply both sides of an inequality by a nonnegative real number.

```

lemma (in real1) Real_ZF_1_2_L14:

```



```

assumes  $a \leq b$  and  $0 \leq c$ 
shows
 $a \cdot c \leq b \cdot c$ 
 $c \cdot a \leq c \cdot b$ 
using assms Real_ZF_1_2_L10 ring1.OrdRing_ZF_1_L9
by auto

```

A special case of `Real_ZF_1_2_L14`: we can multiply an inequality by a real number.

```

lemma (in real1) Real_ZF_1_2_L14A:
  assumes A1:  $a \leq b$  and A2:  $c \in \mathbb{R}_+$ 
  shows  $c \cdot a \leq c \cdot b$ 
  using assms Real_ZF_1_2_L10 ring1.OrdRing_ZF_1_L9A
  by simp

```

In the `real1` context notation  $a \leq b$  implies that  $a$  and  $b$  are real numbers.

```

lemma (in real1) Real_ZF_1_2_L15: assumes  $a \leq b$  shows  $a \in \mathbb{R}$   $b \in \mathbb{R}$ 
  using assms Real_ZF_1_2_L10 group3.OrderedGroup_ZF_1_L4
  by auto

```

$a \leq b$  implies that  $0 \leq b - a$ .

```

lemma (in real1) Real_ZF_1_2_L16: assumes  $a \leq b$ 
  shows  $0 \leq b - a$ 
  using assms Real_ZF_1_2_L10 group3.OrderedGroup_ZF_1_L12A
  by simp

```

A sum of nonnegative elements is nonnegative.

```

lemma (in real1) Real_ZF_1_2_L17: assumes  $0 \leq a$   $0 \leq b$ 
  shows  $0 \leq a + b$ 
  using assms Real_ZF_1_2_L10 group3.OrderedGroup_ZF_1_L12
  by simp

```

We can add sides of two inequalities

```

lemma (in real1) Real_ZF_1_2_L18: assumes  $a \leq b$   $c \leq d$ 
  shows  $a + c \leq b + d$ 
  using assms Real_ZF_1_2_L10 group3.OrderedGroup_ZF_1_L5B
  by simp

```

The order on real is reflexive.

```

lemma (in real1) real_ord_refl: assumes  $a \in \mathbb{R}$  shows  $a \leq a$ 
  using assms Real_ZF_1_2_L10 group3.OrderedGroup_ZF_1_L3
  by simp

```

We can add a real number to both sides of an inequality.

```

lemma (in real1) add_num_to_ineq: assumes  $a \leq b$  and  $c \in \mathbb{R}$ 
  shows  $a + c \leq b + c$ 
  using assms Real_ZF_1_2_L10 IsAnOrdGroup_def by simp

```

We can put a number on the other side of an inequality, changing its sign.

```
lemma (in real1) Real_ZF_1_2_L19:
  assumes a∈ℝ b∈ℝ and c ≤ a+b
  shows c-b ≤ a
  using assms Real_ZF_1_2_L10 group3.OrderedGroup_ZF_1_L9C
  by simp
```

What happens when one real number is not greater or equal than another?

```
lemma (in real1) Real_ZF_1_2_L20: assumes a∈ℝ b∈ℝ and ¬(a≤b)
  shows b < a
proof -
  from assms have I:
    group3(ℝ,RealAddition,OrderOnReals)
    OrderOnReals {is total on} ℝ
    a∈ℝ b∈ℝ ¬(⟨a,b⟩ ∈ OrderOnReals)
    using Real_ZF_1_2_L10 by auto
  then have ⟨b,a⟩ ∈ OrderOnReals
    by (rule group3.OrderedGroup_ZF_1_L8)
  then have b ≤ a by simp
  moreover from I have a≠b by (rule group3.OrderedGroup_ZF_1_L8)
  ultimately show b < a by auto
qed
```

We can put a number on the other side of an inequality, changing its sign, version with a minus.

```
lemma (in real1) Real_ZF_1_2_L21:
  assumes a∈ℝ b∈ℝ and c ≤ a-b
  shows c+b ≤ a
  using assms Real_ZF_1_2_L10 group3.OrderedGroup_ZF_1_L5J
  by simp
```

The order on reals is a relation on reals.

```
lemma (in real1) Real_ZF_1_2_L22: shows OrderOnReals ⊆ ℝ×ℝ
  using Real_ZF_1_2_L10 IsAnOrdGroup_def
  by simp
```

A set that is bounded above in the sense defined by order on reals is a subset of real numbers.

```
lemma (in real1) Real_ZF_1_2_L23:
  assumes A1: IsBoundedAbove(A,OrderOnReals)
  shows A ⊆ ℝ
  using A1 Real_ZF_1_2_L22 Order_ZF_3_L1A
  by blast
```

Properties of the maximum of three real numbers.

```
lemma (in real1) Real_ZF_1_2_L24:
  assumes A1: a∈ℝ b∈ℝ c∈ℝ
```

```

shows
Maximum(OrderOnReals,{a,b,c}) ∈ {a,b,c}
Maximum(OrderOnReals,{a,b,c}) ∈ ℝ
a ≤ Maximum(OrderOnReals,{a,b,c})
b ≤ Maximum(OrderOnReals,{a,b,c})
c ≤ Maximum(OrderOnReals,{a,b,c})
proof -
  have IsLinOrder(ℝ,OrderOnReals)
    using Real_ZF_1_2_L10 group3.group_ord_total_is_lin
    by simp
  with A1 show
    Maximum(OrderOnReals,{a,b,c}) ∈ {a,b,c}
    Maximum(OrderOnReals,{a,b,c}) ∈ ℝ
    a ≤ Maximum(OrderOnReals,{a,b,c})
    b ≤ Maximum(OrderOnReals,{a,b,c})
    c ≤ Maximum(OrderOnReals,{a,b,c})
    using Finite_ZF_1_L2A by auto
qed

```

A form of transitivity for the order on reals.

```

lemma (in real1) real_strict_ord_transit:
  assumes A1: a≤b and A2: b<c
  shows a<c
proof -
  from A1 A2 have I:
    group3(ℝ,RealAddition,OrderOnReals)
    ⟨a,b⟩ ∈ OrderOnReals ⟨b,c⟩ ∈ OrderOnReals ∧ b≠c
    using Real_ZF_1_2_L10 by auto
  then have ⟨a,c⟩ ∈ OrderOnReals ∧ a≠c by (rule group3.group_strict_ord_transit)
  then show a<c by simp
qed

```

We can multiply a right hand side of an inequality between positive real numbers by a number that is greater than one.

```

lemma (in real1) Real_ZF_1_2_L25:
  assumes b ∈ ℝ+ and a≤b and 1<c
  shows a<b·c
  using assms reals_are_ord_ring Real_ZF_1_2_L10 ring1.OrdRing_ZF_3_L17
  by simp

```

We can move a real number to the other side of a strict inequality, changing its sign.

```

lemma (in real1) Real_ZF_1_2_L26:
  assumes a∈ℝ b∈ℝ and a-b < c
  shows a < c+b
  using assms Real_ZF_1_2_L10 group3.OrderedGroup_ZF_1_L12B
  by simp

```

Real order is translation invariant.

```

lemma (in real1) real_ord_transl_inv:
  assumes  $a \leq b$  and  $c \in \mathbb{R}$ 
  shows  $c+a \leq c+b$ 
  using assms Real_ZF_1_2_L10 IsAnOrdGroup_def
  by simp

```

It is convenient to have the transitivity of the order on integers in the notation specific to `real1` context. This may be confusing for the presentation readers: even though  $\leq$  and  $\leq$  are printed in the same way, they are different symbols in the source. In the `real1` context the former denotes inequality between integers, and the latter denotes inequality between real numbers (classes of slopes). The next lemma is about transitivity of the order relation on integers.

```

lemma (in real1) int_order_transitive:
  assumes A1:  $a \leq b$   $b \leq c$ 
  shows  $a \leq c$ 
proof -
  from A1 have
     $\langle a, b \rangle \in \text{IntegerOrder}$  and  $\langle b, c \rangle \in \text{IntegerOrder}$ 
  by auto
  then have  $\langle a, c \rangle \in \text{IntegerOrder}$ 
  by (rule Int_ZF_2_L5)
  then show  $a \leq c$  by simp
qed

```

A property of nonempty subsets of real numbers that don't have a maximum: for any element we can find one that is (strictly) greater.

```

lemma (in real1) Real_ZF_1_2_L27:
  assumes  $A \subseteq \mathbb{R}$  and  $\neg \text{HasAmaximum}(\text{OrderOnReals}, A)$  and  $x \in A$ 
  shows  $\exists y \in A. x < y$ 
  using assms Real_ZF_1_2_L10 group3.OrderedGroup_ZF_2_L2B
  by simp

```

The next lemma shows what happens when one real number is not greater or equal than another.

```

lemma (in real1) Real_ZF_1_2_L28:
  assumes  $a \in \mathbb{R}$   $b \in \mathbb{R}$  and  $\neg(a \leq b)$ 
  shows  $b < a$ 
proof -
  from assms have
    group3( $\mathbb{R}$ , RealAddition, OrderOnReals)
    OrderOnReals {is total on}  $\mathbb{R}$ 
     $a \in \mathbb{R}$   $b \in \mathbb{R}$   $\langle a, b \rangle \notin \text{OrderOnReals}$ 
  using Real_ZF_1_2_L10 by auto
  then have  $\langle b, a \rangle \in \text{OrderOnReals} \wedge b \neq a$ 
  by (rule group3.OrderedGroup_ZF_1_L8)
  then show  $b < a$  by simp
qed

```

If a real number is less than another, then the second one can not be less or equal than the first.

```
lemma (in real1) Real_ZF_1_2_L29:
  assumes a<b shows  $\neg(b \leq a)$ 
proof -
  from assms have
    group3( $\mathbb{R}$ , RealAddition, OrderOnReals)
     $\langle a, b \rangle \in \text{OrderOnReals}$   $a \neq b$ 
    using Real_ZF_1_2_L10 by auto
  then have  $\langle b, a \rangle \notin \text{OrderOnReals}$ 
    by (rule group3.OrderedGroup_ZF_1_L8AA)
  then show  $\neg(b \leq a)$  by simp
qed
```

## 40.4 Inverting reals

In this section we tackle the issue of existence of (multiplicative) inverses of real numbers and show that real numbers form an ordered field. We also restate here some facts specific to ordered fields that we need for the construction. The actual proofs of most of these facts can be found in `Field_ZF.thy` and `OrderedField_ZF.thy`

We rewrite the theorem from `Int_ZF_2.thy` that shows that for every positive slope we can find one that is almost equal and has an inverse.

```
lemma (in real1) pos_slopes_have_inv: assumes  $f \in \mathcal{S}_+$ 
  shows  $\exists g \in \mathcal{S}. f \sim g \wedge (\exists h \in \mathcal{S}. g \circ h \sim \text{id}(\text{int}))$ 
  using assms PositiveSlopes_def Slopes_def PositiveIntegers_def
    int1.pos_slope_has_inv SlopeOp1_def SlopeOp2_def
    BoundedIntMaps_def SlopeEquivalenceRel_def
  by simp
```

The set of real numbers we are constructing is an ordered field.

```
theorem (in real1) reals_are_ord_field: shows
  IsAnOrdField(RealNumbers, RealAddition, RealMultiplication, OrderOnReals)
proof -
  let R = RealNumbers
  let A = RealAddition
  let M = RealMultiplication
  let r = OrderOnReals
  have ring1(R, A, M, r) and  $0 \neq 1$ 
    using reals_are_ord_ring OrdRing_ZF_1_L2 real_zero_not_one
    by auto
  moreover have M {is commutative on} R
    using real_mult_commutative by simp
  moreover have
     $\forall a \in \text{PositiveSet}(R, A, r). \exists b \in R. a \cdot b = 1$ 
  proof
```

```

fix a assume a ∈ PositiveSet(R,A,r)
then obtain f where I: f ∈ S+ and II: a = [f]
  using reals_are_ord_ring Real_ZF_1_2_L2
  by auto
then have ∃g ∈ S. f ~ g ∧ (∃h ∈ S. goh ~ id(int))
  using pos_slopes_have_inv by simp
then obtain g where
  III: g ∈ S and IV: f ~ g and V: ∃h ∈ S. goh ~ id(int)
  by auto
from V obtain h where VII: h ∈ S and VIII: goh ~ id(int)
  by auto
from I III IV have [f] = [g]
  using Real_ZF_1_2_L1 Slopes_def Real_ZF_1_1_L5
  by auto
with II III VII VIII have a · [h] = 1
  using Real_ZF_1_1_L4 Real_ZF_1_1_L5A real_one_cl_identity
  by simp
with VII show ∃b ∈ R. a · b = 1 using Real_ZF_1_1_L3
  by auto
qed
ultimately show thesis using ring1.OrdField_ZF_1_L4
  by simp
qed

```

Reals form a field.

```

lemma reals_are_field:
  shows IsAfield(RealNumbers,RealAddition,RealMultiplication)
  using real1.reals_are_ord_field OrdField_ZF_1_L1A
  by simp

```

Theorem proven in field0 and field1 contexts are valid as applied to real numbers.

```

lemma field_cntxts_ok: shows
  field0(RealNumbers,RealAddition,RealMultiplication)
  field1(RealNumbers,RealAddition,RealMultiplication,OrderOnReals)
  using reals_are_field real1.reals_are_ord_field
  field_field0 OrdField_ZF_1_L2 by auto

```

If  $a$  is positive, then  $a^{-1}$  is also positive.

```

lemma (in real1) Real_ZF_1_3_L1: assumes a ∈ ℝ+
  shows a-1 ∈ ℝ+ a-1 ∈ ℝ
  using assms field_cntxts_ok field1.OrdField_ZF_1_L8 PositiveSet_def
  by auto

```

A technical fact about multiplying strict inequality by the inverse of one of the sides.

```

lemma (in real1) Real_ZF_1_3_L2:
  assumes a ∈ ℝ+ and a-1 < b

```

```

shows 1 < b·a
using assms field_cntxts_ok field1.OrdField_ZF_2_L2
by simp

```

If  $a$  is smaller than  $b$ , then  $(b - a)^{-1}$  is positive.

```

lemma (in real1) Real_ZF_1_3_L3: assumes a<b
  shows (b-a)-1 ∈ ℝ+
  using assms field_cntxts_ok field1.OrdField_ZF_1_L9
  by simp

```

We can put a positive factor on the other side of a strict inequality, changing it to its inverse.

```

lemma (in real1) Real_ZF_1_3_L4:
  assumes A1: a∈ℝ  b∈ℝ+ and A2: a·b < c
  shows a < c·b-1
  using assms field_cntxts_ok field1.OrdField_ZF_2_L6
  by simp

```

We can put a positive factor on the other side of a strict inequality, changing it to its inverse, version with the product initially on the right hand side.

```

lemma (in real1) Real_ZF_1_3_L4A:
  assumes A1: b∈ℝ  c∈ℝ+ and A2: a < b·c
  shows a·c-1 < b
  using assms field_cntxts_ok field1.OrdField_ZF_2_L6A
  by simp

```

We can put a positive factor on the other side of an inequality, changing it to its inverse, version with the product initially on the right hand side.

```

lemma (in real1) Real_ZF_1_3_L4B:
  assumes A1: b∈ℝ  c∈ℝ+ and A2: a ≤ b·c
  shows a·c-1 ≤ b
  using assms field_cntxts_ok field1.OrdField_ZF_2_L5A
  by simp

```

We can put a positive factor on the other side of an inequality, changing it to its inverse, version with the product initially on the left hand side.

```

lemma (in real1) Real_ZF_1_3_L4C:
  assumes A1: a∈ℝ  b∈ℝ+ and A2: a·b ≤ c
  shows a ≤ c·b-1
  using assms field_cntxts_ok field1.OrdField_ZF_2_L5
  by simp

```

A technical lemma about solving a strict inequality with three real numbers and inverse of a difference.

```

lemma (in real1) Real_ZF_1_3_L5:
  assumes a<b and (b-a)-1 < c
  shows 1 + a·c < b·c

```

```

using assms field_cntxts_ok field1.OrdField_ZF_2_L9
by simp

```

We can multiply an inequality by the inverse of a positive number.

```

lemma (in real1) Real_ZF_1_3_L6:
  assumes a ≤ b and c ∈ ℝ+ shows a · c-1 ≤ b · c-1
  using assms field_cntxts_ok field1.OrdField_ZF_2_L3
  by simp

```

We can multiply a strict inequality by a positive number or its inverse.

```

lemma (in real1) Real_ZF_1_3_L7:
  assumes a < b and c ∈ ℝ+ shows
    a · c < b · c
    c · a < c · b
    a · c-1 < b · c-1
  using assms field_cntxts_ok field1.OrdField_ZF_2_L4
  by auto

```

An identity with three real numbers, inverse and cancelling.

```

lemma (in real1) Real_ZF_1_3_L8: assumes a ∈ ℝ b ∈ ℝ b ≠ 0 c ∈ ℝ
  shows a · b · (c · b-1) = a · c
  using assms field_cntxts_ok field0.Field_ZF_2_L6
  by simp

```

## 40.5 Completeness

This goal of this section is to show that the order on real numbers is complete, that is every subset of reals that is bounded above has a smallest upper bound.

If  $m$  is an integer, then  $m^R$  is a real number. Recall that in `real1` context  $m^R$  denotes the class of the slope  $n \mapsto m \cdot n$ .

```

lemma (in real1) real_int_is_real: assumes m ∈ int
  shows mR ∈ ℝ
  using assms int1.Int_ZF_2_5_L1 Real_ZF_1_1_L3 by simp

```

The negative of the real embedding of an integer is the embedding of the negative of the integer.

```

lemma (in real1) Real_ZF_1_4_L1: assumes m ∈ int
  shows (-m)R = -(mR)
  using assms int1.Int_ZF_2_5_L3 int1.Int_ZF_2_5_L1 Real_ZF_1_1_L4A
  by simp

```

The embedding of sum of integers is the sum of embeddings.

```

lemma (in real1) Real_ZF_1_4_L1A: assumes m ∈ int k ∈ int
  shows mR + kR = ((m+k)R)
  using assms int1.Int_ZF_2_5_L1 SlopeOp1_def int1.Int_ZF_2_5_L3A

```



Real\_ZF\_1\_1\_L4 by simp

The embedding of a difference of integers is the difference of embeddings.

```

lemma (in real1) Real_ZF_1_4_L1B: assumes A1: m ∈ int k ∈ int
  shows  $m^R - k^R = (m-k)^R$ 
proof -
  from A1 have  $(-k) \in \text{int}$  using int0.Int_ZF_1_1_L4
  by simp
  with A1 have  $(m-k)^R = m^R + (-k)^R$ 
  using Real_ZF_1_4_L1A by simp
  with A1 show  $m^R - k^R = (m-k)^R$ 
  using Real_ZF_1_4_L1 by simp
qed

```

The embedding of the product of integers is the product of embeddings.

```

lemma (in real1) Real_ZF_1_4_L1C: assumes m ∈ int k ∈ int
  shows  $m^R \cdot k^R = (m \cdot k)^R$ 
  using assms int1.Int_ZF_2_5_L1 SlopeOp2_def int1.Int_ZF_2_5_L3B
  Real_ZF_1_1_L4 by simp

```

For any real numbers there is an integer whose real version is greater or equal.

```

lemma (in real1) Real_ZF_1_4_L2: assumes A1:  $a \in \mathbb{R}$ 
  shows  $\exists m \in \text{int}. a \leq m^R$ 
proof -
  from A1 obtain f where I:  $f \in S$  and II:  $a = [f]$ 
  using Real_ZF_1_1_L3A by auto
  then have  $\exists m \in \text{int}. \exists g \in S.$ 
     $\{\langle n, m \cdot n \rangle . n \in \text{int}\} \sim g \wedge (f \sim g \vee (g + (-f)) \in S_+)$ 
  using int1.Int_ZF_2_5_L2 Slopes_def SlopeOp1_def
    BoundedIntMaps_def SlopeEquivalenceRel_def
    PositiveIntegers_def PositiveSlopes_def
  by simp
  then obtain m g where III:  $m \in \text{int}$  and IV:  $g \in S$  and
     $\{\langle n, m \cdot n \rangle . n \in \text{int}\} \sim g \wedge (f \sim g \vee (g + (-f)) \in S_+)$ 
  by auto
  then have  $m^R = [g]$  and  $f \sim g \vee (g + (-f)) \in S_+$ 
  using Real_ZF_1_1_L5A by auto
  with I II IV have  $a \leq m^R$  using Real_ZF_1_2_L12
  by simp
  with III show  $\exists m \in \text{int}. a \leq m^R$  by auto
qed

```

For any real numbers there is an integer whose real version (embedding) is less or equal.

```

lemma (in real1) Real_ZF_1_4_L3: assumes A1:  $a \in \mathbb{R}$ 
  shows  $\{m \in \text{int}. m^R \leq a\} \neq \emptyset$ 
proof -

```

```

from A1 have  $(-a) \in \mathbb{R}$  using Real_ZF_1_1_L8
  by simp
then obtain m where I:  $m \in \text{int}$  and II:  $(-a) \leq m^R$ 
  using Real_ZF_1_4_L2 by auto
let k = GroupInv(int,IntegerAddition)(m)
from A1 I II have  $k \in \text{int}$  and  $k^R \leq a$ 
  using Real_ZF_1_2_L13 Real_ZF_1_4_L1 int0.Int_ZF_1_1_L4
  by auto
then show thesis by auto
qed

```

Embeddings of two integers are equal only if the integers are equal.

```

lemma (in real1) Real_ZF_1_4_L4:
  assumes A1:  $m \in \text{int}$   $k \in \text{int}$  and A2:  $m^R = k^R$ 
  shows  $m=k$ 
proof -
  let r =  $\{\langle n, \text{IntegerMultiplication } \langle m, n \rangle \rangle . n \in \text{int}\}$ 
  let s =  $\{\langle n, \text{IntegerMultiplication } \langle k, n \rangle \rangle . n \in \text{int}\}$ 
  from A1 A2 have  $r \sim s$ 
    using int1.Int_ZF_2_5_L1 AlmostHoms_def Real_ZF_1_1_L5
    by simp
  with A1 have
     $m \in \text{int}$   $k \in \text{int}$ 
     $\langle r, s \rangle \in \text{QuotientGroupRel}(\text{AlmostHoms}(\text{int}, \text{IntegerAddition}),$ 
     $\text{AlHomOp1}(\text{int}, \text{IntegerAddition}), \text{FinRangeFunctions}(\text{int}, \text{int}))$ 
    using SlopeEquivalenceRel_def Slopes_def SlopeOp1_def
    BoundedIntMaps_def by auto
  then show  $m=k$  by (rule int1.Int_ZF_2_5_L6)
qed

```

The embedding of integers preserves the order.

```

lemma (in real1) Real_ZF_1_4_L5: assumes A1:  $m \leq k$ 
  shows  $m^R \leq k^R$ 
proof -
  let r =  $\{\langle n, m \cdot n \rangle . n \in \text{int}\}$ 
  let s =  $\{\langle n, k \cdot n \rangle . n \in \text{int}\}$ 
  from A1 have  $r \in \mathcal{S}$   $s \in \mathcal{S}$ 
    using int0.Int_ZF_2_L1A int1.Int_ZF_2_5_L1 by auto
  moreover from A1 have  $r \sim s \vee s + (-r) \in \mathcal{S}_+$ 
    using Slopes_def SlopeOp1_def BoundedIntMaps_def SlopeEquivalenceRel_def
    PositiveIntegers_def PositiveSlopes_def
    int1.Int_ZF_2_5_L4 by simp
  ultimately show  $m^R \leq k^R$  using Real_ZF_1_2_L12
  by simp
qed

```

The embedding of integers preserves the strict order.

```

lemma (in real1) Real_ZF_1_4_L5A: assumes A1:  $m \leq k$   $m \neq k$ 
  shows  $m^R < k^R$ 

```

```

proof -
  from A1 have  $m^R \leq k^R$  using Real_ZF_1_4_L5
  by simp
  moreover
  from A1 have T:  $m \in \text{int}$   $k \in \text{int}$ 
    using int0.Int_ZF_2_L1A by auto
  with A1 have  $m^R \neq k^R$  using Real_ZF_1_4_L4
    by auto
  ultimately show  $m^R < k^R$  by simp
qed

```

For any real number there is a positive integer whose real version is (strictly) greater. This is Lemma 14 i) in [2].

```

lemma (in real1) Arthan_Lemma14i: assumes A1:  $a \in \mathbb{R}$ 
  shows  $\exists n \in \mathbb{Z}_+. a < n^R$ 

```

```

proof -
  from A1 obtain m where I:  $m \in \text{int}$  and II:  $a \leq m^R$ 
    using Real_ZF_1_4_L2 by auto
  let n = GreaterOf(IntegerOrder, 1_Z, m) + 1_Z
  from I have T:  $n \in \mathbb{Z}_+$  and  $m \leq n$   $m \neq n$ 
    using int0.Int_ZF_1_5_L7B by auto
  then have III:  $m^R < n^R$ 
    using Real_ZF_1_4_L5A by simp
  with II have  $a < n^R$  by (rule real_strict_ord_transit)
  with T show thesis by auto
qed

```

If one embedding is less or equal than another, then the integers are also less or equal.

```

lemma (in real1) Real_ZF_1_4_L6:
  assumes A1:  $k \in \text{int}$   $m \in \text{int}$  and A2:  $m^R \leq k^R$ 
  shows  $m \leq k$ 

```

```

proof -
  { assume A3:  $\langle m, k \rangle \notin \text{IntegerOrder}$ 
    with A1 have  $\langle k, m \rangle \in \text{IntegerOrder}$ 
      by (rule int0.Int_ZF_2_L19)
    then have  $k^R \leq m^R$  using Real_ZF_1_4_L5
      by simp
    with A2 have  $m^R = k^R$  by (rule real_ord_antisym)
    with A1 have  $k = m$  using Real_ZF_1_4_L4
      by auto
    moreover from A1 A3 have  $k \neq m$  by (rule int0.Int_ZF_2_L19)
    ultimately have False by simp
  } then show  $m \leq k$  by auto
qed

```

The floor function is well defined and has expected properties.

```

lemma (in real1) Real_ZF_1_4_L7: assumes A1:  $a \in \mathbb{R}$ 

```

```

shows
  IsBoundedAbove({m ∈ int. mR ≤ a}, IntegerOrder)
  {m ∈ int. mR ≤ a} ≠ 0
  ⌊a⌋ ∈ int
  ⌊a⌋R ≤ a
proof -
  let A = {m ∈ int. mR ≤ a}
  from A1 obtain K where I: K ∈ int and II: a ≤ (KR)
    using Real_ZF_1_4_L2 by auto
  { fix n assume n ∈ A
    then have III: n ∈ int and IV: nR ≤ a
      by auto
    from IV II have (nR) ≤ (KR)
      by (rule real_ord_transitive)
    with I III have n ≤ K using Real_ZF_1_4_L6
      by simp
  } then have ∀n ∈ A. ⟨n, K⟩ ∈ IntegerOrder
    by simp
  then show IsBoundedAbove(A, IntegerOrder)
    by (rule Order_ZF_3_L10)
  moreover from A1 show A ≠ 0 using Real_ZF_1_4_L3
    by simp
  ultimately have Maximum(IntegerOrder, A) ∈ A
    by (rule int0.int_bounded_above_has_max)
  then show ⌊a⌋ ∈ int   ⌊a⌋R ≤ a by auto
qed

```

Every integer whose embedding is less or equal a real number  $a$  is less or equal than the floor of  $a$ .

```

lemma (in real1) Real_ZF_1_4_L8:
  assumes A1: m ∈ int and A2: mR ≤ a
  shows m ≤ ⌊a⌋
proof -
  let A = {m ∈ int. mR ≤ a}
  from A2 have IsBoundedAbove(A, IntegerOrder) and A ≠ 0
    using Real_ZF_1_2_L15 Real_ZF_1_4_L7 by auto
  then have ∀x ∈ A. ⟨x, Maximum(IntegerOrder, A)⟩ ∈ IntegerOrder
    by (rule int0.int_bounded_above_has_max)
  with A1 A2 show m ≤ ⌊a⌋ by simp
qed

```

Integer zero and one embed as real zero and one.

```

lemma (in real1) int_0_1_are_real_zero_one:
  shows 0ZR = 0   1ZR = 1
  using int1.Int_ZF_2_5_L7 BoundedIntMaps_def
    real_one_cl_identity real_zero_cl_bounded_map
  by auto

```

Integer two embeds as the real two.

```

lemma (in real1) int_two_is_real_two: shows  $2_{\mathbb{Z}^R} = 2$ 
proof -
  have  $2_{\mathbb{Z}^R} = 1_{\mathbb{Z}^R} + 1_{\mathbb{Z}^R}$ 
    using int0.int_zero_one_are_int Real_ZF_1_4_L1A
    by simp
  also have  $\dots = 2$  using int_0_1_are_real_zero_one
    by simp
  finally show  $2_{\mathbb{Z}^R} = 2$  by simp
qed

```

A positive integer embeds as a positive (hence nonnegative) real.

```

lemma (in real1) int_pos_is_real_pos: assumes A1:  $p \in \mathbb{Z}_+$ 
shows
   $p^R \in \mathbb{R}$ 
   $0 \leq p^R$ 
   $p^R \in \mathbb{R}_+$ 
proof -
  from A1 have I:  $p \in \text{int } 0_{\mathbb{Z}} \leq p \ 0_{\mathbb{Z}} \neq p$ 
    using PositiveSet_def by auto
  then have  $p^R \in \mathbb{R} \ 0_{\mathbb{Z}^R} \leq p^R$ 
    using real_int_is_real Real_ZF_1_4_L5 by auto
  then show  $p^R \in \mathbb{R} \ 0 \leq p^R$ 
    using int_0_1_are_real_zero_one by auto
  moreover have  $0 \neq p^R$ 
  proof -
    { assume  $0 = p^R$ 
      with I have False using int_0_1_are_real_zero_one
    int0.int_zero_one_are_int Real_ZF_1_4_L4 by auto
    } then show  $0 \neq p^R$  by auto
  qed
  ultimately show  $p^R \in \mathbb{R}_+$  using PositiveSet_def
    by simp
qed

```

The ordered field of reals we are constructing is archimedean, i.e., if  $x, y$  are its elements with  $y$  positive, then there is a positive integer  $M$  such that  $x$  is smaller than  $M^R y$ . This is Lemma 14 ii) in [2].

```

lemma (in real1) Arthan_Lemma14ii: assumes A1:  $x \in \mathbb{R} \ y \in \mathbb{R}_+$ 
shows  $\exists M \in \mathbb{Z}_+. x < M^R \cdot y$ 
proof -
  from A1 have
     $\exists C \in \mathbb{Z}_+. x < C^R$  and  $\exists D \in \mathbb{Z}_+. y^{-1} < D^R$ 
    using Real_ZF_1_3_L1 Arthan_Lemma14i by auto
  then obtain C D where
    I:  $C \in \mathbb{Z}_+$  and II:  $x < C^R$  and
    III:  $D \in \mathbb{Z}_+$  and IV:  $y^{-1} < D^R$ 
    by auto
  let M = C·D
  from I III have

```

```

T: M ∈ ℤ+ CR ∈ ℝ DR ∈ ℝ
using int0.pos_int_closed_mul_unfold PositiveSet_def real_int_is_real
by auto
with A1 I III have CR.(DR.y) = MR.y
using PositiveSet_def Real_ZF_1_L6A Real_ZF_1_4_L1C
by simp
moreover from A1 I II IV have
x < CR.(DR.y)
using int_pos_is_real_pos Real_ZF_1_3_L2 Real_ZF_1_2_L25
by auto
ultimately have x < MR.y
by auto
with T show thesis by auto
qed

```

Taking the floor function preserves the order.

```

lemma (in real1) Real_ZF_1_4_L9: assumes A1: a ≤ b
shows ⌊a⌋ ≤ ⌊b⌋
proof -
from A1 have T: a ∈ ℝ using Real_ZF_1_2_L15
by simp
with A1 have ⌊a⌋R ≤ a and a ≤ b
using Real_ZF_1_4_L7 by auto
then have ⌊a⌋R ≤ b by (rule real_ord_transitive)
moreover from T have ⌊a⌋ ∈ int using Real_ZF_1_4_L7
by simp
ultimately show ⌊a⌋ ≤ ⌊b⌋ using Real_ZF_1_4_L8
by simp
qed

```

If  $S$  is bounded above and  $p$  is a positive intereger, then  $\Gamma(S, p)$  is well defined.

```

lemma (in real1) Real_ZF_1_4_L10:
assumes A1: IsBoundedAbove(S, OrderOnReals) S ≠ 0 and A2: p ∈ ℤ+
shows
IsBoundedAbove({⌊pR.x⌋. x ∈ S}, IntegerOrder)
Γ(S, p) ∈ {⌊pR.x⌋. x ∈ S}
Γ(S, p) ∈ int
proof -
let A = {⌊pR.x⌋. x ∈ S}
from A1 obtain X where I: ∀x ∈ S. x ≤ X
using IsBoundedAbove_def by auto
{ fix m assume m ∈ A
then obtain x where x ∈ S and II: m = ⌊pR.x⌋
by auto
with I have x ≤ X by simp
moreover from A2 have 0 ≤ pR using int_pos_is_real_pos
by simp
ultimately have pR.x ≤ pR.X using Real_ZF_1_2_L14

```

```

    by simp
  with II have m ≤ ⌊pR·x⌋ using Real_ZF_1_4_L9
    by simp
} then have ∀m∈A. ⟨m, ⌊pR·x⌋⟩ ∈ IntegerOrder
  by auto
then show II: IsBoundedAbove(A, IntegerOrder)
  by (rule Order_ZF_3_L10)
moreover from A1 have III: A ≠ 0 by simp
ultimately have Maximum(IntegerOrder, A) ∈ A
  by (rule int0.int_bounded_above_has_max)
moreover from II III have Maximum(IntegerOrder, A) ∈ int
  by (rule int0.int_bounded_above_has_max)
ultimately show Γ(S, p) ∈ {⌊pR·x⌋. x∈S} and Γ(S, p) ∈ int
  by auto
qed

```

If  $p$  is a positive integer, then for all  $s \in S$  the floor of  $p \cdot x$  is not greater than  $\Gamma(S, p)$ .

```

lemma (in real1) Real_ZF_1_4_L11:
  assumes A1: IsBoundedAbove(S, OrderOnReals) and A2: x∈S and A3: p∈ℤ+
  shows ⌊pR·x⌋ ≤ Γ(S, p)
proof -
  let A = {⌊pR·x⌋. x∈S}
  from A2 have S≠0 by auto
  with A1 A3 have IsBoundedAbove(A, IntegerOrder) A ≠ 0
    using Real_ZF_1_4_L10 by auto
  then have ∀x∈A. ⟨x, Maximum(IntegerOrder, A)⟩ ∈ IntegerOrder
    by (rule int0.int_bounded_above_has_max)
  with A2 show ⌊pR·x⌋ ≤ Γ(S, p) by simp
qed

```

The candidate for supremum is an integer mapping with values given by  $\Gamma$ .

```

lemma (in real1) Real_ZF_1_4_L12:
  assumes A1: IsBoundedAbove(S, OrderOnReals) S≠0 and
  A2: g = {⟨p, Γ(S, p)⟩. p∈ℤ+}
  shows
  g : ℤ+→int
  ∀n∈ℤ+. g(n) = Γ(S, n)
proof -
  from A1 have ∀n∈ℤ+. Γ(S, n) ∈ int using Real_ZF_1_4_L10
    by simp
  with A2 show I: g : ℤ+→int using ZF_fun_from_total by simp
  { fix n assume n∈ℤ+
    with A2 I have g(n) = Γ(S, n) using ZF_fun_from_tot_val
      by simp
  } then show ∀n∈ℤ+. g(n) = Γ(S, n) by simp
qed

```

Every integer is equal to the floor of its embedding.

```

lemma (in real1) Real_ZF_1_4_L14: assumes A1:  $m \in \text{int}$ 
  shows  $\lfloor m^R \rfloor = m$ 
proof -
  let A =  $\{n \in \text{int}. n^R \leq m^R\}$ 
  have antisym(IntegerOrder) using int0.Int_ZF_2_L4
    by simp
  moreover from A1 have  $m \in A$ 
    using real_int_is_real real_ord_refl by auto
  moreover from A1 have  $\forall n \in A. \langle n, m \rangle \in \text{IntegerOrder}$ 
    using Real_ZF_1_4_L6 by auto
  ultimately show  $\lfloor m^R \rfloor = m$  using Order_ZF_4_L14
    by auto
qed

```

Floor of (real) zero is (integer) zero.

```

lemma (in real1) floor_01_is_zero_one: shows
   $\lfloor 0 \rfloor = 0_Z$   $\lfloor 1 \rfloor = 1_Z$ 
proof -
  have  $\lfloor (0_Z)^R \rfloor = 0_Z$  and  $\lfloor (1_Z)^R \rfloor = 1_Z$ 
    using int0.int_zero_one_are_int Real_ZF_1_4_L14
    by auto
  then show  $\lfloor 0 \rfloor = 0_Z$  and  $\lfloor 1 \rfloor = 1_Z$ 
    using int_0_1_are_real_zero_one
    by auto
qed

```

Floor of (real) two is (integer) two.

```

lemma (in real1) floor_2_is_two: shows  $\lfloor 2 \rfloor = 2_Z$ 
proof -
  have  $\lfloor (2_Z)^R \rfloor = 2_Z$ 
    using int0.int_two_three_are_int Real_ZF_1_4_L14
    by simp
  then show  $\lfloor 2 \rfloor = 2_Z$  using int_two_is_real_two
    by simp
qed

```

Floor of a product of embeddings of integers is equal to the product of integers.

```

lemma (in real1) Real_ZF_1_4_L14A: assumes A1:  $m \in \text{int}$   $k \in \text{int}$ 
  shows  $\lfloor m^R \cdot k^R \rfloor = m \cdot k$ 
proof -
  from A1 have T:  $m \cdot k \in \text{int}$ 
    using int0.Int_ZF_1_1_L5 by simp
  from A1 have  $\lfloor m^R \cdot k^R \rfloor = \lfloor (m \cdot k)^R \rfloor$  using Real_ZF_1_4_L1C
    by simp
  with T show  $\lfloor m^R \cdot k^R \rfloor = m \cdot k$  using Real_ZF_1_4_L14
    by simp
qed

```



Floor of the sum of a number and the embedding of an integer is the floor of the number plus the integer.

**lemma** (in real1) Real\_ZF\_1\_4\_L15: assumes A1:  $x \in \mathbb{R}$  and A2:  $p \in \text{int}$   
shows  $\lfloor x + p^R \rfloor = \lfloor x \rfloor + p$

**proof** -

let A =  $\{n \in \text{int}. n^R \leq x + p^R\}$   
have antisym(IntegerOrder) using int0.Int\_ZF\_2\_L4  
by simp  
moreover have  $\lfloor x \rfloor + p \in A$   
**proof** -  
from A1 A2 have  $\lfloor x \rfloor^R \leq x$  and  $p^R \in \mathbb{R}$   
using Real\_ZF\_1\_4\_L7 real\_int\_is\_real by auto  
then have  $\lfloor x \rfloor^R + p^R \leq x + p^R$   
using add\_num\_to\_ineq by simp  
moreover from A1 A2 have  $(\lfloor x \rfloor + p)^R = \lfloor x \rfloor^R + p^R$   
using Real\_ZF\_1\_4\_L7 Real\_ZF\_1\_4\_L1A by simp  
ultimately have  $(\lfloor x \rfloor + p)^R \leq x + p^R$   
by simp  
moreover from A1 A2 have  $\lfloor x \rfloor + p \in \text{int}$   
using Real\_ZF\_1\_4\_L7 int0.Int\_ZF\_1\_1\_L5 by simp  
ultimately show  $\lfloor x \rfloor + p \in A$  by auto

**qed**

moreover have  $\forall n \in A. n \leq \lfloor x \rfloor + p$

**proof**

fix n assume  $n \in A$   
then have I:  $n \in \text{int}$  and  $n^R \leq x + p^R$   
by auto  
with A1 A2 have  $n^R - p^R \leq x$   
using real\_int\_is\_real Real\_ZF\_1\_2\_L19  
by simp  
with A2 I have  $\lfloor (n-p)^R \rfloor \leq \lfloor x \rfloor$   
using Real\_ZF\_1\_4\_L1B Real\_ZF\_1\_4\_L9  
by simp  
moreover  
from A2 I have  $n-p \in \text{int}$   
using int0.Int\_ZF\_1\_1\_L5 by simp  
then have  $\lfloor (n-p)^R \rfloor = n-p$   
using Real\_ZF\_1\_4\_L14 by simp  
ultimately have  $n-p \leq \lfloor x \rfloor$   
by simp  
with A2 I show  $n \leq \lfloor x \rfloor + p$   
using int0.Int\_ZF\_2\_L9C by simp

**qed**

ultimately show  $\lfloor x + p^R \rfloor = \lfloor x \rfloor + p$   
using Order\_ZF\_4\_L14 by auto

**qed**

Floor of the difference of a number and the embedding of an integer is the floor of the number minus the integer.

```

lemma (in real1) Real_ZF_1_4_L16: assumes A1:  $x \in \mathbb{R}$  and A2:  $p \in \text{int}$ 
  shows  $\lfloor x - p^R \rfloor = \lfloor x \rfloor - p$ 
proof -
  from A2 have  $\lfloor x - p^R \rfloor = \lfloor x + (-p)^R \rfloor$ 
    using Real_ZF_1_4_L1 by simp
  with A1 A2 show  $\lfloor x - p^R \rfloor = \lfloor x \rfloor - p$ 
    using int0.Int_ZF_1_1_L4 Real_ZF_1_4_L15 by simp
qed

```

The floor of sum of embeddings is the sum of the integers.

```

lemma (in real1) Real_ZF_1_4_L17: assumes  $m \in \text{int}$   $n \in \text{int}$ 
  shows  $\lfloor (m^R) + n^R \rfloor = m + n$ 
  using assms real_int_is_real Real_ZF_1_4_L15 Real_ZF_1_4_L14
  by simp

```

A lemma about adding one to floor.

```

lemma (in real1) Real_ZF_1_4_L17A: assumes A1:  $a \in \mathbb{R}$ 
  shows  $1 + \lfloor a \rfloor^R = (1_Z + \lfloor a \rfloor)^R$ 
proof -
  have  $1 + \lfloor a \rfloor^R = 1_Z^R + \lfloor a \rfloor^R$ 
    using int_0_1_are_real_zero_one by simp
  with A1 show  $1 + \lfloor a \rfloor^R = (1_Z + \lfloor a \rfloor)^R$ 
    using int0.int_zero_one_are_int Real_ZF_1_4_L7 Real_ZF_1_4_L1A
    by simp
qed

```

The difference between the a number and the embedding of its floor is (strictly) less than one.

```

lemma (in real1) Real_ZF_1_4_L17B: assumes A1:  $a \in \mathbb{R}$ 
  shows
     $a - \lfloor a \rfloor^R < 1$ 
     $a < (1_Z + \lfloor a \rfloor)^R$ 
proof -
  from A1 have T1:  $\lfloor a \rfloor \in \text{int}$   $\lfloor a \rfloor^R \in \mathbb{R}$  and
    T2:  $1 \in \mathbb{R}$   $a - \lfloor a \rfloor^R \in \mathbb{R}$ 
    using Real_ZF_1_4_L7 real_int_is_real Real_ZF_1_L6 Real_ZF_1_L4
    by auto
  { assume  $1 \leq a - \lfloor a \rfloor^R$ 
    with A1 T1 have  $\lfloor 1_Z^R + \lfloor a \rfloor^R \rfloor \leq \lfloor a \rfloor$ 
      using Real_ZF_1_2_L21 Real_ZF_1_4_L9 int_0_1_are_real_zero_one
      by simp
    with T1 have False
      using int0.int_zero_one_are_int Real_ZF_1_4_L17
      int0.Int_ZF_1_2_L3AA by simp
  } then have I:  $\neg(1 \leq a - \lfloor a \rfloor^R)$  by auto
  with T2 show II:  $a - \lfloor a \rfloor^R < 1$ 
    by (rule Real_ZF_1_2_L20)
  with A1 T1 I II have
     $a < 1 + \lfloor a \rfloor^R$ 

```

```

    using Real_ZF_1_2_L26 by simp
  with A1 show  $a < (1_Z + \lfloor a \rfloor)^R$ 
    using Real_ZF_1_4_L17A by simp
qed

```

The next lemma corresponds to Lemma 14 iii) in [2]. It says that we can find a rational number between any two different real numbers.

```

lemma (in real1) Arthan_Lemma14iii: assumes A1:  $x < y$ 
  shows  $\exists M \in \text{int}. \exists N \in \mathbb{Z}_+. x \cdot N^R < M^R \wedge M^R < y \cdot N^R$ 
proof -
  from A1 have  $(y-x)^{-1} \in \mathbb{R}_+$  using Real_ZF_1_3_L3
  by simp
  then have
     $\exists N \in \mathbb{Z}_+. (y-x)^{-1} < N^R$ 
    using Arthan_Lemma14i PositiveSet_def by simp
  then obtain N where I:  $N \in \mathbb{Z}_+$  and II:  $(y-x)^{-1} < N^R$ 
  by auto
  let  $M = 1_Z + \lfloor x \cdot N^R \rfloor$ 
  from A1 I have
    T1:  $x \in \mathbb{R} \quad N^R \in \mathbb{R} \quad N^R \in \mathbb{R}_+ \quad x \cdot N^R \in \mathbb{R}$ 
    using Real_ZF_1_2_L15 PositiveSet_def real_int_is_real
    Real_ZF_1_L6 int_pos_is_real_pos by auto
  then have T2:  $M \in \text{int}$  using
    int0.int_zero_one_are_int Real_ZF_1_4_L7 int0.Int_ZF_1_1_L5
  by simp
  from T1 have III:  $x \cdot N^R < M^R$ 
    using Real_ZF_1_4_L17B by simp
  from T1 have  $(1 + \lfloor x \cdot N^R \rfloor^R) \leq (1 + x \cdot N^R)$ 
    using Real_ZF_1_4_L7 Real_ZF_1_L4 real_ord_transl_inv
  by simp
  with T1 have  $M^R \leq (1 + x \cdot N^R)$ 
    using Real_ZF_1_4_L17A by simp
  moreover from A1 II have  $(1 + x \cdot N^R) < y \cdot N^R$ 
    using Real_ZF_1_3_L5 by simp
  ultimately have  $M^R < y \cdot N^R$ 
    by (rule real_strict_ord_transit)
  with I T2 III show thesis by auto
qed

```

Some estimates for the homomorphism difference of the floor function.

```

lemma (in real1) Real_ZF_1_4_L18: assumes A1:  $x \in \mathbb{R} \quad y \in \mathbb{R}$ 
  shows
     $\text{abs}(\lfloor x+y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor) \leq 2_Z$ 
proof -
  from A1 have T:
     $\lfloor x \rfloor^R \in \mathbb{R} \quad \lfloor y \rfloor^R \in \mathbb{R}$ 
     $x+y - (\lfloor x \rfloor^R) \in \mathbb{R}$ 
    using Real_ZF_1_4_L7 real_int_is_real Real_ZF_1_L6
  by auto

```

```

from A1 have
  0 ≤ x - (⌊x⌋R) + (y - (⌊y⌋R))
  x - (⌊x⌋R) + (y - (⌊y⌋R)) ≤ 2
  using Real_ZF_1_4_L7 Real_ZF_1_2_L16 Real_ZF_1_2_L17
  Real_ZF_1_4_L17B Real_ZF_1_2_L18 by auto
moreover from A1 T have
  x - (⌊x⌋R) + (y - (⌊y⌋R)) = x+y - (⌊x⌋R) - (⌊y⌋R)
  using Real_ZF_1_L7A by simp
ultimately have
  0 ≤ x+y - (⌊x⌋R) - (⌊y⌋R)
  x+y - (⌊x⌋R) - (⌊y⌋R) ≤ 2
  by auto
then have
  ⌊0⌋ ≤ ⌊x+y - (⌊x⌋R) - (⌊y⌋R)⌋
  ⌊x+y - (⌊x⌋R) - (⌊y⌋R)⌋ ≤ ⌊2⌋
  using Real_ZF_1_4_L9 by auto
then have
  0Z ≤ ⌊x+y - (⌊x⌋R) - (⌊y⌋R)⌋
  ⌊x+y - (⌊x⌋R) - (⌊y⌋R)⌋ ≤ 2Z
  using floor_01_is_zero_one floor_2_is_two by auto
moreover from A1 have
  ⌊x+y - (⌊x⌋R) - (⌊y⌋R)⌋ = ⌊x+y⌋ - ⌊x⌋ - ⌊y⌋
  using Real_ZF_1_L6 Real_ZF_1_4_L7 real_int_is_real Real_ZF_1_4_L16
  by simp
ultimately have
  0Z ≤ ⌊x+y⌋ - ⌊x⌋ - ⌊y⌋
  ⌊x+y⌋ - ⌊x⌋ - ⌊y⌋ ≤ 2Z
  by auto
then show abs(⌊x+y⌋ - ⌊x⌋ - ⌊y⌋) ≤ 2Z
  using int0.Int_ZF_2_L16 by simp
qed

```

Suppose  $S \neq \emptyset$  is bounded above and  $\Gamma(S, m) = \lfloor m^R \cdot x \rfloor$  for some positive integer  $m$  and  $x \in S$ . Then if  $y \in S, x \leq y$  we also have  $\Gamma(S, m) = \lfloor m^R \cdot y \rfloor$ .

```

lemma (in real1) Real_ZF_1_4_L20:
  assumes A1: IsBoundedAbove(S, OrderOnReals)  S≠0 and
  A2: n∈ℤ+ x∈S and
  A3: Γ(S, n) = ⌊nR·x⌋ and
  A4: y∈S x≤y
  shows Γ(S, n) = ⌊nR·y⌋
proof -
  from A2 A4 have ⌊nR·x⌋ ≤ ⌊(nR)·y⌋
  using int_pos_is_real_pos Real_ZF_1_2_L14 Real_ZF_1_4_L9
  by simp
  with A3 have ⟨Γ(S, n), ⌊(nR)·y⌋⟩ ∈ IntegerOrder
  by simp
  moreover from A1 A2 A4 have ⟨⌊nR·y⌋, Γ(S, n)⟩ ∈ IntegerOrder
  using Real_ZF_1_4_L11 by simp
  ultimately show Γ(S, n) = ⌊nR·y⌋

```

by (rule int0.Int\_ZF\_2\_L3)  
qed

The homomorphism difference of  $n \mapsto \Gamma(S, n)$  is bounded by 2 on positive integers.

```

lemma (in real1) Real_ZF_1_4_L21:
  assumes A1: IsBoundedAbove(S, OrderOnReals) S ≠ 0 and
  A2: m ∈ ℤ+ n ∈ ℤ+
  shows abs(Γ(S, m+n) - Γ(S, m) - Γ(S, n)) ≤ 2ℤ
proof -
  from A2 have T: m+n ∈ ℤ+ using int0.pos_int_closed_add_unfolded
  by simp
  with A1 A2 have
    Γ(S, m) ∈ {⌊mR·x⌋. x ∈ S} and
    Γ(S, n) ∈ {⌊nR·x⌋. x ∈ S} and
    Γ(S, m+n) ∈ {⌊(m+n)R·x⌋. x ∈ S}
  using Real_ZF_1_4_L10 by auto
  then obtain a b c where I: a ∈ S b ∈ S c ∈ S
  and II:
    Γ(S, m) = ⌊mR·a⌋
    Γ(S, n) = ⌊nR·b⌋
    Γ(S, m+n) = ⌊(m+n)R·c⌋
  by auto
  let d = Maximum(OrderOnReals, {a, b, c})
  from A1 I have a ∈ ℝ b ∈ ℝ c ∈ ℝ
  using Real_ZF_1_2_L23 by auto
  then have IV:
    d ∈ {a, b, c}
    d ∈ ℝ
    a ≤ d
    b ≤ d
    c ≤ d
  using Real_ZF_1_2_L24 by auto
  with I have V: d ∈ S by auto
  from A1 T I II IV V have Γ(S, m+n) = ⌊(m+n)R·d⌋
  using Real_ZF_1_4_L20 by blast
  also from A2 have ... = ⌊((mR)+(nR))·d⌋
  using Real_ZF_1_4_L1A PositiveSet_def by simp
  also from A2 IV have ... = ⌊(mR)·d + (nR)·d⌋
  using PositiveSet_def real_int_is_real Real_ZF_1_L7
  by simp
  finally have Γ(S, m+n) = ⌊(mR)·d + (nR)·d⌋
  by simp
  moreover from A1 A2 I II IV V have Γ(S, m) = ⌊mR·d⌋
  using Real_ZF_1_4_L20 by blast
  moreover from A1 A2 I II IV V have Γ(S, n) = ⌊nR·d⌋
  using Real_ZF_1_4_L20 by blast
  moreover from A1 T I II IV V have Γ(S, m+n) = ⌊(m+n)R·d⌋
  using Real_ZF_1_4_L20 by blast

```

```

ultimately have abs( $\Gamma(S, m+n) - \Gamma(S, m) - \Gamma(S, n)$ ) =
  abs( $\lfloor (m^R) \cdot d + (n^R) \cdot d \rfloor - \lfloor m^R \cdot d \rfloor - \lfloor n^R \cdot d \rfloor$ )
  by simp
with A2 IV show
  abs( $\Gamma(S, m+n) - \Gamma(S, m) - \Gamma(S, n)$ )  $\leq 2_Z$ 
  using PositiveSet_def real_int_is_real Real_ZF_1_L6
    Real_ZF_1_4_L18 by simp
qed

```

The next lemma provides sufficient condition for an odd function to be an almost homomorphism. It says for odd functions we only need to check that the homomorphism difference (denoted  $\delta$  in the `real1` context) is bounded on positive integers. This is really proven in `Int_ZF_2.thy`, but we restate it here for convenience. Recall from `Group_ZF_3.thy` that `OddExtension` of a function defined on the set of positive elements (of an ordered group) is the only odd function that is equal to the given one when restricted to positive elements.

```

lemma (in real1) Real_ZF_1_4_L21A:
  assumes A1:  $f: \mathbb{Z}_+ \rightarrow \text{int}$   $\forall a \in \mathbb{Z}_+. \forall b \in \mathbb{Z}_+. \text{abs}(\delta(f, a, b)) \leq L$ 
  shows OddExtension(int, IntegerAddition, IntegerOrder, f)  $\in \mathcal{S}$ 
  using A1 int1.Int_ZF_2_1_L24 by auto

```

The candidate for (a representant of) the supremum of a nonempty bounded above set is a slope.

```

lemma (in real1) Real_ZF_1_4_L22:
  assumes A1: IsBoundedAbove(S, OrderOnReals)  $S \neq 0$  and
  A2:  $g = \{ \langle p, \Gamma(S, p) \rangle. p \in \mathbb{Z}_+ \}$ 
  shows OddExtension(int, IntegerAddition, IntegerOrder, g)  $\in \mathcal{S}$ 
proof -
  from A1 A2 have  $g: \mathbb{Z}_+ \rightarrow \text{int}$  by (rule Real_ZF_1_4_L12)
  moreover have  $\forall m \in \mathbb{Z}_+. \forall n \in \mathbb{Z}_+. \text{abs}(\delta(g, m, n)) \leq 2_Z$ 
  proof -
    { fix m n assume A3:  $m \in \mathbb{Z}_+ \quad n \in \mathbb{Z}_+$ 
      then have  $m+n \in \mathbb{Z}_+ \quad m \in \mathbb{Z}_+ \quad n \in \mathbb{Z}_+$ 
    }
  using int0.pos_int_closed_add_unfolded
  by auto
  moreover from A1 A2 have  $\forall n \in \mathbb{Z}_+. g(n) = \Gamma(S, n)$ 
  by (rule Real_ZF_1_4_L12)
  ultimately have  $\delta(g, m, n) = \Gamma(S, m+n) - \Gamma(S, m) - \Gamma(S, n)$ 
  by simp
  moreover from A1 A3 have
    abs( $\Gamma(S, m+n) - \Gamma(S, m) - \Gamma(S, n)$ )  $\leq 2_Z$ 
  by (rule Real_ZF_1_4_L21)
  ultimately have abs( $\delta(g, m, n)$ )  $\leq 2_Z$ 
  by simp
} then show  $\forall m \in \mathbb{Z}_+. \forall n \in \mathbb{Z}_+. \text{abs}(\delta(g, m, n)) \leq 2_Z$ 
  by simp
qed

```

ultimately show thesis by (rule Real\_ZF\_1\_4\_L21A)  
qed

A technical lemma used in the proof that all elements of  $S$  are less or equal than the candidate for supremum of  $S$ .

```
lemma (in real1) Real_ZF_1_4_L23:
  assumes A1:  $f \in \mathcal{S}$  and A2:  $N \in \text{int}$   $M \in \text{int}$  and
  A3:  $\forall n \in \mathbb{Z}_+. M \cdot n \leq f(N \cdot n)$ 
  shows  $M^R \leq [f] \cdot (N^R)$ 
proof -
  let  $M^S = \{\langle n, M \cdot n \rangle \mid n \in \text{int}\}$ 
  let  $N^S = \{\langle n, N \cdot n \rangle \mid n \in \text{int}\}$ 
  from A1 A2 have T:  $M^S \in \mathcal{S}$   $N^S \in \mathcal{S}$   $f \circ N^S \in \mathcal{S}$ 
    using int1.Int_ZF_2_5_L1 int1.Int_ZF_2_1_L11 SlopeOp2_def
    by auto
  moreover from A1 A2 A3 have  $M^S \sim f \circ N^S \vee f \circ N^S + (-M^S) \in \mathcal{S}_+$ 
    using int1.Int_ZF_2_5_L8 SlopeOp2_def SlopeOp1_def Slopes_def
    BoundedIntMaps_def SlopeEquivalenceRel_def PositiveIntegers_def
    PositiveSlopes_def by simp
  ultimately have  $[M^S] \leq [f \circ N^S]$  using Real_ZF_1_2_L12
    by simp
  with A1 T show  $M^R \leq [f] \cdot (N^R)$  using Real_ZF_1_1_L4
    by simp
qed
```

A technical lemma aimed used in the proof the candidate for supremum of  $S$  is less or equal than any upper bound for  $S$ .

```
lemma (in real1) Real_ZF_1_4_L23A:
  assumes A1:  $f \in \mathcal{S}$  and A2:  $N \in \text{int}$   $M \in \text{int}$  and
  A3:  $\forall n \in \mathbb{Z}_+. f(N \cdot n) \leq M \cdot n$ 
  shows  $[f] \cdot (N^R) \leq M^R$ 
proof -
  let  $M^S = \{\langle n, M \cdot n \rangle \mid n \in \text{int}\}$ 
  let  $N^S = \{\langle n, N \cdot n \rangle \mid n \in \text{int}\}$ 
  from A1 A2 have T:  $M^S \in \mathcal{S}$   $N^S \in \mathcal{S}$   $f \circ N^S \in \mathcal{S}$ 
    using int1.Int_ZF_2_5_L1 int1.Int_ZF_2_1_L11 SlopeOp2_def
    by auto
  moreover from A1 A2 A3 have
     $f \circ N^S \sim M^S \vee M^S + (-(f \circ N^S)) \in \mathcal{S}_+$ 
    using int1.Int_ZF_2_5_L9 SlopeOp2_def SlopeOp1_def Slopes_def
    BoundedIntMaps_def SlopeEquivalenceRel_def PositiveIntegers_def
    PositiveSlopes_def by simp
  ultimately have  $[f \circ N^S] \leq [M^S]$  using Real_ZF_1_2_L12
    by simp
  with A1 T show  $[f] \cdot (N^R) \leq M^R$  using Real_ZF_1_1_L4
    by simp
qed
```

The essential condition to claim that the candidate for supremum of  $S$  is

greater or equal than all elements of  $S$ .

```

lemma (in real1) Real_ZF_1_4_L24:
  assumes A1: IsBoundedAbove(S,OrderOnReals) and
  A2: x<y y∈S and
  A4: N ∈ ℤ+ M ∈ int and
  A5: MR < y·NR and A6: p ∈ ℤ+
  shows p·M ≤ Γ(S,p·N)
proof -
  from A2 A4 A6 have T1:
    NR ∈ ℝ+ y∈ℝ pR ∈ ℝ+
    p·N ∈ ℤ+ (p·N)R ∈ ℝ+
    using int_pos_is_real_pos Real_ZF_1_2_L15
    int0_pos_int_closed_mul_unfold by auto
  with A4 A6 have T2:
    p ∈ int pR ∈ ℝ NR ∈ ℝ NR ≠ 0 MR ∈ ℝ
    using real_int_is_real PositiveSet_def by auto
  from T1 A5 have ⌊(p·N)R·(MR·(NR)-1)⌋ ≤ ⌊(p·N)R·y⌋
    using Real_ZF_1_3_L4A Real_ZF_1_3_L7 Real_ZF_1_4_L9
    by simp
  moreover from A1 A2 T1 have ⌊(p·N)R·y⌋ ≤ Γ(S,p·N)
    using Real_ZF_1_4_L11 by simp
  ultimately have I: ⌊(p·N)R·(MR·(NR)-1)⌋ ≤ Γ(S,p·N)
    by (rule int_order_transitive)
  from A4 A6 have (p·N)R·(MR·(NR)-1) = pR·NR·(MR·(NR)-1)
    using PositiveSet_def Real_ZF_1_4_L1C by simp
  with A4 T2 have ⌊(p·N)R·(MR·(NR)-1)⌋ = p·M
    using Real_ZF_1_3_L8 Real_ZF_1_4_L14A by simp
  with I show p·M ≤ Γ(S,p·N) by simp
qed

```

An obvious fact about odd extension of a function  $p \mapsto \Gamma(s, p)$  that is used a couple of times in proofs.

```

lemma (in real1) Real_ZF_1_4_L24A:
  assumes A1: IsBoundedAbove(S,OrderOnReals) S≠0 and A2: p ∈ ℤ+
  and A3:
  h = OddExtension(int,IntegerAddition,IntegerOrder,{⟨p,Γ(S,p)⟩. p∈ℤ+})
  shows h(p) = Γ(S,p)
proof -
  let g = {⟨p,Γ(S,p)⟩. p∈ℤ+}
  from A1 have I: g : ℤ+→int using Real_ZF_1_4_L12
  by blast
  with A2 A3 show h(p) = Γ(S,p)
    using int0.Int_ZF_1_5_L11 ZF_fun_from_tot_val
    by simp
qed

```

The candidate for the supremum of  $S$  is not smaller than any element of  $S$ .

```

lemma (in real1) Real_ZF_1_4_L25:

```



```

assumes A1: IsBoundedAbove(S,OrderOnReals) and
A2: ¬HasAmaximum(OrderOnReals,S) and
A3: x∈S and A4:
h = OddExtension(int,IntegerAddition,IntegerOrder,{⟨p,Γ(S,p)⟩. p∈ℤ+})
shows x ≤ [h]
proof -
  from A1 A2 A3 have
    S ⊆ ℝ ¬HasAmaximum(OrderOnReals,S) x∈S
    using Real_ZF_1_2_L23 by auto
  then have ∃y∈S. x<y by (rule Real_ZF_1_2_L27)
  then obtain y where I: y∈S and II: x<y
    by auto
  from II have
    ∃M∈int. ∃N∈ℤ+. x·NR < MR ∧ MR < y·NR
    using Arthan_Lemma14iii by simp
  then obtain M N where III: M ∈ int N∈ℤ+ and
    IV: x·NR < MR MR < y·NR
    by auto
  from II III IV have V: x ≤ MR·(NR)-1
    using int_pos_is_real_pos Real_ZF_1_2_L15 Real_ZF_1_3_L4
    by auto
  from A3 have VI: S≠0 by auto
  with A1 A4 have T1: h ∈ S using Real_ZF_1_4_L22
    by simp
  moreover from III have N ∈ int M ∈ int
    using PositiveSet_def by auto
  moreover have ∀n∈ℤ+. M·n ≤ h(N·n)
proof
  let g = {⟨p,Γ(S,p)⟩. p∈ℤ+}
  fix n assume A5: n∈ℤ+
  with III have T2: N·n ∈ ℤ+
    using int0.pos_int_closed_mul_unfold by simp
  from III A5 have
    N·n = n·N and n·M = M·n
    using PositiveSet_def int0.Int_ZF_1_1_L5 by auto
  moreover
  from A1 I II III IV A5 have
    IsBoundedAbove(S,OrderOnReals)
    x<y y∈S
    N ∈ ℤ+ M ∈ int
    MR < y·NR n ∈ ℤ+
    by auto
  then have n·M ≤ Γ(S,n·N) by (rule Real_ZF_1_4_L24)
  moreover from A1 A4 VI T2 have h(N·n) = Γ(S,N·n)
    using Real_ZF_1_4_L24A by simp
  ultimately show M·n ≤ h(N·n) by auto
qed
ultimately have MR ≤ [h]·NR using Real_ZF_1_4_L23
  by simp

```

```

with III T1 have  $M^R \cdot (N^R)^{-1} \leq [h]$ 
  using int_pos_is_real_pos Real_ZF_1_1_L3 Real_ZF_1_3_L4B
  by simp
with V show  $x \leq [h]$  by (rule real_ord_transitive)
qed

```

The essential condition to claim that the candidate for supremum of  $S$  is less or equal than any upper bound of  $S$ .

```

lemma (in real1) Real_ZF_1_4_L26:
  assumes A1: IsBoundedAbove(S, OrderOnReals) and
  A2:  $x \leq y \implies x \in S$  and
  A4:  $N \in \mathbb{Z}_+$   $M \in \text{int}$  and
  A5:  $y \cdot N^R < M^R$  and A6:  $p \in \mathbb{Z}_+$ 
  shows  $\lfloor (N \cdot p)^R \cdot x \rfloor \leq M \cdot p$ 
proof -
  from A2 A4 A6 have T:
     $p \cdot N \in \mathbb{Z}_+$   $p \in \text{int}$   $N \in \text{int}$ 
     $p^R \in \mathbb{R}_+$   $p^R \in \mathbb{R}$   $N^R \in \mathbb{R}$   $x \in \mathbb{R}$   $y \in \mathbb{R}$ 
    using int0.pos_int_closed_mul_unfold PositiveSet_def
    real_int_is_real Real_ZF_1_2_L15 int_pos_is_real_pos
    by auto
  with A2 have  $(p \cdot N)^R \cdot x \leq (p \cdot N)^R \cdot y$ 
    using int_pos_is_real_pos Real_ZF_1_2_L14A
    by simp
  moreover from A4 T have I:
     $(p \cdot N)^R = p^R \cdot N^R$ 
     $(p \cdot M)^R = p^R \cdot M^R$ 
    using Real_ZF_1_4_L1C by auto
  ultimately have  $(p \cdot N)^R \cdot x \leq p^R \cdot N^R \cdot y$ 
    by simp
  moreover
  from A5 T I have  $p^R \cdot (y \cdot N^R) < (p \cdot M)^R$ 
    using Real_ZF_1_3_L7 by simp
  with T have  $p^R \cdot N^R \cdot y < (p \cdot M)^R$  using Real_ZF_1_1_L9
    by simp
  ultimately have  $(p \cdot N)^R \cdot x < (p \cdot M)^R$ 
    by (rule real_strict_ord_transit)
  then have  $\lfloor (p \cdot N)^R \cdot x \rfloor \leq \lfloor (p \cdot M)^R \rfloor$ 
    using Real_ZF_1_4_L9 by simp
  moreover
  from A4 T have  $p \cdot M \in \text{int}$  using int0.Int_ZF_1_1_L5
    by simp
  then have  $\lfloor (p \cdot M)^R \rfloor = p \cdot M$  using Real_ZF_1_4_L14
    by simp
  moreover from A4 A6 have  $p \cdot N = N \cdot p$  and  $p \cdot M = M \cdot p$ 
    using PositiveSet_def int0.Int_ZF_1_1_L5 by auto
  ultimately show  $\lfloor (N \cdot p)^R \cdot x \rfloor \leq M \cdot p$  by simp
qed

```

A piece of the proof of the fact that the candidate for the supremum of  $S$  is not greater than any upper bound of  $S$ , done separately for clarity (of mind).

```
lemma (in real1) Real_ZF_1_4_L27:
  assumes IsBoundedAbove(S,OrderOnReals)  S≠0 and
  h = OddExtension(int,IntegerAddition,IntegerOrder,{⟨p,Γ(S,p)⟩. p∈ℤ+})
  and p ∈ ℤ+
  shows ∃x∈S. h(p) = ⌊pR·x⌋
  using assms Real_ZF_1_4_L10 Real_ZF_1_4_L24A by auto
```

The candidate for the supremum of  $S$  is not greater than any upper bound of  $S$ .

```
lemma (in real1) Real_ZF_1_4_L28:
  assumes A1: IsBoundedAbove(S,OrderOnReals)  S≠0
  and A2: ∀x∈S. x≤y and A3:
  h = OddExtension(int,IntegerAddition,IntegerOrder,{⟨p,Γ(S,p)⟩. p∈ℤ+})
  shows [h] ≤ y
```

proof -

```
  from A1 obtain a where a∈S by auto
  with A1 A2 A3 have T: y∈ℝ  h ∈ S  [h] ∈ ℝ
    using Real_ZF_1_2_L15 Real_ZF_1_4_L22 Real_ZF_1_1_L3
    by auto
  { assume ¬([h] ≤ y)
    with T have y < [h] using Real_ZF_1_2_L28
      by blast
    then have ∃M∈int. ∃N∈ℤ+. y·NR < MR ∧ MR < [h]·NR
      using Arthan_Lemma14iii by simp
    then obtain M N where I: M∈int  N∈ℤ+ and
      II: y·NR < MR  MR < [h]·NR
      by auto
    from I have III: NR ∈ ℝ+ using int_pos_is_real_pos
      by simp
    have ∀p∈ℤ+. h(N·p) ≤ M·p
    proof
```

```
      fix p assume A4: p∈ℤ+
      with A1 A3 I have ∃x∈S. h(N·p) = ⌊(N·p)R·x⌋
```

```
    using int0.pos_int_closed_mul_unfold Real_ZF_1_4_L27
```

```
    by simp
```

```
      with A1 A2 I II A4 show h(N·p) ≤ M·p
```

```
    using Real_ZF_1_4_L26 by auto
```

```
  qed
```

```
  with T I have [h]·NR ≤ MR
```

```
    using PositiveSet_def Real_ZF_1_4_L23A
```

```
    by simp
```

```
  with T III have [h] ≤ MR·(NR)-1
```

```
    using Real_ZF_1_3_L4C by simp
```

```
  moreover from T II III have MR·(NR)-1 < [h]
```

```
    using Real_ZF_1_3_L4A by simp
```

```
  ultimately have False using Real_ZF_1_2_L29 by blast
```

```

    } then show  $[h] \leq y$  by auto
qed

```

Now we can prove that every nonempty subset of reals that is bounded above has a supremum. Proof by considering two cases: when the set has a maximum and when it does not.

```

lemma (in real1) real_order_complete:
  assumes A1: IsBoundedAbove(S, OrderOnReals)  S ≠ 0
  shows HasAmininum(OrderOnReals,  $\bigcap a \in S. \text{OrderOnReals}\{a\}$ )
proof -
  { assume HasAmaximum(OrderOnReals, S)
    with A1 have HasAmininum(OrderOnReals,  $\bigcap a \in S. \text{OrderOnReals}\{a\}$ )
      using Real_ZF_1_2_L10 IsAnOrdGroup_def IsPartOrder_def
      Order_ZF_5_L6 by simp }
  moreover
  { assume A2: ¬HasAmaximum(OrderOnReals, S)
    let h = OddExtension(int, IntegerAddition, IntegerOrder,  $\{\langle p, \Gamma(S, p) \rangle \mid p \in \mathbb{Z}_+\}$ )
    let r = OrderOnReals
    from A1 have antisym(OrderOnReals)  S ≠ 0
      using Real_ZF_1_2_L10 IsAnOrdGroup_def IsPartOrder_def by auto
    moreover from A1 A2 have  $\forall x \in S. \langle x, [h] \rangle \in r$ 
      using Real_ZF_1_4_L25 by simp
    moreover from A1 have  $\forall y. (\forall x \in S. \langle x, y \rangle \in r) \longrightarrow \langle [h], y \rangle \in r$ 
      using Real_ZF_1_4_L28 by simp
    ultimately have HasAmininum(OrderOnReals,  $\bigcap a \in S. \text{OrderOnReals}\{a\}$ )
      by (rule Order_ZF_5_L5) }
  ultimately show thesis by blast
qed

```

Finally, we are ready to formulate the main result: that the construction of real numbers from the additive group of integers results in a complete ordered field. This theorem completes the construction. It was fun.

```

theorem eudoxus_reals_are_reals: shows
  IsAmodelOfReals(RealNumbers, RealAddition, RealMultiplication, OrderOnReals)
  using real1.reals_are_ord_field real1.real_order_complete
  IsComplete_def IsAmodelOfReals_def by simp
end

```

## 41 Complex\_ZF.thy

**theory** Complex\_ZF **imports** func\_ZF\_1 OrderedField\_ZF

**begin**

The goal of this theory is to define complex numbers and prove that the Metamath complex numbers axioms hold.

### 41.1 From complete ordered fields to complex numbers

This section consists mostly of definitions and a proof context for talking about complex numbers. Suppose we have a set  $R$  with binary operations  $A$  and  $M$  and a relation  $r$  such that the quadruple  $(R, A, M, r)$  forms a complete ordered field. The next definitions take  $(R, A, M, r)$  and construct the sets that represent the structure of complex numbers: the carrier ( $\mathbb{C} = R \times R$ ), binary operations of addition and multiplication of complex numbers and the order relation on  $\mathbb{R} = R \times 0$ . The `ImCxAdd`, `ReCxAdd`, `ImCxMul`, `ReCxMul` are helper meta-functions representing the imaginary part of a sum of complex numbers, the real part of a sum of real numbers, the imaginary part of a product of complex numbers and the real part of a product of real numbers, respectively. The actual operations (subsets of  $(R \times R) \times R$  are named `CplxAdd` and `CplxMul`.

When  $R$  is an ordered field, it comes with an order relation. This induces a natural strict order relation on  $\{\langle x, 0 \rangle : x \in R\} \subseteq R \times R$ . We call the set  $\{\langle x, 0 \rangle : x \in R\}$  `ComplexReals(R,A)` and the strict order relation `CplxROrder(R,A,r)`. The order on the real axis of complex numbers is defined as the relation induced on it by the canonical projection on the first coordinate and the order we have on the real numbers. OK, lets repeat this slower. We start with the order relation  $r$  on a (model of) real numbers  $R$ . We want to define an order relation on a subset of complex numbers, namely on  $R \times \{0\}$ . To do that we use the notion of a relation induced by a mapping. The mapping here is  $f : R \times \{0\} \rightarrow R, f\langle x, 0 \rangle = x$  which is defined under a name of `SliceProjection` in `func_ZF.thy`. This defines a relation  $r_1$  (called `InducedRelation(f,r)`, see `func_ZF`) on  $R \times \{0\}$  such that  $\langle \langle x, 0 \rangle, \langle y, 0 \rangle \in r_1$  iff  $\langle x, y \rangle \in r$ . This way we get what we call `CplxROrder(R,A,r)`. However, this is not the end of the story, because Metamath uses strict inequalities in its axioms, rather than weak ones like `IsarMathLib` (mostly). So we need to take the strict version of this order relation. This is done in the syntax definition of  $<_{\mathbb{R}}$  in the definition of `complex0` context. Since Metamath proves a lot of theorems about the real numbers extended with  $+\infty$  and  $-\infty$ , we define the notation for inequalities on the extended real line as well.

A helper expression representing the real part of the sum of two complex numbers.

**definition**

$$\text{ReCxAdd}(R, A, a, b) \equiv A(\text{fst}(a), \text{fst}(b))$$

An expression representing the imaginary part of the sum of two complex numbers.

**definition**

$$\text{ImCxAdd}(R, A, a, b) \equiv A(\text{snd}(a), \text{snd}(b))$$

The set (function) that is the binary operation that adds complex numbers.

**definition**

$$\begin{aligned} \text{CplxAdd}(R, A) \equiv \\ \{ \langle p, \langle \text{ReCxAdd}(R, A, \text{fst}(p), \text{snd}(p)), \text{ImCxAdd}(R, A, \text{fst}(p), \text{snd}(p)) \rangle \rangle \mid \\ p \in (R \times R) \times (R \times R) \} \end{aligned}$$

The expression representing the imaginary part of the product of complex numbers.

**definition**

$$\text{ImCxMul}(R, A, M, a, b) \equiv A(M(\text{fst}(a), \text{snd}(b)), M(\text{snd}(a), \text{fst}(b)))$$

The expression representing the real part of the product of complex numbers.

**definition**

$$\begin{aligned} \text{ReCxMul}(R, A, M, a, b) \equiv \\ A(M(\text{fst}(a), \text{fst}(b)), \text{GroupInv}(R, A)(M(\text{snd}(a), \text{snd}(b)))) \end{aligned}$$

The function (set) that represents the binary operation of multiplication of complex numbers.

**definition**

$$\begin{aligned} \text{CplxMul}(R, A, M) \equiv \\ \{ \langle p, \langle \text{ReCxMul}(R, A, M, \text{fst}(p), \text{snd}(p)), \text{ImCxMul}(R, A, M, \text{fst}(p), \text{snd}(p)) \rangle \rangle \mid \\ p \in (R \times R) \times (R \times R) \} \end{aligned}$$

The definition real numbers embedded in the complex plane.

**definition**

$$\text{ComplexReals}(R, A) \equiv R \times \{\text{TheNeutralElement}(R, A)\}$$

Definition of order relation on the real line.

**definition**

$$\begin{aligned} \text{CplxROrder}(R, A, r) \equiv \\ \text{InducedRelation}(\text{SliceProjection}(\text{ComplexReals}(R, A)), r) \end{aligned}$$

The next locale defines proof context and notation that will be used for complex numbers.

**locale** complex0 =

**fixes** R and A and M and r

**assumes** R\_are\_reals: IsAmodelOfReals(R, A, M, r)

```

fixes complex ( $\mathbb{C}$ )
defines complex_def[simp]:  $\mathbb{C} \equiv \mathbb{R} \times \mathbb{R}$ 

fixes rone ( $1_R$ )
defines rone_def[simp]:  $1_R \equiv \text{TheNeutralElement}(\mathbb{R}, \mathbb{M})$ 

fixes rzero ( $0_R$ )
defines rzero_def[simp]:  $0_R \equiv \text{TheNeutralElement}(\mathbb{R}, \mathbb{A})$ 

fixes one (1)
defines one_def[simp]:  $1 \equiv \langle 1_R, 0_R \rangle$ 

fixes zero (0)
defines zero_def[simp]:  $0 \equiv \langle 0_R, 0_R \rangle$ 

fixes iunit (i)
defines iunit_def[simp]:  $i \equiv \langle 0_R, 1_R \rangle$ 

fixes creal ( $\mathbb{R}$ )
defines creal_def[simp]:  $\mathbb{R} \equiv \{ \langle r, 0_R \rangle . r \in \mathbb{R} \}$ 

fixes rmul (infixl  $\cdot$  71)
defines rmul_def[simp]:  $a \cdot b \equiv M\langle a, b \rangle$ 

fixes radd (infixl  $+$  69)
defines radd_def[simp]:  $a + b \equiv A\langle a, b \rangle$ 

fixes rneg ( $-$  _ 70)
defines rneg_def[simp]:  $- a \equiv \text{GroupInv}(\mathbb{R}, \mathbb{A})(a)$ 

fixes ca (infixl  $+$  69)
defines ca_def[simp]:  $a + b \equiv \text{CplxAdd}(\mathbb{R}, \mathbb{A})\langle a, b \rangle$ 

fixes cm (infixl  $\cdot$  71)
defines cm_def[simp]:  $a \cdot b \equiv \text{CplxMul}(\mathbb{R}, \mathbb{A}, \mathbb{M})\langle a, b \rangle$ 

fixes cdiv (infixl  $/$  70)
defines cdiv_def[simp]:  $a / b \equiv \bigcup \{ x \in \mathbb{C} . b \cdot x = a \}$ 

fixes sub (infixl  $-$  69)
defines sub_def[simp]:  $a - b \equiv \bigcup \{ x \in \mathbb{C} . b + x = a \}$ 

fixes cneg ( $-$  _ 95)
defines cneg_def[simp]:  $- a \equiv 0 - a$ 

fixes lessr (infix  $<_{\mathbb{R}}$  68)
defines lessr_def[simp]:
 $a <_{\mathbb{R}} b \equiv \langle a, b \rangle \in \text{StrictVersion}(\text{CplxROrder}(\mathbb{R}, \mathbb{A}, r))$ 

```

```

fixes cpnf (+∞)
defines cpnf_def[simp]: +∞ ≡ ℂ

fixes cmnf (−∞)
defines cmnf_def[simp]: −∞ ≡ {ℂ}

fixes cxr (ℝ*)
defines cxr_def[simp]: ℝ* ≡ ℝ ∪ {+∞, −∞}

fixes cxn (ℕ)
defines cxn_def[simp]:
ℕ ≡ ⋂ {N ∈ Pow(ℝ). 1 ∈ N ∧ (∀n. n ∈ N ⟶ n+1 ∈ N)}

fixes cltrrset (<)
defines cltrrset_def[simp]:
< ≡ StrictVersion(CplxROrder(R,A,r)) ∩ ℝ×ℝ ∪
{⟨−∞, +∞⟩} ∪ (ℝ×{+∞}) ∪ ({−∞}×ℝ)

fixes cltrr (infix < 68)
defines cltrr_def[simp]: a < b ≡ ⟨a,b⟩ ∈ <

fixes lsq (infix ≤ 68)
defines lsq_def[simp]: a ≤ b ≡ ¬ (b < a)

fixes two (2)
defines two_def[simp]: 2 ≡ 1 + 1

fixes three (3)
defines three_def[simp]: 3 ≡ 2+1

fixes four (4)
defines four_def[simp]: 4 ≡ 3+1

fixes five (5)
defines five_def[simp]: 5 ≡ 4+1

fixes six (6)
defines six_def[simp]: 6 ≡ 5+1

fixes seven (7)
defines seven_def[simp]: 7 ≡ 6+1

fixes eight (8)
defines eight_def[simp]: 8 ≡ 7+1

fixes nine (9)
defines nine_def[simp]: 9 ≡ 8+1

```



## 41.2 Axioms of complex numbers

In this section we will prove that all Metamath's axioms of complex numbers hold in the `complex0` context.

The next lemma lists some contexts that are valid in the `complex0` context.

```
lemma (in complex0) valid_cntxts: shows
  field1(R,A,M,r)
  field0(R,A,M)
  ring1(R,A,M,r)
  group3(R,A,r)
  ring0(R,A,M)
  M {is commutative on} R
  group0(R,A)
proof -
  from R_are_reals have I: IsAnOrdField(R,A,M,r)
    using IsAmodelOfReals_def by simp
  then show field1(R,A,M,r) using OrdField_ZF_1_L2 by simp
  then show ring1(R,A,M,r) and I: field0(R,A,M)
    using field1.axioms ring1_def field1.OrdField_ZF_1_L1B
    by auto
  then show group3(R,A,r) using ring1.OrdRing_ZF_1_L4
    by simp
  from I have IsAfield(R,A,M) using field0.Field_ZF_1_L1
    by simp
  then have IsARing(R,A,M) and M {is commutative on} R
    using IsAfield_def by auto
  then show ring0(R,A,M) and M {is commutative on} R
    using ring0_def by auto
  then show group0(R,A) using ring0.Ring_ZF_1_L1
    by simp
qed
```

The next lemma shows the definition of real and imaginary part of complex sum and product in a more readable form using notation defined in `complex0` locale.

```
lemma (in complex0) cplx_mul_add_defs: shows
  ReCxAdd(R,A,<a,b>,<c,d>) = a + c
  ImCxAdd(R,A,<a,b>,<c,d>) = b + d
  ImCxMul(R,A,M,<a,b>,<c,d>) = a·d + b·c
  ReCxMul(R,A,M,<a,b>,<c,d>) = a·c + (-b·d)
proof -
  let z1 = <a,b>
  let z2 = <c,d>
  have ReCxAdd(R,A,z1,z2) ≡ A(fst(z1),fst(z2))
    by (rule ReCxAdd_def)
  moreover have ImCxAdd(R,A,z1,z2) ≡ A(snd(z1),snd(z2))
    by (rule ImCxAdd_def)
  moreover have
```

```

    ImCxMul(R,A,M,z1,z2) ≡ A⟨M⟨fst(z1),snd(z2)⟩,M⟨snd(z1),fst(z2)⟩⟩
  by (rule ImCxMul_def)
moreover have
  ReCxMul(R,A,M,z1,z2) ≡
  A⟨M⟨fst(z1),fst(z2)⟩,GroupInv(R,A)(M⟨snd(z1),snd(z2)⟩)⟩
  by (rule ReCxMul_def)
ultimately show
  ReCxAdd(R,A,z1,z2) = a + c
  ImCxAdd(R,A,⟨a,b⟩,⟨c,d⟩) = b + d
  ImCxMul(R,A,M,⟨a,b⟩,⟨c,d⟩) = a·d + b·c
  ReCxMul(R,A,M,⟨a,b⟩,⟨c,d⟩) = a·c + (-b·d)
  by auto
qed

```

Real and imaginary parts of sums and products of complex numbers are real.

```

lemma (in complex0) cplx_mul_add_types:
  assumes A1: z1 ∈ ℂ    z2 ∈ ℂ
  shows
    ReCxAdd(R,A,z1,z2) ∈ ℝ
    ImCxAdd(R,A,z1,z2) ∈ ℝ
    ImCxMul(R,A,M,z1,z2) ∈ ℝ
    ReCxMul(R,A,M,z1,z2) ∈ ℝ
proof -
  let a = fst(z1)
  let b = snd(z1)
  let c = fst(z2)
  let d = snd(z2)
  from A1 have a ∈ ℝ  b ∈ ℝ  c ∈ ℝ  d ∈ ℝ
  by auto
  then have
    a + c ∈ ℝ
    b + d ∈ ℝ
    a·d + b·c ∈ ℝ
    a·c + (- b·d) ∈ ℝ
  using valid_cntxts ring0.Ring_ZF_1_L4 by auto
  with A1 show
    ReCxAdd(R,A,z1,z2) ∈ ℝ
    ImCxAdd(R,A,z1,z2) ∈ ℝ
    ImCxMul(R,A,M,z1,z2) ∈ ℝ
    ReCxMul(R,A,M,z1,z2) ∈ ℝ
  using cplx_mul_add_defs by auto
qed

```

Complex reals are complex. Recall the definition of  $\mathbb{R}$  in the `complex0` locale.

```

lemma (in complex0) axresscn: shows ℝ ⊆ ℂ
  using valid_cntxts group0.group0_2_L2 by auto

```

Complex 1 is not complex 0.

```

lemma (in complex0) ax1ne0: shows 1  $\neq$  0
proof -
  have IsAfield(R,A,M) using valid_cntxts field0.Field_ZF_1_L1
    by simp
  then show 1  $\neq$  0 using IsAfield_def by auto
qed

```

Complex addition is a complex valued binary operation on complex numbers.

```

lemma (in complex0) axaddopr: shows CplxAdd(R,A):  $\mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}$ 
proof -
  have  $\forall p \in \mathbb{C} \times \mathbb{C}.$ 
     $\langle \text{ReCxAdd}(R,A,\text{fst}(p),\text{snd}(p)), \text{ImCxAdd}(R,A,\text{fst}(p),\text{snd}(p)) \rangle \in \mathbb{C}$ 
    using cplx_mul_add_types by simp
  then have
     $\{ \langle p, \langle \text{ReCxAdd}(R,A,\text{fst}(p),\text{snd}(p)), \text{ImCxAdd}(R,A,\text{fst}(p),\text{snd}(p)) \rangle \rangle \mid$ 
     $p \in \mathbb{C} \times \mathbb{C} \} : \mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}$ 
    by (rule ZF_fun_from_total)
  then show CplxAdd(R,A):  $\mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}$  using CplxAdd_def by simp
qed

```

Complex multiplication is a complex valued binary operation on complex numbers.

```

lemma (in complex0) axmulopr: shows CplxMul(R,A,M):  $\mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}$ 
proof -
  have  $\forall p \in \mathbb{C} \times \mathbb{C}.$ 
     $\langle \text{ReCxMul}(R,A,M,\text{fst}(p),\text{snd}(p)), \text{ImCxMul}(R,A,M,\text{fst}(p),\text{snd}(p)) \rangle \in \mathbb{C}$ 
    using cplx_mul_add_types by simp
  then have
     $\{ \langle p, \langle \text{ReCxMul}(R,A,M,\text{fst}(p),\text{snd}(p)), \text{ImCxMul}(R,A,M,\text{fst}(p),\text{snd}(p)) \rangle \rangle \mid$ 
     $p \in \mathbb{C} \times \mathbb{C} \} : \mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}$  by (rule ZF_fun_from_total)
  then show CplxMul(R,A,M):  $\mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}$  using CplxMul_def by simp
qed

```

What are the values of omplex addition and multiplication in terms of their real and imaginary parts?

```

lemma (in complex0) cplx_mul_add_vals:
  assumes A1: a $\in$ R b $\in$ R c $\in$ R d $\in$ R
  shows
     $\langle a,b \rangle + \langle c,d \rangle = \langle a + c, b + d \rangle$ 
     $\langle a,b \rangle \cdot \langle c,d \rangle = \langle a \cdot c + (-b \cdot d), a \cdot d + b \cdot c \rangle$ 
proof -
  let S = CplxAdd(R,A)
  let P = CplxMul(R,A,M)
  let p =  $\langle \langle a,b \rangle, \langle c,d \rangle \rangle$ 
  from A1 have S :  $\mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}$  and p  $\in \mathbb{C} \times \mathbb{C}$ 
    using axaddopr by auto
  moreover have
    S =  $\{ \langle p, \langle \text{ReCxAdd}(R,A,\text{fst}(p),\text{snd}(p)), \text{ImCxAdd}(R,A,\text{fst}(p),\text{snd}(p)) \rangle \rangle \mid$ 

```

```

    p ∈ ℂ × ℂ}
    using CplxAdd_def by simp
ultimately have S(p) = ⟨ReCxAdd(R,A,fst(p),snd(p)),ImCxAdd(R,A,fst(p),snd(p))⟩
  by (rule ZF_fun_from_tot_val)
then show ⟨a,b⟩ + ⟨c,d⟩ = ⟨a + c, b + d⟩
  using cplx_mul_add_defs by simp
from A1 have P : ℂ × ℂ → ℂ and p ∈ ℂ × ℂ
  using axmulopr by auto
moreover have
  P = {⟨p, ⟨ReCxMul(R,A,M,fst(p),snd(p)),ImCxMul(R,A,M,fst(p),snd(p))⟩
}.
  p ∈ ℂ × ℂ}
  using CplxMul_def by simp
ultimately have
  P(p) = ⟨ReCxMul(R,A,M,fst(p),snd(p)),ImCxMul(R,A,M,fst(p),snd(p))⟩
  by (rule ZF_fun_from_tot_val)
then show ⟨a,b⟩ · ⟨c,d⟩ = ⟨a·c + (-b·d), a·d + b·c⟩
  using cplx_mul_add_defs by simp
qed

```

Complex multiplication is commutative.

```

lemma (in complex0) axmulcom: assumes A1: a ∈ ℂ  b ∈ ℂ
  shows a·b = b·a
  using assms cplx_mul_add_vals valid_cntxts ring0.Ring_ZF_1_L4
    field0.field_mult_comm by auto

```

A sum of complex numbers is complex.

```

lemma (in complex0) axaddcl: assumes a ∈ ℂ  b ∈ ℂ
  shows a+b ∈ ℂ
  using assms axaddopr apply_funtype by simp

```

A product of complex numbers is complex.

```

lemma (in complex0) axmulcl: assumes a ∈ ℂ  b ∈ ℂ
  shows a·b ∈ ℂ
  using assms axmulopr apply_funtype by simp

```

Multiplication is distributive with respect to addition.

```

lemma (in complex0) axdistr:
  assumes A1: a ∈ ℂ  b ∈ ℂ  c ∈ ℂ
  shows a·(b + c) = a·b + a·c
proof -
  let ar = fst(a)
  let ai = snd(a)
  let br = fst(b)
  let bi = snd(b)
  let cr = fst(c)
  let ci = snd(c)
  from A1 have T:

```

```

  ar ∈ R  ai ∈ R  br ∈ R  bi ∈ R  cr ∈ R  ci ∈ R
  br+cr ∈ R  bi+ci ∈ R
  ar·br + (-ai·bi) ∈ R
  ar·cr + (-ai·ci) ∈ R
  ar·bi + ai·br ∈ R
  ar·ci + ai·cr ∈ R
  using valid_cntxts ring0.Ring_ZF_1_L4 by auto
with A1 have a·(b + c) =
  ⟨ar·(br+cr) + (-ai·(bi+ci)), ar·(bi+ci) + ai·(br+cr)⟩
  using cplx_mul_add_vals by auto
moreover from T have
  ar·(br+cr) + (-ai·(bi+ci)) =
  ar·br + (-ai·bi) + (ar·cr + (-ai·ci))
  and
  ar·(bi+ci) + ai·(br+cr) =
  ar·bi + ai·br + (ar·ci + ai·cr)
  using valid_cntxts ring0.Ring_ZF_2_L6 by auto
moreover from A1 T have
  ⟨ar·br + (-ai·bi) + (ar·cr + (-ai·ci)),
  ar·bi + ai·br + (ar·ci + ai·cr)⟩ =
  a·b + a·c
  using cplx_mul_add_vals by auto
ultimately show a·(b + c) = a·b + a·c
  by simp
qed

```

Complex addition is commutative.

```

lemma (in complex0) axaddcom: assumes a ∈ ℂ  b ∈ ℂ
  shows a+b = b+a
  using assms cplx_mul_add_vals valid_cntxts ring0.Ring_ZF_1_L4
  by auto

```

Complex addition is associative.

```

lemma (in complex0) axaddass: assumes A1: a ∈ ℂ  b ∈ ℂ  c ∈ ℂ
  shows a + b + c = a + (b + c)
proof -
  let ar = fst(a)
  let ai = snd(a)
  let br = fst(b)
  let bi = snd(b)
  let cr = fst(c)
  let ci = snd(c)
  from A1 have T:
    ar ∈ R  ai ∈ R  br ∈ R  bi ∈ R  cr ∈ R  ci ∈ R
    ar+br ∈ R  ai+bi ∈ R
    br+cr ∈ R  bi+ci ∈ R
    using valid_cntxts ring0.Ring_ZF_1_L4 by auto
  with A1 have a + b + c = ⟨ar+br+cr, ai+bi+ci⟩
    using cplx_mul_add_vals by auto

```

```

also from A1 T have ... = a + (b + c)
  using valid_cntxts ring0.Ring_ZF_1_L11 cplx_mul_add_vals
  by auto
finally show a + b + c = a + (b + c)
  by simp
qed

```

Complex multiplication is associative.

```

lemma (in complex0) axmulass: assumes A1: a ∈ ℂ  b ∈ ℂ  c ∈ ℂ
  shows a · b · c = a · (b · c)
proof -
  let ar = fst(a)
  let ai = snd(a)
  let br = fst(b)
  let bi = snd(b)
  let cr = fst(c)
  let ci = snd(c)
  from A1 have T:
    ar ∈ ℝ  ai ∈ ℝ  br ∈ ℝ  bi ∈ ℝ  cr ∈ ℝ  ci ∈ ℝ
    ar·br + (-ai·bi) ∈ ℝ
    ar·bi + ai·br ∈ ℝ
    br·cr + (-bi·ci) ∈ ℝ
    br·ci + bi·cr ∈ ℝ
    using valid_cntxts ring0.Ring_ZF_1_L4  by auto
  with A1 have a · b · c =
    ⟨(ar·br + (-ai·bi))·cr + (-(ar·bi + ai·br)·ci),
    (ar·br + (-ai·bi))·ci + (ar·bi + ai·br)·cr⟩
    using cplx_mul_add_vals by auto
  moreover from A1 T have
    ⟨ar·(br·cr + (-bi·ci)) + (-ai·(br·ci + bi·cr)),
    ar·(br·ci + bi·cr) + ai·(br·cr + (-bi·ci))⟩ =
    a · (b · c)
    using cplx_mul_add_vals by auto
  moreover from T have
    ar·(br·cr + (-bi·ci)) + (-ai·(br·ci + bi·cr)) =
    (ar·br + (-ai·bi))·cr + (-(ar·bi + ai·br)·ci)
    and
    ar·(br·ci + bi·cr) + ai·(br·cr + (-bi·ci)) =
    (ar·br + (-ai·bi))·ci + (ar·bi + ai·br)·cr
    using valid_cntxts ring0.Ring_ZF_2_L6 by auto
  ultimately show a · b · c = a · (b · c)
    by auto
qed

```

Complex 1 is real. This really means that the pair  $\langle 1, 0 \rangle$  is on the real axis.

```

lemma (in complex0) ax1re: shows 1 ∈ ℝ
  using valid_cntxts ring0.Ring_ZF_1_L2 by simp

```

The imaginary unit is a "square root" of  $-1$  (that is,  $i^2 + 1 = 0$ ).

```

lemma (in complex0) axi2m1: shows i·i + 1 = 0
  using valid_cntxts ring0.Ring_ZF_1_L2 ring0.Ring_ZF_1_L3
  cplx_mul_add_vals ring0.Ring_ZF_1_L6 group0.group0_2_L6
  by simp

```

0 is the neutral element of complex addition.

```

lemma (in complex0) ax0id: assumes a ∈ ℂ
  shows a + 0 = a
  using assms cplx_mul_add_vals valid_cntxts
  ring0.Ring_ZF_1_L2 ring0.Ring_ZF_1_L3
  by auto

```

The imaginary unit is a complex number.

```

lemma (in complex0) axicn: shows i ∈ ℂ
  using valid_cntxts ring0.Ring_ZF_1_L2 by auto

```

All complex numbers have additive inverses.

```

lemma (in complex0) axnegex: assumes A1: a ∈ ℂ
  shows ∃x∈ℂ. a + x = 0
proof -
  let ar = fst(a)
  let ai = snd(a)
  let x = ⟨-ar, -ai⟩
  from A1 have T:
    ar ∈ R    ai ∈ R    (-ar) ∈ R    (-ai) ∈ R
    using valid_cntxts ring0.Ring_ZF_1_L3 by auto
  then have x ∈ ℂ using valid_cntxts ring0.Ring_ZF_1_L3
    by auto
  moreover from A1 T have a + x = 0
    using cplx_mul_add_vals valid_cntxts ring0.Ring_ZF_1_L3
    by auto
  ultimately show ∃x∈ℂ. a + x = 0
    by auto

```

qed

A non-zero complex number has a multiplicative inverse.

```

lemma (in complex0) axrecex: assumes A1: a ∈ ℂ and A2: a ≠ 0
  shows ∃x∈ℂ. a·x = 1
proof -
  let ar = fst(a)
  let ai = snd(a)
  let m = ar·ar + ai·ai
  from A1 have T1: ar ∈ R    ai ∈ R by auto
  moreover from A1 A2 have ar ≠ 0R ∨ ai ≠ 0R
    by auto
  ultimately have ∃c∈R. m·c = 1R
    using valid_cntxts field1.OzdField_ZF_1_L10
    by auto

```

```

then obtain c where I:  $c \in \mathbb{R}$  and II:  $m \cdot c = 1_R$ 
  by auto
let x =  $\langle a_r \cdot c, -a_i \cdot c \rangle$ 
from T1 I have T2:  $a_r \cdot c \in \mathbb{R} \quad (-a_i \cdot c) \in \mathbb{R}$ 
  using valid_cntxts ring0.Ring_ZF_1_L4 ring0.Ring_ZF_1_L3
  by auto
then have  $x \in \mathbb{C}$  by auto
moreover from A1 T1 T2 I II have  $a \cdot x = 1$ 
  using cplx_mul_add_vals valid_cntxts ring0.ring_rearr_3_elemA
  by auto
ultimately show  $\exists x \in \mathbb{C}. a \cdot x = 1$  by auto
qed

```

Complex 1 is a right neutral element for multiplication.

```

lemma (in complex0) ax1id: assumes A1:  $a \in \mathbb{C}$ 
  shows  $a \cdot 1 = a$ 
  using assms valid_cntxts ring0.Ring_ZF_1_L2 cplx_mul_add_vals
  ring0.Ring_ZF_1_L3 ring0.Ring_ZF_1_L6 by auto

```

A formula for sum of (complex) real numbers.

```

lemma (in complex0) sum_of_reals: assumes  $a \in \mathbb{R} \quad b \in \mathbb{R}$ 
  shows
 $a + b = \langle \text{fst}(a) + \text{fst}(b), 0_R \rangle$ 
  using assms valid_cntxts ring0.Ring_ZF_1_L2 cplx_mul_add_vals
  ring0.Ring_ZF_1_L3 by auto

```

The sum of real numbers is real.

```

lemma (in complex0) axaddrcl: assumes A1:  $a \in \mathbb{R} \quad b \in \mathbb{R}$ 
  shows  $a + b \in \mathbb{R}$ 
  using assms sum_of_reals valid_cntxts ring0.Ring_ZF_1_L4
  by auto

```

The formula for the product of (complex) real numbers.

```

lemma (in complex0) prod_of_reals: assumes A1:  $a \in \mathbb{R} \quad b \in \mathbb{R}$ 
  shows  $a \cdot b = \langle \text{fst}(a) \cdot \text{fst}(b), 0_R \rangle$ 
proof -
  let  $a_r = \text{fst}(a)$ 
  let  $b_r = \text{fst}(b)$ 
  from A1 have T:
 $a_r \in \mathbb{R} \quad b_r \in \mathbb{R} \quad 0_R \in \mathbb{R} \quad a_r \cdot b_r \in \mathbb{R}$ 
  using valid_cntxts ring0.Ring_ZF_1_L2 ring0.Ring_ZF_1_L4
  by auto
  with A1 show  $a \cdot b = \langle a_r \cdot b_r, 0_R \rangle$ 
  using cplx_mul_add_vals valid_cntxts ring0.Ring_ZF_1_L2
  ring0.Ring_ZF_1_L6 ring0.Ring_ZF_1_L3 by auto
qed

```

The product of (complex) real numbers is real.



```

lemma (in complex0) axmulrcl: assumes a $\in\mathbb{R}$  b $\in\mathbb{R}$ 
  shows a  $\cdot$  b  $\in \mathbb{R}$ 
  using assms prod_of_reals valid_cntxts ring0.Ring_ZF_1_L4
  by auto

```

The existence of a real negative of a real number.

```

lemma (in complex0) axrnegex: assumes A1: a $\in\mathbb{R}$ 
  shows  $\exists x \in \mathbb{R}. a + x = 0$ 
proof -
  let ar = fst(a)
  let x =  $\langle -a_r, 0_R \rangle$ 
  from A1 have T:
    ar  $\in \mathbb{R}$   $(-a_r) \in \mathbb{R}$  0R  $\in \mathbb{R}$ 
    using valid_cntxts ring0.Ring_ZF_1_L3 ring0.Ring_ZF_1_L2
    by auto
  then have x $\in \mathbb{R}$  by auto
  moreover from A1 T have a + x = 0
    using cplx_mul_add_vals valid_cntxts ring0.Ring_ZF_1_L3
    by auto
  ultimately show  $\exists x \in \mathbb{R}. a + x = 0$  by auto
qed

```

Each nonzero real number has a real inverse

```

lemma (in complex0) axrrecex:
  assumes A1: a  $\in \mathbb{R}$  a  $\neq 0$ 
  shows  $\exists x \in \mathbb{R}. a \cdot x = 1$ 
proof -
  let R0 =  $\mathbb{R} - \{0_R\}$ 
  let ar = fst(a)
  let y = GroupInv(R0, restrict(M, R0  $\times$  R0))(ar)
  from A1 have T:  $\langle y, 0_R \rangle \in \mathbb{R}$  using valid_cntxts field0.Field_ZF_1_L5
  by auto
  moreover from A1 T have a  $\cdot \langle y, 0_R \rangle = 1$ 
    using prod_of_reals valid_cntxts
    field0.Field_ZF_1_L5 field0.Field_ZF_1_L6 by auto
  ultimately show  $\exists x \in \mathbb{R}. a \cdot x = 1$  by auto
qed

```

Our  $\mathbb{R}$  symbol is the real axis on the complex plane.

```

lemma (in complex0) real_means_real_axis: shows  $\mathbb{R} = \text{ComplexReals}(R, A)$ 
  using ComplexReals_def by auto

```

The CplxROrder thing is a relation on the complex reals.

```

lemma (in complex0) cplx_ord_on_cplx_reals:
  shows CplxROrder(R, A, r)  $\subseteq \mathbb{R} \times \mathbb{R}$ 
  using ComplexReals_def slice_proj_bij real_means_real_axis
  CplxROrder_def InducedRelation_def by auto

```

The strict version of the complex relation is a relation on complex reals.

```

lemma (in complex0) cplx_strict_ord_on_cplx_reals:
  shows StrictVersion(CplxROrder(R,A,r))  $\subseteq$   $\mathbb{R} \times \mathbb{R}$ 
  using cplx_ord_on_cplx_reals strict_ver_rel by simp

```

The CplxROrder thing is a relation on the complex reals. Here this is formulated as a statement that in complex0 context  $a < b$  implies that  $a, b$  are complex reals

```

lemma (in complex0) strict_cplx_ord_type: assumes  $a <_{\mathbb{R}} b$ 
  shows  $a \in \mathbb{R}$   $b \in \mathbb{R}$ 
  using assms CplxROrder_def def_of_strict_ver InducedRelation_def
    slice_proj_bij ComplexReals_def real_means_real_axis
  by auto

```

A more readable version of the definition of the strict order relation on the real axis. Recall that in the complex0 context  $r$  denotes the (non-strict) order relation on the underlying model of real numbers.

```

lemma (in complex0) def_of_real_axis_order: shows
   $\langle x, 0_R \rangle <_{\mathbb{R}} \langle y, 0_R \rangle \longleftrightarrow \langle x, y \rangle \in r \wedge x \neq y$ 
proof
  let f = SliceProjection(ComplexReals(R,A))
  assume A1:  $\langle x, 0_R \rangle <_{\mathbb{R}} \langle y, 0_R \rangle$ 
  then have  $\langle f\langle x, 0_R \rangle, f\langle y, 0_R \rangle \rangle \in r \wedge x \neq y$ 
    using CplxROrder_def def_of_strict_ver def_of_ind_relA
    by simp
  moreover from A1 have  $\langle x, 0_R \rangle \in \mathbb{R}$   $\langle y, 0_R \rangle \in \mathbb{R}$ 
    using strict_cplx_ord_type by auto
  ultimately show  $\langle x, y \rangle \in r \wedge x \neq y$ 
    using slice_proj_bij ComplexReals_def by simp
next assume A1:  $\langle x, y \rangle \in r \wedge x \neq y$ 
  let f = SliceProjection(ComplexReals(R,A))
  have f :  $\mathbb{R} \rightarrow \mathbb{R}$ 
    using ComplexReals_def slice_proj_bij real_means_real_axis
    by simp
  moreover from A1 have T:  $\langle x, 0_R \rangle \in \mathbb{R}$   $\langle y, 0_R \rangle \in \mathbb{R}$ 
    using valid_cntxts ring1.OrdRing_ZF_1_L3 by auto
  moreover from A1 T have  $\langle f\langle x, 0_R \rangle, f\langle y, 0_R \rangle \rangle \in r$ 
    using slice_proj_bij ComplexReals_def by simp
  ultimately have  $\langle \langle x, 0_R \rangle, \langle y, 0_R \rangle \rangle \in \text{InducedRelation}(f,r)$ 
    using def_of_ind_relB by simp
  with A1 show  $\langle x, 0_R \rangle <_{\mathbb{R}} \langle y, 0_R \rangle$ 
    using CplxROrder_def def_of_strict_ver
    by simp
qed

```

The (non strict) order on complex reals is antisymmetric, transitive and total.

```

lemma (in complex0) cplx_ord_antsym_trans_tot: shows
  antisym(CplxROrder(R,A,r))

```

```

trans(CplxROrder(R,A,r))
CplxROrder(R,A,r) {is total on}  $\mathbb{R}$ 
proof -
  let f = SliceProjection(ComplexReals(R,A))
  have f  $\in$  ord_iso( $\mathbb{R}$ ,CplxROrder(R,A,r),R,r)
    using ComplexReals_def slice_proj_bij real_means_real_axis
    bij_is_ord_iso CplxROrder_def by simp
  moreover have CplxROrder(R,A,r)  $\subseteq \mathbb{R} \times \mathbb{R}$ 
    using cplx_ord_on_cplx_reals by simp
  moreover have I:
    antisym(r)  r {is total on} R  trans(r)
    using valid_cntxts ring1.OrdRing_ZF_1_L1 IsAnOrdRing_def
    IsLinOrder_def by auto
  ultimately show
    antisym(CplxROrder(R,A,r))
    trans(CplxROrder(R,A,r))
    CplxROrder(R,A,r) {is total on}  $\mathbb{R}$ 
    using ord_iso_pres_antisym ord_iso_pres_tot ord_iso_pres_trans
    by auto
qed

```

The trichotomy law for the strict order on the complex reals.

```

lemma (in complex0) cplx_strict_ord_trich:
  assumes a  $\in \mathbb{R}$   b  $\in \mathbb{R}$ 
  shows Exactly_1_of_3_holds(a< $_{\mathbb{R}}$ b, a=b, b< $_{\mathbb{R}}$ a)
  using assms cplx_ord_antisym_trans_tot strict_ans_tot_trich
  by simp

```

The strict order on the complex reals is kind of antisymmetric.

```

lemma (in complex0) pre_axlttri: assumes A1: a  $\in \mathbb{R}$   b  $\in \mathbb{R}$ 
  shows a < $_{\mathbb{R}}$  b  $\longleftrightarrow \neg(a=b \vee b <_{\mathbb{R}} a)$ 
proof -
  from A1 have Exactly_1_of_3_holds(a< $_{\mathbb{R}}$ b, a=b, b< $_{\mathbb{R}}$ a)
    by (rule cplx_strict_ord_trich)
  then show a < $_{\mathbb{R}}$  b  $\longleftrightarrow \neg(a=b \vee b <_{\mathbb{R}} a)$ 
    by (rule Fol1_L8A)
qed

```

The strict order on complex reals is transitive.

```

lemma (in complex0) cplx_strict_ord_trans:
  shows trans(StrictVersion(CplxROrder(R,A,r)))
  using cplx_ord_antisym_trans_tot strict_of_transB by simp

```

The strict order on complex reals is transitive - the explicit version of cplx\_strict\_ord\_trans.

```

lemma (in complex0) pre_axlttrn:
  assumes A1: a < $_{\mathbb{R}}$  b  b < $_{\mathbb{R}}$  c
  shows a < $_{\mathbb{R}}$  c

```

```

proof -
  let s = StrictVersion(CplxROrder(R,A,r))
  from A1 have
    trans(s)  $\langle a,b \rangle \in s \wedge \langle b,c \rangle \in s$ 
    using cplx_strict_ord_trans by auto
  then have  $\langle a,c \rangle \in s$  by (rule Fol1_L3)
  then show  $a <_{\mathbb{R}} c$  by simp
qed

```

The strict order on complex reals is preserved by translations.

```

lemma (in complex0) pre_axltadd:
  assumes A1:  $a <_{\mathbb{R}} b$  and A2:  $c \in \mathbb{R}$ 
  shows  $c+a <_{\mathbb{R}} c+b$ 
proof -
  from A1 have T:  $a \in \mathbb{R} \quad b \in \mathbb{R}$  using strict_cplx_ord_type
  by auto
  with A1 A2 show  $c+a <_{\mathbb{R}} c+b$ 
  using def_of_real_axis_order valid_cntxts
    group3.group_strict_ord_transl_inv sum_of_reals
  by auto
qed

```

The set of positive complex reals is closed with respect to multiplication.

```

lemma (in complex0) pre_axmulgt0: assumes A1:  $0 <_{\mathbb{R}} a$   $0 <_{\mathbb{R}} b$ 
  shows  $0 <_{\mathbb{R}} a \cdot b$ 
proof -
  from A1 have T:  $a \in \mathbb{R} \quad b \in \mathbb{R}$  using strict_cplx_ord_type
  by auto
  with A1 show  $0 <_{\mathbb{R}} a \cdot b$ 
  using def_of_real_axis_order valid_cntxts field1.pos_mul_closed
    def_of_real_axis_order prod_of_reals
  by auto
qed

```

The order on complex reals is linear and complete.

```

lemma (in complex0) cmplx_reals_ord_lin_compl: shows
  CplxROrder(R,A,r) {is complete}
  IsLinOrder( $\mathbb{R}$ ,CplxROrder(R,A,r))
proof -
  have SliceProjection( $\mathbb{R}$ )  $\in$  bij( $\mathbb{R}$ , $\mathbb{R}$ )
    using slice_proj_bij ComplexReals_def real_means_real_axis
    by simp
  moreover have  $r \subseteq \mathbb{R} \times \mathbb{R}$  using valid_cntxts ring1.OrdRing_ZF_1_L1
    IsAnOrdRing_def by simp
  moreover from R_are_reals have
     $r$  {is complete} and IsLinOrder( $\mathbb{R}$ , $r$ )
    using IsAmodelOfReals_def valid_cntxts ring1.OrdRing_ZF_1_L1
    IsAnOrdRing_def by auto
  ultimately show

```

```

    CplxROrder(R,A,r) {is complete}
    IsLinOrder( $\mathbb{R}$ ,CplxROrder(R,A,r))
    using CplxROrder_def real_means_real_axis ind_rel_pres_compl
    ind_rel_pres_lin by auto
qed

The property of the strict order on complex reals that corresponds to completeness.

lemma (in complex0) pre_axsup: assumes A1:  $X \subseteq \mathbb{R}$     $X \neq 0$  and
  A2:  $\exists x \in \mathbb{R}. \forall y \in X. y <_{\mathbb{R}} x$ 
  shows
     $\exists x \in \mathbb{R}. (\forall y \in X. \neg(x <_{\mathbb{R}} y)) \wedge (\forall y \in \mathbb{R}. (y <_{\mathbb{R}} x \longrightarrow (\exists z \in X. y <_{\mathbb{R}} z)))$ 
proof -
  let s = StrictVersion(CplxROrder(R,A,r))
  have
    CplxROrder(R,A,r)  $\subseteq \mathbb{R} \times \mathbb{R}$ 
    IsLinOrder( $\mathbb{R}$ ,CplxROrder(R,A,r))
    CplxROrder(R,A,r) {is complete}
    using cplx_ord_on_cplx_reals cplx_reals_ord_lin_compl
    by auto
  moreover note A1
  moreover have s = StrictVersion(CplxROrder(R,A,r))
    by simp
  moreover from A2 have  $\exists u \in \mathbb{R}. \forall y \in X. \langle y, u \rangle \in s$ 
    by simp
  ultimately have
     $\exists x \in \mathbb{R}. (\forall y \in X. \langle x, y \rangle \notin s) \wedge$ 
     $(\forall y \in \mathbb{R}. \langle y, x \rangle \in s \longrightarrow (\exists z \in X. \langle y, z \rangle \in s))$ 
    by (rule strict_of_compl)
  then show  $(\exists x \in \mathbb{R}. (\forall y \in X. \neg(x <_{\mathbb{R}} y)) \wedge$ 
     $(\forall y \in \mathbb{R}. (y <_{\mathbb{R}} x \longrightarrow (\exists z \in X. y <_{\mathbb{R}} z))))$ 
    by simp
qed

end

```

## 42 Topology\_ZF.thy

**theory** Topology\_ZF **imports** ZF1 Finite\_ZF Fol1

**begin**

This theory file provides basic definitions and properties of topology, open and closed sets, closure and boundary.

### 42.1 Basic definitions and properties

A typical textbook defines a topology on a set  $X$  as a collection  $T$  of subsets of  $X$  such that  $X \in T$ ,  $\emptyset \in T$  and  $T$  is closed with respect to arbitrary unions and intersection of two sets. One can notice here that since we always have  $\bigcup T = X$ , the set on which the topology is defined (the "carrier" of the topology) can always be constructed from the topology itself and is superfluous in the definition. Moreover, as Marnix Klooster pointed out to me, the fact that the empty set is open can also be proven from other axioms. Hence, we define a topology as a collection of sets that is closed under arbitrary unions and intersections of two sets, without any mention of the set on which the topology is defined. Recall that  $\text{Pow}(T)$  is the powerset of  $T$ , so that if  $M \in \text{Pow}(T)$  then  $M$  is a subset of  $T$ . The sets that belong to a topology  $T$  will be sometimes called "open in"  $T$  or just "open" if the topology is clear from the context.

Topology is a collection of sets that is closed under arbitrary unions and intersections of two sets.

**definition**

$\text{IsATopology } (\_ \text{ {is a topology} } [90] \ 91) \text{ where}$   
 $T \text{ {is a topology} } \equiv ( \forall M \in \text{Pow}(T). \bigcup M \in T ) \wedge$   
 $( \forall U \in T. \forall V \in T. U \cap V \in T )$

We define interior of a set  $A$  as the union of all open sets contained in  $A$ . We use  $\text{Interior}(A, T)$  to denote the interior of  $A$ .

**definition**

$\text{Interior}(A, T) \equiv \bigcup \{U \in T. U \subseteq A\}$

A set is closed if it is contained in the carrier of topology and its complement is open.

**definition**

$\text{IsClosed (infixl {is closed in} 90) where}$   
 $D \text{ {is closed in} } T \equiv (D \subseteq \bigcup T \wedge \bigcup T - D \in T)$

To prove various properties of closure we will often use the collection of closed sets that contain a given set  $A$ . Such collection does not have a separate name in informal math. We will call it  $\text{ClosedCovers}(A, T)$ .

**definition**

$$\text{ClosedCovers}(A, T) \equiv \{D \in \text{Pow}(\bigcup T) . D \text{ \{is closed in\} } T \wedge A \subseteq D\}$$

The closure of a set  $A$  is defined as the intersection of the collection of closed sets that contain  $A$ .

**definition**

$$\text{Closure}(A, T) \equiv \bigcap \text{ClosedCovers}(A, T)$$

We also define boundary of a set as the intersection of its closure with the closure of the complement (with respect to the carrier).

**definition**

$$\text{Boundary}(A, T) \equiv \text{Closure}(A, T) \cap \text{Closure}(\bigcup T - A, T)$$

A set  $K$  is compact if for every collection of open sets that covers  $K$  we can choose a finite one that still covers the set. Recall that  $\text{FinPow}(M)$  is the collection of finite subsets of  $M$  (finite powerset of  $M$ ), defined in IsarMathLib's `Finite_ZF` theory.

**definition**

$$\begin{aligned} &\text{IsCompact (infixl \{is compact in\} 90) where} \\ &K \text{ \{is compact in\} } T \equiv (K \subseteq \bigcup T \wedge \\ &(\forall M \in \text{Pow}(T). K \subseteq \bigcup M \longrightarrow (\exists N \in \text{FinPow}(M). K \subseteq \bigcup N))) \end{aligned}$$

A basic example of a topology: the powerset of any set is a topology.

**lemma** `Pow_is_top`: **shows**  $\text{Pow}(X)$  **\{is a topology\}**

**proof** -

**have**  $\forall A \in \text{Pow}(\text{Pow}(X)). \bigcup A \in \text{Pow}(X)$  **by fast**  
**moreover have**  $\forall U \in \text{Pow}(X). \forall V \in \text{Pow}(X). U \cap V \in \text{Pow}(X)$  **by fast**  
**ultimately show**  $\text{Pow}(X)$  **\{is a topology\}** **using** `IsATopology_def`  
**by auto**

**qed**

Empty set is open.

**lemma** `empty_open`:

**assumes**  $T$  **\{is a topology\}** **shows**  $0 \in T$

**proof** -

**have**  $0 \in \text{Pow}(T)$  **by simp**  
**with assms have**  $\bigcup 0 \in T$  **using** `IsATopology_def` **by blast**  
**thus**  $0 \in T$  **by simp**

**qed**

Union of a collection of open sets is open.

**lemma** `union_open`: **assumes**  $T$  **\{is a topology\}** **and**  $\forall A \in \mathcal{A}. A \in T$

**shows**  $(\bigcup \mathcal{A}) \in T$  **using** `assms IsATopology_def` **by auto**

Union of a indexed family of open sets is open.

**lemma** `union_indexed_open`: **assumes**  $A1$ :  $T$  **\{is a topology\}** **and**  $A2$ :  $\forall i \in I. P(i) \in T$

$P(i) \in T$

shows  $(\bigcup_{i \in I}. P(i)) \in T$  using assms union\_open by simp

The intersection of any nonempty collection of topologies on a set  $X$  is a topology.

```

lemma Inter_tops_is_top:
  assumes A1:  $\mathcal{M} \neq 0$  and A2:  $\forall T \in \mathcal{M}. T \text{ \{is a topology\}}$ 
  shows  $(\bigcap \mathcal{M}) \text{ \{is a topology\}}$ 
proof -
  { fix A assume  $A \in \text{Pow}(\bigcap \mathcal{M})$ 
    with A1 have  $\forall T \in \mathcal{M}. A \in \text{Pow}(T)$  by auto
    with A1 A2 have  $\bigcup A \in \bigcap \mathcal{M}$  using IsATopology_def
    by auto
  } then have  $\forall A. A \in \text{Pow}(\bigcap \mathcal{M}) \longrightarrow \bigcup A \in \bigcap \mathcal{M}$  by simp
  hence  $\forall A \in \text{Pow}(\bigcap \mathcal{M}). \bigcup A \in \bigcap \mathcal{M}$  by auto
  moreover
  { fix U V assume  $U \in \bigcap \mathcal{M}$  and  $V \in \bigcap \mathcal{M}$ 
    then have  $\forall T \in \mathcal{M}. U \in T \wedge V \in T$  by auto
    with A1 A2 have  $\forall T \in \mathcal{M}. U \cup V \in T$  using IsATopology_def
    by simp
  } then have  $\forall U \in \bigcap \mathcal{M}. \forall V \in \bigcap \mathcal{M}. U \cup V \in \bigcap \mathcal{M}$ 
    by auto
  ultimately show  $(\bigcap \mathcal{M}) \text{ \{is a topology\}}$ 
    using IsATopology_def by simp
qed

```

We will now introduce some notation. In Isar, this is done by definining a "locale". Locale is kind of a context that holds some assumptions and notation used in all theorems proven in it. In the locale (context) below called `topology0` we assume that  $T$  is a topology. The interior of the set  $A$  (with respect to the topology in the context) is denoted  $\text{int}(A)$ . The closure of a set  $A \subseteq \bigcup T$  is denoted  $\text{cl}(A)$  and the boundary is  $\partial A$ .

```

locale topology0 =
  fixes T
  assumes topSpaceAssum:  $T \text{ \{is a topology\}}$ 

  fixes int
  defines int_def [simp]:  $\text{int}(A) \equiv \text{Interior}(A, T)$ 

  fixes cl
  defines cl_def [simp]:  $\text{cl}(A) \equiv \text{Closure}(A, T)$ 

  fixes boundary ( $\partial_$  [91] 92)
  defines boundary_def [simp]:  $\partial A \equiv \text{Boundary}(A, T)$ 

```

Intersection of a finite nonempty collection of open sets is open.

```

lemma (in topology0) fin_inter_open_open: assumes  $N \neq 0$   $N \in \text{FinPow}(T)$ 
  shows  $\bigcap N \in T$ 
  using topSpaceAssum assms IsATopology_def inter_two_inter_fin

```



by simp

Having a topology  $T$  and a set  $X$  we can define the induced topology as the one consisting of the intersections of  $X$  with sets from  $T$ . The notion of a collection restricted to a set is defined in ZF1.thy.

```

lemma (in topology0) Top_1_L4:
  shows (T {restricted to} X) {is a topology}
proof -
  let S = T {restricted to} X
  have  $\forall A \in \text{Pow}(S). \bigcup A \in S$ 
  proof
    fix A assume A1:  $A \in \text{Pow}(S)$ 
    have  $\forall V \in A. \bigcup \{U \in T. V = U \cap X\} \in T$ 
    proof -
      { fix V
        let M =  $\{U \in T. V = U \cap X\}$ 
        have  $M \in \text{Pow}(T)$  by auto
        with topSpaceAssum have  $\bigcup M \in T$  using IsATopology_def by simp
        } thus thesis by simp
      qed
      hence  $\bigcup \{U \in T. V = U \cap X\}. V \in A \subseteq T$  by auto
      with topSpaceAssum have  $(\bigcup V \in A. \bigcup \{U \in T. V = U \cap X\}) \in T$ 
        using IsATopology_def by auto
      then have  $(\bigcup V \in A. \bigcup \{U \in T. V = U \cap X\}) \cap X \in S$ 
        using RestrictedTo_def by auto
      moreover
      from A1 have  $\forall V \in A. \exists U \in T. V = U \cap X$ 
        using RestrictedTo_def by auto
      hence  $(\bigcup V \in A. \bigcup \{U \in T. V = U \cap X\}) \cap X = \bigcup A$  by blast
      ultimately show  $\bigcup A \in S$  by simp
    qed
    moreover have  $\forall U \in S. \forall V \in S. U \cap V \in S$ 
    proof -
      { fix U V assume  $U \in S \ V \in S$ 
        then obtain  $U_1 \ V_1$  where
           $U_1 \in T \wedge U = U_1 \cap X$  and  $V_1 \in T \wedge V = V_1 \cap X$ 
        using RestrictedTo_def by auto
        with topSpaceAssum have  $U_1 \cap V_1 \in T$  and  $U \cap V = (U_1 \cap V_1) \cap X$ 
        using IsATopology_def by auto
        then have  $U \cap V \in S$  using RestrictedTo_def by auto
      } thus  $\forall U \in S. \forall V \in S. U \cap V \in S$ 
        by simp
    qed
    ultimately show S {is a topology} using IsATopology_def
      by simp
  qed

```

## 42.2 Interior of a set

In section we show basic properties of the interior of a set.

Interior of a set  $A$  is contained in  $A$ .

```
lemma (in topology0) Top_2_L1: shows  $\text{int}(A) \subseteq A$   
  using Interior_def by auto
```

Interior is open.

```
lemma (in topology0) Top_2_L2: shows  $\text{int}(A) \in T$   
proof -  
  have  $\{U \in T. U \subseteq A\} \in \text{Pow}(T)$  by auto  
  with topSpaceAssum show  $\text{int}(A) \in T$   
    using IsATopology_def Interior_def by auto  
qed
```

A set is open iff it is equal to its interior.

```
lemma (in topology0) Top_2_L3: shows  $U \in T \iff \text{int}(U) = U$   
proof  
  assume  $U \in T$  then show  $\text{int}(U) = U$   
    using Interior_def by auto  
next assume  $A1: \text{int}(U) = U$   
  have  $\text{int}(U) \in T$  using Top_2_L2 by simp  
  with  $A1$  show  $U \in T$  by simp  
qed
```

Interior of the interior is the interior.

```
lemma (in topology0) Top_2_L4: shows  $\text{int}(\text{int}(A)) = \text{int}(A)$   
proof -  
  let  $U = \text{int}(A)$   
  from topSpaceAssum have  $U \in T$  using Top_2_L2 by simp  
  then show  $\text{int}(\text{int}(A)) = \text{int}(A)$  using Top_2_L3 by simp  
qed
```

Interior of a bigger set is bigger.

```
lemma (in topology0) interior_mono:  
  assumes  $A1: A \subseteq B$  shows  $\text{int}(A) \subseteq \text{int}(B)$   
proof -  
  from  $A1$  have  $\forall U \in T. (U \subseteq A \longrightarrow U \subseteq B)$  by auto  
  then show  $\text{int}(A) \subseteq \text{int}(B)$  using Interior_def by auto  
qed
```

An open subset of any set is a subset of the interior of that set.

```
lemma (in topology0) Top_2_L5: assumes  $U \subseteq A$  and  $U \in T$   
  shows  $U \subseteq \text{int}(A)$   
  using assms Interior_def by auto
```

If a point of a set has an open neighborhood contained in the set, then the point belongs to the interior of the set.

```

lemma (in topology0) Top_2_L6: assumes  $\exists U \in T. (x \in U \wedge U \subseteq A)$ 
  shows  $x \in \text{int}(A)$ 
  using assms Interior_def by auto

```

A set is open iff its every point has a an open neighbourhood contained in the set. We will formulate this statement as two lemmas (implication one way and the other way). The lemma below shows that if a set is open then every point has a an open neighbourhood contained in the set.

```

lemma (in topology0) open_open_neigh:
  assumes A1:  $\forall x \in V. \exists U \in T. (x \in U \wedge U \subseteq V)$ 
  shows  $\forall x \in V. \exists U \in T. (x \in U \wedge U \subseteq V)$ 
proof -
  from A1 have  $\forall x \in V. \forall U \in T. x \in U \wedge U \subseteq V$  by simp
  thus thesis by auto
qed

```

If every point of a set has a an open neighbourhood contained in the set then the set is open.

```

lemma (in topology0) open_neigh_open:
  assumes A1:  $\forall x \in V. \exists U \in T. (x \in U \wedge U \subseteq V)$ 
  shows  $V \in T$ 
proof -
  from A1 have  $V = \text{int}(V)$  using Top_2_L1 Top_2_L6
  by blast
  then show  $V \in T$  using Top_2_L3 by simp
qed

```

### 42.3 Closed sets, closure, boundary.

This section is devoted to closed sets and properties of the closure and boundary operators.

The carrier of the space is closed.

```

lemma (in topology0) Top_3_L1: shows  $(\bigcup T) \text{ is closed in } T$ 
proof -
  have  $\bigcup T - \bigcup T = 0$  by auto
  with topSpaceAssum have  $\bigcup T - \bigcup T \in T$  using IsATopology_def by auto
  then show thesis using IsClosed_def by simp
qed

```

Empty set is closed.

```

lemma (in topology0) Top_3_L2: shows  $0 \text{ is closed in } T$ 
  using topSpaceAssum IsATopology_def IsClosed_def by simp

```

The collection of closed covers of a subset of the carrier of topology is never empty. This is good to know, as we want to intersect this collection to get the closure.

```

lemma (in topology0) Top_3_L3:
  assumes A1:  $A \subseteq \bigcup T$  shows  $\text{ClosedCovers}(A, T) \neq 0$ 
proof -
  from A1 have  $\bigcup T \in \text{ClosedCovers}(A, T)$  using ClosedCovers_def Top_3_L1
  by auto
  thus thesis by auto
qed

```

Intersection of a nonempty family of closed sets is closed.

```

lemma (in topology0) Top_3_L4: assumes A1:  $K \neq 0$  and
  A2:  $\forall D \in K. D \text{ \{is closed in\} } T$ 
  shows  $(\bigcap K) \text{ \{is closed in\} } T$ 
proof -
  from A2 have I:  $\forall D \in K. (D \subseteq \bigcup T \wedge (\bigcup T - D) \in T)$ 
  using IsClosed_def by simp
  then have  $\{\bigcup T - D. D \in K\} \subseteq T$  by auto
  with topSpaceAssum have  $(\bigcup \{\bigcup T - D. D \in K\}) \in T$ 
  using IsATopology_def by auto
  moreover from A1 have  $\bigcup \{\bigcup T - D. D \in K\} = \bigcup T - \bigcap K$  by fast
  moreover from A1 I have  $\bigcap K \subseteq \bigcup T$  by blast
  ultimately show  $(\bigcap K) \text{ \{is closed in\} } T$  using IsClosed_def
  by simp
qed

```

The union and intersection of two closed sets are closed.

```

lemma (in topology0) Top_3_L5:
  assumes A1:  $D_1 \text{ \{is closed in\} } T$   $D_2 \text{ \{is closed in\} } T$ 
  shows
     $(D_1 \cap D_2) \text{ \{is closed in\} } T$ 
     $(D_1 \cup D_2) \text{ \{is closed in\} } T$ 
proof -
  have  $\{D_1, D_2\} \neq 0$  by simp
  with A1 have  $(\bigcap \{D_1, D_2\}) \text{ \{is closed in\} } T$  using Top_3_L4
  by fast
  thus  $(D_1 \cap D_2) \text{ \{is closed in\} } T$  by simp
  from topSpaceAssum A1 have  $(\bigcup T - D_1) \cap (\bigcup T - D_2) \in T$ 
  using IsClosed_def IsATopology_def by simp
  moreover have  $(\bigcup T - D_1) \cap (\bigcup T - D_2) = \bigcup T - (D_1 \cup D_2)$ 
  by auto
  moreover from A1 have  $D_1 \cup D_2 \subseteq \bigcup T$  using IsClosed_def
  by auto
  ultimately show  $(D_1 \cup D_2) \text{ \{is closed in\} } T$  using IsClosed_def
  by simp
qed

```

Finite union of closed sets is closed. To understand the proof recall that  $D \in \text{Pow}(\bigcup T)$  means that  $D$  is a subset of the carrier of the topology.

```

lemma (in topology0) fin_union_cl_is_cl:
  assumes

```

```

A1: N ∈ FinPow({D ∈ Pow(⋃T). D {is closed in} T})
shows (⋃N) {is closed in} T
proof -
  let C = {D ∈ Pow(⋃T). D {is closed in} T}
  have 0 ∈ C using Top_3_L2 by simp
  moreover have ∀A ∈ C. ∀B ∈ C. A ∪ B ∈ C
    using Top_3_L5 by auto
  moreover note A1
  ultimately have ⋃N ∈ C by (rule union_two_union_fin)
  thus (⋃N) {is closed in} T by simp
qed

```

Closure of a set is closed.

```

lemma (in topology0) cl_is_closed: assumes A ⊆ ⋃T
  shows cl(A) {is closed in} T
  using assms Closure_def Top_3_L3 ClosedCovers_def Top_3_L4
  by simp

```

Closure of a bigger sets is bigger.

```

lemma (in topology0) top_closure_mono:
  assumes A1: A ⊆ ⋃T B ⊆ ⋃T and A2: A ⊆ B
  shows cl(A) ⊆ cl(B)
proof -
  from A2 have ClosedCovers(B,T) ⊆ ClosedCovers(A,T)
    using ClosedCovers_def by auto
  with A1 show thesis using Top_3_L3 Closure_def by auto
qed

```

Boundary of a set is closed.

```

lemma (in topology0) boundary_closed:
  assumes A1: A ⊆ ⋃T shows ∂A {is closed in} T
proof -
  from A1 have ⋃T - A ⊆ ⋃T by fast
  with A1 show ∂A {is closed in} T
    using cl_is_closed Top_3_L5 Boundary_def by auto
qed

```

A set is closed iff it is equal to its closure.

```

lemma (in topology0) Top_3_L8: assumes A1: A ⊆ ⋃T
  shows A {is closed in} T ⟷ cl(A) = A
proof
  assume A {is closed in} T
  with A1 show cl(A) = A
    using Closure_def ClosedCovers_def by auto
next assume cl(A) = A
  then have ⋃T - A = ⋃T - cl(A) by simp
  with A1 show A {is closed in} T using cl_is_closed IsClosed_def
    by simp

```

qed

Complement of an open set is closed.

```
lemma (in topology0) Top_3_L9:
  assumes A1:  $A \in \mathcal{T}$ 
  shows  $(\bigcup T - A)$  {is closed in} T
proof -
  from topSpaceAssum A1 have  $\bigcup T - (\bigcup T - A) = A$  and  $\bigcup T - A \subseteq \bigcup T$ 
    using IsATopology_def by auto
  with A1 show  $(\bigcup T - A)$  {is closed in} T using IsClosed_def by simp
qed
```

A set is contained in its closure.

```
lemma (in topology0) cl_contains_set: assumes  $A \subseteq \bigcup T$  shows  $A \subseteq \text{cl}(A)$ 
  using assms Top_3_L1 ClosedCovers_def Top_3_L3 Closure_def by auto
```

Closure of a subset of the carrier is a subset of the carrier and closure of the complement is the complement of the interior.

```
lemma (in topology0) Top_3_L11: assumes A1:  $A \subseteq \bigcup T$ 
  shows
     $\text{cl}(A) \subseteq \bigcup T$ 
     $\text{cl}(\bigcup T - A) = \bigcup T - \text{int}(A)$ 
proof -
  from A1 show  $\text{cl}(A) \subseteq \bigcup T$  using Top_3_L1 Closure_def ClosedCovers_def
    by auto
  from A1 have  $\bigcup T - A \subseteq \bigcup T - \text{int}(A)$  using Top_2_L1
    by auto
  moreover have  $I: \bigcup T - \text{int}(A) \subseteq \bigcup T$   $\bigcup T - A \subseteq \bigcup T$  by auto
  ultimately have  $\text{cl}(\bigcup T - A) \subseteq \text{cl}(\bigcup T - \text{int}(A))$ 
    using top_closure_mono by simp
  moreover
  from I have  $(\bigcup T - \text{int}(A))$  {is closed in} T
    using Top_2_L2 Top_3_L9 by simp
  with I have  $\text{cl}((\bigcup T) - \text{int}(A)) = \bigcup T - \text{int}(A)$ 
    using Top_3_L8 by simp
  ultimately have  $\text{cl}(\bigcup T - A) \subseteq \bigcup T - \text{int}(A)$  by simp
  moreover
  from I have  $\bigcup T - A \subseteq \text{cl}(\bigcup T - A)$  using cl_contains_set by simp
  hence  $\bigcup T - \text{cl}(\bigcup T - A) \subseteq A$  and  $\bigcup T - A \subseteq \bigcup T$  by auto
  then have  $\bigcup T - \text{cl}(\bigcup T - A) \subseteq \text{int}(A)$ 
    using cl_is_closed IsClosed_def Top_2_L5 by simp
  hence  $\bigcup T - \text{int}(A) \subseteq \text{cl}(\bigcup T - A)$  by auto
  ultimately show  $\text{cl}(\bigcup T - A) = \bigcup T - \text{int}(A)$  by auto
qed
```

Boundary of a set is the closure of the set minus the interior of the set.

```
lemma (in topology0) Top_3_L12: assumes A1:  $A \subseteq \bigcup T$ 
  shows  $\partial A = \text{cl}(A) - \text{int}(A)$ 
```

```

proof -
  from A1 have  $\partial A = \text{cl}(A) \cap (\bigcup T - \text{int}(A))$ 
    using Boundary_def Top_3_L11 by simp
  moreover from A1 have
     $\text{cl}(A) \cap (\bigcup T - \text{int}(A)) = \text{cl}(A) - \text{int}(A)$ 
    using Top_3_L11 by blast
  ultimately show  $\partial A = \text{cl}(A) - \text{int}(A)$  by simp
qed

```

If a set  $A$  is contained in a closed set  $B$ , then the closure of  $A$  is contained in  $B$ .

```

lemma (in topology0) Top_3_L13:
  assumes A1:  $B \text{ \{is closed in\} } T$     $A \subseteq B$ 
  shows  $\text{cl}(A) \subseteq B$ 
proof -
  from A1 have  $B \subseteq \bigcup T$  using IsClosed_def by simp
  with A1 show  $\text{cl}(A) \subseteq B$  using ClosedCovers_def Closure_def by auto
qed

```

If a set is disjoint with an open set, then we can close it and it will still be disjoint.

```

lemma (in topology0) disj_open_cl_disj:
  assumes A1:  $A \subseteq \bigcup T$     $\forall U \in T. A \cap U = 0$ 
  shows  $\text{cl}(A) \cap V = 0$ 
proof -
  from assms have  $A \subseteq \bigcup T - V$  by auto
  moreover from A1 have  $(\bigcup T - V) \text{ \{is closed in\} } T$  using Top_3_L9 by
simp
  ultimately have  $\text{cl}(A) - (\bigcup T - V) = 0$ 
    using Top_3_L13 by blast
  moreover from A1 have  $\text{cl}(A) \subseteq \bigcup T$  using cl_is_closed IsClosed_def
by simp
  then have  $\text{cl}(A) - (\bigcup T - V) = \text{cl}(A) \cap V$  by auto
  ultimately show thesis by simp
qed

```

A reformulation of `disj_open_cl_disj`: If a point belongs to the closure of a set, then we can find a point from the set in any open neighborhood of the point.

```

lemma (in topology0) cl_inter_neigh:
  assumes A1:  $A \subseteq \bigcup T$  and A2:  $U \in T$  and  $x \in \text{cl}(A) \cap U$ 
  shows  $A \cap U \neq 0$  using assms disj_open_cl_disj by auto

```

A reverse of `cl_inter_neigh`: if every open neighborhood of a point has a nonempty intersection with a set, then that point belongs to the closure of the set.

```

lemma (in topology0) inter_neigh_cl:
  assumes A1:  $A \subseteq \bigcup T$  and A2:  $x \in \bigcup T$  and A3:  $\forall U \in T. x \in U \longrightarrow U \cap A \neq 0$ 

```

```

    shows  $x \in \text{cl}(A)$ 
  proof -
    { assume  $x \notin \text{cl}(A)$ 
      with A1 obtain D where D {is closed in} T and  $A \subseteq D$  and  $x \notin D$ 
      using Top_3_L3 Closure_def ClosedCovers_def by auto
      let  $U = (\bigcup T) - D$ 
      from A2 ' $D$  {is closed in} T' ' $x \notin D$ ' ' $A \subseteq D$ ' have  $U \in T$   $x \in U$  and  $U \cap A =$ 
0
      unfolding IsClosed_def by auto
      with A3 have False by auto
    } thus thesis by auto
  qed
end

```



## 43 Topology\_ZF\_1.thy

**theory** Topology\_ZF\_1 **imports** Topology\_ZF

**begin**

In this theory file we study separation axioms and the notion of base and subbase. Using the products of open sets as a subbase we define a natural topology on a product of two topological spaces.

### 43.1 Separation axioms.

Topological spaces can be classified according to certain properties called "separation axioms". In this section we define what it means that a topological space is  $T_0$ ,  $T_1$  or  $T_2$ .

A topology on  $X$  is  $T_0$  if for every pair of distinct points of  $X$  there is an open set that contains only one of them.

**definition**

**isT0** ( $\_ \{is\ T_0\}$  [90] 91) **where**  
 $T \{is\ T_0\} \equiv \forall\ x\ y. ((x \in \bigcup T \wedge y \in \bigcup T \wedge x \neq y) \longrightarrow$   
 $(\exists U \in T. (x \in U \wedge y \notin U) \vee (y \in U \wedge x \notin U)))$

A topology is  $T_1$  if for every such pair there exist an open set that contains the first point but not the second.

**definition**

**isT1** ( $\_ \{is\ T_1\}$  [90] 91) **where**  
 $T \{is\ T_1\} \equiv \forall\ x\ y. ((x \in \bigcup T \wedge y \in \bigcup T \wedge x \neq y) \longrightarrow$   
 $(\exists U \in T. (x \in U \wedge y \notin U)))$

A topology is  $T_2$  (Hausdorff) if for every pair of points there exist a pair of disjoint open sets each containing one of the points. This is an important class of topological spaces. In particular, metric spaces are Hausdorff.

**definition**

**isT2** ( $\_ \{is\ T_2\}$  [90] 91) **where**  
 $T \{is\ T_2\} \equiv \forall\ x\ y. ((x \in \bigcup T \wedge y \in \bigcup T \wedge x \neq y) \longrightarrow$   
 $(\exists U \in T. \exists V \in T. x \in U \wedge y \in V \wedge U \cap V = \emptyset))$

If a topology is  $T_1$  then it is  $T_0$ . We don't really assume here that  $T$  is a topology on  $X$ . Instead, we prove the relation between  $isT_0$  condition and  $isT_1$ .

**lemma** T1\_is\_T0: **assumes** A1:  $T \{is\ T_1\}$  **shows**  $T \{is\ T_0\}$

**proof** -

**from** A1 **have**  $\forall\ x\ y. x \in \bigcup T \wedge y \in \bigcup T \wedge x \neq y \longrightarrow$   
 $(\exists U \in T. x \in U \wedge y \notin U)$   
**using** isT1\_def **by** simp  
**then have**  $\forall\ x\ y. x \in \bigcup T \wedge y \in \bigcup T \wedge x \neq y \longrightarrow$

```

      ( $\exists U \in T. x \in U \wedge y \notin U \vee y \in U \wedge x \notin U$ )
    by auto
  then show  $T \{is\ T_0\}$  using isT0_def by simp
qed

```

If a topology is  $T_2$  then it is  $T_1$ .

```

lemma T2_is_T1: assumes A1:  $T \{is\ T_2\}$  shows  $T \{is\ T_1\}$ 
proof -
  { fix x y assume  $x \in \bigcup T \ y \in \bigcup T \ x \neq y$ 
    with A1 have  $\exists U \in T. \exists V \in T. x \in U \wedge y \in V \wedge U \cap V = \emptyset$ 
      using isT2_def by auto
    then have  $\exists U \in T. x \in U \wedge y \notin U$  by auto
  } then have  $\forall x y. x \in \bigcup T \wedge y \in \bigcup T \wedge x \neq y \longrightarrow$ 
    ( $\exists U \in T. x \in U \wedge y \notin U$ ) by simp
  then show  $T \{is\ T_1\}$  using isT1_def by simp
qed

```

In a  $T_0$  space two points that can not be separated by an open set are equal.  
Proof by contradiction.

```

lemma Top_1_1_L1: assumes A1:  $T \{is\ T_0\}$  and A2:  $x \in \bigcup T \ y \in \bigcup T$ 
  and A3:  $\forall U \in T. (x \in U \longleftrightarrow y \in U)$ 
  shows  $x=y$ 
proof -
  { assume  $x \neq y$ 
    with A1 A2 have  $\exists U \in T. x \in U \wedge y \notin U \vee y \in U \wedge x \notin U$ 
      using isT0_def by simp
    with A3 have False by auto
  } then show  $x=y$  by auto
qed

```

## 43.2 Bases and subbases.

Sometimes it is convenient to talk about topologies in terms of their bases and subbases. These are certain collections of open sets that define the whole topology.

A base of topology is a collection of open sets such that every open set is a union of the sets from the base.

### definition

```

IsABaseFor (infixl {is a base for} 65) where
B {is a base for} T  $\equiv B \subseteq T \wedge T = \{\bigcup A. A \in \text{Pow}(B)\}$ 

```

A subbase is a collection of open sets such that finite intersection of those sets form a base.

### definition

```

IsASubBaseFor (infixl {is a subbase for} 65) where
B {is a subbase for} T  $\equiv$ 
 $B \subseteq T \wedge \{\bigcap A. A \in \text{FinPow}(B)\} \{is\ a\ base\ for\} T$ 

```

Below we formulate a condition that we will prove to be necessary and sufficient for a collection  $B$  of open sets to form a base. It says that for any two sets  $U, V$  from the collection  $B$  we can find a point  $x \in U \cap V$  with a neighborhood from  $B$  contained in  $U \cap V$ .

**definition**

```
SatisfiesBaseCondition ( _ {satisfies the base condition} [50] 50)
where
B {satisfies the base condition}  $\equiv$ 
 $\forall U V. ((U \in B \wedge V \in B) \longrightarrow (\forall x \in U \cap V. \exists W \in B. x \in W \wedge W \subseteq U \cap V))$ 
```

A collection that is closed with respect to intersection satisfies the base condition.

```
lemma inter_closed_base: assumes  $\forall U \in B. (\forall V \in B. U \cap V \in B)$ 
shows B {satisfies the base condition}
proof -
  { fix U V x assume  $U \in B$  and  $V \in B$  and  $x \in U \cap V$ 
    with assms have  $\exists W \in B. x \in W \wedge W \subseteq U \cap V$  by blast
  } then show thesis using SatisfiesBaseCondition_def by simp
qed
```

Each open set is a union of some sets from the base.

```
lemma Top_1_2_L1: assumes B {is a base for} T and  $U \in T$ 
shows  $\exists A \in \text{Pow}(B). U = \bigcup A$ 
using assms IsAbaseFor_def by simp
```

Elements of base are open.

```
lemma base_sets_open:
assumes B {is a base for} T and  $U \in B$ 
shows  $U \in T$ 
using assms IsAbaseFor_def by auto
```

A base defines topology uniquely.

```
lemma same_base_same_top:
assumes B {is a base for} T and B {is a base for} S
shows  $T = S$ 
using assms IsAbaseFor_def by simp
```

Every point from an open set has a neighborhood from the base that is contained in the set.

```
lemma point_open_base_neigh:
assumes A1: B {is a base for} T and A2:  $U \in T$  and A3:  $x \in U$ 
shows  $\exists V \in B. V \subseteq U \wedge x \in V$ 
proof -
  from A1 A2 obtain A where  $A \in \text{Pow}(B)$  and  $U = \bigcup A$ 
  using Top_1_2_L1 by blast
  with A3 obtain V where  $V \in A$  and  $x \in V$  by auto
  with 'A  $\in \text{Pow}(B)$ ' 'U =  $\bigcup A$ ' show thesis by auto
```

qed

A criterion for a collection to be a base for a topology that is a slight reformulation of the definition. The only thing different that in the definition is that we assume only that every open set is a union of some sets from the base. The definition requires also the opposite inclusion that every union of the sets from the base is open, but that we can prove if we assume that  $T$  is a topology.

```
lemma is_a_base_criterion: assumes A1: T {is a topology}
  and A2: B ⊆ T and A3: ∀ V ∈ T. ∃ A ∈ Pow(B). V = ⋃ A
  shows B {is a base for} T
proof -
  from A3 have T ⊆ {⋃ A. A ∈ Pow(B)} by auto
  moreover have {⋃ A. A ∈ Pow(B)} ⊆ T
  proof
    fix U assume U ∈ {⋃ A. A ∈ Pow(B)}
    then obtain A where A ∈ Pow(B) and U = ⋃ A
    by auto
    with 'B ⊆ T' have A ∈ Pow(T) by auto
    with A1 'U = ⋃ A' show U ∈ T
    unfolding IsATopology_def by simp
  qed
  ultimately have T = {⋃ A. A ∈ Pow(B)} by auto
  with A2 show B {is a base for} T
  unfolding IsAbaseFor_def by simp
qed
```

A necessary condition for a collection of sets to be a base for some topology : every point in the intersection of two sets in the base has a neighborhood from the base contained in the intersection.

```
lemma Top_1_2_L2:
  assumes A1: ∃ T. T {is a topology} ∧ B {is a base for} T
  and A2: V ∈ B W ∈ B
  shows ∀ x ∈ V ∩ W. ∃ U ∈ B. x ∈ U ∧ U ⊆ V ∩ W
proof -
  from A1 obtain T where
    D1: T {is a topology} B {is a base for} T
  by auto
  then have B ⊆ T using IsAbaseFor_def by auto
  with A2 have V ∈ T and W ∈ T using IsAbaseFor_def by auto
  with D1 have ∃ A ∈ Pow(B). V ∩ W = ⋃ A using IsATopology_def Top_1_2_L1
  by auto
  then obtain A where A ⊆ B and V ∩ W = ⋃ A by auto
  then show ∀ x ∈ V ∩ W. ∃ U ∈ B. (x ∈ U ∧ U ⊆ V ∩ W) by auto
qed
```

We will construct a topology as the collection of unions of (would-be) base. First we prove that if the collection of sets satisfies the condition we want

to show to be sufficient, the the intersection belongs to what we will define as topology (am I clear here?). Having this fact ready simplifies the proof of the next lemma. There is not much topology here, just some set theory.

```

lemma Top_1_2_L3:
  assumes A1:  $\forall x \in V \cap W. \exists U \in B. x \in U \wedge U \subseteq V \cap W$ 
  shows  $V \cap W \in \{\bigcup A. A \in \text{Pow}(B)\}$ 
proof
  let A =  $\bigcup_{x \in V \cap W}. \{U \in B. x \in U \wedge U \subseteq V \cap W\}$ 
  show  $A \in \text{Pow}(B)$  by auto
  from A1 show  $V \cap W = \bigcup A$  by blast
qed

```

The next lemma is needed when proving that the would-be topology is closed with respect to taking intersections. We show here that intersection of two sets from this (would-be) topology can be written as union of sets from the topology.

```

lemma Top_1_2_L4:
  assumes A1:  $U_1 \in \{\bigcup A. A \in \text{Pow}(B)\}$   $U_2 \in \{\bigcup A. A \in \text{Pow}(B)\}$ 
  and A2:  $B \text{ \{satisfies the base condition\}}$ 
  shows  $\exists C. C \subseteq \{\bigcup A. A \in \text{Pow}(B)\} \wedge U_1 \cap U_2 = \bigcup C$ 
proof -
  from A1 A2 obtain A1 A2 where
    D1:  $A_1 \in \text{Pow}(B)$   $U_1 = \bigcup A_1$   $A_2 \in \text{Pow}(B)$   $U_2 = \bigcup A_2$ 
  by auto
  let C =  $\bigcup_{U \in A_1. \{U \cap V. V \in A_2\}}$ 
  from D1 have  $(\forall U \in A_1. U \in B) \wedge (\forall V \in A_2. V \in B)$  by auto
  with A2 have  $C \subseteq \{\bigcup A. A \in \text{Pow}(B)\}$ 
    using Top_1_2_L3 SatisfiesBaseCondition_def by auto
  moreover from D1 have  $U_1 \cap U_2 = \bigcup C$  by auto
  ultimately show thesis by auto
qed

```

If  $B$  satisfies the base condition, then the collection of unions of sets from  $B$  is a topology and  $B$  is a base for this topology.

```

theorem Top_1_2_T1:
  assumes A1:  $B \text{ \{satisfies the base condition\}}$ 
  and A2:  $T = \{\bigcup A. A \in \text{Pow}(B)\}$ 
  shows  $T \text{ \{is a topology\}} \text{ and } B \text{ \{is a base for\}} T$ 
proof -
  show  $T \text{ \{is a topology\}}$ 
  proof -
    have I:  $\forall C \in \text{Pow}(T). \bigcup C \in T$ 
    proof -
      { fix C assume A3:  $C \in \text{Pow}(T)$ 
        let Q =  $\bigcup \{\bigcup \{A \in \text{Pow}(B). U = \bigcup A\}. U \in C\}$ 
        from A2 A3 have  $\forall U \in C. \exists A \in \text{Pow}(B). U = \bigcup A$  by auto
        then have  $\bigcup Q = \bigcup C$  using ZF1_1_L10 by simp
        moreover from A2 have  $\bigcup Q \in T$  by auto
      }
    }
  qed

```

```

      ultimately have  $\bigcup C \in T$  by simp
    } thus  $\forall C \in \text{Pow}(T). \bigcup C \in T$  by auto
  qed
  moreover have  $\forall U \in T. \forall V \in T. U \cap V \in T$ 
  proof -
    { fix U V assume  $U \in T \ V \in T$ 
      with A1 A2 have  $\exists C. (C \subseteq T \wedge U \cap V = \bigcup C)$ 
      using Top_1_2_L4 by simp
      then obtain C where  $C \subseteq T$  and  $U \cap V = \bigcup C$ 
      by auto
      with I have  $U \cap V \in T$  by simp
    } then show  $\forall U \in T. \forall V \in T. U \cap V \in T$  by simp
  qed
  ultimately show T {is a topology} using IsATopology_def
  by simp
qed
from A2 have  $B \subseteq T$  by auto
with A2 show B {is a base for} T using IsABaseFor_def
by simp
qed

```

The carrier of the base and topology are the same.

```

lemma Top_1_2_L5: assumes B {is a base for} T
  shows  $\bigcup T = \bigcup B$ 
  using assms IsABaseFor_def by auto

```

If  $B$  is a base for  $T$ , then  $T$  is the smallest topology containing  $B$ .

```

lemma base_smallest_top:
  assumes A1: B {is a base for} T and A2: S {is a topology} and A3:
 $B \subseteq S$ 
  shows  $T \subseteq S$ 
proof
  fix U assume  $U \in T$ 
  with A1 obtain  $B_U$  where  $B_U \subseteq B$  and  $U = \bigcup B_U$  using IsABaseFor_def
  by auto
  with A3 have  $B_U \subseteq S$  by auto
  with A2 ' $U = \bigcup B_U$ ' show  $U \in S$  using IsATopology_def by simp
qed

```

If  $B$  is a base for  $T$  and  $B$  is a topology, then  $B = T$ .

```

lemma base_topology: assumes B {is a topology} and B {is a base for}
T
  shows  $B = T$  using assms base_sets_open base_smallest_top by blast

```

### 43.3 Product topology

In this section we consider a topology defined on a product of two sets.

Given two topological spaces we can define a topology on the product of the carriers such that the cartesian products of the sets of the topologies are a base for the product topology. Recall that for two collections  $S, T$  of sets the product collection is defined (in `ZF1.thy`) as the collections of cartesian products  $A \times B$ , where  $A \in S, B \in T$ .

**definition**

$\text{ProductTopology}(T, S) \equiv \{\bigcup W. W \in \text{Pow}(\text{ProductCollection}(T, S))\}$

The product collection satisfies the base condition.

**lemma** `Top_1_4_L1`:

assumes  $A1$ :  $T$  {is a topology}     $S$  {is a topology}  
 and  $A2$ :  $A \in \text{ProductCollection}(T, S)$      $B \in \text{ProductCollection}(T, S)$   
 shows  $\forall x \in (A \cap B). \exists W \in \text{ProductCollection}(T, S). (x \in W \wedge W \subseteq A \cap B)$

**proof**

fix  $x$  assume  $A3$ :  $x \in A \cap B$   
 from  $A2$  obtain  $U_1 \ V_1 \ U_2 \ V_2$  where  
 $D1$ :  $U_1 \in T \ V_1 \in S \ A = U_1 \times V_1 \ U_2 \in T \ V_2 \in S \ B = U_2 \times V_2$   
 using `ProductCollection_def` by auto  
 let  $W = (U_1 \cap U_2) \times (V_1 \cap V_2)$   
 from  $A1 \ D1$  have  $U_1 \cap U_2 \in T$  and  $V_1 \cap V_2 \in S$   
 using `IsATopology_def` by auto  
 then have  $W \in \text{ProductCollection}(T, S)$  using `ProductCollection_def`  
 by auto  
 moreover from  $A3 \ D1$  have  $x \in W$  and  $W \subseteq A \cap B$  by auto  
 ultimately have  $\exists W. (W \in \text{ProductCollection}(T, S) \wedge x \in W \wedge W \subseteq A \cap B)$   
 by auto  
 thus  $\exists W \in \text{ProductCollection}(T, S). (x \in W \wedge W \subseteq A \cap B)$  by auto

**qed**

The product topology is indeed a topology on the product.

**theorem** `Top_1_4_T1`: assumes  $A1$ :  $T$  {is a topology}     $S$  {is a topology}  
 shows

$\text{ProductTopology}(T, S)$  {is a topology}  
 $\text{ProductCollection}(T, S)$  {is a base for}  $\text{ProductTopology}(T, S)$   
 $\bigcup \text{ProductTopology}(T, S) = \bigcup T \times \bigcup S$

**proof** -

from  $A1$  show  
 $\text{ProductTopology}(T, S)$  {is a topology}  
 $\text{ProductCollection}(T, S)$  {is a base for}  $\text{ProductTopology}(T, S)$   
 using `Top_1_4_L1` `ProductCollection_def`  
`SatisfiesBaseCondition_def` `ProductTopology_def` `Top_1_2_T1`  
 by auto  
 then show  $\bigcup \text{ProductTopology}(T, S) = \bigcup T \times \bigcup S$   
 using `Top_1_2_L5` `ZF1_1_L6` by simp

**qed**

Each point of a set open in the product topology has a neighborhood which is a cartesian product of open sets.

```

lemma prod_top_point_neighb:
  assumes A1: T {is a topology} S {is a topology} and
  A2: U ∈ ProductTopology(T,S) and A3: x ∈ U
  shows ∃ V W. V ∈ T ∧ W ∈ S ∧ V × W ⊆ U ∧ x ∈ V × W
proof -
  from A1 have
    ProductCollection(T,S) {is a base for} ProductTopology(T,S)
  using Top_1_4_T1 by simp
  with A2 A3 obtain Z where
    Z ∈ ProductCollection(T,S) and Z ⊆ U ∧ x ∈ Z
  using point_open_base_neigh by blast
  then obtain V W where V ∈ T and W ∈ S and V × W ⊆ U ∧ x ∈ V × W
  using ProductCollection_def by auto
  thus thesis by auto
qed

```

Products of open sets are open in the product topology.

```

lemma prod_open_open_prod:
  assumes A1: T {is a topology} S {is a topology} and
  A2: U ∈ T V ∈ S
  shows U × V ∈ ProductTopology(T,S)
proof -
  from A1 have
    ProductCollection(T,S) {is a base for} ProductTopology(T,S)
  using Top_1_4_T1 by simp
  moreover from A2 have U × V ∈ ProductCollection(T,S)
  unfolding ProductCollection_def by auto
  ultimately show U × V ∈ ProductTopology(T,S)
  using base_sets_open by simp
qed

```

Sets that are open in the product topology are contained in the product of the carrier.

```

lemma prod_open_type: assumes A1: T {is a topology} S {is a topology}
and
  A2: V ∈ ProductTopology(T,S)
  shows V ⊆ ∪ T × ∪ S
proof -
  from A2 have V ⊆ ∪ ProductTopology(T,S) by auto
  with A1 show thesis using Top_1_4_T1 by simp
qed

```

Suppose we have subsets  $A \subseteq X, B \subseteq Y$ , where  $X, Y$  are topological spaces with topologies  $T, S$ . We can then consider relative topologies on  $T_A, S_B$  on sets  $A, B$  and the collection of cartesian products of sets open in  $T_A, S_B$ , (namely  $\{U \times V : U \in T_A, V \in S_B\}$ ). The next lemma states that this collection is a base of the product topology on  $X \times Y$  restricted to the product  $A \times B$ .



```

lemma prod_restr_base_restr:
  assumes A1: T {is a topology} S {is a topology}
  shows
    ProductCollection(T {restricted to} A, S {restricted to} B)
    {is a base for} (ProductTopology(T,S) {restricted to} A×B)
proof -
  let  $\mathcal{B}$  = ProductCollection(T {restricted to} A, S {restricted to} B)
  let  $\tau$  = ProductTopology(T,S)
  from A1 have ( $\tau$  {restricted to} A×B) {is a topology}
    using Top_1_4_T1 topology0_def topology0.Top_1_L4
    by simp
  moreover have  $\mathcal{B} \subseteq (\tau$  {restricted to} A×B)
proof
  fix U assume U  $\in$   $\mathcal{B}$ 
  then obtain  $U_A U_B$  where U =  $U_A \times U_B$  and
     $U_A \in (T$  {restricted to} A) and  $U_B \in (S$  {restricted to} B)
    using ProductCollection_def by auto
  then obtain  $W_A W_B$  where
     $W_A \in T$   $U_A = W_A \cap A$  and  $W_B \in S$   $U_B = W_B \cap B$ 
    using RestrictedTo_def by auto
  with 'U =  $U_A \times U_B$ ' have U =  $W_A \times W_B \cap (A \times B)$  by auto
  moreover from A1 ' $W_A \in T$ ' and ' $W_B \in S$ ' have  $W_A \times W_B \in \tau$ 
    using prod_open_open_prod by simp
  ultimately show U  $\in \tau$  {restricted to} A×B
    using RestrictedTo_def by auto
qed
moreover have  $\forall U \in \tau$  {restricted to} A×B.
   $\exists C \in \text{Pow}(\mathcal{B}). U = \bigcup C$ 
proof
  fix U assume U  $\in \tau$  {restricted to} A×B
  then obtain W where W  $\in \tau$  and U = W  $\cap (A \times B)$ 
    using RestrictedTo_def by auto
  from A1 ' $W \in \tau$ ' obtain  $A_W$  where
     $A_W \in \text{Pow}(\text{ProductCollection}(T,S))$  and W =  $\bigcup A_W$ 
    using Top_1_4_T1 IsAbaseFor_def by auto
  let C = {V  $\cap A \times B$ . V  $\in A_W$ }
  have C  $\in \text{Pow}(\mathcal{B})$  and U =  $\bigcup C$ 
proof -
  { fix R assume R  $\in$  C
  then obtain V where V  $\in A_W$  and R = V  $\cap A \times B$ 
    by auto
  with ' $A_W \in \text{Pow}(\text{ProductCollection}(T,S))$ ' obtain  $V_T V_S$  where
     $V_T \in T$  and  $V_S \in S$  and V =  $V_T \times V_S$ 
    using ProductCollection_def by auto
  with ' $R = V \cap A \times B$ ' have R  $\in \mathcal{B}$ 
    using ProductCollection_def RestrictedTo_def
    by auto
  } then show C  $\in \text{Pow}(\mathcal{B})$  by auto
  from 'U = W  $\cap (A \times B)$ ' and ' $W = \bigcup A_W$ '

```

```

      show  $U = \bigcup C$  by auto
    qed
    thus  $\exists C \in \text{Pow}(B). U = \bigcup C$  by blast
  qed
  ultimately show thesis by (rule is_a_base_criterion)
qed

```

We can commute taking restriction (relative topology) and product topology. The reason the two topologies are the same is that they have the same base.

```

lemma prod_top_restr_comm:
  assumes A1:  $T$  {is a topology}   $S$  {is a topology}
  shows
    ProductTopology( $T$  {restricted to}  $A, S$  {restricted to}  $B$ ) =
    ProductTopology( $T, S$ ) {restricted to}  $(A \times B)$ 
proof -
  let  $B = \text{ProductCollection}(T$  {restricted to}  $A, S$  {restricted to}  $B)$ 
  from A1 have
     $B$  {is a base for} ProductTopology( $T$  {restricted to}  $A, S$  {restricted
to}  $B$ )
    using topology0_def topology0.Top_1_L4 Top_1_4_T1 by simp
  moreover from A1 have
     $B$  {is a base for} ProductTopology( $T, S$ ) {restricted to}  $(A \times B)$ 
    using prod_restr_base_restr by simp
  ultimately show thesis by (rule same_base_same_top)
qed

```

Projection of a section of an open set is open.

```

lemma prod_sec_open1: assumes A1:  $T$  {is a topology}   $S$  {is a topology}
and
  A2:  $V \in \text{ProductTopology}(T, S)$  and A3:  $x \in \bigcup T$ 
  shows  $\{y \in \bigcup S. \langle x, y \rangle \in V\} \in S$ 
proof -
  let  $A = \{y \in \bigcup S. \langle x, y \rangle \in V\}$ 
  from A1 have topology0( $S$ ) using topology0_def by simp
  moreover have  $\forall y \in A. \exists W \in S. (y \in W \wedge W \subseteq A)$ 
  proof
    fix y assume  $y \in A$ 
    then have  $\langle x, y \rangle \in V$  by simp
    with A1 A2 have  $\langle x, y \rangle \in \bigcup T \times \bigcup S$  using prod_open_type by blast
    hence  $x \in \bigcup T$  and  $y \in \bigcup S$  by auto
    from A1 A2 ' $\langle x, y \rangle \in V$ ' have  $\exists U W. U \in T \wedge W \in S \wedge U \times W \subseteq V \wedge \langle x, y \rangle$ 
 $\in U \times W$ 
    by (rule prod_top_point_neighb)
    then obtain  $U W$  where  $U \in T \wedge W \in S \wedge U \times W \subseteq V \wedge \langle x, y \rangle \in U \times W$ 
    by auto
    with A1 A2 show  $\exists W \in S. (y \in W \wedge W \subseteq A)$  using prod_open_type section_proj
    by auto
  qed
  ultimately show thesis by (rule topology0.open_neigh_open)

```

qed

Projection of a section of an open set is open. This is dual of `prod_sec_open1` with a very similar proof.

**lemma** `prod_sec_open2`: `assumes A1: T {is a topology} S {is a topology}`  
**and**

`A2: V ∈ ProductTopology(T,S) and A3: y ∈  $\bigcup T$ S`

`shows {x ∈  $\bigcup T$ .  $\langle x,y \rangle \in V$ } ∈ T`

**proof** -

`let A = {x ∈  $\bigcup T$ .  $\langle x,y \rangle \in V$ }`

`from A1 have topology0(T) using topology0_def by simp`

`moreover have  $\forall x \in A. \exists W \in T. (x \in W \wedge W \subseteq A)$`

**proof**

`fix x assume x ∈ A`

`then have  $\langle x,y \rangle \in V$  by simp`

`with A1 A2 have  $\langle x,y \rangle \in \bigcup T \times \bigcup S$  using prod_open_type by blast`

`hence x ∈  $\bigcup T$  and y ∈  $\bigcup S$  by auto`

`from A1 A2 ' $\langle x,y \rangle \in V$ ' have  $\exists U W. U \in T \wedge W \in S \wedge U \times W \subseteq V \wedge \langle x,y \rangle$`

`∈ U × W`

`by (rule prod_top_point_neighb)`

`then obtain U W where  $U \in T \wedge W \in S \wedge U \times W \subseteq V \wedge \langle x,y \rangle \in U \times W$`

`by auto`

`with A1 A2 show  $\exists W \in T. (x \in W \wedge W \subseteq A)$  using prod_open_type section_proj`

`by auto`

**qed**

`ultimately show thesis by (rule topology0.open_neigh_open)`

qed

end

## 44 Topology\_ZF\_1b.thy

```
theory Topology_ZF_1b imports Topology_ZF_1
```

```
begin
```

One of the facts demonstrated in every class on General Topology is that in a  $T_2$  (Hausdorff) topological space compact sets are closed. Formalizing the proof of this fact gave me an interesting insight into the role of the Axiom of Choice (AC) in many informal proofs.

A typical informal proof of this fact goes like this: we want to show that the complement of  $K$  is open. To do this, choose an arbitrary point  $y \in K^c$ . Since  $X$  is  $T_2$ , for every point  $x \in K$  we can find an open set  $U_x$  such that  $y \notin \overline{U_x}$ . Obviously  $\{U_x\}_{x \in K}$  covers  $K$ , so select a finite subcollection that covers  $K$ , and so on. I had never realized that such reasoning requires the Axiom of Choice. Namely, suppose we have a lemma that states "In  $T_2$  spaces, if  $x \neq y$ , then there is an open set  $U$  such that  $x \in U$  and  $y \notin \overline{U}$ " (like our lemma `T2_cl_open_sep` below). This only states that the set of such open sets  $U$  is not empty. To get the collection  $\{U_x\}_{x \in K}$  in this proof we have to select one such set among many for every  $x \in K$  and this is where we use the Axiom of Choice. Probably in 99/100 cases when an informal calculus proof states something like  $\forall \varepsilon \exists \delta_\varepsilon \dots$  the proof uses AC. Most of the time the use of AC in such proofs can be avoided. This is also the case for the fact that in a  $T_2$  space compact sets are closed.

### 44.1 Compact sets are closed - no need for AC

In this section we show that in a  $T_2$  topological space compact sets are closed.

First we prove a lemma that in a  $T_2$  space two points can be separated by the closure of an open set.

```
lemma (in topology0) T2_cl_open_sep:
  assumes T {is T2} and x ∈ ⋃ T y ∈ ⋃ T x ≠ y
  shows ∃ U ∈ T. (x ∈ U ∧ y ∉ cl(U))
proof -
  from assms have ∃ U ∈ T. ∃ V ∈ T. x ∈ U ∧ y ∈ V ∧ U ∩ V = 0
  using isT2_def by simp
  then obtain U V where U ∈ T V ∈ T x ∈ U y ∈ V U ∩ V = 0
  by auto
  then have U ∈ T ∧ x ∈ U ∧ y ∈ V ∧ cl(U) ∩ V = 0
  using disj_open_cl_disj by auto
  thus ∃ U ∈ T. (x ∈ U ∧ y ∉ cl(U)) by auto
qed
```

AC-free proof that in a Hausdorff space compact sets are closed. To understand the notation recall that in Isabelle/ZF `Pow(A)` is the powerset (the

set of subsets) of  $A$  and  $\text{FinPow}(A)$  denotes the set of finite subsets of  $A$  in IsarMathLib.

```

theorem (in topology0) in_t2_compact_is_cl:
  assumes A1:  $T \text{ \{is } T_2\}$  and A2:  $K \text{ \{is compact in\} } T$ 
  shows  $K \text{ \{is closed in\} } T$ 
proof -
  let  $X = \bigcup T$ 
  have  $\forall y \in X - K. \exists U \in T. y \in U \wedge U \subseteq X - K$ 
  proof -
    { fix y assume  $y \in X \quad y \notin K$ 
      have  $\exists U \in T. y \in U \wedge U \subseteq X - K$ 
      proof -
        let  $B = \bigcup_{x \in K. \{V \in T. x \in V \wedge y \notin \text{cl}(V)\}}$ 
        have I:  $B \in \text{Pow}(T) \quad \text{FinPow}(B) \subseteq \text{Pow}(B)$ 
          using FinPow_def by auto
        from ' $K \text{ \{is compact in\} } T$ ' ' $y \in X$ ' ' $y \notin K$ ' have
           $\forall x \in K. x \in X \wedge y \in X \wedge x \neq y$ 
          using IsCompact_def by auto
        with ' $T \text{ \{is } T_2\}$ ' have  $\forall x \in K. \{V \in T. x \in V \wedge y \notin \text{cl}(V)\} \neq \emptyset$ 
          using T2_cl_open_sep by auto
        hence  $K \subseteq \bigcup B$  by blast
        with ' $K \text{ \{is compact in\} } T$ ' I have
           $\exists N \in \text{FinPow}(B). K \subseteq \bigcup N$ 
          using IsCompact_def by auto
        then obtain N where  $N \in \text{FinPow}(B) \quad K \subseteq \bigcup N$ 
          by auto
        with I have  $N \subseteq B$  by auto
        hence  $\forall V \in N. V \in B$  by auto
        let  $M = \{\text{cl}(V). V \in N\}$ 
        let  $C = \{D \in \text{Pow}(X). D \text{ \{is closed in\} } T\}$ 
        from ' $N \in \text{FinPow}(B)$ ' have  $\forall V \in B. \text{cl}(V) \in C \quad N \in \text{FinPow}(B)$ 
          using cl_is_closed IsClosed_def by auto
        then have  $M \in \text{FinPow}(C)$  by (rule fin_image_fin)
        then have  $X - \bigcup M \in T$  using fin_union_cl_is_cl IsClosed_def
          by simp
        moreover from ' $y \in X$ ' ' $y \notin K$ ' ' $\forall V \in N. V \in B$ ' have
           $y \in X - \bigcup M$  by simp
        moreover have  $X - \bigcup M \subseteq X - K$ 
        proof -
          from ' $\forall V \in N. V \in B$ ' have  $\bigcup N \subseteq \bigcup M$  using cl_contains_set by auto
          with ' $K \subseteq \bigcup N$ ' show  $X - \bigcup M \subseteq X - K$  by auto
        qed
      qed
    } ultimately have  $\exists U. U \in T \wedge y \in U \wedge U \subseteq X - K$ 
      by auto
  thus  $\exists U \in T. y \in U \wedge U \subseteq X - K$  by auto
  qed
} thus  $\forall y \in X - K. \exists U \in T. y \in U \wedge U \subseteq X - K$ 
  by auto
qed

```

```
with A2 show K {is closed in} T
  using open_neigh_open IsCompact_def IsClosed_def by auto
qed

end
```

## 45 Topology\_ZF\_2.thy

```
theory Topology_ZF_2 imports Topology_ZF_1 func1 Fol1
```

```
begin
```

This theory continues the series on general topology and covers the definition and basic properties of continuous functions. We also introduce the notion of homeomorphism and prove the pasting lemma.

### 45.1 Continuous functions.

In this section we define continuous functions and prove that certain conditions are equivalent to a function being continuous.

In standard math we say that a function is continuous with respect to two topologies  $\tau_1, \tau_2$  if the inverse image of sets from topology  $\tau_2$  are in  $\tau_1$ . Here we define a predicate that is supposed to reflect that definition, with a difference that we don't require in the definition that  $\tau_1, \tau_2$  are topologies. This means for example that when we define measurable functions, the definition will be the same.

The notation  $f^{-1}(A)$  means the inverse image of (a set)  $A$  with respect to (a function)  $f$ .

**definition**

$$\text{IsContinuous}(\tau_1, \tau_2, f) \equiv (\forall U \in \tau_2. f^{-1}(U) \in \tau_1)$$

A trivial example of a continuous function - identity is continuous.

```
lemma id_cont: shows IsContinuous( $\tau, \tau, \text{id}(\bigcup \tau)$ ) using IsContinuous_def
vimage_id_same
```

```
proof -
```

```
  { fix U assume U  $\in \tau$ 
    then have  $\text{id}(\bigcup \tau)^{-1}(U) = U$  using vimage_id_same by auto
    with 'U  $\in \tau$ ' have  $\text{id}(\bigcup \tau)^{-1}(U) \in \tau$  by simp
  } then show IsContinuous( $\tau, \tau, \text{id}(\bigcup \tau)$ ) using IsContinuous_def
    by simp
```

```
qed
```

We will work with a pair of topological spaces. The following locale sets up our context that consists of two topologies  $\tau_1, \tau_2$  and a continuous function  $f : X_1 \rightarrow X_2$ , where  $X_i$  is defined as  $\bigcup \tau_i$  for  $i = 1, 2$ . We also define notation  $\text{cl}_1(A)$  and  $\text{cl}_2(A)$  for closure of a set  $A$  in topologies  $\tau_1$  and  $\tau_2$ , respectively.

```
locale two_top_spaces0 =
```

```
  fixes  $\tau_1$ 
  assumes tau1_is_top:  $\tau_1$  {is a topology}
```

```

fixes  $\tau_2$ 
assumes tau2_is_top:  $\tau_2$  {is a topology}

fixes  $X_1$ 
defines X1_def [simp]:  $X_1 \equiv \bigcup \tau_1$ 

fixes  $X_2$ 
defines X2_def [simp]:  $X_2 \equiv \bigcup \tau_2$ 

fixes f
assumes fmapAssum:  $f: X_1 \rightarrow X_2$ 

fixes isContinuous ( $\_$  {is continuous} [50] 50)
defines isContinuous_def [simp]:  $g$  {is continuous}  $\equiv$  IsContinuous( $\tau_1, \tau_2, g$ )

fixes  $cl_1$ 
defines cl1_def [simp]:  $cl_1(A) \equiv \text{Closure}(A, \tau_1)$ 

fixes  $cl_2$ 
defines cl2_def [simp]:  $cl_2(A) \equiv \text{Closure}(A, \tau_2)$ 

```

First we show that theorems proven in locale topology0 are valid when applied to topologies  $\tau_1$  and  $\tau_2$ .

```

lemma (in two_top_spaces0) topol_cntxs_valid:
  shows topology0( $\tau_1$ ) and topology0( $\tau_2$ )
  using tau1_is_top tau2_is_top topology0_def by auto

```

For continuous functions the inverse image of a closed set is closed.

```

lemma (in two_top_spaces0) TopZF_2_1_L1:
  assumes A1:  $f$  {is continuous} and A2:  $D$  {is closed in}  $\tau_2$ 
  shows  $f^{-1}(D)$  {is closed in}  $\tau_1$ 
proof -
  from fmapAssum have  $f^{-1}(D) \subseteq X_1$  using func1_1_L3 by simp
  moreover from fmapAssum have  $f^{-1}(X_2 - D) = X_1 - f^{-1}(D)$ 
    using Pi_iff function_vimage_Diff func1_1_L4 by auto
  ultimately have  $X_1 - f^{-1}(X_2 - D) = f^{-1}(D)$  by auto
  moreover from A1 A2 have  $(X_1 - f^{-1}(X_2 - D))$  {is closed in}  $\tau_1$ 
    using IsClosed_def IsContinuous_def topol_cntxs_valid topology0.Top_3_L9
    by simp
  ultimately show  $f^{-1}(D)$  {is closed in}  $\tau_1$  by simp
qed

```

If the inverse image of every closed set is closed, then the image of a closure is contained in the closure of the image.

```

lemma (in two_top_spaces0) TopZF_2_1_L2:
  assumes A1:  $\forall D. ((D \text{ {is closed in} } \tau_2) \longrightarrow f^{-1}(D) \text{ {is closed in} } \tau_1)$ 
  and A2:  $A \subseteq X_1$ 

```



```

shows f(cl1(A)) ⊆ cl2(f(A))
proof -
  from fmapAssum have f(A) ⊆ cl2(f(A))
    using func1_1_L6 topol_cntxs_valid topology0.cl_contains_set
    by simp
  with fmapAssum have f-(f(A)) ⊆ f-(cl2(f(A)))
    by auto
  moreover from fmapAssum A2 have A ⊆ f-(f(A))
    using func1_1_L9 by simp
  ultimately have A ⊆ f-(cl2(f(A))) by auto
  with fmapAssum A1 have f(cl1(A)) ⊆ f(f-(cl2(f(A))))
    using func1_1_L6 func1_1_L8 IsClosed_def
    topol_cntxs_valid topology0.cl_is_closed topology0.Top_3_L13
    by simp
  moreover from fmapAssum have f(f-(cl2(f(A)))) ⊆ cl2(f(A))
    using fun_is_function function_image_vimage by simp
  ultimately show f(cl1(A)) ⊆ cl2(f(A))
    by auto
qed

```

If  $f(\overline{A}) \subseteq \overline{f(A)}$  (the image of the closure is contained in the closure of the image), then  $\overline{f^{-1}(B)} \subseteq f^{-1}(\overline{B})$  (the inverse image of the closure contains the closure of the inverse image).

```

lemma (in two_top_spaces0) Top_ZF_2_1_L3:
  assumes A1: ∀ A. ( A ⊆ X1 ⟶ f(cl1(A)) ⊆ cl2(f(A)) )
  shows ∀ B. ( B ⊆ X2 ⟶ cl1(f-(B)) ⊆ f-(cl2(B)) )
proof -
  { fix B assume B ⊆ X2
    from fmapAssum A1 have f(cl1(f-(B))) ⊆ cl2(f(f-(B)))
      using func1_1_L3 by simp
    moreover from fmapAssum 'B ⊆ X2' have cl2(f(f-(B))) ⊆ cl2(B)
      using fun_is_function function_image_vimage func1_1_L6
      topol_cntxs_valid topology0.top_closure_mono
      by simp
    ultimately have f-(f(cl1(f-(B)))) ⊆ f-(cl2(B))
      using fmapAssum fun_is_function by auto
    moreover from fmapAssum 'B ⊆ X2' have
      cl1(f-(B)) ⊆ f-(f(cl1(f-(B))))
      using func1_1_L3 func1_1_L9 IsClosed_def
      topol_cntxs_valid topology0.cl_is_closed by simp
    ultimately have cl1(f-(B)) ⊆ f-(cl2(B)) by auto
  } then show thesis by simp
qed

```

If  $\overline{f^{-1}(B)} \subseteq f^{-1}(\overline{B})$  (the inverse image of a closure contains the closure of the inverse image), then the function is continuous. This lemma closes a series of implications in lemmas Top\_ZF\_2\_1\_L1, Top\_ZF\_2\_1\_L2 and Top\_ZF\_2\_1\_L3 showing equivalence of four definitions of continuity.

```

lemma (in two_top_spaces0) Top_ZF_2_1_L4:
  assumes A1:  $\forall B. (B \subseteq X_2 \longrightarrow \text{cl}_1(f(B)) \subseteq f(\text{cl}_2(B)))$ 
  shows f {is continuous}
proof -
  { fix U assume U  $\in \tau_2$ 
    then have  $(X_2 - U)$  {is closed in}  $\tau_2$ 
      using topol_cntxs_valid topology0.Top_3_L9 by simp
    moreover have  $X_2 - U \subseteq \bigcup \tau_2$  by auto
    ultimately have  $\text{cl}_2(X_2 - U) = X_2 - U$ 
      using topol_cntxs_valid topology0.Top_3_L8 by simp
    moreover from A1 have  $\text{cl}_1(f(X_2 - U)) \subseteq f(\text{cl}_2(X_2 - U))$ 
      by auto
    ultimately have  $\text{cl}_1(f(X_2 - U)) \subseteq f(X_2 - U)$  by simp
    moreover from fmapAssum have  $f(X_2 - U) \subseteq \text{cl}_1(f(X_2 - U))$ 
      using func1_1_L3 topol_cntxs_valid topology0.cl_contains_set
      by simp
    ultimately have  $f(X_2 - U)$  {is closed in}  $\tau_1$ 
      using fmapAssum func1_1_L3 topol_cntxs_valid topology0.Top_3_L8
      by auto
    with fmapAssum have  $f(U) \in \tau_1$ 
      using fun_is_function function_vimage_Diff func1_1_L4
      func1_1_L3 IsClosed_def double_complement by simp
  } then have  $\forall U \in \tau_2. f(U) \in \tau_1$  by simp
  then show thesis using IsContinuous_def by simp
qed

```

Another condition for continuity: it is sufficient to check if the inverse image of every set in a base is open.

```

lemma (in two_top_spaces0) Top_ZF_2_1_L5:
  assumes A1: B {is a base for}  $\tau_2$  and A2:  $\forall U \in B. f(U) \in \tau_1$ 
  shows f {is continuous}
proof -
  { fix V assume A3:  $V \in \tau_1$ 
    with A1 obtain A where  $A \subseteq B$   $V = \bigcup A$ 
      using IsAbaseFor_def by auto
    with A2 have  $\{f(U). U \in A\} \subseteq \tau_1$  by auto
    with tau1_is_top have  $\bigcup \{f(U). U \in A\} \in \tau_1$ 
      using IsATopology_def by simp
    moreover from ' $A \subseteq B$ ' ' $V = \bigcup A$ ' have  $f(V) = \bigcup \{f(U). U \in A\}$ 
      by auto
    ultimately have  $f(V) \in \tau_1$  by simp
  } then show f {is continuous} using IsContinuous_def
    by simp
qed

```

We can strengthen the previous lemma: it is sufficient to check if the inverse image of every set in a subbase is open. The proof is rather awkward, as usual when we deal with general intersections. We have to keep track of the case when the collection is empty.

```

lemma (in two_top_spaces0) Top_ZF_2_1_L6:
  assumes A1: B {is a subbase for}  $\tau_2$  and A2:  $\forall U \in B. f^{-1}(U) \in \tau_1$ 
  shows f {is continuous}
proof -
  let C =  $\{\bigcap A. A \in \text{FinPow}(B)\}$ 
  from A1 have C {is a base for}  $\tau_2$ 
    using IsAsubBaseFor_def by simp
  moreover have  $\forall U \in C. f^{-1}(U) \in \tau_1$ 
  proof
    fix U assume  $U \in C$ 
    { assume  $f^{-1}(U) = \emptyset$ 
      with tau1_is_top have  $f^{-1}(U) \in \tau_1$ 
    }
  using empty_open by simp }
  moreover
    { assume  $f^{-1}(U) \neq \emptyset$ 
      then have  $U \neq \emptyset$  by (rule func1_1_L13)
      moreover from 'U ∈ C' obtain A where
        A ∈ FinPow(B) and  $U = \bigcap A$ 
    }
  by auto
    ultimately have  $\bigcap A \neq \emptyset$  by simp
    then have  $A \neq \emptyset$  by (rule inter_nonempty)
    then have  $\{f^{-1}(W). W \in A\} \neq \emptyset$  by simp
    moreover from A2 'A ∈ FinPow(B)' have  $\{f^{-1}(W). W \in A\} \in \text{FinPow}(\tau_1)$ 
  by (rule fin_image_fin)
    ultimately have  $\bigcap \{f^{-1}(W). W \in A\} \in \tau_1$ 
  using topol_cntxs_valid topology0.fin_inter_open_open by simp
  moreover
    from 'A ∈ FinPow(B)' have  $A \subseteq B$  using FinPow_def by simp
    with tau2_is_top A1 have  $A \subseteq \text{Pow}(X_2)$ 
  using IsAsubBaseFor_def IsATopology_def by auto
    with fmapAssum 'A ≠ ∅' 'U =  $\bigcap A$ ' have  $f^{-1}(U) = \bigcap \{f^{-1}(W). W \in A\}$ 
  using func1_1_L12 by simp
    ultimately have  $f^{-1}(U) \in \tau_1$  by simp }
  ultimately show  $f^{-1}(U) \in \tau_1$  by blast
qed
ultimately show f {is continuous}
  using Top_ZF_2_1_L5 by simp
qed

```

A dual of Top\_ZF\_2\_1\_L5: a function that maps base sets to open sets is open.

```

lemma (in two_top_spaces0) base_image_open:
  assumes A1: B {is a base for}  $\tau_1$  and A2:  $\forall B \in \mathcal{B}. f(B) \in \tau_2$  and A3:
    U ∈  $\tau_1$ 
  shows f(U) ∈  $\tau_2$ 
proof -
  from A1 A3 obtain  $\mathcal{E}$  where  $\mathcal{E} \in \text{Pow}(B)$  and  $U = \bigcup \mathcal{E}$  using Top_1_2_L1
  by blast
  with A1 have  $f(U) = \bigcup \{f(E). E \in \mathcal{E}\}$  using Top_1_2_L5 fmapAssum image_of_Union
  by auto

```

```

moreover
from A2 ' $\mathcal{E} \in \text{Pow}(\mathcal{B})$ ' have  $\{f(E). E \in \mathcal{E}\} \in \text{Pow}(\tau_2)$  by auto
then have  $\bigcup \{f(E). E \in \mathcal{E}\} \in \tau_2$  using tau2_is_top IsATopology_def by
simp
ultimately show thesis using tau2_is_top IsATopology_def by auto
qed

```

A composition of two continuous functions is continuous.

```

lemma comp_cont: assumes IsContinuous(T,S,f) and IsContinuous(S,R,g)
shows IsContinuous(T,R,g  $\circ$  f)
using assms IsContinuous_def vimage_comp by simp

```

A composition of three continuous functions is continuous.

```

lemma comp_cont3:
assumes IsContinuous(T,S,f) and IsContinuous(S,R,g) and IsContinuous(R,P,h)
shows IsContinuous(T,P,h  $\circ$  g  $\circ$  f)
using assms IsContinuous_def vimage_comp by simp

```

## 45.2 Homeomorphisms

This section studies "homeomorphisms" - continuous bijections whose inverses are also continuous. Notions that are preserved by (commute with) homeomorphisms are called "topological invariants".

Homeomorphism is a bijection that preserves open sets.

```

definition IsAhomeomorphism(T,S,f)  $\equiv$ 
  f  $\in$  bij( $\bigcup T, \bigcup S$ )  $\wedge$  IsContinuous(T,S,f)  $\wedge$  IsContinuous(S,T,converse(f))

```

Inverse (converse) of a homeomorphism is a homeomorphism.

```

lemma homeo_inv: assumes IsAhomeomorphism(T,S,f)
shows IsAhomeomorphism(S,T,converse(f))
using assms IsAhomeomorphism_def bij_converse_bij bij_converse_converse
by auto

```

Homeomorphisms are open maps.

```

lemma homeo_open: assumes IsAhomeomorphism(T,S,f) and U $\in$ T
shows f(U)  $\in$  S
using assms image_converse IsAhomeomorphism_def IsContinuous_def by
simp

```

A continuous bijection that is an open map is a homeomorphism.

```

lemma bij_cont_open_homeo:
assumes f  $\in$  bij( $\bigcup T, \bigcup S$ ) and IsContinuous(T,S,f) and  $\forall U \in T. f(U) \in S$ 
shows IsAhomeomorphism(T,S,f)
using assms image_converse IsAhomeomorphism_def IsContinuous_def by
auto

```

A continuous bijection that maps base to open sets is a homeomorphism.

```
lemma (in two_top_spaces0) bij_base_open_homeo:
  assumes A1:  $f \in \text{bij}(X_1, X_2)$  and A2:  $\mathcal{B}$  {is a base for}  $\tau_1$  and A3:  $\mathcal{C}$ 
  {is a base for}  $\tau_2$  and
  A4:  $\forall U \in \mathcal{C}. f^{-1}(U) \in \tau_1$  and A5:  $\forall V \in \mathcal{B}. f(V) \in \tau_2$ 
  shows IsAhomeomorphism( $\tau_1, \tau_2, f$ )
  using assms tau2_is_top tau1_is_top bij_converse_bij bij_is_fun two_top_spaces0_def

  image_converse two_top_spaces0.Top_ZF_2_1_L5 IsAhomeomorphism_def by
simp
```

A bijections that maps base to base is a homeomorphisms.

```
lemma (in two_top_spaces0) bij_base_homeo:
  assumes A1:  $f \in \text{bij}(X_1, X_2)$  and A2:  $\mathcal{B}$  {is a base for}  $\tau_1$  and
  A3:  $\{f(B). B \in \mathcal{B}\}$  {is a base for}  $\tau_2$ 
  shows IsAhomeomorphism( $\tau_1, \tau_2, f$ )
proof -
  note A1
  moreover have  $f$  {is continuous}
  proof -
    { fix C assume  $C \in \{f(B). B \in \mathcal{B}\}$ 
      then obtain B where  $B \in \mathcal{B}$  and I:  $C = f(B)$  by auto
      with A2 have  $B \subseteq X_1$  using Top_1_2_L5 by auto
      with A1 A2 ' $B \in \mathcal{B}$ ' I have  $f^{-1}(C) \in \tau_1$ 
        using bij_def inj_vimage_image base_sets_open by auto
    } hence  $\forall C \in \{f(B). B \in \mathcal{B}\}. f^{-1}(C) \in \tau_1$  by auto
    with A3 show thesis by (rule Top_ZF_2_1_L5)
  qed
  moreover
  from A3 have  $\forall B \in \mathcal{B}. f(B) \in \tau_2$  using base_sets_open by auto
  with A2 have  $\forall U \in \tau_1. f(U) \in \tau_2$  using base_image_open by simp
  ultimately show thesis using bij_cont_open_homeo by simp
qed
```

Interior is a topological invariant.

```
theorem int_top_invariant: assumes A1:  $A \subseteq \bigcup T$  and A2: IsAhomeomorphism( $T, S, f$ )
  shows  $f(\text{Interior}(A, T)) = \text{Interior}(f(A), S)$ 
proof -
  let  $\mathcal{A} = \{U \in T. U \subseteq A\}$ 
  have I:  $\{f(U). U \in \mathcal{A}\} = \{V \in S. V \subseteq f(A)\}$ 
  proof
    from A2 show  $\{f(U). U \in \mathcal{A}\} \subseteq \{V \in S. V \subseteq f(A)\}$ 
      using homeo_open by auto
    { fix V assume  $V \in \{V \in S. V \subseteq f(A)\}$ 
      hence  $V \in S$  and II:  $V \subseteq f(A)$  by auto
      let  $U = f^{-1}(V)$ 
      from II have  $U \subseteq f^{-1}(f(A))$  by auto
      moreover from assms have  $f^{-1}(f(A)) = A$ 
        using IsAhomeomorphism_def bij_def inj_vimage_image by auto
    }
```

```

    moreover from A2 'V ∈ S' have U ∈ T
      using IsAhomeomorphism_def IsContinuous_def by simp
    moreover
    from 'V ∈ S' have V ⊆ ⋃ S by auto
    with A2 have V = f(U)
      using IsAhomeomorphism_def bij_def surj_image_vimage by auto
    ultimately have V ∈ {f(U). U ∈ A} by auto
  } thus {V ∈ S. V ⊆ f(A)} ⊆ {f(U). U ∈ A} by auto
qed
have f(Interior(A,T)) = f(⋃ A) unfolding Interior_def by simp
also from A2 have ... = ⋃ {f(U). U ∈ A}
  using IsAhomeomorphism_def bij_def inj_def image_of_Union by auto
also from I have ... = Interior(f(A),S) unfolding Interior_def by simp
finally show thesis by simp
qed

```

### 45.3 Topologies induced by mappings

In this section we consider various ways a topology may be defined on a set that is the range (or the domain) of a function whose domain (or range) is a topological space.

A bijection from a topological space induces a topology on the range.

**theorem** `bij_induced_top`: assumes A1:  $T$  {is a topology} and A2:  $f \in \text{bij}(\bigcup T, Y)$  shows  
 $\{f(U). U \in T\}$  {is a topology} and  
 $\{ \{f(x). x \in U\}. U \in T \}$  {is a topology} and  
 $(\bigcup \{f(U). U \in T\}) = Y$  and  
 $\text{IsAhomeomorphism}(T, \{f(U). U \in T\}, f)$

**proof** -

```

  from A2 have f ∈ inj(⋃ T, Y) using bij_def by simp
  then have f: ⋃ T → Y using inj_def by simp
  let S = {f(U). U ∈ T}
  { fix M assume M ∈ Pow(S)
    let M_T = {f-(V). V ∈ M}
    have M_T ⊆ T
      proof
        fix W assume W ∈ M_T
        then obtain V where V ∈ M and I: W = f-(V) by auto
        with 'M ∈ Pow(S)' have V ∈ S by auto
        then obtain U where U ∈ T and V = f(U) by auto
        with I have W = f-(f(U)) by simp
        with 'f ∈ inj(⋃ T, Y)' 'U ∈ T' have W = U using inj_vimage_image
      by blast
    with 'U ∈ T' show W ∈ T by simp
  }
qed
with A1 have (⋃ M_T) ∈ T using IsATopology_def by simp
hence f(⋃ M_T) ∈ S by auto
moreover have f(⋃ M_T) = ⋃ M

```

```

proof -
  from 'f:  $\bigcup T \rightarrow Y$ ' 'M_T  $\subseteq T$ ' have f( $\bigcup M_T$ ) =  $\bigcup \{f(U). U \in M_T\}$ 
    using image_of_Union by auto
  moreover have {f(U). U  $\in M_T$ } = M
  proof -
    from 'f:  $\bigcup T \rightarrow Y$ ' have  $\forall U \in T. f(U) \subseteq Y$  using func1_1_L6 by simp
    with 'M  $\in \text{Pow}(S)$ ' have M  $\subseteq \text{Pow}(Y)$  by auto
    with A2 show {f(U). U  $\in M_T$ } = M using bij_def surj_subsets by
auto
    qed
    ultimately show f( $\bigcup M_T$ ) =  $\bigcup M$  by simp
  qed
  ultimately have  $\bigcup M \in S$  by auto
} then have  $\forall M \in \text{Pow}(S). \bigcup M \in S$  by auto
moreover
{ fix U V assume U  $\in S$  V  $\in S$ 
  then obtain U_T V_T where U_T  $\in T$  V_T  $\in T$  and
    I: U = f(U_T) V = f(V_T)
    by auto
  with A1 have U_T  $\cap$  V_T  $\in T$  using IsATopology_def by simp
  hence f(U_T  $\cap$  V_T)  $\in S$  by auto
  moreover have f(U_T  $\cap$  V_T) = U  $\cap$  V
  proof -
    from 'U_T  $\in T$ ' 'V_T  $\in T$ ' have U_T  $\subseteq \bigcup T$  V_T  $\subseteq \bigcup T$ 
      using bij_def by auto
    with 'f  $\in \text{inj}(\bigcup T, Y)$ ' I show f(U_T  $\cap$  V_T) = U  $\cap$  V using inj_image_inter

    by simp
  qed
  ultimately have U  $\cap$  V  $\in S$  by simp
} then have  $\forall U \in S. \forall V \in S. U \cap V \in S$  by auto
ultimately show S {is a topology} using IsATopology_def by simp
moreover from 'f:  $\bigcup T \rightarrow Y$ ' have  $\forall U \in T. f(U) = \{f(x). x \in U\}$ 
  using func_imagedef by blast
ultimately show { {f(x). x  $\in U$ }. U  $\in T$ } {is a topology} by simp
show  $\bigcup S = Y$ 
proof
  from 'f:  $\bigcup T \rightarrow Y$ ' have  $\forall U \in T. f(U) \subseteq Y$  using func1_1_L6 by simp
  thus  $\bigcup S \subseteq Y$  by auto
  from A1 have f( $\bigcup T$ )  $\subseteq \bigcup S$  using IsATopology_def by auto
  with A2 show Y  $\subseteq \bigcup S$  using bij_def surj_range_image_domain
    by auto
qed
show IsAhomeomorphism(T, S, f)
proof -
  from A2 ' $\bigcup S = Y$ ' have f  $\in \text{bij}(\bigcup T, \bigcup S)$  by simp
  moreover have IsContinuous(T, S, f)
  proof -
    { fix V assume V  $\in S$ 

```

```

    then obtain U where U ∈ T and V = f(U) by auto
    hence U ⊆ ⋃ T and f-(V) = f-(f(U)) by auto
    with 'f ∈ inj(⋃ T, Y)' 'U ∈ T' have f-(V) ∈ T using inj_vimage_image

    by simp
  } then show IsContinuous(T, S, f) unfolding IsContinuous_def by auto
qed
ultimately showIsAhomeomorphism(T, S, f) using bij_cont_open_homeo

by auto
qed
qed

```

#### 45.4 Partial functions and continuity

Suppose we have two topologies  $\tau_1, \tau_2$  on sets  $X_i = \bigcup \tau_i, i = 1, 2$ . Consider some function  $f : A \rightarrow X_2$ , where  $A \subseteq X_1$  (we will call such function "partial"). In such situation we have two natural possibilities for the pairs of topologies with respect to which this function may be continuous. One is obviously the original  $\tau_1, \tau_2$  and in the second one the first element of the pair is the topology relative to the domain of the function:  $\{A \cap U | U \in \tau_1\}$ . These two possibilities are not exactly the same and the goal of this section is to explore the differences.

If a function is continuous, then its restriction is continuous in relative topology.

```

lemma (in two_top_spaces0) restr_cont:
  assumes A1: A ⊆ X1 and A2: f {is continuous}
  shows IsContinuous(τ1 {restricted to} A, τ2, restrict(f, A))
proof -
  let g = restrict(f, A)
  { fix U assume U ∈ τ2
    with A2 have f-(U) ∈ τ1 using IsContinuous_def by simp
    moreover from A1 have g-(U) = f-(U) ∩ A
      using fmapAssum func1_2_L1 by simp
    ultimately have g-(U) ∈ (τ1 {restricted to} A)
      using RestrictedTo_def by auto
  } then show thesis using IsContinuous_def by simp
qed

```

If a function is continuous, then it is continuous when we restrict the topology on the range to the image of the domain.

```

lemma (in two_top_spaces0) restr_image_cont:
  assumes A1: f {is continuous}
  shows IsContinuous(τ1, τ2 {restricted to} f(X1), f)
proof -
  have ∀ U ∈ τ2 {restricted to} f(X1). f-(U) ∈ τ1
  proof

```



```

    fix U assume U ∈  $\tau_2$  {restricted to}  $f(X_1)$ 
    then obtain V where V ∈  $\tau_2$  and U = V ∩  $f(X_1)$ 
      using RestrictedTo_def by auto
    with A1 show  $f(U) \in \tau_1$ 
      using fmapAssum inv_im_inter_im IsContinuous_def
      by simp
  qed
  then show thesis using IsContinuous_def by simp
qed

```

A combination of `restr_cont` and `restr_image_cont`.

```

lemma (in two_top_spaces0) restr_restr_image_cont:
  assumes A1:  $A \subseteq X_1$  and A2:  $f$  {is continuous} and
  A3:  $g = \text{restrict}(f, A)$  and
  A4:  $\tau_3 = \tau_1$  {restricted to} A
  shows IsContinuous( $\tau_3$ ,  $\tau_2$  {restricted to}  $g(A), g$ )
proof -
  from A1 A4 have  $\bigcup \tau_3 = A$ 
    using union_restrict by auto
  have two_top_spaces0( $\tau_3$ ,  $\tau_2$ ,  $g$ )
  proof -
    from A4 have
       $\tau_3$  {is a topology} and  $\tau_2$  {is a topology}
      using tau1_is_top tau2_is_top
    topology0_def topology0.Top_1_L4 by auto
    moreover from A1 A3 ' $\bigcup \tau_3 = A$ ' have  $g: \bigcup \tau_3 \rightarrow \bigcup \tau_2$ 
      using fmapAssum restrict_type2 by simp
    ultimately show thesis using two_top_spaces0_def
      by simp
  qed
  moreover from assms have IsContinuous( $\tau_3$ ,  $\tau_2$ ,  $g$ )
    using restr_cont by simp
  ultimately have IsContinuous( $\tau_3$ ,  $\tau_2$  {restricted to}  $g(\bigcup \tau_3), g$ )
    by (rule two_top_spaces0.restr_image_cont)
  moreover note ' $\bigcup \tau_3 = A$ '
  ultimately show thesis by simp
qed

```

We need a context similar to `two_top_spaces0` but without the global function  $f: X_1 \rightarrow X_2$ .

`locale two_top_spaces1 =`

```

  fixes  $\tau_1$ 
  assumes tau1_is_top:  $\tau_1$  {is a topology}

  fixes  $\tau_2$ 
  assumes tau2_is_top:  $\tau_2$  {is a topology}

  fixes  $X_1$ 

```

```
defines X1_def [simp]:  $X_1 \equiv \bigcup \tau_1$ 
```

```
fixes X2
```

```
defines X2_def [simp]:  $X_2 \equiv \bigcup \tau_2$ 
```

If a partial function  $g : X_1 \supseteq A \rightarrow X_2$  is continuous with respect to  $(\tau_1, \tau_2)$ , then  $A$  is open (in  $\tau_1$ ) and the function is continuous in the relative topology.

```
lemma (in two_top_spaces1) partial_fun_cont:
  assumes A1:  $g:A \rightarrow X_2$  and A2:  $\text{IsContinuous}(\tau_1, \tau_2, g)$ 
  shows  $A \in \tau_1$  and  $\text{IsContinuous}(\tau_1 \text{ \{restricted to\} } A, \tau_2, g)$ 
proof -
  from A2 have  $g^{-1}(X_2) \in \tau_1$ 
    using tau2_is_top IsATopology_def IsContinuous_def by simp
  with A1 show  $A \in \tau_1$  using func1_1_L4 by simp
  { fix V assume  $V \in \tau_2$ 
    with A2 have  $g^{-1}(V) \in \tau_1$  using IsContinuous_def by simp
    moreover
    from A1 have  $g^{-1}(V) \subseteq A$  using func1_1_L3 by simp
    hence  $g^{-1}(V) = A \cap g^{-1}(V)$  by auto
    ultimately have  $g^{-1}(V) \in (\tau_1 \text{ \{restricted to\} } A)$ 
      using RestrictedTo_def by auto
  } then show  $\text{IsContinuous}(\tau_1 \text{ \{restricted to\} } A, \tau_2, g)$ 
    using IsContinuous_def by simp
qed
```

For partial function defined on open sets continuity in the whole and relative topologies are the same.

```
lemma (in two_top_spaces1) part_fun_on_open_cont:
  assumes A1:  $g:A \rightarrow X_2$  and A2:  $A \in \tau_1$ 
  shows  $\text{IsContinuous}(\tau_1, \tau_2, g) \longleftrightarrow$ 
     $\text{IsContinuous}(\tau_1 \text{ \{restricted to\} } A, \tau_2, g)$ 
proof
  assume  $\text{IsContinuous}(\tau_1, \tau_2, g)$ 
  with A1 show  $\text{IsContinuous}(\tau_1 \text{ \{restricted to\} } A, \tau_2, g)$ 
    using partial_fun_cont by simp
next
  assume I:  $\text{IsContinuous}(\tau_1 \text{ \{restricted to\} } A, \tau_2, g)$ 
  { fix V assume  $V \in \tau_2$ 
    with I have  $g^{-1}(V) \in (\tau_1 \text{ \{restricted to\} } A)$ 
      using IsContinuous_def by simp
    then obtain W where  $W \in \tau_1$  and  $g^{-1}(V) = A \cap W$ 
      using RestrictedTo_def by auto
    with A2 have  $g^{-1}(V) \in \tau_1$  using tau1_is_top IsATopology_def
      by simp
  } then show  $\text{IsContinuous}(\tau_1, \tau_2, g)$  using IsContinuous_def
    by simp
qed
```

## 45.5 Product topology and continuity

We start with three topological spaces  $(\tau_1, X_1)$ ,  $(\tau_2, X_2)$  and  $(\tau_3, X_3)$  and a function  $f : X_1 \times X_2 \rightarrow X_3$ . We will study the properties of  $f$  with respect to the product topology  $\tau_1 \times \tau_2$  and  $\tau_3$ . This situation is similar as in locale `two_top_spaces0` but the first topological space is assumed to be a product of two topological spaces.

First we define a locale with three topological spaces.

```
locale prod_top_spaces0 =

  fixes  $\tau_1$ 
  assumes tau1_is_top:  $\tau_1$  {is a topology}

  fixes  $\tau_2$ 
  assumes tau2_is_top:  $\tau_2$  {is a topology}

  fixes  $\tau_3$ 
  assumes tau3_is_top:  $\tau_3$  {is a topology}

  fixes  $X_1$ 
  defines X1_def [simp]:  $X_1 \equiv \bigcup_{\tau_1}$ 

  fixes  $X_2$ 
  defines X2_def [simp]:  $X_2 \equiv \bigcup_{\tau_2}$ 

  fixes  $X_3$ 
  defines X3_def [simp]:  $X_3 \equiv \bigcup_{\tau_3}$ 

  fixes  $\eta$ 
  defines eta_def [simp]:  $\eta \equiv \text{ProductTopology}(\tau_1, \tau_2)$ 
```

Fixing the first variable in a two-variable continuous function results in a continuous function.

```
lemma (in prod_top_spaces0) fix_1st_var_cont:
  assumes  $f: X_1 \times X_2 \rightarrow X_3$  and IsContinuous( $\eta, \tau_3, f$ )
  and  $x \in X_1$ 
  shows IsContinuous( $\tau_2, \tau_3, \text{Fix1stVar}(f, x)$ )
  using assms fix_1st_var_vimage IsContinuous_def tau1_is_top tau2_is_top
  prod_sec_open1 by simp
```

Fixing the second variable in a two-variable continuous function results in a continuous function.

```
lemma (in prod_top_spaces0) fix_2nd_var_cont:
  assumes  $f: X_1 \times X_2 \rightarrow X_3$  and IsContinuous( $\eta, \tau_3, f$ )
  and  $y \in X_2$ 
  shows IsContinuous( $\tau_1, \tau_3, \text{Fix2ndVar}(f, y)$ )
  using assms fix_2nd_var_vimage IsContinuous_def tau1_is_top tau2_is_top
```

prod\_sec\_open2 by simp

Having two continuous mappings we can construct a third one on the cartesian product of the domains.

```

lemma cart_prod_cont:
  assumes A1:  $\tau_1$  {is a topology}  $\tau_2$  {is a topology} and
  A2:  $\eta_1$  {is a topology}  $\eta_2$  {is a topology} and
  A3a:  $f_1: \bigcup \tau_1 \rightarrow \bigcup \eta_1$  and A3b:  $f_2: \bigcup \tau_2 \rightarrow \bigcup \eta_2$  and
  A4: IsContinuous( $\tau_1, \eta_1, f_1$ ) IsContinuous( $\tau_2, \eta_2, f_2$ ) and
  A5:  $g = \{\langle p, \langle f_1(\text{fst}(p)), f_2(\text{snd}(p)) \rangle \rangle \mid p \in \bigcup \tau_1 \times \bigcup \tau_2\}$ 
  shows IsContinuous(ProductTopology( $\tau_1, \tau_2$ ), ProductTopology( $\eta_1, \eta_2$ ), g)
proof -
  let  $\tau = \text{ProductTopology}(\tau_1, \tau_2)$ 
  let  $\eta = \text{ProductTopology}(\eta_1, \eta_2)$ 
  let  $X_1 = \bigcup \tau_1$ 
  let  $X_2 = \bigcup \tau_2$ 
  let  $Y_1 = \bigcup \eta_1$ 
  let  $Y_2 = \bigcup \eta_2$ 
  let B = ProductCollection( $\eta_1, \eta_2$ )
  from A1 A2 have  $\tau$  {is a topology} and  $\eta$  {is a topology}
    using Top_1_4_T1 by auto
  moreover have  $g: X_1 \times X_2 \rightarrow Y_1 \times Y_2$ 
  proof -
    { fix p assume  $p \in X_1 \times X_2$ 
      hence  $\text{fst}(p) \in X_1$  and  $\text{snd}(p) \in X_2$  by auto
      from A3a ' $\text{fst}(p) \in X_1$ ' have  $f_1(\text{fst}(p)) \in Y_1$ 
        by (rule apply_funtype)
      moreover from A3b ' $\text{snd}(p) \in X_2$ ' have  $f_2(\text{snd}(p)) \in Y_2$ 
        by (rule apply_funtype)
      ultimately have  $\langle f_1(\text{fst}(p)), f_2(\text{snd}(p)) \rangle \in \bigcup \eta_1 \times \bigcup \eta_2$  by auto
    } hence  $\forall p \in X_1 \times X_2. \langle f_1(\text{fst}(p)), f_2(\text{snd}(p)) \rangle \in Y_1 \times Y_2$ 
      by simp
    with A5 show  $g: X_1 \times X_2 \rightarrow Y_1 \times Y_2$  using ZF_fun_from_total
      by simp
  qed
  moreover from A1 A2 have  $\bigcup \tau = X_1 \times X_2$  and  $\bigcup \eta = Y_1 \times Y_2$ 
    using Top_1_4_T1 by auto
  ultimately have two_top_spaces0( $\tau, \eta, g$ ) using two_top_spaces0_def
    by simp
  moreover from A2 have B {is a base for}  $\eta$  using Top_1_4_T1
    by simp
  moreover have  $\forall U \in B. g^{-1}(U) \in \tau$ 
  proof
    fix U assume  $U \in B$ 
    then obtain V W where  $V \in \eta_1$   $W \in \eta_2$  and  $U = V \times W$ 
      using ProductCollection_def by auto
    with A3a A3b A5 have  $g^{-1}(U) = f_1^{-1}(V) \times f_2^{-1}(W)$ 
      using cart_prod_fun_vimage by simp
    moreover from A1 A4 ' $V \in \eta_1$ ' ' $W \in \eta_2$ ' have  $f_1^{-1}(V) \times f_2^{-1}(W) \in \tau$ 

```

```

      using IsContinuous_def prod_open_open_prod by simp
      ultimately show  $g^{-1}(U) \in \tau$  by simp
    qed
    ultimately show thesis using two_top_spaces0.Top_ZF_2_1_L5
      by simp
  qed

```

A special case of `cart_prod_cont` when the function acting on the second axis is the identity.

```

lemma cart_prod_cont1:
  assumes A1:  $\tau_1$  {is a topology} and A1a:  $\tau_2$  {is a topology} and
    A2:  $\eta_1$  {is a topology} and
    A3:  $f_1: \bigcup \tau_1 \rightarrow \bigcup \eta_1$  and A4: IsContinuous( $\tau_1, \eta_1, f_1$ ) and
    A5:  $g = \{\langle p, \langle f_1(\text{fst}(p)), \text{snd}(p) \rangle \rangle \mid p \in \bigcup \tau_1 \times \bigcup \tau_2\}$ 
  shows IsContinuous(ProductTopology( $\tau_1, \tau_2$ ), ProductTopology( $\eta_1, \tau_2$ ),  $g$ )
proof -
  let  $f_2 = \text{id}(\bigcup \tau_2)$ 
  have  $\forall x \in \bigcup \tau_2. f_2(x) = x$  using id_conv by blast
  hence I:  $\forall p \in \bigcup \tau_1 \times \bigcup \tau_2. \text{snd}(p) = f_2(\text{snd}(p))$  by simp
  note A1 A1a A2 A1a A3
  moreover have  $f_2: \bigcup \tau_2 \rightarrow \bigcup \tau_2$  using id_type by simp
  moreover note A4
  moreover have IsContinuous( $\tau_2, \tau_2, f_2$ ) using id_cont by simp
  moreover have  $g = \{\langle p, \langle f_1(\text{fst}(p)), f_2(\text{snd}(p)) \rangle \rangle \mid p \in \bigcup \tau_1 \times \bigcup \tau_2\}$ 
proof
  from A5 I show  $g \subseteq \{\langle p, \langle f_1(\text{fst}(p)), f_2(\text{snd}(p)) \rangle \rangle \mid p \in \bigcup \tau_1 \times \bigcup \tau_2\}$ 
    by auto
  from A5 I show  $\{\langle p, \langle f_1(\text{fst}(p)), f_2(\text{snd}(p)) \rangle \rangle \mid p \in \bigcup \tau_1 \times \bigcup \tau_2\} \subseteq g$ 
    by auto
qed
ultimately show thesis by (rule cart_prod_cont)
qed

```

## 45.6 Pasting lemma

The classical pasting lemma states that if  $U_1, U_2$  are both open (or closed) and a function is continuous when restricted to both  $U_1$  and  $U_2$  then it is continuous when restricted to  $U_1 \cup U_2$ . In this section we prove a generalization statement stating that the set  $\{U \in \tau_1 \mid f|_U \text{ is continuous}\}$  is a topology.

A typical statement of the pasting lemma uses the notion of a function restricted to a set being continuous without specifying the topologies with respect to which this continuity holds. In `two_top_spaces0` context the notation `g {is continuous}` means continuity with respect to topologies  $\tau_1, \tau_2$ . The next lemma is a special case of `partial_fun_cont` and states that if for some set  $A \subseteq X_1 = \bigcup \tau_1$  the function  $f|_A$  is continuous (with respect to  $(\tau_1, \tau_2)$ ), then  $A$  has to be open. This clears up terminology and indicates

why we need to pay attention to the issue of which topologies we talk about when we say that the restricted (to some closed set for example) function is continuous.

```

lemma (in two_top_spaces0) restriction_continuous1:
  assumes A1:  $A \subseteq X_1$  and A2:  $\text{restrict}(f,A) \text{ \{is continuous\}}$ 
  shows  $A \in \tau_1$ 
proof -
  from assms have two_top_spaces1( $\tau_1, \tau_2$ ) and
     $\text{restrict}(f,A):A \rightarrow X_2$  and  $\text{restrict}(f,A) \text{ \{is continuous\}}$ 
    using tau1_is_top tau2_is_top two_top_spaces1_def fmapAssum restrict_fun
    by auto
  then show thesis using two_top_spaces1.partial_fun_cont by simp
qed

```

If a function is continuous on each set of a collection of open sets, then it is continuous on the union of them. We could use continuity with respect to the relative topology here, but we know that on open sets this is the same as the original topology.

```

lemma (in two_top_spaces0) pasting_lemma1:
  assumes A1:  $M \subseteq \tau_1$  and A2:  $\forall U \in M. \text{restrict}(f,U) \text{ \{is continuous\}}$ 
  shows  $\text{restrict}(f, \bigcup M) \text{ \{is continuous\}}$ 
proof -
  { fix V assume  $V \in \tau_2$ 
    from A1 have  $\bigcup M \subseteq X_1$  by auto
    then have  $\text{restrict}(f, \bigcup M) \text{-(V)} = f \text{-(V)} \cap (\bigcup M)$ 
      using func1_2_L1 fmapAssum by simp
    also have  $\dots = \bigcup \{f \text{-(V)} \cap U. U \in M\}$  by auto
    finally have  $\text{restrict}(f, \bigcup M) \text{-(V)} = \bigcup \{f \text{-(V)} \cap U. U \in M\}$  by simp
    moreover
    have  $\{f \text{-(V)} \cap U. U \in M\} \in \text{Pow}(\tau_1)$ 
    proof -
      { fix W assume  $W \in \{f \text{-(V)} \cap U. U \in M\}$ 
        then obtain U where  $U \in M$  and  $I: W = f \text{-(V)} \cap U$  by auto
        with A2 have  $\text{restrict}(f,U) \text{ \{is continuous\}}$  by simp
        with ' $V \in \tau_2$ ' have  $\text{restrict}(f,U) \text{-(V)} \in \tau_1$ 
          using IsContinuous_def by simp
        moreover from ' $\bigcup M \subseteq X_1$ ' and ' $U \in M$ '
          have  $\text{restrict}(f,U) \text{-(V)} = f \text{-(V)} \cap U$ 
            using fmapAssum func1_2_L1 by blast
          ultimately have  $f \text{-(V)} \cap U \in \tau_1$  by simp
          with I have  $W \in \tau_1$  by simp
        } then show thesis by auto
      }
    qed
    then have  $\bigcup \{f \text{-(V)} \cap U. U \in M\} \in \tau_1$ 
      using tau1_is_top IsATopology_def by auto
    ultimately have  $\text{restrict}(f, \bigcup M) \text{-(V)} \in \tau_1$ 
      by simp
  } then show thesis using IsContinuous_def by simp

```

qed

If a function is continuous on two sets, then it is continuous on intersection.

```

lemma (in two_top_spaces0) cont_inter_cont:
  assumes A1:  $A \subseteq X_1$   $B \subseteq X_1$  and
  A2: restrict(f,A) {is continuous} restrict(f,B) {is continuous}
  shows restrict(f, $A \cap B$ ) {is continuous}
proof -
  { fix V assume  $V \in \tau_2$ 
    with assms have
      restrict(f,A)-(V) =  $f-(V) \cap A$  restrict(f,B)-(V) =  $f-(V) \cap B$  and
      restrict(f,A)-(V)  $\in \tau_1$  and restrict(f,B)-(V)  $\in \tau_1$ 
      using func1_2_L1 fmapAssum IsContinuous_def by auto
    then have (restrict(f,A)-(V))  $\cap$  (restrict(f,B)-(V)) =  $f-(V) \cap (A \cap B)$ 
      by auto
    moreover
    from A2 ' $V \in \tau_2$ ' have
      restrict(f,A)-(V)  $\in \tau_1$  and restrict(f,B)-(V)  $\in \tau_1$ 
      using IsContinuous_def by auto
    then have (restrict(f,A)-(V))  $\cap$  (restrict(f,B)-(V))  $\in \tau_1$ 
      using tau1_is_top IsATopology_def by simp
    moreover
    from A1 have  $(A \cap B) \subseteq X_1$  by auto
    then have restrict(f, $A \cap B$ )-(V) =  $f-(V) \cap (A \cap B)$ 
      using func1_2_L1 fmapAssum by simp
    ultimately have restrict(f, $A \cap B$ )-(V)  $\in \tau_1$  by simp
  } then show thesis using IsContinuous_def by auto
qed

```

The collection of open sets  $U$  such that  $f$  restricted to  $U$  is continuous, is a topology.

```

theorem (in two_top_spaces0) pasting_theorem:
  shows { $U \in \tau_1$ . restrict(f,U) {is continuous}} {is a topology}
proof -
  let T = { $U \in \tau_1$ . restrict(f,U) {is continuous}}
  have  $\forall M \in \text{Pow}(T). \bigcup M \in T$ 
  proof
    fix M assume  $M \in \text{Pow}(T)$ 
    then have restrict(f, $\bigcup M$ ) {is continuous}
      using pasting_lemma1 by auto
    with ' $M \in \text{Pow}(T)$ ' show  $\bigcup M \in T$ 
      using tau1_is_top IsATopology_def by auto
  qed
  moreover have  $\forall U \in T. \forall V \in T. U \cap V \in T$ 
    using cont_inter_cont tau1_is_top IsATopology_def by auto
  ultimately show thesis using IsATopology_def by simp
qed

```

$f$  is continuous.

```

corollary (in two_top_spaces0) zero_continuous: shows 0 {is continuous}
proof -
  let T = {U ∈  $\tau_1$ . restrict(f,U) {is continuous}}
  have T {is a topology} by (rule pasting_theorem)
  then have 0∈T by (rule empty_open)
  hence restrict(f,0) {is continuous} by simp
  moreover have restrict(f,0) = 0 by simp
  ultimately show thesis by simp
qed

end

```



## 46 Topology\_ZF\_3.thy

**theory** Topology\_ZF\_3 **imports** Topology\_ZF\_2 FiniteSeq\_ZF

**begin**

Topology\_ZF\_1 theory describes how we can define a topology on a product of two topological spaces. One way to generalize that is to construct topology for a cartesian product of  $n$  topological spaces. The cartesian product approach is somewhat inconvenient though. Another way to approach product topology on  $X^n$  is to model cartesian product as sets of sequences (of length  $n$ ) of elements of  $X$ . This means that having a topology on  $X$  we want to define a topology on the space  $n \rightarrow X$ , where  $n$  is a natural number (recall that  $n = \{0, 1, \dots, n-1\}$  in ZF). However, this in turn can be done more generally by defining a topology on any function space  $I \rightarrow X$ , where  $I$  is any set of indices. This is what we do in this theory.

### 46.1 The base of the product topology

In this section we define the base of the product topology.

Suppose  $\mathcal{X} = I \rightarrow \bigcup T$  is a space of functions from some index set  $I$  to the carrier of a topology  $T$ . Then take a finite collection of open sets  $W : N \rightarrow T$  indexed by  $N \subseteq I$ . We can define a subset of  $\mathcal{X}$  that models the cartesian product of  $W$

**definition**

$$\text{FinProd}(\mathcal{X}, W) \equiv \{x \in \mathcal{X}. \forall i \in \text{domain}(W). x(i) \in W(i)\}$$

Now we define the base of the product topology as the collection of all finite products (in the sense defined above) of open sets.

**definition**

$$\text{ProductTopBase}(I, T) \equiv \bigcup_{N \in \text{FinPow}(I)} \{\text{FinProd}(I \rightarrow \bigcup T, W). W \in N \rightarrow T\}$$

Finally, we define the product topology on sequences. We use the "Seq" prefix although the definition is good for any index sets, not only natural numbers.

**definition**

$$\text{SeqProductTopology}(I, T) \equiv \{\bigcup B. B \in \text{Pow}(\text{ProductTopBase}(I, T))\}$$

Product topology base is closed with respect to intersections.

**lemma** prod\_top\_base\_inter:

**assumes** A1:  $T$  {is a topology} **and**  
A2:  $U \in \text{ProductTopBase}(I, T) \quad V \in \text{ProductTopBase}(I, T)$   
**shows**  $U \cap V \in \text{ProductTopBase}(I, T)$

**proof** -

**let**  $\mathcal{X} = I \rightarrow \bigcup T$

```

from A2 obtain  $N_1 \quad W_1 \quad N_2 \quad W_2$  where
  I:  $N_1 \in \text{FinPow}(I) \quad W_1 \in N_1 \rightarrow T \quad U = \text{FinProd}(\mathcal{X}, W_1)$  and
  II:  $N_2 \in \text{FinPow}(I) \quad W_2 \in N_2 \rightarrow T \quad V = \text{FinProd}(\mathcal{X}, W_2)$ 
  using ProductTopBase_def by auto
let  $N_3 = N_1 \cup N_2$ 
let  $W_3 =$ 
  { $\langle i, \text{if } i \in N_1 - N_2 \text{ then } W_1(i)$ 
    else if  $i \in N_2 - N_1$  then  $W_2(i)$ 
    else  $(W_1(i)) \cap (W_2(i)) \rangle. i \in N_3$ }
from A1 I II have  $\forall i \in N_1 \cap N_2. (W_1(i) \cap W_2(i)) \in T$ 
  using apply_funtype IsATopology_def by auto
moreover from I II have
   $\forall i \in N_1 - N_2. W_1(i) \in T$  and  $\forall i \in N_2 - N_1. W_2(i) \in T$ 
  using apply_funtype by auto
ultimately have  $W_3: N_3 \rightarrow T$  by (rule fun_union_overlap)
with I II have  $\text{FinProd}(\mathcal{X}, W_3) \in \text{ProductTopBase}(I, T)$  using union_finpov
ProductTopBase_def
  by auto
moreover have  $U \cap V = \text{FinProd}(\mathcal{X}, W_3)$ 
proof
  { fix x assume  $x \in U$  and  $x \in V$ 
    with 'U = FinProd( $\mathcal{X}, W_1$ )' 'W1 ∈ N1 → T' and
      'V = FinProd( $\mathcal{X}, W_2$ )' 'W2 ∈ N2 → T'
    have  $x \in \mathcal{X}$  and  $\forall i \in N_1. x(i) \in W_1(i)$  and  $\forall i \in N_2. x(i) \in W_2(i)$ 
      using func1_1_L1 FinProd_def by auto
    with 'W3: N3 → T' 'x ∈  $\mathcal{X}$ ' have  $x \in \text{FinProd}(\mathcal{X}, W_3)$ 
      using ZF_fun_from_tot_val func1_1_L1 FinProd_def by auto
  } thus  $U \cap V \subseteq \text{FinProd}(\mathcal{X}, W_3)$  by auto
  { fix x assume  $x \in \text{FinProd}(\mathcal{X}, W_3)$ 
    with 'W3: N3 → T' have  $x: I \rightarrow \bigcup T$  and III:  $\forall i \in N_3. x(i) \in W_3(i)$ 
      using FinProd_def func1_1_L1 by auto
    { fix i assume  $i \in N_1$ 
      with 'W3: N3 → T' have  $W_3(i) \subseteq W_1(i)$  using ZF_fun_from_tot_val by
        auto
      with III 'i ∈ N1' have  $x(i) \in W_1(i)$  by auto
    } with 'W1 ∈ N1 → T' 'x: I →  $\bigcup T$ ' 'U = FinProd( $\mathcal{X}, W_1$ )'
      have  $x \in U$  using func1_1_L1 FinProd_def by auto
    moreover
      { fix i assume  $i \in N_2$ 
        with 'W3: N3 → T' have  $W_3(i) \subseteq W_2(i)$  using ZF_fun_from_tot_val
          by auto
        with III 'i ∈ N2' have  $x(i) \in W_2(i)$  by auto
      } with 'W2 ∈ N2 → T' 'x: I →  $\bigcup T$ ' 'V = FinProd( $\mathcal{X}, W_2$ )' have  $x \in V$ 
        using func1_1_L1 FinProd_def by auto
      ultimately have  $x \in U \cap V$  by simp
    } thus  $\text{FinProd}(\mathcal{X}, W_3) \subseteq U \cap V$  by auto
  }
qed
ultimately show thesis by simp

```

qed

In the next theorem we show that the collection of sets defined above as  $\text{ProductTopBase}(\mathcal{X}, T)$  satisfies the base condition. This is a condition, defined in `Topology_ZF_1` that allows to claim that this collection is a base for some topology.

```
theorem prod_top_base_is_base: assumes T {is a topology}
  shows ProductTopBase(I,T) {satisfies the base condition}
  using assms prod_top_base_inter inter_closed_base by simp
```

The (sequence) product topology is indeed a topology on the space of sequences. In the proof we are using the fact that  $(\emptyset \rightarrow X) = \{\emptyset\}$ .

```
theorem seq_prod_top_is_top: assumes T {is a topology}
  shows
    SeqProductTopology(I,T) {is a topology} and
    ProductTopBase(I,T) {is a base for} SeqProductTopology(I,T) and
     $\bigcup \text{SeqProductTopology}(I,T) = (I \rightarrow \bigcup T)$ 
proof -
  from assms show SeqProductTopology(I,T) {is a topology} and
    I: ProductTopBase(I,T) {is a base for} SeqProductTopology(I,T)
    using prod_top_base_is_base SeqProductTopology_def Top_1_2_T1
    by auto
  from I have  $\bigcup \text{SeqProductTopology}(I,T) = \bigcup \text{ProductTopBase}(I,T)$ 
    using Top_1_2_L5 by simp
  also have  $\bigcup \text{ProductTopBase}(I,T) = (I \rightarrow \bigcup T)$ 
  proof
    show  $\bigcup \text{ProductTopBase}(I,T) \subseteq (I \rightarrow \bigcup T)$  using ProductTopBase_def FinProd_def
      by auto
    have  $0 \in \text{FinPow}(I)$  using empty_in_finpow by simp
    hence  $\{\text{FinProd}(I \rightarrow \bigcup T, W). W \in 0 \rightarrow T\} \subseteq$ 
       $(\bigcup N \in \text{FinPow}(I). \{\text{FinProd}(I \rightarrow \bigcup T, W). W \in N \rightarrow T\})$ 
      by blast
    then show  $(I \rightarrow \bigcup T) \subseteq \bigcup \text{ProductTopBase}(I,T)$ 
      using ProductTopBase_def FinProd_def by auto
  qed
  finally show  $\bigcup \text{SeqProductTopology}(I,T) = (I \rightarrow \bigcup T)$  by simp
qed
```

## 46.2 Finite product of topologies

As a special case of the space of functions  $I \rightarrow X$  we can consider space of lists of elements of  $X$ , i.e. space  $n \rightarrow X$ , where  $n$  is a natural number (recall that in ZF set theory  $n = \{0, 1, \dots, n-1\}$ ). Such spaces model finite cartesian products  $X^n$  but are easier to deal with in a formalized way (than the said products). This section discusses natural topology defined on  $n \rightarrow X$  where  $X$  is a topological space.

When the index set is finite, the definition of  $\text{ProductTopBase}(I, T)$  can be

simplified.

lemma fin\_prod\_def\_nat: assumes A1:  $n \in \text{nat}$  and A2:  $T$  {is a topology}

shows  $\text{ProductTopBase}(n, T) = \{\text{FinProd}(n \rightarrow \bigcup T, W). W \in n \rightarrow T\}$

proof

from A1 have  $n \in \text{FinPow}(n)$  using nat\_finpow\_nat fin\_finpow\_self by auto

then show  $\{\text{FinProd}(n \rightarrow \bigcup T, W). W \in n \rightarrow T\} \subseteq \text{ProductTopBase}(n, T)$

using ProductTopBase\_def by auto

{ fix B assume  $B \in \text{ProductTopBase}(n, T)$

then obtain  $N W$  where  $N \in \text{FinPow}(n)$  and  $W \in N \rightarrow T$  and  $B = \text{FinProd}(n \rightarrow \bigcup T, W)$

using ProductTopBase\_def by auto

let  $W_n = \{(i, \text{if } i \in N \text{ then } W(i) \text{ else } \bigcup T). i \in n\}$

from A2 ' $N \in \text{FinPow}(n)$ ' ' $W \in N \rightarrow T$ ' have

$\forall i \in n. (\text{if } i \in N \text{ then } W(i) \text{ else } \bigcup T) \in T$

using apply\_funtype FinPow\_def IsATopology\_def by auto

then have  $W_n: n \rightarrow T$  by (rule ZF\_fun\_from\_total)

moreover have  $B = \text{FinProd}(n \rightarrow \bigcup T, W_n)$

proof

{ fix x assume  $x \in B$

with ' $B = \text{FinProd}(n \rightarrow \bigcup T, W)$ ' have  $x \in n \rightarrow \bigcup T$

using FinProd\_def by simp

moreover have  $\forall i \in \text{domain}(W_n). x(i) \in W_n(i)$

proof

fix i assume  $i \in \text{domain}(W_n)$

with ' $W_n: n \rightarrow T$ ' have  $i \in n$  using func1\_1\_L1 by simp

with ' $x: n \rightarrow \bigcup T$ ' have  $x(i) \in \bigcup T$  using apply\_funtype by blast

with ' $x \in B$ ' ' $B = \text{FinProd}(n \rightarrow \bigcup T, W)$ ' ' $W \in N \rightarrow T$ ' ' $W_n: n \rightarrow T$ ' ' $i \in n$ '

show  $x(i) \in W_n(i)$  using func1\_1\_L1 FinProd\_def ZF\_fun\_from\_tot\_val

by simp

qed

ultimately have  $x \in \text{FinProd}(n \rightarrow \bigcup T, W_n)$  using FinProd\_def by simp

} thus  $B \subseteq \text{FinProd}(n \rightarrow \bigcup T, W_n)$  by auto

next

{ fix x assume  $x \in \text{FinProd}(n \rightarrow \bigcup T, W_n)$

then have  $x \in n \rightarrow \bigcup T$  and  $\forall i \in \text{domain}(W_n). x(i) \in W_n(i)$

using FinProd\_def by auto

with ' $W_n: n \rightarrow T$ ' and ' $N \in \text{FinPow}(n)$ ' have  $\forall i \in N. x(i) \in W_n(i)$

using func1\_1\_L1 FinPow\_def by auto

moreover from ' $W_n: n \rightarrow T$ ' and ' $N \in \text{FinPow}(n)$ '

have  $\forall i \in N. W_n(i) = W(i)$

using ZF\_fun\_from\_tot\_val FinPow\_def by auto

ultimately have  $\forall i \in N. x(i) \in W(i)$  by simp

with ' $W \in N \rightarrow T$ ' ' $x \in n \rightarrow \bigcup T$ ' ' $B = \text{FinProd}(n \rightarrow \bigcup T, W)$ ' have  $x \in B$

using func1\_1\_L1 FinProd\_def by simp

} thus  $\text{FinProd}(n \rightarrow \bigcup T, W_n) \subseteq B$  by auto

qed

ultimately have  $B \in \{\text{FinProd}(n \rightarrow \bigcup T, W). W \in n \rightarrow T\}$  by auto

} thus  $\text{ProductTopBase}(n, T) \subseteq \{\text{FinProd}(n \rightarrow \bigcup T, W). W \in n \rightarrow T\}$  by auto

qed

A technical lemma providing a formula for finite product on one topological space.

```

lemma single_top_prod: assumes A1:  $W:1 \rightarrow \tau$ 
  shows  $\text{FinProd}(1 \rightarrow \bigcup \tau, W) = \{ \{ \langle 0, y \rangle \}. y \in W(0) \}$ 
proof -
  have  $1 = \{0\}$  by auto
  from A1 have  $\text{domain}(W) = \{0\}$  using func1_1_L1 by auto
  then have  $\text{FinProd}(1 \rightarrow \bigcup \tau, W) = \{x \in 1 \rightarrow \bigcup \tau. x(0) \in W(0)\}$ 
    using FinProd_def by simp
  also have  $\{x \in 1 \rightarrow \bigcup \tau. x(0) \in W(0)\} = \{ \{ \langle 0, y \rangle \}. y \in W(0) \}$ 
  proof
    from ' $1 = \{0\}$ ' show  $\{x \in 1 \rightarrow \bigcup \tau. x(0) \in W(0)\} \subseteq \{ \{ \langle 0, y \rangle \}. y \in W(0) \}$ 
      using func_singleton_pair by auto
    { fix x assume  $x \in \{ \{ \langle 0, y \rangle \}. y \in W(0) \}$ 
      then obtain y where  $x = \{ \langle 0, y \rangle \}$  and II:  $y \in W(0)$  by auto
      with A1 have  $y \in \bigcup \tau$  using apply_funtype by auto
      with ' $x = \{ \langle 0, y \rangle \}$ ' ' $1 = \{0\}$ ' have  $x:1 \rightarrow \bigcup \tau$  using pair_func_singleton
        by auto
      with ' $x = \{ \langle 0, y \rangle \}$ ' II have  $x \in \{x \in 1 \rightarrow \bigcup \tau. x(0) \in W(0)\}$ 
        using pair_val by simp
    } thus  $\{ \{ \langle 0, y \rangle \}. y \in W(0) \} \subseteq \{x \in 1 \rightarrow \bigcup \tau. x(0) \in W(0)\}$  by auto
  qed
  finally show thesis by simp
qed

```

Intuitively, the topological space of singleton lists valued in  $X$  is the same as  $X$ . However, each element of this space is a list of length one, i.e a set consisting of a pair  $\langle 0, x \rangle$  where  $x$  is an element of  $X$ . The next lemma provides a formula for the product topology in the corner case when we have only one factor and shows that the product topology of one space is essentially the same as the space.

```

lemma singleton_prod_top: assumes A1:  $\tau$  {is a topology}
  shows
     $\text{SeqProductTopology}(1, \tau) = \{ \{ \{ \langle 0, y \rangle \}. y \in U \}. U \in \tau \}$  and
     $\text{IsAhomeomorphism}(\tau, \text{SeqProductTopology}(1, \tau), \{ \langle y, \{ \langle 0, y \rangle \} \}. y \in \bigcup \tau \})$ 
proof -
  have  $\{0\} = 1$  by auto
  let  $b = \{ \langle y, \{ \langle 0, y \rangle \} \}. y \in \bigcup \tau \}$ 
  have  $b \in \text{bij}(\bigcup \tau, 1 \rightarrow \bigcup \tau)$  using list_singleton_bij by blast
  with A1 have  $\{b(U). U \in \tau\}$  {is a topology} and
     $\text{IsAhomeomorphism}(\tau, \{b(U). U \in \tau\}, b)$ 
    using bij_induced_top by auto
  moreover have  $\forall U \in \tau. b(U) = \{ \{ \langle 0, y \rangle \}. y \in U \}$ 
  proof
    fix U assume  $U \in \tau$ 
    from ' $b \in \text{bij}(\bigcup \tau, 1 \rightarrow \bigcup \tau)$ ' have  $b: \bigcup \tau \rightarrow (1 \rightarrow \bigcup \tau)$ 

```

```

    using bij_def inj_def by simp
  { fix y assume y ∈  $\bigcup \tau$ 
    with 'b:  $\bigcup \tau \rightarrow (1 \rightarrow \bigcup \tau)$ ' have b(y) = {⟨0,y⟩}
      using ZF_fun_from_tot_val by simp
    } hence  $\forall y \in \bigcup \tau. b(y) = \{\langle 0, y \rangle\}$  by auto
    with 'U ∈  $\tau$ ' 'b:  $\bigcup \tau \rightarrow (1 \rightarrow \bigcup \tau)$ ' show b(U) = { {⟨0,y⟩}. y ∈ U }
      using func_imagedef by auto
qed
moreover have ProductTopBase(1,  $\tau$ ) = { { {⟨0,y⟩}. y ∈ U }. U ∈  $\tau$  }
proof
  { fix V assume V ∈ ProductTopBase(1,  $\tau$ )
    with A1 obtain W where W:  $1 \rightarrow \tau$  and V = FinProd( $1 \rightarrow \bigcup \tau$ , W)
      using fin_prod_def_nat by auto
    then have V ∈ { { {⟨0,y⟩}. y ∈ U }. U ∈  $\tau$  }
      using apply_funtype single_top_prod by auto
    } thus ProductTopBase(1,  $\tau$ ) ⊆ { { {⟨0,y⟩}. y ∈ U }. U ∈  $\tau$  } by auto
  { fix V assume V ∈ { { {⟨0,y⟩}. y ∈ U }. U ∈  $\tau$  }
    then obtain U where U ∈  $\tau$  and V = { {⟨0,y⟩}. y ∈ U } by auto
    let W = {⟨0,U⟩}
    from 'U ∈  $\tau$ ' have W:  $\{0\} \rightarrow \tau$  using pair_func_singleton by simp
    with '{0} = 1' have W:  $1 \rightarrow \tau$  and W(0) = U using pair_val by auto
    with 'V = { {⟨0,y⟩}. y ∈ U }' have V = FinProd( $1 \rightarrow \bigcup \tau$ , W)
      using single_top_prod by simp
    with A1 'W:  $1 \rightarrow \tau$ ' have V ∈ ProductTopBase(1,  $\tau$ ) using fin_prod_def_nat
      by auto
    } thus { { {⟨0,y⟩}. y ∈ U }. U ∈  $\tau$  } ⊆ ProductTopBase(1,  $\tau$ ) by auto
qed
ultimately have I: ProductTopBase(1,  $\tau$ ) {is a topology} and
  II: IsAhomeomorphism( $\tau$ , ProductTopBase(1,  $\tau$ ), b) by auto
from A1 have ProductTopBase(1,  $\tau$ ) {is a base for} SeqProductTopology(1,  $\tau$ )
  using seq_prod_top_is_top by simp
with I have ProductTopBase(1,  $\tau$ ) = SeqProductTopology(1,  $\tau$ )
  by (rule base_topology)
with 'ProductTopBase(1,  $\tau$ ) = { { {⟨0,y⟩}. y ∈ U }. U ∈  $\tau$  }' II show
  SeqProductTopology(1,  $\tau$ ) = { { {⟨0,y⟩}. y ∈ U }. U ∈  $\tau$  } and
  IsAhomeomorphism( $\tau$ , SeqProductTopology(1,  $\tau$ ), {⟨y, {⟨0,y⟩}⟩. y ∈  $\bigcup \tau$ })
  by auto
qed

```

A special corner case of `finite_top_prod_homeo`: a space  $X$  is homeomorphic to the space of one element lists of  $X$ .

```

theorem singleton_prod_top1: assumes A1:  $\tau$  {is a topology}
  shows IsAhomeomorphism(SeqProductTopology(1,  $\tau$ ),  $\tau$ , {⟨x, x(0)⟩. x ∈  $1 \rightarrow \bigcup \tau$ })
proof -
  have {⟨x, x(0)⟩. x ∈  $1 \rightarrow \bigcup \tau$ } = converse({⟨y, {⟨0,y⟩}⟩. y ∈  $\bigcup \tau$ })
    using list_singleton_bij by blast
  with A1 show thesis using singleton_prod_top homeo_inv by simp
qed

```

A technical lemma describing the carrier of a (cartesian) product topology of the (sequence) product topology of  $n$  copies of topology  $\tau$  and another copy of  $\tau$ .

```
lemma finite_prod_top:
  assumes  $\tau$  {is a topology} and  $T = \text{SeqProductTopology}(n, \tau)$ 
  shows  $(\bigcup \text{ProductTopology}(T, \tau)) = (n \rightarrow \bigcup \tau) \times \bigcup \tau$ 
  using assms Top_1_4_T1 seq_prod_top_is_top by simp
```

If  $U$  is a set from the base of  $X^n$  and  $V$  is open in  $X$ , then  $U \times V$  is in the base of  $X^{n+1}$ . The next lemma is an analogue of this fact for the function space approach.

```
lemma finite_prod_succ_base:
  assumes A1:  $\tau$  {is a topology} and A2:  $n \in \text{nat}$  and
  A3:  $U \in \text{ProductTopBase}(n, \tau)$  and A4:  $V \in \tau$ 
  shows  $\{x \in \text{succ}(n) \rightarrow \bigcup \tau. \text{Init}(x) \in U \wedge x(n) \in V\} \in \text{ProductTopBase}(\text{succ}(n), \tau)$ 
proof -
  let B =  $\{x \in \text{succ}(n) \rightarrow \bigcup \tau. \text{Init}(x) \in U \wedge x(n) \in V\}$ 
  from A1 A2 have  $\text{ProductTopBase}(n, \tau) = \{\text{FinProd}(n \rightarrow \bigcup \tau, W). W \in n \rightarrow \tau\}$ 
  using fin_prod_def_nat by simp
  with A3 obtain  $W_U$  where  $W_U : n \rightarrow \tau$  and  $U = \text{FinProd}(n \rightarrow \bigcup \tau, W_U)$  by auto
  let  $W = \text{Append}(W_U, V)$ 
  from A4 and ' $W_U : n \rightarrow \tau$ ' have  $W : \text{succ}(n) \rightarrow \tau$  using append_props by simp
  moreover have  $B = \text{FinProd}(\text{succ}(n) \rightarrow \bigcup \tau, W)$ 
proof
  { fix x assume  $x \in B$ 
    with ' $W : \text{succ}(n) \rightarrow \tau$ ' have  $x \in \text{succ}(n) \rightarrow \bigcup \tau$  and  $\text{domain}(W) = \text{succ}(n)$ 

    using func1_1_L1 by auto
    moreover from A2 A4 ' $x \in B$ ' ' $U = \text{FinProd}(n \rightarrow \bigcup \tau, W_U)$ '
    ' $W_U : n \rightarrow \tau$ ' ' $x \in \text{succ}(n) \rightarrow \bigcup \tau$ '
    have  $\forall i \in \text{succ}(n). x(i) \in W(i)$  using func1_1_L1 FinProd_def
    init_props append_props by simp
    ultimately have  $x \in \text{FinProd}(\text{succ}(n) \rightarrow \bigcup \tau, W)$  using FinProd_def
    by simp
  } thus  $B \subseteq \text{FinProd}(\text{succ}(n) \rightarrow \bigcup \tau, W)$  by auto
next
  { fix x assume  $x \in \text{FinProd}(\text{succ}(n) \rightarrow \bigcup \tau, W)$ 
    then have  $x : \text{succ}(n) \rightarrow \bigcup \tau$  and I:  $\forall i \in \text{domain}(W). x(i) \in W(i)$ 
    using FinProd_def by auto
    moreover have  $\text{Init}(x) \in U$ 
  }
proof -
    from A2 and ' $x : \text{succ}(n) \rightarrow \bigcup \tau$ ' have  $\text{Init}(x) : n \rightarrow \bigcup \tau$ 
    using init_props by simp
    moreover have  $\forall i \in \text{domain}(W_U). \text{Init}(x)(i) \in W_U(i)$ 
  }
proof -
    from A2 ' $x \in \text{FinProd}(\text{succ}(n) \rightarrow \bigcup \tau, W)$ ' ' $W : \text{succ}(n) \rightarrow \tau$ '
    have  $\forall i \in n. x(i) \in W(i)$  using FinProd_def func1_1_L1
    by simp
```

```

    moreover from A2 'x: succ(n)→ $\bigcup \tau$ '
      have  $\forall i \in n. \text{Init}(x)(i) = x(i)$  using init_props
      by simp
    moreover from A4 and ' $W_U: n \rightarrow \tau$ ' have  $\forall i \in n. W(i) = W_U(i)$ 
      using append_props by simp
    ultimately have  $\forall i \in n. \text{Init}(x)(i) \in W_U(i)$  by simp
    with ' $W_U: n \rightarrow \tau$ ' show thesis using func1_1_L1 by simp
  qed
  ultimately have  $\text{Init}(x) \in \text{FinProd}(n \rightarrow \bigcup \tau, W_U)$  using FinProd_def
  by simp
  with ' $U = \text{FinProd}(n \rightarrow \bigcup \tau, W_U)$ ' show thesis by simp
qed
moreover have  $x(n) \in V$ 
proof -
  from ' $W: \text{succ}(n) \rightarrow \tau$ ' I have  $x(n) \in W(n)$  using func1_1_L1
  by simp
  moreover from A4 ' $W_U: n \rightarrow \tau$ ' have  $W(n) = V$  using append_props
  by simp
  ultimately show thesis by simp
qed
ultimately have  $x \in B$  by simp
} thus  $\text{FinProd}(\text{succ}(n) \rightarrow \bigcup \tau, W) \subseteq B$  by auto
qed
moreover from A1 A2 have
   $\text{ProductTopBase}(\text{succ}(n), \tau) = \{\text{FinProd}(\text{succ}(n) \rightarrow \bigcup \tau, W). W \in \text{succ}(n) \rightarrow \tau\}$ 
  using fin_prod_def_nat by simp
ultimately show thesis by auto
qed

```

If  $U$  is open in  $X^n$  and  $V$  is open in  $X$ , then  $U \times V$  is open in  $X^{n+1}$ . The next lemma is an analogue of this fact for the function space approach.

```

lemma finite_prod_succ:
  assumes A1:  $\tau$  {is a topology} and A2:  $n \in \text{nat}$  and
  A3:  $U \in \text{SeqProductTopology}(n, \tau)$  and A4:  $V \in \tau$ 
  shows  $\{x \in \text{succ}(n) \rightarrow \bigcup \tau. \text{Init}(x) \in U \wedge x(n) \in V\} \in \text{SeqProductTopology}(\text{succ}(n), \tau)$ 
proof -
  from A1 have  $\text{ProductTopBase}(n, \tau)$  {is a base for}  $\text{SeqProductTopology}(n, \tau)$ 
  and
  I:  $\text{ProductTopBase}(\text{succ}(n), \tau)$  {is a base for}  $\text{SeqProductTopology}(\text{succ}(n), \tau)$ 
  and
  II:  $\text{SeqProductTopology}(\text{succ}(n), \tau)$  {is a topology}
  using seq_prod_top_is_top by auto
  with A3 have  $\exists \mathcal{B} \in \text{Pow}(\text{ProductTopBase}(n, \tau)). U = \bigcup \mathcal{B}$  using Top_1_2_L1
  by simp
  then obtain  $\mathcal{B}$  where  $\mathcal{B} \subseteq \text{ProductTopBase}(n, \tau)$  and  $U = \bigcup \mathcal{B}$  by auto
  then have
     $\{x: \text{succ}(n) \rightarrow \bigcup \tau. \text{Init}(x) \in U \wedge x(n) \in V\} = (\bigcup \mathcal{B} \in \mathcal{B}. \{x: \text{succ}(n) \rightarrow \bigcup \tau.$ 
 $\text{Init}(x) \in \mathcal{B} \wedge x(n) \in V\})$ 
    by auto

```



```

moreover from A1 A2 A4 ' $\mathcal{B} \subseteq \text{ProductTopBase}(n, \tau)$ ' have
   $\forall B \in \mathcal{B}. (\{x: \text{succ}(n) \rightarrow \bigcup \tau. \text{Init}(x) \in B \wedge x(n) \in V\} \in \text{ProductTopBase}(\text{succ}(n), \tau))$ 
  using finite_prod_succ_base by auto
with I II have
   $(\bigcup B \in \mathcal{B}. \{x: \text{succ}(n) \rightarrow \bigcup \tau. \text{Init}(x) \in B \wedge x(n) \in V\}) \in \text{SeqProductTopology}(\text{succ}(n), \tau)$ 
  using base_sets_open union_indexed_open by auto
  ultimately show thesis by simp
qed

```

In the `Topology_ZF_2` theory we define product topology of two topological spaces. The next lemma explains in what sense the topology on finite lists of length  $n$  of elements of topological space  $X$  can be thought as a model of the product topology on the cartesian product of  $n$  copies of that space. Namely, we show that the space of lists of length  $n + 1$  of elements of  $X$  is homeomorphic to the product topology (as defined in `Topology_ZF_2`) of two spaces: the space of lists of length  $n$  and  $X$ . Recall that if  $\mathcal{B}$  is a base (i.e. satisfies the base condition), the the collection  $\{\bigcup B \mid B \in \text{Pow}(\mathcal{B})\}$  is a topology (generated by  $\mathcal{B}$ ).

**theorem** finite\_top\_prod\_homeo: **assumes** A1:  $\tau$  {is a topology} **and** A2:  $n \in \text{nat}$  **and**

A3:  $f = \{\langle x, \langle \text{Init}(x), x(n) \rangle \rangle. x \in \text{succ}(n) \rightarrow \bigcup \tau\}$  **and**

A4:  $T = \text{SeqProductTopology}(n, \tau)$  **and**

A5:  $S = \text{SeqProductTopology}(\text{succ}(n), \tau)$

**shows**  $\text{IsAhomeomorphism}(S, \text{ProductTopology}(T, \tau), f)$

**proof** -

let  $C = \text{ProductCollection}(T, \tau)$

let  $B = \text{ProductTopBase}(\text{succ}(n), \tau)$

**from** A1 A4 **have**  $T$  {is a topology} **using** seq\_prod\_top\_is\_top **by** simp

**with** A1 A5 **have**

$S$  {is a topology} **and**  $\text{ProductTopology}(T, \tau)$  {is a topology}

**using** seq\_prod\_top\_is\_top Top\_1\_4\_T1 **by** auto

**moreover**

**from** assms **have**  $f \in \text{bij}(\bigcup S, \bigcup \text{ProductTopology}(T, \tau))$

**using** lists\_cart\_prod seq\_prod\_top\_is\_top Top\_1\_4\_T1 **by** simp

**then have**  $f: \bigcup S \rightarrow \bigcup \text{ProductTopology}(T, \tau)$  **using** bij\_is\_fun **by** simp

**ultimately have**  $\text{two\_top\_spaces0}(S, \text{ProductTopology}(T, \tau), f)$  **using** two\_top\_spaces0\_def **by** simp

**moreover note** ' $f \in \text{bij}(\bigcup S, \bigcup \text{ProductTopology}(T, \tau))$ '

**moreover from** A1 A5 **have**  $B$  {is a base for}  $S$

**using** seq\_prod\_top\_is\_top **by** simp

**moreover from** A1 ' $T$  {is a topology}' **have**  $C$  {is a base for}  $\text{ProductTopology}(T, \tau)$

**using** Top\_1\_4\_T1 **by** auto

**moreover have**  $\forall W \in C. f^{-1}(W) \in S$

**proof**

fix  $W$  **assume**  $W \in C$

**then obtain**  $U \ V$  **where**  $U \in T \ V \in \tau$  **and**  $W = U \times V$  **using** ProductCollection\_def

**by** auto

**from** A1 A5 ' $f: \bigcup S \rightarrow \bigcup \text{ProductTopology}(T, \tau)$ ' **have**

```

      f: (succ(n) →  $\bigcup \tau$ ) →  $\bigcup \text{ProductTopology}(T, \tau)$ 
      using seq_prod_top_is_top by simp
      with assms 'W = U × V' 'U ∈ T' 'V ∈  $\tau$ ' show f-(W) ∈ S
      using ZF_fun_from_tot_val func1_1_L15 finite_prod_succ by simp
qed
moreover have  $\forall V \in B. f(V) \in \text{ProductTopology}(T, \tau)$ 
proof
  fix V assume V ∈ B
  with A1 A2 obtain WV where
    WV ∈ succ(n) →  $\tau$  and V = FinProd(succ(n) →  $\bigcup \tau$ , WV)
    using fin_prod_def_nat by auto
  let U = FinProd(n →  $\bigcup \tau$ , Init(WV))
  let W = WV(n)
  have U ∈ T
  proof -
    from A1 A2 'WV ∈ succ(n) →  $\tau$ ' have U ∈ ProductTopBase(n,  $\tau$ )
    using fin_prod_def_nat init_props by auto
    with A1 A4 show thesis using seq_prod_top_is_top base_sets_open

    by blast
  qed
  from A1 'WV ∈ succ(n) →  $\tau$ ' 'T {is a topology}' 'U ∈ T'
  have U × W ∈ ProductTopology(T,  $\tau$ )
  using apply_funtype prod_open_open_prod by simp
  moreover have f(V) = U × W
  proof -
    from A2 'WV: succ(n) →  $\tau$ ' have
      Init(WV): n →  $\tau$  and III:  $\forall k \in n. \text{Init}(W_V)(k) = W_V(k)$ 
      using init_props by auto
    then have domain(Init(WV)) = n using func1_1_L1 by simp
    have f(V) = {⟨Init(x), x(n)⟩. x ∈ V}
    proof -
      have f(V) = {f(x). x ∈ V}
      proof -
        from A1 A5 have B {is a base for} S using seq_prod_top_is_top
        by simp
        with 'V ∈ B' have V ⊆  $\bigcup S$  using IsAbaseFor_def by auto
        with 'f:  $\bigcup S \rightarrow \bigcup \text{ProductTopology}(T, \tau)$ ' show thesis using func_imagedef
      by simp
    qed
    moreover have  $\forall x \in V. f(x) = \langle \text{Init}(x), x(n) \rangle$ 
    proof -
      from A1 A3 A5 'V = FinProd(succ(n) →  $\bigcup \tau$ , WV)' have V ⊆  $\bigcup S$  and
        fdef: f = {⟨x, ⟨Init(x), x(n)⟩⟩. x ∈  $\bigcup S$ }
        using seq_prod_top_is_top FinProd_def by auto
      from 'f:  $\bigcup S \rightarrow \bigcup \text{ProductTopology}(T, \tau)$ ' fdef have
         $\forall x \in \bigcup S. f(x) = \langle \text{Init}(x), x(n) \rangle$ 
        by (rule ZF_fun_from_tot_val0)
      with 'V ⊆  $\bigcup S$ ' show thesis by auto
    end
  end
end

```

```

qed
ultimately show thesis by simp
qed
also have  $\{\langle \text{Init}(x), x(n) \rangle. x \in V\} = U \times W$ 
proof
  { fix y assume y  $\in \{\langle \text{Init}(x), x(n) \rangle. x \in V\}$ 
    then obtain x where I:  $y = \langle \text{Init}(x), x(n) \rangle$  and  $x \in V$  by auto

    with 'V = FinProd(succ(n)  $\rightarrow \bigcup \tau, W_V$ )' have
      x: succ(n)  $\rightarrow \bigcup \tau$  and II:  $\forall k \in \text{domain}(W_V). x(k) \in W_V(k)$ 
      unfolding FinProd_def by auto
    with A2 'W_V: succ(n)  $\rightarrow \tau$ ' have IV:  $\forall k \in n. \text{Init}(x)(k) = x(k)$ 
      using init_props by simp
    have Init(x)  $\in U$ 
    proof -
      from A2 'x: succ(n)  $\rightarrow \bigcup \tau$ ' have Init(x):  $n \rightarrow \bigcup \tau$ 
        using init_props by simp
      moreover have  $\forall k \in \text{domain}(\text{Init}(W_V)). \text{Init}(x)(k) \in \text{Init}(W_V)(k)$ 
      proof -
        from A2 'W_V: succ(n)  $\rightarrow \tau$ ' have Init(W_V):  $n \rightarrow \tau$ 
          using init_props by simp
        then have domain(Init(W_V)) = n using func1_1_L1 by simp
        note III IV 'domain(Init(W_V)) = n'
        moreover from II 'W_V  $\in \text{succ}(n) \rightarrow \tau$ '
          have  $\forall k \in n. x(k) \in W_V(k)$ 
          using func1_1_L1 by simp
        ultimately show thesis by simp
      qed
    qed
    ultimately show Init(x)  $\in U$  using FinProd_def by simp
  qed
  moreover from 'W_V: succ(n)  $\rightarrow \tau$ ' II have  $x(n) \in W$  using func1_1_L1
    by simp
  ultimately have  $\langle \text{Init}(x), x(n) \rangle \in U \times W$  by simp
  with I have  $y \in U \times W$  by simp
} thus  $\{\langle \text{Init}(x), x(n) \rangle. x \in V\} \subseteq U \times W$  by auto
{ fix y assume y  $\in U \times W$ 
  then have fst(y)  $\in U$  and snd(y)  $\in W$  by auto
  with 'domain(Init(W_V)) = n' have fst(y):  $n \rightarrow \bigcup \tau$  and
    V:  $\forall k \in n. \text{fst}(y)(k) \in \text{Init}(W_V)(k)$ 
    using FinProd_def by auto
  from 'W_V: succ(n)  $\rightarrow \tau$ ' have W  $\in \tau$  using apply_funtype by simp
  with 'snd(y)  $\in W$ ' have snd(y)  $\in \bigcup \tau$  by auto
  let x = Append(fst(y), snd(y))
  have x  $\in V$ 
  proof -
    from 'fst(y):  $n \rightarrow \bigcup \tau$ ' 'snd(y)  $\in \bigcup \tau$ ' have x: succ(n)  $\rightarrow \bigcup \tau$ 
      using append_props by simp
    moreover have  $\forall i \in \text{domain}(W_V). x(i) \in W_V(i)$ 
    proof -

```

```

from 'fst(y):  $n \rightarrow \bigcup \tau$ ' 'snd(y)  $\in \bigcup \tau$ '
  have  $\forall k \in n. x(k) = \text{fst}(y)(k)$  and  $x(n) = \text{snd}(y)$ 
  using append_props by auto
moreover from III V have  $\forall k \in n. \text{fst}(y)(k) \in W_V(k)$  by simp

moreover note 'snd(y)  $\in W$ '
ultimately have  $\forall i \in \text{succ}(n). x(i) \in W_V(i)$  by simp
with ' $W_V \in \text{succ}(n) \rightarrow \tau$ ' show thesis using func1_1_L1
  by simp
qed
ultimately have  $x \in \text{FinProd}(\text{succ}(n) \rightarrow \bigcup \tau, W_V)$  using FinProd_def
  by simp
with ' $V = \text{FinProd}(\text{succ}(n) \rightarrow \bigcup \tau, W_V)$ ' show  $x \in V$  by simp
qed
moreover from A2 'y  $\in U \times W$ ' 'fst(y):  $n \rightarrow \bigcup \tau$ ' 'snd(y)  $\in \bigcup \tau$ '
  have  $y = \langle \text{Init}(x), x(n) \rangle$ 
  using init_append append_props by auto
  ultimately have  $y \in \{\langle \text{Init}(x), x(n) \rangle. x \in V\}$  by auto
} thus  $U \times W \subseteq \{\langle \text{Init}(x), x(n) \rangle. x \in V\}$  by auto
qed
finally show  $f(V) = U \times W$  by simp
qed
ultimately show  $f(V) \in \text{ProductTopology}(T, \tau)$  by simp
qed
ultimately show thesis using two_top_spaces0.bij_base_open_homeo by
simp
qed
end

```

## 47 Topology\_ZF\_4.thy

```
theory Topology_ZF_4 imports Topology_ZF_1 Order_ZF
begin
```

### 47.1 Convergence on topological spaces

This theory deals with convergence in topological spaces.

#### 47.1.1 Nets

Nets are a generalization of sequences. It is known that sequences do not determine the behavior of the topological spaces that are not first countable; i.e., have a countable neighborhood base for each point. To solve this problem, nets were defined so that the behavior of any topological space can be thought in terms of convergence of nets.

First we need to define what a directed set is:

**definition**

```
IsDirectedSet (_ {directs} _ 90)
  where r {directs} D  $\equiv$  refl(D,r)  $\wedge$  trans(r)  $\wedge$  ( $\forall x \in D. \forall y \in D. \exists z \in D.$ 
 $\langle x, z \rangle \in r \wedge \langle y, z \rangle \in r$ )
```

Any linear order is a directed set; in particular  $(\mathbb{N}, \leq)$ .

**lemma** linorder\_imp\_directed:

```
  assumes IsLinOrder(X,r)
  shows r {directs} X
proof-
  from assms have trans(r) using IsLinOrder_def by auto
  moreover
  from assms have r:refl(X,r) using IsLinOrder_def total_is_refl by auto
  moreover
  {
    fix x y
    assume R:x $\in$ Xy $\in$ X
    with assms have  $\langle x, y \rangle \in r \vee \langle y, x \rangle \in r$  using IsLinOrder_def IsTotal_def by
    auto
    with r have  $(\langle x, y \rangle \in r \wedge \langle y, y \rangle \in r) \vee (\langle y, x \rangle \in r \wedge \langle x, x \rangle \in r)$  using R refl_def
    by auto
    then have  $\exists z \in X. \langle x, z \rangle \in r \wedge \langle y, z \rangle \in r$  using R by auto
  }
  ultimately show thesis using IsDirectedSet_def using function_def by
  auto
qed
```

We are able to define the concept of net, now that we now what a directed set is.

**definition**

```
IsNet (_ {is a net on} _ 90)
  where N {is a net on} X  $\equiv$  fst(N):domain(fst(N)) $\rightarrow$ X  $\wedge$  (snd(N) {directs}
domain(fst(N)))  $\wedge$  domain(fst(N)) $\neq$ 0
```

Provided a topology and a net directed on its underlying set, we can talk about convergence of the net in the topology.

**definition** (in topology0)

```
NetConverges (_  $\rightarrow$  N _ 90)
  where N {is a net on}  $\bigcup T \implies$  NetConverges(N,x)  $\equiv$ 
(x $\in \bigcup T$ )  $\wedge$  ( $\forall U \in \text{Pow}(\bigcup T)$ . (x $\in \text{int}(U) \implies (\exists t \in \text{domain}(\text{fst}(N))$ .  $\forall m \in \text{domain}(\text{fst}(N))$ .
( $\langle t, m \rangle \in \text{snd}(N) \implies \text{fst}(N)m \in U$ ))))
```

One of the most important directed sets, is the neighborhoods of a point.

**theorem** (in topology0) directedset\_neighborhoods:

```
fixes x
defines Neigh $\equiv$ {U $\in$ Pow( $\bigcup T$ ). x $\in$ int(U)}
defines r $\equiv$ { $\langle U, V \rangle \in (\text{Neigh} \times \text{Neigh})$ . V $\subseteq$ U}
shows r {directs} Neigh
proof-
{
  fix U
  assume U $\in$ Neigh
  then have  $\langle U, U \rangle \in r$  using r_def by auto
}
then have refl(Neigh,r) using refl_def by auto
moreover
{
  fix U V W
  assume  $\langle U, V \rangle \in r$   $\langle V, W \rangle \in r$ 
  then have U $\in$ NeighW $\in$ NeighW $\subseteq$ U using r_def by auto
  then have  $\langle U, W \rangle \in r$  using r_def by auto
}
then have trans(r) using trans_def by blast
moreover
{
  fix A B
  assume p:A $\in$ NeighB $\in$ Neigh
  have A $\cap$ B $\in$ Neigh
  proof-
    from p have A $\cap$ B $\in$ Pow( $\bigcup T$ ) using Neigh_def by auto
    moreover
    {from p have x $\in$ int(A)x $\in$ int(B) using Neigh_def by auto
     then have x $\in$ int(A) $\cap$ int(B) by auto
    }
    moreover
    {have int(A) $\cap$ int(B) $\subseteq$ A $\cap$ B using Top_2_L1 by auto
     moreover
```

```

      then have  $\text{int}(A) \cap \text{int}(B) \in T$  using Top_2_L2[of A] Top_2_L2[of B] topSpaceAssum
IsATopology_def by blast
      ultimately
      have  $\text{int}(A) \cap \text{int}(B) \subseteq \text{int}(A \cap B)$  using Top_2_L5
      by auto}
      ultimately have  $x \in \text{int}(A \cap B)$  by auto}
      ultimately
      show thesis using Neigh_def by auto
qed
moreover
then have  $\langle A, A \cap B \rangle \in r \wedge \langle B, A \cap B \rangle \in r$  using r_def p by auto
ultimately
have  $\exists z \in \text{Neigh}. \langle A, z \rangle \in r \wedge \langle B, z \rangle \in r$  by auto
}
ultimately show thesis using IsDirectedSet_def by auto
qed

```

There can be nets directed by the neighborhoods that converge to the point;  
if there is a choice function.

```

theorem (in topology0) net_direct_neigh_converg:
  assumes  $x \in \bigcup T$ 
  defines  $\text{Neigh} \equiv \{U \in \text{Pow}(\bigcup T). x \in \text{int}(U)\}$ 
  defines  $r \equiv \{\langle U, V \rangle \in (\text{Neigh} \times \text{Neigh}). V \subseteq U\}$ 
  assumes  $f: \text{Neigh} \rightarrow \bigcup T \ \forall U \in \text{Neigh}. fU \in U$ 
  shows  $\langle f, r \rangle \rightarrow N \ x$ 
proof-
  have dom_def:  $\text{Neigh} = \text{domain}(f)$  using Pi_def assms(4) by auto
  moreover
  {
    have  $\bigcup T \in T$  using topSpaceAssum IsATopology_def by auto
    then have  $\text{int}(\bigcup T) = \bigcup T$  using Top_2_L3 by auto
    then have  $\bigcup T \in \text{Neigh}$  using Neigh_def assms(1) by auto
    then have  $\bigcup T \in \text{domain}(\text{fst}(\langle f, r \rangle))$  using dom_def by auto
    moreover
    have  $\text{fst}(\langle f, r \rangle): \text{domain}(\text{fst}(\langle f, r \rangle)) \rightarrow \bigcup T$  using assms(4) dom_def by auto
    moreover
    have  $\text{snd}(\langle f, r \rangle) \ \{\text{directs}\} \ \text{domain}(\text{fst}(\langle f, r \rangle))$  using directedset_neighborhoods[of
x] dom_def unfolding r_def Neigh_def
    by simp
    ultimately have  $\langle f, r \rangle \ \{\text{is a net on}\} \ \bigcup T$  unfolding IsNet_def by auto
  }
  then have Net:  $\langle f, r \rangle \ \{\text{is a net on}\} \ \bigcup T$  .
  {
    fix U
    assume  $U \in \text{Pow}(\bigcup T) \ x \in \text{int}(U)$ 
    then have  $U \in \text{Neigh}$  using Neigh_def by auto
    then have  $t: U \in \text{domain}(f)$  using dom_def by auto
    {
      fix W

```

```

    assume A:W∈domain(f) ⟨U,W⟩∈r
    then have W∈Neigh using dom_def by auto
    then have fW∈W using assms(5) by auto
    with A(2) r_def have fW∈U by auto
  }
  then have ∀W∈domain(f). (⟨U,W⟩∈r ⟶ fW∈U) by auto
  with t have ∃V∈domain(f). ∀W∈domain(f). (⟨V,W⟩∈r ⟶ fW∈U) by auto
}
then have ∀U∈Pow(⋃T). (x∈int(U) ⟶ (∃V∈domain(f). ∀W∈domain(f).
(⟨V,W⟩∈r ⟶ fW∈U)))
  by auto
then show thesis using NetConverges_def[OF Net, of x] assms(1) by auto
qed

```

Nets are a generalization of sequences that can make us see that not all topological spaces can be described by sequences. Nevertheless, nets are not always the tool used to deal with convergence. The reason is that they make use of directed sets which are completely unrelated with the topology.

#### 47.1.2 Filters

The topological tools to deal with convergence are what is called filters.

##### definition

```

IsFilter (_ {is a filter on} _ 90)
where  $\mathcal{F}$  {is a filter on}  $X \equiv (0 \notin \mathcal{F}) \wedge (X \in \mathcal{F}) \wedge (\mathcal{F} \subseteq \text{Pow}(X)) \wedge$ 
 $(\forall A \in \mathcal{F}. \forall B \in \mathcal{F}. A \cap B \in \mathcal{F}) \wedge (\forall B \in \mathcal{F}. \forall C \in \text{Pow}(X). B \subseteq C \longrightarrow C \in \mathcal{F})$ 

```

Not all the sets of a filter are needed to be consider at all times; as it happens with a topology we can consider bases.

##### definition

```

IsBaseFilter (_ {is a base filter} _ 90)
where  $C$  {is a base filter}  $\mathcal{F} \equiv C \subseteq \mathcal{F} \wedge \mathcal{F} = \{A \in \text{Pow}(\bigcup \mathcal{F}). (\exists D \in C. D \subseteq A)\}$ 

```

Not every set is a base for a filter, as it happens with topologies, there is a condition to be satisfied.

##### definition

```

SatisfiesFilterBase (_ {satisfies the filter base condition} 90)
where  $C$  {satisfies the filter base condition}  $\equiv (\forall A \in C. \forall B \in C. \exists D \in C. D \subseteq A \cap B) \wedge C \neq 0 \wedge 0 \notin C$ 

```

##### lemma basic\_element\_filter:

```

assumes  $A \in \mathcal{F}$  and  $C$  {is a base filter}  $\mathcal{F}$ 
shows  $\exists D \in C. D \subseteq A$ 

```

##### proof-

```

from assms(2) have t: $\mathcal{F} = \{A \in \text{Pow}(\bigcup \mathcal{F}). (\exists D \in C. D \subseteq A)\}$  using IsBaseFilter_def
by auto
with assms(1) have  $A \in \{A \in \text{Pow}(\bigcup \mathcal{F}). (\exists D \in C. D \subseteq A)\}$  by auto

```



```

    then have  $A \in \text{Pow}(\bigcup \mathcal{F}) \ \exists D \in C. D \subseteq A$  by auto
    then show thesis by auto
qed

```

The following two results state that the filter base condition is necessary and sufficient for the *filter* generated by a base, to be an actual filter. The third result, rewrites the previous two.

**theorem basic\_filter\_1:**

```

  assumes C {is a base filter}  $\mathcal{F}$  and C {satisfies the filter base condition}
  shows  $\mathcal{F}$  {is a filter on}  $\bigcup \mathcal{F}$ 

```

**proof-**

```

{
  fix A B
  assume AF:A $\in\mathcal{F}$  and BF:B $\in\mathcal{F}$ 
  then obtain DA DB where per:DA $\in C$  DB $\in C$  and sub:DA $\subseteq A$  DB $\subseteq B$  using basic_element_filter[OF
AF assms(1)]
    basic_element_filter[OF BF assms(1)] by auto
  from per have  $\exists D \in C. D \subseteq DA \cap DB$  using assms(2) unfolding SatisfiesFilterBase_def
by auto
  then obtain D where D $\in C$  D $\subseteq DA \cap DB$  by auto
  with sub have D $\subseteq A \cap B$  by auto
  with AF BF have  $\exists D \in C. D \subseteq A \cap B \ A \cap B \in \text{Pow}(\bigcup \mathcal{F})$  by auto
  then have  $A \cap B \in \{A \in \text{Pow}(\bigcup \mathcal{F}) . \exists D \in C. D \subseteq A\}$  by auto
  then have  $A \cap B \in \mathcal{F}$  using assms(1) unfolding IsBaseFilter_def by auto

}
moreover
{
  fix A B
  assume AF:A $\in\mathcal{F}$  and BS:B $\in \text{Pow}(\bigcup \mathcal{F})$  and sub:A $\subseteq B$ 
  obtain D where D $\subseteq A$  D $\in C$  using basic_element_filter[OF AF assms(1)]
by auto
  with sub have D $\subseteq B$  D $\in C$  by auto
  then have  $\exists D \in C. D \subseteq B$  by auto
  with BS have B $\in \{A \in \text{Pow}(\bigcup \mathcal{F}). \exists D \in C. D \subseteq A\}$  by auto
  then have B $\in \mathcal{F}$  using assms(1) unfolding IsBaseFilter_def by auto
}
moreover
from assms(2) have C $\neq \emptyset$  using SatisfiesFilterBase_def by auto
then obtain D where D $\in C$  by auto
then have D $\subseteq \bigcup \mathcal{F}$  using IsBaseFilter_def assms(1) by auto
with 'D $\in C$ ' have  $\exists D \in C. D \subseteq \bigcup \mathcal{F}$  by auto
then have  $\bigcup \mathcal{F} \in \{A \in \text{Pow}(\bigcup \mathcal{F}). \exists D \in C. D \subseteq A\}$  by auto
then have  $\bigcup \mathcal{F} \in \mathcal{F}$  using assms(1) unfolding IsBaseFilter_def by auto
moreover
{
  assume 0 $\in \mathcal{F}$ 
  then obtain D where D $\in C$  D $\subseteq \emptyset$  using basic_element_filter[OF _ assms(1)]
by auto

```

```

    then have  $D \in C$   $D = 0$  by auto
    then have  $0 \in C$  by auto
    then have False using assms(2) SatisfiesFilterBase_def by auto
  }
  then have  $0 \notin \mathcal{F}$  by auto
  ultimately show thesis using IsFilter_def by auto
qed

theorem basic_filter_2:
  assumes  $C$  {is a base filter}  $\mathcal{F}$  and  $\mathcal{F}$  {is a filter on}  $\bigcup \mathcal{F}$ 
  shows  $C$  {satisfies the filter base condition}
proof-
  {
    fix A B
    assume AF: $A \in C$  and BF: $B \in C$ 
    then have  $A \in \mathcal{F}$  and  $B \in \mathcal{F}$  using assms(1) IsBaseFilter_def by auto
    then have  $A \cap B \in \mathcal{F}$  using assms(2) IsFilter_def by auto
    then have  $\exists D \in C. D \subseteq A \cap B$  using assms(1) basic_element_filter by blast
  }
  then have  $\forall A \in C. \forall B \in C. \exists D \in C. D \subseteq A \cap B$  by auto
  moreover
  {
    assume  $0 \in C$ 
    then have  $0 \in \mathcal{F}$  using assms(1) IsBaseFilter_def by auto
    then have False using assms(2) IsFilter_def by auto
  }
  then have  $0 \notin C$  by auto
  moreover
  {
    assume  $C = 0$ 
    then have  $\mathcal{F} = 0$  using assms(1) IsBaseFilter_def by auto
    then have False using assms(2) IsFilter_def by auto
  }
  then have  $C \neq 0$  by auto
  ultimately show thesis using SatisfiesFilterBase_def by auto
qed

```

```

theorem basic_filter:
  assumes  $C$  {is a base filter}  $\mathcal{F}$ 
  shows  $(C \text{ {satisfies the filter base condition}}) \longleftrightarrow (\mathcal{F} \text{ {is a filter on} } \bigcup \mathcal{F})$ 
using assms basic_filter_1 basic_filter_2 by auto

```

A base for a filter determines a filter up to the underlying set.

```

theorem base_unique_filter:
  assumes  $C$  {is a base filter}  $\mathcal{F}_1$  and  $C$  {is a base filter}  $\mathcal{F}_2$ 
  shows  $\mathcal{F}_1 = \mathcal{F}_2 \longleftrightarrow \bigcup \mathcal{F}_1 = \bigcup \mathcal{F}_2$ 
using assms unfolding IsBaseFilter_def by auto

```

```

theorem base_unique_filter_set1:
  assumes  $C \subseteq \text{Pow}(X)$  and  $C \neq \emptyset$ 
  shows  $C$  {is a base filter}  $\{A \in \text{Pow}(X). \exists D \in C. D \subseteq A\}$  and  $\bigcup \{A \in \text{Pow}(X). \exists D \in C. D \subseteq A\} = X$ 
proof-
  from assms(1) have  $C \subseteq \{A \in \text{Pow}(X). \exists D \in C. D \subseteq A\}$  by auto
  moreover
  from assms(2) obtain D where  $D \in C$  by auto
  then have  $D \subseteq X$  using assms(1) by auto
  with 'D ∈ C' have  $X \in \{A \in \text{Pow}(X). \exists D \in C. D \subseteq A\}$  by auto
  then show  $\bigcup \{A \in \text{Pow}(X). \exists D \in C. D \subseteq A\} = X$  by auto
  ultimately
  show  $C$  {is a base filter}  $\{A \in \text{Pow}(X). \exists D \in C. D \subseteq A\}$  using IsBaseFilter_def
by auto
qed

theorem base_unique_filter_set2:
  assumes  $C \subseteq \text{Pow}(X)$  and  $C$  {satisfies the filter base condition}
  shows  $((C \text{ {is a base filter} } \mathfrak{F}) \wedge \bigcup \mathfrak{F} = X) \longleftrightarrow \mathfrak{F} = \{A \in \text{Pow}(X). \exists D \in C. D \subseteq A\}$ 
  apply safe using IsBaseFilter_def apply simp using base_unique_filter_set1[OF
assms(1)] assms(2) unfolding SatisfiesFilterBase_def
  apply simp using base_unique_filter_set1[OF assms(1)] assms(2) unfold-
ing SatisfiesFilterBase_def
  by simp

```

The convergence for filters is much easier concept to write. Given a topology and a filter on the same underlying set, we can define convergence as containing all the neighborhoods of the point.

```

definition (in topology0)
  FilterConverges ( $\_ \rightarrow_F \_$  50) where
   $\mathfrak{F}$  {is a filter on}  $\bigcup T \implies \text{FilterConverges}(\mathfrak{F}, x) \equiv$ 
 $x \in \bigcup T \wedge (\{U \in \text{Pow}(\bigcup T). x \in \text{int}(U)\} \subseteq \mathfrak{F})$ 

```

The neighborhoods of a point form a filter that converges to that point.

```

lemma (in topology0) neigh_filter:
  assumes  $x \in \bigcup T$ 
  defines  $\text{Neigh} \equiv \{U \in \text{Pow}(\bigcup T). x \in \text{int}(U)\}$ 
  shows  $\text{Neigh}$  {is a filter on}  $\bigcup T$  and  $\text{Neigh} \rightarrow_F x$ 
proof-
  {
    fix A B
    assume  $p: A \in \text{Neigh} \ B \in \text{Neigh}$ 
    have  $A \cap B \in \text{Neigh}$ 
    proof-
      from p have  $A \cap B \in \text{Pow}(\bigcup T)$  using Neigh_def by auto
      moreover
      {from p have  $x \in \text{int}(A) x \in \text{int}(B)$  using Neigh_def by auto
      then have  $x \in \text{int}(A) \cap \text{int}(B)$  by auto
      moreover

```

```

      {have int(A)∩int(B)⊆A∩B using Top_2_L1 by auto
      moreover
      then have int(A)∩int(B)∈T using Top_2_L2[of A] Top_2_L2[of B] topSpaceAssum
        IsATopology_def by blast
      ultimately
      have int(A)∩int(B)⊆int(A∩B) using Top_2_L5 by auto}
      ultimately have x∈int(A∩B) by auto}
      ultimately
      show thesis using Neigh_def by auto
    qed
  }
  moreover
  {
    fix A B
    assume A:A∈Neigh and B:B∈Pow(⋃T) and sub:A⊆B
    from sub have int(A)∈T int(A)⊆B using Top_2_L2 Top_2_L1[where A=A]
  by auto
    then have int(A)⊆int(B) using Top_2_L5 by auto
    with A have x∈int(B) using Neigh_def by auto
    with B have B∈Neigh using Neigh_def by auto
  }
  moreover
  {
    assume 0∈Neigh
    then have x∈Interior(0,T) using Neigh_def by auto
    then have x∈0 using Top_2_L1 by auto
    then have False by auto
  }
  then have 0∉Neigh by auto
  moreover
  have ⋃T∈T using topSpaceAssum IsATopology_def by auto
  then have Interior(⋃T,T)=⋃T using Top_2_L3 by auto
  then have ab:⋃T∈Neigh unfolding Neigh_def using assms(1) by auto
  moreover
  have Neigh⊆Pow(⋃T) using Neigh_def by auto
  ultimately show Neigh {is a filter on} ⋃T using IsFilter_def by auto
  moreover
  from ab have ⋃Neigh=⋃T unfolding Neigh_def by auto
  ultimately show Neigh →F x using FilterConverges_def assms(1) Neigh_def
  by auto
  qed

```

Note that with the net we built in a previous result, it wasn't clear that we could construct an actual net that converged to the given point without the axiom of choice. With filters, there is no problem.

Another positive point of filters is due to the existence of filter basis. If we have a basis for a filter, then the filter converges to a point iff every neighborhood of that point contains a basic filter element.

```

theorem (in topology0) convergence_filter_base1:
  assumes  $\mathcal{F}$  {is a filter on}  $\bigcup T$  and  $C$  {is a base filter}  $\mathcal{F}$  and  $\mathcal{F} \rightarrow F$ 
  x
  shows  $\forall U \in \text{Pow}(\bigcup T). x \in \text{int}(U) \longrightarrow (\exists D \in C. D \subseteq U)$  and  $x \in \bigcup T$ 
proof(safe)
  fix U
  assume  $U \subseteq (\bigcup T)$   $x \in \text{int}(U)$ 
  then have  $U \in \mathcal{F}$  using assms(3) FilterConverges_def[OF assms(1)] by auto
  then show  $\exists D \in C. D \subseteq U$  using basic_element_filter assms(2) by blast
  next
  show  $x \in \bigcup T$  using assms(3) FilterConverges_def[OF assms(1)] by auto
qed

theorem (in topology0) convergence_filter_base2:
  assumes  $\mathcal{F}$  {is a filter on}  $\bigcup T$  and  $C$  {is a base filter}  $\mathcal{F}$ 
  and  $\forall U \in \text{Pow}(\bigcup T). x \in \text{int}(U) \longrightarrow (\exists D \in C. D \subseteq U)$  and  $x \in \bigcup T$ 
  shows  $\mathcal{F} \rightarrow F$  x
proof-
  {
    fix U
    assume AS:  $U \in \text{Pow}(\bigcup T)$   $x \in \text{int}(U)$ 
    then obtain D where  $pD: D \in C$  and  $s: D \subseteq U$  using assms(3) by blast
    with AS have  $D \in \mathcal{F}$  and  $D \subseteq U$  and  $U \in \text{Pow}(\bigcup T)$  using assms(2) IsBaseFilter_def
  by auto
    then have  $U \in \mathcal{F}$  using assms(1) IsFilter_def by auto
  }
  then show thesis using FilterConverges_def assms(1) assms(4) by auto
qed

theorem (in topology0) convergence_filter_base_eq:
  assumes  $\mathcal{F}$  {is a filter on}  $\bigcup T$  and  $C$  {is a base filter}  $\mathcal{F}$ 
  shows  $(\mathcal{F} \rightarrow F \ x) \longleftrightarrow ((\forall U \in \text{Pow}(\bigcup T). x \in \text{int}(U) \longrightarrow (\exists D \in C. D \subseteq U)) \wedge x \in \bigcup T)$ 
  using convergence_filter_base1[OF assms] convergence_filter_base2[OF
  assms] by (safe,blast+)

```

### 47.1.3 Relation between nets and filters

Let's build now a net from a filter, such that both converge to the same points.

#### definition

$\text{NetOfFilter} (\text{Net}(\_) \ 40)$  where  
 $\mathcal{F}$  {is a filter on}  $\bigcup \mathcal{F} \implies \text{NetOfFilter}(\mathcal{F}) \equiv \langle \{ \langle A, \text{fst}(A) \rangle. A \in \{ \langle x, F \rangle \in (\bigcup \mathcal{F}) \times \mathcal{F}. x \in F \} \}, \{ \langle A, B \rangle \in \{ \langle x, F \rangle \in (\bigcup \mathcal{F}) \times \mathcal{F}. x \in F \} \times \{ \langle x, F \rangle \in (\bigcup \mathcal{F}) \times \mathcal{F}. x \in F \}. \text{snd}(B) \subseteq \text{snd}(A) \} \}$

#### theorem net\_of\_filter\_is\_net:

```

  assumes  $\mathcal{F}$  {is a filter on} X
  shows  $(\text{Net}(\mathcal{F}))$  {is a net on} X
proof-
  from assms have  $X \in \mathcal{F}$   $\mathcal{F} \subseteq \text{Pow}(X)$  using IsFilter_def by auto

```

```

then have uu:  $\bigcup \mathfrak{F} = X$  by blast
let f = {⟨A, fst(A)⟩. A ∈ {⟨x, F⟩ ∈ ( $\bigcup \mathfrak{F}$ ) ×  $\mathfrak{F}$ . x ∈ F}}
let r = {⟨A, B⟩ ∈ {⟨x, F⟩ ∈ ( $\bigcup \mathfrak{F}$ ) ×  $\mathfrak{F}$ . x ∈ F} × {⟨x, F⟩ ∈ ( $\bigcup \mathfrak{F}$ ) ×  $\mathfrak{F}$ . x ∈ F}. snd(B) ⊆ snd(A)}
have function(f) using function_def by auto
moreover
have relation(f) using relation_def by auto
ultimately
have f: domain(f) → range(f) using function_imp_Pi by auto
have range(f) ⊆  $\bigcup \mathfrak{F}$  by auto
with 'f: domain(f) → range(f)' have f: domain(f) →  $\bigcup \mathfrak{F}$  using fun_weaken_type
by auto
moreover
have dom: domain(f) = {⟨x, F⟩ ∈ ( $\bigcup \mathfrak{F}$ ) ×  $\mathfrak{F}$ . x ∈ F} by auto
{
  {
    fix t
    assume pp: t ∈ domain(f)
    then have snd(t) ⊆ snd(t) by auto
    with dom pp have ⟨t, t⟩ ∈ r by auto
  }
  then have refl(domain(f), r) using refl_def by auto
  moreover
  {
    fix t1 t2 t3
    assume ⟨t1, t2⟩ ∈ r ⟨t2, t3⟩ ∈ r
    then have snd(t3) ⊆ snd(t1) t1 ∈ domain(f) t3 ∈ domain(f) using dom
  }
  then have ⟨t1, t3⟩ ∈ r by auto
}
then have trans(r) using trans_def by auto
moreover
{
  fix x y
  assume as: x ∈ domain(f) y ∈ domain(f)
  then have snd(x) ∈  $\mathfrak{F}$  snd(y) ∈  $\mathfrak{F}$  by auto
  then have p: snd(x) ∩ snd(y) ∈  $\mathfrak{F}$  using assms IsFilter_def by auto
  {
    assume snd(x) ∩ snd(y) = 0
    with p have 0 ∈  $\mathfrak{F}$  by auto
    then have False using assms IsFilter_def by auto
  }
  then have snd(x) ∩ snd(y) ≠ 0 by auto
  then obtain xy where xy ∈ snd(x) ∩ snd(y) by auto
  then have xy ∈ snd(x) ∩ snd(y) ⟨xy, snd(x) ∩ snd(y)⟩ ∈ ( $\bigcup \mathfrak{F}$ ) ×  $\mathfrak{F}$  using p
}
by auto
then have ⟨xy, snd(x) ∩ snd(y)⟩ ∈ {⟨x, F⟩ ∈ ( $\bigcup \mathfrak{F}$ ) ×  $\mathfrak{F}$ . x ∈ F} by auto
with dom have d: ⟨xy, snd(x) ∩ snd(y)⟩ ∈ domain(f) by auto
with as have ⟨x, ⟨xy, snd(x) ∩ snd(y)⟩⟩ ∈ r ∧ ⟨y, ⟨xy, snd(x) ∩ snd(y)⟩⟩ ∈ r
by auto

```

```

    with d have  $\exists z \in \text{domain}(f). \langle x, z \rangle \in r \wedge \langle y, z \rangle \in r$  by blast
  }
  then have  $\forall x \in \text{domain}(f). \forall y \in \text{domain}(f). \exists z \in \text{domain}(f). \langle x, z \rangle \in r \wedge \langle y, z \rangle \in r$ 
by blast
  ultimately have  $r \text{ directs } \text{domain}(f)$  using IsDirectedSet_def by blast
}
moreover
{
  have  $p: X \in \mathcal{F}$  and  $0 \notin \mathcal{F}$  using assms IsFilter_def by auto
  then have  $X \neq 0$  by auto
  then obtain  $q$  where  $q \in X$  by auto
  with p dom have  $\langle q, X \rangle \in \text{domain}(f)$  by auto
  then have  $\text{domain}(f) \neq 0$  by blast
}
ultimately have  $\langle f, r \rangle \text{ is a net on } \bigcup \mathcal{F}$  using IsNet_def by auto
then show  $(\text{Net}(\mathcal{F})) \text{ is a net on } X$  using NetOfFilter_def assms uu by
auto
qed

theorem (in topology0) filter_conver_net_of_filter_conver:
  assumes  $\mathcal{F} \text{ is a filter on } \bigcup T$  and  $\mathcal{F} \rightarrow F \ x$ 
  shows  $(\text{Net}(\mathcal{F})) \rightarrow N \ x$ 
proof-
  from assms have  $\bigcup T \in \mathcal{F} \ \mathcal{F} \subseteq \text{Pow}(\bigcup T)$  using IsFilter_def by auto
  then have  $uu: \bigcup \mathcal{F} = \bigcup T$  by blast
  have  $\text{func}: \text{fst}(\text{Net}(\mathcal{F})) = \{ \langle A, \text{fst}(A) \rangle. A \in \{ \langle x, F \rangle \in (\bigcup \mathcal{F}) \times \mathcal{F}. x \in F \} \}$ 
    and  $\text{dir}: \text{snd}(\text{Net}(\mathcal{F})) = \{ \langle A, B \rangle \in \{ \langle x, F \rangle \in (\bigcup \mathcal{F}) \times \mathcal{F}. x \in F \} \times \{ \langle x, F \rangle \in (\bigcup \mathcal{F}) \times \mathcal{F}. x \in F \}. \text{snd}(B) \subseteq \text{snd}(A) \}$ 
  using assms(1) NetOfFilter_def uu by auto
  then have  $\text{dom\_def}: \text{domain}(\text{fst}(\text{Net}(\mathcal{F}))) = \{ \langle x, F \rangle \in (\bigcup \mathcal{F}) \times \mathcal{F}. x \in F \}$  by auto
  have  $\text{fun}: \text{function}(\text{fst}(\text{Net}(\mathcal{F})))$  unfolding function_def using func by
  auto
  have  $NN: (\text{Net}(\mathcal{F})) \text{ is a net on } \bigcup T$  using net_of_filter_is_net assms(1)
  by auto
  moreover
  from assms have  $x \in \bigcup T$  using FilterConverges_def by auto
  moreover
  {
    fix U
    assume  $AS: U \in \text{Pow}(\bigcup T) \ x \in \text{int}(U)$ 
    then have  $U \in \mathcal{F} \ x \in U$  using assms FilterConverges_def Top_2_L1[of U]
  by auto
    then have  $pp: \langle x, U \rangle \in \text{domain}(\text{fst}(\text{Net}(\mathcal{F})))$  using dom_def by auto
    {
      fix m
      assume  $ASS: m \in \text{domain}(\text{fst}(\text{Net}(\mathcal{F}))) \ \langle \langle x, U \rangle, m \rangle \in \text{snd}(\text{Net}(\mathcal{F}))$ 
      then have  $\text{snd}(m) \subseteq U$  using dir by auto
      then have  $\text{fst}(m) \in U$  using ASS(1) dom_def by auto
      with ASS(1) have  $\text{fst}(\text{Net}(\mathcal{F}))m \in U$  using function_apply_Pair[OF fun]
    }
  }

```

```

func by auto
}
then have  $\forall m \in \text{domain}(\text{fst}(\text{Net}(\mathcal{F}))). (\langle x, U \rangle, m) \in \text{snd}(\text{Net}(\mathcal{F})) \longrightarrow \text{fst}(\text{Net}(\mathcal{F}))m \in U$ 
by auto
with pp have  $\exists t \in \text{domain}(\text{fst}(\text{Net}(\mathcal{F}))). \forall m \in \text{domain}(\text{fst}(\text{Net}(\mathcal{F}))). (\langle t, m \rangle \in \text{snd}(\text{Net}(\mathcal{F}))) \longrightarrow \text{fst}(\text{Net}(\mathcal{F}))m \in U$ 
by auto
}
then have  $\forall U \in \text{Pow}(\bigcup T). (x \in \text{int}(U) \longrightarrow (\exists t \in \text{domain}(\text{fst}(\text{Net}(\mathcal{F}))). \forall m \in \text{domain}(\text{fst}(\text{Net}(\mathcal{F}))). (\langle t, m \rangle \in \text{snd}(\text{Net}(\mathcal{F}))) \longrightarrow \text{fst}(\text{Net}(\mathcal{F}))m \in U))$ 
by auto
ultimately show thesis using NetConverges_def by auto
qed

theorem (in topology0) net_of_filter_conver_filter_conver:
assumes  $\mathcal{F}$  {is a filter on}  $\bigcup T$  and  $(\text{Net}(\mathcal{F})) \rightarrow^N x$ 
shows  $\mathcal{F} \rightarrow^F x$ 
proof-
from assms have  $\bigcup T \in \mathcal{F}$   $\mathcal{F} \subseteq \text{Pow}(\bigcup T)$  using IsFilter_def by auto
then have uu:  $\bigcup \mathcal{F} = \bigcup T$  by blast
have  $x \in \bigcup T$  using assms NetConverges_def net_of_filter_is_net by auto
moreover
{
fix U
assume  $U \in \text{Pow}(\bigcup T)$   $x \in \text{int}(U)$ 
then obtain t where  $t: t \in \text{domain}(\text{fst}(\text{Net}(\mathcal{F})))$  and reg:  $\forall m \in \text{domain}(\text{fst}(\text{Net}(\mathcal{F}))). (\langle t, m \rangle \in \text{snd}(\text{Net}(\mathcal{F}))) \longrightarrow \text{fst}(\text{Net}(\mathcal{F}))m \in U$ 
using assms net_of_filter_is_net NetConverges_def by blast
then obtain t1 t2 where t_def:  $t = \langle t1, t2 \rangle$  and  $t1 \in t2$  and tFF:  $t2 \in \mathcal{F}$  using
NetOfFilter_def assms(1) uu by auto
{
fix s
assume  $s \in t2$ 
then have  $\langle s, t2 \rangle \in \{ \langle q1, q2 \rangle \in \bigcup \mathcal{F} \times \mathcal{F}. q1 \in q2 \}$  using tFF by auto
moreover
have  $\text{domain}(\text{fst}(\text{Net}(\mathcal{F}))) = \{ \langle q1, q2 \rangle \in \bigcup \mathcal{F} \times \mathcal{F}. q1 \in q2 \}$  using NetOfFilter_def
assms(1) uu by auto
ultimately
have tt:  $\langle s, t2 \rangle \in \text{domain}(\text{fst}(\text{Net}(\mathcal{F})))$  by auto
moreover
then have  $\langle \langle t1, t2 \rangle, \langle s, t2 \rangle \rangle \in \text{snd}(\text{Net}(\mathcal{F}))$  using NetOfFilter_def assms(1)
uu t t_def by auto
ultimately
have  $\text{fst}(\text{Net}(\mathcal{F}))\langle s, t2 \rangle \in U$  using reg t_def by auto
moreover
have function( $\text{fst}(\text{Net}(\mathcal{F}))$ ) using NetOfFilter_def assms(1) uu unfolding
function_def
by auto
moreover

```



```

      from tt have <<s,t2>,s>∈fst(Net(ℱ)) using NetOfFilter_def assms(1)
uu by auto
      ultimately
      have s∈U using NetOfFilter_def assms(1) uu function_apply_equality
by auto
    }
    then have t2⊆U by auto
    with tFF assms(1) 'U∈Pow(⋃T)' have U∈ℱ using IsFilter_def by auto
  }
  then have {U∈Pow(⋃T). x∈int(U)}⊆ℱ by auto
  ultimately
  show thesis using FilterConverges_def assms(1) by auto
qed

```

```

theorem (in topology0) filter_conver_iff_net_of_filter_conver:
  assumes ℱ {is a filter on} ⋃T
  shows (ℱ →F x) ⟷ ((Net(ℱ)) →N x)
using filter_conver_net_of_filter_conver net_of_filter_conver_filter_conver
assms by auto

```

The previous result states that, when considering convergence, the filters do not generalize nets. When considering a filter, there is always a net that converges to the same points of the original filter.

Now we see that with nets, results come naturally applying the axiom of choice; but with filters, the results come, may be less natural, but with no choice. The reason is that  $\text{Net}\mathcal{F}$  is a net that doesn't come into our attention as a first choice; maybe because we restrict ourselves to the anti-symmetry property of orders without realizing that a directed set is not an order.

The following results will state that filters are not just a subclass of nets, but that nets and filters are equivalent on convergence: for every filter there is a net converging to the same points, and also, for every net there is a filter converging to the same points.

#### definition

```

FilterOfNet (Filter (_ .. _) 40) where
  (N {is a net on} X) ⟹ FilterOfNet(N,X) ≡ {A∈Pow(X). ∃D∈{{fst(N)snd(s).
s∈{s∈domain(fst(N))×domain(fst(N)). s∈snd(N) ∧ fst(s)=t0}}. t0∈domain(fst(N))}.
D⊆A}

```

#### theorem filter\_of\_net\_is\_filter:

```

  assumes N {is a net on} X
  shows (Filter N..X) {is a filter on} X and {{fst(N)snd(s). s∈{s∈domain(fst(N))×domain(f
s∈snd(N) ∧ fst(s)=t0}}. t0∈domain(fst(N))} {is a base filter} (Filter
N..X)

```

#### proof-

```

  let C={{fst(N)snd(s). s∈{s∈domain(fst(N))×domain(fst(N)). s∈snd(N)
  ∧ fst(s)=t0}}. t0∈domain(fst(N))}
  have C⊆Pow(X)

```

```

proof-
  {fix t
   assume t ∈ C
   then obtain t1 where t1 ∈ domain(fst(N)) and t_Def:t={fst(N)snd(s).
s ∈ {s ∈ domain(fst(N)) × domain(fst(N)). s ∈ snd(N) ∧ fst(s)=t1}} by auto
  {
    fix x
    assume x ∈ t
    with t_Def obtain ss where ss ∈ {s ∈ domain(fst(N)) × domain(fst(N)).
s ∈ snd(N) ∧ fst(s)=t1} and x_def:x=fst(N)snd(ss) by blast
    then have snd(ss) ∈ domain(fst(N)) by auto
    then have fst(N)snd(ss) ∈ X using apply_funtype[of fst(N)domain(fst(N))X]
assms unfolding IsNet_def by auto
    then have x ∈ X using x_def by auto
  }
  then have t ⊆ X by auto
}
then show thesis by blast
qed
moreover
have sat:C {satisfies the filter base condition}
proof-
  obtain t1 where t1 ∈ domain(fst(N)) using assms IsNet_def by blast
  then have {fst(N)snd(s). s ∈ {s ∈ domain(fst(N)) × domain(fst(N)). s ∈ snd(N)
∧ fst(s)=t1}} ∈ C by auto
  then have C ≠ 0 by auto
  moreover
  {
    fix U
    assume U ∈ C
    then obtain q where q_dom:q ∈ domain(fst(N)) and U_def:U={fst(N)snd(s).
s ∈ {s ∈ domain(fst(N)) × domain(fst(N)). s ∈ snd(N) ∧ fst(s)=q}} by blast
    then have ⟨q,q⟩ ∈ snd(N) ∧ fst(⟨q,q⟩)=q using assms unfolding IsNet_def
IsDirectedSet_def refl_def by auto
    with q_dom have ⟨q,q⟩ ∈ {s ∈ domain(fst(N)) × domain(fst(N)). s ∈ snd(N)
∧ fst(s)=q} by auto
    with U_def have fst(N)snd(⟨q,q⟩) ∈ U by blast
    then have fst(N)q ∈ U by auto
    then have U ≠ 0 by auto
  }
  then have 0 ∉ C by auto
moreover
have ∀ A ∈ C. ∀ B ∈ C. (∃ D ∈ C. D ⊆ A ∩ B)
proof
fix A
assume pA:A ∈ C
show ∀ B ∈ C. ∃ D ∈ C. D ⊆ A ∩ B
proof
{

```

```

fix B
assume B ∈ C
with pA obtain qA qB where per: qA ∈ domain(fst(N)) qB ∈ domain(fst(N))
and A_def: A = {fst(N)snd(s). s ∈ {s ∈ domain(fst(N)) × domain(fst(N)). s ∈ snd(N)
  ∧ fst(s) = qA}}
  and B_def: B = {fst(N)snd(s). s ∈ {s ∈ domain(fst(N)) × domain(fst(N)).
s ∈ snd(N) ∧ fst(s) = qB}} by blast
have dir: snd(N) {directs} domain(fst(N)) using assms IsNet_def by
auto
with per obtain qD where ine: ⟨qA, qD⟩ ∈ snd(N) ⟨qB, qD⟩ ∈ snd(N) and
perD: qD ∈ domain(fst(N)) unfolding IsDirectedSet_def
  by blast
let D = {fst(N)snd(s). s ∈ {s ∈ domain(fst(N)) × domain(fst(N)). s ∈ snd(N)
  ∧ fst(s) = qD}}
have D ∈ C using perD by auto
moreover
{
  fix d
  assume d ∈ D
  then obtain sd where sd ∈ {s ∈ domain(fst(N)) × domain(fst(N)). s ∈ snd(N)
  ∧ fst(s) = qD} and d_def: d = fst(N)snd(sd) by blast
  then have sdN: sd ∈ snd(N) and qdd: fst(sd) = qD and sd ∈ domain(fst(N)) × domain(fst(N))
by auto
  then obtain qI aa where sd = ⟨aa, qI⟩ qI ∈ domain(fst(N)) aa ∈ domain(fst(N))
by auto
  with qdd have sd_def: sd = ⟨qD, qI⟩ and qIdom: qI ∈ domain(fst(N)) by
auto
  with sdN have ⟨qD, qI⟩ ∈ snd(N) by auto
  moreover
  have trans(snd(N)) using dir unfolding IsDirectedSet_def by auto
  then have ⟨qA, qD⟩ ∈ snd(N) → ⟨qD, qI⟩ ∈ snd(N) → ⟨qA, qI⟩ ∈ snd(N) ⟨qB, qD⟩ ∈ snd(N) → ⟨qD, qI⟩ ∈
  snd(N)
  unfolding trans_def by (safe, blast+)
  with ine calculation have ⟨qA, qI⟩ ∈ snd(N) ⟨qB, qI⟩ ∈ snd(N) by auto
  then have ⟨qA, qI⟩ ∈ {s ∈ domain(fst(N)) × domain(fst(N)). s ∈ snd(N)
  ∧ fst(s) = qA}
  ⟨qB, qI⟩ ∈ {s ∈ domain(fst(N)) × domain(fst(N)). s ∈ snd(N) ∧ fst(s) = qB}
using qIdom per by auto
  then have fst(N)qI ∈ A ∩ B using A_def B_def by auto
  then have fst(N)snd(sd) ∈ A ∩ B using sd_def by auto
  then have d ∈ A ∩ B using d_def by auto
}
then have D ⊆ A ∩ B by blast
ultimately show ∃ D ∈ C. D ⊆ A ∩ B by blast
}
qed
qed
ultimately
show thesis unfolding SatisfiesFilterBase_def by blast
qed

```

```

    moreover
    from base_unique_filter_set2[OF calculation]
    have Base:C {is a base filter} {A∈Pow(X). ∃D∈C. D⊆A} ∪ {A∈Pow(X).
    ∃D∈C. D⊆A}=X by auto
    with sat have {A∈Pow(X). ∃D∈C. D⊆A} {is a filter on} X using basic_filter
    by auto
    then show (Filter N..X) {is a filter on} X using FilterOfNet_def
    assms by auto
    from Base(1) show C {is a base filter} (Filter N..X) using FilterOfNet_def
    assms by auto
  qed

theorem (in topology0) net_conver_filter_of_net_conver:
  assumes N {is a net on} ∪T and N →N x
  shows (Filter N..(∪T)) →F x
proof-
  from assms(2) have x∈∪T using NetConverges_def[OF assms(1)] by auto
  moreover
  {
    fix U
    assume U∈Pow(∪T) x∈int(U)
    then have ∃t∈domain(fst(N)). (∀m∈domain(fst(N)). (<t,m>∈snd(N) →
fst(N)m∈U))
    using assms(2) unfolding NetConverges_def[OF assms(1)] by auto
    then obtain t where t∈domain(fst(N)) and reg:∀m∈domain(fst(N)).
    (<t,m>∈snd(N) → fst(N)m∈U) by auto
    {
      fix f
      assume f∈{fst(N)snd(s). s∈{s∈domain(fst(N))×domain(fst(N)). s∈snd(N)
    ∧ fst(s)=t}}
      then obtain s where s∈{s∈domain(fst(N))×domain(fst(N)). s∈snd(N)
    ∧ fst(s)=t} and f_def:f=fst(N)snd(s)
      by blast
      then have s_p:s∈domain(fst(N))×domain(fst(N)) and s∈snd(N) and
fst(s)=t by auto
      then have s=<t,snd(s)> and snd(s)∈domain(fst(N)) by auto
      with 's∈snd(N)' reg have fst(N)snd(s)∈U by auto
      with f_def have f∈U by auto
    }
    then have {fst(N)snd(s). s∈{s∈domain(fst(N))×domain(fst(N)). s∈snd(N)
    ∧ fst(s)=t}} ⊆ U by blast
    with 't∈domain(fst(N))' have ∃D∈{{fst(N)snd(s). s∈{s∈domain(fst(N))×domain(fst(N)).
    s∈snd(N) ∧ fst(s)=t}}. t∈domain(fst(N))}. D⊆U
    by auto
  }
  then have ∀U∈Pow(∪T). x∈int(U) → (∃D∈{{fst(N)snd(s). s∈{s∈domain(fst(N))×domain(fst
s∈snd(N) ∧ fst(s)=t}}. t∈domain(fst(N))}. D⊆U)
  by auto
  ultimately show (Filter N..(∪T)) →F x using convergence_filter_base2[OF

```

```

filter_of_net_is_filter
  [OF assms(1)]] by blast
qed

```

```

theorem (in topology0) filter_of_net_conver_net_conver:
  assumes N {is a net on}  $\bigcup T$  and (Filter N.. $\bigcup T$ )  $\rightarrow_F x$ 
  shows N  $\rightarrow_N x$ 

```

proof-

```

  from assms(2) have reg: $\forall U \in \text{Pow}(\bigcup T). x \in \text{int}(U) \longrightarrow (\exists D \in \{\{fst(N)snd(s). s \in \{s \in \text{domain}(fst(N)) \times \text{domain}(fst(N)). s \in \text{snd}(N) \wedge fst(s)=t\}\}. t \in \text{domain}(fst(N))\}. D \subseteq U)$ 

```

```

  using convergence_filter_base1[OF filter_of_net_is_filter[OF assms(1)]]

```

by auto

```

  from assms(2) have x $\in \bigcup T$  using convergence_filter_base1[OF filter_of_net_is_filter[OF assms(1)]] by auto

```

moreover

{

fix U

assume  $U \in \text{Pow}(\bigcup T)$   $x \in \text{int}(U)$

```

  with reg have  $\exists D \in \{\{fst(N)snd(s). s \in \{s \in \text{domain}(fst(N)) \times \text{domain}(fst(N)). s \in \text{snd}(N) \wedge fst(s)=t\}\}. t \in \text{domain}(fst(N))\}. D \subseteq U$ 

```

by auto

```

  then obtain D where  $D \in \{\{fst(N)snd(s). s \in \{s \in \text{domain}(fst(N)) \times \text{domain}(fst(N)). s \in \text{snd}(N) \wedge fst(s)=t\}\}. t \in \text{domain}(fst(N))\}$   $D \subseteq U$ 

```

by auto

```

  then obtain td where  $td \in \text{domain}(fst(N))$  and  $D\_def: D = \{fst(N)snd(s). s \in \{s \in \text{domain}(fst(N)) \times \text{domain}(fst(N)). s \in \text{snd}(N) \wedge fst(s)=td\}$ 

```

by auto

{

fix m

assume  $m \in \text{domain}(fst(N))$   $\langle td, m \rangle \in \text{snd}(N)$

```

  with 'td $\in \text{domain}(fst(N))$ ' have  $\langle td, m \rangle \in \{s \in \text{domain}(fst(N)) \times \text{domain}(fst(N)). s \in \text{snd}(N) \wedge fst(s)=td\}$ 

```

by auto

with  $D\_def$  have  $fst(N)m \in D$  by auto

with ' $D \subseteq U$ ' have  $fst(N)m \in U$  by auto

}

then have  $\forall m \in \text{domain}(fst(N)). \langle td, m \rangle \in \text{snd}(N) \longrightarrow fst(N)m \in U$  by auto

with 'td $\in \text{domain}(fst(N))$ ' have  $\exists t \in \text{domain}(fst(N)). \forall m \in \text{domain}(fst(N)).$

```

 $\langle t, m \rangle \in \text{snd}(N) \longrightarrow fst(N)m \in U$ 

```

by auto

}

```

  then have  $\forall U \in \text{Pow}(\bigcup T). x \in \text{int}(U) \longrightarrow (\exists t \in \text{domain}(fst(N)). \forall m \in \text{domain}(fst(N)). \langle t, m \rangle \in \text{snd}(N) \longrightarrow fst(N)m \in U)$ 

```

by auto

ultimately show thesis using NetConverges\_def[OF assms(1)] by auto

qed

```

theorem (in topology0) filter_of_net_conv_iff_net_conv:

```

```

    assumes N {is a net on}  $\bigcup T$ 
    shows  $((\text{Filter } N..(\bigcup T)) \rightarrow_F x) \longleftrightarrow (N \rightarrow_N x)$ 
    using assms filter_of_net_conver_net_conver net_conver_filter_of_net_conver
  by auto

```

We know now that filters and nets are the same thing, when working convergence of topological spaces. Sometimes, the nature of filters makes it easier to generalize them as follows.

Instead of considering all subsets of some set  $X$ , we can consider only open sets (we get an open filter) or closed sets (we get a closed filter). There are many more useful examples that characterize topological properties.

This type of generalization cannot be done with nets.

Also a filter can give us a topology in the following way:

```

theorem top_of_filter:
  assumes  $\mathcal{F}$  {is a filter on}  $\bigcup \mathcal{F}$ 
  shows  $(\mathcal{F} \cup \{0\})$  {is a topology}
proof-
  {
    fix A B
    assume  $A \in (\mathcal{F} \cup \{0\}) B \in (\mathcal{F} \cup \{0\})$ 
    then have  $(A \in \mathcal{F} \wedge B \in \mathcal{F}) \vee (A \cap B = 0)$  by auto
    with assms have  $A \cap B \in (\mathcal{F} \cup \{0\})$  using IsFilter_def by force
  }
  then have  $\forall A \in (\mathcal{F} \cup \{0\}). \forall B \in (\mathcal{F} \cup \{0\}). A \cap B \in (\mathcal{F} \cup \{0\})$  by auto
  moreover
  {
    fix M
    assume  $A : M \in \text{Pow}(\mathcal{F} \cup \{0\})$ 
    then have  $M = 0 \vee M = \{0\} \vee (\exists T \in M. T \in \mathcal{F})$  by blast
    then have  $\bigcup M = 0 \vee (\exists T \in M. T \in \mathcal{F})$  by auto
    then obtain T where  $\bigcup M = 0 \vee (T \in \mathcal{F} \wedge T \in M)$  by auto
    then have  $\bigcup M = 0 \vee (T \in \mathcal{F} \wedge T \subseteq \bigcup M)$  by auto
    moreover
    with A have  $\bigcup M \subseteq \bigcup \mathcal{F}$  by auto
    ultimately have  $\bigcup M \in (\mathcal{F} \cup \{0\})$  using IsFilter_def assms by auto
  }
  then have  $\forall M \in \text{Pow}(\mathcal{F} \cup \{0\}). \bigcup M \in (\mathcal{F} \cup \{0\})$  by auto
  ultimately show thesis using IsATopology_def by auto
qed

```

```

lemma topology0_filter:
  assumes  $\mathcal{F}$  {is a filter on}  $\bigcup \mathcal{F}$ 
  shows topology0  $(\mathcal{F} \cup \{0\})$ 
using top_of_filter topology0_def assms by auto

```

Examples of the previous result are the co-cardinal topologies and the included set topologies, which already appeared in the file `Topology_ZF_examples.thy`.

This construction is considered because of the following result: The filter that defines the topology converges to every point of the underlying set.

**abbreviation** FilConvTop( $\_ \rightarrow F \_ \{in\} \_$ )  
 where FilConvTop( $\mathfrak{F}, x, T$ )  $\equiv$  topology0.FilterConverges( $T, \mathfrak{F}, x$ )

**abbreviation** NetConvTop( $\_ \rightarrow N \_ \{in\} \_$ )  
 where NetConvTop( $N, x, T$ )  $\equiv$  topology0.NetConverges( $T, N, x$ )

**lemma** lim\_filter\_top\_of\_filter:

assumes  $\mathfrak{F}$  {is a filter on}  $\bigcup \mathfrak{F}$  and  $x \in \bigcup \mathfrak{F}$   
 shows  $\mathfrak{F} \rightarrow F x \{in\} (\mathfrak{F} \cup \{0\})$

**proof-**

have  $\bigcup \mathfrak{F} = \bigcup (\mathfrak{F} \cup \{0\})$  by auto  
 with assms(1) have assms1:  $\mathfrak{F}$  {is a filter on}  $\bigcup (\mathfrak{F} \cup \{0\})$  by auto  
 {  
   fix U  
   assume  $U \in \text{Pow}(\bigcup (\mathfrak{F} \cup \{0\}))$   $x \in \text{Interior}(U, (\mathfrak{F} \cup \{0\}))$   
   then have  $\text{Interior}(U, (\mathfrak{F} \cup \{0\})) \in \mathfrak{F}$  using topology0\_def top\_of\_filter[OF  
 assms(1)]  
   topology0.Top\_2\_L2 by blast  
   moreover  
   have  $\text{Interior}(U, (\mathfrak{F} \cup \{0\})) \subseteq U$  using topology0\_def top\_of\_filter[OF assms(1)]  
   topology0.Top\_2\_L1 by auto  
   moreover  
   with ' $U \in \text{Pow}(\bigcup (\mathfrak{F} \cup \{0\}))$ ' have  $U \in \text{Pow}(\bigcup \mathfrak{F})$  by auto  
   ultimately have  $U \in \mathfrak{F}$  using assms(1) IsFilter\_def by auto  
 }  
 then show thesis using assms(2) topology0.FilterConverges\_def[OF \_  
 assms1] top\_of\_filter[OF assms(1)]  
 topology0\_def by auto  
**qed**  
**end**

## 48 Topology\_ZF\_examples.thy

```
theory Topology_ZF_examples imports Topology_ZF CardinalArith
```

```
begin
```

This theory deals with some concrete examples of topologies.

### 48.1 Some new ideas on cardinals

All the results of this section are done without assuming the *Axiom of Choice*. With the *Axiom of Choice* in play, the proofs become easier and some of the assumptions may be dropped.

Since General Topology Theory is closely related to Set Theory, it is very interesting to make use of all the possibilities of Set Theory to try to classify homeomorphic topological spaces. These ideas are generally used to prove that two topological spaces are not homeomorphic.

#### 48.1.1 cases-type results

There exist cardinals which are the successor of another cardinal, but; as happens with ordinal, there are cardinals which are limit cardinal.

**definition**

$$\text{LimitC}(i) \quad \equiv \quad \text{Card}(i) \ \& \ 0 < i \ \& \ (\forall y. (y < i \wedge \text{Card}(y)) \longrightarrow \text{csucc}(y) < i)$$

There are three types of cardinals, the zero one, the successors of other cardinals and the limit cardinals.

**lemma** Card\_cases\_disj:

```
assumes Card(i)
```

```
shows i=0 | ( $\exists j. \text{Card}(j) \ \& \ i=\text{csucc}(j)$ ) | LimitC(i)
```

**proof-**

```
from assms have D:Ord(i) using Card_is_Ord by auto
```

```
{
```

```
  assume F:i $\neq$ 0
```

```
  assume False:~LimitC(i)
```

```
  from F D have 0<i using Ord_0_lt by auto
```

```
  with False assms have  $\exists y. y < i \wedge \text{Card}(y) \wedge \neg \text{csucc}(y) < i$ 
```

```
    using LimitC_def by blast
```

```
  then obtain y where  $y < i \wedge \text{Card}(y) \wedge \neg \text{csucc}(y) < i$  by blast
```

```
  with D have  $y < i \wedge i \leq \text{csucc}(y)$  and 0:Card(y)
```

```
    using not_lt_imp_le lt_Ord Card_csucc Card_is_Ord
```

```
    by auto
```

```
  with assms have  $\text{csucc}(y) \leq i \leq \text{csucc}(y)$  using csucc_le by auto
```

```
  then have  $i=\text{csucc}(y)$  using le_anti_sym by auto
```

```
  with 0 have  $\exists j. \text{Card}(j) \ \& \ i=\text{csucc}(j)$  by auto
```

```
}
```



then show thesis by auto  
qed

```
lemma Card_cases:
  assumes Card (Q)
  obtains (0) Q=0 | (csucc) T where Card(T)  Q=csucc(T) | (limit) LimitC(Q)
  by (insert Card_cases_disj assms, blast)
```

Given an ordinal bounded by a cardinal in ordinal order, we can change to the order of sets.

```
lemma le_imp_lesspoll:
  assumes Card(Q)
  shows  $A \leq Q \implies A \lesssim Q$ 
```

proof-  
 assume  $A \leq Q$   
 then have  $A < Q \vee A = Q$  using le\_iff by auto  
 then have  $A \approx Q \vee A < Q$  using eqpoll\_refl by auto  
 with assms have  $A \approx Q \vee A < Q$  using lt\_Card\_imp\_lesspoll by auto  
 then show  $A \lesssim Q$  using lesspoll\_def eqpoll\_imp\_lepoll by auto  
qed

There are two types of infinite cardinals, the natural numbers and those that have at least one infinite strictly smaller cardinal.

```
lemma InfCard_cases_disj:
  assumes InfCard(Q)
  shows  $Q = \text{nat} \vee (\exists j. \text{csucc}(j) \lesssim Q \ \& \ \text{InfCard}(j))$ 
proof-
  {
    assume  $\forall j. \neg \text{csucc}(j) \lesssim Q \vee \neg \text{InfCard}(j)$ 
    then have  $D: \neg \text{csucc}(\text{nat}) \lesssim Q$  using InfCard_nat by auto
    with D assms have  $\neg(\text{csucc}(\text{nat}) \leq Q)$  using le_imp_lesspoll InfCard_is_Card
  by auto
    with assms have  $Q < (\text{csucc}(\text{nat}))$  using not_le_iff_lt Card_is_Ord Card_csucc
  Card_is_Ord
    Card_is_Ord InfCard_is_Card Card_nat by auto
    with assms have  $Q \leq \text{nat}$  using Card_lt_csucc_iff InfCard_is_Card Card_nat
  by auto
    with assms have  $Q = \text{nat}$  using InfCard_def le_anti_sym by auto
  }
  then show thesis by auto
qed
```

```
lemma InfCard_cases:
  assumes InfCard (Q)
  obtains (nat)  $Q = \text{nat} \mid$  predecessor j where  $\text{csucc}(j) \lesssim Q \ \wedge \ \text{InfCard}(j)$ 
  by (insert InfCard_cases_disj assms,blast)
```

### 48.1.2 Relations between a cardinal and its successor

A set is injective and not bijective to the successor of a cardinal if and only if it is injective and possibly bijective to the cardinal.

**lemma** Card\_less\_csucc\_eq\_le:

assumes Card(m)

shows  $A \prec \text{csucc}(m) \longleftrightarrow A \lesssim m$

**proof**

```

have S:Ord(csucc(m)) using Card_csucc Card_is_Ord assms by auto
{
  assume A:A < csucc(m)
  with S have |A|≈A using lesspoll_imp_eqpoll by auto
  also with A have ...< csucc(m) by auto
  finally have |A|< csucc(m) by auto
  then have |A|<csucc(m)~(|A|≈csucc(m)) using lesspoll_def by auto
  with S have ||A||≤csucc(m)|A|≠csucc(m) using lepoll_cardinal_le
by auto
  then have |A|≤csucc(m)|A|≠csucc(m) using Card_def Card_cardinal
by auto
  then have ~(csucc(m)<|A|) |A|≠csucc(m) using le_imp_not_lt by auto
  then have C:csucc(m)<|A| → |A|<csucc(m)|A|=csucc(m) → |A|<csucc(m)|A|<csucc(m)
→ |A|<csucc(m)
  by auto
  with S have Ord(|A|)Ord(csucc(m)) using Card_cardinal Card_is_Ord
by auto
  with C have |A|<csucc(m) using Ord_linear_lt[where thesis=|A|<csucc(m)]
by auto
  with assms have |A|≤m using Card_lt_csucc_iff Card_cardinal
  by auto
  then have |A|=m∨ |A|< m using le_iff by auto
  then have |A|≈m∨|A|< m using eqpoll_refl by auto
  then have |A|≈m∨|A|< m using lt_Card_imp_lesspoll assms by auto
  then have T:|A|<~m using lesspoll_def eqpoll_imp_lepoll by auto
  from A S have A≈|A| using lesspoll_imp_eqpoll eqpoll_sym by auto
  also with T have ...<~m by auto
  finally show A<~m.
}
{
  assume A:A<~m
  from assms have m<csucc(m) using lt_Card_imp_lesspoll Card_csucc
Card_is_Ord
  lt_csucc by auto
  with A show A<csucc(m) using lesspoll_trans1 by auto
}
qed

```

If the successor of a cardinal is infinite, so is the original cardinal.

**lemma** csucc\_inf\_imp\_inf:

assumes Card(j) and InfCard(csucc(j))

```

shows InfCard(j)
proof-
{
  assume f:Finite (j)
  then obtain n where n∈nat j≈n using Finite_def by auto
  with assms(1) have TT: j=n n∈nat
using cardinal_cong nat_into_Card Card_def by auto
  then have Q:succ(j)∈nat using nat_succI by auto
  with f TT have T:Finite(succ(j))Card(succ(j))
    using nat_into_Card nat_succI by (simp,blast)
  from T(2) have Card(succ(j))∧ j≤j using Card_is_Ord by auto
  moreover
  then have Ord(succ(j)) using Card_is_Ord by auto
  moreover
  {
    fix x
    assume A:x≤j
    {
      assume Card(succ(j))∧ j<x
      with A have False using lt_trans1 by auto
    }
    then have ~(Card(succ(j))∧ j<x) by auto
  }
  ultimately have (LEAST L. Card(L) ∧ j < L)=succ(j)
    using Least_equality[where i=succ(j)] by auto
  then have csucc(j)=succ(j) using csucc_def by auto
  with Q have csucc(j)∈nat by auto
  then have csucc(j)<nat using lt_def Card_nat Card_is_Ord by auto
  with assms(2) have False using InfCard_def lt_trans2 by auto
}
then have ~(Finite (j)) by auto
with assms(1) show thesis using Inf_Card_is_InfCard by auto
qed

```

Since all the cardinals previous to nat are finite, it cannot be a successor cardinal; hence it is a LimitC cardinal.

```

corollary LimitC_nat:
  shows LimitC(nat)
proof-
  note Card_nat
  moreover
  have 0<nat using lt_def by auto
  moreover
  {
    fix y
    assume AS:y<natCard(y)
    then have ord:Ord(y) unfolding lt_def by auto
    then have Cacsucc:Card(csucc(y)) using Card_csucc by auto
    {

```

```

      assume nat ≤ csucc(y)
      with Cacsucc have InfCard(csucc(y)) using InfCard_def by auto
      with AS(2) have InfCard(y) using csucc_inf_imp_inf by auto
      then have nat ≤ y using InfCard_def by auto
      with AS(1) have False using lt_trans2 by auto
    }
    then have ~(nat ≤ csucc(y)) by auto
    then have csucc(y) < nat using not_le_iff_lt Ord_nat Cacsucc Card_is_Ord
  by auto
}
ultimately show thesis using LimitC_def by auto
qed

```

### 48.1.3 Main result on cardinals (without the *Axiom of Choice*)

If two sets are strictly injective to an infinite cardinal, then so is its union. For the case of successor cardinal, this theorem is done in the Isabelle library in a more general setting; but that theorem is of not use in the case where  $\text{LimitC}(Q)$  and it also makes use of the *Axiom of Choice*. The mentioned theorem is in the theory file `Cardinal_AC.thy`

Note that if  $Q$  is finite and different from 1, let's assume  $Q = n$ , then the union of  $A$  and  $B$  is not bounded by  $Q$ . Counterexample: two disjoint sets of  $n - 1$  elements each have a union of  $2n - 2$  elements which are more than  $n$ .

Note also that if  $Q = 1$  then  $A$  and  $B$  must be empty and the union is then empty too; and  $Q$  cannot be 0 because no set is injective and not bijective to 0.

The proof is divided in two parts, first the case when both sets  $A$  and  $B$  are finite; and second, the part when at least one of them is infinite. In the first part, it is used the fact that a finite union of finite sets is finite. In the second part it is used the linear order on cardinals (ordinals). This proof can not be generalized to a setting with an infinite union easily.

```

lemma less_less_imp_un_less:
  assumes A < Q and B < Q and InfCard(Q)
  shows A ∪ B < Q
proof-
{
  assume Finite (A) & Finite(B)
  then have Finite(A ∪ B) using Finite_Un by auto
  then obtain n where R: A ∪ B ≈ n  n ∈ nat using Finite_def
    by auto
  then have |A ∪ B| < nat using lt_def cardinal_cong
    nat_into_Card Card_def Card_nat Card_is_Ord by auto
  with assms(3) have T: |A ∪ B| < Q using InfCard_def lt_trans2 by auto
}

```

```

    from R have Ord(n)  $A \cup B \lesssim n$  using nat_into_Card Card_is_Ord eqpoll_imp_lepoll
  by auto
    then have  $A \cup B \approx |A \cup B|$  using lepoll_Ord_imp_eqpoll eqpoll_sym by
  auto
    also with T assms(3) have  $\dots \prec Q$  using lt_Card_imp_lesspoll InfCard_is_Card
    by auto
    finally have  $A \cup B \prec Q$ .
  }
  moreover
  {
    assume  $\sim(\text{Finite } (A) \ \& \ \text{Finite } (B))$ 
    then have  $A : \sim \text{Finite } (A) \ \vee \ \sim \text{Finite } (B)$  by auto
    from assms have  $B : |A| \approx |B| \approx B$  using lesspoll_imp_eqpoll lesspoll_imp_eqpoll
      InfCard_is_Card Card_is_Ord by auto
    from B(1) have  $A_{\text{eq}} : \forall x. (|A| \approx x) \longrightarrow (A \approx x)$ 
      using eqpoll_sym eqpoll_trans by blast
    from B(2) have  $B_{\text{eq}} : \forall x. (|B| \approx x) \longrightarrow (B \approx x)$ 
      using eqpoll_sym eqpoll_trans by blast
    with A  $A_{\text{eq}}$  have  $\sim \text{Finite } (|A|) \vee \sim \text{Finite } (|B|)$  using Finite_def
    by auto
    then have  $D : \text{InfCard } (|A|) \vee \text{InfCard } (|B|)$  using Inf_Card_is_InfCard Inf_Card_is_InfCard
  Card_cardinal by blast
  {
    assume  $AS : |A| < |B|$ 
    {
      assume  $\sim \text{InfCard } (|A|)$ 
      with D have  $\text{InfCard } (|B|)$  by auto
    }
    moreover
    {
      assume  $\text{InfCard } (|A|)$ 
      then have  $\text{nat} \leq |A|$  using InfCard_def by auto
      with AS have  $\text{nat} < |B|$  using lt_trans1 by auto
      then have  $\text{nat} \leq |B|$  using leI by auto
      then have  $\text{InfCard } (|B|)$  using InfCard_def Card_cardinal by auto
    }
    ultimately have  $\text{InfCard } (|B|)$  by auto
    then have  $2 < |B|$  using InfCard_def lt_trans2[where i=2]
      lt_def by auto
    then have  $AG : 2 \lesssim |B|$  using lt_Card_imp_lesspoll Card_cardinal lesspoll_def
      by auto
    from B(2) have  $|B| \approx B$  .
    also with assms(2) have  $\dots \prec Q$  by auto
    finally have  $TTT : |B| \prec Q$ .
    from B(1) have  $\text{Card } (|B|) A \lesssim |A|$  using eqpoll_sym Card_cardinal eqpoll_imp_lepoll
  by auto
    with AS have  $A \prec |B|$  using lt_Card_imp_lesspoll lesspoll_trans1 by
  auto
    then have  $I1 : A \lesssim |B|$  using lesspoll_def by auto

```

```

    from B(2) have I2:  $B \lesssim |B|$  using eqpoll_sym eqpoll_imp_lepoll by auto
    have  $A \cup B \lesssim A+B$  using Un_lepoll_sum by auto
    also with I1 I2 have  $\dots \lesssim |B| + |B|$  using sum_lepoll_mono by auto
    also with AG have  $\dots \lesssim |B| * |B|$  using sum_lepoll_prod by auto
    also from assms(3) INFB have  $\dots \approx |B|$  using InfCard_square_eqpoll
    by auto
    finally have  $A \cup B \lesssim |B|$ .
    also with TTT have  $\dots < Q$  by auto
    finally have  $A \cup B < Q$ .
  }
  moreover
  {
    assume AS:  $|B| < |A|$ 
    {
      assume  $\sim \text{InfCard}(|B|)$ 
      with D have  $\text{InfCard}(|A|)$  by auto
      moreover
      {
        assume  $\text{InfCard}(|B|)$ 
        then have  $\text{nat} \leq |B|$  using InfCard_def by auto
        with AS have  $\text{nat} < |A|$  using lt_trans1 by auto
        then have  $\text{nat} \leq |A|$  using leI by auto
        then have  $\text{InfCard}(|A|)$  using InfCard_def Card_cardinal by auto
      }
      ultimately have  $\text{INFB} : \text{InfCard}(|A|)$  by auto
      then have  $2 < |A|$  unfolding InfCard_def using lt_trans2[where i=
2]
        using lt_def by auto
      then have  $\text{AG} : 2 \lesssim |A|$  using lt_Card_imp_lesspoll[OF Card_cardinal]
lesspoll_def
        by auto
      from B(1) have  $|A| \approx A$  .
      also with assms(1) have  $\dots < Q$  by auto
      finally have  $\text{TTT} : |A| < Q$ .
      from B(2) have  $\text{Card}(|A|)B \lesssim |B|$  using eqpoll_sym Card_cardinal eqpoll_imp_lepoll
by auto
      with AS have  $B < |A|$  using lt_Card_imp_lesspoll lesspoll_trans1
by auto
      then have  $I1 : B \lesssim |A|$  using lesspoll_def by auto
      from B(1) have  $I2 : A \lesssim |A|$  using eqpoll_sym eqpoll_imp_lepoll by
auto
      have  $A \cup B \lesssim A+B$  using Un_lepoll_sum by auto
      also with I1 I2 have  $\dots \lesssim |A| + |A|$  using sum_lepoll_mono by auto
      also with AG have  $\dots \lesssim |A| * |A|$  using sum_lepoll_prod by auto
      also from INFB assms(3) have  $\dots \approx |A|$  using InfCard_square_eqpoll
        by auto
      finally have  $A \cup B \lesssim |A|$ .
      also with TTT have  $\dots < Q$  by auto
      finally have  $A \cup B < Q$ .
    }
  }

```

```

    }
  moreover
  {
    assume AS:|A|=|B|
    with D have INFB:InfCard(|A|) by auto
    then have 2<|A| using InfCard_def lt_trans2[where i=2]
      using lt_def by auto
    then have AG:2<=|A| using lt_Card_imp_lesspoll Card_cardinal us-
ing lesspoll_def
      by auto
    from B(1) have |A|≈A.
    also with assms(1) have ...<Q by auto
    finally have TTT:|A|<Q.
    from AS B have I1:A<=|A|and I2:B<=|A| using eqpoll_refl eqpoll_imp_lepoll
      eqpoll_sym by auto
    have A ∪ B<=A+B using Un_lepoll_sum by auto
    also with I1 I2 have ...<=|A| + |A| using sum_lepoll_mono by auto
    also with AG have ...<=|A| * |A| using sum_lepoll_prod by auto
    also from assms(3) INFB have ...≈|A| using InfCard_square_eqpoll
      by auto
    finally have A ∪ B<=|A|.
    also with TTT have ...<Q by auto
    finally have A ∪ B<Q.
  }
  ultimately have A ∪ B<Q using Ord_linear_lt[where thesis= A ∪ B<Q]
Card_cardinal Card_is_Ord by auto
}
ultimately show A ∪ B<Q by auto
qed

```

## 48.2 CoCardinal Topology of a set $X$

### 48.2.1 CoCardinal topology is a topology.

The collection of subsets of a set whose complement is strictly bounded by a cardinal is a topology given some assumptions on the cardinal.

**definition** Cocardinal (CoCardinal  $\_ \_ 50$ ) **where**  
 CoCardinal  $X \ T \equiv \{F \in \text{Pow}(X). \ X - F < T\} \cup \{0\}$

For any set and any infinite cardinal; we prove that CoCardinal  $X \ Q$  forms a topology. The proof is done with an infinite cardinal, but it is obvious that the set  $Q$  can be any set equipollent with an infinite cardinal. It is a topology also if the set where the topology is defined is too small or the cardinal too large; in this case, as it is later proved the topology is a discrete topology. And the last case corresponds with  $Q = 1$  which translates in the indiscrete topology.

**lemma** CoCar\_is\_topology:  
 assumes InfCard  $(Q)$

```

    shows (CoCardinal X Q) {is a topology}
proof-
  let T=(CoCardinal X Q)
  {
    fix M
    assume A:M∈Pow(T)
    hence M⊆T by auto
    then have M⊆Pow(X) using Cocardinal_def by auto
    then have  $\bigcup M \in \text{Pow}(X)$  by auto
    moreover
    {
      assume B:M=0
      then have  $\bigcup M \in T$  using Cocardinal_def by auto
    }
    moreover
    {
      assume B:M={0}
      then have  $\bigcup M \in T$  using Cocardinal_def by auto
    }
    moreover
    {
      assume B:M ≠ 0 M≠{0}
      from B obtain T where C:T∈M and T≠0 by auto
      with A have D:X-T < (Q) using Cocardinal_def by auto
      from C have X- $\bigcup M \subseteq X-T$  by blast
      with D have X- $\bigcup M < (Q)$  using subset_imp_lepoll lesspoll_trans1
    }
  }
  by blast
  }
  ultimately have  $\bigcup M \in T$  using Cocardinal_def by auto
}
moreover
{
  fix U and V
  assume U∈T and V∈T
  hence A:U=0 ∨ (U∈Pow(X) ∧ X-U < (Q)) and
    B:V=0 ∨ (V∈Pow(X) ∧ X-V < (Q)) using Cocardinal_def by auto
  hence D:U∈Pow(X) V∈Pow(X) by auto
  have C:X-(U ∩ V)=(X-U)∪(X-V) by fast
  with A B C have U∩V=0∨(U∩V∈Pow(X) ∧ X-(U ∩ V) < (Q)) using less_less_imp_un_less
}
assms
  by auto
  hence U∩V∈T using Cocardinal_def by auto
}
ultimately show thesis using IsATopology_def by auto
qed

theorem topology0_CoCardinal:
  assumes InfCard(T)
  shows topology0(CoCardinal X T)

```



**using** topology0\_def CoCar\_is\_topology **assms by auto**

It can also be proven that, if  $\text{CoCardinal } X \text{ } T$  is a topology,  $X \neq 0$ ,  $\text{Card}(T)$  and  $T \neq 0$ ; then  $T$  is an infinite cardinal,  $X \prec T$  or  $T = 1$ . It follows from the fact that the union of two closed sets is closed.

Choosing the appropriate cardinals, the cofinite and the cocountable topologies are obtained.

The cofinite topology is a very special topology because is extremely related to the separation axiom  $T_1$ . It also appears naturally in algebraic geometry.

**definition**

**Cofinite** ( $\text{CoFinite } _ 90$ ) **where**  
 $\text{CoFinite } X \equiv \text{CoCardinal } X \text{ } \text{nat}$

**definition**

**Cocountable** ( $\text{CoCountable } _ 90$ ) **where**  
 $\text{CoCountable } X \equiv \text{CoCardinal } X \text{ } \text{csucc}(\text{nat})$

## 48.2.2 Total set, Closed sets, Interior, Closure and Boundary

There are several assertions that can be done to the  $\text{CoCardinal } X \text{ } T$  topology. In each case, we will not assume sufficient conditions for  $\text{CoCardinal } X \text{ } T$  to be a topology, but they will be enough to do the calculations in every possible case.

The topology is defined in the set  $X$

**lemma** union\_cocardinal:

**assumes**  $T \neq 0$   
**shows**  $\bigcup (\text{CoCardinal } X \text{ } T) = X$   
**proof-**  
**have**  $X : X - X = 0$  **by auto**  
**have**  $0 \lesssim 0$  **by auto**  
**with assms** **have**  $0 \prec 11 \lesssim T$  **using** not\_0\_is\_lepoll\_1 lepoll\_imp\_lesspoll\_succ

**by auto**

**then** **have**  $0 \prec T$  **using** lesspoll\_trans2 **by auto**  
**with**  $X$  **have**  $(X - X) \prec T$  **by auto**  
**then** **have**  $X \in (\text{CoCardinal } X \text{ } T)$  **using** Cocardinal\_def **by auto**  
**hence**  $X \subseteq \bigcup (\text{CoCardinal } X \text{ } T)$  **by blast**  
**then** **show**  $\bigcup (\text{CoCardinal } X \text{ } T) = X$  **using** Cocardinal\_def **by auto**

**qed**

The closed sets are the small subsets of  $X$  and  $X$  itself.

**lemma** closed\_sets\_cocardinal:

**assumes**  $T \neq 0$   
**shows**  $D \{ \text{is closed in} \} (\text{CoCardinal } X \text{ } T) \longleftrightarrow (D \in \text{Pow}(X) \ \& \ D \prec T) \vee D = X$

**proof-**

{

```

    assume A:D ⊆ X X - D ∈ (CoCardinal X T) D ≠ X
    from A(1,3) have X-(X-D)=D X-D≠0 by (safe,blast+)
    with A(2) have D<T using Cocardinal_def by simp
  }
  with assms have D {is closed in} (CoCardinal X T) ⟶ (D∈Pow(X) & D<T)∨
D=X using IsClosed_def
    union_cocardinal by auto
  moreover
  {
    assume A:D < TD ⊆ X
    from A(2) have X-(X-D)=D by blast
    with A(1) have X-(X-D)< T by auto
    then have X-D∈ (CoCardinal X T) using Cocardinal_def by auto
  }
  with assms have (D∈Pow(X) & D<T)⟶ D {is closed in} (CoCardinal X
T) using union_cocardinal
    IsClosed_def by auto
  moreover
  have X-X=0 by auto
  then have X-X∈ (CoCardinal X T)using Cocardinal_def by auto
  with assms have X{is closed in} (CoCardinal X T) using union_cocardinal
    IsClosed_def by auto
  ultimately show thesis by auto
qed

```

The interior of a set is itself if it is open or 0 if it isn't open.

```

lemma interior_set_cocardinal:
  assumes noC: T≠0 and A⊆X
  shows Interior(A,(CoCardinal X T))= (if ((X-A) < T) then A else 0)
proof-
  from assms(2) have dif_dif:X-(X-A)=A by blast
  {
    assume (X-A) < T
    then have (X-A)∈Pow(X) &(X-A) < T by auto
    with noC have (X-A) {is closed in} (CoCardinal X T) using closed_sets_cocardinal
      by auto
    with noC have X-(X-A)∈(CoCardinal X T) using IsClosed_def union_cocardinal
      by auto
    with dif_dif have A∈(CoCardinal X T) by auto
    hence A∈{U∈(CoCardinal X T). U ⊆ A} by auto
    hence a1:A⊆⋃{U∈(CoCardinal X T). U ⊆ A} by auto
    have a2:⋃{U∈(CoCardinal X T). U ⊆ A}⊆A by blast
    from a1 a2 have Interior(A,(CoCardinal X T))=A using Interior_def
  by auto}
  moreover
  {
    assume as:~((X-A) < T)
    {
      fix U

```

```

    assume U ⊆ A
    hence X-A ⊆ X-U by blast
    then have Q:X-A ≲ X-U using subset_imp_lepoll by auto
    {
      assume X-U ≲ T
      with Q have X-A ≲ T using lesspoll_trans1 by auto
      with as have False by auto
    }
    hence ¬((X-U) ≲ T) by auto
    then have U∉(CoCardinal X T)∨U=0 using Cocardinal_def by auto
  }
  hence {U∈(CoCardinal X T). U ⊆ A}⊆{0} by blast
  then have Interior(A,(CoCardinal X T))=0 using Interior_def by auto
}
ultimately show thesis by auto
qed

```

$X$  is a closed set that contains  $A$ . This lemma is necessary because we cannot use the lemmas proven in the `topology0` context since  $T \neq 0$  is too weak for  $\text{CoCardinal } X \text{ } T$  to be a topology.

```

lemma X_closedcov_cocardinal:
  assumes T≠0A⊆X
  shows X∈ClosedCovers(A,(CoCardinal X T)) using ClosedCovers_def
  using union_cocardinal closed_sets_cocardinal assms by auto

```

The closure of a set is itself if it is closed or  $X$  if it isn't closed.

```

lemma closure_set_cocardinal:
  assumes T≠0A⊆X
  shows Closure(A,(CoCardinal X T))=(if (A ≲ T) then A else X)
proof-
  {
    assume A ≲ T
    with assms have A {is closed in} (CoCardinal X T) using closed_sets_cocardinal
  by auto
    with assms(2) have A∈{D∈Pow(X). D {is closed in} (CoCardinal X
T) ∧ A⊆D} by auto
    with assms(1) have S:A∈ClosedCovers(A,(CoCardinal X T)) using ClosedCovers_def
    using union_cocardinal by auto
    hence 11:⋂ClosedCovers(A,(CoCardinal X T))⊆A by blast
    from S have 12:A⊆⋂ClosedCovers(A,(CoCardinal X T))
      using ClosedCovers_def[where T=CoCardinal X T and A=A] by auto
    from 11 12 have Closure(A,(CoCardinal X T))=A using Closure_def
    by auto
  }
  moreover
  {
    assume as:¬ A ≲ T
    {
      fix U

```

```

    assume  $A \subseteq U$ 
    then have  $Q:A \lesssim U$  using subset_imp_lepoll by auto
    {
      assume  $U \prec T$ 
      with  $Q$  have  $A \prec T$  using lesspoll_trans1 by auto
      with as have False by auto
    }
    hence  $\neg U \prec T$  by auto
    with assms(1) have  $\neg(U \text{ is closed in } (\text{CoCardinal } X \ T)) \vee U=X$  using
closed_sets_cocardinal
    by auto
  }
  with assms(1) have  $\forall U \in \text{Pow}(X). U \text{ is closed in } (\text{CoCardinal } X \ T) \wedge A \subseteq U \longrightarrow U=X$ 
    by auto
  with assms(1) have  $\text{ClosedCovers}(A, (\text{CoCardinal } X \ T)) \subseteq \{X\}$ 
    using union_cocardinal using ClosedCovers_def by auto
  with assms have  $\text{ClosedCovers}(A, (\text{CoCardinal } X \ T)) = \{X\}$  using  $X_{\text{closedcov\_cocardinal}}$ 
    by auto
  then have  $\text{Closure}(A, \text{CoCardinal } X \ T) = X$  using Closure_def by auto
}
ultimately show thesis by auto
qed

```

The boundary of a set is  $\emptyset$  if  $A$  and  $X - A$  are closed,  $X$  if not  $A$  neither  $X - A$  are closed and; if only one is closed, then the closed one is its boundary.

**lemma** boundary\_cocardinal:

```

  assumes  $T \neq \emptyset \wedge A \subseteq X$ 
  shows  $\text{Boundary}(A, (\text{CoCardinal } X \ T)) = (\text{if } A \prec T \text{ then } (\text{if } (X-A) \prec T \text{ then } X-A \text{ else } A) \text{ else } (\text{if } (X-A) \prec T \text{ then } X-A \text{ else } X))$ 

```

**proof-**

```

{
  assume  $AS:A \prec T \wedge X-A \prec T$ 
  from AS(2) assms have  $\text{Closure}(X-A, (\text{CoCardinal } X \ T)) = X-A$  using closure_set_cocardinal[w
 $A=X-A$  and  $T=T$  and  $X=X$ ] by auto
  moreover
  from AS(1) assms have  $\text{Closure}(A, (\text{CoCardinal } X \ T)) = A$ 
    using closure_set_cocardinal by auto
  with calculation assms(1) have  $\text{Boundary}(A, (\text{CoCardinal } X \ T)) = \emptyset$  using
Boundary_def using
    union_cocardinal by auto
}
moreover
{
  assume  $AS:\neg(A \prec T) \wedge X-A \prec T$ 
  from AS(2) assms have  $\text{Closure}(X-A, (\text{CoCardinal } X \ T)) = X-A$  using closure_set_cocardinal[w
 $A=X-A$  and  $T=T$  and  $X=X$ ] by auto
  moreover
  from AS(1) assms have  $\text{Closure}(A, (\text{CoCardinal } X \ T)) = X$ 
    using closure_set_cocardinal by auto

```

```

    with calculation assms(1) have Boundary(A,(CoCardinal X T))=X-A
using Boundary_def
    union_cocardinal by auto
  }
  moreover
  {
    assume AS:~(A< T)~(X-A< T)
    from AS(2) assms have Closure(X-A,(CoCardinal X T))=X using closure_set_cocardinal[wh
A=X-A and T=T and X=X] by auto
    moreover
    from AS(1) assms have Closure(A,(CoCardinal X T))=X
    using closure_set_cocardinal by auto
    with calculation assms(1) have Boundary(A,(CoCardinal X T))=Xusing
Boundary_def
    union_cocardinal by auto
  }
  moreover
  {
    assume AS:A< T~(X-A< T)
    from AS(2) assms have Closure(X-A,(CoCardinal X T))=X using closure_set_cocardinal[wh
A=X-A and T=T and X=X] by auto
    moreover
    from AS(1) assms have Closure(A,(CoCardinal X T))=A
    using closure_set_cocardinal by auto
    with calculation assms have Boundary(A,(CoCardinal X T))=A using
Boundary_def
    union_cocardinal by auto
  }
  ultimately show thesis by auto
qed

```

### 48.2.3 Special cases and subspaces

If the set is too small or the cardinal too large, then the topology is just the discrete topology.

```

lemma discrete_cocardinal:
  assumes X< T
  shows (CoCardinal X T)=(Pow (X))
proof
  {
    fix U
    assume U∈(CoCardinal X T)
    then have U∈Pow (X) using Cocardinal_def by auto
  }
  then show (CoCardinal X T)⊆(Pow (X)) by auto
  {
    fix U
    assume A:U∈Pow(X)
    then have X-U ⊆ X by auto
  }

```

```

    then have  $X-U \lesssim X$  using subset_imp_lepoll by auto
    then have  $X-U \prec T$  using lesspoll_trans1 assms by auto
    with A have  $U \in (\text{CoCardinal } X \ T)$  using Cocardinal_def
    by auto
  }
  then show  $\text{Pow}(X) \subseteq (\text{CoCardinal } X \ T)$  by auto
qed

```

If the cardinal is taken as  $T = 1$  then the topology is indiscrete.

```

lemma indiscrete_cocardinal:
  shows  $(\text{CoCardinal } X \ 1) = \{0, X\}$ 
proof
  {
    fix Q
    assume  $Q \in (\text{CoCardinal } X \ 1)$ 
    then have  $Q \in \text{Pow}(X) \ Q = 0 \vee X - Q \prec 1$  using Cocardinal_def by auto
    then have  $Q \in \text{Pow}(X) \ Q = 0 \vee X - Q = 0$  using lesspoll_succ_iff lepoll_0_iff
  by (safe, blast)
    then have  $Q = 0 \vee Q = X$  by blast
  }
  then show  $(\text{CoCardinal } X \ 1) \subseteq \{0, X\}$  by auto
  have  $0 \in (\text{CoCardinal } X \ 1)$  using Cocardinal_def by auto
  moreover
  have  $0 \prec 1 \ X - X = 0$  using lesspoll_succ_iff by auto
  then have  $X \in (\text{CoCardinal } X \ 1)$  using Cocardinal_def by auto
  ultimately show  $\{0, X\} \subseteq (\text{CoCardinal } X \ 1)$  by auto
qed

```

The topological subspaces of the  $\text{CoCardinal } X \ T$  topology are also  $\text{CoCardinal}$  topologies.

```

lemma subspace_cocardinal:
  shows  $(\text{CoCardinal } X \ T) \text{ \{restricted to\} } Y = (\text{CoCardinal } (Y \cap X) \ T)$ 
proof
  {
    fix M
    assume  $M \in ((\text{CoCardinal } X \ T) \text{ \{restricted to\} } Y)$ 
    then obtain A where  $A1: A: (\text{CoCardinal } X \ T) \ M = Y \cap A$  using RestrictedTo_def
  by auto
    then have  $M \in \text{Pow}(X \cap Y)$  using Cocardinal_def by auto
    moreover
    from A1 have  $(Y \cap X) - M = (Y \cap X) - A$  using Cocardinal_def by auto
    have  $(Y \cap X) - A \subseteq X - A$  by blast
    with ' $(Y \cap X) - M = (Y \cap X) - A$ ' have  $(Y \cap X) - M \subseteq X - A$  by auto
    then have  $(Y \cap X) - M \lesssim X - A$  using subset_imp_lepoll by auto
    with A1 have  $(Y \cap X) - M \prec T \vee M = 0$  using lesspoll_trans1 using Cocardinal_def
    by (cases A=0, simp, cases  $Y \cap A = 0$ , simp+)
    ultimately have  $M \in (\text{CoCardinal } (Y \cap X) \ T)$  using Cocardinal_def
    by auto
  }
}

```

```

    then show (CoCardinal X T) {restricted to} Y  $\subseteq$  (CoCardinal (Y  $\cap$  X)
T) by auto
  {
    fix M
    let A=M  $\cup$  (X-Y)
    assume A:M $\in$ (CoCardinal (Y  $\cap$  X) T)
    {
      assume M=0
      hence M=0  $\cap$  Y by auto
      then have M $\in$ (CoCardinal X T) {restricted to} Y using RestrictedTo_def
        Cocardinal_def by auto
    }
    moreover
    {
      assume AS:M $\neq$ 0
      from A AS have A1:(M $\in$ Pow(Y  $\cap$  X)  $\wedge$  (Y  $\cap$  X)-M $\prec$  T) using Cocardinal_def
by auto
      hence A $\in$ Pow(X) by blast
      moreover
      have X-A=(Y  $\cap$  X)-M by blast
      with A1 have X-A $\prec$  T by auto
      ultimately have A $\in$ (CoCardinal X T) using Cocardinal_def by auto
      then have AT:Y  $\cap$  A $\in$ (CoCardinal X T) {restricted to} Y using RestrictedTo_def
        by auto
      have Y  $\cap$  A=Y  $\cap$  M by blast
      also with A1 have ...=M by auto
      finally have Y  $\cap$  A=M.
      with AT have M $\in$ (CoCardinal X T) {restricted to} Y
        by auto
    }
    ultimately have M $\in$ (CoCardinal X T) {restricted to} Y by auto
  }
  then show (CoCardinal (Y  $\cap$  X) T)  $\subseteq$  (CoCardinal X T) {restricted to}
Y by auto
qed

```

### 48.3 Excluded Set Topology

In this section, we consider all the subsets of a set which have empty intersection with a fixed set.

#### 48.3.1 Excluded set topology is a topology.

**definition**

ExcludedSet (ExcludedSet \_ \_ 50) where  
 ExcludedSet X U  $\equiv$  {F $\in$ Pow(X). U  $\cap$  F=0} $\cup$  {X}

For any set; we prove that ExcludedSet X Q forms a topology.

**theorem** excludedset\_is\_topology:

```

    shows (ExcludedSet X Q) {is a topology}
  proof-
  {
    fix M
    assume M ∈ Pow(ExcludedSet X Q)
    then have A: M ⊆ {F ∈ Pow(X). Q ∩ F = 0} ∪ {X} using ExcludedSet_def by
  auto
    hence ⋃ M ∈ Pow(X) by auto
    moreover
    {
      have B: Q ∩ ⋃ M = ⋃ {Q ∩ T. T ∈ M} by auto
      {
        assume X ∉ M
        with A have M ⊆ {F ∈ Pow(X). Q ∩ F = 0} by auto
        with B have Q ∩ ⋃ M = 0 by auto
      }
      moreover
      {
        assume X ∈ M
        with A have ⋃ M = X by auto
      }
      ultimately have Q ∩ ⋃ M = 0 ∨ ⋃ M = X by auto
    }
    ultimately have ⋃ M ∈ (ExcludedSet X Q) using ExcludedSet_def by auto
  }
  moreover
  {
    fix U V
    assume U ∈ (ExcludedSet X Q) V ∈ (ExcludedSet X Q)
    then have U ∈ Pow(X) V ∈ Pow(X) U = X ∨ U ∩ Q = 0 V = X ∨ V ∩ Q = 0 using ExcludedSet_def
  by auto
    hence U ∈ Pow(X) V ∈ Pow(X) (U ∩ V) = X ∨ Q ∩ (U ∩ V) = 0 by auto
    then have (U ∩ V) ∈ (ExcludedSet X Q) using ExcludedSet_def by auto
  }
  ultimately show thesis using IsATopology_def by auto
qed

```

```

theorem topology0_excludedset:
  shows topology0(ExcludedSet X T)
  using topology0_def excludedset_is_topology by auto

```

Choosing a singleton set, it is considered a point excluded topology.

**definition**

```

  ExcludedPoint (ExcludedPoint _ _ 90) where
  ExcludedPoint X p ≡ ExcludedSet X {p}

```

### 48.3.2 Total set, Closed sets, Interior, Closure and Boundary

The topology is defined in the set  $X$



```

lemma union_excludedset:
  shows  $\bigcup (\text{ExcludedSet } X \ T) = X$ 
proof-
  have  $X \in (\text{ExcludedSet } X \ T)$  using ExcludedSet_def by auto
  then show thesis using ExcludedSet_def by auto
qed

```

The closed sets are those which contain the set  $X \cap T$  and 0.

```

lemma closed_sets_excludedset:
  shows  $D \text{ \{is closed in\} } (\text{ExcludedSet } X \ T) \longleftrightarrow (D \in \text{Pow}(X) \ \& \ (X \cap T) \subseteq D) \vee D = 0$ 
proof-
  {
    fix x
    assume A:  $D \subseteq X$   $X - D \in (\text{ExcludedSet } X \ T)$   $D \neq 0$   $x : Tx : X$ 
    from A(1) have B:  $X - (X - D) = D$  by auto
    from A(2) have  $T \cap (X - D) = 0 \vee X - D = X$  using ExcludedSet_def by auto
    hence  $T \cap (X - D) = 0 \vee X - (X - D) = X - X$  by auto
    with B have  $T \cap (X - D) = 0 \vee D = X - X$  by auto
    hence  $T \cap (X - D) = 0 \vee D = 0$  by auto
    with A(3) have  $T \cap (X - D) = 0$  by auto
    with A(4) have  $x \notin X - D$  by auto
    with A(5) have  $x \in D$  by auto
  }
  moreover
  {
    assume A:  $X \cap T \subseteq D \subseteq X$ 
    from A(1) have  $X - D \subseteq X - (X \cap T)$  by auto
    also have  $\dots = X - T$  by auto
    finally have  $T \cap (X - D) = 0$  by auto
    moreover
    have  $X - D \in \text{Pow}(X)$  by auto
    ultimately have  $X - D \in (\text{ExcludedSet } X \ T)$  using ExcludedSet_def by auto
  }
  ultimately show thesis using IsClosed_def union_excludedset
    ExcludedSet_def by auto
qed

```

The interior of a set is itself if it is  $X$  or the difference with the set  $T$

```

lemma interior_set_excludedset:
  assumes  $A \subseteq X$ 
  shows  $\text{Interior}(A, (\text{ExcludedSet } X \ T)) = (\text{if } A = X \text{ then } X \text{ else } A - T)$ 
proof-
  {
    assume A:  $A \neq X$ 
    from assms have  $A - T \in (\text{ExcludedSet } X \ T)$  using ExcludedSet_def by auto
    then have  $A - T \subseteq \text{Interior}(A, (\text{ExcludedSet } X \ T))$ 
    using Interior_def by auto
    moreover

```

```

    {
      fix U
      assume  $U \in (\text{ExcludedSet } X \ T) \cup A$ 
      then have  $T \cap U = 0 \vee U = X \cup A$  using ExcludedSet_def by auto
      with A assms have  $T \cap U = 0 \cup A$  by auto
      then have  $U - T = U \cup U - T \subseteq A - T$  by (safe,blast+)
      then have  $U \subseteq A - T$  by auto
    }
    then have  $\text{Interior}(A, (\text{ExcludedSet } X \ T)) \subseteq A - T$  using Interior_def by
  auto
    ultimately have  $\text{Interior}(A, (\text{ExcludedSet } X \ T)) = A - T$  by auto
  }
  moreover
  have  $X \in (\text{ExcludedSet } X \ T)$  using ExcludedSet_def
  union_excludedset by auto
  then have  $\text{Interior}(X, (\text{ExcludedSet } X \ T)) = X$  using topology0.Top_2_L3
  topology0_excludedset by auto
  ultimately show thesis by auto
qed

```

The closure of a set is itself if it is 0 or the union with T.

```

lemma closure_set_excludedset:
  assumes  $A \subseteq X$ 
  shows  $\text{Closure}(A, (\text{ExcludedSet } X \ T)) = (\text{if } A = 0 \text{ then } 0 \text{ else } A \cup (X \cap T))$ 
proof-
  have  $0 \in \text{ClosedCovers}(0, (\text{ExcludedSet } X \ T))$  using ClosedCovers_def
  closed_sets_excludedset by auto
  then have  $\text{Closure}(0, (\text{ExcludedSet } X \ T)) \subseteq 0$  using Closure_def by auto
  hence  $\text{Closure}(0, (\text{ExcludedSet } X \ T)) = 0$  by blast
  moreover
  {
    assume  $A \neq 0$ 
    then have  $(A \cup (X \cap T)) \{\text{is closed in}\} (\text{ExcludedSet } X \ T)$ 
      using closed_sets_excludedset[of  $A \cup (X \cap T)$ ] assms A
      by blast
    then have  $(A \cup (X \cap T)) \in \{D \in \text{Pow}(X). D \{\text{is closed in}\} (\text{ExcludedSet } X \ T) \wedge A \subseteq D\}$ 
      using assms by auto
    then have  $(A \cup (X \cap T)) \in \text{ClosedCovers}(A, (\text{ExcludedSet } X \ T))$  unfolding
  ClosedCovers_def
  using union_excludedset by auto
  then have l1:  $\bigcap \text{ClosedCovers}(A, (\text{ExcludedSet } X \ T)) \subseteq (A \cup (X \cap T))$  by
  blast
  {
    fix U
    assume  $U \in \text{ClosedCovers}(A, (\text{ExcludedSet } X \ T))$ 
    then have  $U \{\text{is closed in}\} (\text{ExcludedSet } X \ T) \wedge A \subseteq U$  using ClosedCovers_def
    union_excludedset by auto
    then have  $U = 0 \vee (X \cap T) \subseteq U \subseteq A \cup (X \cap T)$  using closed_sets_excludedset

```

```

    by auto
    then have  $(X \cap T) \subseteq UA \subseteq U$  using A by auto
    then have  $(X \cap T) \cup A \subseteq U$  by auto
  }
  then have  $(A \cup (X \cap T)) \subseteq \bigcap \text{ClosedCovers}(A, (\text{ExcludedSet } X \ T))$  using topology0.Top_3_L3
    topology0_excludedset union_excludedset assms by auto
  with l1 have  $\bigcap \text{ClosedCovers}(A, (\text{ExcludedSet } X \ T)) = (A \cup (X \cap T))$  by auto
  then have  $\text{Closure}(A, \text{ExcludedSet } X \ T) = (A \cup (X \cap T))$ 
    using Closure_def by auto
}
ultimately show thesis by auto
qed

```

The boundary of a set is 0 if  $A$  is  $X$  or 0, and  $X \cap T$  in other case.

```

lemma boundary_excludedset:
  assumes  $A \subseteq X$ 
  shows  $\text{Boundary}(A, (\text{ExcludedSet } X \ T)) = (\text{if } A=0 \vee A=X \text{ then } 0 \text{ else } X \cap T)$ 
proof-
{
  have  $\text{Closure}(0, (\text{ExcludedSet } X \ T)) = 0$ 
  have  $\text{Closure}(X - 0, (\text{ExcludedSet } X \ T)) = X$ 
  using closure_set_excludedset by auto
  then have  $\text{Boundary}(0, (\text{ExcludedSet } X \ T)) = 0$ 
  using Boundary_def using
    union_excludedset assms by auto
}
moreover
{
  have  $X - X = 0$  by blast
  then have  $\text{Closure}(X, (\text{ExcludedSet } X \ T)) = X$ 
  using closure_set_excludedset by auto
  then have  $\text{Boundary}(X, (\text{ExcludedSet } X \ T)) = 0$ 
  using Boundary_def using
    union_excludedset by auto
}
moreover
{
  assume AS:  $(A \neq 0) \wedge (A \neq X)$ 
  then have  $(A \neq 0) (X - A \neq 0)$  using assms by (safe,blast)
  then have  $\text{Closure}(A, (\text{ExcludedSet } X \ T)) = A \cup (X \cap T)$ 
  using closure_set_excludedset[where A=A and X=X] assms closure_set_excludedset[where
    A=X-A
    and X=X] by auto
  then have  $\text{Boundary}(A, (\text{ExcludedSet } X \ T)) = X \cap T$ 
  using Boundary_def
    union_excludedset by auto
}
ultimately show thesis by auto
qed

```

### 48.3.3 Special cases and subspaces

The topology is equal in the sets  $T$  and  $X \cap T$ .

```
lemma smaller_excludedset:
  shows (ExcludedSet X T)=(ExcludedSet X (X∩T))
  using ExcludedSet_def by (simp,blast)
```

If the set which is excluded is disjoint with  $X$ , then the topology is discrete.

```
lemma empty_excludedset:
  assumes  $T \cap X = 0$ 
  shows (ExcludedSet X T)=Pow(X)
  using smaller_excludedset assms ExcludedSet_def by (simp,blast)
```

The topological subspaces of the ExcludedSet  $X$   $T$  topology are also ExcludedSet topologies.

```
lemma subspace_excludedset:
  shows (ExcludedSet X T) {restricted to} Y=(ExcludedSet (Y ∩ X) T)
proof
  {
    fix M
    assume  $M \in ((\text{ExcludedSet } X \ T) \ \{\text{restricted to}\} \ Y)$ 
    then obtain A where  $A1:A:(\text{ExcludedSet } X \ T) \ M=Y \cap A$  unfolding RestrictedTo_def
  by auto
    then have  $M \in \text{Pow}(X \cap Y)$  unfolding ExcludedSet_def by auto
    moreover
    from A1 have  $T \cap M = 0 \vee M=Y \cap X$  unfolding ExcludedSet_def by blast
    ultimately have  $M \in (\text{ExcludedSet } (Y \cap X) \ T)$  unfolding ExcludedSet_def
      by auto
  }
  then show (ExcludedSet X T) {restricted to} Y  $\subseteq$  (ExcludedSet (Y ∩ X)
T) by auto
  {
    fix M
    let  $A=M \cup ((X \cap Y - T) - Y)$ 
    assume  $A:M \in (\text{ExcludedSet } (Y \cap X) \ T)$ 
    {
      assume  $M=Y \cap X$ 
      then have  $M \in (\text{ExcludedSet } X \ T) \ \{\text{restricted to}\} \ Y$  unfolding RestrictedTo_def
        ExcludedSet_def by auto
    }
    moreover
    {
      assume  $AS:M \neq Y \cap X$ 
      from A AS have  $A1:(M \in \text{Pow}(Y \cap X) \ \wedge \ T \cap M = 0)$  unfolding ExcludedSet_def
    by auto
      then have  $A \in \text{Pow}(X)$  by blast
      moreover
      have  $T \cap A = T \cap M$  by blast
      with A1 have  $T \cap A = 0$  by auto
    }
  }
}
```

```

      ultimately have  $A \in (\text{ExcludedSet } X \ T)$  unfolding ExcludedSet_def by
auto
      then have  $AT: Y \cap A \in (\text{ExcludedSet } X \ T)$  {restricted to} Yunfolding
RestrictedTo_def
      by auto
      have  $Y \cap A = Y \cap M$  by blast
      also have  $\dots = M$  using A1 by auto
      finally have  $Y \cap A = M$ .
      then have  $M \in (\text{ExcludedSet } X \ T)$  {restricted to} Y using AT
      by auto
    }
    ultimately have  $M \in (\text{ExcludedSet } X \ T)$  {restricted to} Y by auto
  }
  then show  $(\text{ExcludedSet } (Y \cap X) \ T) \subseteq (\text{ExcludedSet } X \ T)$  {restricted
to} Y by auto
qed

```

## 48.4 Included Set Topology

In this section we consider the subsets of a set which contain a fixed set.

The family defined in this section and the one in the previous section are dual; meaning that the closed set of one are the open sets of the other.

### 48.4.1 Included set topology is a topology.

**definition**

```

IncludedSet (IncludedSet _ _ 50) where
IncludedSet X U  $\equiv \{F \in \text{Pow}(X). U \subseteq F\} \cup \{0\}$ 

```

For any set; we prove that  $\text{IncludedSet } X \ Q$  forms a topology.

**theorem** includedset\_is\_topology:

```

shows  $(\text{IncludedSet } X \ Q)$  {is a topology}

```

**proof-**

```

{
  fix M
  assume  $M \in \text{Pow}(\text{IncludedSet } X \ Q)$ 
  then have  $A: M \subseteq \{F \in \text{Pow}(X). Q \subseteq F\} \cup \{0\}$  using IncludedSet_def by auto
  then have  $\bigcup M \in \text{Pow}(X)$  by auto
  moreover
  have  $Q \subseteq \bigcup M \vee \bigcup M = 0$  using A by blast
  ultimately have  $\bigcup M \in (\text{IncludedSet } X \ Q)$  using IncludedSet_def by auto
}
moreover
{
  fix U V
  assume  $U \in (\text{IncludedSet } X \ Q) \ V \in (\text{IncludedSet } X \ Q)$ 
  then have  $U \in \text{Pow}(X) \ V \in \text{Pow}(X) \ U = 0 \vee Q \subseteq U \vee Q \subseteq V$  using IncludedSet_def
by auto

```

```

    then have  $U \in \text{Pow}(X) \vee V \in \text{Pow}(X) \wedge (U \cap V) = \emptyset \vee Q \subseteq (U \cap V)$  by auto
    then have  $(U \cap V) \in (\text{IncludedSet } X \ Q)$  using IncludedSet_def by auto
  }
  ultimately show thesis using IsATopology_def by auto
qed

```

```

theorem topology0_includedset:
  shows topology0(IncludedSet X T)
  using topology0_def includedset_is_topology by auto

```

Choosing a singleton set, it is considered a point excluded topology. In the following lemmas and theorems, when necessary it will be considered that  $T \neq \emptyset$  and  $T \subseteq X$ . These cases will appear in the special cases section.

**definition**

```

IncludedPoint (IncludedPoint _ _ 90) where
IncludedPoint X p  $\equiv$  IncludedSet X {p}

```

#### 48.4.2 Total set, Closed sets, Interior, Closure and Boundary

The topology is defined in the set  $X$ .

```

lemma union_includedset:
  assumes  $T \subseteq X$ 
  shows  $\bigcup (\text{IncludedSet } X \ T) = X$ 
proof-
  from assms have  $X \in (\text{IncludedSet } X \ T)$  using IncludedSet_def by auto
  then show  $\bigcup (\text{IncludedSet } X \ T) = X$  using IncludedSet_def by auto
qed

```

The closed sets are those which are disjoint with  $T$  and  $X$ .

```

lemma closed_sets_includedset:
  assumes  $T \subseteq X$ 
  shows  $D \text{ \{is closed in\} } (\text{IncludedSet } X \ T) \longleftrightarrow (D \in \text{Pow}(X) \ \& \ (D \cap T) = \emptyset) \vee D = X$ 
proof-
  have  $X - X = \emptyset$  by blast
  then have  $X - X \in (\text{IncludedSet } X \ T)$  using IncludedSet_def by auto
  moreover
  {
    assume  $A: D \subseteq X \wedge X - D \in (\text{IncludedSet } X \ T) \wedge D \neq X$ 
    from A(2) have  $T \subseteq (X - D) \vee X - D = \emptyset$  using IncludedSet_def by auto
    with A(1) have  $T \subseteq (X - D) \vee D = X$  by blast
    with A(3) have  $T \subseteq (X - D)$  by auto
    hence  $D \cap T = \emptyset$  by blast
  }
  moreover
  {
    assume  $A: D \cap T = \emptyset \wedge D \subseteq X$ 
    from A(1) assms have  $T \subseteq (X - D)$  by blast

```

```

    then have X-D∈(IncludedSet X T) using IncludedSet_def by auto
  }
  ultimately show thesis using IsClosed_def union_includedset assms by
auto
qed

```

The interior of a set is itself if it is open or 0 if it isn't.

```

lemma interior_set_includedset:
  assumes  $A \subseteq X$ 
  shows  $\text{Interior}(A, (\text{IncludedSet } X \ T)) = (\text{if } T \subseteq A \text{ then } A \text{ else } 0)$ 
proof-
{
  fix x
  assume A:  $\text{Interior}(A, \text{IncludedSet } X \ T) \neq 0$   $x \in T$ 
  have  $\text{Interior}(A, \text{IncludedSet } X \ T) \in (\text{IncludedSet } X \ T)$  using
    topology0.Top_2_L2 topology0_includedset by auto
  with A(1) have  $T \subseteq \text{Interior}(A, \text{IncludedSet } X \ T)$  using IncludedSet_def
    by auto
  with A(2) have  $x \in \text{Interior}(A, \text{IncludedSet } X \ T)$  by auto
  then have  $x \in A$  using topology0.Top_2_L1 topology0_includedset by auto}
moreover
{
  assume  $T \subseteq A$ 
  with assms have  $A \in (\text{IncludedSet } X \ T)$  using IncludedSet_def by auto
  then have  $\text{Interior}(A, \text{IncludedSet } X \ T) = A$  using topology0.Top_2_L3
    topology0_includedset by auto
}
ultimately show thesis by auto
qed

```

The closure of a set is itself if it is closed or X if it isn't.

```

lemma closure_set_includedset:
  assumes  $A \subseteq X \ T \subseteq X$ 
  shows  $\text{Closure}(A, (\text{IncludedSet } X \ T)) = (\text{if } T \cap A = 0 \text{ then } A \text{ else } X)$ 
proof-
{
  assume AS:  $T \cap A = 0$ 
  then have A {is closed in}  $(\text{IncludedSet } X \ T)$  using closed_sets_includedset
    assms by auto
  with assms(1) have  $\text{Closure}(A, (\text{IncludedSet } X \ T)) = A$  using topology0.Top_3_L8
    topology0_includedset union_includedset assms(2) by auto
}
moreover
{
  assume AS:  $T \cap A \neq 0$ 
  have  $X \in \text{ClosedCovers}(A, (\text{IncludedSet } X \ T))$  using ClosedCovers_def
    closed_sets_includedset union_includedset assms by auto
  then have l1:  $\bigcap \text{ClosedCovers}(A, (\text{IncludedSet } X \ T)) \subseteq X$  using Closure_def
    by auto
}

```

```

moreover
{
  fix U
  assume  $U \in \text{ClosedCovers}(A, (\text{IncludedSet } X \ T))$ 
  then have  $U \{ \text{is closed in} \} (\text{IncludedSet } X \ T) A \subseteq U$  using ClosedCovers_def
  by auto
  then have  $U = X \vee (T \cap U) = 0 \wedge A \subseteq U$  using closed_sets_includedset assms(2)
  by auto
  then have  $U = X \vee (T \cap A) = 0$  by auto
  then have  $U = X$  using AS by auto
}
then have  $X \subseteq \bigcap \text{ClosedCovers}(A, (\text{IncludedSet } X \ T))$  using topology0.Top_3_L3
topology0_includedset union_includedset assms by auto
ultimately have  $\bigcap \text{ClosedCovers}(A, (\text{IncludedSet } X \ T)) = X$  by auto
then have  $\text{Closure}(A, \text{IncludedSet } X \ T) = X$ 
using Closure_def by auto
}
ultimately show thesis by auto
qed

```

The boundary of a set is  $X - A$  if  $A$  contains  $T$  completely, is  $A$  if  $X - A$  contains  $T$  completely and  $X$  if  $T$  is divided between the two sets. The case where  $T = 0$  is considered as an special case.

```

lemma boundary_includedset:
  assumes  $A \subseteq XT \subseteq XT \neq 0$ 
  shows  $\text{Boundary}(A, (\text{IncludedSet } X \ T)) = (\text{if } T \subseteq A \text{ then } X - A \text{ else } (\text{if } T \cap A = 0 \text{ then } A \text{ else } X))$ 
proof-
{
  assume AS:  $(T \subseteq A)$ 
  then have  $T \cap A \neq 0 \wedge T \cap (X - A) = 0$  using assms(2,3) by (auto,blast)
  then have  $\text{Closure}(A, (\text{IncludedSet } X \ T)) = X \text{Closure}(X - A, (\text{IncludedSet } X \ T)) = (X - A)$ 
  using closure_set_includedset[where  $A=A$  and  $X=X$  and  $T=T$ ] assms(1,2)
  closure_set_includedset[where  $A=X - A$ 
  and  $X=X$  and  $T=T$ ] by auto
  then have  $\text{Boundary}(A, (\text{IncludedSet } X \ T)) = X - A$  unfolding Boundary_def
using
  union_includedset assms(2) by auto
}
moreover
{
  assume AS:  $\sim(T \subseteq A) \wedge T \cap A = 0$ 
  then have  $T \cap A = 0 \wedge T \cap (X - A) \neq 0$  using assms(2) by (safe,blast+)
  then have  $\text{Closure}(A, (\text{IncludedSet } X \ T)) = A \text{Closure}(X - A, (\text{IncludedSet } X \ T)) = X$ 
  using closure_set_includedset[where  $A=A$  and  $X=X$  and  $T=T$ ] assms(1,2)
  closure_set_includedset[where  $A=X - A$ 
  and  $X=X$  and  $T=T$ ] by auto
}

```



```

    then have Boundary(A,(IncludedSet X T))=A unfolding Boundary_def
using
    union_includedset assms(1,2) by auto
  }
  moreover
  {
    assume AS:~(T⊆A)T∩A≠0
    then have T∩A≠0T∩(X-A)≠0 using assms(2) by (safe,blast+)
    then have Closure(A,(IncludedSet X T))=XClosure(X-A,(IncludedSet
X T))=X
      using closure_set_includedset[where A=A and X=Xand T=T] assms(1,2)
closure_set_includedset[where A=X-A
and X=Xand T=T] by auto
    then have Boundary(A,(IncludedSet X T))=X unfolding Boundary_def
using
    union_includedset assms(2) by auto
  }
  ultimately show thesis by auto
qed

```

#### 48.4.3 Special cases and subspaces

The topology is discrete if  $T = 0$

```

lemma smaller_includedset:
  shows (IncludedSet X 0)=Pow(X)
  using IncludedSet_def by (simp,blast)

```

If the set which is included is not a subset of  $X$ , then the topology is trivial.

```

lemma empty_includedset:
  assumes ~ (T⊆X)
  shows (IncludedSet X T)={0}
  using assms IncludedSet_def by (simp,blast)

```

The topological subspaces of the  $\text{IncludedSet } X \text{ } T$  topology are also  $\text{IncludedSet}$  topologies. The trivial case does not fit the idea in the demonstration; because if  $Y \subseteq X$  then  $\text{IncludedSet } Y \cap X \text{ } Y \cap T$  is never trivial. There is no need of a separate proof because the only subspace of the trivial topology is itself.

```

lemma subspace_includedset:
  assumes T⊆X
  shows (IncludedSet X T) {restricted to} Y=(IncludedSet (Y ∩ X) (Y∩T))
proof
  {
    fix M
    assume M∈((IncludedSet X T) {restricted to} Y)
    then obtain A where A1:A:(IncludedSet X T) M=Y ∩ A unfolding RestrictedTo_def
  by auto
    then have M∈Pow(X ∩ Y) unfolding IncludedSet_def by auto
  }

```

```

    moreover
    from A1 have  $Y \cap T \subseteq M \vee M = 0$  unfolding IncludedSet_def by blast
    ultimately have  $M \in (\text{IncludedSet } (Y \cap X) (Y \cap T))$  unfolding IncludedSet_def
    by auto
  }
  then show  $(\text{IncludedSet } X \ T) \ \{\text{restricted to}\} \ Y \subseteq (\text{IncludedSet } (Y \cap X) \ (Y \cap T))$ 
  by auto
  {
    fix M
    let A =  $M \cup T$ 
    assume A:  $M \in (\text{IncludedSet } (Y \cap X) (Y \cap T))$ 
    {
      assume M=0
      then have  $M \in (\text{IncludedSet } X \ T) \ \{\text{restricted to}\} \ Y$  unfolding RestrictedTo_def
      IncludedSet_def by auto
    }
    moreover
    {
      assume AS:  $M \neq 0$ 
      from A AS have A1:  $(M \in \text{Pow}(Y \cap X) \wedge Y \cap T \subseteq M)$  unfolding IncludedSet_def
    by auto
      then have  $A \in \text{Pow}(X)$  using assms by blast
      moreover
      have  $T \subseteq A$  by blast
      ultimately have  $A \in (\text{IncludedSet } X \ T)$  unfolding IncludedSet_def by
    auto
      then have AT:  $Y \cap A \in (\text{IncludedSet } X \ T) \ \{\text{restricted to}\} \ Y$  unfolding
    RestrictedTo_def
      by auto
      from A1 have  $Y \cap A = Y \cap M$  by blast
      also with A1 have ... =  $M$  by auto
      finally have  $Y \cap A = M$ .
      with AT have  $M \in (\text{IncludedSet } X \ T) \ \{\text{restricted to}\} \ Y$ 
      by auto
    }
    ultimately have  $M \in (\text{IncludedSet } X \ T) \ \{\text{restricted to}\} \ Y$  by auto
  }
  thus  $(\text{IncludedSet } (Y \cap X) (Y \cap T)) \subseteq (\text{IncludedSet } X \ T) \ \{\text{restricted}$ 
to} Y by auto
qed

end

```

## 49 Topology\_ZF\_examples\_1.thy

```
theory Topology_ZF_examples_1
imports Topology_ZF_1 Order_ZF
begin
```

In this theory file we reformulate the concepts related to a topology in relation with a base of the topology and we give examples of topologies defined by bases or subbases.

### 49.1 New ideas using a base for a topology

#### 49.1.1 The topology of a base

Given a family of subsets satisfying the base condition, it is possible to construct a topology where that family is a base. Even more, it is the only topology with such characteristics.

**definition**

```
TopologyWithBase (TopologyBase _ 50) where
  U {satisfies the base condition}  $\implies$  TopologyBase U  $\equiv$  THE T. U {is a
base for} T
```

**theorem** Base\_topology\_is\_a\_topology:

```
  assumes U {satisfies the base condition}
  shows (TopologyBase U) {is a topology} and U {is a base for} (TopologyBase
U)
```

**proof-**

```
  from assms obtain T where U {is a base for} T using
    Top_1_2_T1(2) by blast
  then have  $\exists!$ T. U {is a base for} T using same_base_same_top ex1I[where
P=
   $\lambda$ T. U {is a base for} T] by blast
  with assms show U {is a base for} (TopologyBase U) using theI[where
P=
   $\lambda$ T. U {is a base for} T] TopologyWithBase_def by auto
  with assms show (TopologyBase U) {is a topology} using Top_1_2_T1(1)
    IsABaseFor_def by auto
```

qed

A base doesn't need the empty set.

**lemma** base\_no\_0:

```
  shows B{is a base for}T  $\longleftrightarrow$  (B-{0}){is a base for}T
```

**proof-**

```
{
  fix M
  assume  $M \in \{\bigcup A \mid A \in \text{Pow}(B)\}$ 
  then obtain Q where  $M = \bigcup Q$   $Q \in \text{Pow}(B)$  by auto
  hence  $M = \bigcup (Q - \{0\})$   $Q - \{0\} \in \text{Pow}(B - \{0\})$  by auto
```

```

    hence  $M \in \{\bigcup A . A \in \text{Pow}(B - \{0\})\}$  by auto
  }
  hence  $\{\bigcup A . A \in \text{Pow}(B)\} \subseteq \{\bigcup A . A \in \text{Pow}(B - \{0\})\}$  by blast
  moreover
  {
    fix M
    assume  $M \in \{\bigcup A . A \in \text{Pow}(B - \{0\})\}$ 
    then obtain Q where  $M = \bigcup Q Q \in \text{Pow}(B - \{0\})$  by auto
    hence  $M = \bigcup (Q) Q \in \text{Pow}(B)$  by auto
    hence  $M \in \{\bigcup A . A \in \text{Pow}(B)\}$  by auto
  }
  hence  $\{\bigcup A . A \in \text{Pow}(B - \{0\})\} \subseteq \{\bigcup A . A \in \text{Pow}(B)\}$ 
    by auto
  ultimately have  $\{\bigcup A . A \in \text{Pow}(B - \{0\})\} = \{\bigcup A . A \in \text{Pow}(B)\}$  by auto
  then show  $B\{\text{is a base for}\}T \longleftrightarrow (B - \{0\})\{\text{is a base for}\}T$  using IsAbaseFor_def
by auto
qed

```

The interior of a set is the union of all the sets of the base which are fully contained by it.

```

lemma interior_set_base_topology:
  assumes U {is a base for} TT{is a topology}
  shows  $\text{Interior}(A, T) = \bigcup \{T \in U. T \subseteq A\}$ 
proof
  have  $\{T \in U. T \subseteq A\} \subseteq U$  by auto
  with assms(1) have  $\bigcup \{T \in U. T \subseteq A\} \in T$ 
    using IsAbaseFor_def by auto
  moreover
  have  $\bigcup \{T \in U. T \subseteq A\} \subseteq A$  by blast
  with calculation assms(2) show  $\bigcup \{T \in U. T \subseteq A\} \subseteq \text{Interior}(A, T)$ 
    using topology0.Top_2_L5 topology0_def by auto
  {
    fix x
    assume  $x \in \text{Interior}(A, T)$ 
    with assms obtain V where  $V \in UV \subseteq \text{Interior}(A, T) x \in V$ 
      using point_open_base_neigh
      topology0.Top_2_L2 topology0_def by blast
    with assms have  $V \in U x \in V V \subseteq A$  using topology0.Top_2_L1 topology0_def
      by (safe, blast)
    hence  $x \in \bigcup \{T \in U. T \subseteq A\}$  by auto
  }
  thus  $\text{Interior}(A, T) \subseteq \bigcup \{T \in U . T \subseteq A\}$  by auto
qed

```

In the following, we offer another lemma about the closure of a set given a basis for a topology. This lemma is based on `cl_inter_neigh` and `inter_neigh_cl`. It states that it is only necessary to check the sets of the base, not all the open sets.

```

lemma closure_set_base_topology:

```

```

assumes U {is a base for} QQ{is a topology}  $A \subseteq \bigcup Q$ 
shows Closure(A,Q) =  $\{x \in \bigcup Q. \forall T \in U. x \in T \longrightarrow A \cap T \neq \emptyset\}$ 
proof
{
  fix x
  assume A:  $x \in \text{Closure}(A,Q)$ 
  with assms(2,3) have B:  $x \in \bigcup Q$  using topology0_def topology0.Top_3_L11(1)
  by blast
  moreover
  {
    fix T
    assume T:  $x \in T$ 
    with assms(1) have TQ:  $x \in T$  using base_sets_open
    by auto
    with assms(2,3) A have AT:  $A \cap T \neq \emptyset$  using topology0_def
      topology0.cl_inter_neigh[where U=T and T=Q and A=A]
    by auto
  }
  hence VTU:  $\forall T \in U. x \in T \longrightarrow A \cap T \neq \emptyset$  by auto
  ultimately have xBUQ:  $x \in \{x \in \bigcup Q. \forall T \in U. x \in T \longrightarrow A \cap T \neq \emptyset\}$  by auto
}
thus Closure(A, Q)  $\subseteq \{x \in \bigcup Q. \forall T \in U. x \in T \longrightarrow A \cap T \neq \emptyset\}$ 
  by auto
{
  fix x
  assume AS:  $x \in \{x \in \bigcup Q. \forall T \in U. x \in T \longrightarrow A \cap T \neq \emptyset\}$ 
  hence xBUQ by blast
  moreover
  {
    fix R
    assume R:  $x \in R$ 
    with assms(1) obtain W where RR:  $W \subseteq R$  using
      IsABaseFor_def by auto
    {
      assume xR:  $x \in R$ 
      with RR(2) obtain WW where TT:  $WW \subseteq W$  by auto
      {
        assume RnA:  $R \cap A = \emptyset$ 
        with RR(2) TT(1) have WWnA:  $WW \cap A = \emptyset$  by auto
        with TT(1) RR(1) have WWUWnA:  $WW \subseteq U \cap WW \cap A = \emptyset$  by auto
        with AS have xBUQWW:  $x \in \bigcup Q - WW$  by auto
        with TT(2) have False by auto
      }
      hence RnAne0:  $R \cap A \neq \emptyset$  by auto
    }
  }
}
hence VUQ:  $\forall U \in Q. x \in U \longrightarrow U \cap A \neq \emptyset$  by auto
with calculation assms(2,3) have xClosure(A,Q) using topology0_def
  topology0.inter_neigh_cl by auto

```

```

}
then show  $\{x \in \bigcup Q . \forall T \in U. x \in T \longrightarrow A \cap T \neq \emptyset\} \subseteq \text{Closure}(A, Q)$ 
by auto
qed

```

The restriction of a base is a base for the restriction.

```

lemma subspace_base_topology:
  assumes B{is a base for}T
  shows (B{restricted to}Y){is a base for}(T{restricted to}Y)
proof-
{
  fix t
  assume  $t \in \text{RepFun}(\{\bigcup A . A \in \text{Pow}(B)\}, \text{op } \cap(Y))$ 
  then obtain x where  $A: t = Y \cap x \in \{\bigcup A . A \in \text{Pow}(B)\}$  by auto
  then obtain A where  $B: x = \bigcup AA \in \text{Pow}(B)$  by auto
  from A(1) B(1) have  $t = \bigcup (A \text{ {restricted to} } Y)$  using RestrictedTo_def
  by auto
  with B(2) have  $t \in \{\bigcup A . A \in \text{Pow}(\text{RepFun}(B, \text{op } \cap(Y)))\}$  unfolding RestrictedTo_def
  by blast
}
hence  $\text{RepFun}(\{\bigcup A . A \in \text{Pow}(B)\}, \text{op } \cap(Y)) \subseteq \{\bigcup A . A \in \text{Pow}(\text{RepFun}(B, \text{op } \cap(Y)))\}$ 
by(auto+)
moreover
{
  fix t
  assume  $t \in \{\bigcup A . A \in \text{Pow}(\text{RepFun}(B, \text{op } \cap(Y)))\}$ 
  then obtain A where  $A: A \subseteq B \text{ {restricted to} } Y, t = \bigcup A$  using RestrictedTo_def
  by auto
  let  $AA = \{C \in B. Y \cap C \in A\}$ 
  from A(1) have  $AA \subseteq B \text{ {restricted to} } Y$  using RestrictedTo_def
  by auto
  with A(2) have  $AA \subseteq B \text{ {restricted to} } Y$  by auto
  then have  $AA \subseteq B \text{ {restricted to} } Y$  using RestrictedTo_def by auto
  hence  $t \in \text{RepFun}(\{\bigcup A . A \in \text{Pow}(B)\}, \text{op } \cap(Y))$  by auto
}
hence  $\{\bigcup A . A \in \text{Pow}(\text{RepFun}(B, \text{op } \cap(Y)))\} \subseteq \text{RepFun}(\{\bigcup A . A \in \text{Pow}(B)\}, \text{op } \cap(Y))$ 
by (auto+)
ultimately have  $\{\bigcup A . A \in \text{Pow}(\text{RepFun}(B, \text{op } \cap(Y)))\} = \text{RepFun}(\{\bigcup A . A \in \text{Pow}(B)\}, \text{op } \cap(Y))$ 
by auto
with assms show thesis using RestrictedTo_def IsAbaseFor_def by auto
qed

```

If the base of a topology is contained in the base of another topology, then the topologies maintain the same relation.

```

theorem base_subset:
  assumes B{is a base for}TB2{is a base for}T2  $B \subseteq B2$ 
  shows  $T \subseteq T2$ 
proof
{

```

```

fix x
assume x ∈ T
with assms(1) obtain M where  $M \subseteq Bx = \bigcup M$  using IsAbaseFor_def by auto
with assms(3) have  $M \subseteq B2x = \bigcup M$  by auto
with assms(2) show  $x \in T2$  using IsAbaseFor_def by auto
}
qed

```

#### 49.1.2 Dual Base for Closed Sets

A dual base for closed sets is the collection of complements of sets of a base for the topology.

**definition**

DualBase (DualBase \_ \_ 80) where  
 $B\{\text{is a base for}\}T \implies \text{DualBase } B \ T \equiv \{\bigcup T - U. \ U \in B\} \cup \{\bigcup T\}$

**lemma** closed\_inter\_dual\_base:

assumes  $D\{\text{is closed in}\}TB\{\text{is a base for}\}T$   
 obtains M where  $M \subseteq \text{DualBase } B \ T$  and  $D = \bigcap M$

**proof-**

```

assume K:  $\bigwedge M. \ M \subseteq \text{DualBase } B \ T \implies D = \bigcap M \implies \text{thesis}$ 
{
  assume AS:  $D \neq \bigcup T$ 
  from assms(1) have D:  $D \in \text{Pow}(\bigcup T) \cup T - D \in T$  using IsClosed_def by auto
  hence A:  $\bigcup T - (\bigcup T - D) = D \cup T - D \in T$  by auto
  with assms(2) obtain Q where QQ:  $Q \in \text{Pow}(B) \cup T - D = \bigcup Q$  using IsAbaseFor_def
by auto
{
  assume Q=0
  then have  $\bigcup Q = 0$  by auto
  with QQ(2) have  $\bigcup T - D = 0$  by auto
  with D(1) have  $D = \bigcup T$  by auto
  with AS have False by auto
}
hence QNN:  $Q \neq 0$  by auto
from QQ(2) A(1) have D:  $D = \bigcup T - \bigcup Q$  by auto
with QNN have D:  $D = \bigcap \{\bigcup T - R. \ R \in Q\}$  by auto
moreover
with assms(2) QQ(1) have  $\{\bigcup T - R. \ R \in Q\} \subseteq \text{DualBase } B \ T$  using DualBase_def
by auto
with calculation K have thesis by auto
}
moreover
{
  assume AS:  $D = \bigcup T$ 
  with assms(2) have  $\{\bigcup T\} \subseteq \text{DualBase } B \ T$  using DualBase_def by auto
  moreover
  have  $\bigcup T = \bigcap \{\bigcup T\}$  by auto
}

```

```

    with calculation K AS have thesis by auto
  }
  ultimately show thesis by auto
qed

```

We have already seen for a base that whenever there is a union of open sets, we can consider only basic open sets due to the fact that any open set is a union of basic open sets. What we should expect now is that when there is an intersection of closed sets, we can consider only dual basic closed sets.

```

lemma closure_dual_base:
  assumes U {is a base for} QQ{is a topology}  $A \subseteq \bigcup Q$ 
  shows  $\text{Closure}(A, Q) = \bigcap \{T \in \text{DualBase } U \ Q. A \subseteq T\}$ 
proof
  from assms(1) have  $T: \bigcup Q \in \text{DualBase } U \ Q$  using DualBase_def by auto
  moreover
  {
    fix T
    assume  $A: T \in \text{DualBase } U \ Q \ A \subseteq T$ 
    with assms(1) obtain R where  $(T = \bigcup Q - R \wedge R \in U) \vee T = \bigcup Q$  using DualBase_def
    by auto
    with A(2) assms(1,2) have  $(T \text{ is closed in } Q) \wedge A \subseteq T \in \text{Pow}(\bigcup Q)$  using
topology0.Top_3_L1 topology0_def
    topology0.Top_3_L9 base_sets_open by auto
  }
  then have  $\text{SUB}: \{T \in \text{DualBase } U \ Q. A \subseteq T\} \subseteq \{T \in \text{Pow}(\bigcup Q). (T \text{ is closed in } Q) \wedge A \subseteq T\}$ 
  by blast
  with calculation assms(3) have  $\bigcap \{T \in \text{Pow}(\bigcup Q). (T \text{ is closed in } Q) \wedge A \subseteq T\} \subseteq \bigcap \{T \in \text{DualBase } U \ Q. A \subseteq T\}$ 
  by auto
  then show  $\text{Closure}(A, Q) \subseteq \bigcap \{T \in \text{DualBase } U \ Q. A \subseteq T\}$  using Closure_def ClosedCovers_def
  by auto
  {
    fix x
    assume  $A: x \in \bigcap \{T \in \text{DualBase } U \ Q. A \subseteq T\}$ 
    {
      fix T
      assume  $B: x \in T \in U$ 
      {
        assume  $C: A \cap T = \emptyset$ 
        from B(2) assms(1) have  $\bigcup Q - T \in \text{DualBase } U \ Q$  using DualBase_def
        by auto
        moreover
        from C assms(3) have  $A \subseteq \bigcup Q - T$  by auto
        moreover
        from B(1) have  $x \notin \bigcup Q - T$  by auto
        ultimately have  $x \notin \bigcap \{T \in \text{DualBase } U \ Q. A \subseteq T\}$  by auto
        with A have False by auto
      }
      hence  $A \cap T \neq \emptyset$  by auto
    }
  }

```



```

    }
    hence  $\forall T \in U. x \in T \longrightarrow A \cap T \neq \emptyset$  by auto
    moreover
    from T A assms(3) have  $x \in \bigcup Q$  by auto
    with calculation assms have  $x \in \text{Closure}(A, Q)$  using closure_set_base_topology
    by auto
  }
  thus  $\bigcap \{T \in \text{DualBase } U \mid Q \subseteq T\} \subseteq \text{Closure}(A, Q)$  by auto
qed

```

## 49.2 Partition topology

In the theory file `Partitions_ZF.thy`; there is a definition to work with partitions. In this setting is much easier to work with a family of subsets.

**definition**

```

IsAPartition ( $\_ \{ \text{is a partition of} \}_ \_ 90$ ) where
( $U \{ \text{is a partition of} \} X$ )  $\equiv (\bigcup U = X \wedge (\forall A \in U. \forall B \in U. A = B \vee A \cap B = \emptyset) \wedge \emptyset \notin U)$ 

```

A subcollection of a partition is a partition of its union.

**lemma** subpartition:

```

  assumes  $U \{ \text{is a partition of} \} X \wedge V \subseteq U$ 
  shows  $V \{ \text{is a partition of} \} \bigcup V$ 
  using assms unfolding IsAPartition_def by auto

```

A restriction of a partition is a partition. If the empty set appears it has to be removed.

**lemma** restriction\_partition:

```

  assumes  $U \{ \text{is a partition of} \} X$ 
  shows  $((U \{ \text{restricted to} \} Y) - \{\emptyset\}) \{ \text{is a partition of} \} (X \cap Y)$ 
  using assms unfolding IsAPartition_def RestrictedTo_def
  by fast

```

Given a partition, the complement of a union of a subfamily is a union of a subfamily.

**lemma** diff\_union\_is\_union\_diff:

```

  assumes  $R \subseteq P \{ \text{is a partition of} \} X$ 
  shows  $X - \bigcup R = \bigcup (P - R)$ 

```

**proof**

```

{
  fix x
  assume  $x \in X - \bigcup R$ 
  hence  $P : x \in X \wedge x \notin \bigcup R$  by auto
  {
    fix T
    assume  $T \in R$ 
    with P(2) have  $x \notin T$  by auto
  }
}

```

```

    with P(1) assms(2) obtain Q where  $Q \in (P-R)x \in Q$  using IsAPartition_def
  by auto
    hence  $x \in \bigcup (P-R)$  by auto
  }
  thus  $X - \bigcup R \subseteq \bigcup (P-R)$  by auto
  {
    fix x
    assume  $x \in \bigcup (P-R)$ 
    then obtain Q where  $Q \in P-Rx \in Q$  by auto
    hence C:  $Q \in P \text{ and } Q \notin Rx \in Q$  by auto
    then have  $x \in \bigcup P$  by auto
    with assms(2) have  $x \in X$  using IsAPartition_def by auto
    moreover
    {
      assume  $x \in \bigcup R$ 
      then obtain t where  $G:t \in R \text{ and } x \in t$  by auto
      with C(3) assms(1) have  $t \cap Q \neq \emptyset$  by auto
      with assms(2) C(1,3) have  $t=Q$  using IsAPartition_def
      by blast
      with C(2) G(1) have False by auto
    }
    hence  $x \notin \bigcup R$  by auto
    ultimately have  $x \in X - \bigcup R$  by auto
  }
  thus  $\bigcup (P-R) \subseteq X - \bigcup R$  by auto
qed

```

#### 49.2.1 Partition topology is a topology.

A partition satisfies the base condition.

```

lemma partition_base_condition:
  assumes P {is a partition of} X
  shows P {satisfies the base condition}
proof-
  {
    fix U V
    assume AS:  $U \in P \wedge V \in P$ 
    with assms have A:  $U=V \vee U \cap V = \emptyset$  using IsAPartition_def by auto
    {
      fix x
      assume ASS:  $x \in U \cap V$ 
      with A have  $U=V$  by auto
      with AS ASS have  $U \in P \text{ and } x \in U \wedge U \subseteq U \cap V$  by auto
      hence  $\exists W \in P. x \in W \wedge W \subseteq U \cap V$  by auto
    }
    hence  $(\forall x \in U \cap V. \exists W \in P. x \in W \wedge W \subseteq U \cap V)$  by auto
  }
  then show thesis using SatisfiesBaseCondition_def by auto
qed

```

Since a partition is a base of a topology, and this topology is uniquely determined; we can build it. In the definition we have to make sure that we have a partition.

**definition**

```
PartitionTopology (PTopology _ _ 50) where
  (U {is a partition of} X)  $\implies$  PTopology X U  $\equiv$  TopologyBase U
```

**theorem** Ptopology\_is\_a\_topology:

```
  assumes U {is a partition of} X
  shows (PTopology X U) {is a topology} and U {is a base for} (PTopology X U)
  using assms Base_topology_is_a_topology partition_base_condition
    PartitionTopology_def by auto
```

**lemma** topology0\_ptopology:

```
  assumes U {is a partition of} X
  shows topology0(PTopology X U)
  using Ptopology_is_a_topology topology0_def assms by auto
```

## 49.2.2 Total set, Closed sets, Interior, Closure and Boundary

The topology is defined in the set  $X$

**lemma** union\_ptopology:

```
  assumes U {is a partition of} X
  shows  $\bigcup$  (PTopology X U)=X
  using assms Ptopology_is_a_topology(2) Top_1_2_L5
    IsAPartition_def by auto
```

The closed sets are the open sets.

**lemma** closed\_sets\_ptopology:

```
  assumes T {is a partition of} X
  showsD {is closed in} (PTopology X T)  $\longleftrightarrow$  D $\in$ (PTopology X T)
```

**proof**

```
  from assms
  have B:T{is a base for}(PTopology X T) using Ptopology_is_a_topology(2)
  by auto
  {
    fix D
    assume D {is closed in} (PTopology X T)
    with assms have A:D $\in$ Pow(X)X-D $\in$ (PTopology X T)
      using IsClosed_def union_ptopology by auto
    from A(2) B obtain R where Q:R $\subseteq$ T X-D= $\bigcup$ R using Top_1_2_L1[where
    B=T and U=X-D]
      by auto
    from A(1) have X-(X-D)=D by blast
    with Q(2) have D=X- $\bigcup$ R by auto
    with Q(1) assms have D= $\bigcup$ (T-R) using diff_union_is_union_diff
      by auto
```

```

with B show  $D \in (\text{PTopology } X \ T)$  using IsAbaseFor_def by auto
}
{
  fix D
  assume  $D \in (\text{PTopology } X \ T)$ 
  with B obtain R where  $Q: R \subseteq T \Rightarrow D = \bigcup R$  using IsAbaseFor_def by auto
  hence  $X - D = X - \bigcup R$  by auto
  with Q(1) assms have  $X - D = \bigcup (T - R)$  using diff_union_is_union_diff
    by auto
  with B have  $X - D \in (\text{PTopology } X \ T)$  using IsAbaseFor_def by auto
  moreover
  from Q have  $D \subseteq \bigcup T$  by auto
  with assms have  $D \subseteq X$  using IsAPartition_def by auto
  with calculation assms show  $D \{ \text{is closed in} \} (\text{PTopology } X \ T)$ 
    using IsClosed_def union_ptopology by auto
}
qed

```

There is a formula for the interior given by an intersection of sets of the dual base. Is the intersection of all the closed sets of the dual basis such that they do not complement  $A$  to  $X$ . Since the interior of  $X$  must be inside  $X$ , we have to enter  $X$  as one of the sets to be intersected.

**lemma interior\_set\_ptopology:**

```

  assumes U {is a partition of}  $X \subseteq X$ 
  shows  $\text{Interior}(A, (\text{PTopology } X \ U)) = \bigcap \{ T \in \text{DualBase } U \mid (\text{PTopology } X \ U). T = X \setminus T \cup A \neq X \}$ 
proof
  {
    fix x
    assume  $x \in \text{Interior}(A, (\text{PTopology } X \ U))$ 
    with assms obtain R where  $A: x \in R \wedge R \in (\text{PTopology } X \ U) \wedge R \subseteq A$ 
      using topology0.open_open_neigh topology0_ptopology
      topology0.Top_2_L2 topology0.Top_2_L1
      by auto
    with assms obtain B where  $B: B \subseteq U \wedge B = \bigcup B$  using Ptopology_is_a_topology(2)
      IsAbaseFor_def by auto
    from A(1,3) assms have  $XX: x \in XX \in \{ T \in \text{DualBase } U \mid (\text{PTopology } X \ U). T = X \setminus T \cup A \neq X \}$ 
      using union_ptopology[of UX] DualBase_def[of U] Ptopology_is_a_topology(2)[of
UX] by (safe,blast,auto)
    moreover
    from B(2) A(1) obtain S where  $C: S \in B \wedge x \in S$  by auto
    {
      fix T
      assume  $AS: T \in \text{DualBase } U \mid (\text{PTopology } X \ U). T \cup A \neq X$ 
      from AS(1) assms obtain w where  $(T = X - w \wedge w \in U) \vee (T = X)$ 
        using DualBase_def union_ptopology Ptopology_is_a_topology(2)
        by auto
      with assms(2) AS(2) have  $D: T = X - ww \in U$  by auto
      from D(2) have  $w \subseteq \bigcup U$  by auto
    }
  }

```

```

    with assms(1) have  $w \subseteq \bigcup (P\text{Topology } X \ U)$  using Ptopology_is_a_topology(2)
Top_1_2_L5[of UPTopology X U]
    by auto
    with assms(1) have  $w \subseteq X$  using union_ptopology by auto
    with D(1) have  $X-T=w$  by auto
    with D(2) have  $X-T \in U$  by auto
    {
      assume  $x \in X-T$ 
      with C B(1) have  $S \in U \cap (X-T) \neq \emptyset$  by auto
      with 'X-T  $\in U$ ' assms(1) have  $X-T=S$  using IsAPartition_def by auto
      with 'X-T=w' 'T=X-w' have  $X-S=T$  by auto
      with AS(2) have  $X-SUA \neq X$  by auto
      from A(3) B(2) C(1) have  $S \subseteq A$  by auto
      hence  $X-A \subseteq X-S$  by auto
      with assms(2) have  $X-SUA=X$  by auto
      with 'X-SUA  $\neq X$ ' have False by auto
    }
    then have  $x \in T$  using XX by auto
  }
  ultimately have  $x \in \bigcap \{T \in \text{DualBase } U \mid (P\text{Topology } X \ U). T=X \vee TUA \neq X\}$ 
    by auto
}
thus Interior(A, (PTopology X U))  $\subseteq \bigcap \{T \in \text{DualBase } U \mid (P\text{Topology } X \ U). T=X \vee TUA \neq X\}$ 
by auto
{
  fix x
  assume  $p: x \in \bigcap \{T \in \text{DualBase } U \mid (P\text{Topology } X \ U). T=X \vee TUA \neq X\}$ 
  hence  $\text{noE}: \bigcap \{T \in \text{DualBase } U \mid (P\text{Topology } X \ U). T=X \vee TUA \neq X\} \neq \emptyset$  by auto
  {
    fix T
    assume  $T \in \text{DualBase } U \mid (P\text{Topology } X \ U)$ 
    with assms(1) obtain w where  $T=X \vee (w \in U \wedge T=X-w)$  using DualBase_def
      Ptopology_is_a_topology(2) union_ptopology by auto
    with assms(1) have  $T=X \vee (w \in (P\text{Topology } X \ U) \wedge T=X-w)$  using base_sets_open
      Ptopology_is_a_topology(2) by blast
    with assms(1) have T{is closed in}(PTopology X U) using topology0.Top_3_L1[where
T=PTopology X U]
      topology0_ptopology topology0.Top_3_L9[where T=PTopology X U]
    union_ptopology
    by auto
  }
  moreover
  from assms(1) p have  $X \in \{T \in \text{DualBase } U \mid (P\text{Topology } X \ U). T=X \vee TUA \neq X\}$  and
X:x  $\in X$  using Ptopology_is_a_topology(2)
    DualBase_def union_ptopology by auto
    with calculation assms(1) have  $(\bigcap \{T \in \text{DualBase } U \mid (P\text{Topology } X \ U). T=X \vee TUA \neq X\}) \{is closed in\}(P\text{Topology } X \ U)$ 
      using topology0.Top_3_L4[where  $K=\{T \in \text{DualBase } U \mid (P\text{Topology } X \ U). T=X \vee TUA \neq X\}$ ] topology0_ptopology[where  $U=U$  and  $X=X$ ]

```

```

    by auto
    with assms(1) have ab:  $(\bigcap \{T \in \text{DualBase } U \mid (\text{PTopology } X \ U). \ T = X \vee T \cup A \neq X\}) \in (\text{PTopology } X \ U)$ 
    using closed_sets_ptopology by auto
    with assms(1) obtain B where  $B \in \text{Pow}(U) \mid (\bigcap \{T \in \text{DualBase } U \mid (\text{PTopology } X \ U). \ T = X \vee T \cup A \neq X\}) = \bigcup B$ 
    using Ptopology_is_a_topology(2) IsAbaseFor_def by auto
    with p obtain R where  $x \in R \implies R \subseteq (\bigcap \{T \in \text{DualBase } U \mid (\text{PTopology } X \ U). \ T = X \vee T \cup A \neq X\})$ 
    by auto
    with assms(1) have  $R: x \in R \implies R \subseteq (\bigcap \{T \in \text{DualBase } U \mid (\text{PTopology } X \ U). \ T = X \vee T \cup A \neq X\}) \mid X - R \in \text{DualBase } U \mid (\text{PTopology } X \ U)$ 
    using base_sets_open Ptopology_is_a_topology(2) DualBase_def union_ptopology
    by (safe,blast,simp,blast)
  {
    assume  $(X - R) \cup A \neq X$ 
    with R(4) have  $X - R \in \{T \in \text{DualBase } U \mid (\text{PTopology } X \ U). \ T = X \vee T \cup A \neq X\}$  by
  auto
    hence  $\bigcap \{T \in \text{DualBase } U \mid (\text{PTopology } X \ U). \ T = X \vee T \cup A \neq X\} \subseteq X - R$  by auto
    with R(3) have  $R \subseteq X - R$  using subset_trans[where A=R and C=X-R] by
  auto
    hence  $R = 0$  by blast
    with R(1) have False by auto
  }
  hence I:  $(X - R) \cup A = X$  by auto
  {
    fix y
    assume ASR:  $y \in R$ 
    with R(2) have  $y \in \bigcup (\text{PTopology } X \ U)$  by auto
    with assms(1) have  $XX: y \in X$  using union_ptopology by auto
    with I have  $y \in (X - R) \cup A$  by auto
    with XX have  $y \notin R \vee y \in A$  by auto
    with ASR have  $y \in A$  by auto
  }
  hence  $R \subseteq A$  by auto
  with R(1,2) have  $\exists R \in (\text{PTopology } X \ U). \ (x \in R \wedge R \subseteq A)$  by auto
  with assms(1) have  $x \in \text{Interior}(A, (\text{PTopology } X \ U))$  using topology0.Top_2_L6
    topology0_ptopology by auto
}
thus  $\bigcap \{T \in \text{DualBase } U \mid (\text{PTopology } X \ U). \ T = X \vee T \cup A \neq X\} \subseteq \text{Interior}(A, \text{PTopology } X \ U)$ 
  by auto
qed

```

The closure of a set is the union of all the sets of the partition which intersect with A.

```

lemma closure_set_ptopology:
  assumes U {is a partition of}  $X \subseteq X$ 
  shows  $\text{Closure}(A, (\text{PTopology } X \ U)) = \bigcup \{T \in U. \ T \cap A \neq 0\}$ 

```

```

proof
{
  fix x
  assume A:x∈Closure(A,(PTopology X U))
  with assms have x∈ $\bigcup$ (PTopology X U) using topology0.Top_3_L11(1)[where
T=PTopology X U
  and A=A] topology0_ptopology union_ptopology by auto
  with assms(1) have x∈ $\bigcup$ U using Top_1_2_L5[where B=U and T=PTopology
X U] Ptopology_is_a_topology(2) by auto
  then obtain W where B:x∈WW∈U by auto
  with A have x∈Closure(A,(PTopology X U))∩W by auto
  moreover
  from assms B(2) have W∈(PTopology X U)A⊆X using base_sets_open Ptopology_is_a_topology
  by (safe,blast)
  with calculation assms(1) have A∩W≠0 using topology0_ptopology[where
U=U and X=X]
  topology0.cl_inter_neigh union_ptopology by auto
  with B have x∈ $\bigcup$ {T∈U. T∩A≠0} by blast
}
thus Closure(A, PTopology X U) ⊆  $\bigcup$ {T ∈ U . T ∩ A ≠ 0} by auto
{
  fix x
  assume x∈ $\bigcup$ {T ∈ U . T ∩ A ≠ 0}
  then obtain T where A:x∈TT∈UT∩A≠0 by auto
  from assms have A⊆ $\bigcup$ (PTopology X U) using union_ptopology by auto
  moreover
  from A(1,2) assms(1) have x∈ $\bigcup$ (PTopology X U) using Top_1_2_L5[where
B=U and T=PTopology X U]
  Ptopology_is_a_topology(2) by auto
  moreover
  {
    fix Q
    assume B:Q∈(PTopology X U)x∈Q
    with assms(1) obtain M where C:Q= $\bigcup$ MM⊆U using
      Ptopology_is_a_topology(2)
      IsAbaseFor_def by auto
    from B(2) C(1) obtain R where D:R∈Mx∈R by auto
    with C(2) A(1,2) have R∩T≠0R∈UT∈U by auto
    with assms(1) have R=T using IsAPartition_def by auto
    with C(1) D(1) have T⊆Q by auto
    with A(3) have Q∩A≠0 by auto
  }
  then have  $\forall Q \in (\text{PTopology } X \text{ U}). x \in Q \longrightarrow Q \cap A \neq 0$  by auto
  with calculation assms(1) have x∈Closure(A,(PTopology X U)) using
topology0.inter_neigh_cl
  topology0_ptopology by auto
}
then show  $\bigcup$ {T ∈ U . T ∩ A ≠ 0} ⊆ Closure(A, PTopology X U) by auto
qed

```

The boundary of a set is given by the union of the sets of the partition which have non empty intersection with the set but that are not fully contained in it. Another equivalent statement would be: the union of the sets of the partition which have non empty intersection with the set and its complement.

```

lemma boundary_set_ptopology:
  assumes U {is a partition of} X A ⊆ X
  shows Boundary(A, (PTopology X U)) = ⋃ {T ∈ U. T ∩ A ≠ 0 ∧ ¬(T ⊆ A)}
proof-
  from assms have Closure(A, (PTopology X U)) = ⋃ {T ∈ U . T ∩ A ≠ 0} using
  closure_set_ptopology by auto
  moreover
  from assms(1) have Interior(A, (PTopology X U)) = ⋃ {T ∈ U . T ⊆ A} using
  interior_set_base_topology Ptopology_is_a_topology[where U=U and
  X=X] by auto
  with calculation assms have A: Boundary(A, (PTopology X U)) = ⋃ {T ∈ U
  . T ∩ A ≠ 0} - ⋃ {T ∈ U . T ⊆ A}
    using topology0.Top_3_L12 topology0_ptopology union_ptopology
    by auto
  from assms(1) have ({T ∈ U . T ∩ A ≠ 0}) {is a partition of} ⋃ ({T
  ∈ U . T ∩ A ≠ 0})
    using subpartition by blast
  moreover
  {
    fix T
    assume T ∈ U ⊆ A
    with assms(1) have T ∩ A = T ≠ 0 using IsAPartition_def by auto
    with 'T ∈ U' have T ∩ A ≠ 0 T ∈ U by auto
  }
  then have {T ∈ U . T ⊆ A} ⊆ {T ∈ U . T ∩ A ≠ 0} by auto
  ultimately have ⋃ {T ∈ U . T ∩ A ≠ 0} - ⋃ {T ∈ U . T ⊆ A} = ⋃ ({T ∈
  U . T ∩ A ≠ 0}) - ({T ∈ U . T ⊆ A})
    using diff_union_is_union_diff by auto
  also have ... = ⋃ ({T ∈ U . T ∩ A ≠ 0 ∧ ¬(T ⊆ A)}) by blast
  with calculation A show thesis by auto
qed

```

### 49.2.3 Special cases and subspaces

The discrete and the indiscrete topologies appear as special cases of this partition topologies.

```

lemma discrete_partition:
  shows {{x}. x ∈ X} {is a partition of} X
  using IsAPartition_def by auto

```

```

lemma indiscrete_partition:
  assumes X ≠ 0

```



```

shows {X} {is a partition of} X
using assms IsAPartition_def by auto

theorem discrete_ptopology:
  shows (PTopology X {{x}.x∈X})=Pow(X)
proof
  {
    fix t
    assume t∈(PTopology X {{x}.x∈X})
    hence t⊆⋃ (PTopology X {{x}.x∈X}) by auto
    then have t∈Pow(X) using union_ptopology
      discrete_partition by auto
  }
  thus (PTopology X {{x}.x∈X})⊆Pow(X) by auto
  {
    fix t
    assume A:t∈Pow(X)
    have ⋃({{x}. x∈t})=t by auto
    moreover
    from A have {{x}. x∈t}∈Pow({{x}.x∈X}) by auto
    hence ⋃({{x}. x∈t})∈{⋃A . A ∈ Pow({{x} . x ∈ X})} by auto
    ultimately
    have t∈(PTopology X {{x} . x ∈ X}) using Ptopology_is_a_topology(2)
      discrete_partition IsAbaseFor_def by auto
  }
  thus Pow(X) ⊆ (PTopology X {{x} . x ∈ X}) by auto
qed

theorem indiscrete_ptopology:
  assumes X≠0
  shows (PTopology X {X})={0,X}
proof
  {
    fix T
    assume T∈(PTopology X {X})
    with assms obtain M where M⊆{X}⋃M=T using Ptopology_is_a_topology(2)
      indiscrete_partition IsAbaseFor_def by auto
    then have T=0∨T=X by auto
  }
  then show (PTopology X {X})⊆{0,X} by auto
  from assms have 0∈(PTopology X {X}) using Ptopology_is_a_topology(1)
    empty_open
    indiscrete_partition by auto
  moreover
  from assms have ⋃ (PTopology X {X})∈(PTopology X {X}) using union_open
    Ptopology_is_a_topology(1)
    indiscrete_partition by auto
  with assms have X∈(PTopology X {X}) using union_ptopology indiscrete_partition
    by auto

```

ultimately show  $\{0, X\} \subseteq (\text{PTopology } X \{X\})$  by auto  
qed

The topological subspaces of the  $\text{PTopology } X \ U$  are partition topologies.

```
lemma subspace_ptopology:
  assumes U{is a partition of}X
  shows (PTopology X U) {restricted to} Y=(PTopology (X∩Y) ((U {restricted
to} Y)-{0}))
proof-
  from assms have U{is a base for}(PTopology X U) using Ptopology_is_a_topology(2)
  by auto
  then have (U{restricted to} Y){is a base for}(PTopology X U){restricted
to} Y
  using subspace_base_topology by auto
  then have ((U{restricted to} Y)-{0}){is a base for}(PTopology X U){restricted
to} Y using base_no_0
  by auto
  moreover
  from assms have ((U{restricted to} Y)-{0}) {is a partition of} (X∩Y)
  using restriction_partition by auto
  then have ((U{restricted to} Y)-{0}){is a base for}(PTopology (X∩Y)
((U {restricted to} Y)-{0}))
  using Ptopology_is_a_topology(2) by auto
  ultimately show thesis using same_base_same_top by auto
qed
```

### 49.3 Order topologies

#### 49.3.1 Order topology is a topology

Given a totally ordered set, several topologies can be defined using the order relation. First we define an open interval, notice that the set defined as Interval is a closed interval; and open rays.

**definition**

IntervalX where  
IntervalX(X,r,b,c)≡(Interval(r,b,c)∩X)-{b,c}

**definition**

LeftRayX where  
LeftRayX(X,r,b)≡{c∈X. ⟨c,b⟩∈r}-{b}

**definition**

RightRayX where  
RightRayX(X,r,b)≡{c∈X. ⟨b,c⟩∈r}-{b}

Intersections of intervals and rays.

**lemma inter\_two\_intervals:**

```
  assumes bu∈Xbv∈Xcu∈Xcv∈XIsLinOrder(X,r)
  shows IntervalX(X,r,bu,cu)∩IntervalX(X,r,bv,cv)=IntervalX(X,r,GreaterOf(r,bu,bv),SmallerOf(bv,bu))
proof
```

```

have T:GreaterOf(r,bu,bv)∈XSmallerOf(r,cu,cv)∈X using assms
  GreaterOf_def SmallerOf_def by (cases ⟨bu,bv⟩∈r,simp,simp,cases ⟨cu,cv⟩∈r,simp,simp)
{
  fix x
  assume ASS:x∈IntervalX(X,r,bu,cu)∩IntervalX(X,r,bv,cv)
  then have x∈IntervalX(X,r,bu,cu)x∈IntervalX(X,r,bv,cv) by auto
  then have BB:x∈Xx∈Interval(r,bu,cu)x≠bux≠cux∈Interval(r,bv,cv)x≠bvx≠cv
  using IntervalX_def assms by auto
  then have x∈X by auto
  moreover
  have x≠GreaterOf(r,bu,bv)x≠SmallerOf(r,cu,cv)
  proof-
    show x≠GreaterOf(r,bu,bv) using GreaterOf_def BB(6,3) by (cases
    ⟨bu,bv⟩∈r,simp+)
    show x≠SmallerOf(r,cu,cv) using SmallerOf_def BB(7,4) by (cases
    ⟨cu,cv⟩∈r,simp+)
  qed
  moreover
  have ⟨bu,x⟩∈r⟨x,cu⟩∈r⟨bv,x⟩∈r⟨x,cv⟩∈r using BB(2,5) Order_ZF_2_L1A
  by auto
  then have ⟨GreaterOf(r,bu,bv),x⟩∈r⟨x,SmallerOf(r,cu,cv)⟩∈r using GreaterOf_def
  SmallerOf_def
    by (cases ⟨bu,bv⟩∈r,simp,simp,cases ⟨cu,cv⟩∈r,simp,simp)
  then have x∈Interval(r,GreaterOf(r,bu,bv),SmallerOf(r,cu,cv)) using
  Order_ZF_2_L1 by auto
  ultimately
  have x∈IntervalX(X,r,GreaterOf(r,bu,bv),SmallerOf(r,cu,cv)) using
  IntervalX_def T by auto
}
then show IntervalX(X, r, bu, cu) ∩ IntervalX(X, r, bv, cv) ⊆ IntervalX(X,
r, GreaterOf(r, bu, bv), SmallerOf(r, cu, cv))
  by auto
{
  fix x
  assume x∈IntervalX(X,r,GreaterOf(r,bu,bv),SmallerOf(r,cu,cv))
  then have BB:x∈Xx∈Interval(r,GreaterOf(r,bu,bv),SmallerOf(r,cu,cv))x≠GreaterOf(r,bu,bv)
  using IntervalX_def T by auto
  then have x∈X by auto
  moreover
  from BB(2) have CC:⟨GreaterOf(r,bu,bv),x⟩∈r⟨x,SmallerOf(r,cu,cv)⟩∈r
  using Order_ZF_2_L1A by auto
  {
    {
      assume AS:⟨bu,bv⟩∈r
      then have GreaterOf(r,bu,bv)=bv using GreaterOf_def by auto
      then have ⟨bv,x⟩∈r using CC(1) by auto
      with AS have ⟨bu,x⟩∈r ⟨bv,x⟩∈r using assms IsLinOrder_def trans_def
    }
  }
}
by (safe, blast)

```

```

    moreover
    {
      assume AS:⟨bu,bv⟩∉r
      then have GreaterOf(r,bu,bv)=bu using GreaterOf_def by auto
      then have ⟨bu,x⟩∈r using CC(1) by auto
      from AS have ⟨bv,bu⟩∈r using assms IsLinOrder_def IsTotal_def
assms by auto
      with '⟨bu,x⟩∈r' have ⟨bu,x⟩∈r ⟨bv,x⟩∈r using assms IsLinOrder_def
trans_def by (safe, blast)
    }
    ultimately have R:⟨bu,x⟩∈r ⟨bv,x⟩∈r by auto
    moreover
    {
      assume AS:x=bu
      then have ⟨bv,bu⟩∈r using R(2) by auto
      then have GreaterOf(r,bu,bv)=bu using GreaterOf_def assms IsLinOrder_def
antisym_def by auto
      then have False using AS BB(3) by auto
    }
    moreover
    {
      assume AS:x=bv
      then have ⟨bu,bv⟩∈r using R(1) by auto
      then have GreaterOf(r,bu,bv)=bv using GreaterOf_def by auto
      then have False using AS BB(3) by auto
    }
    ultimately have ⟨bu,x⟩∈r ⟨bv,x⟩∈rx≠bux≠bv by auto
  }
  moreover
  {
    {
      assume AS:⟨cu,cv⟩∈r
      then have SmallerOf(r,cu,cv)=cu using SmallerOf_def by auto
      then have ⟨x,cu⟩∈r using CC(2) by auto
      with AS have ⟨x,cu⟩∈r ⟨x,cv⟩∈r using assms IsLinOrder_def trans_def
by(safe ,blast)
    }
    moreover
    {
      assume AS:⟨cu,cv⟩∉r
      then have SmallerOf(r,cu,cv)=cv using SmallerOf_def by auto
      then have ⟨x,cv⟩∈r using CC(2) by auto
      from AS have ⟨cv,cu⟩∈r using assms IsLinOrder_def IsTotal_def
by auto
      with '⟨x,cv⟩∈r' have ⟨x,cv⟩∈r ⟨x,cu⟩∈r using assms IsLinOrder_def
trans_def by(safe ,blast)
    }
    ultimately have R:⟨x,cv⟩∈r ⟨x,cu⟩∈r by auto
    moreover

```

```

    {
      assume AS:x=cv
      then have ⟨cv,cu⟩∈r using R(2) by auto
      then have SmallerOf(r,cu,cv)=cv using SmallerOf_def assms IsLinOrder_def
      antisym_def by auto
      then have False using AS BB(4) by auto
    }
  moreover
  {
    assume AS:x=cu
    then have ⟨cu,cv⟩∈r using R(1) by auto
    then have SmallerOf(r,cu,cv)=cu using SmallerOf_def by auto
    then have False using AS BB(4) by auto
  }
  ultimately have ⟨x,cu⟩∈r ⟨x,cv⟩∈r x≠cu x≠cv by auto
}
ultimately
have x∈IntervalX(X,r,bu,cu) x∈IntervalX(X,r,bv,cv) using Order_ZF_2_L1
IntervalX_def
  assms by auto
then have x∈IntervalX(X, r, bu, cu) ∩ IntervalX(X, r, bv, cv) by
auto
}
then show IntervalX(X,r,GreaterOf(r,bu,bv),SmallerOf(r,cu,cv)) ⊆ IntervalX(X,
r, bu, cu) ∩ IntervalX(X, r, bv, cv)
  by auto
qed

lemma inter_rray_interval:
  assumes bv∈X bu∈X cv∈X IsLinOrder(X,r)
  shows RightRayX(X,r,bu)∩IntervalX(X,r,bv,cv)=IntervalX(X,r,GreaterOf(r,bu,bv),cv)
proof
  {
    fix x
    assume x∈RightRayX(X,r,bu)∩IntervalX(X,r,bv,cv)
    then have x∈RightRayX(X,r,bu) x∈IntervalX(X,r,bv,cv) by auto
    then have BB:x∈X x≠bu x≠bv x≠cv (bu,x)∈r x∈Interval(r,bv,cv) using RightRayX_def
    IntervalX_def
      by auto
    then have ⟨bv,x⟩∈r ⟨x,cv⟩∈r using Order_ZF_2_L1A by auto
    with ‘⟨bu,x⟩∈r’ have ⟨GreaterOf(r,bu,bv),x⟩∈r using GreaterOf_def
  by (cases ⟨bu,bv⟩∈r, simp+)
    with ‘⟨x,cv⟩∈r’ have x∈Interval(r,GreaterOf(r,bu,bv),cv) using Order_ZF_2_L1
  by auto
    then have x∈IntervalX(X,r,GreaterOf(r,bu,bv),cv) using BB(1-4) IntervalX_def
    GreaterOf_def
      by (simp)
  }
  then show RightRayX(X, r, bu) ∩ IntervalX(X, r, bv, cv) ⊆ IntervalX(X,

```

```

r, GreaterOf(r, bu, bv), cv) by auto
{
  fix x
  assume x ∈ IntervalX(X, r, GreaterOf(r, bu, bv), cv)
  then have x ∈ Xx ∈ Interval(r, GreaterOf(r, bu, bv), cv) x ≠ cv x ≠ GreaterOf(r,
bu, bv) using IntervalX_def by auto
  then have R: ⟨GreaterOf(r, bu, bv), x⟩ ∈ r ⟨x, cv⟩ ∈ r using Order_ZF_2_L1A
by auto
  with 'x ≠ cv' have ⟨x, cv⟩ ∈ rx ≠ cv by auto
  moreover
  {
    {
      assume AS: ⟨bu, bv⟩ ∈ r
      then have GreaterOf(r, bu, bv) = bv using GreaterOf_def by auto
      then have ⟨bv, x⟩ ∈ r using R(1) by auto
      with AS have ⟨bu, x⟩ ∈ r ⟨bv, x⟩ ∈ r using assms unfolding IsLinOrder_def
trans_def by (safe, blast)
    }
    moreover
    {
      assume AS: ⟨bu, bv⟩ ∉ r
      then have GreaterOf(r, bu, bv) = bu using GreaterOf_def by auto
      then have ⟨bu, x⟩ ∈ r using R(1) by auto
      from AS have ⟨bv, bu⟩ ∈ r using assms unfolding IsLinOrder_def IsTotal_def
using assms by auto
      with '⟨bu, x⟩ ∈ r' have ⟨bu, x⟩ ∈ r ⟨bv, x⟩ ∈ r using assms unfolding IsLinOrder_def
trans_def by (safe, blast)
    }
    ultimately have T: ⟨bu, x⟩ ∈ r ⟨bv, x⟩ ∈ r by auto
    moreover
    {
      assume AS: x = bu
      then have ⟨bv, bu⟩ ∈ r using T(2) by auto
      then have GreaterOf(r, bu, bv) = bu unfolding GreaterOf_def using
assms unfolding IsLinOrder_def
antisym_def by auto
      with 'x ≠ GreaterOf(r, bu, bv)' have False using AS by auto
    }
    moreover
    {
      assume AS: x = bv
      then have ⟨bu, bv⟩ ∈ r using T(1) by auto
      then have GreaterOf(r, bu, bv) = bv unfolding GreaterOf_def by auto
      with 'x ≠ GreaterOf(r, bu, bv)' have False using AS by auto
    }
    ultimately have ⟨bu, x⟩ ∈ r ⟨bv, x⟩ ∈ rx ≠ bu x ≠ bv by auto
  }
  with calculation 'x ∈ X' have x ∈ RightRayX(X, r, bu) x ∈ IntervalX(X, r,
bv, cv) unfolding RightRayX_def IntervalX_def

```

```

    using Order_ZF_2_L1 by auto
    then have  $x \in \text{RightRayX}(X, r, bu) \cap \text{IntervalX}(X, r, bv, cv)$  by auto
  }
  then show  $\text{IntervalX}(X, r, \text{GreaterOf}(r, bu, bv), cv) \subseteq \text{RightRayX}(X, r, bu) \cap \text{IntervalX}(X, r, bv, cv)$  by auto
qed

lemma inter_lray_interval:
  assumes  $bv \in X, cu \in X, cv \in X$  isLinOrder(X,r)
  shows  $\text{LeftRayX}(X, r, cu) \cap \text{IntervalX}(X, r, bv, cv) = \text{IntervalX}(X, r, bv, \text{SmallerOf}(r, cu, cv))$ 
proof
  {
    fix x assume  $x \in \text{LeftRayX}(X, r, cu) \cap \text{IntervalX}(X, r, bv, cv)$ 
    then have  $B: x \neq cu, x \in X, \langle x, cu \rangle \in r, \langle bv, x \rangle \in r, \langle x, cv \rangle \in r, x \neq bv, x \neq cv$  unfolding LeftRayX_def
    IntervalX_def Interval_def
    by auto
    from ' $\langle x, cu \rangle \in r$ ' ' $\langle x, cv \rangle \in r$ ' have  $C: \langle x, \text{SmallerOf}(r, cu, cv) \rangle \in r$  using
    SmallerOf_def by (cases  $\langle cu, cv \rangle \in r$ , simp+)
    from B(7,1) have  $x \neq \text{SmallerOf}(r, cu, cv)$  using SmallerOf_def by (cases
     $\langle cu, cv \rangle \in r$ , simp+)
    then have  $x \in \text{IntervalX}(X, r, bv, \text{SmallerOf}(r, cu, cv))$  using B C IntervalX_def
    Order_ZF_2_L1 by auto
  }
  then show  $\text{LeftRayX}(X, r, cu) \cap \text{IntervalX}(X, r, bv, cv) \subseteq \text{IntervalX}(X, r, bv, \text{SmallerOf}(r, cu, cv))$  by auto
  {
    fix x assume  $x \in \text{IntervalX}(X, r, bv, \text{SmallerOf}(r, cu, cv))$ 
    then have  $R: x \in X, \langle bv, x \rangle \in r, \langle x, \text{SmallerOf}(r, cu, cv) \rangle \in r, x \neq bv, x \neq \text{SmallerOf}(r, cu, cv)$ 
    using IntervalX_def Interval_def
    by auto
    then have  $\langle bv, x \rangle \in r, x \neq bv$  by auto
    moreover
    {
      {
        assume  $AS: \langle cu, cv \rangle \in r$ 
        then have  $\text{SmallerOf}(r, cu, cv) = cu$  using SmallerOf_def by auto
        then have  $\langle x, cu \rangle \in r$  using R(3) by auto
        with AS have  $\langle x, cu \rangle \in r, \langle x, cv \rangle \in r$  using assms unfolding IsLinOrder_def
        trans_def by (safe, blast)
      }
      moreover
      {
        assume  $AS: \langle cu, cv \rangle \notin r$ 
        then have  $\text{SmallerOf}(r, cu, cv) = cv$  using SmallerOf_def by auto
        then have  $\langle x, cv \rangle \in r$  using R(3) by auto
        from AS have  $\langle cv, cu \rangle \in r$  using assms IsLinOrder_def IsTotal_def
        assms by auto
        with ' $\langle x, cv \rangle \in r$ ' have  $\langle x, cv \rangle \in r, \langle x, cu \rangle \in r$  using assms IsLinOrder_def

```

```

trans_def by (safe, blast)
}
ultimately have  $T: \langle x, cv \rangle \in r \ \langle x, cu \rangle \in r$  by auto
moreover
{
  assume AS:  $x = cu$ 
  then have  $\langle cu, cv \rangle \in r$  using T(1) by auto
  then have  $\text{SmallerOf}(r, cu, cv) = cu$  using SmallerOf_def assms IsLinOrder_def
    antisym_def by auto
  with ' $x \neq \text{SmallerOf}(r, cu, cv)$ ' have False using AS by auto
}
moreover
{
  assume AS:  $x = cv$ 
  then have  $\langle cv, cu \rangle \in r$  using T(2) by auto
  then have  $\text{SmallerOf}(r, cu, cv) = cv$  using SmallerOf_def assms IsLinOrder_def
    antisym_def by auto
  with ' $x \neq \text{SmallerOf}(r, cu, cv)$ ' have False using AS by auto
}
ultimately have  $\langle x, cu \rangle \in r \ \langle x, cv \rangle \in r \ x \neq cu \ x \neq cv$  by auto
}
with calculation ' $x \in X$ ' have  $x \in \text{LeftRayX}(X, r, cu) \ x \in \text{IntervalX}(X, r, bv,$ 
 $cv)$  using LeftRayX_def IntervalX_def Interval_def
  by auto
then have  $x \in \text{LeftRayX}(X, r, cu) \cap \text{IntervalX}(X, r, bv, cv)$  by auto
}
then show  $\text{IntervalX}(X, r, bv, \text{SmallerOf}(r, cu, cv)) \subseteq \text{LeftRayX}(X, r,$ 
 $cu) \cap \text{IntervalX}(X, r, bv, cv)$  by auto
qed

lemma inter_lray_rray:
  assumes  $bu \in X \ cv \in X \text{IsLinOrder}(X, r)$ 
  shows  $\text{LeftRayX}(X, r, bu) \cap \text{RightRayX}(X, r, cv) = \text{IntervalX}(X, r, cv, bu)$ 
  unfolding LeftRayX_def RightRayX_def IntervalX_def Interval_def by auto

lemma inter_lray_lray:
  assumes  $bu \in X \ cv \in X \text{IsLinOrder}(X, r)$ 
  shows  $\text{LeftRayX}(X, r, bu) \cap \text{LeftRayX}(X, r, cv) = \text{LeftRayX}(X, r, \text{SmallerOf}(r, bu, cv))$ 
proof
{
  fix x
  assume  $x \in \text{LeftRayX}(X, r, bu) \cap \text{LeftRayX}(X, r, cv)$ 
  then have  $B: x \in X \ \langle x, bu \rangle \in r \ \langle x, cv \rangle \in r \ x \neq bu \ x \neq cv$  using LeftRayX_def by auto
  then have  $C: \langle x, \text{SmallerOf}(r, bu, cv) \rangle \in r$  using SmallerOf_def by (cases
 $\langle bu, cv \rangle \in r$ , auto)
  from B have  $D: x \neq \text{SmallerOf}(r, bu, cv)$  using SmallerOf_def by (cases
 $\langle bu, cv \rangle \in r$ , auto)
  from B C D have  $x \in \text{LeftRayX}(X, r, \text{SmallerOf}(r, bu, cv))$  using LeftRayX_def
  by auto
}

```



```

    }
    then show LeftRayX(X, r, bu)  $\cap$  LeftRayX(X, r, cv)  $\subseteq$  LeftRayX(X, r,
    SmallerOf(r, bu, cv)) by auto
    {
      fix x
      assume x  $\in$  LeftRayX(X, r, SmallerOf(r, bu, cv))
      then have R:  $x \in X \langle x, \text{SmallerOf}(r, bu, cv) \rangle \in r \wedge x \neq \text{SmallerOf}(r, bu, cv)$  using
    LeftRayX_def by auto
      {
        {
          assume AS:  $\langle bu, cv \rangle \in r$ 
          then have SmallerOf(r, bu, cv) = bu using SmallerOf_def by auto
          then have  $\langle x, bu \rangle \in r$  using R(2) by auto
          with AS have  $\langle x, bu \rangle \in r \langle x, cv \rangle \in r$  using assms IsLinOrder_def trans_def
        by(safe, blast)
        }
        moreover
        {
          assume AS:  $\langle bu, cv \rangle \notin r$ 
          then have SmallerOf(r, bu, cv) = cv using SmallerOf_def by auto
          then have  $\langle x, cv \rangle \in r$  using R(2) by auto
          from AS have  $\langle cv, bu \rangle \in r$  using assms IsLinOrder_def IsTotal_def
        assms by auto
          with ' $\langle x, cv \rangle \in r$ ' have  $\langle x, cv \rangle \in r \langle x, bu \rangle \in r$  using assms IsLinOrder_def
        trans_def by(safe, blast)
        }
        ultimately have T:  $\langle x, cv \rangle \in r \langle x, bu \rangle \in r$  by auto
        moreover
        {
          assume AS:  $x = bu$ 
          then have  $\langle bu, cv \rangle \in r$  using T(1) by auto
          then have SmallerOf(r, bu, cv) = bu using SmallerOf_def assms IsLinOrder_def
            antisym_def by auto
          with ' $x \neq \text{SmallerOf}(r, bu, cv)$ ' have False using AS by auto
        }
        moreover
        {
          assume AS:  $x = cv$ 
          then have  $\langle cv, bu \rangle \in r$  using T(2) by auto
          then have SmallerOf(r, bu, cv) = cv using SmallerOf_def assms IsLinOrder_def
            antisym_def by auto
          with ' $x \neq \text{SmallerOf}(r, bu, cv)$ ' have False using AS by auto
        }
        ultimately have  $\langle x, bu \rangle \in r \langle x, cv \rangle \in r \wedge x \neq bu \wedge x \neq cv$  by auto
      }
      with ' $x \in X$ ' have  $x \in \text{LeftRayX}(X, r, bu) \cap \text{LeftRayX}(X, r, cv)$  using
    LeftRayX_def by auto
    }
    then show LeftRayX(X, r, SmallerOf(r, bu, cv))  $\subseteq$  LeftRayX(X, r, bu)

```

$\cap \text{LeftRayX}(X, r, cv)$  by auto  
qed

lemma inter\_rray\_rarray:

assumes  $bu \in X$   $cv \in X$   $\text{IsLinOrder}(X, r)$   
shows  $\text{RightRayX}(X, r, bu) \cap \text{RightRayX}(X, r, cv) = \text{RightRayX}(X, r, \text{GreaterOf}(r, bu, cv))$   
proof  
{  
  fix x  
  assume  $x \in \text{RightRayX}(X, r, bu) \cap \text{RightRayX}(X, r, cv)$   
  then have  $B: x \in X \langle bu, x \rangle \in r \langle cv, x \rangle \in r$   $x \neq bu$   $x \neq cv$  using  $\text{RightRayX\_def}$  by auto  
  then have  $C: \langle \text{GreaterOf}(r, bu, cv), x \rangle \in r$  using  $\text{GreaterOf\_def}$  by (cases  
     $\langle bu, cv \rangle \in r$ , auto)  
  from B have  $D: x \neq \text{GreaterOf}(r, bu, cv)$  using  $\text{GreaterOf\_def}$  by (cases  
     $\langle bu, cv \rangle \in r$ , auto)  
  from B C D have  $x \in \text{RightRayX}(X, r, \text{GreaterOf}(r, bu, cv))$  using  $\text{RightRayX\_def}$   
by auto  
}  
  then show  $\text{RightRayX}(X, r, bu) \cap \text{RightRayX}(X, r, cv) \subseteq \text{RightRayX}(X, r, \text{GreaterOf}(r, bu, cv))$  by auto  
  {  
    fix x  
    assume  $x \in \text{RightRayX}(X, r, \text{GreaterOf}(r, bu, cv))$   
    then have  $R: x \in X \langle \text{GreaterOf}(r, bu, cv), x \rangle \in r$   $x \neq \text{GreaterOf}(r, bu, cv)$  using  
     $\text{RightRayX\_def}$  by auto  
    {  
      {  
        assume  $AS: \langle bu, cv \rangle \in r$   
        then have  $\text{GreaterOf}(r, bu, cv) = cv$  using  $\text{GreaterOf\_def}$  by auto  
        then have  $\langle cv, x \rangle \in r$  using  $R(2)$  by auto  
        with AS have  $\langle bu, x \rangle \in r$   $\langle cv, x \rangle \in r$  using  $\text{assms IsLinOrder\_def trans\_def}$   
by (safe, blast)  
      }  
      moreover  
      {  
        assume  $AS: \langle bu, cv \rangle \notin r$   
        then have  $\text{GreaterOf}(r, bu, cv) = bu$  using  $\text{GreaterOf\_def}$  by auto  
        then have  $\langle bu, x \rangle \in r$  using  $R(2)$  by auto  
        from AS have  $\langle cv, bu \rangle \in r$  using  $\text{assms IsLinOrder\_def IsTotal\_def}$   
assms by auto  
        with ' $\langle bu, x \rangle \in r$ ' have  $\langle cv, x \rangle \in r$   $\langle bu, x \rangle \in r$  using  $\text{assms IsLinOrder\_def trans\_def}$  by (safe, blast)  
      }  
      ultimately have  $T: \langle cv, x \rangle \in r$   $\langle bu, x \rangle \in r$  by auto  
      moreover  
      {  
        assume  $AS: x = bu$   
        then have  $\langle cv, bu \rangle \in r$  using  $T(1)$  by auto  
        then have  $\text{GreaterOf}(r, bu, cv) = bu$  using  $\text{GreaterOf\_def}$   $\text{assms IsLinOrder\_def}$

```

      antisym_def by auto
    with 'x≠GreaterOf(r,bu,cv)' have False using AS by auto
  }
  moreover
  {
    assume AS:x=cv
    then have ⟨bu,cv⟩∈r using T(2) by auto
    then have GreaterOf(r,bu,cv)=cv using GreaterOf_def assms IsLinOrder_def
      antisym_def by auto
    with 'x≠GreaterOf(r,bu,cv)' have False using AS by auto
  }
  ultimately have ⟨bu,x⟩∈r ⟨cv,x⟩∈rx≠bux≠cv by auto
}
with 'x∈X' have x∈RightRayX(X, r, bu) ∩ RightRayX(X, r, cv) using
RightRayX_def by auto
}
then show RightRayX(X, r, GreaterOf(r, bu, cv)) ⊆ RightRayX(X, r, bu)
∩ RightRayX(X, r, cv) by auto
qed

```

The open intervals and rays satisfy the base condition.

**lemma** intervals\_rays\_base\_condition:

```

  assumes IsLinOrder(X,r)
  shows {IntervalX(X,r,b,c). ⟨b,c⟩∈X×X}∪{LeftRayX(X,r,b). b∈X}∪{RightRayX(X,r,b).
b∈X} {satisfies the base condition}

```

**proof-**

```

  let I={IntervalX(X,r,b,c). ⟨b,c⟩∈X×X}
  let R={RightRayX(X,r,b). b∈X}
  let L={LeftRayX(X,r,b). b∈X}
  let B={IntervalX(X,r,b,c). ⟨b,c⟩∈X×X}∪{LeftRayX(X,r,b). b∈X}∪{RightRayX(X,r,b).
b∈X}
  {
    fix U V
    assume A:U∈BV∈B
    then have dU:U∈IVU∈LVU∈Rand dV:V∈IVV∈LVV∈R by auto
    {
      assume S:V∈I
      {
        assume U∈I
        with S obtain bu cu bv cv where A:U=IntervalX(X,r,bu,cu)V=IntervalX(X,r,bv,cv)bu∈X
        by auto
        then have SmallerOf(r,cu,cv)∈XGreaterOf(r,bu,bv)∈X by (cases
⟨cu,cv⟩∈r,simp add:SmallerOf_def A,simp add:SmallerOf_def A,
cases ⟨bu,bv⟩∈r,simp add:GreaterOf_def A,simp add:GreaterOf_def
A)
        with A have U∩V∈B using inter_two_intervals assms by auto
      }
    }
  }
  moreover
  {

```

```

      assume U ∈ L
      with S obtain bu bv cv where A:U=LeftRayX(X, r,bu)V=IntervalX(X,r,bv,cv)bu ∈ Xbv ∈ Xcv
      by auto
      then have SmallerOf(r,bu,cv) ∈ X using SmallerOf_def by (cases
⟨bu,cv⟩ ∈ r, auto)
      with A have U ∩ V ∈ B using inter_lray_interval assms by auto
    }
  moreover
  {
    assume U ∈ R
    with S obtain cu bv cv where A:U=RightRayX(X,r,cu)V=IntervalX(X,r,bv,cv)cu ∈ Xbv ∈ Xcv
    by auto
    then have GreaterOf(r,cu,bv) ∈ X using GreaterOf_def by (cases
⟨cu,bv⟩ ∈ r, auto)
    with A have U ∩ V ∈ B using inter_rray_interval assms by auto
  }
  ultimately have U ∩ V ∈ B using dU by auto
}
moreover
{
  assume S:V ∈ L
  {
    assume U ∈ I
    with S obtain bu bv cv where A:V=LeftRayX(X, r,bu)U=IntervalX(X,r,bv,cv)bu ∈ Xbv ∈ Xcv
    by auto
    then have SmallerOf(r,bu,cv) ∈ X using SmallerOf_def by (cases
⟨bu,cv⟩ ∈ r, auto)
    have U ∩ V = V ∩ U by auto
    with A 'SmallerOf(r,bu,cv) ∈ X' have U ∩ V ∈ B using inter_lray_interval
assms by auto
  }
  moreover
  {
    assume U ∈ R
    with S obtain bu cv where A:V=LeftRayX(X,r,bu)U=RightRayX(X,r,cv)bu ∈ Xcv ∈ X
    by auto
    have U ∩ V = V ∩ U by auto
    with A have U ∩ V ∈ B using inter_lray_rray assms by auto
  }
  moreover
  {
    assume U ∈ L
    with S obtain bu bv where A:U=LeftRayX(X,r,bu)V=LeftRayX(X,r,bv)bu ∈ Xbv ∈ X
    by auto
    then have SmallerOf(r,bu,bv) ∈ X using SmallerOf_def by (cases
⟨bu,bv⟩ ∈ r, auto)
    with A have U ∩ V ∈ B using inter_lray_lray assms by auto
  }
  ultimately have U ∩ V ∈ B using dU by auto
}

```

```

    }
  moreover
  {
    assume S:V∈R
    {
      assume U∈I
      with S obtain cu bv cv where A:V=RightRayX(X,r,cu)U=IntervalX(X,r,bv,cv)cu∈Xbv∈Xcv
      by auto
      then have GreaterOf(r,cu,bv)∈X using GreaterOf_def by (cases
(cu,bv)∈r,auto)
      have U∩V=V∩U by auto
      with A 'GreaterOf(r,cu,bv)∈X' have U∩V∈B using inter_rray_interval
assms by auto
    }
    moreover
    {
      assume U∈L
      with S obtain bu cv where A:U=LeftRayX(X,r,bu)V=RightRayX(X,r,cv)bu∈Xcv∈X
      by auto
      then have U∩V∈B using inter_lray_rray assms by auto
    }
    moreover
    {
      assume U∈R
      with S obtain cu cv where A:U=RightRayX(X,r,cu)V=RightRayX(X,r,cv)cu∈Xcv∈X
      by auto
      then have GreaterOf(r,cu,cv)∈X using GreaterOf_def by (cases
(cu,cv)∈r,auto)
      with A have U∩V∈B using inter_rray_rray assms by auto
    }
    ultimately have U∩V∈B using dU by auto
  }
  ultimately have S:U∩V∈B using dV by auto
  {
    fix x
    assume x∈U∩V
    then have x∈U∩V∧U∩V⊆U∩V by auto
    then have ∃W. W∈(B)∧ x∈W ∧ W ⊆ U∩V using S by blast
    then have ∃W∈(B). x∈W ∧ W ⊆ U∩V by blast
  }
  hence (∀x ∈ U∩V. ∃W∈(B). x∈W ∧ W ⊆ U∩V) by auto
}
then show thesis using SatisfiesBaseCondition_def by auto
qed

```

Since the intervals and rays form a base of a topology, and this topology is uniquely determined; we can built it. In the definition we have to make sure that we have a totally ordered set.

**definition**

```

OrderTopology (OrdTopology _ _ 50) where
  IsLinOrder(X,r)  $\implies$  OrdTopology X r  $\equiv$  TopologyBase {IntervalX(X,r,b,c).
<b,c>∈X×X}∪{LeftRayX(X,r,b). b∈X}∪{RightRayX(X,r,b). b∈X}

```

```

theorem Ordtopology_is_a_topology:
  assumes IsLinOrder(X,r)
  shows (OrdTopology X r) {is a topology} and {IntervalX(X,r,b,c). <b,c>∈X×X}∪{LeftRayX(X,
b∈X}∪{RightRayX(X,r,b). b∈X} {is a base for} (OrdTopology X r)
  using assms Base_topology_is_a_topology intervals_rays_base_condition

  OrderTopology_def by auto

```

```

lemma topology0_ordtopology:
  assumes IsLinOrder(X,r)
  shows topology0(OrdTopology X r)
  using Ordtopology_is_a_topology topology0_def assms by auto

```

### 49.3.2 Total set

The topology is defined in the set  $X$ , when  $X$  has more than one point

```

lemma union_ordtopology:
  assumes IsLinOrder(X,r)∃x y. x≠y ∧ x∈X∧ y∈X
  shows  $\bigcup$  (OrdTopology X r)=X
proof
  let B={IntervalX(X,r,b,c). <b,c>∈X×X}∪{LeftRayX(X,r,b). b∈X}∪{RightRayX(X,r,b).
b∈X}
  have base:B {is a base for} (OrdTopology X r) using Ordtopology_is_a_topology(2)
  assms(1)
  by auto
  from assms(2) obtain x y where T:x≠y ∧ x∈X∧ y∈X by auto
  then have B:x∈LeftRayX(X,r,y)∨x∈RightRayX(X,r,y) using LeftRayX_def
RightRayX_def
  assms(1) IsLinOrder_def IsTotal_def by auto
  then have x∈ $\bigcup$  B using T by auto
  then have x:x∈ $\bigcup$  (OrdTopology X r) using Top_1_2_L5 base by auto
  {
    fix z
    assume z:z∈X
    {
      assume x=z
      then have z∈ $\bigcup$  (OrdTopology X r) using x by auto
    }
    moreover
    {
      assume x≠z
      with z T have z∈LeftRayX(X,r,x)∨z∈RightRayX(X,r,x)x∈X using LeftRayX_def
RightRayX_def
      assms(1) IsLinOrder_def IsTotal_def by auto
      then have z∈ $\bigcup$  B by auto
    }
  }

```

```

      then have  $z \in \bigcup (\text{OrdTopology } X \text{ } r)$  using Top_1_2_L5 base by auto
    }
    ultimately have  $z \in \bigcup (\text{OrdTopology } X \text{ } r)$  by auto
  }
  then show  $X \subseteq \bigcup (\text{OrdTopology } X \text{ } r)$  by auto
  have  $\bigcup B \subseteq X$  using IntervalX_def LeftRayX_def RightRayX_def by auto
  then show  $\bigcup (\text{OrdTopology } X \text{ } r) \subseteq X$  using Top_1_2_L5 base by auto
qed

```

The interior, closure and boundary can be calculated using the formulas proved in the section that deals with this calculations using the base.

The subspace of an order topology doesn't have to be an order topology.

### 49.3.3 Right order and Left order topologies.

Notice that the left and right rays are closed under intersection, hence they form a base of a topology. They are called right order topology and left order topology respectively.

If the order in  $X$  has a minimal or a maximal element, is necessary to consider  $X$  as an element of the base or that limit point wouldn't be in any basic open set.

### 49.3.4 Right and Left Order topologies are topologies

```

lemma leftrays_base_condition:
  assumes IsLinOrder(X,r)
  shows {LeftRayX(X,r,b).  $b \in X \cup \{X\}$ } {satisfies the base condition}
proof-
  {
    fix U V
    assume  $U \in \{\text{LeftRayX}(X,r,b). \ b \in X \cup \{X\}\} \vee U \in \{\text{LeftRayX}(X,r,b). \ b \in X \cup \{X\}\}$ 
    then obtain b c where  $A: (b \in X \wedge U = \text{LeftRayX}(X,r,b)) \vee U = X (c \in X \wedge V = \text{LeftRayX}(X,r,c)) \vee V = XU \subseteq XV \subseteq X$ 
    unfolding LeftRayX_def by auto
    then have  $(U \cap V = \text{LeftRayX}(X,r, \text{SmallerOf}(r,b,c))) \wedge b \in X \wedge c \in X \vee U \cap V = XV (U \cap V = \text{LeftRayX}(X,r,c) \wedge c \in X)$ 
    using inter_lray_lray assms by auto
    moreover
    have  $b \in X \wedge c \in X \longrightarrow \text{SmallerOf}(r,b,c) \in X$  unfolding SmallerOf_def by (cases
    <b,c> ∈ r, auto)
    ultimately have  $U \cap V \in \{\text{LeftRayX}(X,r,b). \ b \in X \cup \{X\}\}$  by auto
    hence  $\forall x \in U \cap V. \ \exists W \in \{\text{LeftRayX}(X,r,b). \ b \in X \cup \{X\}\}. \ x \in W \wedge W \subseteq U \cap V$  by blast
  }
  moreover
  then show thesis using SatisfiesBaseCondition_def by auto
qed

```

```

lemma rightrays_base_condition:

```

```

assumes IsLinOrder(X,r)
shows {RightRayX(X,r,b). b∈X}∪{X} {satisfies the base condition}
proof-
{
  fix U V
  assume U∈{RightRayX(X,r,b). b∈X}∪{X}V∈{RightRayX(X,r,b). b∈X}∪{X}
  then obtain b c where A:(b∈X∧U=RightRayX(X,r,b))∨U=X(c∈X∧V=RightRayX(X,r,c))∨V=XU⊆XV
  unfolding RightRayX_def by auto
  then have (U∩V=RightRayX(X,r,GreaterOf(r,b,c))∧b∈X∧c∈X)∨U∩V=XV(U∩V=RightRayX(X,r,c)∧
    using inter_rray_rray assms by auto
  moreover
  have b∈X∧c∈X ⟶ GreaterOf(r,b,c)∈X using GreaterOf_def by (cases
    ⟨b,c⟩∈r,auto)
  ultimately have U∩V∈{RightRayX(X,r,b). b∈X}∪{X} by auto
  hence ∀x∈U∩V. ∃W∈{RightRayX(X,r,b). b∈X}∪{X}. x∈W∧W⊆U∩V by blast
}
then show thesis using SatisfiesBaseCondition_def by auto
qed

```

**definition**

```

LeftOrderTopology (LOrdTopology _ _ 50) where
  IsLinOrder(X,r) ⟹ LOrdTopology X r ≡ TopologyBase {LeftRayX(X,r,b).
    b∈X}∪{X}

```

**definition**

```

RightOrderTopology (ROrdTopology _ _ 50) where
  IsLinOrder(X,r) ⟹ ROrdTopology X r ≡ TopologyBase {RightRayX(X,r,b).
    b∈X}∪{X}

```

**theorem** LOrdtopology\_ROrdtopology\_are\_topologies:

```

  assumes IsLinOrder(X,r)
  shows (LOrdTopology X r) {is a topology} and {LeftRayX(X,r,b). b∈X}∪{X}
    {is a base for} (LOrdTopology X r)
  and (ROrdTopology X r) {is a topology} and {RightRayX(X,r,b). b∈X}∪{X}
    {is a base for} (ROrdTopology X r)
  using Base_topology_is_a_topology leftrays_base_condition assms rightrays_base_condition
    LeftOrderTopology_def RightOrderTopology_def by auto

```

**lemma** topology0\_lordtopology\_rordtopology:

```

  assumes IsLinOrder(X,r)
  shows topology0(LOrdTopology X r) and topology0(ROrdTopology X r)
  using LOrdtopology_ROrdtopology_are_topologies topology0_def assms by
    auto

```

### 49.3.5 Total set

The topology is defined on the set  $X$

**lemma** union\_lordtopology\_rordtopology:



```

assumes IsLinOrder(X,r)
shows  $\bigcup (L0rdTopology\ X\ r)=X$  and  $\bigcup (R0rdTopology\ X\ r)=X$ 
using Top_1_2_L5[OF L0rdtopology_R0rdtopology_are_topologies(2)[OF assms]]
      Top_1_2_L5[OF L0rdtopology_R0rdtopology_are_topologies(4)[OF assms]]
unfolding LeftRayX_def RightRayX_def by auto

```

## 49.4 Union of Topologies

The union of two topologies is not a topology. A way to overcome this fact is to define the following topology:

**definition**

```

joinT (joinT _ 90) where
  ( $\forall T \in M. T \text{ is a topology} \wedge (\forall Q \in M. \bigcup Q = \bigcup T) \implies (\text{joinT } M \equiv \text{THE } T. (\bigcup M) \text{ is a subbase for } T)$ )

```

First let's proof that given a family of sets, then it is a subbase for a topology.

The first result states that from any family of sets we get a base using finite intersections of them. The second one states that any family of sets is a subbase of some topology.

**theorem subset\_as\_subbase:**

```

shows  $\{\bigcap A. A \in \text{FinPow}(B)\} \text{ satisfies the base condition}$ 
proof-
{
  fix U V
  assume A:  $U \in \{\bigcap A. A \in \text{FinPow}(B)\} \wedge V \in \{\bigcap A. A \in \text{FinPow}(B)\}$ 
  then obtain M R where MR:  $\text{Finite}(M) \text{Finite}(R) M \subseteq B R \subseteq B$ 
  U =  $\bigcap M V = \bigcap R$ 
  using FinPow_def by auto
  {
    fix x
    assume AS:  $x \in U \cap V$ 
    then have N:  $M \neq \emptyset R \neq \emptyset$  using MR(5,6) by auto
    have Finite(M  $\cup$  R) using MR(1,2) by auto
    moreover
    have M  $\cup$  R  $\in \text{Pow}(B)$  using MR(3,4) by auto
    ultimately have M  $\cup$  R  $\in \text{FinPow}(B)$  using FinPow_def by auto
    then have  $\bigcap (M \cup R) \in \{\bigcap A. A \in \text{FinPow}(B)\}$  by auto
    moreover
    from N have  $\bigcap (M \cup R) \subseteq \bigcap M \cap \bigcap (M \cup R) \subseteq \bigcap R$  by auto
    then have  $\bigcap (M \cup R) \subseteq U \cap V$  using MR(5,6) by auto
    moreover
    {
      fix S
      assume S  $\in M \cup R$ 
      then have S  $\in M \vee S \in R$  by auto
      then have  $x \in S$  using AS MR(5,6) by auto
    }
  }
}

```

```

      then have  $x \in \bigcap (M \cup R)$  using N by auto
      ultimately have  $\exists W \in \{\bigcap A. A \in \text{FinPow}(B)\}. x \in W \wedge W \subseteq U \cap V$  by blast
    }
    then have  $(\forall x \in U \cap V. \exists W \in \{\bigcap A. A \in \text{FinPow}(B)\}. x \in W \wedge W \subseteq U \cap V)$  by
auto
  }
  then have  $\forall U V. ((U \in \{\bigcap A. A \in \text{FinPow}(B)\} \wedge V \in \{\bigcap A. A \in \text{FinPow}(B)\})$ 
 $\longrightarrow$ 
     $(\forall x \in U \cap V. \exists W \in \{\bigcap A. A \in \text{FinPow}(B)\}. x \in W \wedge W \subseteq U \cap V))$  by auto
  then show  $\{\bigcap A. A \in \text{FinPow}(B)\}$  {satisfies the base condition}
    using SatisfiesBaseCondition_def by auto
qed

```

```

theorem Top_subbase:
  assumes  $T = \{\bigcup A. A \in \text{Pow}(\{\bigcap A. A \in \text{FinPow}(B)\})\}$ 
  shows  $T$  {is a topology} and  $B$  {is a subbase for}  $T$ 
proof-
  {
    fix S
    assume  $S \in B$ 
    then have  $\{S\} \in \text{FinPow}(B) \cap \{S\} = S$  using FinPow_def by auto
    then have  $\{S\} \in \text{Pow}(\{\bigcap A. A \in \text{FinPow}(B)\})$  by (blast+)
    then have  $\bigcup \{S\} \in \{\bigcup A. A \in \text{Pow}(\{\bigcap A. A \in \text{FinPow}(B)\})\}$  by blast
    then have  $S \in \{\bigcup A. A \in \text{Pow}(\{\bigcap A. A \in \text{FinPow}(B)\})\}$  by auto
    then have  $S \in T$  using assms by auto
  }
  then have  $B \subseteq T$  by auto
  moreover
  have  $\{\bigcap A. A \in \text{FinPow}(B)\}$  {satisfies the base condition}
    using subset_as_subbase by auto
  then have  $T$  {is a topology} and  $\{\bigcap A. A \in \text{FinPow}(B)\}$  {is a base for}
T
    using Top_1_2_T1 assms by auto
  ultimately show  $T$  {is a topology} and  $B$  {is a subbase for}  $T$ 
    using IsASubBaseFor_def by auto
qed

```

A subbase can defines a unique topology.

```

theorem same_subbase_same_top:
  assumes  $B$  {is a subbase for}  $T$  and  $B$  {is a subbase for}  $S$ 
  shows  $T = S$ 
  using IsASubBaseFor_def assms same_base_same_top
  by auto
end

```

## 50 Topology\_ZF\_properties.thy

theory Topology\_ZF\_properties imports Topology\_ZF\_examples Topology\_ZF\_examples\_1

begin

This theory deals with topological properties which make use of cardinals.

### 50.1 Properties of compactness

It is already defined what is a compact topological space, but there is a generalization which may be useful sometimes.

**definition**

```
IsCompactOfCard (_{is compact of cardinal}_ {in}_ 90)
where K{is compact of cardinal} Q{in}T  $\equiv$  (Card(Q)  $\wedge$   $K \subseteq \bigcup T$   $\wedge$ 
 $(\forall M \in \text{Pow}(T). K \subseteq \bigcup M \longrightarrow (\exists N \in \text{Pow}(M). K \subseteq \bigcup N \wedge N \prec Q))$ )
```

The usual compact property is the one defined over the cardinal of the natural numbers.

**lemma** Compact\_is\_card\_nat:

shows  $K\{\text{is compact in}\}T \longleftrightarrow (K\{\text{is compact of cardinal}\} \text{ nat } \{\text{in}\}T)$

**proof**

```
{
  assume K{is compact in}T
  then have sub:  $K \subseteq \bigcup T$  and reg:  $(\forall M \in \text{Pow}(T). K \subseteq \bigcup M \longrightarrow (\exists N \in \text{FinPow}(M). K \subseteq \bigcup N))$ 
  using IsCompact_def by auto
  {
    fix M
    assume  $M \in \text{Pow}(T) \wedge K \subseteq \bigcup M$ 
    with reg obtain N where  $N \in \text{FinPow}(M) \wedge K \subseteq \bigcup N$  by blast
    then have Finite(N) using FinPow_def by auto
    then obtain n where  $A: n \in \text{nat} \wedge N \approx n$  using Finite_def by auto
    from A(1) have  $n \prec \text{nat}$  using n_lesspoll_nat by auto
    with A(2) have  $N \lesssim \text{nat}$  using lesspoll_def eq_lepoll_trans by auto
    moreover
    {
      assume  $N \approx \text{nat}$ 
      then have  $\text{nat} \approx N$  using eqpoll_sym by auto
      with A(2) have  $\text{nat} \approx n$  using eqpoll_trans by blast
      then have  $n \approx \text{nat}$  using eqpoll_sym by auto
      with ' $n \prec \text{nat}$ ' have False using lesspoll_def by auto
    }
    then have  $\sim(N \approx \text{nat})$  by auto
    with calculation ' $K \subseteq \bigcup N$ ' ' $N \in \text{FinPow}(M)$ ' have  $N \prec \text{nat} \wedge K \subseteq \bigcup N$  by auto
  }
  using lesspoll_def
  FinPow_def by auto
  hence  $(\exists N \in \text{Pow}(M). K \subseteq \bigcup N \wedge N \prec \text{nat})$  by auto
}
```

```

    }
    with sub show K{is compact of cardinal} nat {in}T using IsCompactOfCard_def
Card_nat by auto
  }
  {
    assume (K{is compact of cardinal} nat {in}T)
    then have sub:K $\subseteq$  $\bigcup$ T and reg:( $\forall$  M $\in$ Pow(T). K  $\subseteq$   $\bigcup$ M  $\longrightarrow$  ( $\exists$  N  $\in$  Pow(M).
K  $\subseteq$   $\bigcup$ N  $\wedge$  N $\prec$ nat))
    using IsCompactOfCard_def by auto
    {
      fix M
      assume M $\in$ Pow(T)K $\subseteq$  $\bigcup$ M
      with reg have ( $\exists$  N  $\in$  Pow(M). K  $\subseteq$   $\bigcup$ N  $\wedge$  N $\prec$ nat) by auto
      then obtain N where N $\in$ Pow(M)K $\subseteq$  $\bigcup$ NN $\prec$ nat by blast
      then have N $\in$ FinPow(M)K $\subseteq$  $\bigcup$ N using lesspoll_nat_is_Finite FinPow_def
    by auto
    hence  $\exists$ N $\in$ FinPow(M). K $\subseteq$  $\bigcup$ N by auto
    }
    with sub show K{is compact in}T using IsCompact_def by auto
  }
}
qed

```

Another property of this kind widely used is the Lindelöf property; it is the one on the successor of the natural numbers.

**definition**

IsLindelöf ( $\_$ {is Lindelöf in} $\_$  90) **where**  
 K {is Lindelöf in} T $\equiv$ K{is compact of cardinal}csucc(nat){in}T

It would be natural to think that every countable set with any topology is Lindelöf; but this statement is not provable in ZF. The reason is that to build a subcover, most of the time we need to *choose* sets from an infinite collection which cannot be done in ZF. Additional axioms are needed, but strictly weaker than the axiom of choice.

**definition**

AxiomCardinalChoice ({the axiom of} $\_$ {choice holds for subsets} $\_$ ) **where**  
 {the axiom of} Q {choice holds for subsets}K  $\equiv$  Card(Q)  $\wedge$  ( $\forall$  M N. (M  $\lesssim$ Q  $\wedge$  ( $\forall$ t $\in$ M. Nt $\neq$ 0  $\wedge$  Nt $\subseteq$ K))  $\longrightarrow$  ( $\exists$ f. f:Pi(M, $\lambda$ t. Nt)  $\wedge$  ( $\forall$ t $\in$ M. ft $\in$ Nt)))

**definition**

AxiomCardinalChoiceGen ({the axiom of} $\_$ {choice holds}) **where**  
 {the axiom of} Q {choice holds}  $\equiv$  Card(Q)  $\wedge$  ( $\forall$  M N. (M  $\lesssim$ Q  $\wedge$  ( $\forall$ t $\in$ M. Nt $\neq$ 0))  $\longrightarrow$  ( $\exists$ f. f:Pi(M, $\lambda$ t. Nt)  $\wedge$  ( $\forall$ t $\in$ M. ft $\in$ Nt)))

The axiom of choice holds if and only if the AxiomCardinalChoice holds for every couple of a cardinal Q and a set K.

**lemma** choice\_subset\_imp\_choice:

shows {the axiom of} Q {choice holds}  $\longleftrightarrow$  (ALL K. {the axiom of} Q {choice holds for subsets}K)

**unfolding** AxiomCardinalChoice\_def AxiomCardinalChoiceGen\_def by blast

If a set is compact of cardinality  $Q$  for some topology, it is compact of cardinality  $Q$  for every coarser topology.

**theorem** compact\_coarser:

assumes  $T_1 \subseteq T$  and  $\bigcup T_1 = \bigcup T$  and  $(K)\{\text{is compact of cardinality } Q\} \in T$   
 shows  $(K)\{\text{is compact of cardinality } Q\} \in T_1$

**proof-**

{  
 fix  $M$   
 assume  $AS: M \in \text{Pow}(T_1) \text{ and } K \subseteq \bigcup M$   
 then have  $M \in \text{Pow}(T) \text{ and } K \subseteq \bigcup M$  using assms(1) by auto  
 then have  $\exists N \in \text{Pow}(M). K \subseteq \bigcup N \wedge \text{card } N < Q$  using assms(3) unfolding IsCompactOfCard\_def

by auto

}  
 then show  $(K)\{\text{is compact of cardinality } Q\} \in T_1$  using assms(3,2) unfolding

IsCompactOfCard\_def by auto

**qed**

A closed subspace of a compact space of any cardinality, is also compact of the same cardinality.

**theorem** compact\_closed:

assumes  $K \{\text{is compact of cardinality } Q\} \in T$   
 and  $R \{\text{is closed in } T\}$   
 shows  $(K \cap R) \{\text{is compact of cardinality } Q\} \in T$

**proof-**

{  
 fix  $M$   
 assume  $AS: M \in \text{Pow}(T) \text{ and } K \cap R \subseteq \bigcup M$   
 have  $\bigcup T - R \in T$  using assms(2) IsClosed\_def by auto  
 have  $K - R \subseteq (\bigcup T - R)$  using assms(1) IsCompactOfCard\_def by auto  
 with ' $\bigcup T - R \in T$ ' have  $K \subseteq \bigcup (M \cup \{\bigcup T - R\})$  and  $M \cup \{\bigcup T - R\} \in \text{Pow}(T)$   
 proof (safe)

{  
 fix  $x$   
 assume  $x \in M$   
 with AS(1) show  $x \in T$  by auto  
 }  
 {

fix  $x$   
 assume  $x \in K$   
 have  $x \in R \vee x \notin R$  by auto  
 with ' $x \in K$ ' have  $x \in K \cap R \vee x \in K - R$  by auto  
 with AS(2) ' $K - R \subseteq (\bigcup T - R)$ ' have  $x \in \bigcup M \vee x \in (\bigcup T - R)$  by auto  
 then show  $x \in \bigcup (M \cup \{\bigcup T - R\})$  by auto  
 }

**qed**

with assms(1) have  $\exists N \in \text{Pow}(M \cup \{\bigcup T - R\}). K \subseteq \bigcup N \wedge \text{card } N < Q$  unfolding IsCompactOfCard\_def by auto

```

then obtain N where cub:N∈Pow(M∪{⋃T-R}) K⊆⋃N N<Q by auto
have N-{⋃T-R}∈Pow(M)K∩R⊆⋃(N-{⋃T-R}) N-{⋃T-R}<Q
proof (safe)
  {
    fix x
    assume x∈Nx∉M
    then show x=⋃T-R using cub(1) by auto
  }
  {
    fix x
    assume x∈Kx∈R
    then have x∉⋃T-Rx∈K by auto
    then show x∈⋃(N-{⋃T-R}) using cub(2) by blast
  }
  have N-{⋃T-R}⊆N by auto
  with cub(3) show N-{⋃T-R}<Q using subset_imp_lepoll lesspoll_trans1
by blast
qed
then have ∃N∈Pow(M). K∩R⊆⋃N ∧ N<Q by auto
}
then have ∀M∈Pow(T). (K ∩ R ⊆ ⋃M → (∃N∈Pow(M). K ∩ R ⊆ ⋃N ∧ N
< Q)) by auto
then show thesis using IsCompactOfCard_def assms(1) by auto
qed

```

## 50.2 Properties of numerability

The properties of numerability deal with cardinals of some sets built from the topology. The properties which are normally used are the ones related to the cardinal of the natural numbers or its successor.

### definition

IsFirstOfCard ( $\_$  {is of first type of cardinal}\_ 90) where  
 $(T \text{ {is of first type of cardinal}} Q) \equiv \forall x \in \bigcup T. (\exists B. (B \text{ {is a base for}} T) \wedge (\{b \in B. x \in b\} < Q))$

### definition

IsSecondOfCard ( $\_$  {is of second type of cardinal}\_ 90) where  
 $(T \text{ {is of second type of cardinal}} Q) \equiv (\exists B. (B \text{ {is a base for}} T) \wedge (B < Q))$

### definition

IsSeparableOfCard ( $\_$  {is separable of cardinal}\_ 90) where  
 $T \text{ {is separable of cardinal}} Q \equiv \exists U \in \text{Pow}(\bigcup T). \text{Closure}(U, T) = \bigcup T \wedge U < Q$

### definition

IsFirstCountable ( $\_$  {is first countable}\_ 90) where  
 $(T \text{ {is first countable}}) \equiv T \text{ {is of first type of cardinal}} \text{csucc}(\text{nat})$

### definition

IsSecondCountable (\_ {is second countable} 90) where  
 (T {is second countable})  $\equiv$  (T {is of second type of cardinal}csucc(nat))

**definition**

IsSeparable (\_{is separable} 90) where  
 T{is separable} $\equiv$  T{is separable of cardinal}csucc(nat)

If a set is of second type of cardinal Q, then it is of first type of that same cardinal.

**theorem second\_imp\_first:**

assumes T{is of second type of cardinal}Q  
 shows T{is of first type of cardinal}Q

**proof-**

from assms have  $\exists B. (B \text{ {is a base for} } T) \wedge (B \prec Q)$  using IsSecondOfCard\_def  
 by auto  
 then obtain B where base:(B {is a base for} T)  $\wedge$  (B  $\prec$  Q) by auto  
 {  
 fix x  
 assume  $x \in \bigcup T$   
 have  $\{b \in B. x \in b\} \subseteq B$  by auto  
 then have  $\{b \in B. x \in b\} \lesssim B$  using subset\_imp\_lepoll by auto  
 with base have  $\{b \in B. x \in b\} \prec Q$  using lesspoll\_trans1 by auto  
 with base have (B {is a base for} T)  $\wedge$   $\{b \in B. x \in b\} \prec Q$  by auto  
 }  
 then have  $\forall x \in \bigcup T. \exists B. (B \text{ {is a base for} } T) \wedge \{b \in B. x \in b\} \prec Q$  by auto  
 then show thesis using IsFirstOfCard\_def by auto  
 qed

A set is dense iff it intersects all non-empty, open sets of the topology.

**lemma dense\_int\_open:**

assumes T{is a topology} and  $A \subseteq \bigcup T$   
 shows  $\text{Closure}(A, T) = \bigcup T \iff (\forall U \in T. U \neq 0 \longrightarrow A \cap U \neq 0)$

**proof**

assume AS: $\text{Closure}(A, T) = \bigcup T$   
 {  
 fix U  
 assume Uopen: $U \in T$  and  $U \neq 0$   
 then have  $U \cap \bigcup T \neq 0$  by auto  
 with AS have  $U \cap \text{Closure}(A, T) \neq 0$  by auto  
 with assms Uopen have  $U \cap A \neq 0$  using topology0.cl\_inter\_neigh topology0\_def  
 }  
 by blast  
 then show  $\forall U \in T. U \neq 0 \longrightarrow A \cap U \neq 0$  by auto  
 next  
 assume AS: $\forall U \in T. U \neq 0 \longrightarrow A \cap U \neq 0$   
 {  
 fix x  
 assume A: $x \in \bigcup T$   
 then have  $\forall U \in T. x \in U \longrightarrow U \cap A \neq 0$  using AS by auto

```

    with assms A have x∈Closure(A,T) using topology0.inter_neigh_cl topology0_def
  by auto
}
then have  $\bigcup T \subseteq \text{Closure}(A,T)$  by auto
with assms show  $\text{Closure}(A,T) = \bigcup T$  using topology0.Top_3_L11(1) topology0_def
by blast
qed

```

### 50.2.1 Some cardinal related results

If we have a surjective function from a set which is injective to a set of ordinals, then we can find an injection which goes the other way.

```

lemma surj_fun_inv:
  assumes f:surj(A,B) A⊆QOrd(Q)
  shows B≲A
proof-
  let g={⟨m,LEAST j. j∈A∧ fj=m⟩. m∈B}
  have relation(g) unfolding relation_def by auto
  moreover
  have function(g) unfolding function_def by auto
  moreover
  have domain(g)=B by auto
  moreover
  have range(g)=gB by auto
  ultimately
  have fun:g:B→gB using function_imp_Pi[of g] by auto
  from assms(2,3) have 0A:!!j. j∈A ⇒ Ord(j) unfolding lt_def using
Ord_in_Ord by auto
  {
    fix x
    assume x∈gB
    then have x∈range(g) ∃y∈B. ⟨y,x⟩∈g by auto
    then obtain y where T:x=(LEAST j. j∈A∧ fj=y)y∈B by auto
    then obtain z where fz=yz∈A0rd(z) using assms(1) 0A unfolding surj_def
  by auto
    then have (LEAST j. j∈A∧ fj=y)∈A using LeastI[where i=z and P=λz.
z∈A∧fz=y] by auto
    then have x∈A using T by auto
  }
  then have gB⊆A by auto
  with fun have fun2:g:B→A using fun_weaken_type by auto
  then have g∈inj(B,A) unfolding inj_def apply auto
proof-
  fix w x
  assume AS:gw=gxw∈Bx∈B
  from AS(2,3) obtain wz xz where fwz=wfxz=xwz∈Axz∈A0rd(wz)Ord(xz)
using assms(1) 0A unfolding
surj_def by blast
  then have R:f(LEAST j. j∈A∧ fj=w)=wf(LEAST j. j∈A∧ fj=x)=x using

```



```

LeastI[where i=wz and P= $\lambda$ z.  $z \in A \wedge fz=w$ ]
  LeastI[where i=xz and P= $\lambda$ z.  $z \in A \wedge fz=x$ ] by auto
  from AS have (LEAST j.  $j \in A \wedge fj=w$ )=(LEAST j.  $j \in A \wedge fj=x$ ) using apply_equality
fun2 by auto
  then have f(LEAST j.  $j \in A \wedge fj=w$ )=f(LEAST j.  $j \in A \wedge fj=x$ ) by auto
  with R(1) have w=f(LEAST j.  $j \in A \wedge fj=x$ ) by auto
  with R(2) show w=x by auto
qed
then show thesis unfolding lepoll_def by auto
qed

```

The difference with the previous result is that in this one  $A$  is not a subset of an ordinal, it is only injective with one.

```

theorem surj_fun_inv_2:
  assumes f:surj(A,B)  $A \lesssim \aleph_0 \text{ord}(Q)$ 
  shows  $B \lesssim A$ 
proof-
  from assms(2) obtain h where h_def:h $\in$ inj(A,Q) using lepoll_def by
auto
  then have bij:h $\in$ bij(A,range(h)) using inj_bij_range by auto
  then obtain h1 where h1 $\in$ bij(range(h),A) using bij_converse_bij by
auto
  then have h1 $\in$ surj(range(h),A) using bij_def by auto
  then have (f 0 h1) $\in$ surj(range(h),B) using assms(1) comp_surj by auto
  moreover
  {
    fix x
    assume p:x $\in$ range(h)
    from bij have h $\in$ surj(A,range(h)) using bij_def by auto
    with p obtain q where q $\in$ A and hq=x using surj_def by auto
    then have x $\in$ Q using h_def inj_def by auto
  }
  then have range(h) $\subseteq$ Q by auto
  ultimately have  $B \lesssim \text{range}(h)$  using surj_fun_inv[of f 0 h1] assms(3) by
auto
  moreover
  have range(h) $\approx$ A using bij eqpoll_def eqpoll_sym by blast
  ultimately show  $B \lesssim A$  using lepoll_eq_trans by auto
qed

```

## 50.2.2 Relations between numerability properties

It is known that some statements in topology aren't just derived from choice axioms, but also equivalent to them. Here is an example

The following are equivalent:

- Every topological space of second cardinality  $\text{csucc}(Q)$  is separable of cardinality  $\text{csucc}(Q)$ .

- The axiom of  $Q$  choice.

In the article [4] there is a proof of this statement for  $Q = \mathbb{N}$ , with more equivalences.

If a set is of second type of cardinal  $\text{csucc}(Q)$ , then it is separable of the same cardinal. This result makes use of the axiom of choice for the cardinal  $Q$  on subsets of  $\bigcup T$ .

```

theorem Q_choice_imp_second_imp_separable:
  assumes T{is of second type of cardinal}csucc(Q)
    and {the axiom of} Q {choice holds for subsets}  $\bigcup T$ 
    and T{is a topology}
  shows T{is separable of cardinal}csucc(Q)
proof-
  from assms(1) have  $\exists B. (B \text{ {is a base for} } T) \wedge (B \prec \text{csucc}(Q))$  us-
ing IsSecondOfCard_def by auto
  then obtain B where base:(B {is a base for} T)  $\wedge (B \prec \text{csucc}(Q))$  by
auto
  let N= $\lambda b \in B. b$ 
  let B=B- $\{0\}$ 
  have B- $\{0\} \subseteq B$  by auto
  with base have prec:B- $\{0\} \prec \text{csucc}(Q)$  using subset_imp_lepoll lesspoll_trans1
by blast
  from base have baseOpen: $\forall b \in B. \text{Nb} \in T$  using base_sets_open by auto
  from assms(2) have car:Card(Q) and reg:( $\forall M N. (M \lesssim Q \wedge (\forall t \in M. \text{Nt} \neq 0$ 
 $\wedge \text{Nt} \subseteq \bigcup T)) \longrightarrow (\exists f. f:\text{Pi}(M, \lambda t. \text{Nt}) \wedge (\forall t \in M. ft \in \text{Nt}))$ )
  using AxiomCardinalChoice_def by auto
  then have  $(B \lesssim Q \wedge (\forall t \in B. \text{Nt} \neq 0 \wedge \text{Nt} \subseteq \bigcup T)) \longrightarrow (\exists f. f:\text{Pi}(B, \lambda t. \text{Nt})$ 
 $\wedge (\forall t \in B. ft \in \text{Nt}))$  by blast
  with prec have  $(\forall t \in B. \text{Nt} \subseteq \bigcup T) \longrightarrow (\exists f. f:\text{Pi}(B, \lambda t. \text{Nt}) \wedge (\forall t \in B. ft \in \text{Nt}))$ 
using Card_less_csucc_eq_le car by auto
  with baseOpen have  $\exists f. f:\text{Pi}(B, \lambda t. \text{Nt}) \wedge (\forall t \in B. ft \in \text{Nt})$  by blast
  then obtain f where f: $f:\text{Pi}(B, \lambda t. \text{Nt})$  and f2: $\forall t \in B. ft \in \text{Nt}$  by auto
  {
    fix U
    assume  $U \in T$  and  $U \neq 0$ 
    then obtain b where A1: $b \in B - \{0\}$  and  $b \subseteq U$  using Top_1_2_L1 base by
blast
    with f2 have fb $\in U$  by auto
    with A1 have {fb.  $b \in B$ } $\cap U \neq 0$  by auto
  }
  then have r: $\forall U \in T. U \neq 0 \longrightarrow \{fb. b \in B\} \cap U \neq 0$  by auto
  have {fb.  $b \in B$ } $\subseteq \bigcup T$  using f2 baseOpen by auto
  moreover
  with r have Closure({fb.  $b \in B$ }, T)= $\bigcup T$  using dense_int_open assms(3)
by auto
  moreover
  have ffun: $f:B \rightarrow \text{range}(f)$  using f range_of_fun by auto
  then have  $f \in \text{surj}(B, \text{range}(f))$  using fun_is_surj by auto

```

```

    then have des1:range(f)  $\lesssim$  B using surj_fun_inv_2[of fBrange(f)Q] prec
Card_less_csucc_eq_le car
    Card_is_Ord by auto
    then have {fb. b  $\in$  B}  $\subseteq$  range(f) using apply_rangeI[OF ffun] by auto
    then have {fb. b  $\in$  B}  $\lesssim$  range(f) using subset_imp_lepoll by auto
    with des1 have {fb. b  $\in$  B}  $\lesssim$  B using lepoll_trans by blast
    with prec have {fb. b  $\in$  B}  $\prec$  csucc(Q) using lesspoll_trans1 by auto
    ultimately show thesis using IsSeparableOfCard_def by auto
qed

```

The next theorem resolves that the axiom of  $\mathcal{Q}$  choice for subsets of  $\bigcup T$  is necessary for second type spaces to be separable of the same cardinal  $\text{csucc}(Q)$ .

```

theorem second_imp_separable_imp_Q_choice:
  assumes  $\forall T. (T\{\text{is a topology}\} \wedge (T\{\text{is of second type of cardinal}\}\text{csucc}(Q)))$ 
 $\longrightarrow (T\{\text{is separable of cardinal}\}\text{csucc}(Q))$ 
  and Card(Q)
  shows {the axiom of} Q {choice holds}
proof-
  {
    fix N M
    assume AS:M  $\lesssim$  Q  $\wedge (\forall t \in M. Nt \neq 0)$ 

    then obtain h where inj:h  $\in$  inj(M,Q) using lepoll_def by auto
    then have bij:converse(h):bij(range(h),M) using inj_bij_range bij_converse_bij
  by auto
    let T={N(converse(h)i))  $\times$  {i}. i  $\in$  range(h)}
    {
      fix j
      assume AS2:j  $\in$  range(h)
      from bij have converse(h):range(h)  $\rightarrow$  M using bij_def inj_def by
    auto
      with AS2 have converse(h)j  $\in$  M by simp
      with AS have N(converse(h)j)  $\neq$  0 by auto
      then have (N(converse(h)j))  $\times$  {j}  $\neq$  0 by auto
    }
    then have noEmpty:0  $\notin$  T by auto
    moreover
    {
      fix A B
      assume AS2:A  $\in$  T  $\wedge$  B  $\in$  T  $\wedge$  A  $\cap$  B  $\neq$  0
      then obtain j t where A_def:A=N(converse(h)j)  $\times$  {j} and B_def:B=N(converse(h)t)  $\times$  {t}
        and Range:j  $\in$  range(h) t  $\in$  range(h) by auto
      from AS2(3) obtain x where x  $\in$  A  $\cap$  B by auto
      with A_def B_def have j=t by auto
      with A_def B_def have A=B by auto
    }
    then have ( $\forall A \in T. \forall B \in T. A=B \vee A \cap B=0$ ) by auto
    ultimately

```

```

    have Part:T {is a partition of}  $\bigcup T$  unfolding IsAPartition_def by
auto
    let  $\tau$ =PTopology  $\bigcup T$ 
    from Part have top: $\tau$  {is a topology} and base:T {is a base for} $\tau$ 
        using Ptopology_is_a_topology by auto
    let f={⟨i,(N(converse(h)i)) $\times$ {i}⟩. i $\in$ range(h)}
    have f:range(h) $\rightarrow$ T using functionI[of f] Pi_def by auto
    then have f $\in$ surj(range(h),T) unfolding surj_def using apply_equality
by auto
    moreover
    have range(h) $\subseteq$ Q using inj unfolding inj_def range_def domain_def
Pi_def by auto
    ultimately have T $\lesssim$  Q using surj_fun_inv[of frange(h)TQ] assms(2)
Card_is_Ord lepoll_trans
    subset_imp_lepoll by auto
    then have T $\prec$ csucc(Q) using Card_less_csucc_eq_le assms(2) by auto
    with base have ( $\tau$ {is of second type of cardinal}csucc(Q)) using IsSecondOfCard_def
by auto
    with top have  $\tau$ {is separable of cardinal}csucc(Q) using assms(1)
by auto
    then obtain D where sub:D $\in$ Pow( $\bigcup \tau$ ) and clos:Closure(D, $\tau$ )= $\bigcup \tau$  and
cardd:D $\prec$ csucc(Q)
        using IsSeparableOfCard_def by auto

    then have D $\lesssim$ Q using Card_less_csucc_eq_le assms(2) by auto
    then obtain r where r:r $\in$ inj(D,Q) using lepoll_def by auto
    then have bij2:converse(r):bij(range(r),D) using inj_bij_range bij_converse_bij
by auto
    then have surj2:converse(r):surj(range(r),D) using bij_def by auto
    let R= $\lambda i \in$ range(h). {j $\in$ range(r). converse(r)j $\in$ ((N(converse(h)i)) $\times$ {i})}
    {
        fix i
        assume AS:i $\in$ range(h)
        then have T:(N(converse(h)i)) $\times$ {i} $\in$ T by auto
        then have op:(N(converse(h)i)) $\times$ {i} $\in \tau$  using base unfolding IsAbaseFor_def
by blast
        with top sub clos have  $\forall U \in \tau. U \neq 0 \rightarrow D \cap U \neq 0$  using dense_int_open
by auto
        with op have (N(converse(h)i)) $\times$ {i} $\neq 0 \rightarrow D \cap$ (N(converse(h)i)) $\times$ {i} $\neq 0$ 
by auto
        with T noEmpty have D $\cap$ (N(converse(h)i)) $\times$ {i} $\neq 0$  by auto
        then obtain x where x $\in$ D and px:x $\in$ (N(converse(h)i)) $\times$ {i} by auto
        with surj2 obtain j where j $\in$ range(r) and converse(r)j=x unfold-
ing surj_def by blast
        with px have j $\in$ {j $\in$ range(r). converse(r)j $\in$ ((N(converse(h)i)) $\times$ {i})}
by auto
        then have Ri $\neq 0$  using beta_if[of range(h) _ i] AS by auto
    }
    then have nonE: $\forall i \in$ range(h). Ri $\neq 0$  by auto

```

```

    {
      fix i j
      assume i:i∈range(h) and j:j∈Ri
      from j i have converse(r)j∈((N(converse(h)i))×{i}) using beta_if
    }
  by auto
  }
  then have pp:∀i∈range(h). ∀j∈Ri. converse(r)j∈((N(converse(h)i))×{i})
  by auto
  let E={⟨m,fst(converse(r)(LEAST j. j∈R(hm)))⟩. m∈M}
  have ff:function(E) unfolding function_def by auto
  moreover

  {
    fix m
    assume M:m∈M
    with inj have hm:hm∈range(h) using apply_rangeI inj_def by auto
    {
      fix j
      assume j∈R(hm)
      with hm have j∈range(r) using beta_if by auto
      from r have r:surj(D,range(r)) using fun_is_surj inj_def by auto
      with 'j∈range(r)' obtain d where d∈D and rd=j using surj_def
    }
  by auto
    then have j∈Q using r inj_def by auto
  }
  then have subcar:R(hm)⊆Q by blast
  from nonE hm obtain ee where P:ee∈R(hm) by blast
  with subcar have ee∈Q by auto
  then have Ord(ee) using assms(2) Card_is_Ord Ord_in_Ord by auto
  with P have (LEAST j. j∈R(hm))∈R(hm) using LeastI[where i=ee and
P=λj. j∈R(hm)]
  by auto
  with pp hm have converse(r)(LEAST j. j∈R(hm))∈((N(converse(h)(hm)))×{(hm)})
  by auto
  then have converse(r)(LEAST j. j∈R(hm))∈((N(m))×{(hm)}) using
left_inverse[OF inj M]
  by simp
  then have fst(converse(r)(LEAST j. j∈R(hm)))∈(N(m)) by auto
  }
  ultimately have thesis1:∀m∈M. Em∈(N(m)) using function_apply_equality
  by auto
  {
    fix e
    assume e∈E
    then obtain m where m∈M and e=⟨m,Em⟩ using function_apply_equality
  by auto
    with thesis1 have e∈Sigma(M,λt. Nt) by auto
  }
  then have E∈Pow(Sigma(M,λt. Nt)) by auto

```

```

      with ff have E∈Pi(M,λm. Nm) using Pi_iff by auto
      then have (∃f. f:Pi(M,λt. Nt) ∧ (∀t∈M. ft∈Nt)) using thesis1 by
auto
    }
    then show thesis using AxiomCardinalChoiceGen_def assms(2) by auto
qed

```

Here is the equivalence from the two previous results.

```

theorem Q_choice_eq_secon_imp_sepa:
  assumes Card(Q)
  shows (∀T. (T{is a topology} ∧ (T{is of second type of cardinal}csucc(Q)))
→ (T{is separable of cardinal}csucc(Q)))
  <=>({the axiom of} Q {choice holds})
  using Q_choice_imp_second_imp_separable choice_subset_imp_choice
  using second_imp_separable_imp_Q_choice assms by auto

```

Given a base injective with a set, then we can find a base whose elements are indexed by that set.

```

lemma base_to_indexed_base:
  assumes B ≲Q B {is a base for}T
  shows ∃N. {Ni. i∈Q}{is a base for}T
proof-
  from assms obtain f where f_def:f∈inj(B,Q) unfolding lepoll_def by
auto
  let ff={⟨b,fb⟩. b∈B}
  have domain(ff)=B by auto
  moreover
  have relation(ff) unfolding relation_def by auto
  moreover
  have function(ff) unfolding function_def by auto
  ultimately
  have fun:ff:B→range(ff) using function_imp_Pi[of ff] by auto
  then have injj:ff∈inj(B,range(ff)) unfolding inj_def apply simp
  apply safe
proof-
  fix w x
  assume AS:w∈Bx∈B{⟨b, f b⟩ . b ∈ B} w = {⟨b, f b⟩ . b ∈ B} x
  then have fw=fx using apply_equality[OF _ fun] by auto
  then show w=x using f_def inj_def AS(1,2) by auto
qed
then have bij:ff∈bij(B,range(ff)) using inj_bij_range by auto
from fun have range(ff)={fb. b∈B} by auto
then have ran:range(ff)⊆Q using f_def unfolding inj_def by auto
let N={⟨i,(if i∈range(ff) then converse(ff)i else 0)⟩. i∈Q}
have FN:function(N) unfolding function_def by auto
have B ⊆{Ni. i∈Q}
proof
  fix t
  assume a:t∈B

```

```

    from bij have rr:ff:B→range(ff) unfolding bij_def inj_def by auto
    have ig:fft=ft using a apply_equality[OF _ rr] by auto
    have r:fft∈range(ff) using apply_type[OF rr a].
    with ran have t:fft∈Qfft∈range(ff) apply safe by auto
    have N(fft)=converse(ff)(fft) using function_apply_equality[OF _
      FN] t by auto
    then have N(fft)=t using left_inverse[OF injj a] by auto
    then have t=N(fft) by auto
    then have ∃i∈Q. t=Ni using t(1) by auto
    then show t∈{Ni. i∈Q} by simp
qed
moreover
have ∀r∈{Ni. i∈Q}-B. r=0
proof
  fix r
  assume r∈{Ni. i∈Q}-B
  then obtain j where R:j∈Qr=Njr∉B by auto
  {
    assume AS:j∈range(ff)
    with R(1) have Nj=converse(ff)j using function_apply_equality[OF
-
      FN] by auto
    then have Nj∈B using apply_funtype[OF inj_is_fun[OF bij_is_inj[OF
bij_converse_bij[OF bij]]] AS]
    by auto
    then have False using R(3,2) by auto
  }
  then have j∉range(ff) by auto
  then show r=0 using function_apply_equality[OF _ FN] R(1,2) by auto
qed
ultimately have {Ni. i∈Q}=BV{Ni. i∈Q}=B ∪{0} by blast
moreover
have (B ∪{0})-{0}=B-{0} by blast
then have (B ∪{0})-{0} {is a base for}T using base_no_0[of BT] assms(2)
by auto
then have B ∪{0} {is a base for}T using base_no_0[of B ∪{0}T] by auto
ultimately
have {Ni. i∈Q}{is a base for}T using assms(2) by auto
then show thesis by auto
qed

```

### 50.3 Relation between numerability and compactness

If the axiom of  $\mathcal{Q}$  choice holds, then any topology of second type of cardinal  $\text{csucc}(\mathcal{Q})$  is compact of cardinal  $\text{csucc}(\mathcal{Q})$

**theorem compact\_of\_cardinal\_Q:**

```

  assumes {the axiom of} Q {choice holds for subsets} (Pow(Q))
    T{is of second type of cardinal}csucc(Q)
    T{is a topology}

```

```

shows (( $\bigcup T$ ){is compact of cardinal}csucc(Q){in}T)
proof-
  from assms(1) have CC:Card(Q) and reg: $\bigwedge M N. (M \lesssim Q \wedge (\forall t \in M. Nt \neq 0 \wedge Nt \subseteq \text{Pow}(Q)))$ 
 $\longrightarrow (\exists f. f: \text{Pi}(M, \lambda t. Nt) \wedge (\forall t \in M. ft \in Nt))$  using
  AxiomCardinalChoice_def by auto
  from assms(2) obtain R where  $R \lesssim QR$ {is a base for}T unfolding IsSecondOfCard_def
  using Card_less_csucc_eq_le CC by auto
  with base_to_indexed_base obtain N where base:{Ni.  $i \in Q$ }{is a base for}T
  by blast
  {
    fix M
    assume A: $\bigcup T \subseteq \bigcup MM \in \text{Pow}(T)$ 
    let  $\alpha = \lambda U \in M. \{i \in Q. N(i) \subseteq U\}$ 
    have inj: $\alpha \in \text{inj}(M, \text{Pow}(Q))$  unfolding inj_def apply safe apply auto
    using lam_type[of M  $\lambda U. \{i \in Q. N(i) \subseteq U\}$  t.  $\text{Pow}(Q)$ ] apply blast
    proof-
      {
        fix w x
        assume AS: $w \in Mx \in M\{i \in Q. N(i) \subseteq w\} = \{i \in Q. N(i) \subseteq x\}$ 
        from AS(1,2) A(2) have  $w \in Tx \in T$  by auto
        then have  $w = \text{Interior}(w, T)x = \text{Interior}(x, T)$  using assms(3) topology0.Top_2_L3[of
T]
        topology0_def[of T] by auto
        then have  $UN:w = (\bigcup \{B \in \{N(i). i \in Q\}. B \subseteq w\})x = (\bigcup \{B \in \{N(i). i \in Q\}. B \subseteq x\})$ 
        using interior_set_base_topology assms(3) base by auto
        {
          fix b
          assume  $b \in w$ 
          then have  $b \in \bigcup \{B \in \{N(i). i \in Q\}. B \subseteq w\}$  using UN(1) by auto
          then obtain S where  $S: S \in \{N(i). i \in Q\} b \in S S \subseteq w$  by blast
          then obtain j where  $j: j \in QS = N(j)$  by auto
          then have  $j \in \{i \in Q. N(i) \subseteq w\}$  using S(3) by auto
          then have  $N(j) \subseteq xb \in N(j)j \in Q$  using S(2) AS(3) j by auto
          then have  $b \in (\bigcup \{B \in \{N(i). i \in Q\}. B \subseteq x\})$  by auto
          then have  $b \in x$  using UN(2) by auto
        }
        moreover
        {
          fix b
          assume  $b \in x$ 
          then have  $b \in \bigcup \{B \in \{N(i). i \in Q\}. B \subseteq x\}$  using UN(2) by auto
          then obtain S where  $S: S \in \{N(i). i \in Q\} b \in S S \subseteq x$  by blast
          then obtain j where  $j: j \in QS = N(j)$  by auto
          then have  $j \in \{i \in Q. N(i) \subseteq x\}$  using S(3) by auto
          then have  $j \in \{i \in Q. N(i) \subseteq w\}$  using AS(3) by auto
          then have  $N(j) \subseteq wb \in N(j)j \in Q$  using S(2) j(2) by auto
          then have  $b \in (\bigcup \{B \in \{N(i). i \in Q\}. B \subseteq w\})$  by auto
          then have  $b \in w$  using UN(2) by auto
        }
      }
    }
  }

```



```

      ultimately show w=x by auto
    }
  qed
  let X= $\lambda i \in Q. \{\alpha U. U \in \{V \in M. N(i) \subseteq V\}\}$ 
  let M= $\{i \in Q. X_i \neq \emptyset\}$ 
  have subMQ: $M \subseteq Q$  by auto
  then have ddd: $M \lesssim Q$  using subset_imp_lepoll by auto
  then have M  $\lesssim_Q \forall i \in M. X_i \neq \emptyset \forall i \in M. X_i \subseteq \text{Pow}(Q)$  by auto
  then have M  $\lesssim_Q \forall i \in M. X_i \neq \emptyset \forall i \in M. X_i \lesssim \text{Pow}(Q)$  using subset_imp_lepoll
by auto
  then have  $(\exists f. f: \text{Pi}(M, \lambda t. X_t) \wedge (\forall t \in M. f t \in X_t))$  using reg[of MX] by
auto
  then obtain f where  $f: \text{Pi}(M, \lambda t. X_t) (!! t. t \in M \implies f t \in X_t)$  by auto
  {
    fix m
    assume S: $m \in M$ 
    from f(2) S obtain YY where  $YY: (YY \in M) (f m = \alpha YY)$  by auto
    then have  $Y: (YY \in M) \wedge (f m = \alpha YY)$  by auto
    moreover
    {
      fix U
      assume  $U \in M \wedge (f m = \alpha U)$ 
      then have  $U = YY$  using inj inj_def YY by auto
    }
    then have  $r: \bigwedge x. x \in M \wedge (f m = \alpha x) \implies x = YY$  by blast
    have  $\exists ! YY. YY \in M \wedge f m = \alpha YY$  using ex1I[of %Y.  $Y \in M \wedge f m = \alpha Y$ , OF Y r] by
auto
  }
  then have  $\text{ex1YY}: \forall m \in M. \exists ! YY. YY \in M \wedge f m = \alpha YY$  by auto
  let  $YYm = \{m, (\text{THE } YY. YY \in M \wedge f m = \alpha YY)\}. m \in M\}$ 
  have  $\text{aux}: \bigwedge m. m \in M \implies YYm = (\text{THE } YY. YY \in M \wedge f m = \alpha YY)$  unfolding apply_def
by auto
  have  $\text{ree}: \forall m \in M. (YYm) \in M \wedge f m = \alpha (YYm)$ 
  proof
    fix m
    assume C: $m \in M$ 
    then have  $\exists ! YY. YY \in M \wedge f m = \alpha YY$  using ex1YY by auto
    then have  $(\text{THE } YY. YY \in M \wedge f m = \alpha YY) \in M \wedge f m = \alpha (\text{THE } YY. YY \in M \wedge f m = \alpha YY)$ 
      using theI[of %Y.  $Y \in M \wedge f m = \alpha Y$ ] by blast
    then show  $(YYm) \in M \wedge f m = \alpha (YYm)$  apply (simp only: aux[OF C]) done
  qed
  have  $\text{tt}: \bigwedge m. m \in M \implies N(m) \subseteq YYm$ 
  proof-
    fix m
    assume D: $m \in M$ 
    then have  $QQ: m \in Q$  by auto
    from D have  $t: (YYm) \in M \wedge f m = \alpha (YYm)$  using ree by blast
    then have  $f m = \alpha (YYm)$  by blast
    then have  $(\alpha (YYm)) \in (\lambda i \in Q. \{\alpha U. U \in \{V \in M. N(i) \subseteq V\}\})m$  using f(2) [OF

```

```

D]
  by auto
  then have  $(\alpha(YYmm)) \in \{\alpha U. U \in \{V \in M. N(m) \subseteq V\}\}$  using QQ by auto
  then obtain U where  $U \in \{V \in M. N(m) \subseteq V\} \wedge \alpha(YYmm) = \alpha U$  by auto
  then have  $r: U \in MN(m) \subseteq U \wedge \alpha(YYmm) = \alpha U \wedge (YYmm) \in M$  using t by auto
  then have  $YYmm = U$  using inj_apply_equality[OF inj] by blast
  then show  $N(m) \subseteq YYmm$  using r by auto
qed
then have  $(\bigcup_{m \in M}. N(m)) \subseteq (\bigcup_{m \in M}. YYmm)$ 
proof-
{
  fix s
  assume  $s \in (\bigcup_{m \in M}. N(m))$ 
  then obtain t where  $r: t \in Ms \in N(t)$  by auto
  then have  $s \in YYmt$  using tt[OF r(1)] by blast
  then have  $s \in (\bigcup_{m \in M}. YYmm)$  using r(1) by blast
}
then show thesis by blast
qed
moreover
{
  fix x
  assume  $AT: x \in \bigcup T$ 
  with A obtain U where  $BB: U \in MU \in Tx \in U$  by auto
  then obtain j where  $BC: j \in Q \wedge N(j) \subseteq Ux \in N(j)$  using point_open_base_neigh[OF
base,of Ux] by auto
  then have  $Xj \neq 0$  using BB(1) by auto
  then have  $j \in M$  using BC(1) by auto
  then have  $x \in (\bigcup_{m \in M}. N(m))$  using BC(3) by auto
}
then have  $\bigcup T \subseteq (\bigcup_{m \in M}. N(m))$  by blast
ultimately have covers:  $\bigcup T \subseteq (\bigcup_{m \in M}. YYmm)$  using subset_trans[of  $\bigcup T (\bigcup_{m \in M}. N(m)) (\bigcup_{m \in M}. YYmm)$ ]
by auto
have relation(YYm) unfolding relation_def by auto
moreover
have f: function(YYm) unfolding function_def by auto
moreover
have d: domain(YYm) = M by auto
moreover
have r: range(YYm) = YYmM by auto
ultimately
have fun:  $YYm: M \rightarrow YYmM$  using function_imp_Pi[of YYm] by auto
have  $YYm \in \text{surj}(M, YYmM)$  using fun_is_surj[OF fun] r by auto
with surj_fun_inv[OF this subMQ Card_is_Ord[OF CC]]
have  $YYmM \lesssim M$  by auto
with ddd have  $Rw: YYmM \lesssim Q$  using lepoll_trans by blast
{
  fix m assume  $m \in M$ 

```

```

then have ⟨m,YYmm⟩∈YYm using function_apply_Pair[OF f] d by blast
then have YYmm∈YYmM by auto}
then have l1:{YYmm. m∈M}⊆YYmM by blast
{
  fix t assume t∈YYmM
  then have ∃x∈M. ⟨x,t⟩∈YYm unfolding image_def by auto
  then obtain r where S:r∈M⟨r,t⟩∈YYm by auto
  have YYmr=t using apply_equality[OF S(2) fun] by auto
  with S(1) have t∈{YYmm. m∈M} by auto
}
with l1 have {YYmm. m∈M}=YYmM by blast
with Rw have {YYmm. m∈M} ≲Q by auto
with covers have {YYmm. m∈M}∈Pow(M)∧⋃T⊆⋃{YYmm. m∈M}∧{YYmm. m∈M}
<csucc(Q) using ree
  Card_less_csucc_eq_le[OF CC] by blast
  then have ∃N∈Pow(M). ⋃T⊆⋃N∧N<csucc(Q) by auto
}
then have ∀M∈Pow(T). ⋃T⊆⋃M → (∃N∈Pow(M). ⋃T⊆⋃N ∧ N < csucc(Q))
by auto
then show thesis using IsCompactOfCard_def Card_csucc CC Card_is_Ord
by auto
qed

```

In the following proof, we have chosen an infinite cardinal to be able to apply the equation  $Q \times Q \approx Q$ . For finite cardinals; both, the assumption and the axiom of choice, are always true.

```

theorem second_imp_compact_imp_Q_choice_PowQ:
  assumes ∀T. (T{is a topology} ∧ (T{is of second type of cardinal}csucc(Q)))
  → ((⋃T){is compact of cardinal}csucc(Q){in}T)
  and InfCard(Q)
  shows {the axiom of} Q {choice holds for subsets} (Pow(Q))
proof-
{
  fix N M
  assume AS:M ≲Q ∧ (∀t∈M. Nt≠0 ∧ Nt⊆Pow(Q))
  then obtain h where h∈inj(M,Q) using lepoll_def by auto

  have discTop:Pow(Q×M) {is a topology} using Pow_is_top by auto
  {
    fix A
    assume AS:A∈Pow(Q×M)
    have A=⋃{{i}. i∈A} by auto
    with AS have ∃T∈Pow({{i}. i∈Q×M}). A=⋃T by auto
    then have A∈{⋃U. U∈Pow({{i}. i∈Q×M})} by auto
  }
  moreover
  {
    fix A
    assume AS:A∈{⋃U. U∈Pow({{i}. i∈Q×M})}

```

```

    then have A ∈ Pow(Q × M) by auto
  }
  ultimately
  have base: {{x}. x ∈ Q × M} {is a base for} Pow(Q × M) unfolding IsAbaseFor_def
by blast
  let f = {{i, {i}}. i ∈ Q × M}
  have fff: f ∈ Q × M → {{i}. i ∈ Q × M} using Pi_def function_def by auto
  then have f ∈ inj(Q × M, {{i}. i ∈ Q × M}) unfolding inj_def using apply_equality
by auto
  then have f ∈ bij(Q × M, {{i}. i ∈ Q × M}) unfolding bij_def surj_def ap-
ply safe using fff apply simp
  using apply_equality fff by auto
  then have Q × M ≈ {{i}. i ∈ Q × M} using eqpoll_def by auto
  then have {{i}. i ∈ Q × M} ≈ Q × M using eqpoll_sym by auto
  then have {{i}. i ∈ Q × M} ≲ Q × M using eqpoll_imp_lepoll by auto
  then have {{i}. i ∈ Q × M} ≲ Q × Q using AS prod_lepoll_mono[of QMQ] lepoll_refl[of
Q]
  lepoll_trans by blast
  then have {{i}. i ∈ Q × M} ≲ Q using InfCard_square_eqpoll assms(2) lepoll_eq_trans
by auto
  then have {{i}. i ∈ Q × M} < csucc(Q) using Card_less_csucc_eq_le assms(2)
InfCard_is_Card by auto
  then have Pow(Q × M) {is of second type of cardinal} csucc(Q) using
IsSecondOfCard_def base by auto
  then have comp: (Q × M) {is compact of cardinal} csucc(Q) {in} Pow(Q × M)
using discTop assms(1) by auto
  {
    fix W
    assume W ∈ Pow(Q × M)
    then have T: W {is closed in} Pow(Q × M) and (Q × M) ∩ W = W using IsClosed_def
by auto
    with compact_closed[OF comp T] have (W {is compact of cardinal} csucc(Q) {in} Pow(Q × M))
by auto
  }
  then have subCompact: ∀ W ∈ Pow(Q × M). (W {is compact of cardinal} csucc(Q) {in} Pow(Q × M))
by auto
  let cub = ⋃ {{(U) × {t}. U ∈ Nt}. t ∈ M}
  from AS have (⋃ cub) ∈ Pow((Q) × M) apply safe by auto
  with subCompact have Ncomp: ((⋃ cub) {is compact of cardinal} csucc(Q) {in} Pow(Q × M))
by auto
  have cond: (cub) ∈ Pow(Pow(Q × M)) ∧ ⋃ cub ⊆ ⋃ cub using AS by auto
  have ∃ S ∈ Pow(cub). (⋃ cub) ⊆ ⋃ S ∧ S < csucc(Q)
  proof-
  {
    have ((⋃ cub) {is compact of cardinal} csucc(Q) {in} Pow(Q × M)) us-
ing Ncomp by auto
    then have ∀ M ∈ Pow(Pow(Q × M)). ⋃ cub ⊆ ⋃ M → (∃ Na ∈ Pow(M). ⋃ cub
⊆ ⋃ Na ∧ Na < csucc(Q))
      unfolding IsCompactOfCard_def by auto

```

```

    with cond have  $\exists S \in \text{Pow}(\text{cub}). \bigcup \text{cub} \subseteq \bigcup S \wedge S \prec \text{csucc}(Q)$  by auto
  }
  then show thesis by auto
qed
  then have ttt:  $\exists S \in \text{Pow}(\text{cub}). (\bigcup \text{cub}) \subseteq \bigcup S \wedge S \lesssim Q$  using Card_less_csucc_eq_le
assms(2) InfCard_is_Card by auto
  then obtain S where S_def:  $S \in \text{Pow}(\text{cub}) (\bigcup \text{cub}) \subseteq \bigcup S \wedge S \lesssim Q$  by auto
  {
    fix t
    assume AA:  $t \in \text{MNt} \neq \{0\}$ 
    then obtain U where G:  $U \in \text{Nt}$  and notEm:  $U \neq 0$  using AS apply safe
  by blast
    then have  $U \times \{t\} \in \text{cub}$  using AA by auto
    then have  $U \times \{t\} \subseteq \bigcup \text{cub}$  by auto
    with G notEm AA have  $\exists s. \langle s, t \rangle \in \bigcup \text{cub}$  by auto
  }
  then have  $\forall t \in M. (\text{Nt} \neq \{0\}) \longrightarrow (\exists s. \langle s, t \rangle \in \bigcup \text{cub})$  by auto
  then have A:  $\forall t \in M. (\text{Nt} \neq \{0\}) \longrightarrow (\exists s. \langle s, t \rangle \in \bigcup S)$  using S_def(2) ap-
ply safe by blast
  from S_def(1) have B:  $\forall f \in S. \exists t \in M. \exists U \in \text{Nt}. f = U \times \{t\}$  by blast
  from A B have  $\forall t \in M. (\text{Nt} \neq \{0\}) \longrightarrow (\exists U \in \text{Nt}. U \times \{t\} \in S)$  by blast
  then have noEmp:  $\forall t \in M. (\text{Nt} \neq \{0\}) \longrightarrow (S \cap (\{U \times \{t\}. U \in \text{Nt}\}) \neq \emptyset)$  apply safe
  by auto
  from S_def(3) obtain r where r:  $r: \text{inj}(S, Q)$  using lepoll_def by auto
  then have bij2:  $\text{converse}(r): \text{bij}(\text{range}(r), S)$  using inj_bij_range bij_converse_bij
  by auto
  then have surj2:  $\text{converse}(r): \text{surj}(\text{range}(r), S)$  using bij_def by auto
  let R =  $\lambda t \in M. \{j \in \text{range}(r). \text{converse}(r)j \in (\{U \times \{t\}. U \in \text{Nt}\})\}$ 
  {
    fix t
    assume AA:  $t \in \text{MNt} \neq \{0\}$ 
    then have  $(S \cap (\{U \times \{t\}. U \in \text{Nt}\}) \neq \emptyset)$  using noEmp by auto
    then obtain s where ss:  $s \in S \wedge s \in \{U \times \{t\}. U \in \text{Nt}\}$  by blast
    then obtain j where converse(r)j = s j  $\in \text{range}(r)$  using surj2 unfold-
ing surj_def by blast
    then have j  $\in \{j \in \text{range}(r). \text{converse}(r)j \in (\{U \times \{t\}. U \in \text{Nt}\})\}$  using ss
  by auto
    then have Rt  $\neq 0$  using beta_if AA by auto
  }
  then have nonE:  $\forall t \in M. \text{Nt} \neq \{0\} \longrightarrow \text{Rt} \neq 0$  by auto
  {
    fix t j
    assume t  $\in M$  j  $\in \text{Rt}$ 
    then have  $\text{converse}(r)j \in \{U \times \{t\}. U \in \text{Nt}\}$  using beta_if by auto
  }
  then have pp:  $\forall t \in M. \forall j \in \text{Rt}. \text{converse}(r)j \in \{U \times \{t\}. U \in \text{Nt}\}$  by auto
  have reg:  $\forall t \in M. \forall U \in V. U \times \{t\} = V \times \{t\} \longrightarrow U = V$  apply safe
  proof
    fix t U V

```

```

    assume AA:U×{t}=V×{t}
  {
    fix v
    assume v∈V
    then have ⟨v,t⟩∈V ×{t} by auto
    then have ⟨v,t⟩∈U ×{t} using AA by auto
    then have v∈U by auto
  }
  then show V⊆U by auto
  {
    fix u
    assume u∈U
    then have ⟨u,t⟩∈U ×{t} by auto
    then have ⟨u,t⟩∈V ×{t} using AA by auto
    then have u∈V by auto
  }
  then show U⊆V by auto
qed

let E={⟨t,if Nt={0} then 0 else (THE U. converse(r)(LEAST j. j∈Rt)=U×{t})⟩.
t∈M}
have ff:function(E) unfolding function_def by auto
moreover
{
  fix t
  assume pm:t∈M
  { assume nonEE:Nt≠{0}
  {
    fix j
    assume j∈Rt
    with pm(1) have j∈range(r) using beta_if by auto
    from r have r:surj(S,range(r)) using fun_is_surj inj_def by auto
    with 'j∈range(r)' obtain d where d∈S and rd=j using surj_def
  by auto
    then have j∈Q using r inj_def by auto
  }
  then have sub:Rt⊆Q by blast
  from nonE pm nonEE obtain ee where P:ee∈Rt by blast
  with sub have ee∈Q by auto
  then have Ord(ee) using assms(2) Card_is_Ord Ord_in_Ord InfCard_is_Card
by blast
  with P have (LEAST j. j∈Rt)∈Rt using LeastI[where i=ee and P=λj.
j∈Rt] by auto
  with pp pm have converse(r)(LEAST j. j∈Rt)∈{U×{t}. U∈Nt} by auto
  then obtain W where converse(r)(LEAST j. j∈Rt)=W×{t} and s:W∈Nt
by auto
  then have (THE U. converse(r)(LEAST j. j∈Rt)=U×{t})=W using reg
by auto
  with s have (THE U. converse(r)(LEAST j. j∈Rt)=U×{t})∈Nt by auto

```

```

    }
    then have (if Nt={0} then 0 else (THE U. converse(r)(LEAST j. j∈Rt)=U×{t}))∈Nt
  by auto
  }
  ultimately have thesis1:∀t∈M. Et∈Nt using function_apply_equality
by auto
{
  fix e
  assume e∈E
  then obtain m where m∈M and e=⟨m,Em⟩ using function_apply_equality
ff by auto
  with thesis1 have e∈Sigma(M,λt. Nt) by auto
}
then have E∈Pow(Sigma(M,λt. Nt)) by auto
with ff have E∈Pi(M,λm. Nm) using Pi_iff by auto
then have (∃f. f:Pi(M,λt. Nt) ∧ (∀t∈M. ft∈Nt)) using thesis1 by
auto}
then show thesis using AxiomCardinalChoice_def assms(2) InfCard_is_Card
by auto
qed

```

The two previous results, state the following equivalence:

```

theorem Q_choice_Pow_eq_secon_imp_comp:
  assumes InfCard(Q)
  shows (∀T. (T{is a topology} ∧ (T{is of second type of cardinal}csucc(Q)))
  → ((⋃T){is compact of cardinal}csucc(Q){in}T))
  ↔ ({the axiom of} Q {choice holds for subsets} (Pow(Q)))
  using second_imp_compact_imp_Q_choice_PowQ compact_of_cardinal_Q assms
by auto

```

In the next result we will prove that if the space  $(\kappa, Pow(\kappa))$ , for  $\kappa$  an infinite cardinal, is compact of its successor cardinal; then all topological spaces which are of second type of the successor cardinal of  $\kappa$  are also compact of that cardinal.

```

theorem Q_csuccQ_comp_eq_Q_choice_Pow:
  assumes InfCard(Q) (Q){is compact of cardinal}csucc(Q){in}Pow(Q)
  shows ∀T. (T{is a topology} ∧ (T{is of second type of cardinal}csucc(Q)))
  → ((⋃T){is compact of cardinal}csucc(Q){in}T)
proof
  fix T
  {assume top:T {is a topology} and sec:T{is of second type of cardinal}csucc(Q)
  from assms have Card(csucc(Q)) Card(Q) using InfCard_is_Card Card_is_Ord
  Card_csucc by auto
  moreover
  have ⋃T⊆⋃T by auto
  moreover
  {
    fix M
    assume MT:M∈Pow(T) and cover:⋃T⊆⋃M

```

```

    from sec obtain B where B {is a base for} T B<csucc(Q) using IsSecondOfCard_def
  by auto
    with 'Card(Q)' obtain N where base:{Ni. i∈Q}{is a base for}T us-
ing Card_less_csucc_eq_le
    base_to_indexed_base by blast
    let S={⟨u,{i∈Q. Ni⊆u}⟩. u∈M}
    have function(S) unfolding function_def by auto
    then have S:M→Pow(Q) using Pi_iff by auto
    then have S∈inj(M,Pow(Q)) unfolding inj_def apply safe
    proof-
    {
      fix w x
      assume AS:w∈Mx∈M{⟨u, {i ∈ Q . N i ⊆ u}⟩ . u ∈ M} w = {⟨u, {i
∈ Q . N i ⊆ u}⟩ . u ∈ M} x
      with 'S:M→Pow(Q)' have ASS:{i ∈ Q . N i ⊆ w}={i ∈ Q . N i ⊆
x} using apply_equality by auto
      from AS(1,2) MT have w∈Tx∈T by auto
      then have w=Interior(w,T)x=Interior(x,T) using top topology0.Top_2_L3[of
T]

      topology0_def[of T] by auto
      then have UN:w=(⋃{B∈{N(i). i∈Q}. B⊆w})x=(⋃{B∈{N(i). i∈Q}. B⊆x})
      using interior_set_base_topology top base by auto
      {
        fix b
        assume b∈w
        then have b∈⋃{B∈{N(i). i∈Q}. B⊆w} using UN(1) by auto
        then obtain S where S:S∈{N(i). i∈Q} b∈S S⊆w by blast
        then obtain j where j:j∈QS=N(j) by auto
        then have j∈{i ∈ Q . N(i) ⊆ w} using S(3) by auto
        then have N(j)⊆xb∈N(j)j∈Q using S(2) ASS j by auto
        then have b∈(⋃{B∈{N(i). i∈Q}. B⊆x}) by auto
        then have b∈x using UN(2) by auto
      }
      moreover
      {
        fix b
        assume b∈x
        then have b∈⋃{B∈{N(i). i∈Q}. B⊆x} using UN(2) by auto
        then obtain S where S:S∈{N(i). i∈Q} b∈S S⊆x by blast
        then obtain j where j:j∈QS=N(j) by auto
        then have j∈{i ∈ Q . N(i) ⊆ x} using S(3) by auto
        then have j∈{i ∈ Q . N(i) ⊆ w} using ASS by auto
        then have N(j)⊆wb∈N(j)j∈Q using S(2) j(2) by auto
        then have b∈(⋃{B∈{N(i). i∈Q}. B⊆w}) by auto
        then have b∈w using UN(2) by auto
      }
      ultimately show w=x by auto
    }
  }
qed

```



```

    then have  $S \in \text{bij}(M, \text{range}(S))$  using fun_is_surj unfolding bij_def inj_def
surj_def by force
    have  $\text{range}(S) \subseteq \text{Pow}(Q)$  by auto
    then have  $\text{range}(S) \in \text{Pow}(\text{Pow}(Q))$  by auto
    moreover
    have  $(\bigcup (\text{range}(S))) \{ \text{is closed in} \} \text{Pow}(Q) \quad Q \cap (\bigcup \text{range}(S)) = (\bigcup \text{range}(S))$ 
using IsClosed_def by auto
    from this(2) compact_closed[OF assms(2) this(1)] have  $(\bigcup \text{range}(S)) \{ \text{is compact of cardinal} \} \text{csucc}(Q) \{ \text{in} \} \text{Pow}(Q)$ 
    by auto
    moreover
    have  $\bigcup (\text{range}(S)) \subseteq \bigcup (\text{range}(S))$  by auto
    ultimately have  $\exists S \in \text{Pow}(\text{range}(S)). (\bigcup (\text{range}(S))) \subseteq \bigcup S \wedge S \prec \text{csucc}(Q)$ 
using IsCompactOfCard_def by auto
    then obtain SS where SS_def:  $SS \subseteq \text{range}(S) \quad (\bigcup (\text{range}(S))) \subseteq \bigcup SS \quad SS \prec \text{csucc}(Q)$ 
by auto
    with 'S ∈ bij(M, range(S))' have con:  $\text{converse}(S) \in \text{bij}(\text{range}(S), M)$  using
bij_converse_bij by auto
    then have r1:  $\text{restrict}(\text{converse}(S), SS) \in \text{bij}(SS, \text{converse}(S)SS)$  using restrict_bij
bij_def SS_def(1) by auto
    then have rr:  $\text{converse}(\text{restrict}(\text{converse}(S), SS)) \in \text{bij}(\text{converse}(S)SS, SS)$ 
using bij_converse_bij by auto
    {
      fix x
      assume  $x \in \bigcup T$ 
      with cover have  $x \in \bigcup M$  by auto
      then obtain R where  $R \in M \quad x \in R$  by auto
      with MT have  $R \in T \quad x \in R$  by auto
      then have  $\exists V \in \{N_i. i \in Q\}. V \subseteq R \wedge x \in V$  using point_open_base_neigh base
by force
      then obtain j where  $j \in Q \quad N_j \subseteq R$  and  $x_p: x \in N_j$  by auto
      with 'R ∈ M' 'S: M → Pow(Q)' 'S ∈ bij(M, range(S))' have  $SR \in \text{range}(S) \wedge j \in SR$ 
using apply_equality
      bij_def inj_def by auto
      from exI[where P = λt. t ∈ range(S) ∧ j ∈ t, OF this] have  $\exists A \in \text{range}(S).$ 
j ∈ A unfolding Bex_def
      by auto
      then have  $j \in (\bigcup (\text{range}(S)))$  by auto
      then have  $j \in \bigcup SS$  using SS_def(2) by blast
      then obtain SR where  $SR \in SS \quad j \in SR$  by auto
      moreover
      have  $\text{converse}(\text{restrict}(\text{converse}(S), SS)) \in \text{surj}(\text{converse}(S)SS, SS)$  us-
ing rr bij_def by auto
      ultimately obtain RR where  $\text{converse}(\text{restrict}(\text{converse}(S), SS))RR = SR$ 
and p:  $RR \in \text{converse}(S)SS$  unfolding surj_def by blast
      then have  $\text{converse}(\text{converse}(\text{restrict}(\text{converse}(S), SS))) (\text{converse}(\text{restrict}(\text{converse}(S), SS))$ 
      by auto
      moreover
      have  $\text{converse}(\text{restrict}(\text{converse}(S), SS)) \in \text{inj}(\text{converse}(S)SS, SS)$  us-

```

```

ing rr unfolding bij_def by auto
  moreover
    ultimately have RR=converse(converse(restrict(converse(S),SS)))SR
using left_inverse[OF _ p]
  by force
  moreover
    with r1 have restrict(converse(S),SS)∈SS→converse(S)SS unfolding
bij_def inj_def by auto
    then have relation(restrict(converse(S),SS)) using Pi_def relation_def
by auto
    then have converse(converse(restrict(converse(S),SS)))=restrict(converse(S),SS)
using relation_converse_converse by auto
    ultimately have RR=restrict(converse(S),SS)SR by auto
    with 'SR∈SS' have eq:RR=converse(S)SR unfolding restrict by auto
    then have converse(converse(S))RR=converse(converse(S))(converse(S)SR)
by auto
    moreover
      with 'SR∈SS' have SR∈range(S) using SS_def(1) by auto
      from con left_inverse[OF _ this] have converse(converse(S))(converse(S)SR)=SR
unfolding bij_def
      by auto
      ultimately have converse(converse(S))RR=SR by auto
      then have SRR=SR using relation_converse_converse[of S] unfolding
relation_def by auto
    moreover
      have converse(S):range(S)→M using con bij_def inj_def by auto
      with 'SR∈range(S)' have converse(S)SR∈M using apply_funtype
      by auto
      with eq have RR∈M by auto
      ultimately have SR={i∈Q. Ni⊆RR} using 'S:M→Pow(Q)' apply_equality
by auto
    then have Nj⊆RR using 'j∈SR' by auto
    with x_p have x∈RR by auto
    with p have x∈⋃(converse(S)SS) by auto
  }
  then have ⋃T⊆⋃(converse(S)SS) by blast
  moreover
    {from con have converse(S)SS={converse(S)R. R∈SS} using image_function[of
converse(S) SS]
      SS_def(1) unfolding range_def bij_def inj_def Pi_def by auto
      have {converse(S)R. R∈SS}⊆{converse(S)R. R∈range(S)} using SS_def(1)
by auto
    }
    moreover
      have converse(S):range(S)→M using con unfolding bij_def inj_def by
auto
      then have {converse(S)R. R∈range(S)}⊆M using apply_funtype by force
      ultimately
        have (converse(S)SS)⊆M by auto
      }

```

```

    then have converse(S)SS∈Pow(M) by auto
    moreover
    with rr have converse(S)SS≈SS using eqpoll_def by auto
    then have converse(S)SS<csucc(Q) using SS_def(3) eq_lesspoll_trans
  by auto
    ultimately
    have ∃N∈Pow(M).  $\bigcup T \subseteq \bigcup N \wedge N < \text{csucc}(Q)$  by auto
  }
  then have  $\forall M \in \text{Pow}(T). \bigcup T \subseteq \bigcup M \longrightarrow (\exists N \in \text{Pow}(M). \bigcup T \subseteq \bigcup N \wedge N < \text{csucc}(Q))$ 
  by auto
    ultimately have  $(\bigcup T) \{\text{is compact of cardinal}\} \text{csucc}(Q) \{\text{in}\} T$  unfolding
  IsCompactOfCard_def
    by auto
  then show  $(T \{\text{is a topology}\}) \wedge (T \{\text{is of second type of cardinal}\} \text{csucc}(Q))$ 
 $\longrightarrow ((\bigcup T) \{\text{is compact of cardinal}\} \text{csucc}(Q) \{\text{in}\} T)$ 
    by auto
  qed

theorem Q_disc_is_second_card_csuccQ:
  assumes InfCard(Q)
  shows  $\text{Pow}(Q) \{\text{is of second type of cardinal}\} \text{csucc}(Q)$ 
proof-
  {
    fix A
    assume AS:A∈Pow(Q)
    have  $A = \bigcup \{\{i\}. i \in A\}$  by auto
    with AS have  $\exists T \in \text{Pow}(\{\{i\}. i \in Q\}). A = \bigcup T$  by auto
    then have  $A \in \{\bigcup U. U \in \text{Pow}(\{\{i\}. i \in Q\})\}$  by auto
  }
  moreover
  {
    fix A
    assume AS:A∈ $\{\bigcup U. U \in \text{Pow}(\{\{i\}. i \in Q\})\}$ 
    then have A∈Pow(Q) by auto
  }
  ultimately
  have base: $\{\{x\}. x \in Q\} \{\text{is a base for}\} \text{Pow}(Q)$  unfolding IsAbaseFor_def
  by blast
  let f= $\langle i, \{i\} \rangle. i \in Q$ 
  have  $f \in Q \rightarrow \{\{x\}. x \in Q\}$  unfolding Pi_def function_def by auto
  then have  $f \in \text{inj}(Q, \{\{x\}. x \in Q\})$  unfolding inj_def using apply_equality
  by auto
  moreover
  from ' $f \in Q \rightarrow \{\{x\}. x \in Q\}$ ' have  $f \in \text{surj}(Q, \{\{x\}. x \in Q\})$  unfolding surj_def
  using apply_equality
  by auto
  ultimately have  $f \in \text{bij}(Q, \{\{x\}. x \in Q\})$  unfolding bij_def by auto
  then have  $Q \approx \{\{x\}. x \in Q\}$  using eqpoll_def by auto
  then have  $\{\{x\}. x \in Q\} \approx Q$  using eqpoll_sym by auto

```

```

    then have  $\{\{x\}. x \in Q\} \lesssim Q$  using eqpoll_imp_lepoll by auto
    then have  $\{\{x\}. x \in Q\} \prec \text{csucc}(Q)$  using Card_less_csucc_eq_le assms InfCard_is_Card
  by auto
  with base show thesis using IsSecondOfCard_def by auto
qed

```

This previous results give us another equivalence of the axiom of  $Q$  choice that is apparently weaker (easier to check) to the previous one.

```

theorem Q_disc_comp_csuccQ_eq_Q_choice_csuccQ:
  assumes InfCard(Q)
  shows  $(Q\{\text{is compact of cardinal}\}\text{csucc}(Q)\{\text{in}\}(\text{Pow}(Q))) \longleftrightarrow (\{\text{the axiom of}\}Q\{\text{choice holds for subsets}\}(\text{Pow}(Q)))$ 
  apply safe using Q_choice_Pow_eq_secon_imp_comp[OF assms] Q_csuccQ_comp_eq_Q_choice_Pow[OF assms]
  apply blast using Q_disc_is_second_card_csuccQ[OF assms] Q_choice_Pow_eq_secon_imp_comp[OF assms] Pow_is_top[of Q]
  by force

```

end

## 51 Topology\_ZF\_5.thy

```
theory Topology_ZF_5 imports Topology_ZF_examples Topology_ZF_properties
func1 Topology_ZF_examples_1 Topology_ZF_4
begin
```

### 51.1 Some results for separation axioms

First we will give a global characterization of  $T_1$ -spaces; which is interesting because it involves the cardinal  $\aleph_1$ .

```
lemma (in topology0) T1_cocardinal_coarser:
  shows (T {is T1})  $\longleftrightarrow$  (Cofinite ( $\bigcup T$ ))  $\subseteq$  T unfolding Cofinite_def
proof
  {
    assume AS:T {is T1}
    {
      fix x assume p:x $\in\bigcup T$ 
      {
        fix y assume y $\in(\bigcup T)-\{x\}$ 
        with AS p obtain U where U $\in T$  y $\in U$  x $\notin U$  using isT1_def by blast
        then have U $\in T$  y $\in U$  U $\subseteq(\bigcup T)-\{x\}$  by auto
        then have  $\exists U\in T. y\in U \wedge U\subseteq(\bigcup T)-\{x\}$  by auto
      }
      then have  $\forall y\in(\bigcup T)-\{x\}. \exists U\in T. y\in U \wedge U\subseteq(\bigcup T)-\{x\}$  by auto
      then have  $\bigcup T-\{x\}\in T$  using open_neigh_open by auto
      with p have {x} {is closed in} T using IsClosed_def by auto
    }
    then have pointCl: $\forall x\in\bigcup T. \{x\}$  {is closed in} T by auto
    {
      fix A
      assume AS2:A $\in\text{FinPow}(\bigcup T)$ 
      let p= $\langle x, \{x\} \rangle. x\in A$ 
      have p $\in A\rightarrow\{\{x\}. x\in A\}$  using Pi_def unfolding function_def by auto
      then have p:bij(A,  $\{\{x\}. x\in A\}$ ) unfolding bij_def inj_def surj_def
    using apply_equality
      by auto
      then have A $\approx\{\{x\}. x\in A\}$  unfolding eqpoll_def by auto
      with AS2 have Finite( $\{\{x\}. x\in A\}$ ) unfolding FinPow_def using eqpoll_imp_Finite_iff
    by auto
      then have  $\{\{x\}. x\in A\}\in\text{FinPow}(\{D\in\text{Pow}(\bigcup T) . D \text{ {is closed in} } T\})$ 
    using AS2 pointCl unfolding FinPow_def
      by (safe, blast+)
      then have  $(\bigcup\{\{x\}. x\in A\})$  {is closed in} T using fin_union_cl_is_cl
    by auto
      moreover
      have  $\bigcup\{\{x\}. x\in A\}=A$  by auto
      ultimately have A {is closed in} T by simp
    }
  }
  then have reg: $\forall A\in\text{FinPow}(\bigcup T). A$  {is closed in} T by auto
```

```

    {
      fix U
      assume AS2:U∈(CoCardinal (⋃T) nat)
      then have U∈Pow(⋃T) U=0 ∨ ((⋃T)-U)≺nat using Cocardinal_def by
    auto
      then have U∈Pow(⋃T) U=0 ∨ Finite(⋃T-U) using lesspoll_nat_is_Finite
    by auto
      then have U∈Pow(⋃T) U∈TV(⋃T-U) {is closed in} T using empty_open
    topSpaceAssum
      reg unfolding FinPow_def by auto
      then have U∈Pow(⋃T) U∈TV(⋃T-(⋃T-U))∈T using IsClosed_def by
    auto
      moreover
      then have (⋃T-(⋃T-U))=U by blast
      ultimately have U∈T by auto
    }
    then show (CoCardinal (⋃T) nat)⊆T by auto
  }
  {
    assume AS:(CoCardinal (⋃T) nat)⊆T
    {
      fix x y
      assume AS2:x∈⋃T y∈⋃Tx≠y
      have Finite({y}) by auto
      then obtain n where {y}≈n n∈nat using Finite_def by auto
      then have {y}≺nat using n_lesspoll_nat eq_lesspoll_trans by auto
      then have {y} {is closed in} (CoCardinal (⋃T) nat) using closed_sets_cocardinal
        AS2(2) by auto
      then have (⋃T)-{y}∈(CoCardinal (⋃T) nat) using union_cocardinal
    IsClosed_def by auto
      with AS have (⋃T)-{y}∈T by auto
      moreover
      with AS2(1,3) have x∈((⋃T)-{y}) ∧ y∉((⋃T)-{y}) by auto
      ultimately have ∃V∈T. x∈V∧y∉V by (safe,auto)
    }
    then show T {is T1} using isT1_def by auto
  }
}
qed

```

Secondly, let's show that the CoCardinal X Q topologies for different sets Q are all ordered as the as the partial order of sets. (The order is linear when considering only cardinals)

```

lemma order_cocardinal_top:
  fixes X
  assumes Q1≲Q2
  shows (CoCardinal X Q1)⊆(CoCardinal X Q2)
proof
  fix x
  assume x∈(CoCardinal X Q1)

```

```

then have  $x \in \text{Pow}(X)$   $x = 0 \vee (X - x) \prec Q1$  using Cocardinal_def by auto
with assms have  $x \in \text{Pow}(X)$   $x = 0 \vee (X - x) \prec Q2$  using lesspoll_trans2 by auto
then show  $x \in (\text{CoCardinal } X \text{ } Q2)$  using Cocardinal_def by auto
qed

```

corollary cocardinal\_is\_T1:

```

fixes X
assumes InfCard(K)
shows  $(\text{CoCardinal } X \text{ } K) \{ \text{is } T_1 \}$ 
proof-
  have  $\text{nat} \leq K$  using InfCard_def assms by auto
  then have  $\text{nat} \subseteq K$  using le_imp_subset by auto
  then have  $\text{nat} \lesssim K$   $K \neq 0$  using subset_imp_lepoll by auto
  then have  $(\text{CoCardinal } X \text{ } \text{nat}) \subseteq (\text{CoCardinal } X \text{ } K) \cup (\text{CoCardinal } X \text{ } K) = X$ 
using order_cocardinal_top
  union_cocardinal by auto
  then show thesis using topology0.T1_cocardinal_coarser[OF topology0_CoCardinal[OF
assms]] Cofinite_def
  by auto
qed

```

In  $T_2$ -spaces, filters and nets have at most one limit point.

lemma (in topology0) T2\_imp\_unique\_limit\_filter:

```

assumes T {is  $T_2$ }  $\mathcal{F}$  {is a filter on}  $\bigcup T$   $\mathcal{F} \rightarrow F$   $x \in \mathcal{F} \rightarrow F$   $y$ 
shows  $x = y$ 
proof-
  {
    assume  $x \neq y$ 
    from assms(3,4) have  $x \in \bigcup T$   $y \in \bigcup T$  using FilterConverges_def[OF assms(2)]
    by auto
    with 'x ≠ y' have  $\exists U \in T. \exists V \in T. x \in U \wedge y \in V \wedge U \cap V = 0$  using assms(1) isT2_def
  by auto
    then obtain U V where  $x \in U$   $y \in V$   $U \cap V = 0$   $U \in T$   $V \in T$  by auto
    then have  $U \in \{A \in \text{Pow}(\bigcup T). x \in \text{Interior}(A, T)\}$   $V \in \{A \in \text{Pow}(\bigcup T). y \in \text{Interior}(A, T)\}$ 
using Top_2_L3 by auto
    then have  $U \in \mathcal{F}$   $V \in \mathcal{F}$  using FilterConverges_def[OF assms(2)] assms(3,4)
    by auto
    then have  $U \cap V \in \mathcal{F}$  using IsFilter_def assms(2) by auto
    with 'U ∩ V = 0' have  $0 \in \mathcal{F}$  by auto
    then have False using IsFilter_def assms(2) by auto
  }
  then show thesis by auto
qed

```

lemma (in topology0) T2\_imp\_unique\_limit\_net:

```

assumes T {is  $T_2$ } N {is a net on}  $\bigcup T$   $N \rightarrow N$   $x \in N \rightarrow N$   $y$ 
shows  $x = y$ 
proof-
  have  $(\text{Filter } N..(\bigcup T)) \{ \text{is a filter on} \} (\bigcup T)$   $(\text{Filter } N..(\bigcup T)) \rightarrow F$ 

```

```

x (Filter N..( $\bigcup T$ ))  $\rightarrow_F$  y
  using filter_of_net_is_filter(1)[OF assms(2)] net_conver_filter_of_net_conver[OF
assms(2)]
  assms(3,4) by auto
  with assms(1) show thesis using T2_imp_unique_limit_filter by auto
qed

```

In fact,  $T_2$ -spaces are characterized by this property. For this proof we build a filter containing the union of two filters.

```

lemma (in topology0) unique_limit_filter_imp_T2:
  assumes  $\forall x \in \bigcup T. \forall y \in \bigcup T. \forall \mathcal{F}. ((\mathcal{F} \text{ is a filter on } \bigcup T) \wedge (\mathcal{F} \rightarrow_F x) \wedge (\mathcal{F} \rightarrow_F y)) \rightarrow x=y$ 
  shows  $T \text{ is } T_2$ 
proof-
{
  fix x y
  assume  $x \in \bigcup T \ y \in \bigcup T \ x \neq y$ 
  {
    assume  $\forall U \in T. \forall V \in T. (x \in U \wedge y \in V) \rightarrow U \cap V \neq \emptyset$ 
    let  $U_x = \{A \in \text{Pow}(\bigcup T). x \in \text{int}(A)\}$ 
    let  $U_y = \{A \in \text{Pow}(\bigcup T). y \in \text{int}(A)\}$ 
    let  $FF = U_x \cup U_y \cup \{A \cap B. \langle A, B \rangle \in U_x \times U_y\}$ 
    have sat:FF {satisfies the filter base condition}
    proof-
    {
      fix A B
      assume  $A \in FF \ B \in FF$ 
      {
        assume  $A \in U_x$ 
        {
          assume  $B \in U_x$ 
          with 'x  $\in \bigcup T$ ' 'A  $\in U_x$ ' have  $A \cap B \in U_x$  using neigh_filter(1)
IsFilter_def by auto
          then have  $A \cap B \in FF$  by auto
        }
        moreover
        {
          assume  $B \in U_y$ 
          with 'A  $\in U_x$ ' have  $A \cap B \in FF$  by auto
        }
        moreover
        {
          assume  $B \in \{A \cap B. \langle A, B \rangle \in U_x \times U_y\}$ 
          then obtain AA BB where  $B = AA \cap BB \ AA \in U_x \ BB \in U_y$  by auto
          with 'x  $\in \bigcup T$ ' 'A  $\in U_x$ ' have  $A \cap B = (A \cap AA) \cap BB \ A \cap AA \in U_x$  using neigh_filter(1)
IsFilter_def by auto
          with 'BB  $\in U_y$ ' have  $A \cap B \in \{A \cap B. \langle A, B \rangle \in U_x \times U_y\}$  by auto
          then have  $A \cap B \in FF$  by auto
        }
      }
    }
  }
}

```



```

      ultimately have  $A \cap B \in FF$  using 'B  $\in FF$ ' by auto
    }
  moreover
  {
    assume  $A \in U_y$ 
    {
      assume  $B \in U_y$ 
      with 'y  $\in \bigcup T$ ' 'A  $\in U_y$ ' have  $A \cap B \in U_y$  using neigh_filter(1)
IsFilter_def by auto
      then have  $A \cap B \in FF$  by auto
    }
  moreover
  {
    assume  $B \in U_x$ 
    with 'A  $\in U_y$ ' have  $B \cap A \in FF$  by auto
    moreover have  $A \cap B = B \cap A$  by auto
    ultimately have  $A \cap B \in FF$  by auto
  }
  moreover
  {
    assume  $B \in \{A \cap B. \langle A, B \rangle \in U_x \times U_y\}$ 
    then obtain AA BB where  $B = A \cap BB$   $AA \in U_x$   $BB \in U_y$  by auto
    with 'y  $\in \bigcup T$ ' 'A  $\in U_y$ ' have  $A \cap B = A \cap (A \cap BB)$   $A \cap BB \in U_y$  using neigh_filter(1)
IsFilter_def by auto
    with 'AA  $\in U_x$ ' have  $A \cap B \in \{A \cap B. \langle A, B \rangle \in U_x \times U_y\}$  by auto
    then have  $A \cap B \in FF$  by auto
  }
  ultimately have  $A \cap B \in FF$  using 'B  $\in FF$ ' by auto
}
moreover
{
  assume  $A \in \{A \cap B. \langle A, B \rangle \in U_x \times U_y\}$ 
  then obtain AA BB where  $A = A \cap BB$   $AA \in U_x$   $BB \in U_y$  by auto
  {
    assume  $B \in U_y$ 
    with 'BB  $\in U_y$ ' 'y  $\in \bigcup T$ ' have  $B \cap BB \in U_y$  using neigh_filter(1)
IsFilter_def by auto
    moreover from 'A = A  $\cap BB$ ' have  $A \cap B = A \cap (B \cap BB)$  by auto
    ultimately have  $A \cap B \in FF$  using 'AA  $\in U_x$ ' 'B  $\cap BB \in U_y$ ' by auto
  }
  moreover
  {
    assume  $B \in U_x$ 
    with 'AA  $\in U_x$ ' 'x  $\in \bigcup T$ ' have  $B \cap AA \in U_x$  using neigh_filter(1)
IsFilter_def by auto
    moreover from 'A = A  $\cap BB$ ' have  $A \cap B = (B \cap AA) \cap BB$  by auto
    ultimately have  $A \cap B \in FF$  using 'B  $\cap AA \in U_x$ ' 'BB  $\in U_y$ ' by auto
  }
  moreover

```

```

      {
        assume  $B \in \{A \cap B. \langle A, B \rangle \in U_x \times U_y\}$ 
        then obtain AA2 BB2 where  $B = AA2 \cap BB2$   $AA2 \in U_x$   $BB2 \in U_y$  by auto
        from 'B=AA2∩BB2' 'A=AA∩BB' have  $A \cap B = (AA \cap AA2) \cap (BB \cap BB2)$ 
by auto
        moreover
        from 'AA∈Ux' 'AA2∈Ux' 'x∈⋃T' have  $AA \cap AA2 \in U_x$  using neigh_filter(1)
IsFilter_def by auto
        moreover
        from 'BB∈Uy' 'BB2∈Uy' 'y∈⋃T' have  $BB \cap BB2 \in U_y$  using neigh_filter(1)
IsFilter_def by auto
        ultimately have  $A \cap B \in FF$  by auto
      }
      ultimately have  $A \cap B \in FF$  using 'B∈FF' by auto
    }
    ultimately have  $A \cap B \in FF$  using 'A∈FF' by auto
    then have  $\exists D \in FF. D \subseteq A \cap B$  unfolding Bex_def by auto
  }
  then have  $\forall A \in FF. \forall B \in FF. \exists D \in FF. D \subseteq A \cap B$  by force
  moreover
  have  $\bigcup T \in U_x$  using 'x∈⋃T' neigh_filter(1) IsFilter_def by auto
  then have  $FF \neq 0$  by auto
  moreover
  {
    assume  $0 \in FF$ 
    moreover
    have  $0 \notin U_x$  using 'x∈⋃T' neigh_filter(1) IsFilter_def by auto
    moreover
    have  $0 \notin U_y$  using 'y∈⋃T' neigh_filter(1) IsFilter_def by auto
    ultimately have  $0 \in \{A \cap B. \langle A, B \rangle \in U_x \times U_y\}$  by auto
    then obtain A B where  $0 = A \cap B$   $A \in U_x$   $B \in U_y$  by auto
    then have  $x \in \text{int}(A) y \in \text{int}(B)$  by auto
    moreover
    with '0=A∩B' have  $\text{int}(A) \cap \text{int}(B) = 0$  using Top_2_L1 by auto
    moreover
    have  $\text{int}(A) \in T$   $\text{int}(B) \in T$  using Top_2_L2 by auto
    ultimately have False using '∀U∈T. ∀V∈T.  $x \in U \wedge y \in V \longrightarrow U \cap V \neq 0$ '
by auto
  }
  then have  $0 \notin FF$  by auto
  ultimately show thesis using SatisfiesFilterBase_def by auto
qed
moreover
have  $FF \subseteq \text{Pow}(\bigcup T)$  by auto
ultimately have  $\text{bas}: FF \{ \text{is a base filter} \} \{ A \in \text{Pow}(\bigcup T). \exists D \in FF. D \subseteq A \}$ 
 $\bigcup \{ A \in \text{Pow}(\bigcup T). \exists D \in FF. D \subseteq A \} = \bigcup T$  using base_unique_filter_set2[of FF] by
auto
then have  $\text{fil}: \{ A \in \text{Pow}(\bigcup T). \exists D \in FF. D \subseteq A \} \{ \text{is a filter on} \} \bigcup T$  us-
ing basic_filter sat by auto

```

```

      have  $\forall U \in \text{Pow}(\bigcup T). x \in \text{int}(U) \longrightarrow (\exists D \in \text{FF}. D \subseteq U)$  by auto
      then have  $\{A \in \text{Pow}(\bigcup T). \exists D \in \text{FF}. D \subseteq A\} \rightarrow F x$  using convergence_filter_base2[OF
fil bas(1) _ 'x $\in \bigcup T$ '] by auto
      moreover
      then have  $\forall U \in \text{Pow}(\bigcup T). y \in \text{int}(U) \longrightarrow (\exists D \in \text{FF}. D \subseteq U)$  by auto
      then have  $\{A \in \text{Pow}(\bigcup T). \exists D \in \text{FF}. D \subseteq A\} \rightarrow F y$  using convergence_filter_base2[OF
fil bas(1) _ 'y $\in \bigcup T$ '] by auto
      ultimately have  $x=y$  using assms fil 'x $\in \bigcup T$ ' 'y $\in \bigcup T$ ' by blast
      with 'x $\neq y$ ' have False by auto
    }
    then have  $\exists U \in T. \exists V \in T. x \in U \wedge y \in V \wedge U \cap V = \emptyset$  by blast
  }
  then show thesis using isT2_def by auto
qed

```

```

lemma (in topology0) unique_limit_net_imp_T2:
  assumes  $\forall x \in \bigcup T. \forall y \in \bigcup T. \forall N. ((N \text{ is a net on } \bigcup T) \wedge (N \rightarrow N x) \wedge (N \rightarrow N y)) \longrightarrow x=y$ 
  shows  $T \text{ is } T_2$ 
proof-
  {
    fix x y  $\mathcal{F}$ 
    assume  $x \in \bigcup T \ y \in \bigcup T \ \mathcal{F} \text{ is a filter on } \bigcup T \ \mathcal{F} \rightarrow F x \ \mathcal{F} \rightarrow F y$ 
    then have  $(\text{Net}(\mathcal{F})) \text{ is a net on } \bigcup T \ (\text{Net } \mathcal{F}) \rightarrow N x \ (\text{Net } \mathcal{F}) \rightarrow N y$ 
      using filter_conver_net_of_filter_conver net_of_filter_is_net by
auto
    with 'x $\in \bigcup T$ ' 'y $\in \bigcup T$ ' have  $x=y$  using assms by blast
  }
  then have  $\forall x \in \bigcup T. \forall y \in \bigcup T. \forall \mathcal{F}. ((\mathcal{F} \text{ is a filter on } \bigcup T) \wedge (\mathcal{F} \rightarrow F x) \wedge (\mathcal{F} \rightarrow F y)) \longrightarrow x=y$  by auto
  then show thesis using unique_limit_filter_imp_T2 by auto
qed

```

This results make easy to check if a space is  $T_2$ .

The topology which comes from a filter as in  $\mathcal{F} \text{ is a filter on } \bigcup \mathcal{F} \implies (\mathcal{F} \cup \{0\}) \text{ is a topology}$  is not  $T_2$  generally. We will see in this file later on, that the exceptions are a consequence of the spectrum.

```

corollary filter_T2_imp_card1:
  assumes  $(\mathcal{F} \cup \{0\}) \text{ is } T_2 \ \mathcal{F} \text{ is a filter on } \bigcup \mathcal{F} \ x \in \bigcup \mathcal{F}$ 
  shows  $\bigcup \mathcal{F} = \{x\}$ 
proof-
  {
    fix y assume  $y \in \bigcup \mathcal{F}$ 
    then have  $\mathcal{F} \rightarrow F y \ \{in\} \ (\mathcal{F} \cup \{0\})$  using lim_filter_top_of_filter assms(2)
  by auto
    moreover
    have  $\mathcal{F} \rightarrow F x \ \{in\} \ (\mathcal{F} \cup \{0\})$  using lim_filter_top_of_filter assms(2,3)
  by auto

```

```

    moreover
    have  $\bigcup \mathcal{F} = \bigcup (\mathcal{F} \cup \{0\})$  by auto
    ultimately
    have  $y=x$  using topology0.T2_imp_unique_limit_filter[OF topology0_filter[OF
    assms(2)] assms(1)] assms(2)
    by auto
  }
  then have  $\bigcup \mathcal{F} \subseteq \{x\}$  by auto
  with assms(3) show thesis by auto
qed

```

There are more separation axioms that just  $T_0$ ,  $T_1$  or  $T_2$

**definition**

```

  IsRegular (_{is regular} 90)
  where  $T\{is\ regular\} \equiv \forall A. A\{is\ closed\ in\}T \longrightarrow (\forall x \in \bigcup T - A. \exists U \in T. \exists V \in T. A \subseteq U \wedge x \in V \wedge U \cap V = \emptyset)$ 

```

**definition**

```

  isT3 (_{is T3} 90)
  where  $T\{is\ T_3\} \equiv (T\{is\ T_1\}) \wedge (T\{is\ regular\})$ 

```

**definition**

```

  IsNormal (_{is normal} 90)
  where  $T\{is\ normal\} \equiv \forall A. A\{is\ closed\ in\}T \longrightarrow (\forall B. B\{is\ closed\ in\}T \wedge A \cap B = \emptyset \longrightarrow (\exists U \in T. \exists V \in T. A \subseteq U \wedge B \subseteq V \wedge U \cap V = \emptyset))$ 

```

**definition**

```

  isT4 (_{is T4} 90)
  where  $T\{is\ T_4\} \equiv (T\{is\ T_1\}) \wedge (T\{is\ normal\})$ 

```

**lemma** (in topology0) T4\_is\_T3:

assumes  $T\{is\ T_4\}$  shows  $T\{is\ T_3\}$

**proof-**

```

  from assms have nor: $T\{is\ normal\}$  using isT4_def by auto
  from assms have T1: $T\{is\ T_1\}$  using isT4_def by auto
  then have Cofinite  $(\bigcup T) \subseteq T$  using T1_cocardinal_coarser by auto
  {
    fix A
    assume AS: $A\{is\ closed\ in\}T$ 
    {
      fix x
      assume  $x \in \bigcup T - A$ 
      have Finite $(\{x\})$  by auto
      then obtain n where  $\{x\} \approx_n n \in \mathbb{N}$  unfolding Finite_def by auto
      then have  $\{x\} \lesssim_n n \in \mathbb{N}$  using eqpoll_imp_lepoll by auto
      then have  $\{x\} \prec_{\mathbb{N}}$  using n_lesspoll_nat lesspoll_trans1 by auto
      with ' $x \in \bigcup T - A$ ' have  $\{x\} \{is\ closed\ in\} (Cofinite (\bigcup T))$  using Cofinite_def
    }
  }

```

```

      closed_sets_cocardinal by auto
      then have  $\bigcup T - \{x\} \in \text{Cofinite}(\bigcup T)$  unfolding IsClosed_def using union_cocardinal
Cofinite_def
      by auto
      with 'Cofinite  $(\bigcup T) \subseteq T$ ' have  $\bigcup T - \{x\} \in T$  by auto
      with ' $x \in \bigcup T - A$ ' have  $\{x\} \{ \text{is closed in} \} T \wedge \{x\} = 0$  using IsClosed_def
by auto
      with nor AS have  $\exists U \in T. \exists V \in T. A \subseteq U \wedge \{x\} \subseteq V \wedge U \cap V = 0$  unfolding IsNormal_def
by blast
      then have  $\exists U \in T. \exists V \in T. A \subseteq U \wedge x \in V \wedge U \cap V = 0$  by auto
    }
    then have  $\forall x \in \bigcup T - A. \exists U \in T. \exists V \in T. A \subseteq U \wedge x \in V \wedge U \cap V = 0$  by auto
  }
  then have T {is regular} using IsRegular_def by blast
  with 'T {is T1}' show thesis using isT3_def by auto
qed

```

lemma (in topology0) T3\_is\_T2:

assumes T {is T<sub>3</sub>} shows T {is T<sub>2</sub>}

proof-

```

from assms have T {is regular} using isT3_def by auto
from assms have T {is T1} using isT3_def by auto
then have Cofinite  $(\bigcup T) \subseteq T$  using T1_cocardinal_coarser by auto
{

```

```

  fix x y
  assume  $x \in \bigcup T \wedge y \in \bigcup T \wedge x \neq y$ 
  have Finite( $\{x\}$ ) by auto
  then obtain n where  $\{x\} \approx n$   $n \in \text{nat}$  unfolding Finite_def by auto
  then have  $\{x\} \lesssim n$   $n \in \text{nat}$  using eqpoll_imp_lepoll by auto
  then have  $\{x\} < \text{nat}$  using n_lesspoll_nat lesspoll_trans1 by auto
  with ' $x \in \bigcup T$ ' have  $\{x\} \{ \text{is closed in} \} (\text{Cofinite } (\bigcup T))$  using Cofinite_def

```

```

      closed_sets_cocardinal by auto
      then have  $\bigcup T - \{x\} \in \text{Cofinite}(\bigcup T)$  unfolding IsClosed_def using union_cocardinal
Cofinite_def
      by auto
      with 'Cofinite  $(\bigcup T) \subseteq T$ ' have  $\bigcup T - \{x\} \in T$  by auto
      with ' $x \in \bigcup T$ ' ' $y \in \bigcup T$ ' ' $x \neq y$ ' have  $\{x\} \{ \text{is closed in} \} T \wedge y \in \bigcup T - \{x\}$  using
IsClosed_def by auto
      with 'T {is regular}' have  $\exists U \in T. \exists V \in T. \{x\} \subseteq U \wedge y \in V \wedge U \cap V = 0$  unfolding
IsRegular_def by force
      then have  $\exists U \in T. \exists V \in T. x \in U \wedge y \in V \wedge U \cap V = 0$  by auto
    }
  then show thesis using isT2_def by auto
qed

```

### 51.1.1 Hereditability

A topological property is hereditary if whenever a space has it, every subspace also has it.

**definition** IsHer ( $\_is\ hereditary$ ) 90)  
 where  $P\ \{is\ hereditary\} \equiv \forall T. T\{is\ a\ topology\} \wedge P(T) \longrightarrow (\forall A \in Pow(\bigcup T). P(T\{restricted\ to\}A))$

**lemma** subspace\_of\_subspace:  
 assumes  $A \subseteq B \subseteq \bigcup T$   
 shows  $T\{restricted\ to\}A = (T\{restricted\ to\}B)\{restricted\ to\}A$   
**proof**  
 from assms have  $S: \forall S \in T. A \cap (B \cap S) = A \cap S$  by auto  
 then show  $T\ \{restricted\ to\} A \subseteq T\ \{restricted\ to\} B\ \{restricted\ to\} A$   
 A unfolding RestrictedTo\_def  
 by auto  
 from S show  $T\ \{restricted\ to\} B\ \{restricted\ to\} A \subseteq T\ \{restricted\ to\} A$   
 to} A unfolding RestrictedTo\_def  
 by auto  
**qed**

The separation properties  $T_0$ ,  $T_1$ ,  $T_2$  y  $T_3$  are hereditary.

**theorem** regular\_here:  
 assumes  $T\{is\ regular\}$   $A \in Pow(\bigcup T)$  shows  $(T\{restricted\ to\}A)\{is\ regular\}$   
**proof-**  
 {  
 fix C  
 assume  $A: C\{is\ closed\ in\}(T\{restricted\ to\}A)$   
 {fix y assume  $y \in \bigcup (T\{restricted\ to\}A) \ y \notin C$   
 with A have  $(\bigcup (T\{restricted\ to\}A)) - C \in (T\{restricted\ to\}A) C \subseteq \bigcup (T\{restricted\ to\}A) \ y \in \bigcup (T\{restricted\ to\}A) \ y \notin C$  unfolding IsClosed\_def  
 by auto  
 moreover  
 with assms(2) have  $\bigcup (T\{restricted\ to\}A) = A$  unfolding RestrictedTo\_def  
 by auto  
 ultimately have  $A - C \in T\{restricted\ to\}A \ y \in A \ y \notin C C \in Pow(A)$  by auto  
 then obtain S where  $S \in T \ A \cap S = A - C \ y \in A \ y \notin C$  unfolding RestrictedTo\_def  
 by auto  
 then have  $y \in A - C \ A \cap S = A - C$  by auto  
 with 'C ∈ Pow(A)' have  $y \in A \cap S C = A \cap S$  by auto  
 then have  $y \in S \ C = A - S$  by auto  
 with assms(2) have  $y \in S \ C \subseteq \bigcup T - S$  by auto  
 moreover  
 from 'S ∈ T' have  $\bigcup T - (\bigcup T - S) = S$  by auto  
 moreover  
 with 'S ∈ T' have  $(\bigcup T - S)\ \{is\ closed\ in\}T$  using IsClosed\_def by auto  
 ultimately have  $y \in \bigcup T - (\bigcup T - S) \ (\bigcup T - S)\ \{is\ closed\ in\}T$  by auto  
 with assms(1) have  $\forall y \in \bigcup T - (\bigcup T - S). \exists U \in T. \exists V \in T. (\bigcup T - S) \subseteq U \wedge y \in V \wedge U \cap V = \emptyset$   
 unfolding IsRegular\_def by auto

```

with 'y ∈ ⋃ T - (⋃ T - S)' have ∃ U ∈ T. ∃ V ∈ T. (⋃ T - S) ⊆ U ∧ y ∈ V ∧ U ∩ V = 0 by auto
then obtain U V where U ∈ T ∧ V ∈ T ∧ ⋃ T - S ⊆ U ∧ y ∈ V ∧ U ∩ V = 0 by auto
then have A ∩ U ∈ (T {restricted to} A) ∧ A ∩ V ∈ (T {restricted to} A) C ⊆ U ∧ y ∈ V ∧ (A ∩ U) ∩ (A ∩ V) = 0
  unfolding RestrictedTo_def using 'C ⊆ ⋃ T - S' by auto
moreover
with 'C ∈ Pow(A)' 'y ∈ A' have C ⊆ A ∩ U ∧ y ∈ A ∩ V by auto
ultimately have ∃ U ∈ (T {restricted to} A). ∃ V ∈ (T {restricted to} A). C ⊆ U ∧ y ∈ V ∧ U ∩ V = 0
by auto
}
then have ∀ x ∈ ⋃ (T {restricted to} A) - C. ∃ U ∈ (T {restricted to} A). ∃ V ∈ (T {restricted
to} A). C ⊆ U ∧ x ∈ V ∧ U ∩ V = 0 by auto
}
then have ∀ C. C {is closed in} (T {restricted to} A) ⟶ (∀ x ∈ ⋃ (T {restricted
to} A) - C. ∃ U ∈ (T {restricted to} A). ∃ V ∈ (T {restricted to} A). C ⊆ U ∧ x ∈ V ∧ U ∩ V = 0)
by blast
then show thesis using IsRegular_def by auto
qed

```

corollary here\_regular:

```
shows IsRegular {is hereditary} using regular_here IsHer_def by auto
```

theorem T1\_here:

```
assumes T {is T1} A ∈ Pow(⋃ T) shows (T {restricted to} A) {is T1}
```

proof-

```
from assms(2) have un: ⋃ (T {restricted to} A) = A unfolding RestrictedTo_def
```

by auto

```

{
  fix x y
  assume x ∈ A ∧ y ∈ A ∧ x ≠ y
  with 'A ∈ Pow(⋃ T)' have x ∈ ⋃ Ty ∈ ⋃ Tx ≠ y by auto
  then have ∃ U ∈ T. x ∈ U ∧ y ∉ U using assms(1) isT1_def by auto
  then obtain U where U ∈ T ∧ x ∈ U ∧ y ∉ U by auto
  with 'x ∈ A' have A ∩ U ∈ (T {restricted to} A) x ∈ A ∩ U y ∉ A ∩ U unfolding RestrictedTo_def

```

by auto

```
then have ∃ U ∈ (T {restricted to} A). x ∈ U ∧ y ∉ U by blast
```

```
}
```

```
with un have ∀ x y. x ∈ ⋃ (T {restricted to} A) ∧ y ∈ ⋃ (T {restricted to} A)
```

```
∧ x ≠ y ⟶ (∃ U ∈ (T {restricted to} A). x ∈ U ∧ y ∉ U)
```

```
by auto
```

```
then show thesis using isT1_def by auto
```

qed

corollary here\_T1:

```
shows isT1 {is hereditary} using T1_here IsHer_def by auto
```

lemma here\_and:

```
assumes P {is hereditary} Q {is hereditary}
```

```
shows (λ T. P(T) ∧ Q(T)) {is hereditary} using assms unfolding IsHer_def
```

by auto

```

corollary here_T3:
  shows isT3 {is hereditary} using here_and[OF here_T1 here_regular]
  unfolding IsHer_def isT3_def.

lemma T2_here:
  assumes T{is T2} A∈Pow( $\bigcup$ T) shows (T{restricted to}A){is T2}
proof-
  from assms(2) have un: $\bigcup$ (T{restricted to}A)=A unfolding RestrictedTo_def
  by auto
  {
    fix x y
    assume x∈Ay∈Ax≠y
    with 'A∈Pow( $\bigcup$ T)' have x∈ $\bigcup$ Ty∈ $\bigcup$ Tx≠y by auto
    then have  $\exists U \in T. \exists V \in T. x \in U \wedge y \in V \wedge U \cap V = 0$  using assms(1) isT2_def by
  auto
    then obtain U V where U∈T V∈Tx∈Uy∈VU∩V=0 by auto
    with 'x∈A' 'y∈A' have A∩U∈(T{restricted to}A)A∩V∈(T{restricted to}A)
    x∈A∩U y∈A∩V (A∩U)∩(A∩V)=0unfolding RestrictedTo_def by auto
    then have  $\exists U \in (T\{restricted\ to\}A). \exists V \in (T\{restricted\ to\}A). x \in U \wedge y \in V \wedge U \cap V = 0$ 
    unfolding Bex_def by auto
  }
  with un have  $\forall x y. x \in \bigcup (T\{restricted\ to\}A) \wedge y \in \bigcup (T\{restricted\ to\}A) \wedge x \neq y \longrightarrow (\exists U \in (T\{restricted\ to\}A). \exists V \in (T\{restricted\ to\}A). x \in U \wedge y \in V \wedge U \cap V = 0)$ 
  by auto
  then show thesis using isT2_def by auto
qed

corollary here_T2:
  shows isT2 {is hereditary} using T2_here IsHer_def by auto

lemma T0_here:
  assumes T{is T0} A∈Pow( $\bigcup$ T) shows (T{restricted to}A){is T0}
proof-
  from assms(2) have un: $\bigcup$ (T{restricted to}A)=A unfolding RestrictedTo_def
  by auto
  {
    fix x y
    assume x∈Ay∈Ax≠y
    with 'A∈Pow( $\bigcup$ T)' have x∈ $\bigcup$ Ty∈ $\bigcup$ Tx≠y by auto
    then have  $\exists U \in T. (x \in U \wedge y \notin U) \vee (y \in U \wedge x \notin U)$  using assms(1) isT0_def by
  auto
    then obtain U where U∈T (x∈U∧y∉U)∨(y∈U∧x∉U) by auto
    with 'x∈A' 'y∈A' have A∩U∈(T{restricted to}A) (x∈A∩U∧y∉A∩U)∨(y∈A∩U∧x∉A∩U)
    unfolding RestrictedTo_def by auto
    then have  $\exists U \in (T\{restricted\ to\}A). (x \in U \wedge y \notin U) \vee (y \in U \wedge x \notin U)$  unfolding
    Bex_def by auto
  }
  with un have  $\forall x y. x \in \bigcup (T\{restricted\ to\}A) \wedge y \in \bigcup (T\{restricted\ to\}A)$ 

```



```

 $\wedge x \neq y \longrightarrow (\exists U \in (T \text{restricted to } A). (x \in U \wedge y \notin U) \vee (y \in U \wedge x \notin U))$ 
  by auto
  then show thesis using isT0_def by auto
qed

```

```

corollary here_T0:
  shows isT0 {is hereditary} using T0_here IsHer_def by auto

```

## 51.2 Spectrum and anti-properties

The spectrum of a topological property is a class of sets such that all topologies defined over that set have that property.

The spectrum of a property gives us the list of sets for which the property doesn't give any topological information. Being in the spectrum of a topological property is an invariant in the category of sets and function; meaning that equipollent sets are in the same spectra.

```

definition Spec (_ {is in the spectrum of} _ 99)
  where Spec(K,P)  $\equiv \forall T. ((T \text{is a topology} \wedge \bigcup T \approx K) \longrightarrow P(T))$ 

```

```

lemma equipollent_spect:
  assumes A  $\approx$  B B {is in the spectrum of} P
  shows A {is in the spectrum of} P
proof-
  from assms(2) have  $\forall T. ((T \text{is a topology} \wedge \bigcup T \approx B) \longrightarrow P(T))$  using
  Spec_def by auto
  then have  $\forall T. ((T \text{is a topology} \wedge \bigcup T \approx A) \longrightarrow P(T))$  using eqpoll_trans[OF
  _ assms(1)] by auto
  then show thesis using Spec_def by auto
qed

```

```

theorem eqpoll_iff_spec:
  assumes A  $\approx$  B
  shows (B {is in the spectrum of} P)  $\longleftrightarrow$  (A {is in the spectrum of}
  P) apply safe
  using assms equipollent_spect apply simp using assms eqpoll_sym equipollent_spect[of
  BA] by auto

```

From the previous statement, we see that the spectrum could be formed only by representative of classes of sets. If  $AC$  holds, this means that the spectrum can be taken as a set or class of cardinal numbers.

Here is an example of the spectrum. The proof lies in the indiscrete filter  $\{A\}$  that can be build for any set. In this proof, we see that without choice, there is no way to define the spectrum of a property with cardinals because if a set is not comparable with any ordinal, its cardinal is defined as 0 without the set being empty.

```

theorem T4_spectrum:

```

```

shows (A {is in the spectrum of} isT4)  $\longleftrightarrow$  A  $\lesssim$  1
proof
  assume A {is in the spectrum of} isT4
  then have reg: $\forall T. ((T\{\text{is a topology}\} \cup T \approx A) \longrightarrow (T \{\text{is } T_4\}))$  using
  Spec_def by auto
  {
    assume A  $\neq$  0
    then obtain x where x  $\in$  A by auto
    then have x  $\in \bigcup \{A\}$  by auto
    moreover
    then have {A} {is a filter on}  $\bigcup \{A\}$  using IsFilter_def by auto
    moreover
    then have ({A}  $\cup$  {0}) {is a topology}  $\wedge \bigcup ({A} \cup {0}) = A$  using top_of_filter
  by auto
    then have top:({A}  $\cup$  {0}) {is a topology}  $\bigcup ({A} \cup {0}) \approx A$  using eqpoll_refl
  by auto
    then have ({A}  $\cup$  {0}) {is }  $T_4$  using reg by auto
    then have ({A}  $\cup$  {0}) {is }  $T_2$  using topology0.T3_is_T2 topology0.T4_is_T3
  topology0_def top by auto
    ultimately have  $\bigcup \{A\} = \{x\}$  using filter_T2_imp_card1[of {A}x] by auto
    then have A = {x} by auto
    then have A  $\approx$  1 using singleton_eqpoll_1 by auto
  }
  moreover
  have A = 0  $\longrightarrow$  A  $\approx$  0 by auto
  ultimately have A  $\approx$  1  $\vee$  A  $\approx$  0 by blast
  then show A  $\lesssim$  1 using empty_lepollI eqpoll_imp_lepoll eq_lepoll_trans
  by auto
next
  assume A  $\lesssim$  1
  have A = 0  $\vee$  A  $\neq$  0 by auto
  then obtain E where A = 0  $\vee$  E  $\in$  A by auto
  then have A  $\approx$  0  $\vee$  E  $\in$  A by auto
  with 'A  $\lesssim$  1' have A  $\approx$  0  $\vee$  A = {E} using lepoll_1_is_sing by auto
  then have A  $\approx$  0  $\vee$  A  $\approx$  1 using singleton_eqpoll_1 by auto
  {
    fix T
    assume AS:T{is a topology}  $\bigcup T \approx A$ 
    {
      assume A  $\approx$  0
      with AS have T{is a topology} and empty: $\bigcup T = 0$  using eqpoll_trans
    eqpoll_0_is_0 by auto
      then have T{is }  $T_2$  using isT2_def by auto
      then have T{is }  $T_1$  using T2_is_T1 by auto
      moreover
      from empty have T  $\subseteq$  {0} by auto
      with AS(1) have T = {0} using empty_open by auto
      from empty have rr: $\forall A. A\{\text{is closed in}\}T \longrightarrow A = 0$  using IsClosed_def
    by auto
  }

```

```

      have  $\exists U \in T. \exists V \in T. 0 \subseteq U \wedge 0 \subseteq V \wedge U \cap V = 0$  using empty_open AS(1) by auto
      with rr have  $\forall A. A\{\text{is closed in}\}T \longrightarrow (\forall B. B\{\text{is closed in}\}T \wedge$ 
 $A \cap B = 0 \longrightarrow (\exists U \in T. \exists V \in T. A \subseteq U \wedge B \subseteq V \wedge U \cap V = 0))$ 
      by blast
      then have  $T\{\text{is normal}\}$  using IsNormal_def by auto
      with 'T{is T1}' have  $T\{\text{is T}_4\}$  using isT4_def by auto
    }
  moreover
  {
    assume  $A \approx 1$ 
    with AS have  $T\{\text{is a topology}\}$  and NONempty: $\bigcup T \approx 1$  using eqpoll_trans[of
 $\bigcup TA1$ ] by auto
    then have  $\bigcup T \lesssim 1$  using eqpoll_imp_lepoll by auto
    moreover
    {
      assume  $\bigcup T = 0$ 
      then have  $0 \approx \bigcup T$  by auto
      with NONempty have  $0 \approx 1$  using eqpoll_trans by blast
      then have  $0 = 1$  using eqpoll_0_is_0 eqpoll_sym by auto
      then have False by auto
    }
    then have  $\bigcup T \neq 0$  by auto
    then obtain R where  $R \in \bigcup T$  by blast
    ultimately have  $\bigcup T = \{R\}$  using lepoll_1_is_sing by auto
    {
      fix x y
      assume  $x\{\text{is closed in}\}Ty\{\text{is closed in}\}T$   $x \cap y = 0$ 
      then have  $x \subseteq \bigcup Ty \subseteq \bigcup T$  using IsClosed_def by auto
      then have  $x = 0 \vee y = 0$  using 'x ∩ y = 0' ' $\bigcup T = \{R\}$ ' by force
      {
        assume  $x = 0$ 
        then have  $x \subseteq 0 \vee y \subseteq \bigcup T$  using 'y ⊆ ⋃ T' by auto
        moreover
        have  $0 \in T \bigcup T \in T$  using AS(1) IsATopology_def empty_open by auto
        ultimately have  $\exists U \in T. \exists V \in T. x \subseteq U \wedge y \subseteq V \wedge U \cap V = 0$  by auto
      }
    }
    moreover
    {
      assume  $x \neq 0$ 
      with ' $x = 0 \vee y = 0$ ' have  $y = 0$  by auto
      then have  $x \subseteq \bigcup Ty \subseteq 0$  using 'x ⊆ ⋃ T' by auto
      moreover
      have  $0 \in T \bigcup T \in T$  using AS(1) IsATopology_def empty_open by auto
      ultimately have  $\exists U \in T. \exists V \in T. x \subseteq U \wedge y \subseteq V \wedge U \cap V = 0$  by auto
    }
  }
  ultimately
  have  $(\exists U \in T. \exists V \in T. x \subseteq U \wedge y \subseteq V \wedge U \cap V = 0)$  by blast
}
then have  $T\{\text{is normal}\}$  using IsNormal_def by auto

```

```

    moreover
    {
      fix x y
      assume  $x \in \bigcup T_y \in \bigcup T_x \neq y$ 
      with ' $\bigcup T = \{R\}$ ' have False by auto
      then have  $\exists U \in T. x \in U \wedge y \notin U$  by auto
    }
    then have  $T \{is\ T_1\}$  using isT1_def by auto
    ultimately have  $T \{is\ T_4\}$  using isT4_def by auto
  }
  ultimately have  $T \{is\ T_4\}$  using ' $A \approx 0 \vee A \approx 1$ ' by auto
}
then have  $\forall T. (T \{is\ a\ topology\} \wedge \bigcup T \approx A) \longrightarrow (T \{is\ T_4\})$  by auto
then show  $A \{is\ in\ the\ spectrum\ of\} isT4$  using Spec_def by auto
qed

```

If the topological properties are related, then so are the spectra.

```

lemma P_imp_Q_spec_inv:
  assumes  $\forall T. T \{is\ a\ topology\} \longrightarrow (Q(T) \longrightarrow P(T))$   $A \{is\ in\ the\ spectrum\ of\} Q$ 
  shows  $A \{is\ in\ the\ spectrum\ of\} P$ 
proof-
  from assms(2) have  $\forall T. T \{is\ a\ topology\} \wedge \bigcup T \approx A \longrightarrow Q(T)$  using Spec_def
  by auto
  with assms(1) have  $\forall T. T \{is\ a\ topology\} \wedge \bigcup T \approx A \longrightarrow P(T)$  by auto
  then show thesis using Spec_def by auto
qed

```

Since we already now the spectrum of  $T_4$ ; if we now the spectrum of  $T_0$ , it should be easier to compute the spectrum of  $T_1$ ,  $T_2$  and  $T_3$ .

```

theorem T0_spectrum:
  shows  $(A \{is\ in\ the\ spectrum\ of\} isT0) \longleftrightarrow A \lesssim 1$ 
proof
  assume  $A \{is\ in\ the\ spectrum\ of\} isT0$ 
  then have reg: $\forall T. ((T \{is\ a\ topology\} \wedge \bigcup T \approx A) \longrightarrow (T \{is\ T_0\}))$  using Spec_def by auto
  {
    assume  $A \neq 0$ 
    then obtain x where  $x \in A$  by auto
    then have  $x \in \bigcup \{A\}$  by auto
    moreover
    then have  $\{A\} \{is\ a\ filter\ on\} \bigcup \{A\}$  using IsFilter_def by auto
    moreover
    then have  $(\{A\} \cup \{0\}) \{is\ a\ topology\} \wedge \bigcup (\{A\} \cup \{0\}) = A$  using top_of_filter
  by auto
    then have  $(\{A\} \cup \{0\}) \{is\ a\ topology\} \wedge \bigcup (\{A\} \cup \{0\}) \approx A$  using eqpoll_refl
  by auto
    then have  $(\{A\} \cup \{0\}) \{is\ T_0\}$  using reg by auto
  }

```

```

    fix y
    assume  $y \in Ax \neq y$ 
    with
    '({A} ∪ {0}) {is  $T_0$ }' obtain U where  $U \in ({A} \cup \{0\})$  and  $\text{dis}:(x \in U \wedge y \notin U) \vee (y \in U \wedge x \notin U)$  using isT0_def by auto
    then have  $U=A$  by auto
    with  $\text{dis}$  ' $y \in A$ ' ' $x \in \bigcup \{A\}$ ' have False by auto
  }
  then have  $\forall y \in A. y=x$  by auto
  with ' $x \in \bigcup \{A\}$ ' have  $A=\{x\}$  by blast
  then have  $A \approx 1$  using singleton_eqpoll_1 by auto
}
moreover
have  $A=0 \longrightarrow A \approx 0$  by auto
ultimately have  $A \approx 1 \vee A \approx 0$  by blast
then show  $A \lesssim 1$  using empty_lepollI eqpoll_imp_lepoll eq_lepoll_trans
by auto
next
assume  $A \lesssim 1$ 
{
  fix T
  assume T{is a topology}
  then have  $(T\{\text{is } T_4\}) \longrightarrow (T\{\text{is } T_0\})$  using topology0.T4_is_T3 topology0.T3_is_T2
  T2_is_T1 T1_is_T0
  topology0_def by auto
}
then have  $\forall T. T\{\text{is a topology}\} \longrightarrow ((T\{\text{is } T_4\}) \longrightarrow (T\{\text{is } T_0\}))$  by auto
then have  $(A \{\text{is in the spectrum of}\} \text{is } T_4) \longrightarrow (A \{\text{is in the spectrum of}\} \text{is } T_0)$ 
using P_imp_Q_spec_inv[of  $\lambda T. (T\{\text{is } T_4\}) \lambda T. T\{\text{is } T_0\}$ ] by auto
then show  $(A \{\text{is in the spectrum of}\} \text{is } T_0)$  using T4_spectrum ' $A \lesssim 1$ '
by auto
qed

theorem T1_spectrum:
  shows  $(A \{\text{is in the spectrum of}\} \text{is } T_1) \longleftrightarrow A \lesssim 1$ 
proof-
  note T2_is_T1 topology0.T3_is_T2 topology0.T4_is_T3
  then have  $(A \{\text{is in the spectrum of}\} \text{is } T_4) \longrightarrow (A \{\text{is in the spectrum of}\} \text{is } T_1)$ 
  using P_imp_Q_spec_inv[of isT4isT1] topology0_def by auto
  moreover
  note T1_is_T0
  then have  $(A \{\text{is in the spectrum of}\} \text{is } T_1) \longrightarrow (A \{\text{is in the spectrum of}\} \text{is } T_0)$ 
  using P_imp_Q_spec_inv[of isT1isT0] by auto
  moreover
  note T0_spectrum T4_spectrum
  ultimately show thesis by blast

```

qed

theorem T2\_spectrum:

shows (A {is in the spectrum of} isT2)  $\longleftrightarrow$   $A \lesssim 1$

proof-

note topology0.T3\_is\_T2 topology0.T4\_is\_T3

then have (A {is in the spectrum of} isT4)  $\longrightarrow$  (A {is in the spectrum of} isT2)

using P\_imp\_Q\_spec\_inv[of isT4isT2] topology0\_def by auto

moreover

note T2\_is\_T1

then have (A {is in the spectrum of} isT2)  $\longrightarrow$  (A {is in the spectrum of} isT1)

using P\_imp\_Q\_spec\_inv[of isT2isT1] by auto

moreover

note T1\_spectrum T4\_spectrum

ultimately show thesis by blast

qed

theorem T3\_spectrum:

shows (A {is in the spectrum of} isT3)  $\longleftrightarrow$   $A \lesssim 1$

proof-

note topology0.T4\_is\_T3

then have (A {is in the spectrum of} isT4)  $\longrightarrow$  (A {is in the spectrum of} isT3)

using P\_imp\_Q\_spec\_inv[of isT4isT3] topology0\_def by auto

moreover

note topology0.T3\_is\_T2

then have (A {is in the spectrum of} isT3)  $\longrightarrow$  (A {is in the spectrum of} isT2)

using P\_imp\_Q\_spec\_inv[of isT3isT2] topology0\_def by auto

moreover

note T2\_spectrum T4\_spectrum

ultimately show thesis by blast

qed

theorem compact\_spectrum:

shows (A {is in the spectrum of}  $(\lambda T. (\bigcup T) \text{is compact in } T)) \longleftrightarrow \text{Finite}(A)$

proof

assume A {is in the spectrum of}  $(\lambda T. (\bigcup T) \text{is compact in } T)$

then have reg: $\forall T. T \text{is a topology} \wedge \bigcup T \approx A \longrightarrow ((\bigcup T) \text{is compact in } T)$  using Spec\_def by auto

have  $\text{Pow}(A) \text{is a topology} \wedge \bigcup \text{Pow}(A) = A$  using Pow\_is\_top by auto

then have  $\text{Pow}(A) \text{is a topology} \wedge \bigcup \text{Pow}(A) \approx A$  using eqpoll\_refl by auto

with reg have  $A \text{is compact in } \text{Pow}(A)$  by auto

moreover

have  $\{x\}. x \in A \in \text{Pow}(\text{Pow}(A))$  by auto

```

    moreover
    have  $\bigcup \{\{x\}. x \in A\} = A$  by auto
    ultimately have  $\exists N \in \text{FinPow}(\{\{x\}. x \in A\}). A \subseteq \bigcup N$  using IsCompact_def by
auto
    then obtain N where  $N \in \text{FinPow}(\{\{x\}. x \in A\})$   $A \subseteq \bigcup N$  by auto
    then have  $N \subseteq \{\{x\}. x \in A\}$  Finite(N)  $A \subseteq \bigcup N$  using FinPow_def by auto
    {
      fix t
      assume  $t \in \{\{x\}. x \in A\}$ 
      then obtain x where  $x \in t = \{x\}$  by auto
      with ' $A \subseteq \bigcup N$ ' have  $x \in \bigcup N$  by auto
      then obtain B where  $B \in N$   $x \in B$  by auto
      with ' $N \subseteq \{\{x\}. x \in A\}$ ' have  $B = \{x\}$  by auto
      with ' $t = \{x\}$ ' ' $B \in N$ ' have  $t \in N$  by auto
    }
    with ' $N \subseteq \{\{x\}. x \in A\}$ ' have  $N = \{\{x\}. x \in A\}$  by auto
    with 'Finite(N)' have Finite( $\{\{x\}. x \in A\}$ ) by auto
    let  $B = \{\langle x, \{x\} \rangle. x \in A\}$ 
    have  $B : A \rightarrow \{\{x\}. x \in A\}$  unfolding Pi_def function_def by auto
    then have  $B : \text{bij}(A, \{\{x\}. x \in A\})$  unfolding bij_def inj_def surj_def us-
ing apply_equality by auto
    then have  $A \approx \{\{x\}. x \in A\}$  using eqpoll_def by auto
    with 'Finite( $\{\{x\}. x \in A\}$ )' show Finite(A) using eqpoll_imp_Finite_iff
by auto
next
  assume Finite(A)
  {
    fix T assume T {is a topology}  $\bigcup T \approx A$ 
    with 'Finite(A)' have Finite( $\bigcup T$ ) using eqpoll_imp_Finite_iff by
auto
    then have Finite(Pow( $\bigcup T$ )) using Finite_Pow by auto
    moreover
    have  $T \subseteq \text{Pow}(\bigcup T)$  by auto
    ultimately have Finite(T) using subset_Finite by auto
    {
      fix M
      assume  $M \in \text{Pow}(T) \bigcup T \subseteq \bigcup M$ 
      with 'Finite(T)' have Finite(M) using subset_Finite by auto
      with ' $\bigcup T \subseteq \bigcup M$ ' have  $\exists N \in \text{FinPow}(M). \bigcup T \subseteq \bigcup N$  using FinPow_def by
auto
    }
    then have  $(\bigcup T) \{\text{is compact in}\} T$  unfolding IsCompact_def by auto
  }
  then show A {is in the spectrum of}  $(\lambda T. (\bigcup T) \{\text{is compact in}\} T)$  us-
ing Spec_def by auto
qed

```

It is, at least for some people, surprising that the spectrum of some properties cannot be completely determined in  $ZF$ .

```

theorem compactK_spectrum:
  assumes {the axiom of}K{choice holds for subsets}(Pow(K)) Card(K)
  shows (A {is in the spectrum of} ( $\lambda T. ((\bigcup T)\{is compact of cardinal\}$ 
csucc(K){in}T)))  $\longleftrightarrow$  ( $A \lesssim K$ )
proof
  assume A {is in the spectrum of} ( $\lambda T. ((\bigcup T)\{is compact of cardinal\}$ 
csucc(K){in}T))
  then have reg: $\forall T. T\{is a topology\} \wedge \bigcup T \approx A \longrightarrow ((\bigcup T)\{is compact of$ 
cardinal} csucc(K){in}T) using Spec_def by auto
  then have A{is compact of cardinal} csucc(K) {in} Pow(A) using Pow_is_top[of
A] by auto
  then have  $\forall M \in Pow(Pow(A)). A \subseteq \bigcup M \longrightarrow (\exists N \in Pow(M). A \subseteq \bigcup N \wedge N \prec csucc(K))$ 
unfolding IsCompactOfCard_def by auto
  moreover
  have  $\{\{x\}. x \in A\} \in Pow(Pow(A))$  by auto
  moreover
  have  $A = \bigcup \{\{x\}. x \in A\}$  by auto
  ultimately have  $\exists N \in Pow(\{\{x\}. x \in A\}). A \subseteq \bigcup N \wedge N \prec csucc(K)$  by auto
  then obtain N where  $N \in Pow(\{\{x\}. x \in A\})$   $A \subseteq \bigcup N$   $N \prec csucc(K)$  by auto
  then have  $N \subseteq \{\{x\}. x \in A\}$   $N \prec csucc(K)$   $A \subseteq \bigcup N$  using FinPow_def by auto
  {
    fix t
    assume  $t \in \{\{x\}. x \in A\}$ 
    then obtain x where  $x \in t = \{x\}$  by auto
    with ' $A \subseteq \bigcup N$ ' have  $x \in \bigcup N$  by auto
    then obtain B where  $B \in N$   $x \in B$  by auto
    with ' $N \subseteq \{\{x\}. x \in A\}$ ' have  $B = \{x\}$  by auto
    with ' $t = \{x\}$ ' ' $B \in N$ ' have  $t \in N$  by auto
  }
  with ' $N \subseteq \{\{x\}. x \in A\}$ ' have  $N = \{\{x\}. x \in A\}$  by auto
  let  $B = \{\langle x, \{x\} \rangle. x \in A\}$ 
  from ' $N = \{\{x\}. x \in A\}$ ' have  $B: A \rightarrow N$  unfolding Pi_def function_def by auto
  with ' $N = \{\{x\}. x \in A\}$ ' have  $B: inj(A, N)$  unfolding inj_def using apply_equality
by auto
  then have  $A \lesssim N$  using lepoll_def by auto
  with ' $N \prec csucc(K)$ ' have  $A \prec csucc(K)$  using lesspoll_trans1 by auto
  then show  $A \lesssim K$  using Card_less_csucc_eq_le assms(2) by auto
next
  assume  $A \lesssim K$ 
  {
    fix T
    assume  $T\{is a topology\} \bigcup T \approx A$ 
    have  $Pow(\bigcup T)\{is a topology\}$  using Pow_is_top by auto
    {
      fix B
      assume  $AS: B \in Pow(\bigcup T)$ 
      then have  $\{\{i\}. i \in B\} \subseteq \{\{i\}. i \in \bigcup T\}$  by auto
      moreover
      have  $B = \bigcup \{\{i\}. i \in B\}$  by auto
    }
  }

```



```

      ultimately have  $\exists S \in \text{Pow}(\{i\}. i \in \bigcup T). B = \bigcup S$  by auto
      then have  $B \in \{\bigcup U. U \in \text{Pow}(\{i\}. i \in \bigcup T)\}$  by auto
    }
  moreover
  {
    fix B
    assume AS:  $B \in \{\bigcup U. U \in \text{Pow}(\{i\}. i \in \bigcup T)\}$ 
    then have  $B \in \text{Pow}(\bigcup T)$  by auto
  }
  ultimately
  have base:  $\{\{x\}. x \in \bigcup T\}$  {is a base for}  $\text{Pow}(\bigcup T)$  unfolding IsAbaseFor_def
by auto
  let f =  $\langle i, \{i\} \rangle. i \in \bigcup T$ 
  have f:  $f: \bigcup T \rightarrow \{\{x\}. x \in \bigcup T\}$  using Pi_def function_def by auto
  moreover
  {
    fix w x
    assume as:  $w \in \bigcup T, x \in \bigcup T, fw = fx$ 
    with f have fw =  $\{w\}$  fx =  $\{x\}$  using apply_equality by auto
    with as(3) have  $w = x$  by auto
  }
  with f have f:  $\text{inj}(\bigcup T, \{\{x\}. x \in \bigcup T\})$  unfolding inj_def by auto
  moreover
  {
    fix xa
    assume xa:  $xa \in \{\{x\}. x \in \bigcup T\}$ 
    then obtain x where  $x \in \bigcup T, xa = \{x\}$  by auto
    with f have fx = xa using apply_equality by auto
    with 'x  $\in \bigcup T$ ' have  $\exists x \in \bigcup T. fx = xa$  by auto
  }
  then have  $\forall xa \in \{\{x\}. x \in \bigcup T\}. \exists x \in \bigcup T. fx = xa$  by blast
  ultimately have f:  $\text{bij}(\bigcup T, \{\{x\}. x \in \bigcup T\})$  unfolding bij_def surj_def
by auto
  then have  $\bigcup T \approx \{\{x\}. x \in \bigcup T\}$  using eqpoll_def by auto
  then have  $\{\{x\}. x \in \bigcup T\} \approx \bigcup T$  using eqpoll_sym by auto
  with ' $\bigcup T \approx A$ ' have  $\{\{x\}. x \in \bigcup T\} \approx A$  using eqpoll_trans by blast
  then have  $\{\{x\}. x \in \bigcup T\} \lesssim A$  using eqpoll_imp_lepoll by auto
  with ' $A \lesssim K$ ' have  $\{\{x\}. x \in \bigcup T\} \lesssim K$  using lepoll_trans by blast
  then have  $\{\{x\}. x \in \bigcup T\} \prec \text{csucc}(K)$  using assms(2) Card_less_csucc_eq_le
by auto
  with base have  $\text{Pow}(\bigcup T)$  {is of second type of cardinal}  $\text{csucc}(K)$  unfolding IsSecondOfCard_def by auto
  moreover
  have  $\bigcup \text{Pow}(\bigcup T) = \bigcup T$  by auto
  with calculation assms(1) ' $\text{Pow}(\bigcup T)$  {is a topology}' have  $(\bigcup T)$  {is compact of cardinal}  $\text{csucc}(K)$  {in}  $\text{Pow}(\bigcup T)$ 
  using compact_of_cardinal_Q[of  $\text{KPow}(\bigcup T)$ ] by auto
  moreover
  have  $T \subseteq \text{Pow}(\bigcup T)$  by auto

```

```

      ultimately have  $(\bigcup T)$  {is compact of cardinal}  $\text{csucc}(K)$  {in}  $T$  using
compact_coarser by auto
    }
    then show  $A$  {is in the spectrum of}  $(\lambda T. ((\bigcup T)$  {is compact of cardinal}  $\text{csucc}(K)$ 
{in}  $T))$  using Spec_def by auto
qed

```

**theorem compactK\_spectrum\_reverse:**

```

  assumes  $\forall A. (A$  {is in the spectrum of}  $(\lambda T. ((\bigcup T)$  {is compact of cardinal}
 $\text{csucc}(K)$  {in}  $T))) \longleftrightarrow (A \lesssim K) \text{ InfCard}(K)$ 
  shows {the axiom of}  $K$  {choice holds for subsets}  $(\text{Pow}(K))$ 

```

**proof-**

```

  have  $K \lesssim K$  using lepoll_refl by auto
  then have  $K$  {is in the spectrum of}  $(\lambda T. ((\bigcup T)$  {is compact of cardinal}
 $\text{csucc}(K)$  {in}  $T))$  using assms(1) by auto
  moreover
  have  $\text{Pow}(K)$  {is a topology} using Pow_is_top by auto
  moreover
  have  $\bigcup \text{Pow}(K) = K$  by auto
  then have  $\bigcup \text{Pow}(K) \approx K$  using eqpoll_refl by auto
  ultimately
  have  $K$  {is compact of cardinal}  $\text{csucc}(K)$  {in}  $\text{Pow}(K)$  using Spec_def by
auto
  then show thesis using Q_disc_comp_csuccQ_eq_Q_choice_csuccQ assms(2)
by auto
qed

```

This last theorem states that if one of the forms of the axiom of choice related to this compactness property fails, then the spectrum will be different. Notice that even for Lindelöf spaces that will happen.

The spectrum gives us the possibility to define what an anti-property means. A space is anti- $P$  if the only subspaces which have the property are the ones in the spectrum of  $P$ . This concept tries to put together spaces that are completely opposite to spaces where  $P(T)$ .

**definition**

```

antiProperty ( $\_$  {is anti-}  $\_$  50)
where  $T$  {is anti-}  $P \equiv \forall A \in \text{Pow}(\bigcup T). P(T \text{ restricted to } A) \longrightarrow (A$  {is
in the spectrum of}  $P)$ 

```

**abbreviation**

```

ANTI( $P$ )  $\equiv \lambda T. (T$  {is anti-}  $P)$ 

```

A first, very simple but very useful result is the following: when the properties are related and the spectra are equal, then the anti-properties are related in the opposite direction.

**theorem (in topology0) eq\_spect\_rev\_imp\_anti:**

```

  assumes  $\forall T. T$  {is a topology}  $\longrightarrow P(T) \longrightarrow Q(T) \forall A. (A$  {is in the spectrum
of}  $Q) \longrightarrow (A$  {is in the spectrum of}  $P)$ 

```

```

    and T{is anti-}Q
  shows T{is anti-}P
proof-
{
  fix A
  assume A ∈ Pow(⋃ T) P(T{restricted to}A)
  with assms(1) have Q(T{restricted to}A) using Top_1_L4 by auto
  with assms(3) 'A ∈ Pow(⋃ T)' have A{is in the spectrum of}Q using antiProperty_def
by auto
  with assms(2) have A{is in the spectrum of}P by auto
}
then show thesis using antiProperty_def by auto
qed

```

If a space can be  $P(T) \wedge Q(T)$  only in case the underlying set is in the spectrum of  $P$ ; then  $Q(T) \longrightarrow \text{ANTI}(P, T)$  when  $Q$  is hereditary.

```

theorem Q_P_imp_Spec:
  assumes  $\forall T. ((T\text{is a topology}) \wedge P(T) \wedge Q(T)) \longrightarrow ((\bigcup T)\text{is in the spectrum of}P)$ 
  and Q{is hereditary}
  shows  $\forall T. T\text{is a topology} \longrightarrow (Q(T) \longrightarrow (T\text{is anti-}P))$ 
proof
  fix T
  {
    assume T{is a topology}
    {
      assume Q(T)
      {
        assume  $\neg(T\text{is anti-}P)$ 
        then obtain A where  $A \in \text{Pow}(\bigcup T) \ P(T\text{restricted to}A) \wedge \neg(A\text{is in the spectrum of}P)$ 
        unfolding antiProperty_def by auto
        from 'Q(T)' 'T{is a topology}' 'A ∈ Pow(⋃ T)' assms(2) have Q(T{restricted to}A)
        unfolding IsHer_def by auto
        moreover
        note 'P(T{restricted to}A)' assms(1)
        moreover
        from 'T{is a topology}' have (T{restricted to}A){is a topology}
using topology0.Top_1_L4
        topology0_def by auto
        moreover
        from 'A ∈ Pow(⋃ T)' have  $\bigcup (T\text{restricted to}A) = A$  unfolding RestrictedTo_def
by auto
        ultimately have A{is in the spectrum of}P by auto
        with ' $\neg(A\text{is in the spectrum of}P)$ ' have False by auto
      }
    }
  then have T{is anti-}P by auto
}

```

```

    then have  $Q(T) \longrightarrow (T \text{ is anti-}P)$  by auto
  }
  then show  $(T \text{ is a topology}) \longrightarrow (Q(T) \longrightarrow (T \text{ is anti-}P))$  by auto
qed

theorem (in topology0) her_P_imp_anti2P:
  assumes  $P \text{ is hereditary}$   $P(T)$ 
  shows  $T \text{ is anti-}ANTI(P)$ 
proof-
  {
    assume  $\neg(T \text{ is anti-}ANTI(P))$ 
    then have  $\exists A \in \text{Pow}(\bigcup T). ((T \text{ restricted to } A) \text{ is anti-}P) \wedge \neg(A \text{ is in the spectrum of } ANTI(P))$ 
    unfolding antiProperty_def[of _ ANTI(P)] by auto
    then obtain A where  $A\_def: A \in \text{Pow}(\bigcup T) \wedge \neg(A \text{ is in the spectrum of } ANTI(P)) \wedge (T \text{ restricted to } A) \text{ is anti-}P$ 
    by auto
    from 'A ∈ Pow(⋃ T)' have tot:  $\bigcup (T \text{ restricted to } A) = A$  unfolding RestrictedTo_def
    by auto
    from A_def have reg:  $\forall B \in \text{Pow}(\bigcup (T \text{ restricted to } A)). P((T \text{ restricted to } A) \text{ restricted to } B) \longrightarrow (B \text{ is in the spectrum of } P)$ 
    unfolding antiProperty_def by auto
    have  $\forall B \in \text{Pow}(A). (T \text{ restricted to } A) \text{ restricted to } B = T \text{ restricted to } B$  using subspace_of_subspace 'A ∈ Pow(⋃ T)' by auto
    then have  $\forall B \in \text{Pow}(A). P(T \text{ restricted to } B) \longrightarrow (B \text{ is in the spectrum of } P)$  using reg apply (simp only: tot)
    by force
    moreover
    have  $\forall B \in \text{Pow}(A). P(T \text{ restricted to } B)$  using assms 'A ∈ Pow(⋃ T)' unfolding IsHer_def using topSpaceAssum by blast
    ultimately have reg2:  $\forall B \in \text{Pow}(A). (B \text{ is in the spectrum of } P)$  by auto
    from ' $\neg(A \text{ is in the spectrum of } ANTI(P))$ ' have  $\exists T. T \text{ is a topology} \wedge \bigcup T \approx A \wedge \neg(T \text{ is anti-}P)$ 
    unfolding Spec_def by auto
    then obtain S where  $S \text{ is a topology} \wedge \bigcup S \approx A \wedge \neg(S \text{ is anti-}P)$  by auto
    from ' $\neg(S \text{ is anti-}P)$ ' have  $\exists B \in \text{Pow}(\bigcup S). P(S \text{ restricted to } B) \wedge \neg(B \text{ is in the spectrum of } P)$  unfolding antiProperty_def by auto
    then obtain B where  $B\_def: \neg(B \text{ is in the spectrum of } P) \wedge B \in \text{Pow}(\bigcup S)$ 
    by auto
    then have  $B \lesssim \bigcup S$  using subset_imp_lepoll by auto
    with ' $\bigcup S \approx A$ ' have  $B \lesssim A$  using lepoll_eq_trans by auto
    then obtain f where  $f \in \text{inj}(B, A)$  unfolding lepoll_def by auto
    then have  $f \in \text{bij}(B, \text{range}(f))$  using inj_bij_range by auto
    then have  $B \approx \text{range}(f)$  unfolding eqpoll_def by auto
    with B_def(1) have  $\neg(\text{range}(f) \text{ is in the spectrum of } P)$  using eqpoll_iff_spec
    by auto
    moreover
    with 'f ∈ inj(B, A)' have  $\text{range}(f) \subseteq A$  unfolding inj_def Pi_def by auto
  }

```

```

    with reg2 have range(f){is in the spectrum of}P by auto
    ultimately have False by auto
  }
  then show thesis by auto
qed

```

The anti-properties are always hereditary

```

theorem anti_here:
  shows ANTI(P){is hereditary}
proof-
  {
    fix T
    assume T {is a topology}ANTI(P,T)
    {
      fix A
      assume A∈Pow( $\bigcup T$ )
      then have  $\bigcup (T\{\text{restricted to}\}A)=A$  unfolding RestrictedTo_def by
auto
      moreover
      {
        fix B
        assume B∈Pow(A)P((T{restricted to}A){restricted to}B)
        with 'A∈Pow( $\bigcup T$ )' have B∈Pow( $\bigcup T$ )P(T{restricted to}B) using subspace_of_subspace
by auto
        with 'ANTI(P,T)' have B{is in the spectrum of}P unfolding antiProperty_def
by auto
      }
      ultimately have  $\forall B\in\text{Pow}(\bigcup (T\{\text{restricted to}\}A)). (P((T\{\text{restricted to}\}A)\{\text{restricted to}\}B)) \longrightarrow (B\{\text{is in the spectrum of}\}P)$ 
by auto
      then have ANTI(P,(T{restricted to}A)) unfolding antiProperty_def
by auto
    }
    then have  $\forall A\in\text{Pow}(\bigcup T). \text{ANTI}(P,(T\{\text{restricted to}\}A))$  by auto
  }
  then show thesis using IsHer_def by auto
qed

```

```

corollary (in topology0) anti_imp_anti3:
  assumes T{is anti-}P
  shows T{is anti-}ANTI(ANTI(P))
  using anti_here her_P_imp_anti2P assms by auto

```

In the article [5], we can find some results on anti-properties.

```

theorem (in topology0) anti_T0:
  shows (T{is anti-}isT0)  $\longleftrightarrow$  T={0, $\bigcup T$ }
proof
  assume T={0, $\bigcup T$ }
  {

```

```

fix A
assume  $A \in \text{Pow}(\bigcup T) (T\{\text{restricted to}\}A) \{\text{is } T_0\}$ 
{
  fix B
  assume  $B \in T\{\text{restricted to}\}A$ 
  then obtain S where  $S \in T$  and  $B = A \cap S$  unfolding RestrictedTo_def by
auto
  with ' $T = \{0, \bigcup T\}$ ' have  $S \in \{0, \bigcup T\}$  by auto
  then have  $S = 0 \vee S = \bigcup T$  by auto
  with ' $B = A \cap S$ ' ' $A \in \text{Pow}(\bigcup T)$ ' have  $B = 0 \vee B = A$  by auto
}
moreover
{
  have  $0 \in \{0, \bigcup T\} \bigcup T \in \{0, \bigcup T\}$  by auto
  with ' $T = \{0, \bigcup T\}$ ' have  $0 \in T(\bigcup T) \in T$  by auto
  then have  $A \cap 0 \in (T\{\text{restricted to}\}A) \ A \cap (\bigcup T) \in (T\{\text{restricted to}\}A)$ 
using RestrictedTo_def by auto
  moreover
  from ' $A \in \text{Pow}(\bigcup T)$ ' have  $A \cap (\bigcup T) = A$  by auto
  ultimately have  $0 \in (T\{\text{restricted to}\}A) \ A \in (T\{\text{restricted to}\}A)$  by
auto
}
ultimately have  $(T\{\text{restricted to}\}A) = \{0, A\}$  by auto
with ' $(T\{\text{restricted to}\}A) \{\text{is } T_0\}$ ' have  $\{0, A\} \{\text{is } T_0\}$  by auto
{
  assume  $A \neq 0$ 
  then obtain x where  $x \in A$  by blast
  {
    fix y
    assume  $y \in A \wedge y \neq x$ 
    with ' $\{0, A\} \{\text{is } T_0\}$ ' obtain U where  $U \in \{0, A\}$  and  $\text{dis}:(x \in U \wedge$ 
y  $\notin U) \vee (y \in U \wedge x \notin U)$  using isT0_def by auto
    then have  $U = A$  by auto
    with  $\text{dis}$  ' $y \in A$ ' ' $x \in A$ ' have False by auto
  }
  then have  $\forall y \in A. y = x$  by auto
  with ' $x \in A$ ' have  $A = \{x\}$  by blast
  then have  $A \approx 1$  using singleton_eqpoll_1 by auto
  then have  $A \lesssim 1$  using eqpoll_imp_lepoll by auto
  then have  $A \{\text{is in the spectrum of}\} \text{isT0}$  using T0_spectrum by auto
}
moreover
{
  assume  $A = 0$ 
  then have  $A \approx 0$  by auto
  then have  $A \lesssim 1$  using empty_lepollI eq_lepoll_trans by auto
  then have  $A \{\text{is in the spectrum of}\} \text{isT0}$  using T0_spectrum by auto
}
}

```

```

    ultimately have  $A\{\text{is in the spectrum of}\}\text{isT0}$  by auto
  }
  then show  $T\{\text{is anti-}\}\text{isT0}$  using antiProperty_def by auto
next
  assume  $T\{\text{is anti-}\}\text{isT0}$ 
  then have  $\forall A \in \text{Pow}(\bigcup T). (T\{\text{restricted to}\}A)\{\text{is } T_0\} \longrightarrow (A\{\text{is in the spectrum of}\}\text{isT0})$  using antiProperty_def by auto
  then have reg:  $\forall A \in \text{Pow}(\bigcup T). (T\{\text{restricted to}\}A)\{\text{is } T_0\} \longrightarrow (A \lesssim 1)$  using T0_spectrum by auto
  {
    assume  $\exists A \in T. A \neq 0 \wedge A \neq \bigcup T$ 
    then obtain A where  $A \in T \wedge 0A \neq \bigcup T$  by auto
    then obtain x y where  $x \in A \ y \in \bigcup T - A$  by blast
    with 'A ∈ T' have  $s: \{x, y\} \in \text{Pow}(\bigcup T) \ x \neq y$  by auto
    note s
    moreover
    {
      fix b1 b2
      assume  $b1 \in \bigcup (T\{\text{restricted to}\}\{x, y\}) \ b2 \in \bigcup (T\{\text{restricted to}\}\{x, y\}) \ b1 \neq b2$ 
      moreover
      from s have  $\bigcup (T\{\text{restricted to}\}\{x, y\}) = \{x, y\}$  unfolding RestrictedTo_def
    by auto
      ultimately have  $(b1 = x \wedge b2 = y) \vee (b1 = y \wedge b2 = x)$  by auto
      with 'x ≠ y' have  $(b1 \in \{x\} \wedge b2 \notin \{x\}) \vee (b2 \in \{x\} \wedge b1 \notin \{x\})$  by auto
      moreover
      from 'y ∈  $\bigcup T - A$ ' 'x ∈ A' have  $\{x\} = \{x, y\} \cap A$  by auto
      with 'A ∈ T' have  $\{x\} \in (T\{\text{restricted to}\}\{x, y\})$  unfolding RestrictedTo_def
    by auto
      ultimately have  $\exists U \in (T\{\text{restricted to}\}\{x, y\}). (b1 \in U \wedge b2 \notin U) \vee (b2 \in U \wedge b1 \notin U)$ 
    by auto
    }
    then have  $(T\{\text{restricted to}\}\{x, y\})\{\text{is } T_0\}$  using isT0_def by auto
    ultimately have  $\{x, y\} \lesssim 1$  using reg by auto
    moreover
    have  $x \in \{x, y\}$  by auto
    ultimately have  $\{x, y\} = \{x\}$  using lepoll_1_is_sing[of  $\{x, y\} x$ ] by auto
    moreover
    have  $y \in \{x, y\}$  by auto
    ultimately have  $y \in \{x\}$  by auto
    then have  $y = x$  by auto
    with 'x ≠ y' have False by auto
  }
  then have  $T \subseteq \{0, \bigcup T\}$  by auto
  moreover
  from topSpaceAssum have  $0 \in T \ \bigcup T \in T$  using IsATopology_def empty_open by auto
  ultimately show  $T = \{0, \bigcup T\}$  by auto
qed

```

```

lemma indiscrete_spectrum:
  shows (A {is in the spectrum of}( $\lambda T. T=\{0, \bigcup T\}$ ))  $\longleftrightarrow A \lesssim 1$ 
proof
  assume (A {is in the spectrum of}( $\lambda T. T=\{0, \bigcup T\}$ ))
  then have reg: $\forall T. ((T\{\text{is a topology}\} \wedge \bigcup T \approx A) \longrightarrow T = \{0, \bigcup T\})$  using
Spec_def by auto
  moreover
  have  $\bigcup \text{Pow}(A) = A$  by auto
  then have  $\bigcup \text{Pow}(A) \approx A$  by auto
  moreover
  have Pow(A) {is a topology} using Pow_is_top by auto
  ultimately have P:Pow(A)={0,A} by auto
  {
    assume  $A \neq 0$ 
    then obtain x where  $x \in A$  by blast
    then have  $\{x\} \in \text{Pow}(A)$  by auto
    with P have  $\{x\} = A$  by auto
    then have  $A \approx 1$  using singleton_eqpoll_1 by auto
    then have  $A \lesssim 1$  using eqpoll_imp_lepoll by auto
  }
  moreover
  {
    assume  $A = 0$ 
    then have  $A \approx 0$  by auto
    then have  $A \lesssim 1$  using empty_lepollI eq_lepoll_trans by auto
  }
  ultimately show  $A \lesssim 1$  by auto
next
assume  $A \lesssim 1$ 
{
  fix T
  assume  $T\{\text{is a topology}\} \bigcup T \approx A$ 
  {
    assume  $A = 0$ 
    with ' $\bigcup T \approx A$ ' have  $\bigcup T \approx 0$  by auto
    then have  $\bigcup T = 0$  using eqpoll_0_is_0 by auto
    then have  $T \subseteq \{0\}$  by auto
    with ' $T\{\text{is a topology}\}$ ' have  $T = \{0\}$  using empty_open by auto
    then have  $T = \{0, \bigcup T\}$  by auto
  }
  moreover
  {
    assume  $A \neq 0$ 
    then obtain E where  $E \in A$  by blast
    with ' $A \lesssim 1$ ' have  $A = \{E\}$  using lepoll_1_is_sing by auto
    then have  $A \approx 1$  using singleton_eqpoll_1 by auto
    with ' $\bigcup T \approx A$ ' have NONempty: $\bigcup T \approx 1$  using eqpoll_trans by blast
    then have  $\bigcup T \lesssim 1$  using eqpoll_imp_lepoll by auto
    moreover

```



```

    {
      assume  $\bigcup T = 0$ 
      then have  $0 \approx \bigcup T$  by auto
      with NONempty have  $0 \approx 1$  using eqpoll_trans by blast
      then have  $0 = 1$  using eqpoll_0_is_0 eqpoll_sym by auto
      then have False by auto
    }
    then have  $\bigcup T \neq 0$  by auto
    then obtain R where  $R \in \bigcup T$  by blast
    ultimately have  $\bigcup T = \{R\}$  using lepoll_1_is_sing by auto
    moreover
    have  $T \subseteq \text{Pow}(\bigcup T)$  by auto
    ultimately have  $T \subseteq \text{Pow}(\{R\})$  by auto
    then have  $T \subseteq \{0, \{R\}\}$  by blast
    moreover
    with 'T{is a topology}' have  $0 \in T \bigcup T \in T$  using IsATopology_def by
auto
    moreover
    note ' $\bigcup T = \{R\}$ '
    ultimately have  $T = \{0, \bigcup T\}$  by auto
  }
  ultimately have  $T = \{0, \bigcup T\}$  by auto
}
then show A {is in the spectrum of}  $(\lambda T. T = \{0, \bigcup T\})$  using Spec_def by
auto
qed

theorem (in topology0) anti_indiscrete:
  shows (T{is anti-}  $(\lambda T. T = \{0, \bigcup T\})$ )  $\longleftrightarrow$  T{is  $T_0$ }
proof
  assume T{is  $T_0$ }
  {
    fix A
    assume  $A \in \text{Pow}(\bigcup T)$  T{restricted to}  $A = \{0, \bigcup (T\text{restricted to } A)\}$ 
    then have un:  $\bigcup (T\text{restricted to } A) = A$  T{restricted to}  $A = \{0, A\}$  using
RestrictedTo_def by auto
    from 'T{is  $T_0$ }' ' $A \in \text{Pow}(\bigcup T)$ ' have  $(T\text{restricted to } A)\{is\ } T_0$  using
T0_here by auto
    {
      assume  $A = 0$ 
      then have  $A \approx 0$  by auto
      then have  $A \lesssim 1$  using empty_lepollI eq_lepoll_trans by auto
    }
    moreover
    {
      assume  $A \neq 0$ 
      then obtain E where  $E \in A$  by blast
      {
        fix y

```

```

      assume  $y \in A \wedge y \neq E$ 
      with 'E ∈ A' un have  $y \in \bigcup (T \{ \text{restricted to} \} A) \wedge E \in \bigcup (T \{ \text{restricted to} \} A)$ 
by auto
      with '(T {restricted to} A) {is T0} 'y ≠ E' have  $\exists U \in (T \{ \text{restricted to} \} A). (E \in U \wedge y \notin U) \vee (E \notin U \wedge y \in U)$ 
      unfolding isT0_def by blast
      then obtain U where  $U \in (T \{ \text{restricted to} \} A) \wedge (E \in U \wedge y \notin U) \vee (E \notin U \wedge y \in U)$ 
by auto
      with 'T {restricted to} A = {0, A}' have  $U = 0 \vee U = A$  by auto
      with '(E ∈ U ∧ y ∉ U) ∨ (E ∉ U ∧ y ∈ U) 'y ∈ A' 'E ∈ A' have False by auto
    }
    then have  $\forall y \in A. y = E$  by auto
    with 'E ∈ A' have  $A = \{E\}$  by blast
    then have  $A \approx 1$  using singleton_eqpoll_1 by auto
    then have  $A \lesssim 1$  using eqpoll_imp_lepoll by auto
  }
  ultimately have  $A \lesssim 1$  by auto
  then have  $A \{ \text{is in the spectrum of} \} (\lambda T. T = \{0, \bigcup T\})$  using indiscrete_spectrum
by auto
}
then show  $T \{ \text{is anti-} \} (\lambda T. T = \{0, \bigcup T\})$  unfolding antiProperty_def by
auto
next
  assume  $T \{ \text{is anti-} \} (\lambda T. T = \{0, \bigcup T\})$ 
  then have  $\forall A \in \text{Pow}(\bigcup T). (T \{ \text{restricted to} \} A) = \{0, \bigcup (T \{ \text{restricted to} \} A)\}$ 
 $\longrightarrow (A \{ \text{is in the spectrum of} \} (\lambda T. T = \{0, \bigcup T\}))$  using antiProperty_def
by auto
  then have  $\forall A \in \text{Pow}(\bigcup T). (T \{ \text{restricted to} \} A) = \{0, \bigcup (T \{ \text{restricted to} \} A)\}$ 
 $\longrightarrow A \lesssim 1$  using indiscrete_spectrum by auto
  moreover
  have  $\forall A \in \text{Pow}(\bigcup T). \bigcup (T \{ \text{restricted to} \} A) = A$  unfolding RestrictedTo_def
by auto
  ultimately have  $\text{reg}: \forall A \in \text{Pow}(\bigcup T). (T \{ \text{restricted to} \} A) = \{0, A\} \longrightarrow A \lesssim 1$ 
by auto
  {
    fix x y
    assume  $x \in \bigcup T \wedge y \in \bigcup T \wedge x \neq y$ 
    {
      assume  $\forall U \in T. (x \in U \wedge y \in U) \vee (x \notin U \wedge y \notin U)$ 
      then have  $T \{ \text{restricted to} \} \{x, y\} \subseteq \{0, \{x, y\}\}$  unfolding RestrictedTo_def
by auto
      moreover
      from 'x ∈ ⋃ T' 'y ∈ ⋃ T' have  $\text{emp}: 0 \in T \{x, y\} \cap 0 = 0$  and  $\text{tot}: \{x, y\} = \{x, y\} \cap \bigcup T$ 
      using topSpaceAssum empty_open IsATopology_def by auto
      from emp have  $0 \in T \{ \text{restricted to} \} \{x, y\}$  unfolding RestrictedTo_def
by auto
      moreover
      from tot have  $\{x, y\} \in T \{ \text{restricted to} \} \{x, y\}$  unfolding RestrictedTo_def
by auto
    }
  }

```

```

ultimately have T{restricted to}{x,y}={0,{x,y}} by auto
with reg 'x∈⋃T' 'y∈⋃T' have {x,y}≲1 by auto
moreover
have x∈{x,y} by auto
ultimately have {x,y}={x} using lepoll_1_is_sing[of {x,y}x] by auto
moreover
have y∈{x,y} by auto
ultimately have y∈{x} by auto
then have y=x by auto
then have False using 'x≠y' by auto
}
then have ∃U∈T. (x∉U∨y∉U)∧(x∈U∨y∈U) by auto
then have ∃U∈T. (x∈U∧y∉U)∨(x∉U∧y∈U) by auto
}
then have ∀x y. x∈⋃T∧y∈⋃T∧ x≠y ⟶ (∃U∈T. (x∈U∧y∉U)∨(y∈U∧x∉U))
by auto
then show T {is T0} using isT0_def by auto
qed

```

The conclusion is that being  $T_0$  is just the opposite to being indiscrete.

Next, let's compute the anti- $T_i$  for  $i = 1, 2, 3$  or  $4$ . Surprisingly, they are all the same. Meaning, that the total negation of  $T_1$  is enough to negate all of these axioms.

**theorem anti\_T1:**

shows  $(T\{\text{is anti-}\}\text{isT1}) \longleftrightarrow (\text{IsLinOrder}(T, \{\langle U, V \rangle \in \text{Pow}(\bigcup T) \times \text{Pow}(\bigcup T). U \subseteq V\}))$

**proof**

```

assume T{is anti-}isT1
let r={⟨U,V⟩∈Pow(⋃T)×Pow(⋃T). U⊆V}
have antisym(r) unfolding antisym_def by auto
moreover
have trans(r) unfolding trans_def by auto
moreover
{
  fix A B
  assume A∈TB∈T
  {
    assume ¬(A⊆B∨B⊆A)
    then have A-B≠0B-A≠0 by auto
    then obtain x y where x∈Ax∉By∈By∉A x≠y by blast
    then have {x,y}∩A={x}{x,y}∩B={y} by auto
    moreover
    from 'A∈T' 'B∈T' have {x,y}∩A∈T{restricted to}{x,y}{x,y}∩B∈T{restricted
to}{x,y} unfolding
      RestrictedTo_def by auto
    ultimately have open_set:{x}∈T{restricted to}{x,y}{y}∈T{restricted
to}{x,y} by auto
    have x∈⋃Ty∈⋃T using 'A∈T' 'B∈T' 'x∈A' 'y∈B' by auto

```

```

    then have sub: {x,y} ∈ Pow(⋃ T) by auto
    then have tot: ⋃ (T{restricted to}{x,y}) = {x,y} unfolding RestrictedTo_def
by auto
  {
    fix s t
    assume s ∈ ⋃ (T{restricted to}{x,y}) t ∈ ⋃ (T{restricted to}{x,y}) s ≠ t
    with tot have s ∈ {x,y} t ∈ {x,y} s ≠ t by auto
    then have (s=x ∧ t=y) ∨ (s=y ∧ t=x) by auto
    with open_set have ∃ U ∈ (T{restricted to}{x,y}). s ∈ U ∧ t ∉ U using
'x ≠ y' by auto
  }
  then have (T{restricted to}{x,y}){is T1} unfolding isT1_def by
auto
  with sub 'T{is anti-}isT1' tot have {x,y} {is in the spectrum of}isT1
using antiProperty_def
  by auto
  then have {x,y} ≲ 1 using T1_spectrum by auto
  moreover
  have x ∈ {x,y} by auto
  ultimately have {x} = {x,y} using lepoll_1_is_sing[of {x,y}x] by auto
  moreover
  have y ∈ {x,y} by auto
  ultimately
  have y ∈ {x} by auto
  then have x=y by auto
  then have False using 'x ∈ A' 'y ∉ A' by auto
}
  then have A ⊆ B ∨ B ⊆ A by auto
}
  then have r {is total on}T using IsTotal_def by auto
  ultimately
  show IsLinOrder(T,r) using IsLinOrder_def by auto
next
  assume IsLinOrder(T, {(U,V) ∈ Pow(⋃ T) × Pow(⋃ T). U ⊆ V})
  then have ordTot: ∀ S ∈ T. ∀ B ∈ T. S ⊆ B ∨ B ⊆ S unfolding IsLinOrder_def IsTotal_def
by auto
  {
    fix A
    assume A ∈ Pow(⋃ T) and T1: (T{restricted to}A) {is T1}
    then have tot: ⋃ (T{restricted to}A) = A unfolding RestrictedTo_def by
auto
  }
  {
    fix U V
    assume U ∈ T{restricted to}A ∨ V ∈ T{restricted to}A
    then obtain AU AV where AU ∈ T ∨ V ∈ T = A ∩ AU ∨ V ∈ T = A ∩ AV unfolding RestrictedTo_def
by auto
  }
  with ordTot have U ⊆ V ∨ V ⊆ U by auto
}
  then have ordTotSub: ∀ S ∈ T{restricted to}A. ∀ B ∈ T{restricted to}A.

```

```

S⊆BVBS by auto
{
  assume A=0
  then have A≈0 by auto
  moreover
  have 0≤1 using empty_lepollI by auto
  ultimately have A≤1 using eq_lepoll_trans by auto
  then have A{is in the spectrum of}isT1 using T1_spectrum by auto
}
moreover
{
  assume A≠0
  then obtain t where t∈A by blast
  {
    fix y
    assume y∈A y≠t
    with 't∈A' tot T1 obtain U where U∈(T{restricted to}A) y∈U t∉U
  }
  unfolding isT1_def
  by auto
  from 'y≠t' have t≠y by auto
  with 'y∈A' 't∈A' tot T1 obtain V where V∈(T{restricted to}A) t∈V y∉V
  unfolding isT1_def
  by auto
  with 'y∈U' 't∉U' have ¬(U⊆V∨V⊆U) by auto
  with ordTotSub 'U∈(T{restricted to}A)' 'V∈(T{restricted to}A)'
  have False by auto
}
then have ∀y∈A. y=t by auto
with 't∈A' have A={t} by blast
then have A≈1 using singleton_eqpoll_1 by auto
then have A≤1 using eqpoll_imp_lepoll by auto
then have A{is in the spectrum of}isT1 using T1_spectrum by auto
}
ultimately
have A{is in the spectrum of}isT1 by auto
}
then show T{is anti-}isT1 using antiProperty_def by auto
qed

corollary linordtop_here:
  shows (λT. IsLinOrder(T, {⟨U,V⟩∈Pow(⋃T)×Pow(⋃T). U⊆V})) {is hereditary}
  using anti_T1 anti_here[of isT1] by auto

theorem (in topology0) anti_T4:
  shows (T{is anti-}isT4) ⟷ (IsLinOrder(T, {⟨U,V⟩∈Pow(⋃T)×Pow(⋃T).
  U⊆V}))
proof
  assume T{is anti-}isT4
  let r={⟨U,V⟩∈Pow(⋃T)×Pow(⋃T). U⊆V}

```

```

have antisym(r) unfolding antisym_def by auto
moreover
have trans(r) unfolding trans_def by auto
moreover
{
  fix A B
  assume A ∈ T B ∈ T
  {
    assume ¬(A ⊆ B ∨ B ⊆ A)
    then have A - B ≠ 0 B - A ≠ 0 by auto
    then obtain x y where x ∈ A x ∉ B y ∈ B y ∉ A x ≠ y by blast
    then have {x, y} ∩ A = {x} {x, y} ∩ B = {y} by auto
    moreover
    from 'A ∈ T' 'B ∈ T' have {x, y} ∩ A ∈ T {restricted to} {x, y} {x, y} ∩ B ∈ T {restricted
to} {x, y} unfolding
      RestrictedTo_def by auto
    ultimately have open_set: {x} ∈ T {restricted to} {x, y} {y} ∈ T {restricted
to} {x, y} by auto
    have x ∈ ⋃ Ty ∈ ⋃ T using 'A ∈ T' 'B ∈ T' 'x ∈ A' 'y ∈ B' by auto
    then have sub: {x, y} ∈ Pow(⋃ T) by auto
    then have tot: ⋃ (T {restricted to} {x, y}) = {x, y} unfolding RestrictedTo_def
by auto
    {
      fix s t
      assume s ∈ ⋃ (T {restricted to} {x, y}) t ∈ ⋃ (T {restricted to} {x, y}) s ≠ t
      with tot have s ∈ {x, y} t ∈ {x, y} s ≠ t by auto
      then have (s = x ∧ t = y) ∨ (s = y ∧ t = x) by auto
      with open_set have ∃ U ∈ (T {restricted to} {x, y}). s ∈ U ∧ t ∉ U using
'x ≠ y' by auto
    }
    then have (T {restricted to} {x, y}) {is T1} unfolding isT1_def by
auto
    moreover
    {
      fix s
      assume AS: s {is closed in} (T {restricted to} {x, y})
      {
        fix t
        assume AS2: t {is closed in} (T {restricted to} {x, y}) s ∩ t = 0
        have (T {restricted to} {x, y}) {is a topology} using Top_1_L4 by
auto
        with tot have 0 ∈ (T {restricted to} {x, y}) {x, y} ∈ (T {restricted
to} {x, y}) using empty_open
          union_open [where A = T {restricted to} {x, y}] by auto
        moreover
        note open_set
        moreover
        have T {restricted to} {x, y} ⊆ Pow(⋃ (T {restricted to} {x, y})) by
blast

```

```

    with tot have  $T\{\text{restricted to}\{x,y\}\subseteq\text{Pow}(\{x,y\})$  by auto
    ultimately have  $T\{\text{restricted to}\{x,y\}=\{0,\{x\},\{y\},\{x,y\}\}$  by blast
    then have  $P:T\{\text{restricted to}\{x,y\}=\text{Pow}(\{x,y\})$  apply simp by
blast
    have  $S:\{A\in\text{Pow}(\{x,y\}). A\{\text{is closed in}\}(T\{\text{restricted to}\{x,y\})\}=T\{\text{restricted to}\{x,y\}$ 
    unfolding IsClosed_def
    apply (simp only:tot) apply (simp only:P) by auto
    from AS AS2(1) have  $s\in\text{Pow}(\{x,y\})$   $t\in\text{Pow}(\{x,y\})$  unfolding IsClosed_def
using tot by auto
    moreover
    note AS2(1) AS
    ultimately have  $s\in\{A\in\text{Pow}(\{x,y\}). A\{\text{is closed in}\}(T\{\text{restricted to}\{x,y\})\}$ 
     $t\in\{A\in\text{Pow}(\{x,y\}). A\{\text{is closed in}\}(T\{\text{restricted to}\{x,y\})\}$ 
    by auto
    with S AS2(2) have  $s\in T\{\text{restricted to}\{x,y\}$   $t\in T\{\text{restricted to}\{x,y\}$   $s\cap t=0$ 
by auto
    then have  $\exists U\in(T\{\text{restricted to}\{x,y\}). \exists V\in(T\{\text{restricted to}\{x,y\}).$ 
 $s\subseteq U\wedge t\subseteq V\wedge U\cap V=0$  by auto
    }
    then have  $\forall t. t\{\text{is closed in}\}(T\{\text{restricted to}\{x,y\})\wedge s\cap t=0 \longrightarrow$ 
 $(\exists U\in(T\{\text{restricted to}\{x,y\}). \exists V\in(T\{\text{restricted to}\{x,y\}). s\subseteq U\wedge t\subseteq V\wedge U\cap V=0)$ 
    by auto
    }
    then have  $\forall s. s\{\text{is closed in}\}(T\{\text{restricted to}\{x,y\}) \longrightarrow (\forall t. t\{\text{is closed in}\}(T\{\text{restricted to}\{x,y\})\wedge s\cap t=0 \longrightarrow (\exists U\in(T\{\text{restricted to}\{x,y\}). \exists V\in(T\{\text{restricted to}\{x,y\}). s\subseteq U\wedge t\subseteq V\wedge U\cap V=0))$ 
    by auto
    then have  $(T\{\text{restricted to}\{x,y\})\{\text{is normal}\}$  using IsNormal_def
by auto
    ultimately have  $(T\{\text{restricted to}\{x,y\})\{\text{is } T_4\}$  using isT4_def by
auto
    with sub 'T{is anti-}isT4' tot have  $\{x,y\}\{\text{is in the spectrum of}\}$ isT4
using antiProperty_def
    by auto
    then have  $\{x,y\}\lesssim 1$  using T4_spectrum by auto
    moreover
    have  $x\in\{x,y\}$  by auto
    ultimately have  $\{x\}=\{x,y\}$  using lepoll_1_is_sing[of  $\{x,y\}x$ ] by auto
    moreover
    have  $y\in\{x,y\}$  by auto
    ultimately
    have  $y\in\{x\}$  by auto
    then have  $x=y$  by auto
    then have False using 'x∈A' 'y∉A' by auto
    }
    then have  $A\subseteq B\vee B\subseteq A$  by auto
    }
    then have  $r\{\text{is total on}\}T$  using IsTotal_def by auto
    ultimately

```

```

    show IsLinOrder(T,r) using IsLinOrder_def by auto
next
  assume IsLinOrder(T, {⟨U,V⟩ ∈ Pow(⋃T) × Pow(⋃T) . U ⊆ V})
  then have T{is anti-}isT1 using anti_T1 by auto
  moreover
  have ∀T. T{is a topology} ⟶ (T{is T4}) ⟶ (T{is T1}) using topology0.T4_is_T3

    topology0.T3_is_T2 T2_is_T1 topology0_def by auto
  moreover
  have ∀A. (A {is in the spectrum of} isT1) ⟶ (A {is in the spectrum
of} isT4) using T1_spectrum T4_spectrum
    by auto
  ultimately show T{is anti-}isT4 using eq_spect_rev_imp_anti[of isT4isT1]
by auto
qed

theorem (in topology0) anti_T3:
  shows (T{is anti-}isT3) ⟷ (IsLinOrder(T,{⟨U,V⟩∈Pow(⋃T)×Pow(⋃T).
U⊆V}))
proof
  assume T{is anti-}isT3
  moreover
  have ∀T. T{is a topology} ⟶ (T{is T4}) ⟶ (T{is T3}) using topology0.T4_is_T3

    topology0_def by auto
  moreover
  have ∀A. (A {is in the spectrum of} isT3) ⟶ (A {is in the spectrum
of} isT4) using T3_spectrum T4_spectrum
    by auto
  ultimately have T{is anti-}isT4 using eq_spect_rev_imp_anti[of isT4isT3]
by auto
  then show IsLinOrder(T,{⟨U,V⟩∈Pow(⋃T)×Pow(⋃T). U⊆V}) using anti_T4
by auto
next
  assume IsLinOrder(T,{⟨U,V⟩∈Pow(⋃T)×Pow(⋃T). U⊆V})
  then have T{is anti-}isT1 using anti_T1 by auto
  moreover
  have ∀T. T{is a topology} ⟶ (T{is T3}) ⟶ (T{is T1}) using
    topology0.T3_is_T2 T2_is_T1 topology0_def by auto
  moreover
  have ∀A. (A {is in the spectrum of} isT1) ⟶ (A {is in the spectrum
of} isT3) using T1_spectrum T3_spectrum
    by auto
  ultimately show T{is anti-}isT3 using eq_spect_rev_imp_anti[of isT3isT1]
by auto
qed

theorem (in topology0) anti_T2:
  shows (T{is anti-}isT2) ⟷ (IsLinOrder(T,{⟨U,V⟩∈Pow(⋃T)×Pow(⋃T).

```



```

 $U \subseteq V$ )))
proof
  assume T{is anti-}isT2
  moreover
  have  $\forall T. T\{\text{is a topology}\} \longrightarrow (T\{\text{is } T_4\}) \longrightarrow (T\{\text{is } T_2\})$  using topology0.T4_is_T3

  topology0.T3_is_T2 topology0_def by auto
  moreover
  have  $\forall A. (A \{\text{is in the spectrum of}\} \text{isT2}) \longrightarrow (A \{\text{is in the spectrum of}\} \text{isT4})$  using T2_spectrum T4_spectrum
  by auto
  ultimately have T{is anti-}isT4 using eq_spect_rev_imp_anti[of isT4isT2]
by auto
  then show IsLinOrder( $T, \{\langle U, V \rangle \in \text{Pow}(\bigcup T) \times \text{Pow}(\bigcup T). U \subseteq V\}$ ) using anti_T4
by auto
next
  assume IsLinOrder( $T, \{\langle U, V \rangle \in \text{Pow}(\bigcup T) \times \text{Pow}(\bigcup T). U \subseteq V\}$ )
  then have T{is anti-}isT1 using anti_T1 by auto
  moreover
  have  $\forall T. T\{\text{is a topology}\} \longrightarrow (T\{\text{is } T_2\}) \longrightarrow (T\{\text{is } T_1\})$  using T2_is_T1
by auto
  moreover
  have  $\forall A. (A \{\text{is in the spectrum of}\} \text{isT1}) \longrightarrow (A \{\text{is in the spectrum of}\} \text{isT2})$  using T1_spectrum T2_spectrum
  by auto
  ultimately show T{is anti-}isT2 using eq_spect_rev_imp_anti[of isT2isT1]
by auto
qed

lemma linord_spectrum:
  shows  $(A \{\text{is in the spectrum of}\} (\lambda T. \text{IsLinOrder}(T, \{\langle U, V \rangle \in \text{Pow}(\bigcup T) \times \text{Pow}(\bigcup T). U \subseteq V\}))) \longleftrightarrow A \lesssim 1$ 
proof
  assume  $A \{\text{is in the spectrum of}\} (\lambda T. \text{IsLinOrder}(T, \{\langle U, V \rangle \in \text{Pow}(\bigcup T) \times \text{Pow}(\bigcup T). U \subseteq V\})))$ 
  then have reg:  $\forall T. T\{\text{is a topology}\} \wedge \bigcup T \approx A \longrightarrow \text{IsLinOrder}(T, \{\langle U, V \rangle \in \text{Pow}(\bigcup T) \times \text{Pow}(\bigcup T). U \subseteq V\})$ 
  using Spec_def by auto
  {
    assume  $A = 0$ 
    moreover
    have  $0 \lesssim 1$  using empty_lepollI by auto
    ultimately have  $A \lesssim 1$  using eq_lepoll_trans by auto
  }
  moreover
  {
    assume  $A \neq 0$ 
    then obtain x where  $x \in A$  by blast
    moreover

```

```

{
  fix y
  assume y ∈ A
  have Pow(A) {is a topology} using Pow_is_top by auto
  moreover
  have  $\bigcup \text{Pow}(A) = A$  by auto
  then have  $\bigcup \text{Pow}(A) \approx A$  by auto
  note reg
  ultimately have IsLinOrder(Pow(A), {⟨U, V⟩ ∈ Pow( $\bigcup \text{Pow}(A)$ ) × Pow( $\bigcup \text{Pow}(A)$ ) .
U ⊆ V}) by auto
  then have IsLinOrder(Pow(A), {⟨U, V⟩ ∈ Pow(A) × Pow(A) . U ⊆ V}) by auto
  with 'x ∈ A' 'y ∈ A' have {x} ⊆ {y} ∨ {y} ⊆ {x} unfolding IsLinOrder_def
IsTotal_def by auto
  then have x = y by auto
}
ultimately have A = {x} by blast
then have A ≈ 1 using singleton_eqpoll_1 by auto
then have A ≲ 1 using eqpoll_imp_lepoll by auto
}
ultimately show A ≲ 1 by auto
next
  assume A ≲ 1
  then have ind: A {is in the spectrum of} (λ T. T = {0,  $\bigcup T$ }) using indiscrete_spectrum
by auto
  {
    fix T
    assume AS: T {is a topology} T = {0,  $\bigcup T$ }
    have trans({⟨U, V⟩ ∈ Pow( $\bigcup T$ ) × Pow( $\bigcup T$ ) . U ⊆ V}) unfolding trans_def by
auto
    moreover
    have antisym({⟨U, V⟩ ∈ Pow( $\bigcup T$ ) × Pow( $\bigcup T$ ) . U ⊆ V}) unfolding antisym_def
by auto
    moreover
    have {⟨U, V⟩ ∈ Pow( $\bigcup T$ ) × Pow( $\bigcup T$ ) . U ⊆ V} {is total on} T unfolding IsTotal_def
using AS(2) apply (auto)
    proof-
      fix c b x xa
      assume c ∈ T b ∈ T x ∈ b x a ∈ c
      with AS(2) have b ∈ {0,  $\bigcup T$ } b ≠ 0 by auto
      then have b =  $\bigcup T$  by auto
      with 'xa ∈ c' 'c ∈ T' show xa ∈ b by auto
    qed
    ultimately have IsLinOrder(T, {⟨U, V⟩ ∈ Pow( $\bigcup T$ ) × Pow( $\bigcup T$ ) . U ⊆ V}) un-
folding IsLinOrder_def by auto
  }
  then have  $\forall T. T \text{ {is a topology}} \longrightarrow T = \{0, \bigcup T\} \longrightarrow \text{IsLinOrder}(T,$ 
{⟨U, V⟩ ∈ Pow( $\bigcup T$ ) × Pow( $\bigcup T$ ) . U ⊆ V}) by auto
  then show A {is in the spectrum of} (λ T. IsLinOrder(T, {⟨U, V⟩ ∈ Pow( $\bigcup T$ ) × Pow( $\bigcup T$ ) .
U ⊆ V}))

```

```

    using P_imp_Q_spec_inv[of  $\lambda T. T = \{0, \bigcup T\} \lambda T. \text{IsLinOrder}(T, \{(U, V) \in \text{Pow}(\bigcup T) \times \text{Pow}(\bigcup T). U \subseteq V\})$ ]]
    ind by auto
qed

theorem (in topology0) anti_linord:
  shows ( $T \{ \text{is anti-} \} (\lambda T. \text{IsLinOrder}(T, \{(U, V) \in \text{Pow}(\bigcup T) \times \text{Pow}(\bigcup T). U \subseteq V\})) \longleftrightarrow T \{ \text{is } T_1 \}$ )
proof
  assume AS:  $T \{ \text{is anti-} \} (\lambda T. \text{IsLinOrder}(T, \{(U, V) \in \text{Pow}(\bigcup T) \times \text{Pow}(\bigcup T). U \subseteq V\}))$ 
  {
    assume  $\neg(T \{ \text{is } T_1 \})$ 
    then obtain x y where  $x \in \bigcup T, y \in \bigcup T, x \neq y, \forall U \in T. x \notin U \vee y \notin U$  unfolding isT1_def
  by auto
    {
      assume  $\{x\} \in T \{ \text{restricted to} \} \{x, y\}$ 
      then obtain U where  $U \in T, \{x\} = \{x, y\} \cap U$  unfolding RestrictedTo_def
    by auto
      moreover
      have  $x \in \{x\}$  by auto
      ultimately have  $U \in T, x \in U$  by auto
      moreover
      {
        assume  $y \in U$ 
        then have  $y \in \{x, y\} \cap U$  by auto
        with ' $\{x\} = \{x, y\} \cap U$ ' have  $y \in \{x\}$  by auto
        with ' $x \neq y$ ' have False by auto
      }
      then have  $y \notin U$  by auto
      moreover
      note ' $\forall U \in T. x \notin U \vee y \notin U$ '
      ultimately have False by auto
    }
    then have  $\{x\} \notin T \{ \text{restricted to} \} \{x, y\}$  by auto
    moreover
    have tot:  $\bigcup (T \{ \text{restricted to} \} \{x, y\}) = \{x, y\}$  using ' $x \in \bigcup T, y \in \bigcup T$ ' unfolding RestrictedTo_def by auto
    moreover
    have  $T \{ \text{restricted to} \} \{x, y\} \subseteq \text{Pow}(\bigcup (T \{ \text{restricted to} \} \{x, y\}))$  by auto
    ultimately have  $T \{ \text{restricted to} \} \{x, y\} \subseteq \text{Pow}(\{x, y\}) - \{\{x\}\}$  by auto
    moreover
    have  $\text{Pow}(\{x, y\}) = \{0, \{x, y\}, \{x\}, \{y\}\}$  by blast
    ultimately have  $T \{ \text{restricted to} \} \{x, y\} \subseteq \{0, \{x, y\}, \{y\}\}$  by auto
    moreover
    have  $\text{IsLinOrder}(\{0, \{x, y\}, \{y\}\}, \{(U, V) \in \text{Pow}(\{x, y\}) \times \text{Pow}(\{x, y\}). U \subseteq V\})$ 
    unfolding IsLinOrder_def antisym_def trans_def IsTotal_def apply
  safe by auto
    ultimately have  $\text{IsLinOrder}(T \{ \text{restricted to} \} \{x, y\}, \{(U, V) \in \text{Pow}(\{x, y\}) \times \text{Pow}(\{x, y\}). U \subseteq V\})$ 
    using ord_linear_subset

```

```

      by auto
      with tot have IsLinOrder(T{restricted to}{x,y},{(U,V)∈Pow(⋃ (T{restricted
to}{x,y}))×Pow(⋃ (T{restricted to}{x,y})). U⊆V})
      by auto
      then have IsLinOrder(T{restricted to}{x,y},Collect(Pow(⋃ (T {restricted
to}{x,y})) × Pow(⋃ (T {restricted to}{x,y})), split(op ⊆))) by auto
      moreover
      from 'x∈⋃T' 'y∈⋃T' have {x,y}∈Pow(⋃T) by auto
      moreover
      note AS
      ultimately have {x,y}{is in the spectrum of}(λT. IsLinOrder(T,{(U,V)∈Pow(⋃T)×Pow(⋃T.
U⊆V})) unfolding antiProperty_def
      by simp
      then have {x,y}≲1 using linord_spectrum by auto
      moreover
      have x∈{x,y} by auto
      ultimately have {x}={x,y} using lepoll_1_is_sing[of {x,y}x] by auto
      moreover
      have y∈{x,y} by auto
      ultimately
      have y∈{x} by auto
      then have x=y by auto
      then have False using 'x≠y' by auto
    }
    then show T {is T1} by auto
  next
    assume T1:T {is T1}
    {
      fix A
      assume A_def:A∈Pow(⋃T)IsLinOrder((T{restricted to}A) ,(U,V)∈Pow(⋃ (T{restricted
to}A))×Pow(⋃ (T{restricted to}A)). U⊆V})
      {
        fix x
        assume AS1:x∈A
        {
          fix y
          assume AS:y∈Ax≠y
          with AS1 have {x,y}∈Pow(⋃T) using 'A∈Pow(⋃T)' by auto
          from 'x∈A' 'y∈A' have {x,y}∈Pow(A) by auto
          from '{x,y}∈Pow(⋃T)' have T11:(T{restricted to}{x,y}){is T1}
        }
      }
    }
  using T1_here T1 by auto
  moreover
  have tot:⋃ (T{restricted to}{x,y})={x,y} unfolding RestrictedTo_def
  using '{x,y}∈Pow(⋃T)' by auto
  moreover
  note AS(2)
  ultimately obtain U where x∈Uy∉UU∈(T{restricted to}{x,y}) un-
folding isT1_def by auto
  moreover

```

```

      from AS(2) tot T11 obtain V where  $y \in Vx \neq VV \in (T\{\text{restricted to}\}\{x,y\})$ 
    unfolding isT1_def by auto
      ultimately have  $x \in U - Vy \in V - UU \in (T\{\text{restricted to}\}\{x,y\}) V \in (T\{\text{restricted to}\}\{x,y\})$  by auto
      then have  $\neg(U \subseteq V \vee V \subseteq U) U \in (T\{\text{restricted to}\}\{x,y\}) V \in (T\{\text{restricted to}\}\{x,y\})$  by auto
      then have  $\neg(\langle U, V \rangle \in \text{Pow}(\bigcup (T\{\text{restricted to}\}\{x,y\})) \times \text{Pow}(\bigcup (T\{\text{restricted to}\}\{x,y\}))) . U \subseteq V \}$  {is total on}  $(T\{\text{restricted to}\}\{x,y\})$ 
      unfolding IsTotal_def by auto
      then have  $\neg(\text{IsLinOrder}((T\{\text{restricted to}\}\{x,y\}), \{\langle U, V \rangle \in \text{Pow}(\bigcup (T\{\text{restricted to}\}\{x,y\})) \times \text{Pow}(\bigcup (T\{\text{restricted to}\}\{x,y\})) . U \subseteq V\}))$ 
      unfolding IsLinOrder_def by auto
    moreover
    {
      have  $(T\{\text{restricted to}\}A)$  {is a topology} using Top_1_L4 by
    auto
      moreover
      note A_def(2) linordtop_here
      ultimately have  $\forall B \in \text{Pow}(\bigcup (T\{\text{restricted to}\}A)) . \text{IsLinOrder}((T\{\text{restricted to}\}A)\{\text{restricted to}\}B, \{\langle U, V \rangle \in \text{Pow}(\bigcup ((T\{\text{restricted to}\}A)\{\text{restricted to}\}B)) \times \text{Pow}(\bigcup ((T\{\text{restricted to}\}A)\{\text{restricted to}\}B)) . U \subseteq V\})$ 
      unfolding IsHer_def by auto
      moreover
      have  $\text{tot} : \bigcup (T\{\text{restricted to}\}A) = A$  unfolding RestrictedTo_def
    using 'A ∈ Pow(⋃ T)' by auto
      ultimately have  $\forall B \in \text{Pow}(A) . \text{IsLinOrder}((T\{\text{restricted to}\}A)\{\text{restricted to}\}B, \{\langle U, V \rangle \in \text{Pow}(\bigcup ((T\{\text{restricted to}\}A)\{\text{restricted to}\}B)) \times \text{Pow}(\bigcup ((T\{\text{restricted to}\}A)\{\text{restricted to}\}B)) . U \subseteq V\})$  by auto
      moreover
      have  $\forall B \in \text{Pow}(A) . (T\{\text{restricted to}\}A)\{\text{restricted to}\}B = T\{\text{restricted to}\}B$  using subspace_of_subspace 'A ∈ Pow(⋃ T)' by auto
      ultimately
      have  $\forall B \in \text{Pow}(A) . \text{IsLinOrder}((T\{\text{restricted to}\}B), \{\langle U, V \rangle \in \text{Pow}(\bigcup ((T\{\text{restricted to}\}A)\{\text{restricted to}\}B)) \times \text{Pow}(\bigcup ((T\{\text{restricted to}\}A)\{\text{restricted to}\}B)) . U \subseteq V\})$  by auto
      moreover
      have  $\forall B \in \text{Pow}(A) . \bigcup ((T\{\text{restricted to}\}A)\{\text{restricted to}\}B) = B$  using 'A ∈ Pow(⋃ T)' unfolding RestrictedTo_def by auto
      ultimately have  $\forall B \in \text{Pow}(A) . \text{IsLinOrder}((T\{\text{restricted to}\}B), \{\langle U, V \rangle \in \text{Pow}(B) \times \text{Pow}(B) . U \subseteq V\})$  by auto
      with '{x,y} ∈ Pow(A)' have  $\text{IsLinOrder}((T\{\text{restricted to}\}\{x,y\}), \{\langle U, V \rangle \in \text{Pow}(\{x,y\}) \times \text{Pow}(\{x,y\}) . U \subseteq V\})$  by auto
    }
      ultimately have False using tot by auto
    }
  then have  $A = \{x\}$  using AS1 by auto
  then have  $A \approx 1$  using singleton_eqpoll_1 by auto
  then have  $A \lesssim 1$  using eqpoll_imp_lepoll by auto
  then have  $A$  {is in the spectrum of}  $(\lambda T . \text{IsLinOrder}(T, \{\langle U, V \rangle \in \text{Pow}(\bigcup T) \times \text{Pow}(\bigcup T) .$ 

```

```

U⊆V})) using linord_spectrum
      by auto
    }
  moreover
  {
    assume A=0
    then have A≈0 by auto
    moreover
    have 0≲1 using empty_lepollI by auto
    ultimately have A≲1 using eq_lepoll_trans by auto
    then have A{is in the spectrum of}(λT. IsLinOrder(T,{⟨U,V⟩∈Pow(⋃T)×Pow(⋃T)}.
U⊆V})) using linord_spectrum
      by auto
    }
    ultimately have A{is in the spectrum of}(λT. IsLinOrder(T,{⟨U,V⟩∈Pow(⋃T)×Pow(⋃T)}.
U⊆V})) by blast
  }
  then show T{is anti-}(λT. IsLinOrder(T, {⟨U,V⟩ ∈ Pow(⋃T) × Pow(⋃T)
. U ⊆ V})) unfolding antiProperty_def
    by auto
qed

```

In conclusion,  $T_1$  is also an anti-property.

end

## 52 Topology\_ZF\_6.thy

```
theory Topology_ZF_6 imports Topology_ZF_4 Topology_ZF_2 Topology_ZF_1
```

```
begin
```

This theory deals with the relations between continuous functions and convergence of filters.

### 52.1 Image filter

First of all, we will define the appropriate tools to work with functions and filters together.

**definition**

```
ImageFilter (["_"].._ 98)
  where  $\mathfrak{F}$  {is a filter on}  $X \implies f:X \rightarrow Y \implies f[\mathfrak{F}]..Y \equiv \{A \in \text{Pow}(Y). \exists D \in \{fB . B \in \mathfrak{F}\}. D \subseteq A\}$ 
```

Note that in the previous definition, it is necessary to state  $Y$  as the final set because  $f$  is also a function to every superset of its range.  $X$  can be changed by  $\text{domain}(f)$  without any change in the definition.

**lemma base\_image\_filter:**

```
  assumes  $\mathfrak{F}$  {is a filter on}  $X f:X \rightarrow Y$ 
  shows  $\{fB . B \in \mathfrak{F}\}$  {is a base filter}  $(f[\mathfrak{F}]..Y)$  and  $(f[\mathfrak{F}]..Y)$  {is a filter on}  $Y$ 
```

**proof-**

```
{
  assume  $0 \in \{fB . B \in \mathfrak{F}\}$ 
  then obtain B where  $B \in \mathfrak{F}$  and  $f_B : fB = 0$  by auto
  then have  $B \in \text{Pow}(X)$  using assms(1) IsFilter_def by auto
  then have  $fB = \{fb. b \in B\}$  using image_fun assms(2) by auto
  with  $f_B$  have  $\{fb. b \in B\} = 0$  by auto
  then have  $B = 0$  by auto
  with ' $B \in \mathfrak{F}$ ' have False using IsFilter_def assms(1) by auto
}
then have  $0 \notin \{fB . B \in \mathfrak{F}\}$  by auto
moreover
from assms(1) obtain S where  $S \in \mathfrak{F}$  using IsFilter_def by auto
then have  $fS \in \{fB . B \in \mathfrak{F}\}$  by auto
then have  $nA : \{fB . B \in \mathfrak{F}\} \neq 0$  by auto
moreover
{
  fix A B
  assume  $A \in \{fB . B \in \mathfrak{F}\}$  and  $B \in \{fB . B \in \mathfrak{F}\}$ 
  then obtain AB BB where  $A = fAB$   $B = fBB$   $AB \in \mathfrak{F}$   $BB \in \mathfrak{F}$  by auto
  then have  $A \cap B = (fAB) \cap (fBB)$  by auto
  then have  $f(AB \cap BB) \subseteq A \cap B$  by auto
  moreover
```

```

    with 'AB ∈ ℱ' 'BB ∈ ℱ' have AB ∩ BB ∈ ℱ using IsFilter_def assms(1) by auto
    ultimately have ∃ D ∈ {fB . B ∈ ℱ}. D ⊆ A ∩ B by auto
  }
  then have ∀ A ∈ {fB . B ∈ ℱ}. ∀ B ∈ {fB . B ∈ ℱ}. ∃ D ∈ {fB . B ∈ ℱ}. D ⊆ A ∩ B by auto
  ultimately have sbc: {fB . B ∈ ℱ} {satisfies the filter base condition}
using SatisfiesFilterBase_def
  by auto
moreover
{
  fix t
  assume t ∈ {fB . B ∈ ℱ}
  then obtain B where B ∈ ℱ and im_def: fB = t by auto
  then have B ∈ Pow(X) using assms(1) unfolding IsFilter_def by auto
  with im_def have t = {fx. x ∈ B} using image_fun assms(2) by auto
  with 'B ∈ Pow(X)' have t ⊆ Y using apply_funtype[OF assms(2)] by auto
}
then have nB: {fB . B ∈ ℱ} ⊆ Pow(Y) by auto
ultimately
show {fB . B ∈ ℱ} {is a base filter}(f[ℱ]..Y) unfolding ImageFilter_def[OF
assms]
  using base_unique_filter_set2[of {fB . B ∈ ℱ} Y {A ∈ Pow(Y). ∃ D ∈ {fB . B ∈ ℱ}.
D ⊆ A}] by simp
moreover
note sbc
moreover
{from nA obtain D where D ∈ {fB . B ∈ ℱ} by blast
moreover
with nB have D ⊆ Y by auto
ultimately have Y ∈ {A ∈ Pow(Y). ∃ D ∈ {fB . B ∈ ℱ}. D ⊆ A} by auto}
then have ⋃ {A ∈ Pow(Y). ∃ D ∈ {fB . B ∈ ℱ}. D ⊆ A} = Y by auto
with basic_filter[OF calculation(1)] show (f[ℱ]..Y) {is a filter on}
Y using calculation(2)
  unfolding ImageFilter_def[OF assms] by auto
qed

```

## 52.2 Continuous at a point vs. globally continuous

If a function is continuous, then it is continuous at every point.

**lemma** cont\_global\_imp\_continuous\_x:

```

  fixes x
  assumes IsContinuous(τ1, τ2, f) f ∈ (⋃ τ1) → (⋃ τ2) x ∈ ⋃ τ1
  shows ∀ U ∈ τ2. fx ∈ U → (∃ V ∈ τ1. x ∈ V ∧ fV ⊆ U)

```

**proof-**

```

{
  fix U
  assume AS: U ∈ τ2 fx ∈ U
  then have f-(U) ∈ τ1 using assms(1) IsContinuous_def by auto
  moreover
  have f(f-(U)) ⊆ U using function_image_vimage fun_is_fun assms(2) by

```



```

auto
  moreover
    from AS(2) have  $x \in f^{-1}U$  using func1_1_L15[OF assms(2)] assms(3) by
auto
  ultimately have  $\exists V \in \tau_1. x \in V \wedge fV \subseteq U$  by auto
}
then show  $\forall U \in \tau_2. f^{-1}U \longrightarrow (\exists V \in \tau_1. x \in V \wedge fV \subseteq U)$  by auto
qed

lemma ccontinuous_all_x_imp_cont_global:
  assumes  $\forall x \in \bigcup \tau_1. \forall U \in \tau_2. f^{-1}U \longrightarrow (\exists V \in \tau_1. x \in V \wedge fV \subseteq U)$   $f \in (\bigcup \tau_1) \rightarrow (\bigcup \tau_2)$ 
   $\tau_1$  {is a topology}
  shows IsContinuous( $\tau_1, \tau_2, f$ )
proof-
{
  fix U
  assume  $U \in \tau_2$ 
  {
    note ' $U \in \tau_2$ '
    moreover
    fix x
    assume AS: $x \in f^{-1}U$ 
    then have  $x \in \bigcup \tau_1$  using func1_1_L6A[OF assms(2)] by auto
    then have  $\forall U \in \tau_2. f^{-1}U \longrightarrow (\exists V \in \tau_1. x \in V \wedge fV \subseteq U)$  using assms(1)
  by auto
    moreover
    from AS have  $f^{-1}U$  using func1_1_L15 assms(2) by auto
    ultimately have  $\exists V \in \tau_1. x \in V \wedge fV \subseteq U$  by auto
    then obtain V where  $V \in \tau_1$   $x \in V$   $fV \subseteq U$  by auto
    moreover
    then have  $V \subseteq \bigcup \tau_1$  by auto
    moreover
    then have  $V \subseteq f^{-1}(fV)$  using func1_1_L9[OF assms(2)] by auto
    ultimately have  $V \subseteq f^{-1}U$  by blast
    with ' $V \in \tau_1$ ' ' $x \in V$ ' have  $\exists V \in \tau_1. x \in V \wedge V \subseteq f^{-1}U$  by auto
  }
  then have  $\forall x \in f^{-1}U. \exists V \in \tau_1. x \in V \wedge V \subseteq f^{-1}U$  by auto
  then have  $f^{-1}(U) \in \tau_1$  using topology0.open_neigh_open topology0_def
  assms(3) by auto
}
then have  $\forall U \in \tau_2. f^{-1}U \in \tau_1$  by auto
then show thesis using IsContinuous_def by auto
qed

```

### 52.3 Continuous functions and filters

Now, let's get to the continuity-filter relation. If the function is continuous; then, if the filter converges to a point, the image filter converges to the image point.

```

lemma (in two_top_spaces0) cont_imp_filter_conver_preserved:
  assumes  $\mathcal{F}$  {is a filter on}  $X_1$   $f$  {is continuous}  $\mathcal{F} \rightarrow F x$  {in}  $\tau_1$ 
  shows  $(f[\mathcal{F}]..X_2) \rightarrow F (fx)$  {in}  $\tau_2$ 
proof-
  have  $x1:x \in X_1$  using assms(3) topology0.FilterConverges_def[OF topol_cntxs_valid(1)]
  assms(1)  $X1\_def$  by auto
  then have  $fx \in \bigcup \tau_2$  using apply_funtype[OF fmapAssum] by simp
  moreover
  {
    fix  $U$ 
    assume  $U \in \text{Pow}(X_2)$   $(fx) \in \text{Interior}(U, \tau_2)$ 
    then have  $xim:x \in f-(\text{Interior}(U, \tau_2))$  and  $sub:f-(\text{Interior}(U, \tau_2)) \in \text{Pow}(X_1)$ 
  using func1_1_L6A[OF fmapAssum] func1_1_L15[OF fmapAssum]  $x1$  by auto
    note sub
    moreover
    have  $\text{Interior}(U, \tau_2) \in \tau_2$  using topology0.Top_2_L2 topol_cntxs_valid(2)
  by auto
    then have  $f-(\text{Interior}(U, \tau_2)) \in \tau_1$  using assms(2) unfolding isContinuous_def
  IsContinuous_def
    by auto
    with  $xim$  have  $x \in \text{Interior}(f-(\text{Interior}(U, \tau_2)), \tau_1)$  using topology0.Top_2_L3
    topol_cntxs_valid(1) by auto
    moreover
    have  $\{U \in \text{Pow}(X_1). x \in \text{Interior}(U, \tau_1)\} \subseteq \mathcal{F}$  using assms(3) topology0.FilterConverges_def[OF
  topol_cntxs_valid(1), of  $\mathcal{F}x$ ]
    assms(1)  $X1\_def$  by auto
    ultimately have  $f-(\text{Interior}(U, \tau_2)) \in \mathcal{F}$  by auto
    moreover
    have  $f(f-(\text{Interior}(U, \tau_2))) \subseteq \text{Interior}(U, \tau_2)$  using function_image_vimage
  fun_is_fun fmapAssum
    by auto
    then have  $f(f-(\text{Interior}(U, \tau_2))) \subseteq U$  using topology0.Top_2_L1 topol_cntxs_valid(2)
  by auto
    ultimately have  $\exists D \in \{fB . B \in \mathcal{F}\}. D \subseteq U$  by auto
  }
  then have  $\forall U \in \text{Pow}(\bigcup \tau_2). (fx) \in \text{Interior}(U, \tau_2) \longrightarrow (\exists D \in \{fB . B \in \mathcal{F}\}. D \subseteq U)$ 
  by auto
  moreover
  have  $\{fB . B \in \mathcal{F}\}$  {is a base filter}  $(f[\mathcal{F}]..X_2)$  and  $(f[\mathcal{F}]..X_2)$  {is a filter
  on}  $(\bigcup \tau_2)$ 
    using base_image_filter[OF assms(1) fmapAssum] unfolding  $X1\_def$   $X2\_def$ 
  by auto
  from topology0.convergence_filter_base2[OF topol_cntxs_valid(2) this(2)
  this(1) calculation(2) calculation(1)] show thesis .
qed

lemma (in two_top_spaces0) filter_conver_preserved_imp_cont:
  assumes  $\forall x \in \bigcup \tau_1. \forall \mathcal{F}. ((\mathcal{F} \text{ {is a filter on} } X_1) \wedge (\mathcal{F} \rightarrow F x \text{ {in} } \tau_1))$ 
 $\longrightarrow ((f[\mathcal{F}]..X_2) \rightarrow F (fx) \text{ {in} } \tau_2)$ 

```

```

    shows f{is continuous}
proof-
  {
    fix x
    assume as2:  $x \in \bigcup \tau_1$ 
    with assms have reg:  $\forall \mathcal{F}. ((\mathcal{F} \text{ {is a filter on}} X_1) \wedge (\mathcal{F} \rightarrow_F x \text{ {in}} \tau_1)) \longrightarrow ((f[\mathcal{F}]..X_2) \rightarrow_F (fx) \text{ {in}} \tau_2)$  by auto
    let Neig =  $\{U \in \text{Pow}(\bigcup \tau_1) . x \in \text{Interior}(U, \tau_1)\}$ 
    {
      fix U
      assume  $U \in \tau_2$   $fx \in U$ 
      then have  $U \in \text{Pow}(\bigcup \tau_2)$   $fx \in \text{Interior}(U, \tau_2)$  using topology0.Top_2_L3 by auto
      moreover
        from topology0.neigh_filter[OF topol_cntxs_valid(1) as2] reg have
         $(f[\text{Neig}]..X_2) \rightarrow_F (fx) \text{ {in}} \tau_2$ 
        by auto
        ultimately have  $U \in (f[\text{Neig}]..X_2)$  using topology0.FilterConverges_def[OF
        topol_cntxs_valid(2) base_image_filter(2)[OF
        topology0.neigh_filter(1)[OF topol_cntxs_valid(1) as2] ]] fmapAssum
        unfolding X1_def X2_def by auto
        moreover
          have  $\{fB . B \in \text{Neig}\} \text{ {is a base filter}} (f[\text{Neig}]..X_2)$  using base_image_filter(1)[OF
          topology0.neigh_filter(1)[OF topol_cntxs_valid(1) as2] ] fmapAssum
        unfolding X1_def X2_def by auto
        ultimately have  $\exists V \in \{fB . B \in \text{Neig}\}. V \subseteq U$  using basic_element_filter
      by blast
      then obtain B where  $B \in \text{Neig}$   $fB \subseteq U$  by auto
      moreover
        have  $\text{Interior}(B, \tau_1) \subseteq B$  using topology0.Top_2_L1 topol_cntxs_valid(1)
      by auto
      then have  $f\text{Interior}(B, \tau_1) \subseteq fB$  by auto
      moreover
        have  $\text{Interior}(B, \tau_1) \in \tau_1$  using topology0.Top_2_L2 topol_cntxs_valid(1)
      by auto
      ultimately
        have  $\exists V \in \tau_1. x \in V \wedge fV \subseteq U$  by force
    }
    then have  $\forall U \in \tau_2. fx \in U \longrightarrow (\exists V \in \tau_1. x \in V \wedge fV \subseteq U)$  by auto
  }
  then have  $\forall x \in \bigcup \tau_1. \forall U \in \tau_2. fx \in U \longrightarrow (\exists V \in \tau_1. x \in V \wedge fV \subseteq U)$  by auto
  then show thesis using ccontinuous_all_x_imp_cont_global fmapAssum
  unfolding X1_def X2_def isContinuous_def using tau1_is_top by auto
qed

end

```



## 53 Topology\_ZF\_7.thy

```
theory Topology_ZF_7 imports Topology_ZF_5
begin
```

### 53.1 Connection Properties

Another type of topological properties are the connection properties. This properties stablish if the space is formed of several pieces or just one.

A space is connected iff there is no clopen set other that the empty set and the total set.

```
definition IsConnected (_{is connected} 70)
  where T {is connected}  $\equiv \forall U. (U \in T \wedge (U \text{ {is closed in } } T)) \longrightarrow U = 0 \vee U = \bigcup T$ 
```

```
lemma indiscrete_connected:
  shows {0,X} {is connected}
  unfolding IsConnected_def IsClosed_def by auto
```

The anti-property of connectedness is called total-diconnectedness.

```
definition IsTotDis (_ {is totally-disconnected} 70)
  where IsTotDis  $\equiv \text{ANTI}(\text{IsConnected})$ 
```

```
lemma conn_spectrum:
  shows (A{is in the spectrum of}IsConnected)  $\longleftrightarrow A \lesssim 1$ 
```

**proof**

```
  assume A{is in the spectrum of}IsConnected
  then have  $\forall T. (T \text{ {is a topology} } \wedge \bigcup T \approx A) \longrightarrow (T \text{ {is connected} })$  using
Spec_def by auto
  moreover
  have Pow(A){is a topology} using Pow_is_top by auto
  moreover
  have  $\bigcup (\text{Pow}(A)) = A$  by auto
  then have  $\bigcup (\text{Pow}(A)) \approx A$  by auto
  ultimately have Pow(A) {is connected} by auto
  {
    assume  $A \neq 0$ 
    then obtain E where  $E \in A$  by blast
    then have  $\{E\} \in \text{Pow}(A)$  by auto
    moreover
    have  $A - \{E\} \in \text{Pow}(A)$  by auto
    ultimately have  $\{E\} \in \text{Pow}(A) \wedge \{E\} \text{ {is closed in } } \text{Pow}(A)$  unfolding IsClosed_def
  by auto
    with 'Pow(A) {is connected}' have  $\{E\} = A$  unfolding IsConnected_def
  by auto
    then have  $A \approx 1$  using singleton_eqpoll_1 by auto
    then have  $A \lesssim 1$  using eqpoll_imp_lepoll by auto
  }
  moreover
```

```

{
  assume A=0
  then have  $A \lesssim 1$  using empty_lepollI[of 1] by auto
}
ultimately show  $A \lesssim 1$  by auto
next
assume  $A \lesssim 1$ 
{
  fix T
  assume T{is a topology}  $\bigcup T \approx A$ 
  {
    assume  $\bigcup T = 0$ 
    with 'T{is a topology}' have T={0} using empty_open by auto
    then have T{is connected} unfolding IsConnected_def by auto
  }
  moreover
  {
    assume  $\bigcup T \neq 0$ 
    moreover
    from ' $A \lesssim 1$ ' ' $\bigcup T \approx A$ ' have  $\bigcup T \lesssim 1$  using eq_lepoll_trans by auto
    ultimately
    obtain E where  $\bigcup T = \{E\}$  using lepoll_1_is_sing by blast
    moreover
    have  $T \subseteq \text{Pow}(\bigcup T)$  by auto
    ultimately have  $T \subseteq \text{Pow}(\{E\})$  by auto
    then have  $T \subseteq \{0, \{E\}\}$  by blast
    with 'T{is a topology}' have  $\{0\} \subseteq T \subseteq \{0, \{E\}\}$  using empty_open
  by auto
  then have T{is connected} unfolding IsConnected_def by auto
  }
  ultimately have T{is connected} by auto
}
then show A{is in the spectrum of}IsConnected unfolding Spec_def by
auto
qed

```

The discrete space is a first example of totally-disconnected space.

```

lemma discrete_tot_dis:
  shows Pow(X) {is totally-disconnected}
proof-
{
  fix A assume A ∈ Pow(X) and con: (Pow(X){restricted to}A){is connected}
  have res: (Pow(X){restricted to}A)=Pow(A) unfolding RestrictedTo_def
using 'A ∈ Pow(X)'
  by blast
  {
    assume A=0
    then have  $A \lesssim 1$  using empty_lepollI[of 1] by auto
    then have A{is in the spectrum of}IsConnected using conn_spectrum

```

```

by auto
}
moreover
{
  assume  $A \neq 0$ 
  then obtain E where  $E \in A$  by blast
  then have  $\{E\} \in \text{Pow}(A)$  by auto
  moreover
  have  $A - \{E\} \in \text{Pow}(A)$  by auto
  ultimately have  $\{E\} \in \text{Pow}(A) \wedge \{E\} \{\text{is closed in}\} \text{Pow}(A)$  unfolding IsClosed_def
by auto
  with con res have  $\{E\} = A$  unfolding IsConnected_def by auto
  then have  $A \approx 1$  using singleton_eqpoll_1 by auto
  then have  $A \lesssim 1$  using eqpoll_imp_lepoll by auto
  then have  $A \{\text{is in the spectrum of}\} \text{IsConnected}$  using conn_spectrum
by auto
}
ultimately have  $A \{\text{is in the spectrum of}\} \text{IsConnected}$  by auto
}
then show thesis unfolding IsTotDis_def antiProperty_def by auto
qed

```

An space is hyperconnected iff every two non-empty open sets meet.

**definition** IsHConnected ( $\_ \{\text{is hyperconnected}\} 90$ )  
 where  $T \{\text{is hyperconnected}\} \equiv \forall U V. U \in T \wedge V \in T \wedge U \cap V = 0 \longrightarrow U = 0 \vee V = 0$

Every hyperconnected space is connected.

```

lemma HConn_imp_Conn:
  assumes  $T \{\text{is hyperconnected}\}$ 
  shows  $T \{\text{is connected}\}$ 
proof-
{
  fix U
  assume  $U \in T$   $\{ \text{is closed in} \} T$ 
  then have  $\bigcup T - U \in T$  using IsClosed_def by auto
  moreover
  have  $(\bigcup T - U) \cap U = 0$  by auto
  moreover
  note assms
  ultimately
  have  $U = 0 \vee (\bigcup T - U) = 0$  using IsHConnected_def by auto
  with 'U ∈ T' have  $U = 0 \vee U = \bigcup T$  by auto
}
then show thesis using IsConnected_def by auto
qed

```

```

lemma Indiscrete_HConn:
  shows  $\{0, X\} \{\text{is hyperconnected}\}$ 
  unfolding IsHConnected_def by auto

```

A first example of an hyperconnected space but not indiscrete, is the cofinite topology on the natural numbers.

```

lemma Cofinite_nat_HConn:
  shows (CoFinite nat){is hyperconnected}
proof-
  {
    fix U V
    assume U∈(CoFinite nat)V∈(CoFinite nat)U∩V=0
    then have eq:(nat-U)≺nat∨U=0(nat-V)≺nat∨V=0 unfolding Cofinite_def
      Cocardinal_def by auto
    from 'U∩V=0' have un:(nat-U)∪(nat-V)=nat by auto
    {
      assume AS:(nat-U)≺nat(nat-V)≺nat
      from un have nat≺nat using less_less_imp_un_less[OF AS InfCard_nat]
by auto
      then have False by auto
    }
    with eq(1,2) have U=0∨V=0 by auto
  }
  then show (CoFinite nat){is hyperconnected} using IsHConnected_def
by auto
qed

```

```

lemma HConn_spectrum:
  shows (A{is in the spectrum of}IsHConnected) ⟷ A≲1
proof
  assume A{is in the spectrum of}IsHConnected
  then have ∀T. (T{is a topology}∧⋃T≈A) ⟶ (T{is hyperconnected})
using Spec_def by auto
  moreover
  have Pow(A){is a topology} using Pow_is_top by auto
  moreover
  have ⋃(Pow(A))=A by auto
  then have ⋃(Pow(A))≈A by auto
  ultimately
  have HC_Pow:Pow(A){is hyperconnected} by auto
  {
    assume A=0
    then have A≲1 using empty_lepollI by auto
  }
  moreover
  {
    assume A≠0
    then obtain e where e∈A by blast
    then have {e}∈Pow(A) by auto
    moreover
    have A-{e}∈Pow(A) by auto
    moreover
    have {e}∩(A-{e})=0 by auto

```



```

    moreover
    note HC_Pow
    ultimately have  $A - \{e\} = 0$  unfolding IsHConnected_def by blast
    with 'e ∈ A' have  $A = \{e\}$  by auto
    then have  $A \approx 1$  using singleton_eqpoll_1 by auto
    then have  $A \lesssim 1$  using eqpoll_imp_lepoll by auto
  }
  ultimately show  $A \lesssim 1$  by auto
next
assume  $A \lesssim 1$ 
{
  fix T
  assume T{is a topology}  $\bigcup T \approx A$ 
  {
    assume  $\bigcup T = 0$ 
    with 'T{is a topology}' have  $T = \{0\}$  using empty_open by auto
    then have T{is hyperconnected} unfolding IsHConnected_def by auto
  }
  moreover
  {
    assume  $\bigcup T \neq 0$ 
    moreover
    from ' $A \lesssim 1$ ' ' $\bigcup T \approx A$ ' have  $\bigcup T \lesssim 1$  using eq_lepoll_trans by auto
    ultimately
    obtain E where  $\bigcup T = \{E\}$  using lepoll_1_is_sing by blast
    moreover
    have  $T \subseteq \text{Pow}(\bigcup T)$  by auto
    ultimately have  $T \subseteq \text{Pow}(\{E\})$  by auto
    then have  $T \subseteq \{0, \{E\}\}$  by blast
    with 'T{is a topology}' have  $\{0\} \subseteq T \subseteq \{0, \{E\}\}$  using empty_open
  by auto
    then have T{is hyperconnected} unfolding IsHConnected_def by auto
  }
  ultimately have T{is hyperconnected} by auto
}
then show A{is in the spectrum of}IsHConnected unfolding Spec_def by
auto
qed

```

In the following results we will show that anti-hyperconnectedness is a separation property between  $T_1$  and  $T_2$ . We will show also that both implications are proper.

First, the closure of a point in every topological space is always hyperconnected. This is the reason why every anti-hyperconnected space must be  $T_1$ : every singleton must be closed.

```

lemma (in topology0) cl_point_imp_HConn:
  assumes  $x \in \bigcup T$ 
  shows (T{restricted to}Closure( $\{x\}, T$ )){is hyperconnected}

```

```

proof-
  from assms have sub: Closure({x}, T)  $\subseteq$   $\bigcup T$  using Top_3_L11 by auto
  then have tot:  $\bigcup (T \text{restricted to } \text{Closure}(\{x\}, T)) = \text{Closure}(\{x\}, T)$  unfolding RestrictedTo_def by auto
  {
    fix A B
    assume AS:  $A \in (T \text{restricted to } \text{Closure}(\{x\}, T)) \wedge B \in (T \text{restricted to } \text{Closure}(\{x\}, T)) \wedge A \cap B = \emptyset$ 
    then have  $B \subseteq \bigcup ((T \text{restricted to } \text{Closure}(\{x\}, T))) \wedge A \subseteq \bigcup ((T \text{restricted to } \text{Closure}(\{x\}, T)))$ 
    by auto
    with tot have  $B \subseteq \text{Closure}(\{x\}, T) \wedge A \subseteq \text{Closure}(\{x\}, T)$  by auto
    from AS(1,2) obtain UA UB where UAUB:  $UA \in T \wedge UB \in T \wedge A = UA \cap \text{Closure}(\{x\}, T) \wedge B = UB \cap \text{Closure}(\{x\}, T)$ 
    unfolding RestrictedTo_def by auto
    then have  $\text{Closure}(\{x\}, T) - A = \text{Closure}(\{x\}, T) - (UA \cap \text{Closure}(\{x\}, T)) \wedge \text{Closure}(\{x\}, T) - B = \text{Closure}(\{x\}, T) - (UB \cap \text{Closure}(\{x\}, T))$ 
    by auto
    then have  $\text{Closure}(\{x\}, T) - A = \text{Closure}(\{x\}, T) - UA \wedge \text{Closure}(\{x\}, T) - B = \text{Closure}(\{x\}, T) - UB$ 
    by auto
    with sub have  $\text{Closure}(\{x\}, T) - A = \text{Closure}(\{x\}, T) \cap (\bigcup T - UA) \wedge \text{Closure}(\{x\}, T) - B = \text{Closure}(\{x\}, T) \cap (\bigcup T - UB)$ 
  }
  by auto
  moreover
  from UAUB have  $(\bigcup T - UA) \text{ is closed in } T \wedge (\bigcup T - UB) \text{ is closed in } T$  using Top_3_L9 by auto
  moreover
  have  $\text{Closure}(\{x\}, T) \text{ is closed in } T$  using cl_is_closed assms by auto
  ultimately have  $(\text{Closure}(\{x\}, T) - A) \text{ is closed in } T \wedge (\text{Closure}(\{x\}, T) - B) \text{ is closed in } T$ 
  using Top_3_L5(1) by auto
  moreover
  {
    have  $x \in \text{Closure}(\{x\}, T)$  using cl_contains_set assms by auto
    moreover
    from AS(3) have  $x \notin A \vee x \notin B$  by auto
    ultimately have  $x \in (\text{Closure}(\{x\}, T) - A) \vee x \in (\text{Closure}(\{x\}, T) - B)$  by auto
  }
  ultimately have  $\text{Closure}(\{x\}, T) \subseteq (\text{Closure}(\{x\}, T) - A) \vee \text{Closure}(\{x\}, T) \subseteq (\text{Closure}(\{x\}, T) - B)$ 
  using Top_3_L13 by auto
  then have  $A \cap \text{Closure}(\{x\}, T) = \emptyset \vee B \cap \text{Closure}(\{x\}, T) = \emptyset$  by auto
  with 'B  $\subseteq$  Closure({x}, T)' 'A  $\subseteq$  Closure({x}, T)' have  $A = \emptyset \vee B = \emptyset$  using cl_contains_set
  by blast
  }
  then show thesis unfolding IsHConnected_def by auto
qed

```

A consequence is that every totally-disconnected space is  $T_1$ .

```

lemma (in topology0) tot_dis_imp_T1:
  assumes T{is totally-disconnected}
  shows T{is T1}

```

```

proof-
  {

```

```

fix x y
assume  $y \in \bigcup T x \in \bigcup T y \neq x$ 
then have  $(T\{\text{restricted to}\}\text{Closure}(\{x\}, T))\{\text{is hyperconnected}\}$  us-
ing cl_point_imp_HConn by auto
then have  $(T\{\text{restricted to}\}\text{Closure}(\{x\}, T))\{\text{is connected}\}$  using HConn_imp_Conn
by auto
moreover
from ' $x \in \bigcup T$ ' have  $\text{Closure}(\{x\}, T) \subseteq \bigcup T$  using Top_3_L11(1) by auto
moreover
note assms
ultimately have  $\text{Closure}(\{x\}, T)\{\text{is in the spectrum of}\}\text{IsConnected}$  un-
folding IsTotDis_def antiProperty_def
by auto
then have  $\text{Closure}(\{x\}, T) \lesssim 1$  using conn_spectrum by auto
moreover
from ' $x \in \bigcup T$ ' have  $x \in \text{Closure}(\{x\}, T)$  using cl_contains_set by auto
ultimately have  $\text{Closure}(\{x\}, T) = \{x\}$  using lepoll_1_is_sing[of  $\text{Closure}(\{x\}, T)$ 
x] by auto
then have  $\{x\}\{\text{is closed in}\}T$  using Top_3_L8 ' $x \in \bigcup T$ ' by auto
then have  $\bigcup T - \{x\} \in T$  unfolding IsClosed_def by auto
moreover
from ' $y \in \bigcup T$ ' ' $y \neq x$ ' have  $y \in \bigcup T - \{x\} \wedge x \notin \bigcup T - \{x\}$  by auto
ultimately have  $\exists U \in T. y \in U \wedge x \notin U$  by force
}
then show thesis unfolding isT1_def by auto
qed

```

In the literature, there exists a class of spaces called sober spaces; where the only non-empty closed hyperconnected subspaces are the closures of points and closures of different singletons are different.

**definition** IsSober ( $\_ \{\text{is sober}\}90$ )  
 where  $T\{\text{is sober}\} \equiv \forall A \in \text{Pow}(\bigcup T) - \{0\}. (A\{\text{is closed in}\}T \wedge ((T\{\text{restricted to}\}A)\{\text{is hyperconnected}\})) \longrightarrow (\exists x \in \bigcup T. A = \text{Closure}(\{x\}, T) \wedge (\forall y \in \bigcup T. A = \text{Closure}(\{y\}, T) \longrightarrow y = x))$

Being sober is weaker than being anti-hyperconnected.

**theorem** (in topology0) anti\_HConn\_imp\_sober:

assumes  $T\{\text{is anti-}\}\text{IsHConnected}$   
 shows  $T\{\text{is sober}\}$

**proof-**

```

{
  fix A assume  $A \in \text{Pow}(\bigcup T) - \{0\}$   $A\{\text{is closed in}\}T$   $(T\{\text{restricted to}\}A)\{\text{is hyperconnected}\}$ 
  with assms have  $A\{\text{is in the spectrum of}\}\text{IsHConnected}$  unfolding antiProperty_def
  by auto
  then have  $A \lesssim 1$  using HConn_spectrum by auto
  moreover
  with ' $A \in \text{Pow}(\bigcup T) - \{0\}$ ' have  $A \neq 0$  by auto
  then obtain x where  $x \in A$  by auto

```

```

ultimately have  $A=\{x\}$  using lepoll_1_is_sing by auto
with ' $A\{\text{is closed in}\}T$ ' have  $\{x\}\{\text{is closed in}\}T$  by auto
moreover from ' $x\in A$ ' ' $A\in\text{Pow}(\bigcup T)-\{0\}$ ' have  $\{x\}\in\text{Pow}(\bigcup T)$  by auto
ultimately
have  $\text{Closure}(\{x\},T)=\{x\}$  unfolding Closure_def ClosedCovers_def by
auto
with ' $A=\{x\}$ ' have  $A=\text{Closure}(\{x\},T)$  by auto
moreover
{
  fix y assume  $y\in\bigcup T$   $A=\text{Closure}(\{y\},T)$ 
  then have  $\{y\}\subseteq\text{Closure}(\{y\},T)$  using cl_contains_set by auto
  with ' $A=\text{Closure}(\{y\},T)$ ' have  $y\in A$  by auto
  with ' $A=\{x\}$ ' have  $y=x$  by auto
}
then have  $\forall y\in\bigcup T. A=\text{Closure}(\{y\},T) \longrightarrow y=x$  by auto
moreover note ' $\{x\}\in\text{Pow}(\bigcup T)$ '
ultimately have  $\exists x\in\bigcup T. A=\text{Closure}(\{x\},T)\wedge(\forall y\in\bigcup T. A=\text{Closure}(\{y\},T) \longrightarrow y=x)$  by auto
}
then show thesis using IsSober_def by auto
qed

```

Every sober space is  $T_0$ .

```

lemma (in topology0) sober_imp_T0:
  assumes T{is sober}
  shows T{is T0}
proof-
  {
    fix x y
    assume AS: $x\in\bigcup T$   $y\in\bigcup T$   $x\neq y$   $\forall U\in T. x\in U \longleftrightarrow y\in U$ 
    from ' $x\in\bigcup T$ ' have  $\text{cl}_x:\text{Closure}(\{x\},T)\{\text{is closed in}\}T$  using cl_is_closed
    by auto
    with ' $x\in\bigcup T$ ' have  $(\bigcup T-\text{Closure}(\{x\},T))\in T$  using Top_3_L11(1) unfolding
    IsClosed_def by auto
    moreover
    from ' $x\in\bigcup T$ ' have  $x\in\text{Closure}(\{x\},T)$  using cl_contains_set by auto
    moreover
    note AS(1,4)
    ultimately have  $y\notin(\bigcup T-\text{Closure}(\{x\},T))$  by auto
    with AS(2) have  $y\in\text{Closure}(\{x\},T)$  by auto
    with  $\text{cl}_x$  have  $\text{ineq1}:\text{Closure}(\{y\},T)\subseteq\text{Closure}(\{x\},T)$  using Top_3_L13
    by auto
    from ' $y\in\bigcup T$ ' have  $\text{cl}_y:\text{Closure}(\{y\},T)\{\text{is closed in}\}T$  using cl_is_closed
    by auto
    with ' $y\in\bigcup T$ ' have  $(\bigcup T-\text{Closure}(\{y\},T))\in T$  using Top_3_L11(1) unfolding
    IsClosed_def by auto
    moreover
    from ' $y\in\bigcup T$ ' have  $y\in\text{Closure}(\{y\},T)$  using cl_contains_set by auto
    moreover

```

```

note AS(2,4)
ultimately have  $x \notin (\bigcup T - \text{Closure}(\{y\}, T))$  by auto
with AS(1) have  $x \in \text{Closure}(\{y\}, T)$  by auto
with cly have  $\text{Closure}(\{x\}, T) \subseteq \text{Closure}(\{y\}, T)$  using Top_3_L13 by auto
with ineq1 have  $\text{eq} : \text{Closure}(\{x\}, T) = \text{Closure}(\{y\}, T)$  by auto
have  $\text{Closure}(\{x\}, T) \in \text{Pow}(\bigcup T - \{0\})$  using Top_3_L11(1) 'x ∈ ⋃ T' 'x ∈ Closure({x}, T)'
by auto
  moreover note assms clx
  ultimately have  $\exists t \in \bigcup T. (\text{Closure}(\{x\}, T) = \text{Closure}(\{t\}, T) \wedge (\forall y \in \bigcup T. \text{Closure}(\{x\}, T) = \text{Closure}(\{y\}, T) \longrightarrow y = t))$ 
    unfolding IsSober_def using cl_point_imp_HConn[OF 'x ∈ ⋃ T'] by auto
    then obtain t where t_def:  $t \in \bigcup T \wedge \text{Closure}(\{x\}, T) = \text{Closure}(\{t\}, T) \wedge \forall y \in \bigcup T. \text{Closure}(\{x\}, T) = \text{Closure}(\{y\}, T) \longrightarrow y = t$ 
      by blast
    with eq have  $y = t$  using 'y ∈ ⋃ T' by auto
    moreover from t_def 'x ∈ ⋃ T' have  $x = t$  by blast
    ultimately have  $y = x$  by auto
    with 'x ≠ y' have False by auto
  }
then have  $\forall x y. x \in \bigcup T \wedge y \in \bigcup T \wedge x \neq y \longrightarrow (\exists U \in T. (x \in U \wedge y \notin U) \vee (y \in U \wedge x \notin U))$ 
by auto
then show thesis using isT0_def by auto
qed

```

Every  $T_2$  space is anti-hyperconnected.

```

theorem (in topology0) T2_imp_anti_HConn:
  assumes T{is T2}
  shows T{is anti-}IsHConnected
proof-
  {
    fix TT
    assume TT{is a topology} TT{is hyperconnected} TT{is T2}
    {
      assume  $\bigcup TT = 0$ 
      then have  $\bigcup TT \lesssim 1$  using empty_lepollI by auto
      then have  $(\bigcup TT)\{\text{is in the spectrum of}\}\text{IsHConnected}$  using HConn_spectrum
    }
    by auto
  }
  moreover
  {
    assume  $\bigcup TT \neq 0$ 
    then obtain x where  $x \in \bigcup TT$  by blast
    {
      fix y
      assume  $y \in \bigcup TT \wedge x \neq y$ 
      with 'TT{is T2}' 'x ∈ ⋃ TT' obtain U V where  $U \in TT \wedge x \in U \wedge y \in V \wedge U \cap V = 0$ 
    }
    unfolding isT2_def by blast
    with 'TT{is hyperconnected}' have False using IsHConnected_def
  }
  by auto

```

```

    }
    with 'x ∈ ⋃ TT' have ⋃ TT = {x} by auto
    then have ⋃ TT ≈ 1 using singleton_eqpoll_1 by auto
    then have ⋃ TT ≲ 1 using eqpoll_imp_lepoll by auto
    then have (⋃ TT){is in the spectrum of}IsHConnected using HConn_spectrum
  by auto
}
ultimately have (⋃ TT){is in the spectrum of}IsHConnected by blast
}
then have ∀ T. ((T{is a topology} ∧ (T{is hyperconnected})) ∧ (T{is T2})) →
((⋃ T){is in the spectrum of}IsHConnected))
  by auto
  moreover
  note here_T2
  ultimately
  have ∀ T. T{is a topology} → ((T{is T2} → (T{is anti-}IsHConnected)))
using Q_P_imp_Spec[where P=IsHConnected and Q=isT2]
  by auto
  then show thesis using assms topSpaceAssum by auto
qed

```

Every anti-hyperconnected space is  $T_1$ .

```

theorem anti_HConn_imp_T1:
  assumes T{is anti-}IsHConnected
  shows T{is T1}
proof-
{
  fix x y
  assume x ∈ ⋃ Ty ∈ ⋃ Tx ≠ y
  {
    assume AS: ∀ U ∈ T. x ∉ U ∨ y ∈ U
    from 'x ∈ ⋃ T' 'y ∈ ⋃ T' have {x,y} ∈ Pow(⋃ T) by auto
    then have sub: (T{restricted to}{x,y}) ⊆ Pow({x,y}) using RestrictedTo_def
  by auto
  {
    fix U V
    assume H: U ∈ T{restricted to}{x,y} V ∈ (T{restricted to}{x,y}) ∪ V = 0
    with AS have x ∈ U → y ∈ U ∧ x ∈ V → y ∈ V unfolding RestrictedTo_def by
  auto
    with H(1,2) sub have x ∈ U → U = {x,y} ∧ x ∈ V → V = {x,y} by auto
    with H sub have x ∈ U → (U = {x,y} ∧ V = 0) ∧ x ∈ V → (V = {x,y} ∧ U = 0) by auto
    then have (x ∈ U ∨ x ∈ V) → (U = 0 ∨ V = 0) by auto
    moreover
    from sub H have (x ∉ U ∧ x ∉ V) → (U = 0 ∨ V = 0) by blast
    ultimately have U = 0 ∨ V = 0 by auto
  }
  then have (T{restricted to}{x,y}){is hyperconnected} unfolding IsHConnected_def
  by auto
  with assms '{x,y} ∈ Pow(⋃ T)' have {x,y}{is in the spectrum of}IsHConnected

```

```

unfolding antiProperty_def
  by auto
  then have  $\{x,y\} \lesssim 1$  using HConn_spectrum by auto
  moreover
  have  $x \in \{x,y\}$  by auto
  ultimately have  $\{x,y\} = \{x\}$  using lepoll_1_is_sing[of  $\{x,y\}x$ ] by auto
  moreover
  have  $y \in \{x,y\}$  by auto
  ultimately have  $y \in \{x\}$  by auto
  then have  $y = x$  by auto
  with ' $x \neq y$ ' have False by auto
}
then have  $\exists U \in T. x \in U \wedge y \notin U$  by auto
}
then show thesis using isT1_def by auto
qed

```

There is at least one topological space that is  $T_1$ , but not anti-hyperconnected.  
This space is the cofinite topology on the natural numbers.

```

lemma Cofinite_not_anti_HConn:
  shows  $\neg((\text{CoFinite nat})\{\text{is anti-}\}\text{IsHConnected})$  and  $(\text{CoFinite nat})\{\text{is } T_1\}$ 
proof-
  {
    assume  $(\text{CoFinite nat})\{\text{is anti-}\}\text{IsHConnected}$ 
    moreover
    have  $\bigcup (\text{CoFinite nat}) = \text{nat}$  unfolding Cofinite_def using union_cocardinal
  by auto
    moreover
    have  $(\text{CoFinite nat})\{\text{restricted to}\}\text{nat} = (\text{CoFinite nat})$  using subspace_cocardinal
  unfolding Cofinite_def
    by auto
    moreover
    note Cofinite_nat_HConn
    ultimately have  $\text{nat}\{\text{is in the spectrum of}\}\text{IsHConnected}$  unfolding antiProperty_def
  by auto
    then have  $\text{nat} \lesssim 1$  using HConn_spectrum by auto
    moreover
    have  $1 \in \text{nat}$  by auto
    then have  $1 < \text{nat}$  using n_lesspoll_nat by auto
    ultimately have  $\text{nat} < \text{nat}$  using lesspoll_trans1 by auto
    then have False by auto
  }
  then show  $\neg((\text{CoFinite nat})\{\text{is anti-}\}\text{IsHConnected})$  by auto
next
  show  $(\text{CoFinite nat})\{\text{is } T_1\}$  using cocardinal_is_T1 InfCard_nat unfolding
  Cofinite_def by auto
qed

```

The join-topology build from the cofinite topology on the natural numbers, and the excluded set topology on the natural numbers excluding  $\{0, 1\}$ ; is just the union of both.

```

lemma join_top_cofinite_excluded_set:
  shows (joinT {CoFinite nat, ExcludedSet nat {0,1}})=(CoFinite nat)∪
(ExcludedSet nat {0,1})
proof-
  have coftop: (CoFinite nat){is a topology} unfolding Cofinite_def us-
ing CoCar_is_topology InfCard_nat by auto
  moreover
  have (ExcludedSet nat {0,1}){is a topology} using excludedset_is_topology
by auto
  moreover
  have exuni: ∪ (ExcludedSet nat {0,1})=nat using union_excludedset by
auto
  moreover
  have cofuni: ∪ (CoFinite nat)=nat using union_cocardinal unfolding Cofinite_def
by auto
  ultimately have (joinT {CoFinite nat, ExcludedSet nat {0,1}}) = (THE
T. (CoFinite nat)∪(ExcludedSet nat {0,1}) {is a subbase for} T)
    using joinT_def by auto
  moreover
  have ∪ (CoFinite nat)∈CoFinite nat using CoCar_is_topology[OF InfCard_nat]
unfolding Cofinite_def IsATopology_def
    by auto
  with cofuni have n:nat∈CoFinite nat by auto
  have Pa: (CoFinite nat)∪(ExcludedSet nat {0,1}) {is a subbase for} {∪ A.
A∈Pow({∩ B. B∈FinPow((CoFinite nat)∪(ExcludedSet nat {0,1})))}}
    using Top_subbase(2) by auto
  have {∪ A. A∈Pow({∩ B. B∈FinPow((CoFinite nat)∪(ExcludedSet nat {0,1})))}}=(THE
T. (CoFinite nat)∪(ExcludedSet nat {0,1}) {is a subbase for} T)
    using same_subbase_same_top[where B=(CoFinite nat)∪(ExcludedSet nat
{0,1}), OF _ Pa] the_equality[where a={∪ A. A∈Pow({∩ B. B∈FinPow((CoFinite
nat)∪(ExcludedSet nat {0,1})))}} and P=λT. ((CoFinite nat)∪(ExcludedSet
nat {0,1}))is a subbase for}T,
    OF Pa] by auto
  ultimately have equal: (joinT {CoFinite nat, ExcludedSet nat {0,1}})
={∪ A. A∈Pow({∩ B. B∈FinPow((CoFinite nat)∪(ExcludedSet nat {0,1})))}}
    by auto
  {
    fix U assume U∈{∪ A. A∈Pow({∩ B. B∈FinPow((CoFinite nat)∪(ExcludedSet
nat {0,1})))}}
    then obtain AU where U=∪ AU and base: AU∈Pow({∩ B. B∈FinPow((CoFinite
nat)∪(ExcludedSet nat {0,1})))}}
      by auto
    have (CoFinite nat)⊆Pow(∪ (CoFinite nat)) by auto
    moreover
    have (ExcludedSet nat {0,1})⊆Pow(∪ (ExcludedSet nat {0,1})) by auto
    moreover

```



```

    note cofuni exuni
    ultimately have sub: (CoFinite nat) ∪ (ExcludedSet nat {0,1}) ⊆ Pow(nat)
  by auto
    from base have ∀ S ∈ AU. S ∈ {⋂ B. B ∈ FinPow((CoFinite nat) ∪ (ExcludedSet
nat {0,1}))} by blast
    then have ∀ S ∈ AU. ∃ B ∈ FinPow((CoFinite nat) ∪ (ExcludedSet nat {0,1})).
S = ⋂ B by blast
    then have eq: ∀ S ∈ AU. ∃ B ∈ Pow((CoFinite nat) ∪ (ExcludedSet nat {0,1})).
S = ⋂ B unfolding FinPow_def by blast
    {
      fix S assume S ∈ AU
      with eq obtain B where B ∈ Pow((CoFinite nat) ∪ (ExcludedSet nat {0,1})) S = ⋂ B
    by auto
      with sub have B ∈ Pow(Pow(nat)) by auto
      {
        fix x assume x ∈ ⋂ B
        then have ∀ N ∈ B. x ∈ N ≠ 0 by auto
        with 'B ∈ Pow(Pow(nat))' have x ∈ nat by blast
      }
      with 'S = ⋂ B' have S ∈ Pow(nat) by auto
    }
    then have ∀ S ∈ AU. S ∈ Pow(nat) by blast
    with 'U = ⋃ AU' have U ∈ Pow(nat) by auto
    {
      assume 0 ∈ U ∨ 1 ∈ U
      with 'U = ⋃ AU' obtain S where S ∈ AU 0 ∈ S ∨ 1 ∈ S by auto
      with base obtain BS where S = ⋂ BS and bsbase: BS ∈ FinPow((CoFinite
nat) ∪ (ExcludedSet nat {0,1})) by auto
      with '0 ∈ S ∨ 1 ∈ S' have ∀ M ∈ BS. 0 ∈ M ∨ 1 ∈ M by auto
      then have ∀ M ∈ BS. M ⊄ (ExcludedSet nat {0,1}) - {nat} unfolding ExcludedPoint_def
ExcludedSet_def by auto
      moreover
      note bsbase n
      ultimately have BS ∈ FinPow(CoFinite nat) unfolding FinPow_def by
auto
      moreover
      from '0 ∈ S ∨ 1 ∈ S' have S ≠ 0 by auto
      with 'S = ⋂ BS' have BS ≠ 0 by auto
      moreover
      note coftop
      ultimately have ⋂ BS ∈ CoFinite nat using topology0.fin_inter_open_open[OF
topology0_CoCardinal[OF InfCard_nat]]
      unfolding Cofinite_def by auto
      with 'S = ⋂ BS' have S ∈ CoFinite nat by auto
      with '0 ∈ S ∨ 1 ∈ S' have nat - S ≠ nat unfolding Cofinite_def Cocardinal_def
    by auto
      moreover
      from 'U = ⋃ AU' 'S ∈ AU' have S ⊆ U by auto
      then have nat - U ⊆ nat - S by auto

```

```

    then have nat- $\mathcal{U} \lesssim$  nat-S using subset_imp_lepoll by auto
    ultimately
    have nat- $\mathcal{U} \prec$  nat using lesspoll_trans1 by auto
    with 'U ∈ Pow(nat)' have U ∈ CoFinite nat unfolding Cofinite_def Cocardinal_def
  by auto
    with 'U ∈ Pow(nat)' have U ∈ (CoFinite nat) ∪ (ExcludedSet nat {0,1})
  by auto
    }
    with 'U ∈ Pow(nat)' have U ∈ (CoFinite nat) ∪ (ExcludedSet nat {0,1})
  unfolding ExcludedSet_def by blast
    }
    then have ( $\{\bigcup A . A \in \text{Pow}(\{\bigcap B . B \in \text{FinPow}((\text{CoFinite nat}) \cup (\text{ExcludedSet nat } \{0,1\}))\})\} \subseteq (\text{CoFinite nat}) \cup (\text{ExcludedSet nat } \{0,1\})$ )
    by blast
    moreover
    {
      fix U
      assume U ∈ (CoFinite nat) ∪ (ExcludedSet nat {0,1})
      then have  $\{U\} \in \text{FinPow}((\text{CoFinite nat}) \cup (\text{ExcludedSet nat } \{0,1\}))$  un-
    folding FinPow_def by auto
      then have  $\{U\} \in \text{Pow}(\{\bigcap B . B \in \text{FinPow}((\text{CoFinite nat}) \cup (\text{ExcludedSet nat } \{0,1\}))\})$  by blast
      moreover
      have  $U = \bigcup \{U\}$  by auto
      ultimately have  $U \in \{\bigcup A . A \in \text{Pow}(\{\bigcap B . B \in \text{FinPow}((\text{CoFinite nat}) \cup (\text{ExcludedSet nat } \{0,1\}))\})\}$  by blast
    }
    then have  $(\text{CoFinite nat}) \cup (\text{ExcludedSet nat } \{0,1\}) \subseteq \{\bigcup A . A \in \text{Pow}(\{\bigcap B . B \in \text{FinPow}((\text{CoFinite nat}) \cup (\text{ExcludedSet nat } \{0,1\}))\})\}$ 
    by auto
    ultimately have  $(\text{CoFinite nat}) \cup (\text{ExcludedSet nat } \{0,1\}) = \{\bigcup A . A \in \text{Pow}(\{\bigcap B . B \in \text{FinPow}((\text{CoFinite nat}) \cup (\text{ExcludedSet nat } \{0,1\}))\})\}$ 
    by auto
    with equal show thesis by auto
  qed

```

The previous topology is not  $T_2$ , but is anti-hyperconnected.

**theorem join\_Cofinite\_ExclPoint\_not\_T2:**

shows  $\neg((\text{joinT } \{\text{CoFinite nat}, \text{ExcludedSet nat } \{0,1\}\}) \text{ is } T_2)$  and  $(\text{joinT } \{\text{CoFinite nat}, \text{ExcludedSet nat } \{0,1\}\}) \text{ is anti-IsHConnected}$

**proof-**

have  $(\text{CoFinite nat}) \subseteq (\text{CoFinite nat}) \cup (\text{ExcludedSet nat } \{0,1\})$  by auto

have  $\bigcup ((\text{CoFinite nat}) \cup (\text{ExcludedSet nat } \{0,1\})) = (\bigcup (\text{CoFinite nat})) \cup (\bigcup (\text{ExcludedSet nat } \{0,1\}))$

by auto

moreover

have ... = nat unfolding Cofinite\_def using union\_cocardinal union\_excludedset by auto

ultimately have  $\text{tot} : \bigcup ((\text{CoFinite nat}) \cup (\text{ExcludedSet nat } \{0,1\})) = \text{nat}$

```

by auto
{
  assume (joinT {CoFinite nat, ExcludedSet nat {0, 1}}) {is T2}
  then have t2:((CoFinite nat) ∪ (ExcludedSet nat {0,1})) {is T2} us-
ing join_top_cofinite_excluded_set
  by auto
  with tot have ∃U∈((CoFinite nat) ∪ (ExcludedSet nat {0,1})). ∃V∈((CoFinite
nat) ∪ (ExcludedSet nat {0,1})). 0∈U ∧ 1∈V ∧ U ∩ V = 0 using isT2_def by auto
  then obtain U V where U ∈ (CoFinite nat) ∨ (0 ∉ U ∧ 1 ∉ U) V ∈ (CoFinite
nat) ∨ (0 ∉ V ∧ 1 ∉ V) 0∈U ∧ 1∈V ∧ U ∩ V = 0
  unfolding ExcludedSet_def by auto
  then have U∈(CoFinite nat) V∈(CoFinite nat) by auto
  with '0∈U' '1∈V' have U ∩ V ≠ 0 using Cofinite_nat_HConn IsHConnected_def
by auto
  with 'U ∩ V = 0' have False by auto
}
then show ¬((joinT {CoFinite nat, ExcludedSet nat {0,1}}) {is T2}) by
auto
{
  fix A assume AS:A∈Pow(⋃((CoFinite nat) ∪ (ExcludedSet nat {0,1})))(((CoFinite
nat) ∪ (ExcludedSet nat {0,1})) {restricted to} A) {is hyperconnected}
  with tot have A∈Pow(nat) by auto
  then have sub:A ∩ nat = A by auto
  have ((CoFinite nat) ∪ (ExcludedSet nat {0,1})) {restricted to} A = ((CoFinite
nat) {restricted to} A) ∪ ((ExcludedSet nat {0,1}) {restricted to} A)
  unfolding RestrictedTo_def by auto
  also from sub have .. = (CoFinite A) ∪ (ExcludedSet A {0,1}) using subspace_excludedset[of
subspace_cocardinal[of nat nat A] unfolding Cofinite_def
  by auto
  finally have ((CoFinite nat) ∪ (ExcludedSet nat {0,1})) {restricted to} A = (CoFinite
A) ∪ (ExcludedSet A {0,1}) by auto
  with AS(2) have eq:((CoFinite A) ∪ (ExcludedSet A {0,1})) {is hyperconnected}
by auto
  {
    assume {0,1} ∩ A = 0
    then have (CoFinite A) ∪ (ExcludedSet A {0,1}) = Pow(A) using empty_excludedset[of
{0,1} A] unfolding Cofinite_def Cocardinal_def
    by auto
    with eq have Pow(A) {is hyperconnected} by auto
    then have Pow(A) {is connected} using HConn_imp_Conn by auto
    moreover
    have Pow(A) {is anti-} IsConnected using discrete_tot_dis unfold-
ing IsTotDis_def by auto
    moreover
    have ⋃ (Pow(A)) ∈ Pow(⋃ (Pow(A))) by auto
    moreover
    have Pow(A) {restricted to} ⋃ (Pow(A)) = Pow(A) unfolding RestrictedTo_def
by blast
    ultimately have (⋃ (Pow(A))) {is in the spectrum of} IsConnected un-

```

```

folding antiProperty_def
  by auto
  then have A{is in the spectrum of}IsConnected by auto
  then have  $A \lesssim 1$  using conn_spectrum by auto
  then have A{is in the spectrum of}IsHConnected using HConn_spectrum
by auto
}
moreover
{
  assume AS:{0,1} $\cap$ A $\neq$ 0
  {
    assume A={0} $\vee$ A={1}
    then have  $A \approx 1$  using singleton_eqpoll_1 by auto
    then have  $A \lesssim 1$  using eqpoll_imp_lepoll by auto
    then have A{is in the spectrum of}IsHConnected using HConn_spectrum
  }
}
moreover
{
  assume AS2: $\neg$ (A={0} $\vee$ A={1})
  {
    assume AS3:A $\subseteq$ {0,1}
    with AS AS2 AS3 have A_def:A={0,1} by blast
    then have (ExcludedSet A {0,1})=(ExcludedSet A A) by auto
    moreover have (ExcludedSet A A)={0,A} unfolding ExcludedSet_def
  }
}
by blast
ultimately have (ExcludedSet A {0,1})={0,A} by auto
moreover
have 0 $\in$ (CoFinite A) using empty_open[of CoFinite A]
  CoCar_is_topology[OF InfCard_nat,of A] unfolding Cofinite_def
by auto
moreover
have  $\bigcup$  (CoFinite A)=A using union_cocardinal unfolding Cofinite_def
by auto
then have A $\in$ (CoFinite A) using CoCar_is_topology[OF InfCard_nat,of
A] unfolding Cofinite_def
  IsATopology_def by auto
ultimately have (CoFinite A) $\cup$ (ExcludedSet A {0,1})=(CoFinite
A) by auto
with eq have(CoFinite A){is hyperconnected} by auto
with A_def have hyp:(CoFinite {0,1}){is hyperconnected} by
auto
have {0} $\approx$ 1{1} $\approx$ 1 using singleton_eqpoll_1 by auto
moreover
have 1 $\prec$ nat using n_lesspoll_nat by auto
ultimately have {0} $\prec$ nat{1} $\prec$ nat using eq_lesspoll_trans by auto
moreover
have {0,1}-{1}={0}{0,1}-{0}={1} by auto
ultimately have {1} $\in$ (CoFinite {0,1}){0} $\in$ (CoFinite {0,1}) {1} $\cap$ {0}=0

```

```

unfolding Cofinite_def Cocardinal_def
  by auto
  with hyp have False unfolding IsHConnected_def by auto
}
then obtain t where t∈A t≠0 t≠1 by auto
then have {t}∈(ExcludedSet A {0,1}) unfolding ExcludedSet_def
by auto
moreover
{
  have {t}≈1 using singleton_eqpoll_1 by auto
  moreover
  have 1<nat using n_lesspoll_nat by auto
  ultimately have {t}<nat using eq_lesspoll_trans by auto
  moreover
  with 't∈A' have A-(A-{t})={t} by auto
  ultimately have A-{t}∈(CoFinite A) unfolding Cofinite_def Cocardinal_def
    by auto
}
ultimately have {t}∈((CoFinite A)∪(ExcludedSet A {0,1}))A-{t}∈((CoFinite
A)∪(ExcludedSet A {0,1}))
  {t}∩(A-{t})=0 by auto
with eq have A-{t}=0 unfolding IsHConnected_def by auto
with 't∈A' have A={t} by auto
then have A≈1 using singleton_eqpoll_1 by auto
then have A≤1 using eqpoll_imp_lepoll by auto
then have A{is in the spectrum of}IsHConnected using HConn_spectrum
by auto
}
ultimately have A{is in the spectrum of}IsHConnected by auto
}
ultimately have A{is in the spectrum of}IsHConnected by auto
}
then have ((CoFinite nat)∪(ExcludedSet nat {0,1})) {is anti-}IsHConnected
unfolding antiProperty_def
  by auto
then show (joinT {CoFinite nat, ExcludedSet nat {0,1}}) {is anti-}IsHConnected
using join_top_cofinite_excluded_set
  by auto
qed

```

Let's show that anti-hyperconnected is in fact  $T_1$  and sober. The trick of the proof lies in the fact that if a subset is hyperconnected, its closure is so too (the closure of a point is then always hyperconnected because singletons are in the spectrum); since the closure is closed, we can apply the sober property on it.

```

theorem (in topology0) T1_sober_imp_anti_HConn:
  assumes T{is  $T_1$ } and T{is sober}
  shows T{is anti-}IsHConnected
proof-

```

```

{
  fix A assume AS:A∈Pow(⋃T)(T{restricted to}A){is hyperconnected}
  {
    assume A=0
    then have A≤1 using empty_lepollI by auto
    then have A{is in the spectrum of}IsHConnected using HConn_spectrum
  }
by auto
}
moreover
{
  assume A≠0
  then obtain x where x∈A by blast
  {
    assume ¬((T{restricted to}Closure(A,T)){is hyperconnected})
    then obtain U V where UV_def:U∈(T{restricted to}Closure(A,T))V∈(T{restricted
to}Closure(A,T))
      UV=0U≠0V≠0 using IsHConnected_def by auto
    then obtain UCA VCA where UCA∈TVCA∈TU=UCA∩Closure(A,T)V=VCA∩Closure(A,T)
      unfolding RestrictedTo_def by auto
    from 'A∈Pow(⋃T)' have A⊆Closure(A,T) using cl_contains_set by
auto
    then have UCA∩A⊆UCA∩Closure(A,T)VCA∩A⊆VCA∩Closure(A,T) by auto
    with 'U=UCA∩Closure(A,T)' 'V=VCA∩Closure(A,T)' 'UV=0' have (UCA∩A)∩(VCA∩A)=0
  }
by auto
  moreover
  from 'UCA∈T' 'VCA∈T' have UCA∩A∈(T{restricted to}A)VCA∩A∈(T{restricted
to}A)
    unfolding RestrictedTo_def by auto
  moreover
  note AS(2)
  ultimately have UCA∩A=0∨VCA∩A=0 using IsHConnected_def by auto
  with 'A⊆Closure(A,T)' have A⊆Closure(A,T)-UCA∨A⊆Closure(A,T)-VCA
by auto
  moreover
  {
    have Closure(A,T)-UCA=Closure(A,T)∩(⋃T-UCA)Closure(A,T)-VCA=Closure(A,T)∩(⋃T-VCA)
      using Top_3_L11(1) AS(1) by auto
    moreover
    with 'UCA∈T' 'VCA∈T' have (⋃T-UCA){is closed in}T(⋃T-VCA){is
closed in}TClosure(A,T){is closed in}T
      using Top_3_L9 cl_is_closed AS(1) by auto
    ultimately have (Closure(A,T)-UCA){is closed in}T(Closure(A,T)-VCA){is
closed in}T
      using Top_3_L5(1) by auto
  }
  ultimately
  have Closure(A,T)⊆Closure(A,T)-UCA∨Closure(A,T)⊆Closure(A,T)-VCA
using Top_3_L13
  by auto

```

```

    then have  $U \cap \text{Closure}(A, T) = 0 \vee V \cap \text{Closure}(A, T) = 0$  by auto
    with 'U= $U \cap \text{Closure}(A, T)$ ' 'V= $V \cap \text{Closure}(A, T)$ ' have  $U=0 \vee V=0$  by
auto
    with ' $U \neq 0$ ' ' $V \neq 0$ ' have False by auto
  }
  then have  $(T \{\text{restricted to}\} \text{Closure}(A, T)) \{\text{is hyperconnected}\}$  by
auto
    moreover
    have  $\text{Closure}(A, T) \{\text{is closed in}\} T$  using cl_is_closed AS(1) by auto
    moreover
    from ' $x \in A$ ' have  $\text{Closure}(A, T) \neq 0$  using cl_contains_set AS(1) by
auto
    moreover
    from AS(1) have  $\text{Closure}(A, T) \subseteq \bigcup T$  using Top_3_L11(1) by auto
    ultimately have  $\text{Closure}(A, T) \in \text{Pow}(\bigcup T) - \{0\} (T \{\text{restricted to}\} \text{Closure}(A,$ 
 $T)) \{\text{is hyperconnected}\} \text{Closure}(A, T) \{\text{is closed in}\} T$ 
    by auto
    moreover note assms(2)
    ultimately have  $\exists x \in \bigcup T. (\text{Closure}(A, T) = \text{Closure}(\{x\}, T) \wedge (\forall y \in \bigcup T.$ 
 $\text{Closure}(A, T) = \text{Closure}(\{y\}, T) \longrightarrow y = x))$  unfolding IsSober_def
    by auto
    then obtain y where  $y \in \bigcup T \text{Closure}(A, T) = \text{Closure}(\{y\}, T)$  by auto
    moreover
    {
      fix z assume  $z \in (\bigcup T) - \{y\}$ 
      with assms(1) ' $y \in \bigcup T$ ' obtain U where  $U \in T \ z \in U \ y \notin U$  using isT1_def
by blast
      then have  $U \in T \ z \in U \ U \subseteq (\bigcup T) - \{y\}$  by auto
      then have  $\exists U \in T. z \in U \wedge U \subseteq (\bigcup T) - \{y\}$  by auto
    }
    then have  $\forall z \in (\bigcup T) - \{y\}. \exists U \in T. z \in U \wedge U \subseteq (\bigcup T) - \{y\}$  by auto
    then have  $\bigcup T - \{y\} \in T$  using open_neigh_open by auto
    with ' $y \in \bigcup T$ ' have  $\{y\} \{\text{is closed in}\} T$  using IsClosed_def by auto
    with ' $y \in \bigcup T$ ' have  $\text{Closure}(\{y\}, T) = \{y\}$  using Top_3_L8 by auto
    with ' $\text{Closure}(A, T) = \text{Closure}(\{y\}, T)$ ' have  $\text{Closure}(A, T) = \{y\}$  by auto
    with AS(1) have  $A \subseteq \{y\}$  using cl_contains_set[of A] by auto
    with ' $A \neq 0$ ' have  $A = \{y\}$  by auto
    then have  $A \approx 1$  using singleton_eqpoll_1 by auto
    then have  $A \lesssim 1$  using eqpoll_imp_lepoll by auto
    then have  $A \{\text{is in the spectrum of}\} \text{IsHConnected}$  using HConn_spectrum
by auto
  }
  ultimately have  $A \{\text{is in the spectrum of}\} \text{IsHConnected}$  by blast
}
then show thesis using antiProperty_def by auto
qed

```

```

theorem (in topology0) anti_HConn_iff_T1_sober:
  shows  $(T \{\text{is anti-}\} \text{IsHConnected}) \longleftrightarrow (T \{\text{is sober}\} \wedge T \{\text{is } T_1\})$ 

```

```

using T1_sober_imp_anti_HConn anti_HConn_imp_T1 anti_HConn_imp_sober
by auto

```

A space is ultraconnected iff every two non-empty closed sets meet.

```

definition IsUConnected (_{is ultraconnected}80)
  where T{is ultraconnected}≡  $\forall A B. A\{\text{is closed in}\}T \wedge B\{\text{is closed in}\}T \wedge A \cap B = 0$ 
   $\longrightarrow A = 0 \vee B = 0$ 

```

Every ultraconnected space is trivially normal.

```

lemma (in topology0)UConn_imp_normal:
  assumes T{is ultraconnected}
  shows T{is normal}
proof-
{
  fix A B
  assume AS:A{is closed in}T B{is closed in}T  $A \cap B = 0$ 
  with assms have  $A = 0 \vee B = 0$  using IsUConnected_def by auto
  with AS(1,2) have  $(A \subseteq 0 \wedge B \subseteq \bigcup T) \vee (A \subseteq \bigcup T \wedge B \subseteq 0)$  unfolding IsClosed_def
by auto
  moreover
  have  $0 \in T$  using empty_open topSpaceAssum by auto
  moreover
  have  $\bigcup T \in T$  using topSpaceAssum unfolding IsATopology_def by auto
  ultimately have  $\exists U \in T. \exists V \in T. A \subseteq U \wedge B \subseteq V \wedge U \cap V = 0$  by auto
}
then show thesis unfolding IsNormal_def by auto
qed

```

Every ultraconnected space is connected.

```

lemma UConn_imp_Conn:
  assumes T{is ultraconnected}
  shows T{is connected}
proof-
{
  fix U V
  assume  $U \in T \wedge V \{\text{is closed in}\}T$ 
  then have  $\bigcup T - (\bigcup T - U) = U$  by auto
  with 'U ∈ T' have  $(\bigcup T - U) \{\text{is closed in}\}T$  unfolding IsClosed_def by
auto
  with 'U{is closed in}T' assms have  $U = 0 \vee \bigcup T - U = 0$  unfolding IsUConnected_def
by auto
  with 'U ∈ T' have  $U = 0 \vee U = \bigcup T$  by auto
}
then show thesis unfolding IsConnected_def by auto
qed

```

```

lemma UConn_spectrum:
  shows (A{is in the spectrum of}IsUConnected)  $\longleftrightarrow A \lesssim 1$ 
proof

```



```

assume A_spec:(A{is in the spectrum of}IsUConnected)
{
  assume A=0
  then have  $A \lesssim 1$  using empty_lepollI by auto
}
moreover
{
  assume  $A \neq 0$ 
  from A_spec have  $\forall T. (T\{\text{is a topology}\} \wedge \bigcup T \approx A) \longrightarrow (T\{\text{is ultraconnected}\})$ 
unfolding Spec_def by auto
  moreover
  have  $\text{Pow}(A)\{\text{is a topology}\}$  using Pow_is_top by auto
  moreover
  have  $\bigcup \text{Pow}(A) = A$  by auto
  then have  $\bigcup \text{Pow}(A) \approx A$  by auto
  ultimately have  $\text{ult}:\text{Pow}(A)\{\text{is ultraconnected}\}$  by auto
  moreover
  from ' $A \neq 0$ ' obtain b where  $b \in A$  by auto
  then have  $\{b\}\{\text{is closed in}\}\text{Pow}(A)$  unfolding IsClosed_def by auto
  {
    fix c
    assume  $c \in A \neq b$ 
    then have  $\{c\}\{\text{is closed in}\}\text{Pow}(A)\{c\} \cap \{b\} = \emptyset$  unfolding IsClosed_def
  by auto
    with  $\text{ult} \text{ ' $\{b\}\{\text{is closed in}\}\text{Pow}(A)$ ' }$  have False using IsUConnected_def
  by auto
  }
  with ' $b \in A$ ' have  $A = \{b\}$  by auto
  then have  $A \approx 1$  using singleton_eqpoll_1 by auto
  then have  $A \lesssim 1$  using eqpoll_imp_lepoll by auto
}
ultimately show  $A \lesssim 1$  by auto
next
assume  $A \lesssim 1$ 
{
  fix T
  assume  $T\{\text{is a topology}\} \bigcup T \approx A$ 
  {
    assume  $\bigcup T = \emptyset$ 
    with ' $T\{\text{is a topology}\}$ ' have  $T = \{\emptyset\}$  using empty_open by auto
    then have  $T\{\text{is ultraconnected}\}$  unfolding IsUConnected_def IsClosed_def
  by auto
  }
  moreover
  {
    assume  $\bigcup T \neq \emptyset$ 
    moreover
    from ' $A \lesssim 1$ ' ' $\bigcup T \approx A$ ' have  $\bigcup T \lesssim 1$  using eq_lepoll_trans by auto
    ultimately

```

```

    obtain E where eq:  $\bigcup T = \{E\}$  using lepoll_1_is_sing by blast
    moreover
    have  $T \subseteq \text{Pow}(\bigcup T)$  by auto
    ultimately have  $T \subseteq \text{Pow}(\{E\})$  by auto
    then have  $T \subseteq \{0, \{E\}\}$  by blast
    with 'T{is a topology}' have  $\{0\} \subseteq T \subseteq \{0, \{E\}\}$  using empty_open
  by auto
    then have T{is ultraconnected} unfolding IsUConnected_def IsClosed_def
  by (simp only: eq, safe, force)
    }
    ultimately have T{is ultraconnected} by auto
  }
  then show A{is in the spectrum of}IsUConnected unfolding Spec_def by
auto
qed

```

This time, anti-ultraconnected is an old property.

```

theorem (in topology0) anti_UConn:
  shows (T{is anti-}IsUConnected)  $\longleftrightarrow$  T{is  $T_1$ }
proof
  assume T{is  $T_1$ }
  {
    fix TT
    {
      assume TT{is a topology}TT{is  $T_1$ }TT{is ultraconnected}
      {
        assume  $\bigcup TT = 0$ 
        then have  $\bigcup TT \lesssim 1$  using empty_lepollI by auto
        then have (( $\bigcup TT$ ){is in the spectrum of}IsUConnected) using UConn_spectrum
      by auto
      }
      moreover
      {
        assume  $\bigcup TT \neq 0$ 
        then obtain t where  $t \in \bigcup TT$  by blast
        {
          fix x
          assume  $p : x \in \bigcup TT$ 
          {
            fix y assume  $y \in (\bigcup TT) - \{x\}$ 
            with 'TT{is  $T_1$ }' p obtain U where  $U \in TT$   $y \in U$   $x \notin U$  using isT1_def
          by blast
            then have  $U \in TT$   $y \in U$   $U \subseteq (\bigcup TT) - \{x\}$  by auto
            then have  $\exists U \in TT. y \in U \wedge U \subseteq (\bigcup TT) - \{x\}$  by auto
          }
          then have  $\forall y \in (\bigcup TT) - \{x\}. \exists U \in TT. y \in U \wedge U \subseteq (\bigcup TT) - \{x\}$  by auto
          with 'TT{is a topology}' have  $\bigcup TT - \{x\} \in TT$  using topology0.open_neigh_open
        unfolding topology0_def by auto
        with p have  $\{x\}$  {is closed in}TT using IsClosed_def by auto
      }
    }
  }

```

```

    }
    then have reg:  $\forall x \in \bigcup TT. \{x\}$  {is closed in}  $TT$  by auto
    with 't  $\in \bigcup TT$ ' have t_cl:  $\{t\}$  {is closed in}  $TT$  by auto
    {
      fix y
      assume  $y \in \bigcup TT$ 
      with reg have  $\{y\}$  {is closed in}  $TT$  by auto
      with ' $TT$  {is ultraconnected}' t_cl have  $y=t$  unfolding IsUConnected_def
by auto
    }
    with 't  $\in \bigcup TT$ ' have  $\bigcup TT = \{t\}$  by blast
    then have  $\bigcup TT \approx 1$  using singleton_eqpoll_1 by auto
    then have  $\bigcup TT \lesssim 1$  using eqpoll_imp_lepoll by auto
    then have  $(\bigcup TT)$  {is in the spectrum of} IsUConnected using UConn_spectrum
by auto
  }
  ultimately have  $(\bigcup TT)$  {is in the spectrum of} IsUConnected by blast
}
then have  $(TT$  {is a topology}  $\wedge TT$  {is  $T_1$ }  $\wedge (TT$  {is ultraconnected}))  $\longrightarrow$ 
 $((\bigcup TT)$  {is in the spectrum of} IsUConnected)
  by auto
}
then have  $\forall TT. (TT$  {is a topology}  $\wedge TT$  {is  $T_1$ }  $\wedge (TT$  {is ultraconnected}))  $\longrightarrow$ 
 $((\bigcup TT)$  {is in the spectrum of} IsUConnected)
  by auto
moreover
note here_T1
ultimately have  $\forall T. T$  {is a topology}  $\longrightarrow ((T$  {is  $T_1$ })  $\longrightarrow (T$  {is anti-} IsUConnected))
using Q_P_imp_Spec[where Q=isT1 and P=IsUConnected]
  by auto
with topSpaceAssum have  $(T$  {is  $T_1$ })  $\longrightarrow (T$  {is anti-} IsUConnected) by auto
with ' $T$  {is  $T_1$ }' show  $T$  {is anti-} IsUConnected by auto
next
assume ASS:  $T$  {is anti-} IsUConnected
{
  fix x y
  assume  $x \in \bigcup Ty \in \bigcup Tx \neq y$ 
  then have tot:  $\bigcup (T$  {restricted to}  $\{x,y\}) = \{x,y\}$  unfolding RestrictedTo_def
by auto
  {
    assume AS:  $\forall U \in T. x \in U \longrightarrow y \in U$ 
    {
      assume  $\{y\}$  {is closed in}  $(T$  {restricted to}  $\{x,y\})$ 
      moreover
      from ' $x \neq y$ ' have  $\{x,y\} - \{y\} = \{x\}$  by auto
      ultimately have  $\{x\} \in (T$  {restricted to}  $\{x,y\})$  unfolding IsClosed_def
by (simp only: tot)
      then obtain U where  $U \in T$   $\{x\} = \{x,y\} \cap U$  unfolding RestrictedTo_def
by auto
    }
  }
}

```

```

    moreover
    with 'x≠y' have y∉{x} y∈{x,y} by (blast+)
    with '{x}={x,y}∩U' have y∉U by auto
    moreover have x∈{x} by auto
    with '{x}={x,y}∩U' have x∈U by auto
    ultimately have x∈Uy∉UU∈T by auto
    with AS have False by auto
  }
  then have y_no_cl:¬({y}{is closed in}(T{restricted to}{x,y})) by
auto
  {
    fix A B
    assume cl:A{is closed in}(T{restricted to}{x,y})B{is closed in}(T{restricted
to}{x,y})A∩B=0
    with tot have A⊆{x,y}B⊆{x,y}A∩B=0 unfolding IsClosed_def by
auto
    then have x∈A→x∉B y∈A→y∉BA⊆{x,y}B⊆{x,y} by auto
    {
      assume x∈A
      with 'x∈A→x∉B' 'B⊆{x,y}' have B⊆{y} by auto
      then have B=0∨B={y} by auto
      with y_no_cl cl(2) have B=0 by auto
    }
    moreover
    {
      assume x∉A
      with 'A⊆{x,y}' have A⊆{y} by auto
      then have A=0∨A={y} by auto
      with y_no_cl cl(1) have A=0 by auto
    }
    ultimately have A=0∨B=0 by auto
  }
  then have (T{restricted to}{x,y}){is ultraconnected} unfolding IsUConnected_def
by auto
  with ASS 'x∈⋃T' 'y∈⋃T' have {x,y}{is in the spectrum of}IsUConnected
unfolding antiProperty_def
  by auto
  then have {x,y}≲1 using UConn_spectrum by auto
  moreover have x∈{x,y} by auto
  ultimately have {x}={x,y} using lepoll_1_is_sing[of {x,y}x] by auto
  moreover
  have y∈{x,y} by auto
  ultimately have y∈{x} by auto
  then have y=x by auto
  then have False using 'x≠y' by auto
}
then have ∃U∈T. x∈U∧y∉U by auto
}
then show T{is T1} unfolding isT1_def by auto

```

qed

Is is natural that separation axioms and connection axioms are anti-properties of each other; as the concepts of connectedness and separation are opposite.

To end this section, let's try to characterize anti-sober spaces.

lemma sober\_spectrum:

shows  $(A\{\text{is in the spectrum of}\}\text{IsSober}) \longleftrightarrow A \lesssim 1$

proof

assume AS:A{is in the spectrum of}IsSober

{

assume A=0

then have  $A \lesssim 1$  using empty\_lepollI by auto

}

moreover

{

assume  $A \neq 0$

note AS

moreover

have  $\text{top}:\{0,A\}\{\text{is a topology}\}$  unfolding IsATopology\_def by auto

moreover

have  $\bigcup\{0,A\}=A$  by auto

then have  $\bigcup\{0,A\}\approx A$  by auto

ultimately have  $\{0,A\}\{\text{is sober}\}$  using Spec\_def by auto

moreover

have  $\{0,A\}\{\text{is hyperconnected}\}$  using Indiscrete\_HConn by auto

moreover

have  $\{0,A\}\{\text{restricted to}\}A=\{0,A\}$  unfolding RestrictedTo\_def by auto

moreover

have  $A\{\text{is closed in}\}\{0,A\}$  unfolding IsClosed\_def by auto

moreover

note ' $A \neq 0$ '

ultimately have  $\exists x \in A. A = \text{Closure}(\{x\}, \{0,A\}) \wedge (\forall y \in \bigcup\{0,A\}. A = \text{Closure}(\{y\}, \{0,A\}) \longrightarrow y = x)$  unfolding IsSober\_def by auto

then obtain x where  $x \in A$   $A = \text{Closure}(\{x\}, \{0,A\})$  and reg: $\forall y \in A. A = \text{Closure}(\{y\}, \{0,A\}) \longrightarrow y = x$  by auto

{

fix y assume  $y \in A$

with top have  $\text{Closure}(\{y\}, \{0,A\})\{\text{is closed in}\}\{0,A\}$  using topology0.cl\_is\_closed topology0\_def by auto

moreover

from ' $y \in A$ ' top have  $y \in \text{Closure}(\{y\}, \{0,A\})$  using topology0.cl\_contains\_set topology0\_def by auto

ultimately have  $A - \text{Closure}(\{y\}, \{0,A\}) \in \{0,A\} \text{Closure}(\{y\}, \{0,A\}) \cap A \neq 0$

unfolding IsClosed\_def

by auto

then have  $A - \text{Closure}(\{y\}, \{0,A\}) = A \setminus A - \text{Closure}(\{y\}, \{0,A\}) = 0$

by auto

moreover

```

      from 'y ∈ A' 'y ∈ Closure({y}, {0, A})' have y ∈ A y ∉ A - Closure({y}, {0, A})
by auto
      ultimately have A - Closure({y}, {0, A}) = 0 by (cases A - Closure({y}, {0, A}) = A,
simp, auto)
      moreover
      from 'y ∈ A' top have Closure({y}, {0, A}) ⊆ A using topology0_def topology0.Top_3_L11(1)
by blast
      then have A - (A - Closure({y}, {0, A})) = Closure({y}, {0, A}) by auto
      ultimately have A = Closure({y}, {0, A}) by auto
    }
    with reg have ∀ y ∈ A. x = y by auto
    with 'x ∈ A' have A = {x} by blast
    then have A ≈ 1 using singleton_eqpoll_1 by auto
    then have A ≲ 1 using eqpoll_imp_lepoll by auto
  }
  ultimately show A ≲ 1 by auto
next
assume A ≲ 1
{
  fix T assume T {is a topology} ∪ T ≈ A
  {
    assume ∪ T = 0
    then have T {is sober} unfolding IsSober_def by auto
  }
  moreover
  {
    assume ∪ T ≠ 0
    then obtain x where x ∈ ∪ T by blast
    moreover
    from '∪ T ≈ A' 'A ≲ 1' have ∪ T ≲ 1 using eq_lepoll_trans by auto
    ultimately have ∪ T = {x} using lepoll_1_is_sing by auto
    moreover
    have T ⊆ Pow(∪ T) by auto
    ultimately have T ⊆ Pow({x}) by auto
    then have T ⊆ {0, {x}} by blast
    moreover
    from 'T {is a topology}' have 0 ∈ T using empty_open by auto
    moreover
    from 'T {is a topology}' have ∪ T ∈ T unfolding IsATopology_def by
auto
    with '∪ T = {x}' have {x} ∈ T by auto
    ultimately have T_def: T = {0, {x}} by auto
    then have dd: Pow(∪ T) - {0} = {{x}} by auto
    {
      fix B assume B ∈ Pow(∪ T) - {0}
      with dd have B_def: B = {x} by auto
      from 'T {is a topology}' have (∪ T) {is closed in} T using topology0_def
topology0.Top_3_L1
      by auto
    }
  }
}

```

```

    with '⋃T={x}' 'T{is a topology}' have Closure({x},T)={x} us-
ing topology0.Top_3_L8
    unfolding topology0_def by auto
    with B_def have B=Closure({x},T) by auto
    moreover
    {
      fix y assume y∈⋃T
      with '⋃T={x}' have y=x by auto
    }
    then have (∀y∈⋃T. B = Closure({y}, T) → y = x) by auto
    moreover note 'x∈⋃T'
    ultimately have (∃x∈⋃T. B = Closure({x}, T) ∧ (∀y∈⋃T. B = Closure({y},
T) → y = x))
      by auto
  }
  then have T{is sober} unfolding IsSober_def by auto
}
ultimately have T{is sober} by blast
}
then show A {is in the spectrum of} IsSober unfolding Spec_def by auto
qed

theorem (in topology0)anti_sober:
  shows (T{is anti-}IsSober) ↔ T={0,⋃T}
proof
  assume T={0,⋃T}
  {
    fix A assume A∈Pow(⋃T)(T{restricted to}A){is sober}
    {
      assume A=0
      then have A≤1 using empty_lepollI by auto
      then have A{is in the spectrum of}IsSober using sober_spectrum
by auto
    }
    moreover
    {
      assume A≠0
      have ⋃T∈{0,⋃T}0∈{0,⋃T} by auto
      with 'T={0,⋃T}' have (⋃T)∈T 0∈T by auto
      with 'A∈Pow(⋃T)' have {0,A}⊆(T{restricted to}A) unfolding RestrictedTo_def
by auto
    }
    moreover
    have ∀B∈{0,⋃T}. B=0∨B=⋃T by auto
    with 'T={0,⋃T}' have ∀B∈T. B=0∨B=⋃T by auto
    with 'A∈Pow(⋃T)' have T{restricted to}A⊆{0,A} unfolding RestrictedTo_def
by auto
    ultimately have top_def:T{restricted to}A={0,A} by auto
    moreover
    have A{is closed in}{0,A} unfolding IsClosed_def by auto

```

```

    moreover
    have {0,A}{is hyperconnected} using Indiscrete_HConn by auto
    moreover
    from 'A∈Pow(⋃T)' have (T{restricted to}A){restricted to}A=T{restricted
to}A using subspace_of_subspace[of AAT]
    by auto
    moreover
    note 'A≠0' 'A∈Pow(⋃T)'
    ultimately have A∈Pow(⋃(T{restricted to}A))-{0}A{is closed in}(T{restricted
to}A)((T{restricted to}A){restricted to}A){is hyperconnected}
    by auto
    with '(T{restricted to}A){is sober}' have  $\exists x \in \bigcup (T\{restricted\ to\}A).$ 
A=Closure({x},T{restricted to}A) $\wedge (\forall y \in \bigcup (T\{restricted\ to\}A). A=Closure(\{y\},T\{restricted$ 
to}A)  $\longrightarrow y=x$ )
    unfolding IsSober_def by auto
    with top_def have  $\exists x \in A. A=Closure(\{x\},\{0,A\}) \wedge (\forall y \in A. A=Closure(\{y\},\{0,A\})$ 
 $\longrightarrow y=x$ ) by auto
    then obtain x where  $x \in A = Closure(\{x\},\{0,A\})$  and reg: $\forall y \in A. A=Closure(\{y\},\{0,A\})$ 
 $\longrightarrow y=x$  by auto
    {
    fix y assume  $y \in A$ 
    from 'A≠0' have top:{0,A}{is a topology} using indiscrete_ptopology[of
A] indiscrete_partition[of A] Ptopology_is_a_topology(1)[of {A}A]
    by auto
    with 'y∈A' have Closure({y},{0,A}){is closed in}{0,A} using topology0.cl_is_closed
topology0_def by auto
    moreover
    from 'y∈A' top have  $y \in Closure(\{y\},\{0,A\})$  using topology0.cl_contains_set
topology0_def by auto
    ultimately have  $A-Closure(\{y\},\{0,A\}) \in \{0,A\} Closure(\{y\},\{0,A\}) \cap A \neq 0$ 
unfolding IsClosed_def
    by auto
    then have  $A-Closure(\{y\},\{0,A\}) = A \vee A-Closure(\{y\},\{0,A\}) = 0$ 
    by auto
    moreover
    from 'y∈A' 'y∈Closure({y},{0,A})' have  $y \in A \wedge y \notin A-Closure(\{y\},\{0,A\})$ 
by auto
    ultimately have  $A-Closure(\{y\},\{0,A\}) = 0$  by (cases A-Closure({y},{0,A})=A,
simp, auto)
    moreover
    from 'y∈A' top have  $Closure(\{y\},\{0,A\}) \subseteq A$  using topology0_def
topology0.Top_3_L11(1) by blast
    then have  $A-(A-Closure(\{y\},\{0,A\})) = Closure(\{y\},\{0,A\})$  by auto
    ultimately have  $A=Closure(\{y\},\{0,A\})$  by auto
    }
    with reg 'x∈A' have  $A=\{x\}$  by blast
    then have  $A \approx 1$  using singleton_eqpoll_1 by auto
    then have  $A \lesssim 1$  using eqpoll_imp_lepoll by auto
    then have A{is in the spectrum of}IsSober using sober_spectrum

```



```

by auto
  }
  ultimately have A{is in the spectrum of}IsSober by auto
}
then show T{is anti-}IsSober using antiProperty_def by auto
next
  assume T{is anti-}IsSober
  {
    fix A
    assume  $A \in T \setminus \emptyset \neq \bigcup T$ 
    then obtain x y where  $x \in A, y \in \bigcup T - A, x \neq y$  by blast
    then have  $\{x\} = \{x, y\} \cap A$  by auto
    with 'A ∈ T' have  $\{x\} \in T\{\text{restricted to}\}\{x, y\}$  unfolding RestrictedTo_def
  }
by auto
  {
    assume  $\{y\} \in T\{\text{restricted to}\}\{x, y\}$ 
    from 'y ∈  $\bigcup T - A$ ' 'x ∈ A' 'A ∈ T' have  $\bigcup (T\{\text{restricted to}\}\{x, y\}) = \{x, y\}$ 
  }
unfolding RestrictedTo_def
  by auto
  with 'x ≠ y' ' $\{y\} \in T\{\text{restricted to}\}\{x, y\}$ ' ' $\{x\} \in T\{\text{restricted to}\}\{x, y\}$ '
have  $(T\{\text{restricted to}\}\{x, y\})\{\text{is } T_2\}$ 
  unfolding isT2_def by auto
  then have  $(T\{\text{restricted to}\}\{x, y\})\{\text{is sober}\}$  using topology0.T2_imp_anti_HConn[of
T{restricted to}{x,y}]
  Top_1_L4 topology0_def topology0.anti_HConn_iff_T1_sober[of T{restricted
to}{x,y}] by auto
}
moreover
{
  assume  $\{y\} \notin T\{\text{restricted to}\}\{x, y\}$ 
  moreover
  from 'y ∈  $\bigcup T - A$ ' 'x ∈ A' 'A ∈ T' have  $T\{\text{restricted to}\}\{x, y\} \subseteq \text{Pow}(\{x, y\})$ 
unfolding RestrictedTo_def by auto
  then have  $T\{\text{restricted to}\}\{x, y\} \subseteq \{0, \{x\}, \{y\}, \{x, y\}\}$  by blast
  moreover
  note ' $\{x\} \in T\{\text{restricted to}\}\{x, y\}$ ' empty_open[OF Top_1_L4[of {x,y}]]
  moreover
  from 'y ∈  $\bigcup T - A$ ' 'x ∈ A' 'A ∈ T' have tot:  $\bigcup (T\{\text{restricted to}\}\{x, y\}) = \{x, y\}$ 
unfolding RestrictedTo_def
  by auto
  from Top_1_L4[of {x,y}] have  $\bigcup (T\{\text{restricted to}\}\{x, y\}) \in T\{\text{restricted
to}\}\{x, y\}$  unfolding IsATopology_def
  by auto
  with tot have  $\{x, y\} \in T\{\text{restricted to}\}\{x, y\}$  by auto
  ultimately have top_d_def:  $T\{\text{restricted to}\}\{x, y\} = \{0, \{x\}, \{x, y\}\}$  by
auto
  {
    fix B assume  $B \in \text{Pow}(\{x, y\}) - \{0\}$  B{is closed in}(T{restricted to}{x,y})
    with top_d_def have  $(\bigcup (T\{\text{restricted to}\}\{x, y\})) - B \in \{0, \{x\}, \{x, y\}\}$ 

```

```

unfolding IsClosed_def
  apply simp using 'B∈Pow({x,y})-{0}' by blast
  with tot have {x,y}-B∈{0,{x},{x,y}} by auto
  have xin:x∈Closure({x},T{restricted to}{x,y}) using topology0.cl_contains_set[of
T{restricted to}{x,y}{x}]
    Top_1_L4[of {x,y}] unfolding topology0_def[of (T {restricted
to} {x, y})] using tot by auto
  {
    assume {x}{is closed in}(T{restricted to}{x,y})
    then have {x,y}-{x}∈(T{restricted to}{x,y}) unfolding IsClosed_def
using tot
      by auto
    moreover
    from 'x≠y' have {x,y}-{x}={y} by auto
    ultimately have {y}∈(T{restricted to}{x,y}) by auto
    then have False using '{y}∉(T{restricted to}{x,y})' by auto
  }
  then have ¬({x}{is closed in}(T{restricted to}{x,y})) by auto
  moreover
  from tot have (Closure({x},T{restricted to}{x,y})){is closed
in}(T{restricted to}{x,y})
    using topology0.cl_is_closed unfolding topology0_def using Top_1_L4[of
{x,y}]
      tot by auto
  ultimately have ¬(Closure({x},T{restricted to}{x,y})={x}) by
auto
  moreover note xin topology0.Top_3_L11(1)[of T{restricted to}{x,y}{x}]
  tot
    ultimately have cl_x:Closure({x},T{restricted to}{x,y})={x,y}
unfolding topology0_def
  using Top_1_L4[of {x,y}] by auto
  have {y}{is closed in}(T{restricted to}{x,y}) unfolding IsClosed_def
using tot
  top_d_def 'x≠y' by auto
  then have cl_y:Closure({y},T{restricted to}{x,y})={y} using topology0.Top_3_L8[of
T{restricted to}{x,y}]
    unfolding topology0_def using Top_1_L4[of {x,y}] tot by auto
  {
    assume {x,y}-B=0
    with 'B∈Pow({x,y})-{0}' have B:{x,y}=B by auto
    with cl_x cl_y 'x≠y' have (∀m∈{x,y}. B=Closure({m},T{restricted
to}{x,y})→m=x )
      apply safe apply simp using 'x∈Closure({x},T{restricted to}{x,y})'
by auto
    moreover
    have B=Closure({x},T{restricted to}{x,y}) using cl_x B by auto
    ultimately have ∃t∈{x,y}. B=Closure({t},T{restricted to}{x,y})
    ∧ (∀m∈{x,y}. B=Closure({m},T{restricted to}{x,y})→m=t )
      by auto
  }

```

```

    }
    moreover
    {
      assume {x,y}-B≠0
      with ‘{x,y}-B∈{0,{x},{x,y}}’ have or:{x,y}-B={x}∨{x,y}-B={x,y}
by auto
      {
        assume {x,y}-B={x}
        then have x∈{x,y}-B by auto
        with ‘B∈{{x},{y},{x,y}}’ ‘x≠y’ have B:B={y} by blast
        with cl_x cl_y ‘x≠y’ have (∀m∈{x,y}. B=Closure({m},T{restricted
to}{x,y}))→m=y )
          apply safe apply simp using ‘x∈Closure({x},T{restricted
to}{x,y})’ by auto
          moreover
          have B=Closure({y},T{restricted to}{x,y}) using cl_y B by
auto
          ultimately have ∃t∈{x,y}. B=Closure({t},T{restricted to}{x,y})
∧ (∀m∈{x,y}. B=Closure({m},T{restricted to}{x,y})→m=t )
            by auto
            }
      }
      moreover
      {
        assume {x,y}-B≠{x}
        with or have {x,y}-B={x,y} by auto
        then have x∈{x,y}-By∈{x,y}-B by auto
        with ‘B∈{{x},{y},{x,y}}’ ‘x≠y’ have False by auto
      }
      ultimately have ∃t∈{x,y}. B=Closure({t},T{restricted to}{x,y})
∧ (∀m∈{x,y}. B=Closure({m},T{restricted to}{x,y})→m=t )
        by auto
      }
      ultimately have ∃t∈{x,y}. B=Closure({t},T{restricted to}{x,y})
∧ (∀m∈{x,y}. B=Closure({m},T{restricted to}{x,y})→m=t )
        by auto
      }
    }
    then have (T{restricted to}{x,y}){is sober} unfolding IsSober_def
using tot by auto
  }
  ultimately have (T{restricted to}{x,y}){is sober} by auto
  with ‘T{is anti-}IsSober’ have {x,y}{is in the spectrum of}IsSober
unfolding antiProperty_def
    using ‘x∈A’ ‘A∈T’ ‘y∈⋃T-A’ by auto
  then have {x,y}≲1 using sober_spectrum by auto
  moreover
  have x∈{x,y} by auto
  ultimately have {x,y}={x} using lepoll_1_is_sing[of {x,y}x] by auto
  moreover have y∈{x,y} by auto
  ultimately have y∈{x} by auto

```

```

      then have False using 'x≠y' by auto
    }
    then have  $T \subseteq \{0, \bigcup T\}$  by auto
    with empty_open[OF topSpaceAssum] topSpaceAssum show  $T = \{0, \bigcup T\}$  unfolding IsATopology_def
      by auto
  qed

end

```

## 54 TopologicalGroup\_ZF.thy

```
theory TopologicalGroup_ZF imports Topology_ZF_3 Group_ZF_1 Semigroup_ZF
```

```
begin
```

This theory is about the first subject of algebraic topology: topological groups.

### 54.1 Topological group: definition and notation

Topological group is a group that is a topological space at the same time. This means that a topological group is a triple of sets, say  $(G, f, T)$  such that  $T$  is a topology on  $G$ ,  $f$  is a group operation on  $G$  and both  $f$  and the operation of taking inverse in  $G$  are continuous. Since IsarMathLib defines topology without using the carrier, (see `Topology_ZF`), in our setup we just use  $\bigcup T$  instead of  $G$  and say that the pair of sets  $(\bigcup T, f)$  is a group. This way our definition of being a topological group is a statement about two sets: the topology  $T$  and the group operation  $f$  on  $G = \bigcup T$ . Since the domain of the group operation is  $G \times G$ , the pair of topologies in which  $f$  is supposed to be continuous is  $T$  and the product topology on  $G \times G$  (which we will call  $\tau$  below).

This way we arrive at the following definition of a predicate that states that pair of sets is a topological group.

**definition**

```
IsAtopologicalGroup(T,f)  $\equiv$  (T {is a topology})  $\wedge$  IsAgroup( $\bigcup T$ ,f)  $\wedge$ 
IsContinuous(ProductTopology(T,T),T,f)  $\wedge$ 
IsContinuous(T,T,GroupInv( $\bigcup T$ ,f))
```

We will inherit notation from the `topology0` locale. That locale assumes that  $T$  is a topology. For convenience we will denote  $G = \bigcup T$  and  $\tau$  to be the product topology on  $G \times G$ . To that we add some notation specific to groups. We will use additive notation for the group operation, even though we don't assume that the group is abelian. The notation  $g + A$  will mean the left translation of the set  $A$  by element  $g$ , i.e.  $g + A = \{g + a \mid a \in A\}$ . The group operation  $G$  induces a natural operation on the subsets of  $G$  defined as  $\langle A, B \rangle \mapsto \{x + y \mid x \in A, y \in B\}$ . Such operation has been considered in `func_ZF` and called  $f$  "lifted to subsets of"  $G$ . We will denote the value of such operation on sets  $A, B$  as  $A + B$ . The set of neighborhoods of zero (denoted  $\mathcal{N}_0$ ) is the collection of (not necessarily open) sets whose interior contains the neutral element of the group.

```
locale topgroup = topology0 +
```

```
fixes G
```

```
defines G_def [simp]: G  $\equiv$   $\bigcup T$ 
```

```

fixes prodtop ( $\tau$ )
defines prodtop_def [simp]:  $\tau \equiv \text{ProductTopology}(T,T)$ 

fixes f

assumes Ggroup: IsAgroup(G,f)

assumes fcon: IsContinuous( $\tau,T,f$ )

assumes inv_cont: IsContinuous( $T,T,\text{GroupInv}(G,f)$ )

fixes grop (infixl + 90)
defines grop_def [simp]:  $x+y \equiv f\langle x,y \rangle$ 

fixes grinv (- _ 89)
defines grinv_def [simp]:  $(-x) \equiv \text{GroupInv}(G,f)(x)$ 

fixes grsub (infixl - 90)
defines grsub_def [simp]:  $x-y \equiv x+(-y)$ 

fixes setinv (- _ 72)
defines setninv_def [simp]:  $-A \equiv \text{GroupInv}(G,f)(A)$ 

fixes ltrans (infix + 73)
defines ltrans_def [simp]:  $x + A \equiv \text{LeftTranslation}(G,f,x)(A)$ 

fixes rtrans (infix + 73)
defines rtrans_def [simp]:  $A + x \equiv \text{RightTranslation}(G,f,x)(A)$ 

fixes setadd (infixl + 71)
defines setadd_def [simp]:  $A+B \equiv (f \text{ \{lifted to subsets of\} } G)\langle A,B \rangle$ 

fixes gzero (0)
defines gzero_def [simp]:  $0 \equiv \text{TheNeutralElement}(G,f)$ 

fixes zerohoods ( $\mathcal{N}_0$ )
defines zerohoods_def [simp]:  $\mathcal{N}_0 \equiv \{A \in \text{Pow}(G). 0 \in \text{int}(A)\}$ 

fixes listsum ( $\sum$  _ 70)
defines listsum_def[simp]:  $\sum k \equiv \text{Fold1}(f,k)$ 

```

The first lemma states that we indeed talk about topological group in the context of `topgroup` locale.

```

lemma (in topgroup) topGroup: shows IsAtopologicalGroup(T,f)
  using topSpaceAssum Ggroup fcon inv_cont IsAtopologicalGroup_def
  by simp

```

If a pair of sets  $(T, f)$  forms a topological group, then all theorems proven

in the `topgroup` context are valid as applied to  $(T, f)$ .

```
lemma topGroupLocale: assumes IsAtopologicalGroup(T,f)
  shows topgroup(T,f)
  using assms IsAtopologicalGroup_def topgroup_def
    topgroup_axioms.intro topology0_def by simp
```

We can use the `group0` locale in the context of `topgroup`.

```
lemma (in topgroup) group0_valid_in_tgroup: shows group0(G,f)
  using Ggroup group0_def by simp
```

We can use `semigr0` locale in the context of `topgroup`.

```
lemma (in topgroup) semigr0_valid_in_tgroup: shows semigr0(G,f)
  using Ggroup IsAgroup_def IsAmonoid_def semigr0_def by simp
```

We can use the `prod_top_spaces0` locale in the context of `topgroup`.

```
lemma (in topgroup) prod_top_spaces0_valid: shows prod_top_spaces0(T,T,T)
  using topSpaceAssum prod_top_spaces0_def by simp
```

Negative of a group element is in group.

```
lemma (in topgroup) neg_in_tgroup: assumes g∈G shows (-g) ∈ G
proof -
  from assms have GroupInv(G,f)(g) ∈ G
    using group0_valid_in_tgroup group0.inverse_in_group by blast
  thus thesis by simp
qed
```

Zero is in the group.

```
lemma (in topgroup) zero_in_tgroup: shows 0∈G
proof -
  have TheNeutralElement(G,f) ∈ G
    using group0_valid_in_tgroup group0.group0_2_L2 by blast
  then show 0∈G by simp
qed
```

Of course the product topology is a topology (on  $G \times G$ ).

```
lemma (in topgroup) prod_top_on_G:
  shows  $\tau$  {is a topology} and  $\bigcup \tau = G \times G$ 
  using topSpaceAssum Top_1_4_T1 by auto
```

Let's recall that  $f$  is a binary operation on  $G$  in this context.

```
lemma (in topgroup) topgroup_f_binop: shows f : G×G → G
  using Ggroup group0_def group0.group_oper_assocA by simp
```

A subgroup of a topological group is a topological group with relative topology and restricted operation. Relative topology is the same as  $T \text{ \{restricted to\} } H$  which is defined to be  $\{V \cap H : V \in T\}$  in ZF1 theory.

```
lemma (in topgroup) top_subgroup: assumes A1: IsAsubgroup(H,f)
```

```

shows IsAtopologicalGroup(T {restricted to} H, restrict(f, H×H))
proof -
  let  $\tau_0 = T$  {restricted to} H
  let  $f_H = \text{restrict}(f, H \times H)$ 
  have  $\bigcup \tau_0 = G \cap H$  using union_restrict by simp
  also from A1 have ... = H
    using group0_valid_in_tgroup group0.group0_3_L2 by blast
  finally have  $\bigcup \tau_0 = H$  by simp
  have  $\tau_0$  {is a topology} using Top_1_L4 by simp
  moreover from A1 ' $\bigcup \tau_0 = H$ ' have IsAgroup( $\bigcup \tau_0, f_H$ )
    using IsAsubgroup_def by simp
  moreover have IsContinuous(ProductTopology( $\tau_0, \tau_0$ ),  $\tau_0, f_H$ )
proof -
  have two_top_spaces0( $\tau, T, f$ )
    using topSpaceAssum prod_top_on_G topgroup_f_binop prod_top_on_G
two_top_spaces0_def by simp
  moreover
  from A1 have  $H \subseteq G$  using group0_valid_in_tgroup group0.group0_3_L2
  by simp
  then have  $H \times H \subseteq \bigcup \tau$  using prod_top_on_G by auto
  moreover have IsContinuous( $\tau, T, f$ ) using fcon by simp
  ultimately have
    IsContinuous( $\tau$  {restricted to}  $H \times H$ ,  $T$  {restricted to}  $f_H(H \times H), f_H$ )
    using two_top_spaces0.restr_restr_image_cont by simp
  moreover have
    ProductTopology( $\tau_0, \tau_0$ ) =  $\tau$  {restricted to}  $H \times H$ 
    using topSpaceAssum prod_top_restr_comm by simp
  moreover from A1 have  $f_H(H \times H) = H$  using image_subgr_op
  by simp
  ultimately show thesis by simp
qed
moreover have IsContinuous( $\tau_0, \tau_0, \text{GroupInv}(\bigcup \tau_0, f_H)$ )
proof -
  let  $g = \text{restrict}(\text{GroupInv}(G, f), H)$ 
  have  $\text{GroupInv}(G, f) : G \rightarrow G$ 
    using Ggroup group0_2_T2 by simp
  then have two_top_spaces0( $T, T, \text{GroupInv}(G, f)$ )
    using topSpaceAssum two_top_spaces0_def by simp
  moreover from A1 have  $H \subseteq \bigcup T$ 
    using group0_valid_in_tgroup group0.group0_3_L2
  by simp
  ultimately have
    IsContinuous( $\tau_0, T$  {restricted to}  $g(H), g$ )
    using inv_cont two_top_spaces0.restr_restr_image_cont
  by simp
  moreover from A1 have  $g(H) = H$ 
    using group0_valid_in_tgroup group0.restr_inv_onto
  by simp
  moreover

```



```

    from A1 have GroupInv(H,fH) = g
      using group0_valid_in_tgroup group0.group0_3_T1
      by simp
    with '⋃ τ0 = H' have g = GroupInv(⋃ τ0,fH) by simp
    ultimately show thesis by simp
  qed
  ultimately show thesis unfolding IsAtopologicalGroup_def by simp
qed

```

## 54.2 Interval arithmetic, translations and inverse of set

In this section we list some properties of operations of translating a set and reflecting it around the neutral element of the group. Many of the results are proven in other theories, here we just collect them and rewrite in notation specific to the `topgroup` context.

Different ways of looking at adding sets.

```

lemma (in topgroup) interval_add: assumes A⊆G B⊆G shows
  A+B ⊆ G and A+B = f(A×B)  A+B = (⋃ x∈A. x+B)
proof -
  from assms show A+B ⊆ G and A+B = f(A×B)
    using topgroup_f_binop lift_subsets_explained by auto
  from assms show A+B = (⋃ x∈A. x+B)
    using group0_valid_in_tgroup group0.image_ltrans_union by simp
qed

```

Right and left translations are continuous.

```

lemma (in topgroup) trans_cont: assumes g∈G shows
  IsContinuous(T,T,RightTranslation(G,f,g)) and
  IsContinuous(T,T,LeftTranslation(G,f,g))
using assms group0_valid_in_tgroup group0.trans_eq_section
topgroup_f_binop fcon prod_top_spaces0_valid
prod_top_spaces0.fix_1st_var_cont prod_top_spaces0.fix_2nd_var_cont
by auto

```

Left and right translations of an open set are open.

```

lemma (in topgroup) open_tr_open: assumes g∈G and V∈T
  shows g+V ∈ T and V+g ∈ T
using assms neg_in_tgroup trans_cont IsContinuous_def
group0_valid_in_tgroup group0.trans_image_vimage by auto

```

Right and left translations are homeomorphisms.

```

lemma (in topgroup) tr_homeo: assumes g∈G shows
  IsAhomeomorphism(T,T,RightTranslation(G,f,g)) and
  IsAhomeomorphism(T,T,LeftTranslation(G,f,g))
using assms group0_valid_in_tgroup group0.trans_bij trans_cont open_tr_open
bij_cont_open_homeo by auto

```

Translations preserve interior.

```
lemma (in topgroup) trans_interior: assumes A1:  $g \in G$  and A2:  $A \subseteq G$ 
  shows  $g + \text{int}(A) = \text{int}(g+A)$ 
proof -
  from assms have  $A \subseteq \bigcup T$  and IsAhomeomorphism( $T, T, \text{LeftTranslation}(G, f, g)$ )
  using tr_homeo by auto
  then show thesis using int_top_invariant by simp
qed
```

Inverse of an open set is open.

```
lemma (in topgroup) open_inv_open: assumes  $V \in T$  shows  $(-V) \in T$ 
  using assms group0_valid_in_tgroup group0.inv_image_vimage
  inv_cont IsContinuous_def by simp
```

Inverse is a homeomorphism.

```
lemma (in topgroup) inv_homeo: shows IsAhomeomorphism( $T, T, \text{GroupInv}(G, f)$ )
  using group0_valid_in_tgroup group0.group_inv_bij inv_cont open_inv_open
  bij_cont_open_homeo by simp
```

Taking negative preserves interior.

```
lemma (in topgroup) int_inv_inv_int: assumes  $A \subseteq G$ 
  shows  $\text{int}(-A) = -(\text{int}(A))$ 
  using assms inv_homeo int_top_invariant by simp
```

### 54.3 Neighborhoods of zero

Zero neighborhoods are (not necessarily open) sets whose interior contains the neutral element of the group. In the topgroup locale the collection of neighborhoods of zero is denoted  $\mathcal{N}_0$ .

The whole sspace is a neighborhood of zero.

```
lemma (in topgroup) zneigh_not_empty: shows  $G \in \mathcal{N}_0$ 
  using topSpaceAssum IsATopology_def Top_2_L3 zero_in_tgroup
  by simp
```

Any element belongs to the interior of any neighborhood of zero translated by that element.

```
lemma (in topgroup) elem_in_int_trans:
  assumes A1:  $g \in G$  and A2:  $H \in \mathcal{N}_0$ 
  shows  $g \in \text{int}(g+H)$ 
proof -
  from A2 have  $0 \in \text{int}(H)$  and  $\text{int}(H) \subseteq G$  using Top_2_L2 by auto
  with A1 have  $g \in g + \text{int}(H)$ 
  using group0_valid_in_tgroup group0.neut_trans_elem by simp
  with assms show thesis using trans_interior by simp
qed
```

Negative of a neighborhood of zero is a neighborhood of zero.

```

lemma (in topgroup) neg_neigh_neigh: assumes  $H \in \mathcal{N}_0$ 
  shows  $(-H) \in \mathcal{N}_0$ 
proof -
  from assms have  $\text{int}(H) \subseteq G$  and  $0 \in \text{int}(H)$  using Top_2_L1 by auto
  with assms have  $0 \in \text{int}(-H)$  using group0_valid_in_tgroup group0.neut_inv_neut
    int_inv_inv_int by simp
  moreover
  have GroupInv( $G, f$ ):  $G \rightarrow G$  using Ggroup group0_2_T2 by simp
  then have  $(-H) \subseteq G$  using func1_1_L6 by simp
  ultimately show thesis by simp
qed

```

Translating an open set by a negative of a point that belongs to it makes it a neighborhood of zero.

```

lemma (in topgroup) open_trans_neigh: assumes A1:  $U \in \mathcal{T}$  and  $g \in U$ 
  shows  $(-g) + U \in \mathcal{N}_0$ 
proof -
  let  $H = (-g) + U$ 
  from assms have  $g \in G$  by auto
  then have  $(-g) \in G$  using neg_in_tgroup by simp
  with A1 have  $H \in \mathcal{T}$  using open_tr_open by simp
  hence  $H \subseteq G$  by auto
  moreover have  $0 \in \text{int}(H)$ 
  proof -
    from assms have  $U \subseteq G$  and  $g \in U$  by auto
    with ' $H \in \mathcal{T}$ ' show  $0 \in \text{int}(H)$ 
      using group0_valid_in_tgroup group0.elem_trans_neut Top_2_L3
      by auto
  qed
  ultimately show thesis by simp
qed

```

## 54.4 Closure in topological groups

This section is devoted to a characterization of closure in topological groups.

Closure of a set is contained in the sum of the set and any neighborhood of zero.

```

lemma (in topgroup) cl_contains_zneigh:
  assumes A1:  $A \subseteq G$  and A2:  $H \in \mathcal{N}_0$ 
  shows  $\text{cl}(A) \subseteq A + H$ 
proof
  fix  $x$  assume  $x \in \text{cl}(A)$ 
  from A1 have  $\text{cl}(A) \subseteq G$  using Top_3_L11 by simp
  with ' $x \in \text{cl}(A)$ ' have  $x \in G$  by auto
  have  $\text{int}(H) \subseteq G$  using Top_2_L2 by auto
  let  $V = \text{int}(x + (-H))$ 
  have  $V = x + (-\text{int}(H))$ 
  proof -

```

```

    from A2 'x∈G' have V = x + int(-H)
      using neg_neigh_neigh trans_interior by simp
    with A2 show thesis using int_inv_inv_int by simp
  qed
  have A∩V ≠ 0
  proof -
    from A2 'x∈G' 'x ∈ cl(A)' have V∈T and x ∈ cl(A) ∩ V
      using neg_neigh_neigh elem_in_int_trans Top_2_L2 by auto
    with A1 show A∩V ≠ 0 using cl_inter_neigh by simp
  qed
  then obtain y where y∈A and y∈V by auto
  with 'V = x + (-int(H))' 'int(H) ⊆ G' 'x∈G' have x ∈ y+int(H)
    using group0_valid_in_tgroup group0.ltrans_inv_in by simp
  with 'y∈A' have x ∈ (⋃y∈A. y+H) using Top_2_L1 func1_1_L8 by auto
  with assms show x ∈ A+H using interval_add by simp
qed

```

The next theorem provides a characterization of closure in topological groups in terms of neighborhoods of zero.

```

theorem (in topgroup) cl_topgroup:
  assumes A⊆G shows cl(A) = (⋂H∈N0. A+H)
proof
  from assms show cl(A) ⊆ (⋂H∈N0. A+H)
    using zneigh_not_empty cl_contains_zneigh by auto
next
  { fix x assume x ∈ (⋂H∈N0. A+H)
    then have x ∈ A+G using zneigh_not_empty by auto
    with assms have x∈G using interval_add by blast
    have ∀U∈T. x∈U → U∩A ≠ 0
    proof -
      { fix U assume U∈T and x∈U
        let H = -((-x)+U)
        from 'U∈T' and 'x∈U' have (-x)+U ⊆ G and H ∈ N0
          using open_trans_neigh neg_neigh_neigh by auto
        with 'x ∈ (⋂H∈N0. A+H)' have x ∈ A+H by auto
        with assms 'H ∈ N0' obtain y where y∈A and x ∈ y+H
          using interval_add by auto
        have y∈U
        proof -
          from assms 'y∈A' have y∈G by auto
          with '(-x)+U ⊆ G' and 'x ∈ y+H' have y ∈ x+((-x)+U)
            using group0_valid_in_tgroup group0.ltrans_inv_in by simp
          with 'U∈T' 'x∈G' show y∈U
            using neg_in_tgroup group0_valid_in_tgroup group0.trans_comp_image
              group0.group0_2_L6 group0.trans_neutral image_id_same
              by auto
        qed
        with 'y∈A' have U∩A ≠ 0 by auto
      } thus thesis by simp
    }

```

```

qed
with assms 'x∈G' have x ∈ cl(A) using inter_neigh_cl by simp
} thus (⋂ H∈N0. A+H) ⊆ cl(A) by auto
qed

```

## 54.5 Sums of sequences of elements and subsets

In this section we consider properties of the function  $G^n \rightarrow G$ ,  $x = (x_0, x_1, \dots, x_{n-1}) \mapsto \sum_{i=0}^{n-1} x_i$ . We will model the cartesian product  $G^n$  by the space of sequences  $n \rightarrow G$ , where  $n = \{0, 1, \dots, n-1\}$  is a natural number. This space is equipped with a natural product topology defined in `Topology_ZF_3`.

Let's recall first that the sum of elements of a group is an element of the group.

```

lemma (in topgroup) sum_list_in_group:
  assumes n ∈ nat and x: succ(n)→G
  shows (∑ x) ∈ G
proof -
  from assms have semigr0(G,f) and n ∈ nat x: succ(n)→G
  using semigr0_valid_in_tgroup by auto
  then have Fold1(f,x) ∈ G by (rule semigr0.prod_type)
  thus (∑ x) ∈ G by simp
qed

```

In this context  $x+y$  is the same as the value of the group operation on the elements  $x$  and  $y$ . Normally we shouldn't need to state this as a separate lemma.

```

lemma (in topgroup) grop_def1: shows f⟨x,y⟩ = x+y by simp

```

Another theorem from `Semigroup_ZF` theory that is useful to have in the additive notation.

```

lemma (in topgroup) shorter_set_add:
  assumes n ∈ nat and x: succ(succ(n))→G
  shows (∑ x) = (∑ Init(x)) + (x(succ(n)))
proof -
  from assms have semigr0(G,f) and n ∈ nat x: succ(succ(n))→G
  using semigr0_valid_in_tgroup by auto
  then have Fold1(f,x) = f⟨Fold1(f,Init(x)),x(succ(n))⟩
  by (rule semigr0.shorter_seq)
  thus thesis by simp
qed

```

Sum is a continuous function in the product topology.

```

theorem (in topgroup) sum_continuous: assumes n ∈ nat
  shows IsContinuous(SeqProductTopology(succ(n),T),T,{⟨x,∑ x⟩.x∈succ(n)→G})
proof -
  note 'n ∈ nat'

```

```

moreover have IsContinuous(SeqProductTopology(succ(0),T),T,{⟨x,∑x⟩.x∈succ(0)→G})
proof -
  have {⟨x,∑x⟩.x∈succ(0)→G} = {⟨x,x(0)⟩. x∈1→G}
    using semigr0_valid_in_tgroup semigr0.prod_of_1elem by simp
  moreover have
    IsAhomeomorphism(SeqProductTopology(1,T),T,{⟨x,x(0)⟩. x∈1→⋃T})
    using topSpaceAssum singleton_prod_top1 by simp
  ultimately show thesis using IsAhomeomorphism_def by simp
qed
moreover have ∀k∈nat.
  IsContinuous(SeqProductTopology(succ(k),T),T,{⟨x,∑x⟩.x∈succ(k)→G})
  →
  IsContinuous(SeqProductTopology(succ(succ(k)),T),T,{⟨x,∑x⟩.x∈succ(succ(k))→G})
proof -
  { fix k assume k ∈ nat
    let s = {⟨x,∑x⟩.x∈succ(k)→G}
    let g = {⟨p,⟨s(fst(p)),snd(p)⟩⟩. p ∈ (succ(k)→G)×G}
    let h = {⟨x,⟨Init(x),x(succ(k))⟩⟩. x ∈ succ(succ(k))→G}
    let φ = SeqProductTopology(succ(k),T)
    let ψ = SeqProductTopology(succ(succ(k)),T)
    assume IsContinuous(φ,T,s)
    from 'k ∈ nat' have s: (succ(k)→G) → G
      using sum_list_in_group ZF_fun_from_total by simp
    have h: (succ(succ(k))→G)→(succ(k)→G)×G
    proof -
      { fix x assume x ∈ succ(succ(k))→G
        with 'k ∈ nat' have Init(x) ∈ (succ(k)→G)
          using init_props by simp
        with 'k ∈ nat' 'x : succ(succ(k))→G'
          have ⟨Init(x),x(succ(k))⟩ ∈ (succ(k)→G)×G
            using apply_funtype by blast
        } then show thesis using ZF_fun_from_total by simp
      }
    qed
    moreover have g: ((succ(k)→G)×G)→(G×G)
    proof -
      { fix p assume p ∈ (succ(k)→G)×G
        hence fst(p): succ(k)→G and snd(p) ∈ G by auto
        with 's: (succ(k)→G) → G' have ⟨s(fst(p)),snd(p)⟩ ∈ G×G
          using apply_funtype by blast
        } then show g: ((succ(k)→G)×G)→(G×G) using ZF_fun_from_total
          by simp
      }
    qed
    moreover have f : G×G → G using topgroup_f_binop by simp
    ultimately have f 0 g 0 h : (succ(succ(k))→G)→G using comp_fun
      by blast
    from 'k ∈ nat' have IsContinuous(ψ,ProductTopology(φ,T),h)
      using topSpaceAssum finite_top_prod_homeo IsAhomeomorphism_def
      by simp
    moreover have IsContinuous(ProductTopology(φ,T),τ,g)

```

```

proof -
  from topSpaceAssum have
    T {is a topology}  $\varphi$  {is a topology}  $\bigcup \varphi = \text{succ}(k) \rightarrow G$ 
    using seq_prod_top_is_top by auto
  moreover from ' $\bigcup \varphi = \text{succ}(k) \rightarrow G$ ' 's:  $(\text{succ}(k) \rightarrow G) \rightarrow G$ '
    have s:  $\bigcup \varphi \rightarrow \bigcup T$  by simp
  moreover note 'IsContinuous( $\varphi, T, s$ )'
  moreover from ' $\bigcup \varphi = \text{succ}(k) \rightarrow G$ '
    have g =  $\{\langle p, \langle s(\text{fst}(p)), \text{snd}(p) \rangle \rangle \mid p \in \bigcup \varphi \times \bigcup T\}$ 
    by simp
  ultimately have IsContinuous(ProductTopology( $\varphi, T$ ), ProductTopology( $T, T$ ), g)
    using cart_prod_cont1 by blast
  thus thesis by simp
qed
moreover have IsContinuous( $\tau, T, f$ ) using fcon by simp
moreover have  $\{\langle x, \sum x \rangle \mid x \in \text{succ}(\text{succ}(k)) \rightarrow G\} = f \circ g \circ h$ 
proof -
  let d =  $\{\langle x, \sum x \rangle \mid x \in \text{succ}(\text{succ}(k)) \rightarrow G\}$ 
  from 'k ∈ nat' have  $\forall x \in \text{succ}(\text{succ}(k)) \rightarrow G. (\sum x) \in G$ 
    using sum_list_in_group by blast
  then have d:  $(\text{succ}(\text{succ}(k)) \rightarrow G) \rightarrow G$ 
    using sum_list_in_group ZF_fun_from_total by simp
  moreover note 'f ∘ g ∘ h :  $(\text{succ}(\text{succ}(k)) \rightarrow G) \rightarrow G$ '
  moreover have  $\forall x \in \text{succ}(\text{succ}(k)) \rightarrow G. d(x) = (f \circ g \circ h)(x)$ 
proof
  fix x assume x ∈  $\text{succ}(\text{succ}(k)) \rightarrow G$ 
  then have I:  $h(x) = \langle \text{Init}(x), x(\text{succ}(k)) \rangle$ 
    using ZF_fun_from_tot_val1 by simp
  moreover from 'k ∈ nat' 'x ∈  $\text{succ}(\text{succ}(k)) \rightarrow G$ '
    have Init(x):  $\text{succ}(k) \rightarrow G$ 
    using init_props by simp
  moreover from 'k ∈ nat' 'x:  $\text{succ}(\text{succ}(k)) \rightarrow G$ '
    have II:  $x(\text{succ}(k)) \in G$ 
    using apply_funtype by blast
  ultimately have  $h(x) \in (\text{succ}(k) \rightarrow G) \times G$  by simp
  then have  $g(h(x)) = \langle s(\text{fst}(h(x))), \text{snd}(h(x)) \rangle$ 
    using ZF_fun_from_tot_val1 by simp
  with I have  $g(h(x)) = \langle s(\text{Init}(x)), x(\text{succ}(k)) \rangle$ 
    by simp
  with 'Init(x):  $\text{succ}(k) \rightarrow G$ ' have  $g(h(x)) = \langle \sum \text{Init}(x), x(\text{succ}(k)) \rangle$ 
    using ZF_fun_from_tot_val1 by simp
  with 'k ∈ nat' 'x:  $\text{succ}(\text{succ}(k)) \rightarrow G$ '
    have  $f(g(h(x))) = (\sum x)$ 
    using shorter_set_add by simp
  with 'x ∈  $\text{succ}(\text{succ}(k)) \rightarrow G$ ' have  $f(g(h(x))) = d(x)$ 
    using ZF_fun_from_tot_val1 by simp
moreover from
  'h:  $(\text{succ}(\text{succ}(k)) \rightarrow G) \rightarrow (\text{succ}(k) \rightarrow G) \times G$ '
  'g:  $((\text{succ}(k) \rightarrow G) \times G) \rightarrow (G \times G)$ '

```

```

      'f:(G×G)→G' 'x∈succ(succ(k))→G'
      have (f 0 g 0 h)(x) = f(g(h(x))) by (rule func1_1_L18)
      ultimately show d(x) = (f 0 g 0 h)(x) by simp
    qed
    ultimately show {⟨x, ∑ x⟩.x∈succ(succ(k))→G} = f 0 g 0 h
      using func_eq by simp
  qed
  moreover note 'IsContinuous(τ,T,f)'
  ultimately have IsContinuous(ψ,T,{⟨x, ∑ x⟩.x∈succ(succ(k))→G})
    using comp_cont3 by simp
} thus thesis by simp
qed
ultimately show thesis by (rule ind_on_nat)
qed
end

```



## 55 Metamath\_interface.thy

```
theory Metamath_interface imports Complex_ZF MMI_prelude
```

```
begin
```

This theory contains some lemmas that make it possible to use the theorems translated from Metamath in a the `complex0` context.

### 55.1 MMIsar0 and complex0 contexts.

In the section we show a lemma that the assumptions in `complex0` context imply the assumptions of the `MMIsar0` context. The `Metamath_sampler` theory provides examples how this lemma can be used.

The next lemma states that we can use the theorems proven in the `MMIsar0` context in the `complex0` context. Unfortunately we have to use low level Isabelle methods "rule" and "unfold" in the proof, simp and blast fail on the order axioms.

```
lemma (in complex0) MMIsar_valid:
  shows MMIsar0( $\mathbb{R}$ ,  $\mathbb{C}$ , 1, 0, i, CplxAdd(R,A), CplxMul(R,A,M),
    StrictVersion(CplxROrder(R,A,r)))
proof -
  let real =  $\mathbb{R}$ 
  let complex =  $\mathbb{C}$ 
  let zero = 0
  let one = 1
  let iunit = i
  let caddset = CplxAdd(R,A)
  let cmulset = CplxMul(R,A,M)
  let lessrrel = StrictVersion(CplxROrder(R,A,r))
  have ( $\forall a\ b. a \in \text{real} \wedge b \in \text{real} \longrightarrow$ 
     $\langle a, b \rangle \in \text{lessrrel} \longleftrightarrow \neg (a = b \vee \langle b, a \rangle \in \text{lessrrel})$ )
  proof -
    have I:
       $\forall a\ b. a \in \mathbb{R} \wedge b \in \mathbb{R} \longrightarrow (a <_{\mathbb{R}} b \longleftrightarrow \neg(a=b \vee b <_{\mathbb{R}} a))$ 
      using pre_axlttri by blast
    { fix a b assume  $a \in \text{real} \wedge b \in \text{real}$ 
      with I have  $(a <_{\mathbb{R}} b \longleftrightarrow \neg(a=b \vee b <_{\mathbb{R}} a))$ 
    }
  by blast
  hence
     $\langle a, b \rangle \in \text{lessrrel} \longleftrightarrow \neg (a = b \vee \langle b, a \rangle \in \text{lessrrel})$ 
  by simp
  } thus ( $\forall a\ b. a \in \text{real} \wedge b \in \text{real} \longrightarrow$ 
    ( $\langle a, b \rangle \in \text{lessrrel} \longleftrightarrow \neg (a = b \vee \langle b, a \rangle \in \text{lessrrel})$ ))
  by blast
qed
moreover
```

```

have (∀ a b c.
  a ∈ real ∧ b ∈ real ∧ c ∈ real →
  ⟨a, b⟩ ∈ lessrrel ∧ ⟨b, c⟩ ∈ lessrrel → ⟨a, c⟩ ∈ lessrrel)
proof -
  have II: ∀ a b c. a ∈ ℝ ∧ b ∈ ℝ ∧ c ∈ ℝ →
    ((a <ℝ b ∧ b <ℝ c) → a <ℝ c)
    using pre_axlttrn by blast
  { fix a b c assume a ∈ real ∧ b ∈ real ∧ c ∈ real
    with II have (a <ℝ b ∧ b <ℝ c) → a <ℝ c
  }
by blast
  hence
  ⟨a, b⟩ ∈ lessrrel ∧ ⟨b, c⟩ ∈ lessrrel → ⟨a, c⟩ ∈ lessrrel
by simp
} thus (∀ a b c.
  a ∈ real ∧ b ∈ real ∧ c ∈ real →
  ⟨a, b⟩ ∈ lessrrel ∧ ⟨b, c⟩ ∈ lessrrel → ⟨a, c⟩ ∈ lessrrel)
  by blast
qed
moreover have (∀ A B C.
  A ∈ real ∧ B ∈ real ∧ C ∈ real →
  ⟨A, B⟩ ∈ lessrrel →
  ⟨caddset ⟨C, A⟩, caddset ⟨C, B⟩⟩ ∈ lessrrel)
  using pre_axltadd by simp
moreover have (∀ A B. A ∈ real ∧ B ∈ real →
  ⟨zero, A⟩ ∈ lessrrel ∧ ⟨zero, B⟩ ∈ lessrrel →
  ⟨zero, cmulset ⟨A, B⟩⟩ ∈ lessrrel)
  using pre_axmulgt0 by simp
moreover have
  (∀ S. S ⊆ real ∧ S ≠ 0 ∧ (∃ x ∈ real. ∀ y ∈ S. ⟨y, x⟩ ∈ lessrrel) →
  (∃ x ∈ real.
    (∀ y ∈ S. ⟨x, y⟩ ∉ lessrrel) ∧
    (∀ y ∈ real. ⟨y, x⟩ ∈ lessrrel → (∃ z ∈ S. ⟨y, z⟩ ∈ lessrrel))))
  using pre_axsup by simp
moreover have ℝ ⊆ ℂ using axresscn by simp
moreover have 1 ≠ 0 using ax1ne0 by simp
moreover have ℂ isASet by simp
moreover have CplxAdd(R,A) : ℂ × ℂ → ℂ
  using axaddopr by simp
moreover have CplxMul(R,A,M) : ℂ × ℂ → ℂ
  using axmulopr by simp
moreover have
  ∀ a b. a ∈ ℂ ∧ b ∈ ℂ → a · b = b · a
  using axmulcom by simp
hence (∀ a b. a ∈ ℂ ∧ b ∈ ℂ →
  cmulset ⟨a, b⟩ = cmulset ⟨b, a⟩
) by simp
moreover have ∀ a b. a ∈ ℂ ∧ b ∈ ℂ → a + b ∈ ℂ
  using axaddcl by simp
hence (∀ a b. a ∈ ℂ ∧ b ∈ ℂ →

```

```

      caddset ⟨a, b⟩ ∈ ℂ
    ) by simp
  moreover have ∀ a b. a ∈ ℂ ∧ b ∈ ℂ ⟶ a · b ∈ ℂ
    using axmulcl by simp
  hence (∀ a b. a ∈ ℂ ∧ b ∈ ℂ ⟶
    cmulset ⟨a, b⟩ ∈ ℂ ) by simp
  moreover have
    ∀ a b c. a ∈ ℂ ∧ b ∈ ℂ ∧ c ∈ ℂ ⟶
    a · (b + c) = a · b + a · c
    using axdistr by simp
  hence ∀ a b c.
    a ∈ ℂ ∧ b ∈ ℂ ∧ c ∈ ℂ ⟶
    cmulset ⟨a, caddset ⟨b, c⟩⟩ =
    caddset
    ⟨cmulset ⟨a, b⟩, cmulset ⟨a, c⟩⟩
    by simp
  moreover have ∀ a b. a ∈ ℂ ∧ b ∈ ℂ ⟶
    a + b = b + a
    using axaddcom by simp
  hence ∀ a b.
    a ∈ ℂ ∧ b ∈ ℂ ⟶
    caddset ⟨a, b⟩ = caddset ⟨b, a⟩ by simp
  moreover have ∀ a b c. a ∈ ℂ ∧ b ∈ ℂ ∧ c ∈ ℂ ⟶
    a + b + c = a + (b + c)
    using axaddass by simp
  hence ∀ a b c.
    a ∈ ℂ ∧ b ∈ ℂ ∧ c ∈ ℂ ⟶
    caddset ⟨caddset ⟨a, b⟩, c⟩ =
    caddset ⟨a, caddset ⟨b, c⟩⟩ by simp
  moreover have
    ∀ a b c. a ∈ ℂ ∧ b ∈ ℂ ∧ c ∈ ℂ ⟶ a · b · c = a · (b · c)
    using axmulass by simp
  hence ∀ a b c.
    a ∈ ℂ ∧ b ∈ ℂ ∧ c ∈ ℂ ⟶
    cmulset ⟨cmulset ⟨a, b⟩, c⟩ =
    cmulset ⟨a, cmulset ⟨b, c⟩⟩ by simp
  moreover have 1 ∈ ℝ using ax1re by simp
  moreover have i · i + 1 = 0
    using axi2m1 by simp
  hence caddset ⟨cmulset ⟨i, i⟩, 1⟩ = 0 by simp
  moreover have ∀ a. a ∈ ℂ ⟶ a + 0 = a
    using ax0id by simp
  hence ∀ a. a ∈ ℂ ⟶ caddset ⟨a, 0⟩ = a by simp
  moreover have i ∈ ℂ using axicn by simp
  moreover have ∀ a. a ∈ ℂ ⟶ (∃ x ∈ ℂ. a + x = 0)
    using axnegex by simp
  hence ∀ a. a ∈ ℂ ⟶
    (∃ x ∈ ℂ. caddset ⟨a, x⟩ = 0) by simp
  moreover have ∀ a. a ∈ ℂ ∧ a ≠ 0 ⟶ (∃ x ∈ ℂ. a · x = 1)

```

using axrecex by simp  
 hence  $\forall a. a \in \mathbb{C} \wedge a \neq 0 \longrightarrow$   
    $(\exists x \in \mathbb{C}. \text{cmulset } \langle a, x \rangle = 1)$  by simp  
 moreover have  $\forall a. a \in \mathbb{C} \longrightarrow a \cdot 1 = a$   
   using ax1id by simp  
 hence  $\forall a. a \in \mathbb{C} \longrightarrow$   
    $\text{cmulset } \langle a, 1 \rangle = a$  by simp  
 moreover have  $\forall a b. a \in \mathbb{R} \wedge b \in \mathbb{R} \longrightarrow a + b \in \mathbb{R}$   
   using axaddrcl by simp  
 hence  $\forall a b. a \in \mathbb{R} \wedge b \in \mathbb{R} \longrightarrow$   
    $\text{caddset } \langle a, b \rangle \in \mathbb{R}$  by simp  
 moreover have  $\forall a b. a \in \mathbb{R} \wedge b \in \mathbb{R} \longrightarrow a \cdot b \in \mathbb{R}$   
   using axmulrcl by simp  
 hence  $\forall a b. a \in \mathbb{R} \wedge b \in \mathbb{R} \longrightarrow$   
    $\text{cmulset } \langle a, b \rangle \in \mathbb{R}$  by simp  
 moreover have  $\forall a. a \in \mathbb{R} \longrightarrow (\exists x \in \mathbb{R}. a + x = 0)$   
   using axrnegex by simp  
 hence  $\forall a. a \in \mathbb{R} \longrightarrow$   
    $(\exists x \in \mathbb{R}. \text{caddset } \langle a, x \rangle = 0)$  by simp  
 moreover have  $\forall a. a \in \mathbb{R} \wedge a \neq 0 \longrightarrow (\exists x \in \mathbb{R}. a \cdot x = 1)$   
   using axrrecex by simp  
 hence  $\forall a. a \in \mathbb{R} \wedge a \neq 0 \longrightarrow$   
    $(\exists x \in \mathbb{R}. \text{cmulset } \langle a, x \rangle = 1)$  by simp

ultimately have

(
   
   (
   
     (
   
        $\forall a b.$ 
  
        $a \in \mathbb{R} \wedge b \in \mathbb{R} \longrightarrow$ 
  
        $\langle a, b \rangle \in \text{lessrrel} \longleftrightarrow$ 
  
        $\neg (a = b \vee \langle b, a \rangle \in \text{lessrrel})$ 
  
     )  $\wedge$ 
  
     (
   
        $\forall a b c.$ 
  
        $a \in \mathbb{R} \wedge b \in \mathbb{R} \wedge c \in \mathbb{R} \longrightarrow$ 
  
        $\langle a, b \rangle \in \text{lessrrel} \wedge$ 
  
        $\langle b, c \rangle \in \text{lessrrel} \longrightarrow$ 
  
        $\langle a, c \rangle \in \text{lessrrel}$ 
  
     )  $\wedge$ 
  
     (
   
        $\forall a b c.$ 
  
        $a \in \mathbb{R} \wedge b \in \mathbb{R} \wedge c \in \mathbb{R} \longrightarrow$ 
  
        $\langle a, b \rangle \in \text{lessrrel} \longrightarrow$ 
  
        $\langle \text{caddset } \langle C, a \rangle, \text{caddset } \langle C, b \rangle \rangle \in$ 
  
        $\text{lessrrel}$ 
  
     )
   
   )  $\wedge$

```

(
  ( (∀ a b.
    a ∈ ℝ ∧ b ∈ ℝ →
    ⟨0, a⟩ ∈ lessrrel ∧
    ⟨0, b⟩ ∈ lessrrel →
    ⟨0, cmulset ⟨a, b⟩⟩ ∈
    lessrrel
  ) ∧

  ( (∀ S. S ⊆ ℝ ∧ S ≠ 0 ∧
    ( ∃ x ∈ ℝ. ∀ y ∈ S. ⟨y, x⟩ ∈ lessrrel
    ) →
    ( ∃ x ∈ ℝ.
      ( ∀ y ∈ S. ⟨x, y⟩ ∉ lessrrel
      ) ∧
      ( ∀ y ∈ ℝ. ⟨y, x⟩ ∈ lessrrel →
        ( ∃ z ∈ S. ⟨y, z⟩ ∈ lessrrel
        )
      )
    )
  )
)
) ∧

ℝ ⊆ ℂ ∧
1 ≠ 0
) ∧

( ℂ isASet ∧ caddset ∈ ℂ × ℂ → ℂ ∧
  cmulset ∈ ℂ × ℂ → ℂ
) ∧

(
  (∀ a b.
    a ∈ ℂ ∧ b ∈ ℂ →
    cmulset ⟨a, b⟩ = cmulset ⟨b, a⟩
  ) ∧

  (∀ a b. a ∈ ℂ ∧ b ∈ ℂ →
    caddset ⟨a, b⟩ ∈ ℂ
  )
) ∧

(∀ a b. a ∈ ℂ ∧ b ∈ ℂ →
  cmulset ⟨a, b⟩ ∈ ℂ
) ∧

(∀ a b c.
  a ∈ ℂ ∧ b ∈ ℂ ∧ c ∈ ℂ →

```

$$\begin{aligned}
& \text{cmulset } \langle a, \text{caddset } \langle b, C \rangle \rangle = \\
& \text{caddset} \\
& \langle \text{cmulset } \langle a, b \rangle, \text{cmulset } \langle a, C \rangle \rangle \\
& ) \\
& ) \wedge \\
& ( \\
& ( \\
& (\forall a \ b. \\
& \quad a \in \mathbb{C} \wedge b \in \mathbb{C} \longrightarrow \\
& \quad \text{caddset } \langle a, b \rangle = \text{caddset } \langle b, a \rangle \\
& ) \wedge \\
& (\forall a \ b \ C. \\
& \quad a \in \mathbb{C} \wedge b \in \mathbb{C} \wedge C \in \mathbb{C} \longrightarrow \\
& \quad \text{caddset } \langle \text{caddset } \langle a, b \rangle, C \rangle = \\
& \quad \text{caddset } \langle a, \text{caddset } \langle b, C \rangle \rangle \\
& ) \wedge \\
& (\forall a \ b \ C. \\
& \quad a \in \mathbb{C} \wedge b \in \mathbb{C} \wedge C \in \mathbb{C} \longrightarrow \\
& \quad \text{cmulset } \langle \text{cmulset } \langle a, b \rangle, C \rangle = \\
& \quad \text{cmulset } \langle a, \text{cmulset } \langle b, C \rangle \rangle \\
& ) \\
& ) \wedge \\
& (1 \in \mathbb{R} \wedge \\
& \quad \text{caddset } \langle \text{cmulset } \langle i, i \rangle, 1 \rangle = 0 \\
& ) \wedge \\
& (\forall a. \ a \in \mathbb{C} \longrightarrow \text{caddset } \langle a, 0 \rangle = a \\
& ) \wedge \\
& i \in \mathbb{C} \\
& ) \wedge \\
& ( \\
& (\forall a. \ a \in \mathbb{C} \longrightarrow \\
& \quad (\exists x \in \mathbb{C}. \ \text{caddset } \langle a, x \rangle = 0 \\
& \quad ) \\
& ) \wedge \\
& ( \forall a. \ a \in \mathbb{C} \wedge a \neq 0 \longrightarrow \\
& \quad ( \exists x \in \mathbb{C}. \ \text{cmulset } \langle a, x \rangle = 1 \\
& \quad ) \\
& ) \wedge
\end{aligned}$$

```

      (  $\forall a. a \in \mathbb{C} \longrightarrow$ 
         $\text{cmulset } \langle a, 1 \rangle = a$ 
      )
    )  $\wedge$ 

    (
      (  $\forall a\ b. a \in \mathbb{R} \wedge b \in \mathbb{R} \longrightarrow$ 
         $\text{caddset } \langle a, b \rangle \in \mathbb{R}$ 
      )  $\wedge$ 

      (  $\forall a\ b. a \in \mathbb{R} \wedge b \in \mathbb{R} \longrightarrow$ 
         $\text{cmulset } \langle a, b \rangle \in \mathbb{R}$ 
      )
    )  $\wedge$ 

    (  $\forall a. a \in \mathbb{R} \longrightarrow$ 
      (  $\exists x \in \mathbb{R}. \text{caddset } \langle a, x \rangle = 0$  )
    )  $\wedge$ 

    (  $\forall a. a \in \mathbb{R} \wedge a \neq 0 \longrightarrow$ 
      (  $\exists x \in \mathbb{R}. \text{cmulset } \langle a, x \rangle = 1$  )
    )
  )
  by blast
then show MMIsar0( $\mathbb{R}, \mathbb{C}, 1, 0, i, \text{CplxAdd}(\mathbb{R}, A), \text{CplxMul}(\mathbb{R}, A, M),$ 
  StrictVersion(CplxROrder( $\mathbb{R}, A, r$ ))) unfolding MMIsar0_def by blast
qed

end

```

## 56 Metamath\_sampler.thy

```
theory Metamath_sampler imports Metamath_interface MMI_Complex_ZF_2
```

```
begin
```

The theorems translated from Metamath reside in the `MMI_Complex_ZF`, `MMI_Complex_ZF_1` and `MMI_Complex_ZF_2` theories. The proofs of these theorems are very verbose and for this reason the theories are not shown in the proof document or the FormaMath.org site. This theory file contains some examples of theorems translated from Metamath and formulated in the `complex0` context. This serves two purposes: to give an overview of the material covered in the translated theorems and to provide examples of how to take a translated theorem (proven in the `MMIsar0`) context and transfer it to the `complex0` context. The typical procedure for moving a theorem from `MMIsar0` to `complex0` is as follows: First we define certain aliases that map names defined in the `complex0` to their corresponding names in the `MMIsar0` context. This makes it easy to copy and paste the statement of the theorem as displayed with ProofGeneral. Then we run the Isabelle from ProofGeneral up to the theorem we want to move. When the theorem is verified ProofGeneral displays the statement in the raw set theory notation, stripped from any notation defined in the `MMIsar0` locale. This is what we copy to the proof in the `complex0` locale. After that we just can write "then have ?thesis by simp" and the simplifier translates the raw set theory notation to the one used in `complex0`.

### 56.1 Extended reals and order

In this section we import a couple of theorems about the extended real line and the linear order on it.

Metamath uses the set of real numbers extended with  $+\infty$  and  $-\infty$ . The  $+\infty$  and  $-\infty$  symbols are defined quite arbitrarily as  $\mathbb{C}$  and  $\{\mathbb{C}\}$ , respectively. The next lemma that corresponds to Metamath's `renfdisj` states that  $+\infty$  and  $-\infty$  are not elements of  $\mathbb{R}$ .

```
lemma (in complex0) renfdisj: shows  $\mathbb{R} \cap \{+\infty, -\infty\} = \emptyset$ 
```

```
proof -
```

```
  let real =  $\mathbb{R}$ 
  let complex =  $\mathbb{C}$ 
  let one = 1
  let zero = 0
  let iunit = i
  let caddset = CplxAdd(R,A)
  let cmulset = CplxMul(R,A,M)
  let lessrrel = StrictVersion(CplxROrder(R,A,r))
  have MMIsar0
```



```

    (real, complex, one, zero, iunit, caddset, cmulset, lessrrel)
    using MMIsar_valid by simp
  then have  $\mathbb{R} \cap \{\text{complex}, \{\text{complex}\}\} = 0$ 
    by (rule MMIsar0.MMI_renfdisj)
  thus  $\mathbb{R} \cap \{+\infty, -\infty\} = 0$  by simp
qed

```

The order relation used most often in Metamath is defined on the set of complex reals extended with  $+\infty$  and  $-\infty$ . The next lemma allows to use Metamath's `xrltso` that states that the  $<$  relations is a strict linear order on the extended set.

```

lemma (in complex0) xrltso: shows < Orders  $\mathbb{R}^*$ 
proof -
  let real =  $\mathbb{R}$ 
  let complex =  $\mathbb{C}$ 
  let one = 1
  let zero = 0
  let iunit = i
  let caddset = CplxAdd(R,A)
  let cmulset = CplxMul(R,A,M)
  let lessrrel = StrictVersion(CplxROrder(R,A,r))
  have MMIsar0
    (real, complex, one, zero, iunit, caddset, cmulset, lessrrel)
    using MMIsar_valid by simp
  then have
    (lessrrel  $\cap$  real  $\times$  real  $\cup$ 
      $\{\langle \text{complex}, \text{complex} \rangle \cup \text{real} \times \{\text{complex}\} \cup$ 
      $\{\{\text{complex}\} \times \text{real}\}$  Orders (real  $\cup \{\text{complex}, \{\text{complex}\}\}$ )
    by (rule MMIsar0.MMI_xrltso)
  moreover have lessrrel  $\cap$  real  $\times$  real = lessrrel
    using cplx_strict_ord_on_cplx_reals by auto
  ultimately show < Orders  $\mathbb{R}^*$  by simp
qed

```

Metamath defines the usual  $<$  and  $\leq$  ordering relations for the extended real line, including  $+\infty$  and  $-\infty$ .

```

lemma (in complex0) xrrebnadt: assumes A1:  $x \in \mathbb{R}^*$ 
  shows  $x \in \mathbb{R} \iff (-\infty < x \wedge x < +\infty)$ 
proof -
  let real =  $\mathbb{R}$ 
  let complex =  $\mathbb{C}$ 
  let one = 1
  let zero = 0
  let iunit = i
  let caddset = CplxAdd(R,A)
  let cmulset = CplxMul(R,A,M)
  let lessrrel = StrictVersion(CplxROrder(R,A,r))
  have MMIsar0
    (real, complex, one, zero, iunit, caddset, cmulset, lessrrel)

```

```

    using MMIsar_valid by simp
  then have x ∈ ℝ ∪ {ℂ, {ℂ}} ⟶
    x ∈ ℝ ⟷ ⟨{ℂ}, x⟩ ∈ lessrrel ∩ ℝ × ℝ ∪ ⟨{ℂ}, ℂ⟩ ∪
    ℝ × {ℂ} ∪ {{ℂ}} × ℝ ∧
    ⟨x, ℂ⟩ ∈ lessrrel ∩ ℝ × ℝ ∪ ⟨{ℂ}, ℂ⟩ ∪
    ℝ × {ℂ} ∪ {{ℂ}} × ℝ
    by (rule MMIsar0.MMI_xrrebnDt)
  then have x ∈ ℝ* ⟶ ( x ∈ ℝ ⟷ ( -∞ < x ∧ x < +∞ ) )
    by simp
  with A1 show thesis by simp
qed

```

A quite involved inequality.

```

lemma (in complex0) lt2mul2divt:
  assumes A1: a ∈ ℝ  b ∈ ℝ  c ∈ ℝ  d ∈ ℝ and
  A2: 0 < b  0 < d
  shows a·b < c·d ⟷ a/d < c/b
proof -
  let real = ℝ
  let complex = ℂ
  let one = 1
  let zero = 0
  let iunit = i
  let caddset = CplxAdd(R,A)
  let cmulset = CplxMul(R,A,M)
  let lessrrel = StrictVersion(CplxROrder(R,A,r))
  have MMIsar0
    (real, complex, one, zero, iunit, caddset, cmulset, lessrrel)
    using MMIsar_valid by simp
  then have
    (a ∈ real ∧ b ∈ real) ∧
    (c ∈ real ∧ d ∈ real) ∧
    ⟨zero, b⟩ ∈ lessrrel ∩ real × real ∪
    ⟨{complex}, complex⟩ ∪ real × {complex} ∪ {{complex}} × real ∧
    ⟨zero, d⟩ ∈ lessrrel ∩ real × real ∪
    ⟨{complex}, complex⟩ ∪ real × {complex} ∪ {{complex}} × real ⟶
    ⟨cmulset ⟨a, b⟩, cmulset ⟨c, d⟩⟩ ∈
    lessrrel ∩ real × real ∪ ⟨{complex}, complex⟩ ∪
    real × {complex} ∪ {{complex}} × real ⟷
    ⟨⋃{x ∈ complex . cmulset ⟨d, x⟩ = a},
    ⋃{x ∈ complex . cmulset ⟨b, x⟩ = c}⟩ ∈
    lessrrel ∩ real × real ∪ ⟨{complex}, complex⟩ ∪
    real × {complex} ∪ {{complex}} × real
    by (rule MMIsar0.MMI_lt2mul2divt)
  with A1 A2 show thesis by simp
qed

```

A real number is smaller than its half iff it is positive.

```

lemma (in complex0) halfpos: assumes A1: a ∈ ℝ

```

```

shows 0 < a  $\longleftrightarrow$  a/2 < a
proof -
  let real =  $\mathbb{R}$ 
  let complex =  $\mathbb{C}$ 
  let one = 1
  let zero = 0
  let iunit = i
  let caddset = CplxAdd(R,A)
  let cmulset = CplxMul(R,A,M)
  let lessrrel = StrictVersion(CplxROrder(R,A,r))
  from A1 have MMIisar0
    (real, complex, one, zero, iunit, caddset, cmulset, lessrrel)
    and a  $\in$  real
    using MMIisar_valid by auto
  then have
     $\langle$ zero, a $\rangle \in$ 
    lessrrel  $\cap$  real  $\times$  real  $\cup \{\langle$ complex, complex $\rangle\} \cup$ 
    real  $\times$  {complex}  $\cup \{\{complex\} \times$  real  $\longleftrightarrow$ 
     $\langle \bigcup \{x \in \text{complex} . \text{cmulset } \langle \text{caddset } \langle \text{one}, \text{one} \rangle, x \rangle = a\}, a \rangle \in$ 
    lessrrel  $\cap$  real  $\times$  real  $\cup$ 
     $\{\langle$ complex, complex $\rangle\} \cup$  real  $\times$  {complex}  $\cup \{\{complex\} \times$  real
    by (rule MMIisar0.MMI_halfpos)
  then show thesis by simp
qed

```

One more inequality.

```

lemma (in complex0) ledivp1:
  assumes A1: a  $\in \mathbb{R}$     b  $\in \mathbb{R}$  and
  A2: 0  $\leq$  a    0  $\leq$  b
  shows (a/(b + 1)) $\cdot$ b  $\leq$  a
proof -
  let real =  $\mathbb{R}$ 
  let complex =  $\mathbb{C}$ 
  let one = 1
  let zero = 0
  let iunit = i
  let caddset = CplxAdd(R,A)
  let cmulset = CplxMul(R,A,M)
  let lessrrel = StrictVersion(CplxROrder(R,A,r))
  have MMIisar0
    (real, complex, one, zero, iunit, caddset, cmulset, lessrrel)
    using MMIisar_valid by simp
  then have
    (a  $\in$  real  $\wedge \langle$ a, zero $\rangle \notin$ 
    lessrrel  $\cap$  real  $\times$  real  $\cup \{\langle$ complex, complex $\rangle\} \cup$ 
    real  $\times$  {complex}  $\cup \{\{complex\} \times$  real)  $\wedge$ 
    b  $\in$  real  $\wedge \langle$ b, zero $\rangle \notin$  lessrrel  $\cap$  real  $\times$  real  $\cup$ 
     $\{\langle$ complex, complex $\rangle\} \cup$  real  $\times$  {complex}  $\cup$ 
     $\{\{complex\} \times$  real  $\longrightarrow$ 

```

```

    ⟨a, cmulset(⟨⋃{x ∈ complex . cmulset(caddset(b, one), x) = a}, b)⟩ ∉
    lessrrel ∩ real × real ∪ {⟨{complex}, complex⟩} ∪
    real × {complex} ∪ {{complex}} × real
    by (rule MMIIsar0.MMI_ledivp1t)
  with A1 A2 show thesis by simp
qed

```

## 56.2 Natural real numbers

In standard mathematics natural numbers are treated as a subset of real numbers. From the set theory point of view however those are quite different objects. In this section we talk about "real natural" numbers i.e. the counterpart of natural numbers that is a subset of the reals.

Two ways of saying that there are no natural numbers between  $n$  and  $n + 1$ .

**lemma** (in complex0) no\_nats\_between:

assumes A1:  $n \in \mathbb{N}$   $k \in \mathbb{N}$

shows

$n \leq k \longleftrightarrow n < k + 1$

$n < k \longleftrightarrow n + 1 \leq k$

**proof** -

let real =  $\mathbb{R}$

let complex =  $\mathbb{C}$

let one = 1

let zero = 0

let iunit =  $i$

let caddset = CplxAdd(R,A)

let cmulset = CplxMul(R,A,M)

let lessrrel = StrictVersion(CplxROrder(R,A,r))

have I: MMIIsar0

(real, complex, one, zero, iunit, caddset, cmulset, lessrrel)

using MMIIsar\_valid by simp

then have

$n \in \bigcap \{N \in \text{Pow}(\text{real}) . \text{one} \in N \wedge$

$(\forall n. n \in N \longrightarrow \text{caddset } \langle n, \text{one} \rangle \in N)\}$   $\wedge$

$k \in \bigcap \{N \in \text{Pow}(\text{real}) . \text{one} \in N \wedge$

$(\forall n. n \in N \longrightarrow \text{caddset } \langle n, \text{one} \rangle \in N)\} \longrightarrow$

$\langle k, n \rangle \notin$

$\text{lessrrel} \cap \text{real} \times \text{real} \cup \{\langle \{\text{complex}\}, \text{complex} \rangle\} \cup \text{real} \times \{\text{complex}\}$

∪

$\{\{\text{complex}\}\} \times \text{real} \longleftrightarrow$

$\langle n, \text{caddset } \langle k, \text{one} \rangle \rangle \in$

$\text{lessrrel} \cap \text{real} \times \text{real} \cup \{\langle \{\text{complex}\}, \text{complex} \rangle\} \cup \text{real} \times \{\text{complex}\}$

∪

$\{\{\text{complex}\}\} \times \text{real}$  by (rule MMIIsar0.MMI\_nnleltp1t)

then have  $n \in \mathbb{N} \wedge k \in \mathbb{N} \longrightarrow n \leq k \longleftrightarrow n < k + 1$

by simp

with A1 show  $n \leq k \longleftrightarrow n < k + 1$  by simp

from I have

```

n ∈ ⋂{N ∈ Pow(real) . one ∈ N ∧
(∀n. n ∈ N → caddset ⟨n, one⟩ ∈ N)} ∧
k ∈ ⋂{N ∈ Pow(real) . one ∈ N ∧
(∀n. n ∈ N → caddset ⟨n, one⟩ ∈ N)} →
⟨n, k⟩ ∈
lessrrel ∩ real × real ∪
{⟨{complex}, complex⟩} ∪ real × {complex} ∪
{{complex}} × real ↔ ⟨k, caddset ⟨n, one⟩⟩ ∉
lessrrel ∩ real × real ∪ {⟨{complex}, complex⟩} ∪ real × {complex}
∪
{{complex}} × real by (rule MMIsar0.MMI_nnltp1let)
then have n ∈ N ∧ k ∈ N → n < k ↔ n + 1 ≤ k
  by simp
with A1 show n < k ↔ n + 1 ≤ k by simp
qed

```

Metamath has some very complicated and general version of induction on (complex) natural numbers that I can't even understand. As an exercise I derived a more standard version that is imported to the `complex0` context below.

```

lemma (in complex0) cplx_nat_ind: assumes A1: ψ(1) and
  A2: ∀k ∈ N. ψ(k) → ψ(k+1) and
  A3: n ∈ N
  shows ψ(n)
proof -
  let real = ℝ
  let complex = ℂ
  let one = 1
  let zero = 0
  let iunit = i
  let caddset = CplxAdd(R,A)
  let cmulset = CplxMul(R,A,M)
  let lessrrel = StrictVersion(CplxROrder(R,A,r))
  have I: MMIsar0
    (real, complex, one, zero, iunit, caddset, cmulset, lessrrel)
    using MMIsar_valid by simp
  moreover from A1 A2 A3 have
    ψ(one)
    ∀k ∈ ⋂{N ∈ Pow(real) . one ∈ N ∧
      (∀n. n ∈ N → caddset ⟨n, one⟩ ∈ N)}.
    ψ(k) → ψ(caddset ⟨k, one⟩)
    n ∈ ⋂{N ∈ Pow(real) . one ∈ N ∧
      (∀n. n ∈ N → caddset ⟨n, one⟩ ∈ N)}
    by auto
  ultimately show ψ(n) by (rule MMIsar0.nnind1)
qed

```

Some simple arithmetics.

```

lemma (in complex0) arith: shows

```

```

2 + 2 = 4
2·2 = 4
3·2 = 6
3·3 = 9
proof -
  let real = ℝ
  let complex = ℂ
  let one = 1
  let zero = 0
  let iunit = i
  let caddset = CplxAdd(R,A)
  let cmulset = CplxMul(R,A,M)
  let lessrrel = StrictVersion(CplxR0Order(R,A,r))
  have I: MMIisar0
    (real, complex, one, zero, iunit, caddset, cmulset, lessrrel)
    using MMIisar_valid by simp
  then have
    caddset ⟨caddset ⟨one, one⟩, caddset ⟨one, one⟩⟩ =
    caddset ⟨caddset ⟨caddset ⟨one, one⟩, one⟩, one⟩
    by (rule MMIisar0.MMI_2p2e4)
  thus 2 + 2 = 4 by simp
  from I have
    cmulset⟨caddset⟨one, one⟩, caddset⟨one, one⟩⟩ =
    caddset⟨caddset⟨caddset⟨one, one⟩, one⟩, one⟩
    by (rule MMIisar0.MMI_2t2e4)
  thus 2·2 = 4 by simp
  from I have
    cmulset⟨caddset⟨caddset⟨one, one⟩, one⟩, caddset⟨one, one⟩⟩ =
    caddset ⟨caddset⟨caddset⟨caddset⟨caddset
    ⟨one, one⟩, one⟩, one⟩, one⟩, one⟩
    by (rule MMIisar0.MMI_3t2e6)
  thus 3·2 = 6 by simp
  from I have cmulset
    ⟨caddset⟨caddset⟨one, one⟩, one⟩,
    caddset⟨caddset⟨one, one⟩, one⟩⟩ =
    caddset⟨caddset⟨caddset ⟨caddset
    ⟨caddset⟨caddset⟨caddset⟨caddset⟨one, one⟩, one⟩, one⟩, one⟩,
    one⟩, one⟩, one⟩, one⟩
    by (rule MMIisar0.MMI_3t3e9)
  thus 3·3 = 9 by simp
qed

```

### 56.3 Infimum and supremum in real numbers

Real numbers form a complete ordered field. Here we import a couple of Metamath theorems about supremu and infimum.

If a set  $S$  has a smallest element, then the infimum of  $S$  belongs to it.

**lemma** (in complex0) lbinfmcl: assumes A1:  $S \subseteq \mathbb{R}$  and

```

A2:  $\exists x \in S. \forall y \in S. x \leq y$ 
shows  $\text{Infim}(S, \mathbb{R}, <) \in S$ 
proof -
  let real =  $\mathbb{R}$ 
  let complex =  $\mathbb{C}$ 
  let one = 1
  let zero = 0
  let iunit = i
  let caddset = CplxAdd(R,A)
  let cmulset = CplxMul(R,A,M)
  let lessrrel = StrictVersion(CplxROrder(R,A,r))
  have I: MMIsar0
    (real, complex, one, zero, iunit, caddset, cmulset, lessrrel)
    using MMIsar_valid by simp
  then have
     $S \subseteq \text{real} \wedge (\exists x \in S. \forall y \in S. \langle y, x \rangle \notin$ 
     $\text{lessrrel} \cap \text{real} \times \text{real} \cup \{\langle \text{complex}, \text{complex} \rangle\} \cup$ 
     $\text{real} \times \{\text{complex}\} \cup \{\{\text{complex}\} \times \text{real}\}) \longrightarrow$ 
     $\text{Sup}(S, \text{real},$ 
     $\text{converse}(\text{lessrrel} \cap \text{real} \times \text{real} \cup$ 
     $\{\langle \text{complex}, \text{complex} \rangle\} \cup \text{real} \times \{\text{complex}\} \cup$ 
     $\{\{\text{complex}\} \times \text{real}\}) \in S$ 
    by (rule MMIsar0.MMI_lbinfmcl)
  then have
     $S \subseteq \mathbb{R} \wedge (\exists x \in S. \forall y \in S. x \leq y) \longrightarrow$ 
     $\text{Sup}(S, \mathbb{R}, \text{converse}(<)) \in S$  by simp
  with A1 A2 show thesis using Infim_def by simp
qed

```

Supremum of any subset of reals that is bounded above is real.

```

lemma (in complex0) sup_is_real:
  assumes  $A \subseteq \mathbb{R}$  and  $A \neq 0$  and  $\exists x \in \mathbb{R}. \forall y \in A. y \leq x$ 
  shows  $\text{Sup}(A, \mathbb{R}, <) \in \mathbb{R}$ 

```

```

proof -
  let real =  $\mathbb{R}$ 
  let complex =  $\mathbb{C}$ 
  let one = 1
  let zero = 0
  let iunit = i
  let caddset = CplxAdd(R,A)
  let cmulset = CplxMul(R,A,M)
  let lessrrel = StrictVersion(CplxROrder(R,A,r))
  have MMIsar0
    (real, complex, one, zero, iunit, caddset, cmulset, lessrrel)
    using MMIsar_valid by simp
  then have
     $A \subseteq \text{real} \wedge A \neq 0 \wedge (\exists x \in \text{real}. \forall y \in A. \langle x, y \rangle \notin$ 
     $\text{lessrrel} \cap \text{real} \times \text{real} \cup \{\langle \text{complex}, \text{complex} \rangle\} \cup$ 
     $\text{real} \times \{\text{complex}\} \cup \{\{\text{complex}\} \times \text{real}\}) \longrightarrow$ 

```

```

    Sup(A, real,
    lessrrel  $\cap$  real  $\times$  real  $\cup$   $\{\langle \text{complex}, \text{complex} \rangle\} \cup$ 
    real  $\times$   $\{\text{complex}\} \cup \{\{\text{complex}\} \times \text{real}\} \in \text{real}$ 
    by (rule MMIsar0.MMI_suprc1)
  with assms show thesis by simp
qed

```

If a real number is smaller than the supremum of  $A$ , then we can find an element of  $A$  greater than it.

```

lemma (in complex0) suprlub:
  assumes  $A \subseteq \mathbb{R}$  and  $A \neq 0$  and  $\exists x \in \mathbb{R}. \forall y \in A. y \leq x$ 
  and  $B \in \mathbb{R}$  and  $B < \text{Sup}(A, \mathbb{R}, <)$ 
  shows  $\exists z \in A. B < z$ 
proof -
  let real =  $\mathbb{R}$ 
  let complex =  $\mathbb{C}$ 
  let one = 1
  let zero = 0
  let iunit = i
  let caddset = CplxAdd(R,A)
  let cmulset = CplxMul(R,A,M)
  let lessrrel = StrictVersion(CplxROrder(R,A,r))
  have MMIsar0
    (real, complex, one, zero, iunit, caddset, cmulset, lessrrel)
  using MMIsar_valid by simp
  then have  $(A \subseteq \text{real} \wedge A \neq 0 \wedge (\exists x \in \text{real}. \forall y \in A. \langle x, y \rangle \notin$ 
    lessrrel  $\cap$  real  $\times$  real  $\cup \{\langle \text{complex}, \text{complex} \rangle\} \cup$ 
    real  $\times$   $\{\text{complex}\} \cup$ 
     $\{\{\text{complex}\} \times \text{real}\}) \wedge B \in \text{real} \wedge \langle B, \text{Sup}(A, \text{real},$ 
    lessrrel  $\cap$  real  $\times$  real  $\cup \{\langle \text{complex}, \text{complex} \rangle\} \cup$ 
    real  $\times$   $\{\text{complex}\} \cup$ 
     $\{\{\text{complex}\} \times \text{real}\}) \in \text{lessrrel} \cap \text{real} \times \text{real} \cup$ 
     $\{\langle \text{complex}, \text{complex} \rangle\} \cup \text{real} \times \{\text{complex}\} \cup$ 
     $\{\{\text{complex}\} \times \text{real}\} \rightarrow$ 
     $(\exists z \in A. \langle B, z \rangle \in \text{lessrrel} \cap \text{real} \times \text{real} \cup$ 
     $\{\langle \text{complex}, \text{complex} \rangle\} \cup \text{real} \times \{\text{complex}\} \cup$ 
     $\{\{\text{complex}\} \times \text{real}\})$ 
  by (rule MMIsar0.MMI_suprlub)
  with assms show thesis by simp
qed

```

Something a bit more interesting: infimum of a set that is bounded below is real and equal to the minus supremum of the set flipped around zero.

```

lemma (in complex0) infmsup:
  assumes  $A \subseteq \mathbb{R}$  and  $A \neq 0$  and  $\exists x \in \mathbb{R}. \forall y \in A. x \leq y$ 
  shows
    Infim(A,  $\mathbb{R}, <$ )  $\in \mathbb{R}$ 
    Infim(A,  $\mathbb{R}, <$ ) =  $(-\text{Sup}(\{z \in \mathbb{R}. (-z) \in A\}, \mathbb{R}, <))$ 
proof -

```



```

let real = ℝ
let complex = ℂ
let one = 1
let zero = 0
let iunit = i
let caddset = CplxAdd(R,A)
let cmulset = CplxMul(R,A,M)
let lessrrel = StrictVersion(CplxROrder(R,A,r))
have I: MMIisar0
  (real, complex, one, zero, iunit, caddset, cmulset, lessrrel)
  using MMIisar_valid by simp
then have
   $A \subseteq \text{real} \wedge A \neq 0 \wedge (\exists x \in \text{real}. \forall y \in A. \langle y, x \rangle \notin$ 
   $\text{lessrrel} \cap \text{real} \times \text{real} \cup \{\langle \{\text{complex}\}, \text{complex} \rangle\} \cup$ 
   $\text{real} \times \{\text{complex}\} \cup$ 
   $\{\{\text{complex}\}\} \times \text{real}) \longrightarrow \text{Sup}(A, \text{real}, \text{converse}$ 
   $(\text{lessrrel} \cap \text{real} \times \text{real} \cup \{\langle \{\text{complex}\}, \text{complex} \rangle\} \cup$ 
   $\text{real} \times \{\text{complex}\} \cup \{\{\text{complex}\}\} \times \text{real})) =$ 
   $\bigcup \{x \in \text{complex} . \text{caddset}$ 
   $\langle \text{Sup}(\{z \in \text{real} . \bigcup \{x \in \text{complex} . \text{caddset}(z, x) = \text{zero}\} \in A\}, \text{real},$ 
   $\text{lessrrel} \cap \text{real} \times \text{real} \cup \{\langle \{\text{complex}\}, \text{complex} \rangle\} \cup$ 
   $\text{real} \times \{\text{complex}\} \cup \{\{\text{complex}\}\} \times \text{real}), x) = \text{zero}\}$ 
  by (rule MMIisar0.MMI_infm_sup)
then have  $A \subseteq \mathbb{R} \wedge \neg(A = 0) \wedge (\exists x \in \mathbb{R}. \forall y \in A. x \leq y) \longrightarrow$ 
   $\text{Sup}(A, \mathbb{R}, \text{converse}(\lt)) = (\text{-Sup}(\{z \in \mathbb{R}. (-z) \in A\}, \mathbb{R}, \lt))$ 
  by simp
with assms show
   $\text{Infim}(A, \mathbb{R}, \lt) = (\text{-Sup}(\{z \in \mathbb{R}. (-z) \in A\}, \mathbb{R}, \lt))$ 
  using Infim_def by simp
from I have
   $A \subseteq \text{real} \wedge A \neq 0 \wedge (\exists x \in \text{real}. \forall y \in A. \langle y, x \rangle \notin$ 
   $\text{lessrrel} \cap \text{real} \times \text{real} \cup \{\langle \{\text{complex}\}, \text{complex} \rangle\} \cup$ 
   $\text{real} \times \{\text{complex}\} \cup$ 
   $\{\{\text{complex}\}\} \times \text{real}) \longrightarrow \text{Sup}(A, \text{real}, \text{converse}$ 
   $(\text{lessrrel} \cap \text{real} \times \text{real} \cup \{\langle \{\text{complex}\}, \text{complex} \rangle\} \cup$ 
   $\text{real} \times \{\text{complex}\} \cup \{\{\text{complex}\}\} \times \text{real})) \in \text{real}$ 
  by (rule MMIisar0.MMI_infmrcl)
with assms show  $\text{Infim}(A, \mathbb{R}, \lt) \in \mathbb{R}$ 
  using Infim_def by simp
qed
end

```

## References

- [1] N. A'Campo. A natural construction for the real numbers. 2003.

- [2] R. D. Arthan. The Eudoxus Real Numbers. 2004.
- [3] R. Street at al. The Efficient Real Numbers. 2003.
- [4] Strecker G.E. Herrlich H. When is  $\mathbb{N}$  lindelöf? *Comment. Math. Univ. Carolinae*, 1997.
- [5] I. L. Reilly and M. K. Vamanamurthy. Some topological anti-properties. *Illinois J. Math.*, 24:382–389, 1980.