

# 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 . . . . .	9
<b>2</b>	<b>Order_ZF.thy</b>	<b>12</b>
2.1	Definitions . . . . .	12
2.2	Intervals . . . . .	15
2.3	Bounded sets . . . . .	16
<b>3</b>	<b>Order_ZF_1a.thy</b>	<b>20</b>
3.1	Maximum and minimum of a set . . . . .	20
3.2	Supremum and Infimum . . . . .	23
3.3	Strict versions of order relations . . . . .	24
<b>4</b>	<b>NatOrder_ZF.thy</b>	<b>27</b>
4.1	Order on natural numbers . . . . .	27
<b>5</b>	<b>func_ZF.thy</b>	<b>28</b>
5.1	Lifting operations to a function space . . . . .	28
5.2	Associative and commutative operations . . . . .	29
5.3	Restricting operations . . . . .	30
5.4	Compositions . . . . .	32
5.5	Identity function . . . . .	32
5.6	Lifting to subsets . . . . .	33
5.7	Distributive operations . . . . .	35

<b>6</b>	<b>func_ZF_1.thy</b>	<b>37</b>
6.1	Functions and order . . . . .	37
6.2	Projections in cartesian products . . . . .	38
6.3	Induced relations and order isomorphisms . . . . .	39
<b>7</b>	<b>Generalization_ZF.thy</b>	<b>43</b>
7.1	Generalization situation . . . . .	43
7.2	Arbitrary generalizations . . . . .	44
7.3	ZF generalization . . . . .	45
<b>8</b>	<b>NatGenIntEx_ZF.thy</b>	<b>47</b>
<b>9</b>	<b>Finite_ZF.thy</b>	<b>48</b>
9.1	Definition and basic properties of finite powerset . . . . .	48
<b>10</b>	<b>Finite1.thy</b>	<b>53</b>
10.1	Finite powerset . . . . .	53
10.2	Finite range functions . . . . .	57
<b>11</b>	<b>Finite_ZF_1.thy</b>	<b>58</b>
11.1	Finite vs. bounded sets . . . . .	58
<b>12</b>	<b>FinOrd_ZF.thy</b>	<b>60</b>
12.1	Finite vs. bounded sets . . . . .	60
12.2	Order isomorphisms of finite sets . . . . .	60
<b>13</b>	<b>EquivClass1.thy</b>	<b>63</b>
13.1	Congruent functions and projections on the quotient . . . . .	63
13.2	Projecting commutative, associative and distributive operations. . . . .	66
13.3	Saturated sets . . . . .	67
<b>14</b>	<b>Fold_ZF.thy</b>	<b>70</b>
14.1	Folding in ZF . . . . .	70
<b>15</b>	<b>Partitions_ZF.thy</b>	<b>73</b>
15.1	Bisections . . . . .	73
15.2	Partitions . . . . .	74
<b>16</b>	<b>Enumeration_ZF.thy</b>	<b>76</b>
16.1	Enumerations: definition and notation . . . . .	76
16.2	Properties of enumerations . . . . .	77

<b>17 Semigroup_ZF.thy</b>	<b>79</b>
17.1 Products of sequences of semigroup elements . . . . .	79
17.2 Products over sets of indices . . . . .	81
17.3 Commutative semigroups . . . . .	83
<b>18 Semigroup_ZF.thy</b>	<b>87</b>
18.1 Sum of a function over a set . . . . .	87
<b>19 Monoid_ZF.thy</b>	<b>89</b>
19.1 Definition and basic properties . . . . .	89
<b>20 Group_ZF.thy</b>	<b>92</b>
20.1 Definition and basic properties of groups . . . . .	92
20.2 Subgroups . . . . .	98
<b>21 Group_ZF_1.thy</b>	<b>101</b>
21.1 Translations . . . . .	101
21.2 Odd functions . . . . .	104
<b>22 Group_ZF_1b.thy</b>	<b>105</b>
22.1 An alternative definition of group . . . . .	105
<b>23 AbelianGroup_ZF.thy</b>	<b>107</b>
23.1 Rearrangement formulae . . . . .	107
<b>24 Group_ZF_2.thy</b>	<b>113</b>
24.1 Lifting groups to function spaces . . . . .	113
24.2 Equivalence relations on groups . . . . .	115
24.3 Normal subgroups and quotient groups . . . . .	116
24.4 Function spaces as monoids . . . . .	119
<b>25 Group_ZF_3.thy</b>	<b>121</b>
25.1 Group valued finite range functions . . . . .	121
25.2 Almost homomorphisms . . . . .	122
25.3 The classes of almost homomorphisms . . . . .	127
25.4 Compositions of almost homomorphisms . . . . .	128
25.5 Shifting almost homomorphisms . . . . .	132
<b>26 DirectProduct_ZF.thy</b>	<b>133</b>
26.1 Definition . . . . .	133
26.2 Associative and commutative operations . . . . .	134
<b>27 OrderedGroup_ZF.thy</b>	<b>135</b>
27.1 Ordered groups . . . . .	135
27.2 Inequalities . . . . .	139

27.3	The set of positive elements . . . . .	145
27.4	Intervals and bounded sets . . . . .	148
<b>28</b>	<b>OrderedGroup_ZF_1.thy</b>	<b>151</b>
28.1	Absolute value and the triangle inequality . . . . .	151
28.2	Maximum absolute value of a set . . . . .	156
28.3	Alternative definitions . . . . .	157
28.4	Odd Extensions . . . . .	159
28.5	Functions with infinite limits . . . . .	160
<b>29</b>	<b>Ring_ZF.thy</b>	<b>162</b>
29.1	Definition and basic properties . . . . .	162
29.2	Rearrangement lemmas . . . . .	167
<b>30</b>	<b>Ring_ZF_1.thy</b>	<b>169</b>
30.1	The ring of classes of almost homomorphisms . . . . .	169
<b>31</b>	<b>OrderedRing_ZF.thy</b>	<b>171</b>
31.1	Definition and notation . . . . .	171
31.2	Absolute value for ordered rings . . . . .	176
31.3	Positivity in ordered rings . . . . .	177
<b>32</b>	<b>Field_ZF.thy</b>	<b>182</b>
32.1	Definition and basic properties . . . . .	182
32.2	Equations and identities . . . . .	184
32.3	$1/0=0$ . . . . .	184
<b>33</b>	<b>OrderedField_ZF.thy</b>	<b>186</b>
33.1	Definition and basic properties . . . . .	186
33.2	Inequalities . . . . .	188
33.3	Definition of real numbers . . . . .	190
<b>34</b>	<b>Int_ZF.thy</b>	<b>191</b>
34.1	Addition and multiplication as ZF-functions. . . . .	191
34.2	Integers as an ordered group . . . . .	195
34.3	Induction on integers. . . . .	203
34.4	Bounded vs. finite subsets of integers . . . . .	205
<b>35</b>	<b>Int_ZF_1.thy</b>	<b>207</b>
35.1	Integers as a ring . . . . .	207
35.2	Rearrangement lemmas . . . . .	209
35.3	Integers as an ordered ring . . . . .	212
35.4	Maximum and minimum of a set of integers . . . . .	218
35.5	The set of nonnegative integers . . . . .	220
35.6	Functions with infinite limits . . . . .	224

35.7	Miscellaneous . . . . .	226
<b>36</b>	<b>IntDiv_ZF_IML.thy</b>	<b>228</b>
36.1	Quotient and remainder . . . . .	228
<b>37</b>	<b>Int_ZF_2.thy</b>	<b>230</b>
37.1	Slopes . . . . .	230
37.2	Composing slopes . . . . .	239
<b>38</b>	<b>Int_ZF_3.thy</b>	<b>241</b>
38.1	Positive slopes . . . . .	241
38.2	Inverting slopes . . . . .	244
38.3	Completeness . . . . .	247
<b>39</b>	<b>Real_ZF.thy</b>	<b>249</b>
39.1	The definition of real numbers . . . . .	249
<b>40</b>	<b>Real_ZF_1.thy</b>	<b>255</b>
40.1	Definitions and notation . . . . .	255
40.2	Multiplication of real numbers . . . . .	257
40.3	The order on reals . . . . .	259
40.4	Inverting reals . . . . .	265
40.5	Completeness . . . . .	267
<b>41</b>	<b>Complex_ZF.thy</b>	<b>275</b>
41.1	From complete ordered fields to complex numbers . . . . .	275
41.2	Axioms of complex numbers . . . . .	279
<b>42</b>	<b>Topology_ZF.thy</b>	<b>285</b>
42.1	Basic definitions and properties . . . . .	285
42.2	Interior of a set . . . . .	287
42.3	Closed sets, closure, boundary. . . . .	288
<b>43</b>	<b>Topology_ZF_1.thy</b>	<b>292</b>
43.1	Separation axioms. . . . .	292
43.2	Bases and subbases. . . . .	293
43.3	Product topology . . . . .	295
<b>44</b>	<b>Topology_ZF_1b.thy</b>	<b>298</b>
44.1	Compact sets are closed - no need for AC . . . . .	298
<b>45</b>	<b>Topology_ZF_2.thy</b>	<b>300</b>
45.1	Continuous functions. . . . .	300
45.2	Homeomorphisms . . . . .	302
45.3	Topologies induced by mappings . . . . .	303

45.4	Partial functions and continuity . . . . .	304
45.5	Product topology and continuity . . . . .	305
45.6	Pasting lemma . . . . .	306
<b>46</b>	<b>Topology_ZF_3.thy</b>	<b>308</b>
46.1	The base of the product topology . . . . .	308
46.2	Finite product of topologies . . . . .	309
<b>47</b>	<b>Topology_ZF_4.thy</b>	<b>312</b>
47.1	Convergence on topological spaces . . . . .	312
47.1.1	Nets . . . . .	312
47.1.2	Filters . . . . .	313
47.1.3	Relation between nets and filters . . . . .	315
<b>48</b>	<b>Topology_ZF_examples.thy</b>	<b>318</b>
48.1	Some new ideas on cardinals . . . . .	318
48.1.1	cases-type results . . . . .	318
48.1.2	Relations between a cardinal and its successor . . . . .	319
48.1.3	Main result on cardinals (without the <i>Axiom of Choice</i> )	319
48.2	CoCardinal Topology of a set $X$ . . . . .	320
48.2.1	CoCardinal topology is a topology. . . . .	320
48.2.2	Total set, Closed sets, Interior, Closure and Boundary	321
48.2.3	Special cases and subspaces . . . . .	322
48.3	Excluded Set Topology . . . . .	322
48.3.1	Excluded set topology is a topology. . . . .	322
48.3.2	Total set, Closed sets, Interior, Closure and Boundary	323
48.3.3	Special cases and subspaces . . . . .	323
48.4	Included Set Topology . . . . .	324
48.4.1	Included set topology is a topology. . . . .	324
48.4.2	Total set, Closed sets, Interior, Closure and Boundary	324
48.4.3	Special cases and subspaces . . . . .	325
<b>49</b>	<b>Topology_ZF_examples_1.thy</b>	<b>327</b>
49.1	New ideas using a base for a topology . . . . .	327
49.1.1	The topology of a base . . . . .	327
49.1.2	Dual Base for Closed Sets . . . . .	328
49.2	Partition topology . . . . .	328
49.2.1	Partition topology is a topology. . . . .	329
49.2.2	Total set, Closed sets, Interior, Closure and Boundary	329
49.2.3	Special cases and subspaces . . . . .	330
49.3	Order topologies . . . . .	331
49.3.1	Order topology is a topology . . . . .	331
49.3.2	Total set . . . . .	332
49.3.3	Right order and Left order topologies. . . . .	333

49.3.4	Right and Left Order topologies are topologies . . . .	333
49.3.5	Total set . . . . .	334
49.4	Union of Topologies . . . . .	334
<b>50</b>	<b>Topology_ZF_properties.thy</b>	<b>335</b>
50.1	Properties of compactness . . . . .	335
50.2	Properties of numerability . . . . .	336
50.2.1	Some cardinal related results . . . . .	337
50.2.2	Relations between numerability properties . . . . .	337
50.3	Relation between numerability and compactness . . . . .	338
<b>51</b>	<b>Topology_ZF_5.thy</b>	<b>340</b>
51.1	Some results for separation axioms . . . . .	340
51.1.1	Hereditability . . . . .	341
51.2	Spectrum and anti-properties . . . . .	342
<b>52</b>	<b>Topology_ZF_6.thy</b>	<b>347</b>
52.1	Image filter . . . . .	347
52.2	Continuous at a point vs. globally continuous . . . . .	347
52.3	Continuous functions and filters . . . . .	347
<b>53</b>	<b>Topology_ZF_7.thy</b>	<b>349</b>
53.1	Connection Properties . . . . .	349
<b>54</b>	<b>TopologicalGroup_ZF.thy</b>	<b>353</b>
54.1	Topological group: definition and notation . . . . .	353
54.2	Interval arithmetic, translations and inverse of set . . . . .	355
54.3	Neighborhoods of zero . . . . .	356
54.4	Closure in topological groups . . . . .	357
54.5	Sums of sequences of elements and subsets . . . . .	357
<b>55</b>	<b>Metamath_interface.thy</b>	<b>359</b>
55.1	MMisar0 and complex0 contexts. . . . .	359
<b>56</b>	<b>Metamath_sampler.thy</b>	<b>360</b>
56.1	Extended reals and order . . . . .	360
56.2	Natural real numbers . . . . .	361
56.3	Infimum and supremum in real numbers . . . . .	362

# 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 `≡` 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 ≡ A ∩ 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>*

## 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  $a_0 \cdot a_1 \cdot \dots \cdot a_n$ , (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 using 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**

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

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  $r\text{-}(A)$  denotes the inverse image of the set  $A$  by relation  $r$  (i.e.  $r\text{-}(A) = \{x : \langle x,y \rangle \in r \text{ for some } y \in A\}$ ).

**definition**

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

Infimum is defined analogously.

**definition**

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

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

**definition**

`IsComplete` (`_ {is complete}`) **where**  
`r {is complete}`  $\equiv$   
 $\forall A. \text{IsBoundedAbove}(A, r) \wedge A \neq 0 \longrightarrow \text{HasAminimum}(r, \bigcap_{a \in A} r\{a\})$

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

**lemma** `Order_ZF_1_L1`: **assumes** `r {is total on} X` **and** `a ∈ X`  
**shows** `⟨a, a⟩ ∈ r` *⟨proof⟩*

A total relation is reflexive.

**lemma** `total_is_refl`:  
**assumes** `r {is total on} X`  
**shows** `refl(X, r)` *⟨proof⟩*

A linear order is partial order.

**lemma** `Order_ZF_1_L2`: **assumes** `IsLinOrder(X, r)`  
**shows** `IsPartOrder(X, r)`  
*⟨proof⟩*

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)`  
*⟨proof⟩*

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 ⊆ X`  
**shows** `r {is total on} A`  
*⟨proof⟩*

A linear relation is linear on any subset.

**lemma** `ord_linear_subset`: **assumes** `IsLinOrder(X, r)` **and** `A ⊆ X`  
**shows** `IsLinOrder(A, r)`  
*⟨proof⟩*

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 ⊆ X` **and** `a ∈ X`  
**shows** `A = {x ∈ A. ⟨x, a⟩ ∈ r} ∪ {x ∈ A. ⟨a, x⟩ ∈ r}`  
*⟨proof⟩*

A technical fact about reflexive relations.

**lemma** refl\_add\_point:  
 assumes refl(X,r) and  $A \subseteq B \cup \{x\}$  and  $B \subseteq X$  and  
 $x \in X$  and  $\forall y \in B. \langle y, x \rangle \in r$   
 shows  $\forall a \in A. \langle a, x \rangle \in r$   
*<proof>*

## 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  $x \in \text{Interval}(r, a, b) \longleftrightarrow \langle a, x \rangle \in r \wedge \langle x, b \rangle \in r$   
*<proof>*

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  $x \in \text{Interval}(r, a, b)$   
 shows  $\langle a, x \rangle \in r \quad \langle x, b \rangle \in r$   
*<proof>*

Order\_ZF\_2\_L1, implication from right to left.

**lemma** Order\_ZF\_2\_L1B: assumes  $\langle a, x \rangle \in r \quad \langle x, b \rangle \in r$   
 shows  $x \in \text{Interval}(r, a, b)$   
*<proof>*

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

**lemma** Order\_ZF\_2\_L2: assumes refl(X,r)  
 and  $a \in X \quad b \in X$  and  $\langle a, b \rangle \in r$   
 shows  
 $a \in \text{Interval}(r, a, b)$   
 $b \in \text{Interval}(r, a, b)$   
*<proof>*

Under the assumptions of Order\_ZF\_2\_L2, the interval is nonempty.

**lemma** Order\_ZF\_2\_L2A: assumes refl(X,r)  
 and  $a \in X \quad b \in X$  and  $\langle a, b \rangle \in r$   
 shows  $\text{Interval}(r, a, b) \neq 0$   
*<proof>*

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:  $\langle a, b \rangle \in r \quad \langle b, c \rangle \in r \quad \langle c, d \rangle \in r$   
 shows  $\text{Interval}(r, b, c) \subseteq \text{Interval}(r, a, d)$   
*<proof>*

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

**lemma** Order\_ZF\_2\_L4:  
**assumes** A1:  $\text{refl}(X,r)$  **and** A2:  $\text{antisym}(r)$  **and** A3:  $a \in X$   
**shows**  $\text{Interval}(r,a,a) = \{a\}$   
*<proof>*

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

**lemma** Order\_ZF\_2\_L5: **assumes** A1:  $\text{trans}(r)$  **and** A2:  $\langle a,b \rangle \notin r$   
**shows**  $\text{Interval}(r,a,b) = 0$   
*<proof>*

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**  $\text{Interval}(r,a,b) \subseteq X$   
*<proof>*

### 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**  $\text{refl}(X,r)$  **and**  $a \in X$   
**shows**  $\text{IsBounded}(\{a\},r)$   
*<proof>*

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

**lemma** Order\_ZF\_3\_L1A: **assumes**  $r \subseteq X \times X$   
**and**  $\text{IsBoundedAbove}(A,r)$   
**shows**  $A \subseteq X$  *<proof>*

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

**lemma** Order\_ZF\_3\_L1B: **assumes**  $r \subseteq X \times X$   
**and**  $\text{IsBoundedBelow}(A,r)$   
**shows**  $A \subseteq X$  *<proof>*

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**  $x \in X$   $y \in X$   
**shows**  
 $\langle x, \text{GreaterOf}(r,x,y) \rangle \in r$   
 $\langle y, \text{GreaterOf}(r,x,y) \rangle \in r$   
 $\langle \text{SmallerOf}(r,x,y), x \rangle \in r$   
 $\langle \text{SmallerOf}(r,x,y), y \rangle \in r$   
*<proof>*

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:  $\text{trans}(r)$   
and A3:  $u \in X$   $w \in X$   
and A4:  $\forall x \in A. \langle x, u \rangle \in r$   $\forall x \in B. \langle x, w \rangle \in r$   
shows  $\forall x \in A \cup B. \langle x, \text{GreaterOf}(r, u, w) \rangle \in r$

*<proof>*

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>*

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>*

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>*

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>*

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>*

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

**theorem** Order\_ZF\_3\_T1:  
**assumes**  $r$  {is total on}  $X$  **and**  $\text{trans}(r)$   
**and**  $\text{IsBounded}(A,r)$   $\text{IsBounded}(B,r)$   
**and**  $r \subseteq X \times X$   
**shows**  $\text{IsBounded}(A \cup B, r)$   
*<proof>*

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**  $\text{trans}(r)$   
**and**  $\text{IsBounded}(A,r)$  **and**  $a \in X$  **and**  $r \subseteq X \times X$   
**shows**  $\text{IsBounded}(A \cup \{a\}, r)$   
*<proof>*

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**  $\text{IsBoundedBelow}(A, r)$   
*<proof>*

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**  $\text{IsBoundedAbove}(A, r)$   
*<proof>*

Intervals are bounded.

**lemma** Order\_ZF\_3\_L11: **shows**  
 $\text{IsBoundedAbove}(\text{Interval}(r, a, b), r)$   
 $\text{IsBoundedBelow}(\text{Interval}(r, a, b), r)$   
 $\text{IsBounded}(\text{Interval}(r, a, b), r)$   
*<proof>*

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

**lemma** Order\_ZF\_3\_L12: **assumes** A1:  $\text{IsBoundedBelow}(A, r)$  **and** A2:  $B \subseteq A$   
**shows**  $\text{IsBoundedBelow}(B, r)$   
*<proof>*

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

**lemma** Order\_ZF\_3\_L13: **assumes** A1:  $\text{IsBoundedAbove}(A, r)$  **and** A2:  $B \subseteq A$   
**shows**  $\text{IsBoundedAbove}(B, r)$   
*<proof>*

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:  $\text{trans}(r)$  **and** A3:  $\text{antisym}(r)$   
  **and** A4:  $r \subseteq X \times X$  **and** A5:  $X \neq 0$   
  **and** A6:  $\forall x \in X. \exists a \in A. x \neq a \wedge \langle x, a \rangle \in r$   
  **shows**  $\neg \text{IsBoundedAbove}(A, r)$   
*<proof>*

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

**lemma** Order\_ZF\_3\_L15: **shows**  $\text{IsBoundedAbove}(\{x \in A. \langle x, a \rangle \in r\}, r)$   
*<proof>*

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:  $\text{IsBoundedBelow}(A, r)$   
  **shows**  $\text{IsBounded}(\{x \in A. \langle x, a \rangle \in r\}, r)$   
*<proof>*

**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 maximums 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>*

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>*

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>*

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) ∈ A`  $\forall x \in A. \langle \text{Minimum}(r,A), x \rangle \in r$   
*<proof>*

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 ∪ B)` **and** A2: `trans(r)`  
**and** A3: `HasAmaximum(r,A) HasAmaximum(r,B)`  
**shows** `HasAmaximum(r,A ∪ B)`  
*<proof>*

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:  $\text{trans}(r)$   
**and** A3:  $\text{HasAmininum}(r, A)$   $\text{HasAmininum}(r, B)$   
**shows**  $\text{HasAmininum}(r, A \cup B)$   
*<proof>*

Set that has a maximum is bounded above.

**lemma** Order\_ZF\_4\_L7:  
**assumes**  $\text{HasAmaximum}(r, A)$   
**shows**  $\text{IsBoundedAbove}(A, r)$   
*<proof>*

Set that has a minimum is bounded below.

**lemma** Order\_ZF\_4\_L8A:  
**assumes**  $\text{HasAmininum}(r, A)$   
**shows**  $\text{IsBoundedBelow}(A, r)$   
*<proof>*

For reflexive relations singletons have a minimum and maximum.

**lemma** Order\_ZF\_4\_L8: **assumes**  $\text{refl}(X, r)$  **and**  $a \in X$   
**shows**  $\text{HasAmaximum}(r, \{a\})$   $\text{HasAmininum}(r, \{a\})$   
*<proof>*

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:  $\text{trans}(r)$   
**and** A3:  $A \subseteq X$  **and** A4:  $a \in X$  **and** A5:  $\text{HasAmaximum}(r, A)$   
**shows**  $\text{HasAmaximum}(r, A \cup \{a\})$   
*<proof>*

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:  $\text{trans}(r)$   
**and** A3:  $A \subseteq X$  **and** A4:  $a \in X$  **and** A5:  $\text{HasAmininum}(r, A)$   
**shows**  $\text{HasAmininum}(r, A \cup \{a\})$   
*<proof>*

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:  $\text{trans}(r)$  **and**  
A3:  $r \subseteq X \times X$  **and**  
A4:  $\forall A. \text{IsBounded}(A, r) \wedge A \neq \emptyset \longrightarrow \text{HasAmininum}(r, A)$  **and**

A5:  $B \neq 0$  and A6:  $\text{IsBoundedBelow}(B, r)$   
**shows**  $\text{HasAminimum}(r, B)$   
*<proof>*

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:  $\text{trans}(r)$  and  
A3:  $r \subseteq X \times X$  and  
A4:  $\forall A. \text{IsBounded}(A, r) \wedge A \neq 0 \longrightarrow \text{HasAmaximum}(r, A)$  and  
A5:  $B \neq 0$  and A6:  $\text{IsBoundedAbove}(B, r)$   
**shows**  $\text{HasAmaximum}(r, B)$   
*<proof>*

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**  $\text{antisym}(r)$  and  $\text{HasAminimum}(r, A)$  and  $\forall a \in A. \langle L, a \rangle \in r$   
**shows**  $\langle L, \text{Minimum}(r, A) \rangle \in r$   
*<proof>*

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**  $\text{antisym}(r)$  and  $\text{HasAmaximum}(r, A)$  and  $\forall a \in A. \langle a, M \rangle \in r$   
**shows**  $\langle \text{Maximum}(r, A), M \rangle \in r$   
*<proof>*

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:  $\text{antisym}(r)$  and A2:  $M \in A$  and  
A3:  $\forall a \in A. \langle a, M \rangle \in r$   
**shows**  $\text{Maximum}(r, A) = M$   
*<proof>*

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:  $\text{antisym}(r)$  and A2:  $m \in A$  and  
A3:  $\forall a \in A. \langle m, a \rangle \in r$   
**shows**  $\text{Minimum}(r, A) = m$   
*<proof>*

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>*

### 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**  $\langle a, u \rangle \in r$   
*<proof>*

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**  $\langle l, a \rangle \in r$   
*<proof>*

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:  $\text{HasAminimum}(r, \bigcap a \in A. r\{a\})$  **and**  
A4:  $\forall a \in A. \langle a, u \rangle \in r$   
**shows**  $\langle \text{Supremum}(r, A), u \rangle \in r$   
*<proof>*

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:  $\text{HasAmaximum}(r, \bigcap a \in A. r-\{a\})$  **and**  
A4:  $\forall a \in A. \langle l, a \rangle \in r$   
**shows**  $\langle l, \text{Infimum}(r, A) \rangle \in r$   
*<proof>*

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**

$\text{HasAminimum}(r, \bigcap_{a \in A} r\{a\})$   
 $z = \text{Supremum}(r, A)$   
*<proof>*

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

**lemma** Order\_ZF\_5\_L6:  
**assumes** A1:  $\text{antisym}(r)$  and A2:  $A \neq 0$  and  
A3:  $\text{HasAmaximum}(r, A)$   
**shows**  
 $\text{HasAminimum}(r, \bigcap_{a \in A} r\{a\})$   
 $\text{Maximum}(r, A) = \text{Supremum}(r, A)$   
*<proof>*

Properties of supremum of a set for complete relations.

**lemma** Order\_ZF\_5\_L7:  
**assumes** A1:  $r \subseteq X \times X$  and A2:  $\text{antisym}(r)$  and  
A3:  $r$  {is complete} and  
A4:  $A \subseteq X$   $A \neq 0$  and A5:  $\exists x \in X. \forall y \in A. \langle y, x \rangle \in r$   
**shows**  
 $\text{Supremum}(r, A) \in X$   
 $\forall x \in A. \langle x, \text{Supremum}(r, A) \rangle \in r$   
*<proof>*

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:  $\text{IsLinOrder}(X, r)$  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>*

### 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**  
 $\langle x,y \rangle \in \text{StrictVersion}(r) \longleftrightarrow \langle x,y \rangle \in r \wedge x \neq y$   
*<proof>*

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

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

The strict version of totality.

**lemma** `strict_of_tot`:  
**assumes** `r {is total on} X` **and** `a ∈ X` `b ∈ X` `a ≠ b`  
**shows**  $\langle a,b \rangle \in \text{StrictVersion}(r) \vee \langle b,a \rangle \in \text{StrictVersion}(r)$   
*<proof>*

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( $\langle a,b \rangle \in s$ ,  $a=b$ ,  $\langle b,a \rangle \in s$ )`  
*<proof>*

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( $\langle a,b \rangle \in s$ ,  $a=b$ ,  $\langle b,a \rangle \in s$ )`  
*<proof>*

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:  $\langle a,b \rangle \in r$`   
**shows**  $\langle b,a \rangle \notin \text{StrictVersion}(r)$   
*<proof>*

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:  $\langle a,b \rangle \in s$`   `$\langle b,c \rangle \in s$`   
**shows**  $\langle a,c \rangle \in s$   
*<proof>*

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>*

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>*

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

**lemma** `strict_ver_rel`: **assumes** `A1: r ⊆ A×A`  
 **shows** `StrictVersion(r) ⊆ A×A`  
*<proof>*

**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>
```

$\leq$  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>
```

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  $\in$  nat shows IsLinOrder(n,Le)  
<proof>
```

```
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}  $X \equiv$   
   $\{\langle p, \{x, f(\text{fst}(p)(x), \text{snd}(p)(x))\}. x \in X\}\}$   
   $p \in (X \rightarrow \text{range}(f)) \times (X \rightarrow \text{range}(f))\}$

The result of the lift belongs to the function space.

**lemma** func\_ZF\_1\_L1:

**assumes** A1:  $f : Y \times Y \rightarrow Y$   
  **and** A2:  $p \in (X \rightarrow \text{range}(f)) \times (X \rightarrow \text{range}(f))$   
  **shows**  
   $\{\langle x, f(\text{fst}(p)(x), \text{snd}(p)(x))\}. x \in X\} : X \rightarrow \text{range}(f)$   
   $\langle \text{proof} \rangle$

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:  $P = \{\langle x, f(\text{fst}(p)(x), \text{snd}(p)(x))\}. x \in X\}$   
  **shows**  $P(x) = f(\text{fst}(p)(x), \text{snd}(p)(x))$   
   $\langle \text{proof} \rangle$

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

```

theorem func_ZF_1_L3:
  assumes f : Y×Y→Y
  and F = f {lifted to function space over} X
  shows F : (X→range(f))×(X→range(f))→(X→range(f))
  ⟨proof⟩

```

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×Y→Y
  and A2: F = f {lifted to function space over} X
  and A3: s:X→range(f) r:X→range(f)
  and A4: x∈X
  shows (F⟨s,r⟩)(x) = f⟨s(x),r(x)⟩
  ⟨proof⟩

```

## 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 ≡ P : G×G→G ∧
  (∀ x ∈ G. ∀ y ∈ G. ∀ z ∈ G.
  ( P⟨P⟨x,y⟩,z⟩ = P⟨x,P⟨y,z⟩⟩ ))

```

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 ≡ ∀x∈G. ∀y∈G. f⟨x,y⟩ = f⟨y,x⟩

```

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⟩

```

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))
  ⟨proof⟩

```

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⟩

```

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⟩

```

### 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⟩

```

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:  $A \subseteq X$  and A3: A {is closed under} f
  and A4:  $x \in A$   $y \in A$   $z \in A$ 
  and A5:  $g = \text{restrict}(f, A \times A)$ 
  shows  $g\langle g\langle x, y \rangle, z \rangle = g\langle x, g\langle y, z \rangle \rangle$ 
  <proof>
```

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:  $A \subseteq X$  and A3: A {is closed under} f
  shows  $\text{restrict}(f, A \times A)$  {is associative on} A
  <proof>
```

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  $A \subseteq B$  and  $x \in A$   $y \in A$  and  $g = \text{restrict}(f, B \times B)$ 
  shows  $g\langle x, y \rangle \in A$ 
  <proof>
```

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:  $A \subseteq B$ 
  shows A {is closed under}  $\text{restrict}(f, B \times B)$ 
  <proof>
```

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  $x \in A \cap B$   $y \in A \cap B$ 
  shows  $f\langle x, y \rangle \in A \cap B$  <proof>
```

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  $A \cap B$  {is closed under} f
  <proof>
```

## 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)  
  <proof>
```

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>
```

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))  
  <proof>
```

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>
```

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 $\rightarrow$ X)  
  <proof>
```

## 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>`

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>`

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

**lemma** `singleton_fun_id`: **shows** `{x} → {x} = {id({x})}`  
`<proof>`

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

**lemma** `single_bij_id`: **shows** `bij({x},{x}) = {id({x})}`  
`<proof>`

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>`

## 5.6 Lifting to subsets

Suppose we have a binary operation  $f : X \times X \rightarrow X$  written additively as  $f(x, y) = x + y$ . 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  $p \in Pow(X) \times Pow(X)$ , say  $p = \langle A, B \rangle$ , where  $A, B \subseteq X$ . Then we assign this pair of sets the set  $\{f(x, y) : x \in A, y \in B\} = \{f(x') : x' \in A \times B\}$ . 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 `fst(p)` and `snd(p)`, resp. Recall that in Isabelle/ZF `fst(p)` and `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  $\equiv$   
 $\{\langle p, f(\text{fst}(p) \times \text{snd}(p)) \rangle\}$ .  $p \in \text{Pow}(X) \times \text{Pow}(X)$

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

**lemma lift\_subsets\_binop:** assumes A1:  $f : X \times X \rightarrow Y$   
 shows  $(f \text{ {lifted to subsets of} } X) : \text{Pow}(X) \times \text{Pow}(X) \rightarrow \text{Pow}(Y)$   
*<proof>*

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:  $f : X \times X \rightarrow Y$   
 and A2:  $A \subseteq X$   $B \subseteq X$  and A3:  $F = f \text{ {lifted to subsets of} } X$   
 shows  
 $F\langle A, B \rangle \subseteq Y$  and  
 $F\langle A, B \rangle = f(A \times B)$   
 $F\langle A, B \rangle = \{f(p) . p \in A \times B\}$   
 $F\langle A, B \rangle = \{f\langle x, y \rangle . \langle x, y \rangle \in A \times B\}$   
*<proof>*

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

**lemma lift\_subset\_suff:** assumes A1:  $f : X \times X \rightarrow Y$  and  
 A2:  $A \subseteq X$   $B \subseteq X$  and A3:  $x \in A$   $y \in B$  and  
 A4:  $F = f \text{ {lifted to subsets of} } X$   
 shows  $f\langle x, y \rangle \in F\langle A, B \rangle$   
*<proof>*

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:  $F = f \text{ {lifted to subsets of} } X$  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>*

Lifting to subsets inherits commutativity.

**lemma lift\_subset\_comm:** assumes A1:  $f : X \times X \rightarrow Y$  and  
 A2:  $f \text{ {is commutative on} } X$  and  
 A3:  $F = f \text{ {lifted to subsets of} } X$   
 shows  $F \text{ {is commutative on} } \text{Pow}(X)$   
*<proof>*

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:  $f : X \times X \rightarrow X$  **and**  
 A2:  $f$  {is associative on}  $X$  **and**  
 A3:  $F = f$  {lifted to subsets of}  $X$   
**shows**  $F$  {is associative on}  $\text{Pow}(X)$   
*<proof>*

## 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

$\text{IsDistributive}(X, A, M) \equiv (\forall a \in X. \forall b \in X. \forall c \in X.$   
 $M\langle a, A\langle b, c \rangle \rangle = A\langle M\langle a, b \rangle, M\langle a, c \rangle \rangle \wedge$   
 $M\langle A\langle b, c \rangle, a \rangle = A\langle M\langle b, a \rangle, M\langle c, a \rangle \rangle)$

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:  $\text{IsDistributive}(X, A, M)$   
**and** A2:  $Y \subseteq X$   
**and** A3:  $Y$  {is closed under}  $A$   $Y$  {is closed under}  $M$   
**and** A4:  $A_r = \text{restrict}(A, Y \times Y)$   $M_r = \text{restrict}(M, Y \times Y)$   
**and** A5:  $a \in Y$   $b \in Y$   $c \in Y$   
**shows**  $M_r\langle a, A_r\langle b, c \rangle \rangle = A_r\langle M_r\langle a, b \rangle, M_r\langle a, c \rangle \rangle \wedge$   
 $M_r\langle A_r\langle b, c \rangle, a \rangle = A_r\langle M_r\langle b, a \rangle, M_r\langle c, a \rangle \rangle$   
*<proof>*

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

**lemma** func\_ZF\_7\_L2:  
**assumes**  $\text{IsDistributive}(X, A, M)$   
**and**  $Y \subseteq X$   
**and**  $Y$  {is closed under}  $A$   
 $Y$  {is closed under}  $M$   
**and**  $A_r = \text{restrict}(A, Y \times Y)$   $M_r = \text{restrict}(M, Y \times Y)$   
**shows**  $\text{IsDistributive}(Y, A_r, M_r)$   
*<proof>*

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>*

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>*

Identity is an order isomorphism.

**lemma** id\_ord\_iso: **shows**  $\text{id}(X) \in \text{ord\_iso}(X, r, X, r)$

*<proof>*

Identity is the only order automorphism of a singleton.

**lemma** id\_ord\_auto\_singleton:

**shows**  $\text{ord\_iso}(\{x\}, r, \{x\}, r) = \{\text{id}(\{x\})\}$

*<proof>*

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:  $\text{antisym}(r)$  **and** A2:  $\text{antisym}(R)$  **and**

A3:  $f \in \text{ord\_iso}(A, r, B, R)$  **and**

A4:  $\text{HasAmaximum}(r, A)$

**shows**  $\text{HasAmaximum}(R, B)$  **and**  $\text{Maximum}(R, B) = f(\text{Maximum}(r, A))$

*<proof>*

Maximum is a fixpoint of order automorphism.

**lemma** max\_auto\_fixpoint:  
 assumes antisym(r) and  $f \in \text{ord\_iso}(A,r,A,r)$   
 and HasAmaximum(r,A)  
 shows  $\text{Maximum}(r,A) = f(\text{Maximum}(r,A))$   
*<proof>*

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:  $f \in \text{ord\_iso}(A,r,B,R)$  and A2:  $a \in A$   
 shows  $\text{restrict}(f,A-\{a\}) \in \text{ord\_iso}(A-\{a\},r,B-\{f(a)\},R)$   
*<proof>*

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  $f \in \text{ord\_iso}(A,r,B,R)$  and  
 A4: HasAmaximum(r,A) and A5:  $M = \text{Maximum}(r,A)$   
 shows  $\text{restrict}(f,A-\{M\}) \in \text{ord\_iso}(A-\{M\}, r, B-\{f(M)\},R)$   
*<proof>*

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

**lemma** ord\_iso\_extend: assumes A1:  $f \in \text{ord\_iso}(A,r,B,R)$  and  
 A2:  $M_A \notin A$   $M_B \notin B$  and  
 A3:  $\forall a \in A. \langle a, M_A \rangle \in r \quad \forall b \in B. \langle b, M_B \rangle \in R$  and  
 A4: antisym(r) antisym(R) and  
 A5:  $\langle M_A, M_A \rangle \in r \iff \langle M_B, M_B \rangle \in R$   
 shows  $f \cup \{ \langle M_A, M_B \rangle \} \in \text{ord\_iso}(A \cup \{M_A\}, r, B \cup \{M_B\}, R)$   
*<proof>*

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)  
 $\text{ord\_iso}(X - \{\text{Maximum}(r,X)\}, r, Y - \{\text{Maximum}(R,Y)\}, R) \neq 0$   
 shows  $\text{ord\_iso}(X,r,Y,R) \neq 0$   
*<proof>*

## 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×{y})`. This is really the ZF equivalent of the meta-function `fst(x)`.

**definition**

`SliceProjection(X) ≡ {⟨p,fst(p)⟩. p ∈ X }`

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

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

`SliceProjection(X×{y}): X×{y} → X`  
`domain(SliceProjection(X×{y})) = X×{y}`  
`∀p∈X×{y}. SliceProjection(X×{y})(p) = fst(p)`  
`SliceProjection(X×{y}) ∈ bij(X×{y},X)`

*⟨proof⟩*

### 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`

*⟨proof⟩*

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)`

*⟨proof⟩*

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

**lemma ord\_iso\_apply\_conv:**  
**assumes**  $f \in \text{ord\_iso}(A,r,B,R)$  **and**  
 $\langle f(x),f(y) \rangle \in R$  **and**  $x \in A \quad y \in A$   
**shows**  $\langle x,y \rangle \in r$   
*<proof>*

The next lemma tells us where the induced relation is defined

**lemma ind\_rel\_domain:**  
**assumes**  $R \subseteq B \times B$  **and**  $f:A \rightarrow B$   
**shows**  $\text{InducedRelation}(f,R) \subseteq A \times A$   
*<proof>*

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

**lemma bij\_is\_ord\_iso:** **assumes**  $A1: f \in \text{bij}(A,B)$   
**shows**  $f \in \text{ord\_iso}(A,\text{InducedRelation}(f,R),B,R)$   
*<proof>*

An order isomorphism preserves antisymmetry.

**lemma ord\_iso\_pres\_antisym:** **assumes**  $A1: f \in \text{ord\_iso}(A,r,B,R)$  **and**  
 $A2: r \subseteq A \times A$  **and**  $A3: \text{antisym}(R)$   
**shows**  $\text{antisym}(r)$   
*<proof>*

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>*

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>*

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**  $\text{IsLinOrder}(A,r)$   
*<proof>*

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>*

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:  $\text{IsBoundedAbove}(C,r) \quad C \neq 0$

shows  $\text{IsBoundedAbove}(f(C),R) \quad f(C) \neq 0$

*<proof>*

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:  $\text{HasAmininum}(R,f(C))$

shows  $\text{HasAmininum}(r,C)$

*<proof>*

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>*

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:  $r \subseteq A \times A \quad R \subseteq B \times B$  and

A3:  $C \subseteq A$

shows  $\{f(r\{a\}). a \in C\} = \{R\{b\}. b \in f(C)\}$

*<proof>*

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:  $r \subseteq A \times A \quad R \subseteq B \times B$  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>*

Order isomorphisms preserve completeness.

**lemma** ord\_iso\_pres\_compl:

assumes A1:  $f \in \text{ord\_iso}(A,r,B,R)$  and

A2:  $r \subseteq A \times A \quad R \subseteq B \times B$  and A3:  $R$  {is complete}

shows  $r$  {is complete}

*<proof>*

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>*

**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)  
  <proof>
```

`Spec` maps range of `embed` to `small`.

```
lemma (in generalization) spec_fun: shows spec: small2 $\rightarrow$ small  
  <proof>
```

`Embed` maps `smallsmall` to `big`.

```
lemma (in generalization) embed_fun: shows embed: small $\rightarrow$ big  
  <proof>
```

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

**lemma** (in `generalization`) `embed_surj`: shows `embed`  $\in$  `surj`(`small`, `small2`)  
*<proof>*

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

**theorem** (in `generalization`) `embed_bij`: shows `embed`  $\in$  `bij`(`small`, `small2`)  
*<proof>*

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

**theorem** (in `generalization`) `small2_sub_big`: shows `small2`  $\subseteq$  `big`  
*<proof>*

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

**theorem** (in `generalization`) `spec_bij`: shows `spec`  $\in$  `bij`(`small2`, `small`)  
*<proof>*

## 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  $\in$  bij(big, newbig)
  assumes move_embed: move  $\circ$  embed = id(small)
```

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

**definition** (in `generalization1`) `ret`  $\equiv$  `converse`(`move`)

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

**lemma** (in `generalization1`) `move_fun`: shows `move`: `big` $\rightarrow$ `newbig`  
*<proof>*

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

**lemma** (in `generalization1`) `move_inj`: shows `move`  $\in$  `inj`(`big`, `newbig`)  
*<proof>*

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

**lemma** (in `generalization1`) `move_surj`: shows `move`  $\in$  `surj`(`big`, `newbig`)  
*<proof>*

`big` is the domain of `move`.

**lemma** (in `generalization1`) `move_domain`: shows `domain`(`move`) = `big`  
*<proof>*

Composing move with embed takes elements of small to themselves.

**theorem** (in generalization1) move\_embed\_plain: assumes  $x \in \text{small}$   
shows  $\text{move}(\text{embed}(x)) = x$   
*<proof>*

ret is a bijection from newbignewbig to big.

**lemma** (in generalization1) ret\_bij: shows  $\text{ret} \in \text{bij}(\text{newbig}, \text{big})$   
*<proof>*

ret is an injection from newbig onto big.

**lemma** (in generalization1) ret\_inj: shows  $\text{ret} \in \text{inj}(\text{newbig}, \text{big})$   
*<proof>*

ret is a surjection from newbig onto big.

**lemma** (in generalization1) ret\_surj: shows  $\text{ret} \in \text{surj}(\text{newbig}, \text{big})$   
*<proof>*

embed is a restriction of ret to small.

**lemma** (in generalization1) ret\_restrict: shows  $\text{embed} = \text{restrict}(\text{ret}, \text{small})$   
*<proof>*

### 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  $\{t\} \notin t$   
*<proof>*

Definition of token.

**definition** (in generalization) token  $\equiv \text{Pow}(\bigcup(\bigcup(\text{small})))$

Definition of function moving the small set into big.

**definition** (in generalization)  
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 zf\_move - the ZF version of zf\_move\_fun.

**definition** (in generalization)  
zf\_move  $\equiv \{(x, \text{zf\_move\_fun}(x)) \mid x \in \text{big}\}$

Definition of zf\_newbig as the range of zf\_move.

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

zf\_move is a function that maps big to newbig.

**lemma** (in generalization) zf\_move\_fun: shows zf\_move: big $\rightarrow$ zf\_newbig  
*<proof>*

token is not in small.

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

Domain of zf\_move is big.

**lemma** (in generalization) zf\_move\_domain: shows domain(zf\_move) = big  
*<proof>*

small is a subset of big.

**theorem** (in generalization) small\_less\_zf\_newbig:  
shows small  $\subseteq$  zf\_newbig  
*<proof>*

zf\_move is an injection from big to zf\_newbig.

**theorem** (in generalization) zf\_move\_inj: shows zf\_move  $\in$  inj(big, zf\_newbig)  
*<proof>*

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

**theorem** (in generalization) zf\_move\_surj:  
shows zf\_move  $\in$  surj(big, zf\_newbig)  
*<proof>*

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

**theorem** (in generalization) zf\_move\_bij: shows zf\_move  $\in$  bij(big, zf\_newbig)  
*<proof>*

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

**theorem** (in generalization) zf\_move\_embed:  
assumes  $x \in \text{small}$  shows zf\_move(embed(x)) = x  
*<proof>*

Composition of zf\_move and embed is identity.

**theorem** (in generalization) zf\_embed\_move: shows zf\_move  $\circ$  embed = id(small)  
*<proof>*

**end**

## 8 NatGenIntEx\_ZF.thy

```
theory NatGenIntEx_ZF imports Int_ZF Generalization_ZF
```

```
begin
```

This theory shows an example application of 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⟩
```

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⟩
```

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

Naturals are a subset of integers.

```
lemma nat ⊆ int_obj ⟨proof⟩
```

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  $\text{FinPow}(X)$  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**  $A \approx |A|$

*<proof>*

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>*

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**  $|A| = n$

*<proof>*

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:  $A \in \text{FinPow}(X)$  **and** A2:  $a \in X - A$   
**shows**  
 $|A \cup \{a\}| = \text{succ}(|A|)$   
 $|A \cup \{a\}| = |A| \cup \{|A|\}$   
*<proof>*

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

**lemma** finpow\_decomp:  
**shows**  $\text{FinPow}(X) = (\bigcup n \in \text{nat}. \{A \in \text{Pow}(X). A \approx n\})$   
*<proof>*

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

**lemma** finpow\_union\_card\_nat:  
**shows**  $\text{FinPow}(X) = (\bigcup n \in \text{nat}. \{A \in \text{Pow}(X). A \lesssim n\})$   
*<proof>*

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**  $n \in \text{nat}$   $A \subseteq X$   $A \lesssim n$   
**shows**  $A \in \text{FinPow}(X)$   
*<proof>*

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

**lemma** nat\_finpow\_nat: **assumes**  $n \in \text{nat}$  **shows**  $n \in \text{FinPow}(\text{nat})$   
*<proof>*

A finite subset is a finite subset of itself.

**lemma** fin\_finpow\_self: **assumes**  $A \in \text{FinPow}(X)$  **shows**  $A \in \text{FinPow}(A)$   
*<proof>*

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

**lemma** rem\_add\_eq: **assumes**  $a \in A$  **shows**  $(A - \{a\}) \cup \{a\} = A$   
*<proof>*

Induction for finite powerset. This is similar to the standard Isabelle's Fin\_induct.

**theorem** FinPow\_induct: **assumes** A1:  $P(0)$  **and**  
A2:  $\forall A \in \text{FinPow}(X). P(A) \longrightarrow (\forall a \in X. P(A \cup \{a\}))$  **and**  
A3:  $B \in \text{FinPow}(X)$   
**shows**  $P(B)$   
*<proof>*

A subset of a finite subset is a finite subset.

**lemma** subset\_finpow: **assumes**  $A \in \text{FinPow}(X)$  **and**  $B \subseteq A$

**shows**  $B \in \text{FinPow}(X)$   
*<proof>*

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

**lemma** `diff_finpow`:  
**assumes**  $A \in \text{FinPow}(X)$  **shows**  $A-B \in \text{FinPow}(X)$   
*<proof>*

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

**corollary** `fin_rem_point_fin`: **assumes**  $A \in \text{FinPow}(X)$   
**shows**  $A - \{a\} \in \text{FinPow}(X)$   
*<proof>*

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

**lemma** `card_non_empty_succ`:  
**assumes**  $A1: A \in \text{FinPow}(X)$  **and**  $A2: A \neq 0$   
**shows**  $\exists n \in \text{nat}. |A| = \text{succ}(n)$   
*<proof>*

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**  $A \in \text{FinPow}(X)$  **and**  $A \neq 0$   
**shows**  $|A| \neq 0$   
*<proof>*

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**  
 $A2: \forall k \in \text{nat}.$   
 $(\forall A \in \text{FinPow}(X). A \lesssim k \longrightarrow P(A)) \longrightarrow$   
 $(\forall A \in \text{FinPow}(X). A \lesssim \text{succ}(k) \longrightarrow P(A))$   
**and**  $A3: A \in \text{FinPow}(X)$  **shows**  $P(A)$   
*<proof>*

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>*

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>*

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:  $\forall V \in T$ .  $\forall W \in T$ .  $V \cap W \in T$  and`

`A2:  $N \neq 0$  and A3:  $N \in \text{FinPow}(T)$`

**shows**  `$(\bigcap N) \in T$`

*<proof>*

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>*

Empty set is in finite power set.

**lemma** `empty_in_finpow`: **shows**  `$0 \in \text{FinPow}(X)$`

*<proof>*

Singleton is in the finite powerset.

**lemma** `singleton_in_finpow`: **assumes**  `$x \in X$`

**shows**  `$\{x\} \in \text{FinPow}(X)$  <proof>`

Union of two finite subsets is a finite subset.

**lemma** `union_finpow`: **assumes**  `$A \in \text{FinPow}(X)$  and  $B \in \text{FinPow}(X)$`

**shows**  `$A \cup B \in \text{FinPow}(X)$`

*<proof>*

Union of finite number of finite sets is finite.

**lemma** `fin_union_finpow`: **assumes**  `$M \in \text{FinPow}(\text{FinPow}(X))$`

**shows**  `$\bigcup M \in \text{FinPow}(X)$`

*<proof>*

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>*

An image of a finite set is finite.

**lemma** `fin_image_fin`: **assumes**  $\forall V \in B. K(V) \in C$  **and** `N ∈ FinPow(B)`  
  **shows** `{K(V). V ∈ N} ∈ FinPow(C)`  
*<proof>*

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

**lemma** `union_fin_list_fin`:  
  **assumes** `A1: n ∈ nat` **and** `A2: ∀k ∈ n. N(k) ∈ FinPow(X)`  
  **shows**  
  `{N(k). k ∈ n} ∈ FinPow(FinPow(X))` **and**  $(\bigcup_{k \in n} N(k)) \in \text{FinPow}(X)$   
*<proof>*

**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 surprisingly 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**

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

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**  $A: \forall V \in TA. \exists U \in T. V = U \cap A$

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

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

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

*<proof>*

Now we are ready to prove the statement we need.

**theorem FinRestr0:** **assumes**  $A: \forall V \in TA. \exists U \in T. V = U \cap A$

**shows**  $\forall M \in \text{Fin}(TA). \text{Prfin}(T,A,M)$

*<proof>*

This is a different form of the above theorem:

**theorem ZF1FinRestr:**

**assumes**  $A1: M \in \text{Fin}(TA)$  **and**  $A2: M \neq 0$

**and** A3:  $\forall V \in T. \exists U \in T. V = U \cap A$   
**shows**  $\exists N \in \text{Fin}(T). (\forall V \in M. \exists U \in N. (V = U \cap A)) \wedge N \neq 0$   
*<proof>*

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:  $\exists U V. (U \in T \wedge V \in T \wedge x \in U \wedge y \in V \wedge U \cap V = 0)$   
**shows**  $\exists U \in T. (x \in U \wedge y \notin U)$   
*<proof>*

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>*

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>*

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**  $\text{IntPr}(T, \text{cons}(A, N))$   
*<proof>*

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**  $\text{IntPr}(T, N)$   
*<proof>*

Next is a restatement of the above lemma that does not depend on the  $\text{IntPr}$  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>*

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**  $\{K(V). V \in \text{cons}(U, N)\} \in \text{Fin}(C)$   
*<proof>*

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>*

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>*

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>*

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>*

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>*

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>*

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:  $A \in \text{Fin}(X)$  **shows**  $A \in \text{Fin}(A)$   
*<proof>*

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

**lemma** Finite1\_L14: **assumes** A1:  $A \in \text{Fin}(X)$   $B \in \text{Fin}(Y)$   
**shows**  $A \times B \in \text{Fin}(X \times Y)$   
*<proof>*

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

**lemma** Finite1\_L15:  
**assumes** A1:  $\{b(x). x \in A\} \in \text{Fin}(B)$   $\{c(x). x \in A\} \in \text{Fin}(C)$   
**and** A2:  $f : B \times C \rightarrow E$   
**shows**  $\{f \langle b(x), c(x) \rangle. x \in A\} \in \text{Fin}(E)$   
*<proof>*

Singletons are in the finite powerset.

**lemma** Finite1\_L16: **assumes**  $x \in X$  **shows**  $\{x\} \in \text{Fin}(X)$   
*<proof>*

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>*

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>*

## 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 an 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**  $c \in Y$  **and**  $X \neq 0$   
**shows**  $\text{ConstantFunction}(X,c) \in \text{FinRangeFunctions}(X,Y)$   
*<proof>*

Finite range functions have finite range.

**lemma** `Finite1_L18`: **assumes**  $f \in \text{FinRangeFunctions}(X,Y)$   
**shows**  $\{f(x). x \in X\} \in \text{Fin}(Y)$   
*<proof>*

An alternative form of the definition of finite range functions.

**lemma** `Finite1_L19`: **assumes**  $f : X \rightarrow Y$   
**and**  $\{f(x). x \in X\} \in \text{Fin}(Y)$   
**shows**  $f \in \text{FinRangeFunctions}(X,Y)$   
*<proof>*

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

**lemma** `Finite1_L20`: **assumes** A1:  $f \in \text{FinRangeFunctions}(X,Y)$   
**and** A2:  $g : Y \rightarrow Z$   
**shows**  $g \circ f \in \text{FinRangeFunctions}(X,Z)$   
*<proof>*

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

**lemma** `Finite1_L21`:  
**assumes**  $f \in \text{FinRangeFunctions}(X,Y)$  **and**  $A \subseteq X$   
**shows**  $f(A) \in \text{Fin}(Y)$   
*<proof>*

**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: trans(r)`  
**and** `A3: A ∈ Fin(X) and A4: x ∈ X and A5: A = 0 ∨ HasAmaximum(r, A)`  
**shows** `A ∪ {x} = 0 ∨ HasAmaximum(r, A ∪ {x})`

*<proof>*

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: trans(r)`  
**and** `A3: B ∈ Fin(X)`  
**shows** `B = 0 ∨ HasAmaximum(r, B)`

*<proof>*

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** `A ∪ {x} = 0 ∨ HasAminimum(r, A ∪ {x})`

*<proof>*

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>*

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>*

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:  $A \in \text{Fin}(X)$  **and** A3:  $A \neq 0$

**shows**

Maximum(r,A)  $\in A$

Minimum(r,A)  $\in A$

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

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

*<proof>*

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:  $a \in X \quad b \in X \quad c \in X$

**shows**

Maximum(r,{a,b,c})  $\in \{a,b,c\}$

Minimum(r,{a,b,c})  $\in \{a,b,c\}$

Maximum(r,{a,b,c})  $\in X$

Minimum(r,{a,b,c})  $\in X$

$\langle a, \text{Maximum}(r,\{a,b,c\}) \rangle \in r$

$\langle b, \text{Maximum}(r,\{a,b,c\}) \rangle \in r$

$\langle c, \text{Maximum}(r,\{a,b,c\}) \rangle \in r$

*<proof>*

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:  $r \subseteq X \times X$  **and** A5:  $X \neq 0$

**and** A6:  $\forall x \in X. \exists a \in A. x \neq a \wedge \langle x, a \rangle \in r$

**shows**  $A \notin \text{Fin}(X)$

*<proof>*

**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>*

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`:  $\text{IsLinOrder}(X, r)$  **and**

`A2`:  $A \in \text{FinPow}(X)$   $A \neq 0$

**shows**

$\text{Maximum}(r, A) \in A$

$\text{Maximum}(r, A) \in X$

$\forall a \in A. \langle a, \text{Maximum}(r, A) \rangle \in r$

*<proof>*

### 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**  $\text{ord\_iso}(0, r, 0, R) \neq 0$

*<proof>*

Even weirder than `empty_ord_iso` The order automorphism of the empty set is unique.

**lemma** `empty_ord_iso_uniq`:  
 assumes  $f \in \text{ord\_iso}(0,r,0,R)$   $g \in \text{ord\_iso}(0,r,0,R)$   
 shows  $f = g$   
*<proof>*

The empty set is the only order automorphism of itself.

**lemma** `empty_ord_iso_empty`: shows  $\text{ord\_iso}(0,r,0,R) = \{0\}$   
*<proof>*

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:  $\text{IsLinOrder}(X,r)$  and A2:  $P(0)$  and  
 A3:  $\forall A \in \text{FinPow}(X). A \neq 0 \longrightarrow (P(A - \{\text{Maximum}(r,A)\}) \longrightarrow P(A))$   
 and A4:  $B \in \text{FinPow}(X)$  shows  $P(B)$   
*<proof>*

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:  $\text{IsLinOrder}(X,r)$  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>*

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:  $\text{IsLinOrder}(X,r)$  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>*

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

**theorem** `fin_ord_auto_id`: assumes A1:  $\text{IsLinOrder}(X,r)$   
 and A2:  $B \in \text{FinPow}(X)$  and A3:  $B \neq 0$   
 shows  $\text{ord\_iso}(B,r,B,r) = \{\text{id}(B)\}$   
*<proof>*

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 ∈ nat  
  shows ∀A ∈ FinPow(X). ∀B ∈ FinPow(Y).  
  A ≈ n ∧ B ≈ n → ord_iso(A,r,B,R) ≠ 0  
<proof>
```

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>
```

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 ∃!f. f ∈ ord_iso(A,r,B,R)  
<proof>
```

**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**

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

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**

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

Elements of equivalence classes belong to the set.

**lemma** EquivClass\_1\_L1:

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

**shows**  $x \in A$   
*<proof>*

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

**lemma** EquivClass\_1\_L1A:  
**assumes**  $A \subseteq X$  **shows**  $\{r\{x\}. x \in A\} \subseteq X//r$   
*<proof>*

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

**lemma** EquivClass\_1\_L2:  
**assumes** A1:  $\text{equiv}(A,r)$   $C \in A//r$  **and** A2:  $x \in C$   
**shows**  $r\{x\} = C$   
*<proof>*

Elements that belong to the same equivalence class are equivalent.

**lemma** EquivClass\_1\_L2A:  
**assumes**  $\text{equiv}(A,r)$   $C \in A//r$   $x \in C$   $y \in C$   
**shows**  $\langle x,y \rangle \in r$   
*<proof>*

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

**lemma** EquivClass\_1\_L2B:  
**assumes** A1:  $\text{equiv}(A,r)$  **and** A2:  $y \in A$  **and** A3:  $x \in r\{y\}$   
**shows**  $\langle x,y \rangle \in r$   
*<proof>*

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:  $\text{equiv}(A,r)$  **and** A2:  $\text{Congruent}(r,f)$   
**and** A3:  $C \in A//r$   $x \in C$   $y \in C$   
**shows**  $r\{f(x)\} = r\{f(y)\}$   
*<proof>*

The values of congruent functions are in the space.

**lemma** EquivClass\_1\_L4:  
**assumes** A1:  $\text{equiv}(A,r)$  **and** A2:  $C \in A//r$   $x \in C$   
**and** A3:  $\text{Congruent}(r,f)$   
**shows**  $f(x) \in A$   
*<proof>*

Equivalence classes are not empty.

**lemma** EquivClass\_1\_L5:  
**assumes** A1:  $\text{refl}(A,r)$  **and** A2:  $C \in A//r$   
**shows**  $C \neq \emptyset$   
*<proof>*

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 ∈ A//r`  
**shows**  $(\bigcup_{x \in C} r\{f(x)\}) \in A//r$   
 $\langle proof \rangle$

Congruent functions can be projected.

**lemma** `EquivClass_1_T0`:  
**assumes** `equiv(A,r)` `Congruent(r,f)`  
**shows** `ProjFun(A,r,f) : A//r → A//r`  
 $\langle proof \rangle$

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

**definition**  
`Congruent2(r,f) ≡`  
 $(\forall x_1 x_2 y_1 y_2. \langle x_1, x_2 \rangle \in r \wedge \langle y_1, y_2 \rangle \in r \longrightarrow$   
 $\langle f\langle x_1, y_1 \rangle, f\langle x_2, y_2 \rangle \rangle \in r)$

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

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 ∈ A//r C2 ∈ A//r`  
**and** `A4: z1 ∈ C1 × C2 z2 ∈ C1 × C2`  
**shows**  $r\{f(z_1)\} = r\{f(z_2)\}$   
 $\langle proof \rangle$

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

**lemma** `EquivClass_1_L8`:  
**assumes** `A1: equiv(A,r)` **and** `A2: C1 ∈ A//r` **and** `A3: C2 ∈ A//r`  
**and** `A4: z ∈ C1 × C2` **and** `A5: Congruent2(r,f)`  
**shows**  $f(z) \in A$   
 $\langle proof \rangle$

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:  $x \in A \quad y \in A$   
 and A3: Congruent2(r,f)  
 shows  $f\langle x,y \rangle \in A$   
 $\langle proof \rangle$

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

Congruent functions of two variables can be projected.

**theorem** EquivClass\_1\_T1:  
 assumes equiv(A,r) Congruent2(r,f)  
 shows ProjFun2(A,r,f) :  $(A//r) \times (A//r) \rightarrow A//r$   
 $\langle proof \rangle$

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:  $x \in A \quad y \in A$   
 shows  $\text{ProjFun2}(A,r,f)\langle r\{x\}, r\{y\} \rangle = r\{f\langle x,y \rangle\}$   
 $\langle proof \rangle$

## 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:  $c1 \in A//r \quad c2 \in A//r$   
 shows  $\text{ProjFun2}(A,r,f)\langle c1,c2 \rangle = \text{ProjFun2}(A,r,f)\langle c2,c1 \rangle$   
 $\langle proof \rangle$

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  $\text{ProjFun2}(A,r,f)$  {is commutative on}  $A//r$

*<proof>*

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>*

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>*

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 ∈ X//r b ∈ X//r c ∈ X//r  
  **and** A5: A<sub>p</sub> = ProjFun2(X,r,A) M<sub>p</sub> = ProjFun2(X,r,M)  
  **shows** M<sub>p</sub>⟨a,A<sub>p</sub>⟨b,c⟩⟩ = A<sub>p</sub>⟨ M<sub>p</sub>⟨a,b⟩,M<sub>p</sub>⟨a,c⟩⟩ ∧  
  M<sub>p</sub>⟨ A<sub>p</sub>⟨b,c⟩,a ⟩ = A<sub>p</sub>⟨ M<sub>p</sub>⟨b,a⟩, M<sub>p</sub>⟨c,a⟩⟩  
*<proof>*

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>*

### 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**

$\text{IsSaturated}(r,A) \equiv A = r^{-1}(r(A))$

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

**lemma** `EquivClass_3_L1`: **assumes**  $A1$ :  $\text{equiv}(X,r)$

**shows**  $\text{IsSaturated}(r,A) \longleftrightarrow A = r^{-1}(r(A))$

*<proof>*

For equivalence relations sets are contained in their images.

**lemma** `EquivClass_3_L2`: **assumes**  $A1$ :  $\text{equiv}(X,r)$  **and**  $A2$ :  $A \subseteq X$

**shows**  $A \subseteq r^{-1}(r(A))$

*<proof>*

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**  $A1$ :  $\text{equiv}(X,r)$

**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**  $\text{IsSaturated}(r,A)$

*<proof>*

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**  $A1$ :  $\text{equiv}(X,r)$

**and**  $A2$ :  $\text{IsSaturated}(r,A)$  **and**  $A3$ :  $A \subseteq X$

**and**  $A4$ :  $\langle x,y \rangle \in r$

**and**  $A5$ :  $x \in X \ y \in A$

**shows**  $x \in A$

*<proof>*

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**  $A1$ :  $\text{equiv}(X,r)$

**and**  $A2$ :  $\text{IsSaturated}(r,A)$  **and**  $A3$ :  $A \subseteq X$

**and**  $A4$ :  $x \in X \ y \in X$

**and**  $A5$ :  $\langle x,y \rangle \in r$

**shows**  $x \in A \longleftrightarrow y \in A$

*<proof>*

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

**lemma** `EquivClass_3_L6`: **assumes**  $A1$ :  $\text{equiv}(X,r)$

```

and A2: IsSaturated(r,A) and A3:  $A \subseteq X$  and A4:  $x \in X$ 
and A5:  $B = \{r\{x\}. x \in A\}$ 
shows  $x \in A \iff r\{x\} \in B$ 
<proof>

```

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 Xor is here, this is true for any predicate.

```

lemma EquivClass_3_L7: assumes equiv(X,r)
and IsSaturated(r,A) and  $A \subseteq X$ 
and  $x \in X$   $y \in X$ 
and  $B = \{r\{x\}. x \in A\}$ 
and  $(x \in A) \text{ Xor } (y \in A)$ 
shows  $(r\{x\} \in B) \text{ Xor } (r\{y\} \in B)$ 
<proof>

```

**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**

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

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>*

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>*

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**

$n \in \text{nat}$   $k \in \text{succ}(n)$  **and**  
 $i \in \text{nat}$   $f : X \times Y \rightarrow X$   $a : n \rightarrow Y$   $b : i \rightarrow Y$  **and**  
 $n \subseteq i$   $\forall j \in n. b(j) = a(j)$   $x \in X$   $Y \neq 0$   
**shows**  $\text{FoldSeq}(f, x, b)(k) = \text{FoldSeq}(f, x, a)(k)$

*<proof>*

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**  $n \in \text{nat}$   $f : X \times Y \rightarrow X$   $a : n \rightarrow Y$  **and**  
 $x \in X$   $k \in \text{succ}(n)$   $y \in Y$   
**shows**  $\text{FoldSeq}(f, x, \text{Append}(a, y))(k) = \text{FoldSeq}(f, x, a)(k)$

*<proof>*

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:**  $f : X \times Y \rightarrow X$   $a : n \rightarrow Y$   $x \in X$   $Y \neq 0$

**shows**

$\text{Fold}(f, x, a) = \text{FoldSeq}(f, x, a)(n)$  **and**

$\text{Fold}(f, x, a) \in X$

*<proof>*

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

**theorem fold\_empty:** **assumes A1:**  $f : X \times Y \rightarrow X$  **and**

**A2:**  $a : 0 \rightarrow Y$   $x \in X$   $Y \neq 0$

**shows**  $\text{Fold}(f, x, a) = x$

*<proof>*

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>*

**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**  
 $A \neq 0 \quad B \neq 0 \quad A \subseteq X \quad B \subseteq X \quad A \cap B = 0 \quad A \cup B = X \quad X \neq 0$   
*<proof>*

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

**lemma** `is_bisec`:

**assumes**  $A \neq 0 \quad B \neq 0 \quad A \cap B = 0$   
**shows**  $\langle A, B \rangle \in \text{Bisections}(A \cup B)$  *<proof>*

Bisection of  $X$  is a pair of subsets of  $X$ .

**lemma** `bisec_is_pair`: **assumes**  $Q \in \text{Bisections}(X)$   
**shows**  $Q = \langle \text{fst}(Q), \text{snd}(Q) \rangle$   
*<proof>*

The set of bisections of the empty set is empty.

**lemma** `bisec_empty`: **shows**  $\text{Bisections}(0) = 0$   
*<proof>*

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>*

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>*

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>*

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>*

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>*

## 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}

We can turn every injection into a partition.

**lemma** inj\_partition:  
**assumes** A1:  $b \in \text{inj}(X, Y)$   
**shows**  
 $\forall x \in X. \{x, \{b(x)\}. x \in X\}(x) = \{b(x)\}$  **and**  
 $\{x, \{b(x)\}. x \in X\}$  {is partition}  
{proof}

**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**

```
Enumeration(A,r)  $\equiv$   $\bigcup$  ord_iso(|A|,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  $\leq$  70)
defines ler_def[simp]:  $x \leq y \equiv \langle x,y \rangle \in r$ 

fixes  $\sigma$ 
```

```

defines  $\sigma\_def$  [simp]:  $\sigma(A) \equiv Enumeration(A,r)$ 

fixes  $append$  (infix  $\leftarrow$  72)
defines  $append\_def$ [simp]:  $a \leftarrow x \equiv Append(a,x)$ 

fixes  $concat$  (infixl  $\sqcup$  69)
defines  $concat\_def$ [simp]:  $a \sqcup b \equiv Concat(a,b)$ 

```

## 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  $A \in FinPow(X)$  and  $n \in nat$  and  $A \approx n$ 
  shows  $\exists !f. f \in ord\_iso(n,Le,A,r)$ 
  <proof>

```

An enumeration is an order isomorphism, a bijection, and a list.

```

lemma (in  $enums$ )  $enum\_props$ : assumes  $A \in FinPow(X)$ 
  shows
     $\sigma(A) \in ord\_iso(|A|,Le, A,r)$ 
     $\sigma(A) \in bij(|A|,A)$ 
     $\sigma(A) : |A| \rightarrow A$ 
  <proof>

```

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  $A \in FinPow(X)$ 
  shows  $\sigma(A) : |A| \rightarrow X$ 
  <proof>

```

If a list is an order isomorphism then it must be the enumeration.

```

lemma (in  $enums$ )  $ord\_iso\_enum$ : assumes  $A1: A \in FinPow(X)$  and
   $A2: n \in nat$  and  $A3: f \in ord\_iso(n,Le,A,r)$ 
  shows  $f = \sigma(A)$ 
  <proof>

```

What is the enumeration of the empty set?

```

lemma (in  $enums$ )  $empty\_enum$ : shows  $\sigma(0) = 0$ 
  <proof>

```

Adding a new maximum to a set appends it to the enumeration.

```

lemma (in  $enums$ )  $enum\_append$ :
  assumes  $A1: A \in FinPow(X)$  and  $A2: b \in X-A$  and
   $A3: \forall a \in A. a \leq b$ 

```

**shows**  $\sigma(A \cup \{b\}) = \sigma(A) \dot{\leftarrow} b$   
*<proof>*

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>*

**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 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]:  $x \cdot y \equiv f(x,y)$ 

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  $x \cdot y \cdot z = x \cdot (y \cdot z)$ 
  <proof>

```

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  $f : G \times G \rightarrow G$ 
  <proof>

```

Semigroup operation is closed.

```

lemma (in semigr0) semigr_closed:
assumes  $a \in G \quad b \in G$  shows  $a \cdot b \in G$ 
  <proof>

```

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  $a \sqcup b = a \leftarrow b(0)$ 
  <proof>

```

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  $(a \sqcup \text{Init}(b)) \leftarrow b(k) = a \sqcup b$ 
  <proof>

```

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>

```

What is the product of one element list?

```
lemma (in semigr0) prod_of_1elem: assumes A1: a: 1 → G
  shows (∏ a) = a(0)
⟨proof⟩
```

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⟩
```

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⟩
```

## 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

```
SetFold(f, a, Λ, r) = Fold1(f, a 0 Enumeration(Λ, 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)
  <proof>

```

Definition of product over a set expressed in notation of the `semigr0` locale.

```

lemma (in semigr1) setproddef:
  shows [](Λ,a) = [] (a 0 σ(Λ))
  <proof>

```

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>

```

The `enum_append` lemma from the `Enumeration` theory specialized for natural numbers.

```

lemma (in semigr1) semigr1_enum_append:
  assumes Λ ∈ FinPow(X) and
  n ∈ X - Λ and ∀k∈Λ. ⟨k,n⟩ ∈ r
  shows σ(Λ ∪ {n}) = σ(Λ)↔ n
  <proof>

```

What is product over a singleton?

```

lemma (in semigr1) gen_prod_singleton:
  assumes A1: x ∈ X
  shows []({x},a) = a(x)
  <proof>

```

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>
```

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>
```

### 17.3 Commutative semigroups

Commutative semigroups are those whose operation is commutative, i.e.  $\cdot b = b \cdot a$ . 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
  <proof>
```

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>
```

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:  $k \in \text{nat}$  and  
 A2:  $a \in \text{succ}(\text{succ}(k)) \rightarrow G$   
 shows  $(\prod a) = (\prod \text{Init}(a)) \cdot a(\text{succ}(k))$   
*<proof>*

A lemma useful in the induction step of the main theorem.

**lemma** (in semigr0) prod\_distr\_ind\_step:  
 assumes A1:  $k \in \text{nat}$  and  
 A2:  $a : \text{succ}(\text{succ}(k)) \rightarrow G$  and  
 A3:  $b : \text{succ}(\text{succ}(k)) \rightarrow G$  and  
 A4:  $c : \text{succ}(\text{succ}(k)) \rightarrow G$  and  
 A5:  $\forall j \in \text{succ}(\text{succ}(k)). c(j) = a(j) \cdot b(j)$   
 shows  
 Init(a) :  $\text{succ}(k) \rightarrow G$   
 Init(b) :  $\text{succ}(k) \rightarrow G$   
 Init(c) :  $\text{succ}(k) \rightarrow G$   
 $\forall j \in \text{succ}(k). \text{Init}(c)(j) = \text{Init}(a)(j) \cdot \text{Init}(b)(j)$   
*<proof>*

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:  $f$  {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>*

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  $n \in \text{nat}$  and  
 $a : \text{succ}(n) \rightarrow G$   $b : \text{succ}(n) \rightarrow G$   $c : \text{succ}(n) \rightarrow G$  and  
 $\forall j \in \text{succ}(n). c(j) = a(j) \cdot b(j)$   
 shows  $(\prod c) = (\prod a) \cdot (\prod b)$   
*<proof>*

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:  $\Lambda \in \text{FinPow}(X)$   
 shows  
 $\forall P \in \text{Bisections}(\Lambda). \prod(\Lambda, a) = (\prod(\text{fst}(P), a)) \cdot (\prod(\text{snd}(P), a))$   
*<proof>*

A better looking reformulation of `prod_bisect`.

**theorem** (in `semigr1`) `prod_disjoint`: **assumes**  
 A1: `f` {is commutative on} `G` **and**  
 A2: `A` ∈ `FinPow(X)` `A` ≠ 0 **and**  
 A3: `B` ∈ `FinPow(X)` `B` ≠ 0 **and**  
 A4: `A` ∩ `B` = 0  
**shows**  $\prod(A \cup B, a) = (\prod(A, a)) \cdot (\prod(B, a))$   
*<proof>*

A generalization of `prod_disjoint`.

**lemma** (in `semigr1`) `prod_list_of_lists`: **assumes**  
 A1: `f` {is commutative on} `G` **and** A2: `n` ∈ `nat`  
**shows**  $\forall M \in \text{succ}(n) \rightarrow \text{FinPow}(X)$ .  
`M` {is partition}  $\rightarrow$   
 $(\prod \{i, \prod(M(i), a)\}. i \in \text{succ}(n)\}) =$   
 $(\prod(\cup i \in \text{succ}(n). M(i), a))$   
*<proof>*

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**  
 $(\prod \{i, \prod(M(i), a)\}. i \in n\}) = (\prod(\cup i \in n. M(i), a))$   
*<proof>*

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**  $(\prod (a \circ b)) = \prod(A, a)$   
*<proof>*

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 (∏ (a 0 b)) = (∏ (a 0 c))
  ⟨proof⟩

end
```

## 18 Semigroup\_ZF.thy

```
theory CommutativeSemigroup_ZF imports Semigroup_ZF
```

```
begin
```

In the `Semigroup` theory we introduced a notion of `SetFold(f,a,Λ,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,Λ,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 cslistsun ( $\sum$  _ 70)
defines cslistsun_def[simp]:  $\sum$ k  $\equiv$  Fold1(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)})
  ⟨proof⟩

```

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⟩

```

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  $\in$  FinPow(X) A  $\neq$  0
  shows  $\sum$ (A,a)  $\in$  G and
   $\forall$ x  $\in$  X-A.  $\sum$ (A  $\cup$  {x},a) = ( $\sum$ (A,a)) + a(x)
  ⟨proof⟩

```

**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 monoidAssum: IsAmonoid(G,f)
```

```
  fixes monoper (infixl  $\oplus$  70)  
  defines monoper_def [simp]: a  $\oplus$  b  $\equiv$  f(a,b)
```

The result of the monoid operation is in the monoid (carrier).

```
lemma (in monoid0) group0_1_L1:  
  assumes a  $\in$  G b  $\in$  G shows a  $\oplus$  b  $\in$  G  
  <proof>
```

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>
```

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⟩
```

The monoid carrier is not empty.

```
lemma (in monoid0) group0_1_L3A: shows G≠0
⟨proof⟩
```

The range of the monoid operation is the whole monoid carrier.

```
lemma (in monoid0) group0_1_L3B: shows range(f) = G
⟨proof⟩
```

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
⟨proof⟩
```

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⟩
```

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⟩
```

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,restrict(f,H $\times$ H))
  <proof>

```

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:  $H \subseteq G$ 
  and A4: TheNeutralElement(G,f)  $\in$  H
  shows TheNeutralElement(H,restrict(f,H $\times$ H)) = TheNeutralElement(G,f)
  <proof>

```

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  $a \oplus b \neq$  TheNeutralElement(G,f)
  shows  $a \neq$  TheNeutralElement(G,f)  $\vee$   $b \neq$  TheNeutralElement(G,f)
  <proof>

```

**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**

```
IsAgroup(G,f) ≡  
(IsAmonoid(G,f) ∧ (∀g∈G. ∃b∈G. f⟨g,b⟩ = 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**

```
GroupInv(G,f) ≡ {⟨x,y⟩ ∈ G×G. f⟨x,y⟩ = 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 ≡ TheNeutralElement(G,P)
```

```
  fixes groper (infixl · 70)
```

```
  defines groper_def[simp]: a · b ≡ P⟨a,b⟩
```

```
  fixes inv (_-1 [90] 91)
```

```
  defines inv_def[simp]: x-1 ≡ 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)
```

```
  ⟨proof⟩
```

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)
  <proof>
```

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  $1 \in G \wedge (\forall g \in G. (1 \cdot g = g \wedge g \cdot 1 = g))$ 
  <proof>
```

The group is closed under the group operation. Used all the time, useful to have handy.

```
lemma (in group0) group_op_closed: assumes  $a \in G \quad b \in G$ 
  shows  $a \cdot b \in G$  <proof>
```

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  $a \in G \quad b \in G \quad c \in G$  shows  $a \cdot (b \cdot c) = a \cdot b \cdot c$ 
  <proof>
```

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  $P : G \times G \rightarrow G$ 
  <proof>
```

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>
```

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>
```

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>
```

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>*

The inverse is in the group.

**lemma** (in group0) inverse\_in\_group: assumes A1:  $x \in G$  shows  $x^{-1} \in G$   
*<proof>*

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>*

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>*

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>*

The inverse of the neutral element is the neutral element.

**lemma** (in group0) group\_inv\_of\_one: shows  $1^{-1} = 1$   
*<proof>*

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>*

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  $a^{-1} \neq 1$  *<proof>*

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**  $a \neq 1$   
*<proof>*

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>*

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>*

What is the inverse of a product?

**lemma** (in group0) group\_inv\_of\_two:  
**assumes** A1:  $a \in G$  and A2:  $b \in G$   
**shows**  $b^{-1} \cdot a^{-1} = (a \cdot b)^{-1}$   
*<proof>*

What is the inverse of a product of three elements?

**lemma** (in group0) group\_inv\_of\_three:  
**assumes** A1:  $a \in G$   $b \in G$   $c \in G$   
**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>*

The inverse of the inverse is the element.

**lemma** (in group0) group\_inv\_of\_inv:  
**assumes**  $a \in G$  **shows**  $a = (a^{-1})^{-1}$   
*<proof>*

Group inverse is nilpotent, therefore a bijection and involution.

**lemma** (in group0) group\_inv\_bij:  
**shows**  $\text{GroupInv}(G,P) \circ \text{GroupInv}(G,P) = \text{id}(G)$  and  $\text{GroupInv}(G,P) \in \text{bij}(G,G)$   
**and**  
 $\text{GroupInv}(G,P) = \text{converse}(\text{GroupInv}(G,P))$   
*<proof>*

For the group inverse the image is the same as inverse image.

**lemma** (in group0) inv\_image\_vimage: **shows**  $\text{GroupInv}(G,P)(V) = \text{GroupInv}(G,P)^{-1}(V)$

*<proof>*

If the unit is in a set then it is in the inverse of that set.

**lemma** (in group0) neut\_inv\_neut: assumes  $A \subseteq G$  and  $1 \in A$   
shows  $1 \in \text{GroupInv}(G, P)(A)$   
*<proof>*

The group inverse is onto.

**lemma** (in group0) group\_inv\_surj: shows  $\text{GroupInv}(G, P)(G) = G$   
*<proof>*

If  $a^{-1} \cdot b = 1$ , then  $a = b$ .

**lemma** (in group0) group0\_2\_L11:  
assumes A1:  $a \in G$   $b \in G$  and A2:  $a^{-1} \cdot b = 1$   
shows  $a = b$   
*<proof>*

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>*

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>*

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>*

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  
 $a \cdot c^{-1} = (a \cdot b^{-1}) \cdot (b \cdot c^{-1})$   
 $a^{-1} \cdot c = (a^{-1} \cdot b) \cdot (b^{-1} \cdot c)$   
 $a \cdot (b \cdot c)^{-1} = a \cdot c^{-1} \cdot b^{-1}$

$$\begin{aligned} a \cdot (b \cdot c^{-1}) &= a \cdot b \cdot c^{-1} \\ (a \cdot b^{-1} \cdot c^{-1})^{-1} &= c \cdot b \cdot a^{-1} \\ a \cdot b \cdot c^{-1} \cdot (c \cdot b^{-1}) &= a \\ a \cdot (b \cdot c) \cdot c^{-1} &= a \cdot b \end{aligned}$$

*<proof>*

Another lemma about rearranging a product of four group elements.

**lemma** (in group0) group0\_2\_L15:  
**assumes** A1:  $a \in G$   $b \in G$   $c \in G$   $d \in G$   
**shows**  $(a \cdot b) \cdot (c \cdot d)^{-1} = a \cdot (b \cdot d^{-1}) \cdot a^{-1} \cdot (a \cdot c^{-1})$

*<proof>*

We can cancel an element with its inverse that is written next to it.

**lemma** (in group0) inv\_cancel\_two:  
**assumes** A1:  $a \in G$   $b \in G$   
**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>*

Another lemma about cancelling with two group elements.

**lemma** (in group0) group0\_2\_L16A:  
**assumes** A1:  $a \in G$   $b \in G$   
**shows**  $a \cdot (b \cdot a)^{-1} = b^{-1}$

*<proof>*

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

*<proof>*

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>*

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>*

## 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) ≡ IsAgroup(H, restrict(P,H×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>*

A subgroup is contained in the group.

### lemma (in `group0`) `group0_3_L2`:

`assumes A1: IsAsubgroup(H,P)`  
`shows H ⊆ G`

*<proof>*

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 ∀h∈H. 1·h = h ∧ h·1 = h`

*<proof>*

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>*

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>*

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>*

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>*

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>*

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**  $\forall h \in H. \text{GroupInv}(H,g)(h) = h^{-1}$   
*<proof>*

Subgroups are closed with respect to taking the group inverse.

**theorem** (in group0) group0\_3\_T3A:  
**assumes** A1: IsAsubgroup(H,P) **and** A2: h∈H  
**shows**  $h^{-1} \in H$   
*<proof>*

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>

```

Intersection of subgroups is a subgroup.

```

lemma group0_3_L7:
  assumes A1: IsAgroup( $G, f$ )
  and A2: IsAsubgroup( $H_1, f$ )
  and A3: IsAsubgroup( $H_2, f$ )
  shows IsAsubgroup( $H_1 \cap H_2, \text{restrict}(f, H_1 \times H_1)$ )
  <proof>

```

The range of the subgroup operation is the whole subgroup.

```

lemma image_subgr_op: assumes A1: IsAsubgroup( $H, P$ )
  shows  $\text{restrict}(P, H \times H)(H \times H) = H$ 
  <proof>

```

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  $\text{restrict}(\text{GroupInv}(G, P), H)(H) = H$ 
  <proof>

```

**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>*

The values of the translations are what we expect.

**lemma** (in group0) group0\_5\_L2: **assumes**  $g \in G$   $a \in G$

**shows**

$\text{RightTranslation}(G, P, g)(a) = a \cdot g$

$\text{LeftTranslation}(G, P, g)(a) = g \cdot a$

*<proof>*

Composition of left translations is a left translation by the product.

**lemma** (in group0) group0\_5\_L4: **assumes** A1:  $g \in G$   $h \in G$   $a \in G$  and

A2:  $T_g = \text{LeftTranslation}(G, P, g)$   $T_h = \text{LeftTranslation}(G, P, h)$

**shows**

$T_g(T_h(a)) = g \cdot h \cdot a$

$T_g(T_h(a)) = \text{LeftTranslation}(G,P,g \cdot h)(a)$   
*<proof>*

Composition of right translations is a right translation by the product.

**lemma** (in group0) group0\_5\_L5: **assumes** A1:  $g \in G$   $h \in G$   $a \in G$  **and**  
 A2:  $T_g = \text{RightTranslation}(G,P,g)$   $T_h = \text{RightTranslation}(G,P,h)$   
**shows**  
 $T_g(T_h(a)) = a \cdot h \cdot g$   
 $T_g(T_h(a)) = \text{RightTranslation}(G,P,h \cdot g)(a)$   
*<proof>*

Point free version of group0\_5\_L4 and group0\_5\_L5.

**lemma** (in group0) trans\_comp: **assumes**  $g \in G$   $h \in G$  **shows**  
 $\text{RightTranslation}(G,P,g) \circ \text{RightTranslation}(G,P,h) = \text{RightTranslation}(G,P,h \cdot g)$   
 $\text{LeftTranslation}(G,P,g) \circ \text{LeftTranslation}(G,P,h) = \text{LeftTranslation}(G,P,g \cdot h)$   
*<proof>*

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:  $g \in G$   $h \in G$  **and**  
 A2:  $T_g = \text{LeftTranslation}(G,P,g)$   $T_h = \text{LeftTranslation}(G,P,h)$   
**shows**  $T_g(T_h(A)) = \text{LeftTranslation}(G,P,g \cdot h)(A)$   
*<proof>*

Another form of the image of a set under a composition of translations

**lemma** (in group0) group0\_5\_L6:  
**assumes** A1:  $g \in G$   $h \in G$  **and** A2:  $A \subseteq G$  **and**  
 A3:  $T_g = \text{RightTranslation}(G,P,g)$   $T_h = \text{RightTranslation}(G,P,h)$   
**shows**  $T_g(T_h(A)) = \{a \cdot h \cdot g. a \in A\}$   
*<proof>*

The translation by neutral element is the identity on group.

**lemma** (in group0) trans\_neutral: **shows**  
 $\text{RightTranslation}(G,P,1) = \text{id}(G)$  **and**  $\text{LeftTranslation}(G,P,1) = \text{id}(G)$   
*<proof>*

Composition of translations by an element and its inverse is identity.

**lemma** (in group0) trans\_comp\_id: **assumes**  $g \in G$  **shows**  
 $\text{RightTranslation}(G,P,g) \circ \text{RightTranslation}(G,P,g^{-1}) = \text{id}(G)$  **and**  
 $\text{RightTranslation}(G,P,g^{-1}) \circ \text{RightTranslation}(G,P,g) = \text{id}(G)$  **and**  
 $\text{LeftTranslation}(G,P,g) \circ \text{LeftTranslation}(G,P,g^{-1}) = \text{id}(G)$  **and**  
 $\text{LeftTranslation}(G,P,g^{-1}) \circ \text{LeftTranslation}(G,P,g) = \text{id}(G)$   
*<proof>*

Translations are bijective.

**lemma** (in group0) trans\_bij: **assumes**  $g \in G$  **shows**  
 $\text{RightTranslation}(G,P,g) \in \text{bij}(G,G)$  **and**  $\text{LeftTranslation}(G,P,g) \in \text{bij}(G,G)$

*<proof>*

Converse of a translation is translation by the inverse.

**lemma** (in group0) trans\_conv\_inv: assumes  $g \in G$  shows  
     $\text{converse}(\text{RightTranslation}(G,P,g)) = \text{RightTranslation}(G,P,g^{-1})$  and  
     $\text{converse}(\text{LeftTranslation}(G,P,g)) = \text{LeftTranslation}(G,P,g^{-1})$  and  
     $\text{LeftTranslation}(G,P,g) = \text{converse}(\text{LeftTranslation}(G,P,g^{-1}))$  and  
     $\text{RightTranslation}(G,P,g) = \text{converse}(\text{RightTranslation}(G,P,g^{-1}))$   
*<proof>*

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  $g \in G$  shows  
     $\text{LeftTranslation}(G,P,g)(A) = \text{LeftTranslation}(G,P,g^{-1})^{-1}(A)$  and  
     $\text{RightTranslation}(G,P,g)(A) = \text{RightTranslation}(G,P,g^{-1})^{-1}(A)$   
*<proof>*

Another way of looking at translations is that they are sections of the group operation.

**lemma** (in group0) trans\_eq\_section: assumes  $g \in G$  shows  
     $\text{RightTranslation}(G,P,g) = \text{Fix2ndVar}(P,g)$  and  
     $\text{LeftTranslation}(G,P,g) = \text{Fix1stVar}(P,g)$   
*<proof>*

A lemma about translating sets.

**lemma** (in group0) ltrans\_image: assumes  $A1: V \subseteq G$  and  $A2: x \in G$   
    shows  $\text{LeftTranslation}(G,P,x)(V) = \{x.v. v \in V\}$   
*<proof>*

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>*

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  
     $(P \text{ \{lifted to subsets of\} } G)(A,B) = (\bigcup_{a \in A} \text{LeftTranslation}(G,P,a)(B))$   
*<proof>*

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  $A1: A \subseteq G$   $g \in G$  and  $A2: 1 \in A$   
    shows  $g \in \text{LeftTranslation}(G,P,g)(A)$   
*<proof>*

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>
```

## 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) ↔ ( ∀a∈G. p(a-1) = (p(a))-1 )
  <proof>
```

We can express the definition of an odd function in two ways.

```
lemma (in group0) group0_6_L2:
  assumes A1: p : G→G
  shows
    (∀a∈G. p(a-1) = (p(a))-1) ↔ (∀a∈G. (p(a-1))-1 = p(a))
  <proof>
```

**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 {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>

```

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>

```

```

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 parantheses 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 parantheses, then rearrange the elements in proper order, then put the parantheses 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 parantheses 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>
```

Another useful rearrangement.

```
lemma (in group0) group0_4_L3:
  assumes A1:P {is commutative on} G
  and A2: a∈G b∈G and A3: c∈G d∈G E∈G F∈G
  shows a·b·((c·d)-1·(E·F)-1) = (a·(E·c)-1)·(b·(F·d)-1)
<proof>
```

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.a-1 = a-1.b-1
    (a.b)-1 = a-1.b-1
    (a.b-1)-1 = a-1.b
  <proof>
```

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.b.c = c.a.b
    a-1.(b-1.c-1)-1 = (a.(b.c)-1)-1
    a.(b.c)-1 = a.b-1.c-1
    a.(b.c-1)-1 = a.b-1.c
    a.b-1.c-1 = a.c-1.b-1
  <proof>
```

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
  <proof>
```

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>
```

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>*

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>*

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>*

Another lemma about cancelling with two elements.

```
lemma (in group0) group0_4_L6AA:
  assumes A1: P {is commutative on} G and A2: a∈G b∈G
  shows a·b-1·a-1 = b-1
```

*<proof>*

Another lemma about cancelling with two elements.

```
lemma (in group0) group0_4_L6AB:
  assumes A1: P {is commutative on} G and A2: a∈G b∈G
  shows
  a·(a·b)-1 = b-1
  a·(b·a-1) = b
```

*<proof>*

Another lemma about cancelling with two elements.

```
lemma (in group0) group0_4_L6AC:
  assumes P {is commutative on} G and a∈G b∈G
  shows a·(a·b-1)-1 = b
```

*<proof>*

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∈G b∈G c∈G
  shows
  a·b·c·a-1 = b·c
  a-1·b·c·a = b·c
```

*<proof>*

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<sup>-1</sup> = b·c·d

*<proof>*

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<sup>-1</sup>·(a·c<sup>-1</sup>)<sup>-1</sup> = c·b<sup>-1</sup>  
(a·c)<sup>-1</sup>·(b·c) = a<sup>-1</sup>·b  
a·(b·(c·a<sup>-1</sup>·b<sup>-1</sup>)) = c  
a·b·c<sup>-1</sup>·(c·a<sup>-1</sup>) = b

*<proof>*

Another useful rearrangement of three elements and cancelling.

**lemma** (in group0) group0\_4\_L6E:  
assumes A1: P {is commutative on} G  
and A2: a∈G b∈G c∈G  
shows  
a·b·(a·c)<sup>-1</sup> = b·c<sup>-1</sup>

*<proof>*

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∈G b∈G  
shows a·b<sup>-1</sup>·(a·b)<sup>-1</sup> = b<sup>-1</sup>·b<sup>-1</sup>

*<proof>*

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>*

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  
 $a \cdot b^{-1} \cdot c^{-1} \cdot d^{-1} = a \cdot d^{-1} \cdot b^{-1} \cdot c^{-1}$   
 $a \cdot b \cdot c \cdot d^{-1} = a \cdot d^{-1} \cdot b \cdot c$   
 $a \cdot b \cdot c^{-1} \cdot d^{-1} = a \cdot c^{-1} \cdot (b \cdot d^{-1})$   
 ⟨proof⟩

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  
 $a \cdot b \cdot c \cdot d^{-1} = a \cdot d^{-1} \cdot b \cdot c$   
 $a \cdot d \cdot (b \cdot d \cdot (c \cdot d))^{-1} = a \cdot (b \cdot c)^{-1} \cdot d^{-1}$   
 $a \cdot (b \cdot c) \cdot d = a \cdot b \cdot d \cdot c$   
 ⟨proof⟩

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⟩

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  
 $a \cdot b^{-1} \cdot (c \cdot d^{-1}) = a \cdot c \cdot (b^{-1} \cdot d^{-1})$   
 $a \cdot b^{-1} \cdot (c \cdot d^{-1}) = a \cdot c \cdot b^{-1} \cdot d^{-1}$   
 ⟨proof⟩

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<sup>-1</sup> · d<sup>-1</sup>  
 shows  
 $d = b \cdot a^{-1} \cdot c^{-1}$   
 $d = a^{-1} \cdot b \cdot c^{-1}$

$b = a \cdot d \cdot c$   
*<proof>*

**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>
```

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>
```

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>
```

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>
```

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>

```

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)
<proof>

```

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)
<proof>

```

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>

```

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>

```

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>

```

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**  $\forall s \in (X \rightarrow G). \text{GroupInv}(X \rightarrow G, F)(s) = \text{GroupInv}(G, P) \circ s$   
*<proof>*

What is the value of the group inverse for the lifted group?

**corollary** (in group0) lift\_gr\_inv\_val:  
**assumes**  $F = P$  {lifted to function space over}  $X$  and  
 $s : X \rightarrow G$  and  $x \in X$   
**shows**  $(\text{GroupInv}(X \rightarrow G, F)(s))(x) = (s(x))^{-1}$   
*<proof>*

What is the group inverse in a subgroup of the lifted group?

**lemma** (in group0) Group\_ZF\_2\_1\_L6A:  
**assumes** A1:  $F = P$  {lifted to function space over}  $X$   
**and** A2: IsAsubgroup( $H, F$ )  
**and** A3:  $g = \text{restrict}(F, H \times H)$   
**and** A4:  $s \in H$   
**shows**  $\text{GroupInv}(H, g)(s) = \text{GroupInv}(G, P) \circ s$   
*<proof>*

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:  $F = P$  {lifted to function space over}  $X$   
**and** A2:  $P$  {is commutative on}  $G$   
**shows**  $F$  {is commutative on}  $(X \rightarrow G)$   
*<proof>*

## 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:  $F = \text{ProjFun2}(G, r, f)$   
**and** A4:  $e = \text{TheNeutralElement}(G, f)$   
**shows**  $r\{e\} \in G//r \wedge$   
 $(\forall c \in G//r. F\langle r\{e\}, c \rangle = c \wedge F\langle c, r\{e\} \rangle = c)$   
*<proof>*

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:  $F = \text{ProjFun2}(G, r, f)$   
**shows** IsAmonoid( $G//r, F$ )  
*<proof>*

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>
```

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>
```

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>
```

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>
```

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∈G
  shows r{a-1} = GroupInv(G//r,F)(r{a})
<proof>
```

### 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**

$$\text{IsAnormalSubgroup}(G,P,N) \equiv \text{IsASubgroup}(N,P) \wedge (\forall n \in N. \forall g \in G. P \langle P \langle g, n \rangle, \text{GroupInv}(G,P)(g) \rangle \in N)$$

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**  $g \in G \ n \in H$   
**shows**  $g \cdot n \cdot g^{-1} \in H$   
*<proof>*

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))  
*<proof>*

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>*

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>*

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>*

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>*

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)

*<proof>*

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))

*<proof>*

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))

*<proof>*

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**  $\langle a, 1 \rangle \in \text{QuotientGroupRel}(G,P,H) \iff a \in H$

*<proof>*

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  $\longleftrightarrow$  ⟨a,1⟩ ∈ r  
 ⟨proof⟩

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  $\longleftrightarrow$  a∈H  
 ⟨proof⟩

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: IsAsubgroup(H,P)  
 and A3: g∈G h∈H  
 shows g·h·g<sup>-1</sup> ∈ H  
 ⟨proof⟩

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: IsAsubgroup(H,P)  
 shows IsAnormalSubgroup(G,P,H)  
 QuotientGroupOp(G,P,H) {is commutative on} (G//QuotientGroupRel(G,P,H))  
 ⟨proof⟩

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∈G and r = QuotientGroupRel(G,P,H)  
 and F = QuotientGroupOp(G,P,H)  
 shows r{a<sup>-1</sup>} = GroupInv(G//r,F)(r{a})  
 ⟨proof⟩

## 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**  $\exists I \in (X \rightarrow X). \forall f \in (X \rightarrow X). F(I, f) = f \wedge F(f, I) = f$   
*<proof>*

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>*

**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:  $s \in \text{FinRangeFunctions}(X,G)$   $r \in \text{FinRangeFunctions}(X,G)$   
  **shows**  $F\langle s,r \rangle \in \text{FinRangeFunctions}(X,G)$   
*<proof>*

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**  $\text{FinRangeFunctions}(X,G)$  {is closed under}  $F$   
*<proof>*

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**  $\text{GroupInv}(G,P) \circ s \in \text{FinRangeFunctions}(X,G)$   
*<proof>*

The set of finite range functions is a subgroup of the lifted group.

**theorem** Group\_ZF\_3\_1\_T1:  
  **assumes** A1:  $\text{IsAgroup}(G,P)$   
  **and** A2:  $F = P$  {lifted to function space over}  $X$   
  **and** A3:  $X \neq \emptyset$   
  **shows**  $\text{IsASubgroup}(\text{FinRangeFunctions}(X,G),F)$   
*<proof>*

## 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 integers 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)}
```

`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 `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**  $\text{HomDiff}(G,P,s, \langle m,n \rangle) = s(m \cdot n) \cdot (s(m) \cdot s(n))^{-1}$   
*<proof>*

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**  
 $\{\text{HomDiff}(G,P,s,x) . x \in G \times G\} = \{s(m \cdot n) \cdot (s(m) \cdot s(n))^{-1} . \langle m,n \rangle \in G \times G\}$   
*<proof>*

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  $\equiv$  AlmostHoms(G,P)

**fixes** Op1  
**defines** Op1\_def [simp]: Op1  $\equiv$  AlHomOp1(G,P)

**fixes** Op2  
**defines** Op2\_def [simp]: Op2  $\equiv$  AlHomOp2(G,P)

**fixes** FR  
**defines** FR\_def [simp]: FR  $\equiv$  FinRangeFunctions(G,G)

**fixes** neg ( $\sim$  [90] 91)  
**defines** neg\_def [simp]:  $\sim s \equiv \text{GroupInv}(G,P) 0 s$

**fixes**  $\delta$   
**defines**  $\delta$ \_def [simp]:  $\delta(s,x) \equiv \text{HomDiff}(G,P,s,x)$

**fixes** AHprod (**infix**  $\cdot$  69)  
**defines** AHprod\_def [simp]:  $s \cdot r \equiv \text{AlHomOp1}(G,P)\langle s,r \rangle$

**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 A1Eq_def [simp]:
s ≈ r ≡ ⟨s,r⟩ ∈ QuotientGroupRel(AH,Op1,FR)

```

HomDiff is a homomorphism on the lifted group structure.

```

lemma (in group1) Group_ZF_3_2_L1:
  assumes A1: s:G→G r:G→G
  and A2: x ∈ G×G
  and A3: F = P {lifted to function space over} G
  shows δ(F⟨ s,r⟩,x) = δ(s,x)·δ(r,x)
⟨proof⟩

```

The group operation lifted to the function space over  $G$  preserves almost homomorphisms.

```

lemma (in group1) Group_ZF_3_2_L2: assumes A1: s ∈ AH r ∈ AH
  and A2: F = P {lifted to function space over} G
  shows F⟨ s,r⟩ ∈ AH
⟨proof⟩

```

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
⟨proof⟩

```

The terms in the homomorphism difference for a function are in the group.

```

lemma (in group1) Group_ZF_3_2_L4:
  assumes s:G→G and m∈G n∈G
  shows
  m·n ∈ G
  s(m·n) ∈ G
  s(m) ∈ G s(n) ∈ G
  δ(s,⟨ m,n⟩) ∈ G
  s(m)·s(n) ∈ G
⟨proof⟩

```

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 ∈ AH and m∈G n∈G
  shows m·n ∈ G
  s(m·n) ∈ G
  s(m) ∈ G s(n) ∈ G
  δ(s,⟨ m,n⟩) ∈ G
  s(m)·s(n) ∈ G
⟨proof⟩

```

The terms in the homomorphism difference are in the group, a different form.

**lemma** (in group1) Group\_ZF\_3\_2\_L4B:  
 assumes A1:  $s \in \text{AH}$  and A2:  $x \in G \times G$   
 shows  $\text{fst}(x) \cdot \text{snd}(x) \in G$   
 $s(\text{fst}(x) \cdot \text{snd}(x)) \in G$   
 $s(\text{fst}(x)) \in G$   $s(\text{snd}(x)) \in G$   
 $\delta(s, x) \in G$   
 $s(\text{fst}(x)) \cdot s(\text{snd}(x)) \in G$   
*<proof>*

What are the values of the inverse of an almost homomorphism?

**lemma** (in group1) Group\_ZF\_3\_2\_L5:  
 assumes  $s \in \text{AH}$  and  $n \in G$   
 shows  $(\sim s)(n) = (s(n))^{-1}$   
*<proof>*

Homomorphism difference commutes with the inverse for almost homomorphisms.

**lemma** (in group1) Group\_ZF\_3\_2\_L6:  
 assumes A1:  $s \in \text{AH}$  and A2:  $x \in G \times G$   
 shows  $\delta(\sim s, x) = (\delta(s, x))^{-1}$   
*<proof>*

The inverse of an almost homomorphism maps the group into itself.

**lemma** (in group1) Group\_ZF\_3\_2\_L7:  
 assumes  $s \in \text{AH}$   
 shows  $\sim s : G \rightarrow G$   
*<proof>*

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:  $s \in \text{AH}$   
 shows  $\text{GroupInv}(G \rightarrow G, F)(s) \in \text{AH}$   
*<proof>*

The function that assigns the neutral element everywhere is an almost homomorphism.

**lemma** (in group1) Group\_ZF\_3\_2\_L9: shows  
 $\text{ConstantFunction}(G, 1) \in \text{AH}$  and  $\text{AH} \neq 0$   
*<proof>*

If the group is abelian, then almost homomorphisms form a subgroup of the lifted group.

**lemma** Group\_ZF\_3\_2\_L10:  
 assumes A1:  $\text{IsAgroup}(G, P)$   
 and A2:  $P$  {is commutative on}  $G$   
 and A3:  $F = P$  {lifted to function space over}  $G$

**shows** IsSubgroup(AlmostHoms(G,P),F)  
*<proof>*

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)  
*<proof>*

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>*

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)  
*<proof>*

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>*

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))<sup>-1</sup>  
*<proof>*

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**

$\text{Op1}\langle s, r \rangle \in \text{AH}$   
 $\text{GroupInv}(\text{AH}, \text{Op1})(r) \in \text{AH}$   
 $\text{Op1}\langle s, \text{GroupInv}(\text{AH}, \text{Op1})(r) \rangle \in \text{AH}$   
*<proof>*

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**  $s \in \text{AH}$   $r \in \text{AH}$   
**shows**  $s \cdot r \in \text{AH}$   $s \cdot (\sim r) \in \text{AH}$   
*<proof>*

### 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**  $\text{FR} \subseteq \text{AH}$   
*<proof>*

Finite range functions valued in an abelian group form a normal subgroup of almost homomorphisms.

**lemma** `Group_ZF_3_3_L2`: **assumes**  $A1: \text{IsAgroup}(G, f)$   
**and**  $A2: f \text{ \{is commutative on\} } G$   
**shows**  
 $\text{IsAsubgroup}(\text{FinRangeFunctions}(G, G), \text{AlHomOp1}(G, f))$   
 $\text{IsANormalSubgroup}(\text{AlmostHoms}(G, f), \text{AlHomOp1}(G, f),$   
 $\text{FinRangeFunctions}(G, G))$   
*<proof>*

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**  
 $\text{IsAgroup}(\text{AH} // \text{QuotientGroupRel}(\text{AH}, \text{Op1}, \text{FR}), \text{QuotientGroupOp}(\text{AH}, \text{Op1}, \text{FR}))$   
**and**  
 $\text{QuotientGroupOp}(\text{AH}, \text{Op1}, \text{FR}) \text{ \{is commutative on\} } (\text{AH} // \text{QuotientGroupRel}(\text{AH}, \text{Op1}, \text{FR}))$   
*<proof>*

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**  
 $\text{QuotientGroupRel}(\text{AH}, \text{Op1}, \text{FR}) \subseteq \text{AH} \times \text{AH}$  **and**

equiv(AH, QuotientGroupRel(AH, Op1, FR))  
 ⟨proof⟩

The "almost equal" relation is symmetric.

**lemma** (in group1) Group\_ZF\_3\_3\_L3A: assumes A1:  $s \approx r$   
 shows  $r \approx s$   
 ⟨proof⟩

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)  
 ⟨proof⟩

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  $s \in \text{AH}$  and  
 $r = \text{QuotientGroupRel}(\text{AH}, \text{Op1}, \text{FR})$  and  
 $\text{TheNeutralElement}(\text{AH} // r, \text{QuotientGroupOp}(\text{AH}, \text{Op1}, \text{FR})) = e$   
 shows  $r\{s\} = e \iff s \in \text{FR}$   
 ⟨proof⟩

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:  $s \in \text{AH}$  and  
 $r = \text{QuotientGroupRel}(\text{AH}, \text{Op1}, \text{FR})$  and  
 $F = \text{ProjFun2}(\text{AH}, r, \text{Op1})$   
 shows  $r\{\sim s\} = \text{GroupInv}(\text{AH} // r, F)(r\{s\})$   
 ⟨proof⟩

## 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  $s \in \text{AH}$  and  $m \in G$   $n \in G$

**shows**  $s(m \cdot n) = s(m) \cdot s(n) \cdot \delta(s, \langle m, n \rangle)$   
*<proof>*

What is the value of a composition of almost homomorphisms?

**lemma** (in group1) Group\_ZF\_3\_4\_L2:  
**assumes**  $s \in \text{AH}$   $r \in \text{AH}$  **and**  $m \in G$   
**shows**  $(s \circ r)(m) = s(r(m))$   $s(r(m)) \in G$   
*<proof>*

What is the homomorphism difference of a composition?

**lemma** (in group1) Group\_ZF\_3\_4\_L3:  
**assumes** A1:  $s \in \text{AH}$   $r \in \text{AH}$  **and** A2:  $m \in G$   $n \in G$   
**shows**  $\delta(s \circ r, \langle m, n \rangle) =$   
 $\delta(s, \langle r(m), r(n) \rangle) \cdot s(\delta(r, \langle m, n \rangle)) \cdot \delta(s, \langle r(m) \cdot r(n), \delta(r, \langle m, n \rangle) \rangle)$   
*<proof>*

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:  $s \in \text{AH}$   $r \in \text{AH}$  **and** A2:  $x \in G \times G$   
**and** A3:  
 $A = \delta(s, \langle r(\text{fst}(x)), r(\text{snd}(x)) \rangle)$   
 $B = s(\delta(r, x))$   
 $C = \delta(s, \langle (r(\text{fst}(x)) \cdot r(\text{snd}(x))), \delta(r, x) \rangle)$   
**shows**  $\delta(s \circ r, x) = A \cdot B \cdot C$   
*<proof>*

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:  $s \in \text{AH}$   $r \in \text{AH}$   
**shows**  $\{\delta(\text{Composition}(G) \langle s, r \rangle, x) \mid x \in G \times G\} \in \text{Fin}(G)$   
*<proof>*

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>*

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**  
 $\text{AH} \{\text{is closed under}\} \text{Composition}(G)$

AlHomOp2(G,P) {is associative on} AH  
 ⟨proof⟩

Type information related to the situation of two almost homomorphisms.

**lemma** (in group1) Group\_ZF\_3\_4\_L7:  
 assumes A1:  $s \in \text{AH}$   $r \in \text{AH}$  and A2:  $n \in G$   
 shows  
 $s(n) \in G$   $(r(n))^{-1} \in G$   
 $s(n) \cdot (r(n))^{-1} \in G$   $s(r(n)) \in G$   
 ⟨proof⟩

Type information related to the situation of three almost homomorphisms.

**lemma** (in group1) Group\_ZF\_3\_4\_L8:  
 assumes A1:  $s \in \text{AH}$   $r \in \text{AH}$   $q \in \text{AH}$  and A2:  $n \in G$   
 shows  
 $q(n) \in G$   
 $s(r(n)) \in G$   
 $r(n) \cdot (q(n))^{-1} \in G$   
 $s(r(n) \cdot (q(n))^{-1}) \in G$   
 $\delta(s, \langle q(n), r(n) \cdot (q(n))^{-1} \rangle) \in G$   
 ⟨proof⟩

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:  $s1 \in \text{AH}$   $r1 \in \text{AH}$   $s2 \in \text{AH}$   $r2 \in \text{AH}$   
 and A2:  $n \in G$   
 shows  $(s1 \circ r1)(n) \cdot ((s2 \circ r2)(n))^{-1} =$   
 $s1(r2(n)) \cdot (s2(r2(n)))^{-1} \cdot s1(r1(n)) \cdot (r2(n))^{-1} \cdot$   
 $\delta(s1, \langle r2(n), r1(n) \cdot (r2(n))^{-1} \rangle)$   
 ⟨proof⟩

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:  $s \in \text{AH}$   $r \in \text{AH}$   
 and A2:  $n \in G$   
 shows  $(s \cdot (\text{GroupInv}(\text{AH}, \text{Op1})(r)))(n) = s(n) \cdot (r(n))^{-1}$   
 ⟨proof⟩

A necessary condition for two a. h. to be almost equal.

**lemma** (in group1) Group\_ZF\_3\_4\_L11:  
 assumes A1:  $s \approx r$   
 shows  $\{s(n) \cdot (r(n))^{-1} \cdot n \in G\} \in \text{Fin}(G)$   
 ⟨proof⟩

A sufficient condition for two a. h. to be almost equal.

**lemma** (in group1) Group\_ZF\_3\_4\_L12: **assumes** A1:  $s \in \text{AH}$   $r \in \text{AH}$   
**and** A2:  $\{s(n) \cdot (r(n))^{-1}. n \in G\} \in \text{Fin}(G)$   
**shows**  $s \approx r$   
*<proof>*

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**  $s \in \text{AH}$   $r \in \text{AH}$   
**and**  $s \cdot (\text{GroupInv}(\text{AH}, \text{Op1})(r)) \in \text{FR}$   
**shows**  $s \approx r$   $r \approx s$   
*<proof>*

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**  $s \approx r$   
**shows**  $s \cdot (\text{GroupInv}(\text{AH}, \text{Op1})(r)) \in \text{FR}$   
*<proof>*

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:  $s_1 \approx s_2$   $r_1 \approx r_2$   
**shows**  $(s_1 \circ r_1) \approx (s_2 \circ r_2)$   
*<proof>*

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>*

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>*

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>*

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>

```

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>

```

## 25.5 Shifting almost homomorphisms

In this 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>

```

**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)  $\equiv$   
{ $\langle x, \langle P\langle \text{fst}(\text{fst}(x)), \text{fst}(\text{snd}(x)) \rangle \rangle, Q\langle \text{snd}(\text{fst}(x)), \text{snd}(\text{snd}(x)) \rangle \rangle$ }.  
 $x \in (G \times H) \times (G \times H)$ }
```

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>
```

And it has the intended value.

```
lemma (in direct0) DirectProduct_ZF_1_L2:  
  shows  $\forall x \in (G \times H). \forall y \in (G \times H).  
  R\langle x, y \rangle = \langle P\langle \text{fst}(x), \text{fst}(y) \rangle, Q\langle \text{snd}(x), \text{snd}(y) \rangle \rangle$   
<proof>
```

And the value belongs to the set the operation is defined on.

```
lemma (in direct0) DirectProduct_ZF_1_L3:  
  shows  $\forall x \in (G \times H). \forall y \in (G \times H). R\langle x, y \rangle \in G \times H$   
<proof>
```

## 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 {is commutative on} G and Q {is commutative on} H
  shows R {is commutative on} G×H
<proof>
```

Direct product of associative operations is associative.

```
lemma (in direct0) DirectProduct_ZF_2_L2:
  assumes P {is associative on} G and Q {is associative on} H
  shows R {is associative on} G×H
<proof>
```

**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**

$$\text{IsAnOrdGroup}(G, P, r) \equiv (\text{IsAGroup}(G, P) \wedge r \subseteq G \times G \wedge \text{IsPartOrder}(G, r) \wedge (\forall g \in G. \forall a \ b. \langle a, b \rangle \in r \longrightarrow \langle P\langle a, g \rangle, P\langle b, g \rangle \rangle \in r \wedge \langle P\langle g, a \rangle, P\langle g, b \rangle \rangle \in r))$$

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**

$$\text{PositiveSet}(G, P, r) \equiv \{x \in G. \langle \text{TheNeutralElement}(G, P), x \rangle \in r \wedge \text{TheNeutralElement}(G, P) \neq x\}$$

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**

$$\text{AbsoluteValue}(G, P, r) \equiv \text{id}(\text{Nonnegative}(G, P, r)) \cup \text{restrict}(\text{GroupInv}(G, P), G - \text{Nonnegative}(G, P, r))$$

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 · b ≡ P⟨ a,b⟩

```

```

fixes inv (_-1 [90] 91)

```

```

defines inv_def [simp]: x-1 ≡ GroupInv(G,P)(x)

```

```

fixes lesseq (infix ≤ 68)

```

```

defines lesseq_def [simp]: a ≤ b ≡ ⟨ a,b⟩ ∈ r

```

```

fixes sless (infix < 68)

```

```

defines sless_def [simp]: a < b ≡ a ≤ b ∧ a ≠ b

```

```

fixes nonnegative (G+)

```

```

defines nonnegative_def [simp]: G+ ≡ Nonnegative(G,P,r)

```

```

fixes positive (G+)

```

```

defines positive_def [simp]: G+ ≡ PositiveSet(G,P,r)

```

```

fixes setinv (- _ 72)

```

```

defines setinv_def [simp]: -A ≡ GroupInv(G,P)(A)

```

```

fixes abs (| _ |)

```

```

defines abs_def [simp]: |a| ≡ AbsoluteValue(G,P,r)(a)

```

```

fixes oddext (_°)

```

```

defines oddext_def [simp]: f° ≡ 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)  
*<proof>*

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  $G \neq 0$   
*<proof>*

The next lemma is just to see the definition of the nonnegative set in our notation.

**lemma** (in group3) OrderedGroup\_ZF\_1\_L2:  
shows  $g \in G^+ \iff 1 \leq g$   
*<proof>*

The next lemma is just to see the definition of the positive set in our notation.

**lemma** (in group3) OrderedGroup\_ZF\_1\_L2A:  
shows  $g \in G_+ \iff (1 \leq g \wedge g \neq 1)$   
*<proof>*

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:  $r$  {is total on}  $G$  and A2:  $a \in G - G^+$   
shows  $a \leq 1$   
*<proof>*

The group order is reflexive.

**lemma** (in group3) OrderedGroup\_ZF\_1\_L3: assumes  $g \in G$   
shows  $g \leq g$   
*<proof>*

1 is nonnegative.

**lemma** (in group3) OrderedGroup\_ZF\_1\_L3A: shows  $1 \in G^+$   
*<proof>*

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  $a \in G$   $b \in G$   
*<proof>*

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>*

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>*

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>*

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>*

Strict order is preserved by translations.

**lemma** (in group3) group\_strict\_ord\_transl\_inv:  
 assumes  $a < b$  and  $c \in G$   
 shows

$a \cdot c < b \cdot c$

$c \cdot a < c \cdot b$

*<proof>*

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( $G, r$ )

*<proof>*

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  $a \in G^+$  and  $b \in G - G^+$   
 shows  $b \leq a$

*<proof>*

If  $a \leq 1$  and  $a \neq 1$ , then  $a \in G \setminus G^+$ .

**lemma** (in group3) OrderedGroup\_ZF\_1\_L4C:  
 assumes A1:  $a \leq 1$  and A2:  $a \neq 1$   
 shows  $a \in G - G^+$

*<proof>*

An element smaller than an element in  $G \setminus G^+$  is in  $G \setminus G^+$ .

**lemma** (in group3) OrderedGroup\_ZF\_1\_L4D:  
 assumes A1:  $a \in G - G^+$  and A2:  $b \leq a$   
 shows  $b \in G - G^+$

*<proof>*

The nonnegative set is contained in the group.

**lemma** (in group3) OrderedGroup\_ZF\_1\_L4E: shows  $G^+ \subseteq G$   
*<proof>*

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>*

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>*

If 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>*

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>*

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>*

## 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>*

We can cancel the same element on both sides of an inequality.

**lemma** (in group3) OrderedGroup\_ZF\_1\_L5AE:  
 assumes A1:  $a \in G$   $b \in G$   $c \in G$  and A2:  $a \cdot b \leq a \cdot c$   
 shows  $b \leq c$   
*<proof>*

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:  $a \in G$   $b \in G$   $c \in G$  and A2:  $a \cdot b^{-1} \leq a \cdot c^{-1}$   
 shows  $c \leq b$   
*<proof>*

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:  $a \in G$  and A2:  $a^{-1} \leq b$   
 shows  $b^{-1} \leq a$   
*<proof>*

We can multiply the sides of two inequalities.

**lemma** (in group3) OrderedGroup\_ZF\_1\_L5B:  
 assumes A1:  $a \leq b$  and A2:  $c \leq d$   
 shows  $a \cdot c \leq b \cdot d$   
*<proof>*

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>*

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:  $c \leq c_1$   
 shows  $a \leq b \cdot c_1$   
*<proof>*

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>*

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>*

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>*

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>*

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  $a \cdot d^{-1} \leq b \cdot c^{-1}$   
*<proof>*

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>*

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>*

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>*

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>*

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**  $a \leq 1$   $a^{-1} \in G^+$   $\text{restrict}(\text{GroupInv}(G,P), G - G^+)(a) \in G^+$   
*<proof>*

If a property is invariant with respect to taking the inverse and it is true on the nonnegative set, than 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:  $a \in G$   $b \in G$   
**shows**  $Q(a,b)$   
*<proof>*

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:  $a \in G$   $b \in G$   
**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>*

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:  $a \in G$   $b \in G$   
**and** A3:  $\neg(a \leq b)$   
**shows**  $b \leq a$   $a^{-1} \leq b^{-1}$   $a \neq b$   $b < a$   
*<proof>*

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>*

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:  $a \in G$  **and** A3:  $\neg(1 \leq a)$   
**shows**  $1 \leq a^{-1}$   $1 \neq a$   $a \leq 1$   
*<proof>*

A negative element can not be nonnegative.

**lemma** (in group3) OrderedGroup\_ZF\_1\_L8B:  
**assumes** A1:  $a \leq 1$  **and** A2:  $a \neq 1$  **shows**  $\neg(1 \leq a)$   
*<proof>*

An element is greater or equal than another iff the difference is nonpositive.

**lemma** (in group3) OrderedGroup\_ZF\_1\_L9:  
**assumes** A1:  $a \in G$   $b \in G$   
**shows**  $a \leq b \iff a \cdot b^{-1} \leq 1$   
*<proof>*

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>*

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>*

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>*

If an element is greater or equal than another then the difference is nonnegative.

**lemma** (in group3) OrderedGroup\_ZF\_1\_L9D: **assumes** A1:  $a \leq b$   
**shows**  $1 \leq b \cdot a^{-1}$   
*<proof>*

If an element is greater than another then the difference is positive.

**lemma** (in group3) OrderedGroup\_ZF\_1\_L9E:  
 assumes A1:  $a \leq b$   $a \neq b$   
 shows  $1 \leq b \cdot a^{-1}$   $1 \neq b \cdot a^{-1}$   $b \cdot a^{-1} \in G_+$   
*<proof>*

If the difference is nonnegative, then  $a \leq b$ .

**lemma** (in group3) OrderedGroup\_ZF\_1\_L9F:  
 assumes A1:  $a \in G$   $b \in G$  and A2:  $1 \leq b \cdot a^{-1}$   
 shows  $a \leq b$   
*<proof>*

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  $a \cdot c \cdot b \leq a \cdot d \cdot b$   
*<proof>*

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>*

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>*

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>*

We can move an element to the other side of a strict inequality.

**lemma** (in group3) OrderedGroup\_ZF\_1\_L12B:  
 assumes A1:  $a \in G$   $b \in G$  and A2:  $a \cdot b^{-1} < c$   
 shows  $a < c \cdot b$   
*<proof>*

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:  $c \leq d$   
 shows  $a \cdot c < b \cdot d$   
*<proof>*

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:  $a \leq b$  and A2:  $c < d$   
 shows  $a \cdot c < b \cdot d$   
*<proof>*

### 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>*

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:  $a \in G$   
 shows  $a = 1 \vee a \in G_+ \vee a^{-1} \in G_+$   
*<proof>*

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>*

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>*

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>*

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:  $a \in G$   
 and A3:  $a \neq 1$   $a \notin G_+$   
 shows  $a^{-1} \in G_+$   
*<proof>*

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:  $a \in G - G_+$   
 shows  $a \leq 1$   
*<proof>*

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:  $b \in G$   
 and A3:  $Q(1)$  and A4:  $\forall a \in G_+. Q(a)$  and A5:  $\forall a \in G_+. Q(a^{-1})$   
 shows  $Q(b)$   
*<proof>*

All elements greater or equal than an element of  $G_+$  belong to  $G_+$ .

**lemma** (in group3) OrderedGroup\_ZF\_1\_L19:  
 assumes A1:  $a \in G_+$  and A2:  $a \leq b$   
 shows  $b \in G_+$   
*<proof>*

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:  $a \in G_+$   
 shows  $a^{-1} \notin G_+$   
*<proof>*

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:  $G \neq \{1\}$   
 shows  $G_+ \neq \emptyset$   
*<proof>*

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:  $a \in G$   $b \in G_+$   
 shows  $a \leq a \cdot b$   $a \neq a \cdot b$   $a \cdot b \in G$   
*<proof>*

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>*

The  $G^+$  is  $G_+$  plus the unit.

**lemma** (in group3) OrderedGroup\_ZF\_1\_L24: shows  $G^+ = G_+ \cup \{1\}$   
*<proof>*

What is  $-G_+$ , really?

**lemma** (in group3) OrderedGroup\_ZF\_1\_L25: shows  
 $(-G_+) = \{a^{-1}. a \in G_+\}$   
 $(-G_+) \subseteq G$   
*<proof>*

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>*

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  $a^{-1} \in G_+$   
*<proof>*

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  
 $G = G_+ \cup (-G_+) \cup \{1\}$   
 $G_+ \cap (-G_+) = \emptyset$   
 $1 \notin G_+ \cup (-G_+)$   
*<proof>*

If  $a \cdot b^{-1}$  is nonnegative, then  $b \leq a$ . This may be used to recover the order from the set of nonnegative elements and serve as a way to define order by prescribing 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>*

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>*

A bit stronger than 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  $a \leq b$   
*<proof>*

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>*

## 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  $a \leq M \cdot L^{-1}$   $1 \leq a$   
*<proof>*

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:  $\text{IsBounded}(A, r)$   
 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>*

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:  $\forall g \in G^+. \text{Interval}(r, 1, g) \in \text{Fin}(G)$   
 and A2:  $\text{IsBounded}(A, r)$   
 shows  $A \in \text{Fin}(G)$   
*<proof>*

In linearly ordered groups finite sets are bounded.

**theorem** (in group3) ord\_group\_fin\_bounded:  
 assumes  $r$  {is total on}  $G$  and  $B \in \text{Fin}(G)$   
 shows  $\text{IsBounded}(B, r)$   
*<proof>*

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>*

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>*

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>*

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  $\text{IsBoundedAbove}(G \setminus G_+, r)$   
*<proof>*

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**  $\text{IsBoundedAbove}(A,r)$   
*<proof>*

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:  $\text{IsBoundedAbove}(-A,r)$   
**shows**  $\text{IsBoundedBelow}(A,r)$   
*<proof>*

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**  $f(\text{Interval}(r,a,b)) \neq 0$   
*<proof>*

**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) :  $G \rightarrow G$   
*<proof>*

If  $a \in G^+$ , then  $|a| = a$ .

**lemma** (in group3) OrderedGroup\_ZF\_3\_L2:  
  **assumes** A1:  $a \in G^+$  **shows**  $|a| = a$   
*<proof>*

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**  $|1| = 1$  *<proof>*

If  $a$  is positive, then  $|a| = a$ .

**lemma** (in group3) OrderedGroup\_ZF\_3\_L2B:  
  **assumes**  $a \in G_+$  **shows**  $|a| = a$   
*<proof>*

If  $a \in G \setminus G^+$ , then  $|a| = a^{-1}$ .

**lemma** (in group3) OrderedGroup\_ZF\_3\_L3:  
  **assumes** A1:  $a \in G - G^+$  **shows**  $|a| = a^{-1}$   
*<proof>*

For elements that not greater than the unit, the absolute value is the inverse.

**lemma** (in group3) OrderedGroup\_ZF\_3\_L3A:  
  **assumes** A1:  $a \leq 1$   
  **shows**  $|a| = a^{-1}$   
*<proof>*

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:  $a \in G$   
  **shows**  $|a| \in G^+$

*<proof>*

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>*

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>*

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  $1 \leq |a|$   
*<proof>*

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>*

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>*

$a^{-1} \leq |a|$  (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>*

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  
  $a \cdot b \leq |a| \cdot |b|$   
  $a \cdot b^{-1} \leq |a| \cdot |b|$   
  $a^{-1} \cdot b \leq |a| \cdot |b|$

$a^{-1} \cdot b^{-1} \leq |a| \cdot |b|$   
*<proof>*

$|a^{-1}| \leq |a|.$

**lemma** (in group3) OrderedGroup\_ZF\_3\_L7:  
 assumes r {is total on} G and a ∈ G  
 shows  $|a^{-1}| \leq |a|$   
*<proof>*

$|a^{-1}| = |a|.$

**lemma** (in group3) OrderedGroup\_ZF\_3\_L7A:  
 assumes A1: r {is total on} G and A2: a ∈ G  
 shows  $|a^{-1}| = |a|$   
*<proof>*

$|a \cdot b^{-1}| = |b \cdot a^{-1}|.$  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  $|a \cdot b^{-1}| = |b \cdot a^{-1}|$   
*<proof>*

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  $|a \cdot b| \leq |a| \cdot |b|$   
*<proof>*

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:  $|a| \leq c$   $|b| \leq d$   
 shows  $|a \cdot b| \leq c \cdot d$   
*<proof>*

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  $|a| \leq c$   $|b| \leq d$   
 shows  $|a \cdot b^{-1}| \leq c \cdot d$   
*<proof>*

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>*

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>*

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  $b·c^{-1} ≤ a$   
*<proof>*

An application of the triangle inequality with four group elements.

**lemma** (in group3) OrderedGroup\_ZF\_3\_L7F:  
 assumes A1: P {is commutative on} G  
 and A2: r {is total on} G and  
 A3: a∈G b∈G c∈G d∈G  
 shows  $|a·c^{-1}| ≤ |a·b|·|c·d|·|b·d^{-1}|$   
*<proof>*

$|a| ≤ L$  implies  $L^{-1} ≤ a$  (it would be  $-L ≤ a$  in the additive notation).

**lemma** (in group3) OrderedGroup\_ZF\_3\_L8:  
 assumes A1: a∈G and A2:  $|a| ≤ L$   
 shows  
 $L^{-1} ≤ a$   
*<proof>*

In linearly ordered groups  $|a| ≤ L$  implies  $a ≤ L$  (it would be  $a ≤ L$  in the additive notation).

**lemma** (in group3) OrderedGroup\_ZF\_3\_L8A:  
 assumes A1: r {is total on} G  
 and A2: a∈G and A3:  $|a| ≤ L$   
 shows

$a \leq L$   
 $1 \leq L$   
*<proof>*

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>*

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>*

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>*

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>*

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:  $f: X \rightarrow G$  and A3:  $A \subseteq X$   
 and A4:  $\forall x \in A. |f(x)| \leq L$   
 shows IsBounded( $f(A), r$ )  
*<proof>*

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:  $l \leq a \leq u$   
 shows

$|a| \leq \text{GreaterOf}(r, |1|, |u|)$   
*<proof>*

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>*

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  $\exists L. \forall x \in X. |b(x)| \leq L$   
*<proof>*

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:  $\{b(x). x \in X\} \in \text{Fin}(G)$   
 shows  $\exists L \in G. \forall x \in X. |b(x)| \leq L$   
*<proof>*

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:  $a \in G$  and A3:  $a \neq 1$   
 shows  $|a| \in G_+$   
*<proof>*

## 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  $A \subseteq G$   
 and HasAmaximum( $r, A$ ) HasAminimum( $r, A$ )  
 and  $M = \text{GreaterOf}(r, |\text{Minimum}(r, A)|, |\text{Maximum}(r, A)|)$

**shows**  $M \in \text{AbsoluteValue}(G,P,r)(A)$   
*<proof>*

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:  $a \in A$   
**shows**  $|a| \leq \text{GreaterOf}(r, |\text{Minimum}(r,A)|, |\text{Maximum}(r,A)|)$   
*<proof>*

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**  $b \in \text{AbsoluteValue}(G,P,r)(A)$   
**shows**  $b \leq \text{GreaterOf}(r, |\text{Minimum}(r,A)|, |\text{Maximum}(r,A)|)$   
*<proof>*

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( $r, \text{AbsoluteValue}(G,P,r)(A)$ )  
*<proof>*

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**  $|a| \leq \text{Maximum}(r, \text{AbsoluteValue}(G,P,r)(A))$   
*<proof>*

### 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 ∈ G×G. fst(p) = snd(p) ∨ fst(p)-1·snd(p) ∈ H}
  shows ⟨a,b⟩ ∈ r ↔ a∈G ∧ b∈G ∧ a-1·b ∈ H ∪ {1}
⟨proof⟩
```

The relation defined by a positive set is antisymmetric.

```
lemma (in group0) OrderedGroup_ZF_5_L2:
  assumes A1: r = {p ∈ G×G. fst(p) = snd(p) ∨ fst(p)-1·snd(p) ∈ H}
  and A2: ∀a∈G. a≠1 → (a∈H) Xor (a-1∈H)
  shows antisym(r)
⟨proof⟩
```

The relation defined by a positive set is transitive.

```
lemma (in group0) OrderedGroup_ZF_5_L3:
  assumes A1: r = {p ∈ G×G. fst(p) = snd(p) ∨ fst(p)-1·snd(p) ∈ H}
  and A2: H⊆G H {is closed under} P
  shows trans(r)
⟨proof⟩
```

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 ∈ G×G. fst(p) = snd(p) ∨ fst(p)-1·snd(p) ∈ H}
  and A2: P {is commutative on} G
  and A3: ⟨a,b⟩ ∈ r and A4: c∈G
  shows ⟨a·c,b·c⟩ ∈ r ∧ ⟨c·a,c·b⟩ ∈ r
⟨proof⟩
```

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⊆G H {is closed under} P
  and A3: ∀a∈G. a≠1 → (a∈H) Xor (a-1∈H)
  and A4: r = {p ∈ G×G. fst(p) = snd(p) ∨ fst(p)-1·snd(p) ∈ H}
  shows
```

```

  IsAnOrdGroup(G,P,r)
  r {is total on} G
  Nonnegative(G,P,r) = PositiveSet(G,P,r) ∪ {1}
⟨proof⟩

```

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⊆G and 1 ∉ H
  and r = {p ∈ G×G. fst(p) = snd(p) ∨ fst(p)-1·snd(p) ∈ H}
  shows PositiveSet(G,P,r) = H
⟨proof⟩

```

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}
⟨proof⟩

```

## 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  $x \in G_+$ ,  $f^\circ(1) = 1$  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  $f^\circ = f \cup \{(a, (f(a^{-1}))^{-1}) \mid a \in -G_+ \} \cup \{(1,1)\}$ 
  <proof>
```

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  $f: G_+ \rightarrow G$  and  $a \in -G_+$ 
  shows
     $f(a^{-1}) \in G$ 
     $(f(a^{-1}))^{-1} \in G$ 
  <proof>
```

The main theorem about odd extensions. It basically says that the odd extension of a function is what we want to be.

```
lemma (in group3) odd_ext_props:
  assumes A1:  $r$  {is total on}  $G$  and A2:  $f: G_+ \rightarrow G$ 
  shows
     $f^\circ : G \rightarrow G$ 
     $\forall a \in G_+. (f^\circ)(a) = f(a)$ 
     $\forall a \in (-G_+). (f^\circ)(a) = (f(a^{-1}))^{-1}$ 
     $(f^\circ)(1) = 1$ 
  <proof>
```

Odd extensions are odd, of course.

```
lemma (in group3) oddext_is_odd:
  assumes A1:  $r$  {is total on}  $G$  and A2:  $f: G_+ \rightarrow G$ 
  and A3:  $a \in G$ 
  shows  $(f^\circ)(a^{-1}) = ((f^\circ)(a))^{-1}$ 
  <proof>
```

Another way of saying that odd extensions are odd.

```
lemma (in group3) oddext_is_odd_alt:
  assumes A1:  $r$  {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>
```

## 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:  $\text{IsBoundedAbove}(f(A), r)$   
**shows**  $\text{IsBoundedAbove}(A, r)$   
*<proof>*

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>*

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**  $\exists l. \forall x \in X. l \leq b(x)$   
*<proof>*

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:  $X \neq 0$  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:  $\forall a \in G. \exists b \in G_+. \forall y. b \leq y \longrightarrow f(y^{-1}) \leq a$  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>*

**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(a,b) = 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(a,b)
```

```
  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
  ⟨proof⟩

```

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
  ⟨proof⟩

```

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
  ⟨proof⟩

```

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
⟨proof⟩

```

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
⟨proof⟩

```

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
⟨proof⟩

```

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⟩

```

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⟩

```

Minus times minus is plus.

```

lemma (in ring0) Ring_ZF_1_L7A: assumes a∈R b∈R
shows (-a)·(-b) = a·b
⟨proof⟩

```

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
⟨proof⟩

```

Other basic properties involving two elements of a ring.

**lemma** (in ring0) Ring\_ZF\_1\_L9: **assumes**  $a \in R$   $b \in R$   
**shows**  
 $(-b) - a = (-a) - b$   
 $-(a+b) = (-a) - b$   
 $-(a-b) = ((-a)+b)$   
 $a - (-b) = a+b$   
*<proof>*

If the difference of two element is zero, then those elements are equal.

**lemma** (in ring0) Ring\_ZF\_1\_L9A:  
**assumes** A1:  $a \in R$   $b \in R$  **and** A2:  $a - b = 0$   
**shows**  $a = b$   
*<proof>*

Other basic properties involving three elements of a ring.

**lemma** (in ring0) Ring\_ZF\_1\_L10:  
**assumes**  $a \in R$   $b \in R$   $c \in R$   
**shows**  
 $a + (b+c) = a+b+c$   
  
 $a - (b+c) = a-b-c$   
 $a - (b-c) = a-b+c$   
*<proof>*

Another property with three elements.

**lemma** (in ring0) Ring\_ZF\_1\_L10A:  
**assumes** A1:  $a \in R$   $b \in R$   $c \in R$   
**shows**  $a + (b-c) = a+b-c$   
*<proof>*

Associativity of addition and multiplication.

**lemma** (in ring0) Ring\_ZF\_1\_L11:  
**assumes**  $a \in R$   $b \in R$   $c \in R$   
**shows**  
 $a+b+c = a+(b+c)$   
 $a \cdot b \cdot c = a \cdot (b \cdot c)$   
*<proof>*

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**  $a \in R$   $a \neq 0$   $b \in R$   $b \neq 0$   
**shows**  $a \cdot b \neq 0$   
*<proof>*

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:  $a \in R$   $b \in R$   $c \in R$

**and A3:  $a \cdot c = b \cdot c$  and A4:  $c \neq 0$**   
**shows  $a = b$**   
*<proof>*

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)**  
 **$a \in R \quad b \in R \quad c \in R \quad a \neq b \quad c \neq 0$**   
**shows  $a \cdot c \neq b \cdot c$**   
*<proof>*

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:  $a \in R \quad b \in R$  and A3:  $0 \neq a \quad 1 \neq b$**   
**shows  $a \neq a \cdot b$**   
*<proof>*

If a square is nonzero, then the element is nonzero.

**lemma (in ring0) Ring\_ZF\_1\_L13:**  
**assumes  $a \in R$  and  $a^2 \neq 0$**   
**shows  $a \neq 0$**   
*<proof>*

Square of an element and its opposite are the same.

**lemma (in ring0) Ring\_ZF\_1\_L14:**  
**assumes  $a \in R$  shows  $(-a)^2 = ((a)^2)$**   
*<proof>*

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  $H \subseteq R$  and  $H$  {is closed under} A**  
**shows  $(H \cup \{0\})$  {is closed under} A**  
*<proof>*

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:  $H \subseteq R$  and A2:  $H$  {is closed under} M**  
**shows  $(H \cup \{0\})$  {is closed under} M**  
*<proof>*

The ring is trivial iff  $0 = 1$ .

**lemma (in ring0) Ring\_ZF\_1\_L17: shows  $R = \{0\} \iff 0 = 1$**

*<proof>*

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>*

## 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**  $a + b \cdot a = (b + 1) \cdot a$   
*<proof>*

Rearrangements with two elements and cancelling.

**lemma** (in ring0) Ring\_ZF\_2\_L1A: **assumes**  $a \in R$   $b \in R$   
**shows**  
 $a - b + b = a$   
 $a + b - a = b$   
 $(-a) + b + a = b$   
 $(-a) + (b + a) = b$   
 $a + (b - a) = b$   
*<proof>*

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:  $a \in R$   $b \in R$   $c \in R$   $d \in R$   
**shows**  $a - (b + 1) \cdot c = (a - d - c) + (d - b \cdot c)$   
*<proof>*

Rearrangement about adding linear functions.

**lemma** (in ring0) Ring\_ZF\_2\_L3:  
**assumes** A1:  $a \in R$   $b \in R$   $c \in R$   $d \in R$   $x \in R$   
**shows**  $(a \cdot x + b) + (c \cdot x + d) = (a + c) \cdot x + (b + d)$   
*<proof>*

Rearrangement with three elements

**lemma** (in ring0) Ring\_ZF\_2\_L4:  
**assumes** M {is commutative on} R  
**and**  $a \in R$   $b \in R$   $c \in R$

**shows**  $a \cdot (b \cdot c) = a \cdot c \cdot b$   
*<proof>*

Some other rearrangements with three elements.

**lemma** (in ring0) ring\_rearr\_3\_elemA:  
**assumes** A1: M {is commutative on} R **and**  
A2:  $a \in R$   $b \in R$   $c \in R$   
**shows**  
 $a \cdot (a \cdot c) - b \cdot (-b \cdot c) = (a \cdot a + b \cdot b) \cdot c$   
 $a \cdot (-b \cdot c) + b \cdot (a \cdot c) = \mathbf{0}$   
*<proof>*

Some rearrangements with four elements. Properties of abelian groups.

**lemma** (in ring0) Ring\_ZF\_2\_L5:  
**assumes**  $a \in R$   $b \in R$   $c \in R$   $d \in R$   
**shows**  
 $a - b - c - d = a - d - b - c$   
 $a + b + c - d = a - d + b + c$   
 $a + b - c - d = a - c + (b - d)$   
 $a + b + c + d = a + c + (b + d)$   
*<proof>*

Two big rearrangements with six elements, useful for proving properties of complex addition and multiplication.

**lemma** (in ring0) Ring\_ZF\_2\_L6:  
**assumes** A1:  $a \in R$   $b \in R$   $c \in R$   $d \in R$   $e \in R$   $f \in R$   
**shows**  
 $a \cdot (c \cdot e - d \cdot f) - b \cdot (c \cdot f + d \cdot e) =$   
 $(a \cdot c - b \cdot d) \cdot e - (a \cdot d + b \cdot c) \cdot f$   
 $a \cdot (c \cdot f + d \cdot e) + b \cdot (c \cdot e - d \cdot f) =$   
 $(a \cdot c - b \cdot d) \cdot f + (a \cdot d + b \cdot c) \cdot e$   
 $a \cdot (c + e) - b \cdot (d + f) = a \cdot c - b \cdot d + (a \cdot e - b \cdot f)$   
 $a \cdot (d + f) + b \cdot (c + e) = a \cdot d + b \cdot c + (a \cdot f + b \cdot e)$   
*<proof>*

**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∈AH r∈AH q∈AH and A2: n∈G
  shows
    ((s◦(r·q))(n))·(((s◦r)·(s◦q))(n))-1 = δ(s,⟨ r(n),q(n)⟩)
    ((r·q)◦s)(n) = ((r◦s)·(q◦s))(n)
  ⟨proof⟩
```

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
    s◦(r·q) ≈ (s◦r)·(s◦q)
    (r·q)◦s = (r◦s)·(q◦s)
  ⟨proof⟩
```

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⟩
```

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>
```

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)  
  <proof>
```

**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 $\rangle \langle$   $\in$  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)
  <proof>

```

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)
  <proof>

```

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
  <proof>

```

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>

```

The order relation in rings is transitive.

```

lemma (in ring1) ring_ord_transitive: assumes A1: a ≤ b  b ≤ c
shows a ≤ c
  <proof>

```

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 ≤ c
shows a < c
  <proof>

```

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 ≤ b and A2: b < c
shows a < c
  <proof>

```

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>*

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:  $a \in R$   
 shows  $a \leq 0 \vee (0 \leq a \wedge a \neq 0)$   
*<proof>*

Taking minus on both sides reverses an inequality.

**lemma** (in ring1) OrdRing\_ZF\_1\_L4B: assumes  $a \leq b$   
 shows  $(-b) \leq (-a)$   
*<proof>*

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  $0 \leq a$   $0 \leq b$   
 shows  $0 \leq a \cdot b$   
*<proof>*

Double nonnegative is nonnegative.

**lemma** (in ring1) OrdRing\_ZF\_1\_L5A: assumes A1:  $0 \leq a$   
 shows  $0 \leq 2 \cdot a$   
*<proof>*

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)  
*<proof>*

$a \leq b$  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  $a \in R$   $b \in R$   
 shows  $a \leq b \iff a - b \leq 0$   
*<proof>*

Negative times positive is negative.

**lemma** (in ring1) OrdRing\_ZF\_1\_L8:  
 assumes A1:  $a \leq 0$  and A2:  $0 \leq b$   
 shows  $a \cdot b \leq 0$   
*<proof>*

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:  $a \leq b$  and A2:  $0 \leq c$   
 shows  
 $a \cdot c \leq b \cdot c$   
 $c \cdot a \leq c \cdot b$   
*<proof>*

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:  $c \in R_+$   
 shows  
 $a \cdot c \leq b \cdot c$   
 $c \cdot a \leq c \cdot b$   
*<proof>*

A square is nonnegative.

**lemma** (in ring1) OrdRing\_ZF\_1\_L10:  
 assumes A1:  $a \in R$  shows  $0 \leq (a^2)$   
*<proof>*

1 is nonnegative.

**corollary** (in ring1) ordring\_one\_is\_nonneg: shows  $0 \leq 1$   
*<proof>*

In nontrivial rings one is positive.

**lemma** (in ring1) ordring\_one\_is\_pos: assumes  $0 \neq 1$   
 shows  $1 \in R_+$   
*<proof>*

Nonnegative is not negative. Property of ordered groups.

**lemma** (in ring1) OrdRing\_ZF\_1\_L11: assumes  $0 \leq a$   
 shows  $\neg(a \leq 0 \wedge a \neq 0)$   
*<proof>*

A negative element cannot be a square.

```
lemma (in ring1) OrdRing_ZF_1_L12:
  assumes A1:  $a \leq 0$   $a \neq 0$ 
  shows  $\neg(\exists b \in R. a = (b^2))$ 
<proof>
```

If  $a \leq b$ , then  $0 \leq b - a$ .

```
lemma (in ring1) OrdRing_ZF_1_L13: assumes  $a \leq b$ 
  shows  $0 \leq b - a$ 
<proof>
```

If  $a < b$ , then  $0 < b - a$ .

```
lemma (in ring1) OrdRing_ZF_1_L14: assumes  $a \leq b$   $a \neq b$ 
  shows
 $0 \leq b - a$   $0 \neq b - a$ 
 $b - a \in R_+$ 
<proof>
```

If the difference is nonnegative, then  $a \leq b$ .

```
lemma (in ring1) OrdRing_ZF_1_L15:
  assumes  $a \in R$   $b \in R$  and  $0 \leq b - a$ 
  shows  $a \leq b$ 
<proof>
```

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>
```

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:  $0 \leq a$  and A2:  $a \leq b$  and A3:  $1 \leq c$ 
  shows  $a \leq b \cdot c$ 
<proof>
```

Strict order is preserved by translations.

```
lemma (in ring1) ring_strict_ord_trans_inv:
  assumes  $a < b$  and  $c \in R$ 
  shows
 $a + c < b + c$ 
 $c + a < c + b$ 
<proof>
```

We can put an element on the other side of a strict inequality, changing its sign.

**lemma** (in ring1) OrdRing\_ZF\_1\_L18:  
**assumes**  $a \in R$   $b \in R$  **and**  $a - b < c$   
**shows**  $a < c + b$   
*<proof>*

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**  $c \leq d$   
**shows**  $a + c < b + d$   
*<proof>*

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**  $a + c < b + d$   
*<proof>*

## 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**  $|a \cdot b| = |a| \cdot |b|$   
*<proof>*

The absolute value of an element and its negative are the same.

**lemma** (in ring1) OrdRing\_ZF\_2\_L2: **assumes**  $a \in R$   
**shows**  $|-a| = |a|$   
*<proof>*

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**  
 $|(-a) \cdot b| = |a \cdot b|$   
 $|a \cdot (-b)| = |a \cdot b|$   
 $|(-a) \cdot (-b)| = |a \cdot b|$   
*<proof>*

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**  $0 \leq (-a)$   $0 \neq a$   
*<proof>*

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>*

Triangle inequality. Property of linearly ordered abelian groups.

**lemma** (in ring1) ord\_ring\_triangle\_ineq: **assumes**  $a \in R$   $b \in R$   
**shows**  $|a+b| \leq |a|+|b|$   
*<proof>*

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**  $a+b \leq 2 \cdot c$   
*<proof>*

### 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  
*<proof>*

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 ( $a=0$ ,  $a \in R_+$ ,  $(-a) \in R_+$ )  
*<proof>*

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**  $(-a) \in R_+$   
*<proof>*

$R_+$  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>*

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:  $M \text{ \{is commutative on\} } R$  **and**  
A2:  $P \subseteq R$   $P \text{ \{is closed under\} } A$   $0 \notin P$  **and**  
A3:  $\forall a \in R. a \neq 0 \longrightarrow (a \in P) \text{ Xor } ((-a) \in P)$  **and**  
A4:  $P \text{ \{is closed under\} } M$  **and**  
A5:  $r = \text{OrderFromPosSet}(R, A, P)$   
**shows**  
`IsAnOrdGroup`( $R, A, r$ )  
`IsAnOrdRing`( $R, A, M, r$ )  
 $r \text{ \{is total on\} } R$   
`PositiveSet`( $R, A, r$ ) =  $P$   
`Nonnegative`( $R, A, r$ ) =  $P \cup \{0\}$   
`HasNoZeroDivs`( $R, A, M$ )  
*<proof>*

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**  
 $R_+ \notin \text{Fin}(R)$   
 $R \notin \text{Fin}(R)$   
*<proof>*

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**  
 $\neg \text{IsBoundedAbove}(B, r)$   
 $B \notin \text{Fin}(R)$   
*<proof>*

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>*

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>*

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>*

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>*

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  $a \leq a+b$   $a \neq a+b$   
*<proof>*

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  $a \leq a+1$   $a \neq a+1$   
*<proof>*

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>*

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>*

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>*

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  $a \in R_+$   
*<proof>*

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  $0 \leq a^2$   $a^2 \neq 0$   $a^2 \in R_+$   
*<proof>*

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  $a \leq a \cdot b$   $a \neq a \cdot b$   
*<proof>*

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>*

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:  $a \in R_+$  and  
 A3:  $a \leq b$  and A4:  $1 < c$   
 shows  $a < b \cdot c$   
*<proof>*

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:  $a \in R$   $b \in R$  and  
 A3:  $a \neq 0 \vee b \neq 0$

**shows**  $0 < a^2 + b^2$   
*<proof>*

**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)  $\wedge$   
( $\forall a \in K. a \neq \text{TheNeutralElement}(K,A) \longrightarrow$   
( $\exists b \in K. M\langle a,b \rangle = \text{TheNeutralElement}(K,M)$ )))
```

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)  
  <proof>
```

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)
```

*<proof>*

Let's have an explicit statement that the multiplication in fields is commutative.

**lemma** (in field0) field\_mult\_comm: **assumes**  $a \in K$   $b \in K$   
**shows**  $a \cdot b = b \cdot a$   
*<proof>*

Fields do not have zero divisors.

**lemma** (in field0) field\_has\_no\_zero\_divs: **shows** HasNoZeroDivs(K,A,M)  
*<proof>*

$K_0$  (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  
*<proof>*

Any nonzero element has a right inverse that is nonzero.

**lemma** (in field0) Field\_ZF\_1\_L3: **assumes** A1:  $a \in K_0$   
**shows**  $\exists b \in K_0. a \cdot b = 1$   
*<proof>*

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,  $K_0 \times K_0$ ))  
 $1 = \text{TheNeutralElement}(K_0, \text{restrict}(M, K_0 \times K_0))$   
*<proof>*

The inverse of a nonzero field element is nonzero.

**lemma** (in field0) Field\_ZF\_1\_L5: **assumes** A1:  $a \in K$   $a \neq 0$   
**shows**  $a^{-1} \in K_0$   $(a^{-1})^2 \in K_0$   $a^{-1} \in K$   $a^{-1} \neq 0$   
*<proof>*

The inverse is really the inverse.

**lemma** (in field0) Field\_ZF\_1\_L6: **assumes** A1:  $a \in K$   $a \neq 0$   
**shows**  $a \cdot a^{-1} = 1$   $a^{-1} \cdot a = 1$   
*<proof>*

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**  
 $a \cdot b \cdot b^{-1} = a$   
 $a \cdot b^{-1} \cdot b = a$   
*<proof>*

## 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)

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  $a \cdot c^{-1} \neq b \cdot c^{-1}$   
(proof)

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)

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  $a \in K$   $a \neq 0$  and  $b^{-1} \neq a$   
shows  $a^{-1} \neq b$   
(proof)

An identity with two field elements, one and an inverse.

**lemma** (in field0) Field\_ZF\_2\_L5:  
assumes  $a \in K$   $b \in K$   $b \neq 0$   
shows  $(1 + a \cdot b) \cdot b^{-1} = a + b^{-1}$   
(proof)

An identity with three field elements, inverse and cancelling.

**lemma** (in field0) Field\_ZF\_2\_L6: assumes A1:  $a \in K$   $b \in K$   $b \neq 0$   $c \in K$   
shows  $a \cdot b \cdot (c \cdot b^{-1}) = a \cdot c$   
(proof)

## 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 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  $\equiv \{(p, \text{fst}(p) \cdot \text{snd}(p)^{-1}) . p \in K \times K_0\}$ 

  fixes fdiv (infixl / 95)
  defines fdiv_def[simp]: x/y  $\equiv \text{division}(x,y)$ 
```

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>
```

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>
```

```
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**

```
IsAnOrdField(K,A,M,r)  $\equiv$  (IsAnOrdRing(K,A,M,r)  $\wedge$   
  (M {is commutative on} K)  $\wedge$   
  TheNeutralElement(K,A)  $\neq$  TheNeutralElement(K,M)  $\wedge$   
  ( $\forall a \in K. a \neq$ TheNeutralElement(K,A)  $\longrightarrow$   
  ( $\exists b \in K. M\{a,b\} =$  TheNeutralElement(K,M))))
```

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  $\neq$  1
```

```
  assumes inv_exists:  $\forall a \in R. a \neq 0 \longrightarrow (\exists b \in R. a \cdot b = 1)$ 
```

```
  fixes non_zero (R0)
```

```
  defines non_zero_def[simp]: R0  $\equiv$  R - {0}
```

```
  fixes inv ( $_^{-1}$  [96] 97)
```

```
  defines inv_def[simp]:  $a^{-1} \equiv$  GroupInv(R0, restrict(M, R0  $\times$  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)  
⟨proof⟩

Ordered field is a field, of course.

**lemma** OrdField\_ZF\_1\_L1A: assumes IsAnOrdField(K,A,M,r)  
shows IsAfield(K,A,M)  
⟨proof⟩

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)  
⟨proof⟩

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)  
⟨proof⟩

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⟩

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)  
⟨proof⟩

The set of positive field elements is closed under multiplication.

**lemma** (in field1) OrdField\_ZF\_1\_L5: shows  $R_+$  {is closed under} M  
⟨proof⟩

The set of positive field elements is closed under multiplication: the explicit version.

**lemma** (in field1) pos\_mul\_closed:  
assumes A1:  $0 < a \quad 0 < b$   
shows  $0 < a \cdot b$   
⟨proof⟩

In fields square of a nonzero element is positive.

**lemma** (in field1) OrdField\_ZF\_1\_L6: assumes  $a \in R \quad a \neq 0$

**shows**  $a^2 \in R_+$   
*<proof>*

The next lemma restates the fact `Field_ZF` that our 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**  $a \cdot (a^{-1}) = 1$   $(a^{-1}) \cdot a = 1$   
*<proof>*

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>*

Some properties of the inverse of a positive element.

**lemma** (in `field1`) `OrdField_ZF_1_L8`: **assumes**  $A1: a \in R_+$   
**shows**  $a^{-1} \in R_+$   $a \cdot (a^{-1}) = 1$   $(a^{-1}) \cdot a = 1$   
*<proof>*

If  $a < b$ , then  $(b - a)^{-1}$  is positive.

**lemma** (in `field1`) `OrdField_ZF_1_L9`: **assumes**  $a < b$   
**shows**  $(b - a)^{-1} \in R_+$   
*<proof>*

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**  $A1: a \in R$   $b \in R$  **and**  $A2: a \neq 0 \vee b \neq 0$   
**shows**  $0 < a^2 + b^2$  **and**  $\exists c \in R. (a^2 + b^2) \cdot c = 1$   
*<proof>*

## 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**  $c \in R_+$   
**shows**  $a \cdot c < b \cdot c$   
*<proof>*

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:  $a \in \mathbb{R}_+$  and A2:  $a^{-1} < b$   
 shows  $1 < b \cdot a$   
*<proof>*

We can multiply an inequality by the inverse of a positive element.

**lemma** (in field1) OrdField\_ZF\_2\_L3:  
 assumes  $a \leq b$  and  $c \in \mathbb{R}_+$  shows  $a \cdot (c^{-1}) \leq b \cdot (c^{-1})$   
*<proof>*

We can multiply a strict inequality by a positive element or its inverse.

**lemma** (in field1) OrdField\_ZF\_2\_L4:  
 assumes  $a < b$  and  $c \in \mathbb{R}_+$   
 shows  
 $a \cdot c < b \cdot c$   
 $c \cdot a < c \cdot b$   
 $a \cdot c^{-1} < b \cdot c^{-1}$   
*<proof>*

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:  $a \in \mathbb{R}$   $b \in \mathbb{R}_+$  and A2:  $a \cdot b \leq c$   
 shows  $a \leq c \cdot b^{-1}$   
*<proof>*

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>*

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>*

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>*

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>

```

Sometimes we can reverse a strict inequality by taking inverse on both sides.

```

lemma (in field1) OrdField_ZF_2_L8:
  assumes A1:  $a \in \mathbb{R}_+$  and A2:  $a^{-1} < b$ 
  shows  $b^{-1} < a$ 
<proof>

```

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  $1 + a \cdot c < b \cdot c$ 
<proof>

```

### 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 `×`.

**definition**

$$\text{IntegerMultiplication} \equiv \\ \{ \langle x, c \rangle \in (\text{int} \times \text{int}) \times \text{int}. \text{fst}(x) \$\times \text{snd}(x) = c \}$$

Definition of natural order on integers as a relation on `int`. In the standard Isabelle/ZF the inequality relation on integers is denoted `≤` 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 ≡ PositiveSet(int,IntegerAddition,IntegerOrder)`

`IntegerAddition` and `IntegerMultiplication` are functions on `int × int`.

**lemma** `Int_ZF_1_L1`: **shows**

`IntegerAddition : int×int → int`

`IntegerMultiplication : int×int → int`

*<proof>*

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≤n` for integers and write `m..n` to denote the integer interval with endpoints in `m` and `n`. `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 ≤ 0`. Unfortunately we cannot use the `|·|` 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 `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 (Z)`

`defines ints_def [simp]: Z ≡ int`

`fixes ia (infixl + 69)`

`defines ia_def [simp]: a+b ≡ IntegerAddition⟨ a,b⟩`

`fixes iminus (- _ 72)`

`defines rminus_def [simp]: -a ≡ GroupInv(Z,IntegerAddition)(a)`

`fixes isub (infixl - 69)`

`defines isub_def [simp]: a-b ≡ a+ (- b)`

`fixes imult (infixl · 70)`

`defines imult_def [simp]: a·b ≡ IntegerMultiplication⟨ a,b⟩`

`fixes setneg (- _ 72)`

`defines setneg_def [simp]: -A ≡ GroupInv(Z,IntegerAddition)(A)`

`fixes izero (0)`

`defines izero_def [simp]: 0 ≡ TheNeutralElement(Z,IntegerAddition)`

`fixes ione (1)`

`defines ione_def [simp]: 1 ≡ TheNeutralElement(Z,IntegerMultiplication)`

`fixes itwo (2)`

`defines itwo_def [simp]: 2 ≡ 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:  $a \in \mathbb{Z}$   $b \in \mathbb{Z}$ 
shows
   $a+b = a \ \$+ \ b$ 
   $a \cdot b = a \ \$\times \ b$ 
 $\langle proof \rangle$ 

```

Integer addition and multiplication are associative.

```

lemma (in int0) Int_ZF_1_L3:
assumes  $x \in \mathbb{Z}$   $y \in \mathbb{Z}$   $z \in \mathbb{Z}$ 
shows  $x+y+z = x+(y+z)$   $x \cdot y \cdot z = x \cdot (y \cdot z)$ 
 $\langle proof \rangle$ 

```

Integer addition and multiplication are commutative.

```

lemma (in int0) Int_ZF_1_L4:
assumes  $x \in \mathbb{Z}$   $y \in \mathbb{Z}$ 
shows  $x+y = y+x$   $x \cdot y = y \cdot x$ 
 $\langle proof \rangle$ 

```

Zero is neutral for addition and one for multiplication.

**lemma** (in int0) Int\_ZF\_1\_L5: **assumes** A1:  $x \in \mathbb{Z}$   
**shows**  $(\# 0) + x = x \wedge x + (\# 0) = x$   
 $(\# 1) \cdot x = x \wedge x \cdot (\# 1) = x$   
*<proof>*

Zero is neutral for addition and one for multiplication.

**lemma** (in int0) Int\_ZF\_1\_L6: **shows**  $(\# 0) \in \mathbb{Z} \wedge$   
 $(\forall x \in \mathbb{Z}. (\# 0) + x = x \wedge x + (\# 0) = x)$   
 $(\# 1) \in \mathbb{Z} \wedge$   
 $(\forall x \in \mathbb{Z}. (\# 1) \cdot x = x \wedge x \cdot (\# 1) = x)$   
*<proof>*

Integers with addition and integers with multiplication form monoids.

**theorem** (in int0) Int\_ZF\_1\_T1: **shows**  
 $\text{IsAmonoid}(\mathbb{Z}, \text{IntegerAddition})$   
 $\text{IsAmonoid}(\mathbb{Z}, \text{IntegerMultiplication})$   
*<proof>*

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**  $(\# 0) = \mathbf{0} \quad (\# 1) = \mathbf{1}$   
*<proof>*

0 and 1, as defined in int0 context, are integers.

**lemma** (in int0) Int\_ZF\_1\_L8A: **shows**  $\mathbf{0} \in \mathbb{Z} \quad \mathbf{1} \in \mathbb{Z}$   
*<proof>*

Zero is not one.

**lemma** (in int0) int\_zero\_not\_one: **shows**  $\mathbf{0} \neq \mathbf{1}$   
*<proof>*

The set of integers is not empty, of course.

**lemma** (in int0) int\_not\_empty: **shows**  $\mathbb{Z} \neq \emptyset$   
*<proof>*

The set of integers has more than just zero in it.

**lemma** (in int0) int\_not\_trivial: **shows**  $\mathbb{Z} \neq \{\mathbf{0}\}$   
*<proof>*

Each integer has an inverse (in the addition sense).

**lemma** (in int0) Int\_ZF\_1\_L9: **assumes** A1:  $g \in \mathbb{Z}$   
**shows**  $\exists b \in \mathbb{Z}. g + b = \mathbf{0}$   
*<proof>*

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)  
 ⟨proof⟩

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⟩

Subtracting integers corresponds to adding the negative.

**lemma** (in int0) Int\_ZF\_1\_L10: **assumes** A1:  $m \in \mathbb{Z}$   $n \in \mathbb{Z}$   
**shows**  $m - n = m + -n$   
 ⟨proof⟩

Negative of zero is zero.

**lemma** (in int0) Int\_ZF\_1\_L11: **shows**  $(-0) = 0$   
 ⟨proof⟩

A trivial calculation lemma that allows to subtract and add one.

**lemma** Int\_ZF\_1\_L12:  
**assumes**  $m \in \text{int}$  **shows**  $m - \#1 + \#1 = m$   
 ⟨proof⟩

A trivial calculation lemma that allows to subtract and add one, version with ZF-operation.

**lemma** (in int0) Int\_ZF\_1\_L13: **assumes**  $m \in \mathbb{Z}$   
**shows**  $(m - \#1) + 1 = m$   
 ⟨proof⟩

Adding or subtracting one changes integers.

**lemma** (in int0) Int\_ZF\_1\_L14: **assumes** A1:  $m \in \mathbb{Z}$   
**shows**  
 $m + 1 \neq m$   
 $m - 1 \neq m$   
 ⟨proof⟩

If the difference is zero, the integers are equal.

**lemma** (in int0) Int\_ZF\_1\_L15:  
**assumes** A1:  $m \in \mathbb{Z}$   $n \in \mathbb{Z}$  **and** A2:  $m - n = 0$   
**shows**  $m = n$   
 ⟨proof⟩

## 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>
```

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>
```

Integer order is a relation on integers.

```
lemma Int_ZF_2_L1B: shows IntegerOrder  $\subseteq$  int $\times$ int  
<proof>
```

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>
```

The order on integers is reflexive.

```
lemma (in int0) int_ord_is_refl: shows refl( $\mathbb{Z}$ ,IntegerOrder)  
<proof>
```

The essential condition to show antisymmetry of the order on integers.

```
lemma (in int0) Int_ZF_2_L3:  
  assumes A1:  $m \leq n$   $n \leq m$   
  shows  $m=n$   
<proof>
```

The order on integers is antisymmetric.

```
lemma (in int0) Int_ZF_2_L4: shows antisym(IntegerOrder)  
<proof>
```

The essential condition to show that the order on integers is transitive.

```
lemma Int_ZF_2_L5:  
  assumes A1:  $\langle m,n \rangle \in$  IntegerOrder  $\langle n,k \rangle \in$  IntegerOrder  
  shows  $\langle m,k \rangle \in$  IntegerOrder  
<proof>
```

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:  $m \leq n$   $n \leq k$ 
```

**shows**  $m \leq k$   
*<proof>*

The order on integers is transitive.

**lemma** Int\_ZF\_2\_L6: **shows** trans(IntegerOrder)  
*<proof>*

The order on integers is a partial order.

**lemma** Int\_ZF\_2\_L7: **shows** IsPartOrder(int,IntegerOrder)  
*<proof>*

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**  $m+k \leq n+k$      $k+m \leq k+n$   
*<proof>*

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>*

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**  $i \ll m$   
*<proof>*

This shows how Isabelle's  $\ll$  operator translates to IsarMathLib notation.

**lemma** (in int0) Int\_ZF\_2\_L9AA: **assumes** A1:  $m \in \mathbb{Z}$      $n \in \mathbb{Z}$   
  **and** A2:  $m \ll n$   
  **shows**  $m \leq n$      $m \neq n$   
*<proof>*

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:  $m \leq k$   $\ll$  ( $\#$  1)  
  **shows**  $m+1 \leq k$   
*<proof>*

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**  $i+m \leq k \iff i \leq k-m$   
*<proof>*

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**  $i \leq k+m$   
*<proof>*

Taking (higher order) minus on both sides of inequality reverses it.

**lemma** (in int0) Int\_ZF\_2\_L10: **assumes**  $k \leq i$   
**shows**  
 $(-i) \leq (-k)$   
 $\$-i \leq \$-k$   
*<proof>*

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**  $n \leq (-m)$   
*<proof>*

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**  $k \leq n$   
*<proof>*

If an integer is nonpositive, then its opposite is nonnegative.

**lemma** (in int0) Int\_ZF\_2\_L10A: **assumes**  $k \leq 0$   
**shows**  $0 \leq (-k)$   
*<proof>*

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**  $k \leq 0$   
*<proof>*

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>*

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>*

Adding one increases integers.

**lemma** (in int0) Int\_ZF\_2\_L12A: **assumes** A1:  $j \leq k$   
**shows**  $j \leq k + 1$   $j \leq k + 1$   
*<proof>*

Adding one increases integers, yet one more version.

**lemma** (in int0) Int\_ZF\_2\_L12B: **assumes** A1:  $m \in \mathbb{Z}$  **shows**  $m \leq m + 1$   
*<proof>*

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:  $k \in \mathbb{Z}$   $m \in \mathbb{Z}$  **and** A2:  $n \in \text{nat}$   
**and** A3:  $k + (n + 1) = m + n + \text{succ}(n)$   
**shows**  $m \leq k$   
*<proof>*

The absolute value of an integer is an integer.

**lemma** (in int0) Int\_ZF\_2\_L14: **assumes** A1:  $m \in \mathbb{Z}$   
**shows**  $\text{abs}(m) \in \mathbb{Z}$   
*<proof>*

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**  
 $(-m) \leq n$   
 $0 \leq m + n$   
*<proof>*

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>*

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**  
 $a + c \leq b + d$   
 $a - d \leq b - c$   
*<proof>*

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>*

If we increase the second component in a sum of three integers, the whole sum increases.

**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>*

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  $m \leq n+m$   
 *<proof>*

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  
  $m+n \leq \text{abs}(m)+\text{abs}(n)$   
  $m-n \leq \text{abs}(m)+\text{abs}(n)$   
  $(-m)+n \leq \text{abs}(m)+\text{abs}(n)$   
  $(-m)-n \leq \text{abs}(m)+\text{abs}(n)$   
 *<proof>*

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  $m \leq k+n$   $m \leq n+k$   
 *<proof>*

Triangle inequality for integers.

**lemma** (in int0) Int\_triangle\_ineq:  
 assumes  $m \in \mathbb{Z}$   $n \in \mathbb{Z}$   
 shows  $\text{abs}(m+n) \leq \text{abs}(m)+\text{abs}(n)$   
 *<proof>*

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  $\text{abs}(m) = m$   
 *<proof>*

$0 \leq 1$ , so  $|1| = 1$ .

**lemma** (in int0) Int\_ZF\_2\_L16A: shows  $0 \leq 1$  and  $\text{abs}(1) = 1$

*<proof>*

$1 \leq 2$ .

**lemma** (in int0) Int\_ZF\_2\_L16B: shows  $1 \leq 2$

*<proof>*

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>*

Absolute value is the same for an integer and its opposite.

**lemma** (in int0) Int\_ZF\_2\_L17:

assumes  $m \in \mathbb{Z}$  shows  $\text{abs}(-m) = \text{abs}(m)$

*<proof>*

The absolute value of zero is zero.

**lemma** (in int0) Int\_ZF\_2\_L18: shows  $\text{abs}(0) = 0$

*<proof>*

A different version of the triangle inequality.

**lemma** (in int0) Int\_triangle\_ineq1:

assumes A1:  $m \in \mathbb{Z}$   $n \in \mathbb{Z}$

shows

$\text{abs}(m-n) \leq \text{abs}(n)+\text{abs}(m)$

$\text{abs}(m-n) \leq \text{abs}(m)+\text{abs}(n)$

*<proof>*

Another version of the triangle inequality.

**lemma** (in int0) Int\_triangle\_ineq2:

assumes  $m \in \mathbb{Z}$   $n \in \mathbb{Z}$

and  $\text{abs}(m-n) \leq k$

shows

$\text{abs}(m) \leq \text{abs}(n)+k$

$m-k \leq n$

$m \leq n+k$

$n-k \leq m$

*<proof>*

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>*

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**  $m \leq n$   $(-n) \leq (-m)$   $m \neq n$   
*<proof>*

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>*

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>*

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>*

An integer is not greater than its absolute value.

**lemma** (in int0) Int\_ZF\_2\_L19C: **assumes** A1:  $m \in \mathbb{Z}$   
**shows**  
 $m \leq \text{abs}(m)$   
 $(-m) \leq \text{abs}(m)$   
*<proof>*

$$|m - n| = |n - m|.$$

**lemma** (in int0) Int\_ZF\_2\_L20: **assumes**  $m \in \mathbb{Z}$   $n \in \mathbb{Z}$   
**shows**  $\text{abs}(m-n) = \text{abs}(n-m)$   
*<proof>*

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:  $\text{abs}(m) \leq k$   $\text{abs}(n) \leq 1$   
**shows**

```

abs(m+n) ≤ k + 1
abs(m-n) ≤ k + 1
⟨proof⟩

```

Absolute value is nonnegative.

```

lemma (in int0) int_abs_nonneg: assumes A1: m ∈ ℤ
  shows abs(m) ∈ ℤ+ 0 ≤ abs(m)
⟨proof⟩

```

If a 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
⟨proof⟩

```

### 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⟩

```

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⟩

```

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⟩

```

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⟩

```

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>*

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>*

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>*

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>*

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>*

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>*

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>*

### 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 is 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>*

A trivial calculation lemma that allows to subtract and add one.

**lemma** `Int_ZF_4_L1A`:  
**assumes**  $m \in \text{int}$  **shows**  $m \ \$- \ \$\#1 \ \$+ \ \$\#1 = m$   
*<proof>*

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>*

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>*

Extending an integer interval by one is the same as adding the new endpoint.

**lemma** (in `int0`) `Int_ZF_4_L3`: **assumes**  $A1: m \leq k$   
**shows**  $m..(k \ \$+ \ \$\#1) = m..k \ \cup \ \{k \ \$+ \ \$\#1\}$   
*<proof>*

Integer intervals are finite - induction step.

**lemma** (in `int0`) `Int_ZF_4_L4`:  
**assumes**  $A1: i \leq m$  **and**  $A2: i..m \in \text{Fin}(\mathbb{Z})$   
**shows**  $i..(m \ \$+ \ \$\#1) \in \text{Fin}(\mathbb{Z})$   
*<proof>*

Integer intervals are finite.

**lemma** (in `int0`) `Int_ZF_4_L5`: **assumes**  $A1: i \in \mathbb{Z} \ k \in \mathbb{Z}$   
**shows**  $i..k \in \text{Fin}(\mathbb{Z})$   
*<proof>*

Bounded integer sets are finite.

**lemma** (in int0) Int\_ZF\_4\_L6: **assumes** A1: IsBounded(A,IntegerOrder)  
**shows** A ∈ Fin( $\mathbb{Z}$ )  
*<proof>*

A subset of integers is bounded iff it is finite.

**theorem** (in int0) Int\_bounded\_iff\_fin:  
**shows** IsBounded(A,IntegerOrder)  $\longleftrightarrow$  A ∈ Fin( $\mathbb{Z}$ )  
*<proof>*

The image of an interval by any integer function is finite, hence bounded.

**lemma** (in int0) Int\_ZF\_4\_L8:  
**assumes** A1:  $i \in \mathbb{Z}$   $k \in \mathbb{Z}$  and A2:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$   
**shows**  
 $f(i..k) \in \text{Fin}(\mathbb{Z})$   
IsBounded( $f(i..k)$ ,IntegerOrder)  
*<proof>*

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>*

**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
     $a \cdot (b+c) = a \cdot b + a \cdot c$ 
     $(b+c) \cdot a = b \cdot a + c \cdot a$ 
  <proof>
```

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>
```

Zero and one are integers.

```
lemma (in int0) int_zero_one_are_int: shows  $0 \in \mathbb{Z}$   $1 \in \mathbb{Z}$ 
  <proof>
```

Negative of zero is zero.

```
lemma (in int0) int_zero_one_are_intA: shows  $(-0) = 0$ 
  <proof>
```

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>
```

Properties that require two integers.

**lemma** (in int0) Int\_ZF\_1\_1\_L5: **assumes**  $a \in \mathbb{Z}$   $b \in \mathbb{Z}$   
**shows**  
 $a+b \in \mathbb{Z}$   
 $a-b \in \mathbb{Z}$   
 $a \cdot b \in \mathbb{Z}$   
 $a+b = b+a$   
 $a \cdot b = b \cdot a$   
 $(-b)-a = (-a)-b$   
 $-(a+b) = (-a)-b$   
 $-(a-b) = ((-a)+b)$   
 $(-a) \cdot b = -(a \cdot b)$   
 $a \cdot (-b) = -(a \cdot b)$   
 $(-a) \cdot (-b) = a \cdot b$   
*<proof>*

2 and 3 are integers.

**lemma** (in int0) int\_two\_three\_are\_int: **shows**  $2 \in \mathbb{Z}$   $3 \in \mathbb{Z}$   
*<proof>*

Another property with two integers.

**lemma** (in int0) Int\_ZF\_1\_1\_L5B:  
**assumes**  $a \in \mathbb{Z}$   $b \in \mathbb{Z}$   
**shows**  $a-(-b) = a+b$   
*<proof>*

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**  
 $a-(b+c) = a-b-c$   
 $a-(b-c) = a-b+c$   
 $a \cdot (b-c) = a \cdot b - a \cdot c$   
 $(b-c) \cdot a = b \cdot a - c \cdot a$   
*<proof>*

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**  $a+(b-c) = a+b-c$   
*<proof>*

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**  
 $a+b+c = a+(b+c)$   
 $a \cdot b \cdot c = a \cdot (b \cdot c)$   
*<proof>*

## 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**  $\text{abs}(a)+1 = \text{abs}(a+1)$   
*<proof>*

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**  $a+(\text{abs}(b)+1) \cdot a = (\text{abs}(b+1)+1) \cdot a$   
*<proof>*

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**  
 $a+b-a = b$   
 $a+(b-a) = b$   
 $a+b-b = a$   
 $a-b+b = a$   
 $(-a)+(a+b) = b$   
 $a+(b-a) = b$   
 $(-b)+(a+b) = a$   
 $a-(b+a) = -b$   
 $a-(a+b) = -b$   
 $a-(a-b) = b$   
 $a-b-a = -b$   
 $a-b - (a+b) = (-b)-b$   
*<proof>*

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:  $a \leq b$   
**shows**  $a-1 \leq b$   
*<proof>*

Subtracting one does not increase integers, special case.

**lemma** (in int0) Int\_ZF\_1\_2\_L3AA:  
**assumes** A1:  $a \in \mathbb{Z}$  **shows**  
 $a-1 \leq a$   
 $a-1 \neq a$   
 $\neg(a \leq a-1)$   
 $\neg(a+1 \leq a)$   
 $\neg(1+a \leq a)$   
*<proof>*

A formula with a nonpositive integer.

**lemma** (in int0) Int\_ZF\_1\_2\_L4: **assumes**  $a \leq 0$   
**shows**  $\text{abs}(a)+1 = \text{abs}(a-1)$   
*<proof>*

A formula with two integers, one negative.

**lemma** (in int0) Int\_ZF\_1\_2\_L5: **assumes** A1:  $a \in \mathbb{Z}$  and A2:  $b \leq 0$   
**shows**  $a+(\text{abs}(b)+1) \cdot a = (\text{abs}(b-1)+1) \cdot a$   
*<proof>*

A rearrangement with four integers.

**lemma** (in int0) Int\_ZF\_1\_2\_L6:  
**assumes** A1:  $a \in \mathbb{Z}$   $b \in \mathbb{Z}$   $c \in \mathbb{Z}$   $d \in \mathbb{Z}$   
**shows**  
 $a-(b-1) \cdot c = (d-b \cdot c)-(d-a-c)$   
*<proof>*

Some other rearrangements with two integers.

**lemma** (in int0) Int\_ZF\_1\_2\_L7: **assumes**  $a \in \mathbb{Z}$   $b \in \mathbb{Z}$   
**shows**  
 $a \cdot b = (a-1) \cdot b + b$   
 $a \cdot (b+1) = a \cdot b + a$   
 $(b+1) \cdot a = b \cdot a + a$   
 $(b+1) \cdot a = a + b \cdot a$   
*<proof>*

Another rearrangement with two integers.

**lemma** (in int0) Int\_ZF\_1\_2\_L8:  
**assumes** A1:  $a \in \mathbb{Z}$   $b \in \mathbb{Z}$   
**shows**  $a+1+(b+1) = b+a+2$   
*<proof>*

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**  
 $(a-b)+(b-c) = a-c$   
 $(a-b)-(a-c) = c-b$   
 $a+(b+(c-a-b)) = c$   
 $(-a)-b+c = c-a-b$   
 $(-b)-a+c = c-a-b$   
 $(-((-a)+b+c)) = a-b-c$   
 $a+b+c-a = b+c$   
 $a+b-(a+c) = b-c$   
*<proof>*

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>*

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>*

A technical rearrangement involving inequalities with absolute value.

**lemma** (in int0) Int\_ZF\_1\_2\_L10A:  
**assumes** A1:  $a \in \mathbb{Z}$   $b \in \mathbb{Z}$   $c \in \mathbb{Z}$   $e \in \mathbb{Z}$   
**and** A2:  $\text{abs}(a \cdot b - c) \leq d$   $\text{abs}(b \cdot a - e) \leq f$   
**shows**  $\text{abs}(c - e) \leq f + d$   
*<proof>*

Some arithmetics.

**lemma** (in int0) Int\_ZF\_1\_2\_L11: **assumes** A1:  $a \in \mathbb{Z}$   
**shows**  
 $a+1+2 = a+3$   
 $a = 2 \cdot a - a$   
*<proof>*

A simple rearrangement with three integers.

**lemma** (in int0) Int\_ZF\_1\_2\_L12:  
**assumes**  $a \in \mathbb{Z}$   $b \in \mathbb{Z}$   $c \in \mathbb{Z}$   
**shows**  
 $(b-c) \cdot a = a \cdot b - a \cdot c$   
*<proof>*

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**  $(x+(a \cdot x+b)+c) \cdot d = d \cdot (a+1) \cdot x + (b \cdot d+c \cdot d)$   
*<proof>*

Rearrangement 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**  $(a \cdot x + b) + (c \cdot x + d) = (a+c) \cdot x + (b+d)$   
*<proof>*

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>

```

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
<proof>

```

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>

```

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>

```

### 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≤a 0≤b
  and A3: 0 ≤ a·b
  shows 0 ≤ a·(b+1)
<proof>

```

Product of nonnegative integers is nonnegative.

```

lemma (in int0) Int_ZF_1_3_L2: assumes A1: 0≤a 0≤b
  shows 0≤a·b
<proof>

```

The set of nonnegative integers is closed under multiplication.

```

lemma (in int0) Int_ZF_1_3_L2A: shows
  ℤ+ {is closed under} IntegerMultiplication

```

*<proof>*

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)`  
*<proof>*

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>*

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>*

$|a \cdot (-b)| = |(-a) \cdot b| = |(-a) \cdot (-b)| = |a \cdot b|$  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**  
   `$\text{abs}((-a) \cdot b) = \text{abs}(a \cdot b)$`   
   `$\text{abs}(a \cdot (-b)) = \text{abs}(a \cdot b)$`   
   `$\text{abs}((-a) \cdot (-b)) = \text{abs}(a \cdot b)$`   
*<proof>*

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**  `$\text{abs}(a \cdot b) = \text{abs}(a) \cdot \text{abs}(b)$`   
*<proof>*

Double nonnegative is nonnegative. Property of ordered rings.

**lemma** (in `int0`) `Int_ZF_1_3_L5A`: **assumes**  `$0 \leq a$`   
  **shows**  `$0 \leq 2 \cdot a$`   
*<proof>*

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>*

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**  $b \leq a \vee a+1 \leq b$   
*<proof>*

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>*

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>*

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:  $a \in \mathbb{Z}$   $b \in \mathbb{Z}$   
**shows**  $a=b \vee (a \leq b-1) \vee (b+1 \leq a)$   
*<proof>*

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>*

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**  $\neg(a \leq 0) \longleftrightarrow 1 \leq a$   
*<proof>*

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**  $\neg((a \cdot b) \leq 0)$   
*<proof>*

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>*

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**  $a \leq b \iff a - b \leq 0$   
*<proof>*

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**  $0 \leq b - a$   
*<proof>*

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>*

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>*

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**  $a \cdot b \leq 0$   
*<proof>*

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**  
 $a \cdot c \leq b \cdot c$   
 $c \cdot a \leq c \cdot b$

*<proof>*

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>*

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>*

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>*

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>*

Negative of a nonnegative is nonpositive.

**lemma** (in int0) Int\_ZF\_1\_3\_L16: assumes A1:  $0 \leq m$   
 shows  $(-m) \leq 0$

*<proof>*

Some statements about intervals centered at 0.

**lemma** (in int0) Int\_ZF\_1\_3\_L17: assumes A1:  $m \in \mathbb{Z}$   
 shows  
  $(-\text{abs}(m)) \leq \text{abs}(m)$   
  $(-\text{abs}(m)) \dots \text{abs}(m) \neq 0$

*<proof>*

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 ≤ GreaterOf(IntegerOrder,m,n)
SmallerOf(IntegerOrder,m,n) ≤ m
SmallerOf(IntegerOrder,m,n) ≤ n
⟨proof⟩

```

If  $|m| \leq n$ , then  $m \in -n..n$ .

```

lemma (in int0) Int_ZF_1_3_L19:
  assumes A1: m∈ℤ and A2: abs(m) ≤ n
  shows
    (-n) ≤ m m ≤ n
    m ∈ (-n)..n
    0 ≤ n
⟨proof⟩

```

A slight generalization of the above lemma.

```

lemma (in int0) Int_ZF_1_3_L19A:
  assumes A1: m∈ℤ and A2: abs(m) ≤ n and A3: 0≤k
  shows -(n+k) ≤ m
⟨proof⟩

```

Sets of integers that have absolute value bounded are bounded.

```

lemma (in int0) Int_ZF_1_3_L20:
  assumes A1: ∀x∈X. b(x) ∈ ℤ ∧ abs(b(x)) ≤ L
  shows IsBounded({b(x). x∈X},IntegerOrder)
⟨proof⟩

```

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 IsBounded(A,IntegerOrder)
  shows ∃L. ∀a∈A. abs(a) ≤ L
⟨proof⟩

```

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∈ℤ} ∈ Fin(ℤ)
  shows ∃L∈ℤ. ∀x∈ℤ. abs(b(x)) ≤ L
⟨proof⟩

```

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⟩

```

A special case of the previous lemma for a function from integers to integers.

**corollary** (in int0) Int\_ZF\_1\_3\_L20C:  
 assumes  $f:\mathbb{Z}\rightarrow\mathbb{Z}$  and  $\forall m\in\mathbb{Z}. \text{abs}(f(m)) \leq L$   
 shows  $f(\mathbb{Z}) \in \text{Fin}(\mathbb{Z})$   
*<proof>*

A triangle inequality with three integers. Property of linearly ordered abelian groups.

**lemma** (in int0) int\_triangle\_ineq3:  
 assumes A1:  $a\in\mathbb{Z}$   $b\in\mathbb{Z}$   $c\in\mathbb{Z}$   
 shows  $\text{abs}(a-b-c) \leq \text{abs}(a) + \text{abs}(b) + \text{abs}(c)$   
*<proof>*

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:  $a\leq c$   $b\leq c$  shows  $a+b \leq 2\cdot c$   
*<proof>*

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  $a\leq b$  and  $c\in\mathbb{Z}$  and  $b\leq c+a$   
 shows  $\text{abs}(b-a) \leq c$   
*<proof>*

An application of the triangle inequality with four integers. Property of linearly ordered abelian groups.

**lemma** (in int0) Int\_ZF\_1\_3\_L22A:  
 assumes  $a\in\mathbb{Z}$   $b\in\mathbb{Z}$   $c\in\mathbb{Z}$   $d\in\mathbb{Z}$   
 shows  $\text{abs}(a-c) \leq \text{abs}(a+b) + \text{abs}(c+d) + \text{abs}(b-d)$   
*<proof>*

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:  $a\leq b$  and A2:  $c\in\mathbb{Z}$  and A3:  $b\leq a+c$   
 shows  $\text{abs}(b-a) \leq c$   
*<proof>*

### 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:  $A \in \text{Fin}(\mathbb{Z})$  and A2:  $A\neq 0$   
 shows

HasAmaximum(IntegerOrder,A)  
 HasAminimum(IntegerOrder,A)  
 Maximum(IntegerOrder,A)  $\in$  A  
 Minimum(IntegerOrder,A)  $\in$  A  
 $\forall x \in A. x \leq$  Maximum(IntegerOrder,A)  
 $\forall x \in A. \text{Minimum(IntegerOrder,A)} \leq x$   
 Maximum(IntegerOrder,A)  $\in \mathbb{Z}$   
 Minimum(IntegerOrder,A)  $\in \mathbb{Z}$   
*<proof>*

Bounded nonempty integer subsets attain maximum and minimum.

**theorem** (in int0) Int\_bounded\_have\_max\_min:  
 assumes IsBounded(A,IntegerOrder) and  $A \neq 0$   
 shows  
 HasAmaximum(IntegerOrder,A)  
 HasAminimum(IntegerOrder,A)  
 Maximum(IntegerOrder,A)  $\in$  A  
 Minimum(IntegerOrder,A)  $\in$  A  
 $\forall x \in A. x \leq$  Maximum(IntegerOrder,A)  
 $\forall x \in A. \text{Minimum(IntegerOrder,A)} \leq x$   
 Maximum(IntegerOrder,A)  $\in \mathbb{Z}$   
 Minimum(IntegerOrder,A)  $\in \mathbb{Z}$   
*<proof>*

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:  $A \neq 0$   
 shows  
 HasAminimum(IntegerOrder,A)  
 Minimum(IntegerOrder,A)  $\in$  A  
  
 $\forall x \in A. \text{Minimum(IntegerOrder,A)} \leq x$   
*<proof>*

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)  $\in \mathbb{Z}$   
 $\forall x \in A. x \leq$  Maximum(IntegerOrder,A)  
*<proof>*

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:  $A \neq 0$

```

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>

```

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})  $\in \mathbb{Z}$ 
 $a \leq \text{Maximum(IntegerOrder,{a,b,c})}$ 
 $b \leq \text{Maximum(IntegerOrder,{a,b,c})}$ 
 $c \leq \text{Maximum(IntegerOrder,{a,b,c})}$ 
<proof>

```

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
maxf(f,a..b)  $\in \mathbb{Z}$ 
 $\forall c \in a..b. f(c) \leq \text{maxf(f,a..b)}$ 
 $\exists c \in a..b. f(c) = \text{maxf(f,a..b)}$ 
minf(f,a..b)  $\in \mathbb{Z}$ 
 $\forall c \in a..b. \text{minf(f,a..b)} \leq f(c)$ 
 $\exists c \in a..b. f(c) = \text{minf(f,a..b)}$ 
<proof>

```

### 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
<proof>

```

Text expanded 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**  $a+b \in \mathbb{Z}_+$   
*<proof>*

$\mathbb{Z}^+$  is bounded below.

**lemma** (in int0) Int\_ZF\_1\_5\_L1: **shows**  
 IsBoundedBelow( $\mathbb{Z}^+$ , IntegerOrder)  
 IsBoundedBelow( $\mathbb{Z}_+$ , IntegerOrder)  
*<proof>*

Subsets of  $\mathbb{Z}^+$  are bounded below.

**lemma** (in int0) Int\_ZF\_1\_5\_L1A: **assumes**  $A \subseteq \mathbb{Z}^+$   
**shows** IsBoundedBelow( $A$ , IntegerOrder)  
*<proof>*

Subsets of  $\mathbb{Z}_+$  are bounded below.

**lemma** (in int0) Int\_ZF\_1\_5\_L1B: **assumes**  $A_1: A \subseteq \mathbb{Z}_+$   
**shows** IsBoundedBelow( $A$ , IntegerOrder)  
*<proof>*

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,  $A$ )  $\in A$   
 $\forall x \in A. \text{Minimum(IntegerOrder, } A) \leq x$   
*<proof>*

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**  $A_1: A \subseteq \mathbb{Z}^+$  **and**  $A_2: A \notin \text{Fin}(\mathbb{Z})$  **and**  $A_3: D \in \mathbb{Z}$   
**shows**  $\exists n \in A. D \leq n$   
*<proof>*

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**  $A_1: A \subseteq \mathbb{Z}_+$  **and**  $A_2: A \notin \text{Fin}(\mathbb{Z})$  **and**  $A_3: D \in \mathbb{Z}$   
**shows**  $\exists n \in A. D \leq n$   
*<proof>*

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 ( $m=0, m \in \mathbb{Z}_+, (-m) \in \mathbb{Z}_+$ )  
*<proof>*

An integer is zero, positive, or it's inverse is positive.

**lemma** (in int0) int\_decomp\_cases: **assumes**  $m \in \mathbb{Z}$   
**shows**  $m=0 \vee m \in \mathbb{Z}_+ \vee (-m) \in \mathbb{Z}_+$   
*<proof>*

An integer is in the positive set iff it is greater or equal one.

**lemma** (in int0) Int\_ZF\_1\_5\_L3: **shows**  $m \in \mathbb{Z}_+ \iff 1 \leq m$   
*<proof>*

The set of positive integers is closed under multiplication. The unfolded form.

**lemma** (in int0) pos\_int\_closed\_mul\_unfold:  
**assumes**  $a \in \mathbb{Z}_+ \quad b \in \mathbb{Z}_+$   
**shows**  $a \cdot b \in \mathbb{Z}_+$   
*<proof>*

The set of positive integers is closed under multiplication.

**lemma** (in int0) pos\_int\_closed\_mul: **shows**  
 $\mathbb{Z}_+$  {is closed under} IntegerMultiplication  
*<proof>*

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( $\mathbb{Z}$ , IntegerAddition, IntegerMultiplication)  
*<proof>*

Nonnegative integers are positive ones plus zero.

**lemma** (in int0) Int\_ZF\_1\_5\_L3A: **shows**  $\mathbb{Z}^+ = \mathbb{Z}_+ \cup \{0\}$   
*<proof>*

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:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  and A2:  $K \in \mathbb{Z} \quad N \in \mathbb{Z}$   
**shows**  $\exists C \in \mathbb{Z}. \forall n \in \mathbb{Z}_+. K \leq f(n) + C \implies N \leq n$   
*<proof>*

Absolute value is identity on positive integers.

**lemma** (in int0) Int\_ZF\_1\_5\_L4A:  
**assumes**  $a \in \mathbb{Z}_+$  **shows**  $\text{abs}(a) = a$   
*<proof>*

One and two are in  $\mathbb{Z}_+$ .

**lemma** (in int0) int\_one\_two\_are\_pos: **shows**  $1 \in \mathbb{Z}_+ \quad 2 \in \mathbb{Z}_+$   
*<proof>*

The image of  $\mathbb{Z}_+$  by a function defined on integers is not empty.

**lemma** (in int0) Int\_ZF\_1\_5\_L5: **assumes** A1:  $f : \mathbb{Z} \rightarrow X$   
**shows**  $f(\mathbb{Z}_+) \neq 0$   
*<proof>*

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>*

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>*

Adding a positive integer increases integers.

**lemma** (in int0) Int\_ZF\_1\_5\_L7A: **assumes**  $a \in \mathbb{Z}$   $b \in \mathbb{Z}_+$   
**shows**  $a \leq a+b$   $a \neq a+b$   $a+b \in \mathbb{Z}$   
*<proof>*

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**  
 $a \leq \text{GreaterOf}(\text{IntegerOrder}, 1, a)$   
 $\text{GreaterOf}(\text{IntegerOrder}, 1, a) \in \mathbb{Z}_+$   
 $\text{GreaterOf}(\text{IntegerOrder}, 1, a) + 1 \in \mathbb{Z}_+$   
 $a \leq \text{GreaterOf}(\text{IntegerOrder}, 1, a) + 1$   
 $a \neq \text{GreaterOf}(\text{IntegerOrder}, 1, a) + 1$   
*<proof>*

The opposite of an element of  $\mathbb{Z}_+$  cannot belong to  $\mathbb{Z}_+$ .

**lemma** (in int0) Int\_ZF\_1\_5\_L8: **assumes**  $a \in \mathbb{Z}_+$   
**shows**  $(-a) \notin \mathbb{Z}_+$   
*<proof>*

For every integer there is one in  $\mathbb{Z}_+$  that is greater or equal.

**lemma** (in int0) Int\_ZF\_1\_5\_L9: **assumes**  $a \in \mathbb{Z}$   
**shows**  $\exists b \in \mathbb{Z}_+. a \leq b$   
*<proof>*

A theorem about odd extensions. Recall from `OrderedGroup_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 :  $\mathbb{Z}_+ \rightarrow \mathbb{Z}$ 
  shows OddExtension( $\mathbb{Z}$ , IntegerAddition, IntegerOrder, f) :  $\mathbb{Z} \rightarrow \mathbb{Z}$ 
  <proof>
```

On  $\mathbb{Z}_+$ , the odd extension of  $f$  is the same as  $f$ .

```
lemma (in int0) Int_ZF_1_5_L11: assumes f :  $\mathbb{Z}_+ \rightarrow \mathbb{Z}$  and a  $\in \mathbb{Z}_+$  and
  g = OddExtension( $\mathbb{Z}$ , IntegerAddition, IntegerOrder, f)
  shows g(a) = f(a)
  <proof>
```

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 :  $\mathbb{Z}_+ \rightarrow \mathbb{Z}$  and a  $\in (-\mathbb{Z}_+)$  and
  g = OddExtension( $\mathbb{Z}$ , IntegerAddition, IntegerOrder, f)
  shows g(a) = -(f(-a))
  <proof>
```

Odd extensions are odd on  $\mathbb{Z}$ .

```
lemma (in int0) int_oddext_is_odd:
  assumes f :  $\mathbb{Z}_+ \rightarrow \mathbb{Z}$  and a  $\in \mathbb{Z}$  and
  g = OddExtension( $\mathbb{Z}$ , IntegerAddition, IntegerOrder, f)
  shows g(-a) = -(g(a))
  <proof>
```

Alternative definition of an odd function.

```
lemma (in int0) Int_ZF_1_5_L13: assumes A1: f :  $\mathbb{Z} \rightarrow \mathbb{Z}$  shows
  ( $\forall a \in \mathbb{Z}. f(-a) = -(f(a))$ )  $\longleftrightarrow$  ( $\forall a \in \mathbb{Z}. -(f(-a)) = f(a)$ )
  <proof>
```

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 = OddExtension( $\mathbb{Z}$ , IntegerAddition, IntegerOrder, f)
  shows (-g(-a)) = g(a)
  <proof>
```

## 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**  
**IsBoundedAbove**( $f(A)$ , IntegerOrder)  
**shows** **IsBoundedAbove**( $A$ , IntegerOrder)  
*<proof>*

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>*

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**  $\exists l. \forall x \in X. l \leq b(x)$   
*<proof>*

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>*

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:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  **and** A2:  $N \in \mathbb{Z}$  **and**  
A3:  $\forall m. N \leq m \longrightarrow L \leq f(m)$  **and**  
A4:  $\text{IsBoundedBelow}(A, \text{IntegerOrder})$   
**shows**  $\text{IsBoundedBelow}(f(A), \text{IntegerOrder})$   
*<proof>*

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>*

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>*

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>*

### 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:  $A \in \mathbb{Z} \quad B \in \mathbb{Z}$   
**shows**  $\exists L. \forall p \in \mathbb{Z}. F(p) \leq L$   
*<proof>*

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**  $a \in \mathbb{Z} \quad b \in \mathbb{Z}$   
**shows**  
 $0 \leq a \wedge 0 \leq b \vee a \leq 0 \wedge b \leq 0 \vee$   
 $a \leq 0 \wedge 0 \leq b \wedge 0 \leq a+b \vee a \leq 0 \wedge 0 \leq b \wedge a+b \leq 0 \vee$   
 $0 \leq a \wedge b \leq 0 \wedge 0 \leq a+b \vee 0 \leq a \wedge b \leq 0 \wedge a+b \leq 0$   
*<proof>*

**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∈ℤ n∈ℤ
  shows m = n·(m zdiv n) + (m zmod n)
  <proof>
```

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∈ℤ and A2: 0≤n n≠0
  shows
    0 ≤ m zmod n
    m zmod n ≤ n    m zmod n ≠ n
    m zmod n ≤ n-1
  <proof>
```

$(m \cdot k) \text{ div } k = m$ .

```
lemma (in int0) IntDiv_ZF_1_L3:
  assumes m∈ℤ k∈ℤ and k≠0
  shows
    (m·k) zdiv k = m
    (k·m) zdiv k = m
  <proof>
```

The next lemma essentially translates `zdiv_mono1` from standard Isabelle to our notation.

```
lemma (in int0) IntDiv_ZF_1_L4:
  assumes A1: m ≤ k and A2: 0≤n n≠0
  shows m zdiv n ≤ k zdiv n
  <proof>
```

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>*

**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 "o" symbol denotes the second operation on almost homomorphisms (see `Group_ZF_3` for definition), defined for the group of integers. In short "o" is the composition of slopes. The " $^{-1}$ " symbol acts as an infix operator that assigns the value  $\min\{n \in Z_+ : p \leq f(n)\}$  to a pair (of sets)  $f$  and  $p$ . In application  $f$  represents a function defined on  $Z_+$  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)
  <proof>

```

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
   $m+n \in \mathbb{Z}$ 
   $f(m+n) \in \mathbb{Z}$ 
   $f(m) \in \mathbb{Z}$   $f(n) \in \mathbb{Z}$ 
   $f(m) + f(n) \in \mathbb{Z}$ 
   $\text{HomDiff}(\mathbb{Z}, \text{IntegerAddition}, f, \langle m, n \rangle) \in \mathbb{Z}$ 
  <proof>

```

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
   $m+n \in \mathbb{Z}$ 
   $f(m+n) \in \mathbb{Z}$   $f(m) \in \mathbb{Z}$   $f(n) \in \mathbb{Z}$ 
   $f(m) + f(n) \in \mathbb{Z}$ 
   $\text{HomDiff}(\mathbb{Z}, \text{IntegerAddition}, f, \langle m, n \rangle) \in \mathbb{Z}$ 
  <proof>

```

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>

```

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  $\text{HomDiff}(\mathbb{Z}, \text{IntegerAddition}, f, \langle m, n \rangle) = \delta(f, m, n)$ 
  <proof>

```

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:  $m \in \mathbb{Z}$   $n \in \mathbb{Z}$ 
shows

```

$f(m+n) = f(m) + (f(n) + \delta(f, m, n))$   
*<proof>*

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**  $m \in \mathbb{Z}$   $n \in \mathbb{Z}$   
**shows**  $\delta(f, m, n) \in \mathbb{Z}$   
*<proof>*

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:  $m \in \mathbb{Z}$   $n \in \mathbb{Z}$   
**shows**  $f(m+n) = \delta(f, m, n) + f(n) + f(m)$   
*<proof>*

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**  $\{\text{abs}(\text{HomDiff}(\mathbb{Z}, \text{IntegerAddition}, f, x)). x \in \mathbb{Z} \times \mathbb{Z}\} =$   
 $\{\text{abs}(\delta(f, m, n)). \langle m, n \rangle \in \mathbb{Z} \times \mathbb{Z}\}$   
*<proof>*

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>*

The absolute value of homomorphism difference of a slope  $s$  does not exceed  $\text{max}\delta(s)$ .

**lemma** (in int1) Int\_ZF\_2\_1\_L7:  
**assumes** A1:  $s \in \mathcal{S}$  **and** A2:  $n \in \mathbb{Z}$   $m \in \mathbb{Z}$   
**shows**  
 $\text{abs}(\delta(s, m, n)) \leq \text{max}\delta(s)$   
 $\delta(s, m, n) \in \mathbb{Z}$   $\text{max}\delta(s) \in \mathbb{Z}$   
 $(-\text{max}\delta(s)) \leq \delta(s, m, n)$   
*<proof>*

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**  
 $\text{abs}(s(0)) \leq \text{max}\delta(s)$   
 $0 \leq \text{max}\delta(s)$   
 $\text{abs}(s(0)) \in \mathbb{Z}$   $\text{max}\delta(s) \in \mathbb{Z}$   
 $\text{abs}(s(0)) + \text{max}\delta(s) \in \mathbb{Z}$   
*<proof>*

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**  $A1: s \in \mathcal{S} \quad r \in \mathcal{S}$   
**and**  $A2: \forall m \in \mathbb{Z}. \text{abs}(s(m) - r(m)) \leq L$   
**shows**  $s \sim r$   
 $\langle \text{proof} \rangle$

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**  $s \sim r$   
**shows**  
 $\exists L \in \mathbb{Z}. \forall m \in \mathbb{Z}. \text{abs}(s(m) - r(m)) \leq L$   
 $s \in \mathcal{S} \quad r \in \mathcal{S}$   
 $\langle \text{proof} \rangle$

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**  
 $\text{AlEqRel} \subseteq \mathcal{S} \times \mathcal{S}$   
 $\text{equiv}(\mathcal{S}, \text{AlEqRel})$   
 $\langle \text{proof} \rangle$

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**  $s \in \mathcal{S} \quad r \in \mathcal{S}$  **and**  
 $s + (-r) \in \text{FinRangeFunctions}(\mathbb{Z}, \mathbb{Z})$   
**shows**  
 $s \sim r$   
 $r \sim s$   
 $\langle \text{proof} \rangle$

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**  $A1: s \sim r$   
**shows**  $s + (-r) \in \text{FinRangeFunctions}(\mathbb{Z}, \mathbb{Z})$   
 $\langle \text{proof} \rangle$

What is the value of a composition of slopes?

**lemma** (in int1) Int\_ZF\_2\_1\_L10:  
**assumes**  $s \in \mathcal{S}$   $r \in \mathcal{S}$  **and**  $m \in \mathbb{Z}$   
**shows**  $(s \circ r)(m) = s(r(m))$   $s(r(m)) \in \mathbb{Z}$   
*<proof>*

Composition of slopes is a slope.

**lemma** (in int1) Int\_ZF\_2\_1\_L11:  
**assumes**  $s \in \mathcal{S}$   $r \in \mathcal{S}$   
**shows**  $s \circ r \in \mathcal{S}$   
*<proof>*

Negative of a slope is a slope.

**lemma** (in int1) Int\_ZF\_2\_1\_L12: **assumes**  $s \in \mathcal{S}$  **shows**  $-s \in \mathcal{S}$   
*<proof>*

What is the value of a negative of a slope?

**lemma** (in int1) Int\_ZF\_2\_1\_L12A:  
**assumes**  $s \in \mathcal{S}$  **and**  $m \in \mathbb{Z}$  **shows**  $(-s)(m) = -(s(m))$   
*<proof>*

What are the values of a sum of slopes?

**lemma** (in int1) Int\_ZF\_2\_1\_L12B: **assumes**  $s \in \mathcal{S}$   $r \in \mathcal{S}$  **and**  $m \in \mathbb{Z}$   
**shows**  $(s+r)(m) = s(m) + r(m)$   
*<proof>*

Sum of slopes is a slope.

**lemma** (in int1) Int\_ZF\_2\_1\_L12C: **assumes**  $s \in \mathcal{S}$   $r \in \mathcal{S}$   
**shows**  $s+r \in \mathcal{S}$   
*<proof>*

A simple but useful identity.

**lemma** (in int1) Int\_ZF\_2\_1\_L13:  
**assumes**  $s \in \mathcal{S}$  **and**  $n \in \mathbb{Z}$   $m \in \mathbb{Z}$   
**shows**  $s(n \cdot m) + (s(m) + \delta(s, n \cdot m, m)) = s((n+1) \cdot m)$   
*<proof>*

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>*

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>*

The next lemma allows to use the expression  $\max f(f, \mathbf{0}..M-1)$ . 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  
 $\max f(s, \mathbf{0}..(M-1)) \in \mathbb{Z}$   
 $\forall n \in \mathbf{0}..(M-1). s(n) \leq \max f(s, \mathbf{0}..(M-1))$   
 $\min f(s, \mathbf{0}..(M-1)) \in \mathbb{Z}$   
 $\forall n \in \mathbf{0}..(M-1). \min f(s, \mathbf{0}..(M-1)) \leq s(n)$   
*<proof>*

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:  $k\in\mathbf{0}..(M-1)$   
 shows  $s(m\cdot M) + (\min f(s, \mathbf{0}..(M-1)) - \max \delta(s)) \leq s(m\cdot M + k)$   
*<proof>*

Identity is a slope.

**lemma** (in int1) Int\_ZF\_2\_1\_L17: shows  $\text{id}(\mathbb{Z}) \in \mathcal{S}$   
*<proof>*

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:  $m\in\mathbb{Z}$   $n\in\mathbb{Z}$   
 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>*

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:  $m\in\mathbb{Z}$   $n\in\mathbb{Z}$   
 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>*

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>*

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>*

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>*

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>*

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**  $\text{OddExtension}(\mathbb{Z}, \text{IntegerAddition}, \text{IntegerOrder}, f) \in \mathcal{S}$   
*<proof>*

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>*

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>*

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>*

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>*

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>*

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:  $s \in \mathcal{S}$   
**shows**  
 $\exists M \in \mathbb{Z}. \forall m \in \mathbb{Z}. \forall n \in \mathbb{Z}. \forall k \in \mathbb{Z}. \text{abs}(s(m-n-k) - (s(m) - s(n) - s(k))) \leq M$   
*<proof>*

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>*

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:  $s \in \mathcal{S}$   $r \in \mathcal{S}$   
**and** A2:  $\forall m \in \mathbb{Z}_+. \text{abs}(s(m) - r(m)) \leq L$   
**shows**  $s \sim r$   
*<proof>*

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:  $s \in \mathcal{S}$   $M \in \mathbb{Z}$   
**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>*

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:  $r = \{m, s(m) + c\}. m \in \mathbb{Z}$   
**shows**  
 $\forall m \in \mathbb{Z}. r(m) = s(m) + c$   
 $r \in \mathcal{S}$   
 $s \sim r$   
*<proof>*

## 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:  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  **and** A2:  $p \in \mathbb{Z}$   $q \in \mathbb{Z}$   
**shows**  
 $\text{abs}(f((p+1) \cdot q) - (p+1) \cdot f(q)) \leq \text{abs}(\delta(f, p \cdot q, q)) + \text{abs}(f(p \cdot q) - p \cdot f(q))$   
 $\text{abs}(f((p-1) \cdot q) - (p-1) \cdot f(q)) \leq \text{abs}(\delta(f, (p-1) \cdot q, q)) + \text{abs}(f(p \cdot q) - p \cdot f(q))$

*<proof>*

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:  $f \in \mathcal{S}$  and A2:  $0 \leq p \quad q \in \mathbb{Z}$   
 and A3:  $\text{abs}(f(p \cdot q) - p \cdot f(q)) \leq (\text{abs}(p) + 1) \cdot \max \delta(f)$   
 shows  
  $\text{abs}(f((p+1) \cdot q) - (p+1) \cdot f(q)) \leq (\text{abs}(p+1) + 1) \cdot \max \delta(f)$

*<proof>*

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  $p \leq 0$ .

**lemma** (in int1) Int\_ZF\_2\_2\_L3:  
 assumes A1:  $f \in \mathcal{S}$  and A2:  $p \leq 0 \quad q \in \mathbb{Z}$   
 and A3:  $\text{abs}(f(p \cdot q) - p \cdot f(q)) \leq (\text{abs}(p) + 1) \cdot \max \delta(f)$   
 shows  $\text{abs}(f((p-1) \cdot q) - (p-1) \cdot f(q)) \leq (\text{abs}(p-1) + 1) \cdot \max \delta(f)$

*<proof>*

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:  $f \in \mathcal{S}$  and A2:  $p \in \mathbb{Z} \quad q \in \mathbb{Z}$   
 shows  $\text{abs}(f(p \cdot q) - p \cdot f(q)) \leq (\text{abs}(p) + 1) \cdot \max \delta(f)$

*<proof>*

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  $\text{abs}(q \cdot f(p) - p \cdot f(q)) \leq (\text{abs}(p) + \text{abs}(q) + 2) \cdot \max \delta(f)$

*<proof>*

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>*

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:  $f \in \mathcal{S} \quad g \in \mathcal{S}$   
 shows  $f \circ g \sim g \circ f$

*<proof>*

**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**  $f: \mathbb{Z} \rightarrow \mathbb{Z}$   
*<proof>*

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>*

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>*

A special case of Arthan\_Lem\_3 when  $D = 1$ .

**corollary** (in int1) Arthan\_L\_3\_spec: **assumes** A1:  $f \in \mathcal{S}_+$   
**shows**  $\exists M \in \mathbb{Z}_+$ .  $\forall n \in \mathbb{Z}_+$ .  $n+1 \leq f(n \cdot M)$   
*<proof>*

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  $\mathcal{S}_+$ . 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  $\mathcal{S}_+$  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**  $f \in \mathcal{S}$     $f \notin \mathcal{S}_+$   
*<proof>*

We want to show that if  $f$  is a slope and neither  $f$  nor  $-f$  are in  $\mathcal{S}_+$ , then  $f$  is bounded. The next lemma is the first step towards that goal and shows that if slope is not in  $\mathcal{S}_+$  then  $f(\mathbb{Z}_+)$  is bounded above.

**lemma** (in int1) Int\_ZF\_2\_3\_L2: **assumes** A1:  $f \in \mathcal{S}$  and A2:  $f \notin \mathcal{S}_+$   
**shows**  $\text{IsBoundedAbove}(f(\mathbb{Z}_+), \text{IntegerOrder})$   
*<proof>*

If  $f$  is a slope and  $-f \notin \mathcal{S}_+$ , then  $f(\mathbb{Z}_+)$  is bounded below.

**lemma** (in int1) Int\_ZF\_2\_3\_L3: **assumes** A1:  $f \in \mathcal{S}$  and A2:  $-f \notin \mathcal{S}_+$   
**shows**  $\text{IsBoundedBelow}(f(\mathbb{Z}_+), \text{IntegerOrder})$   
*<proof>*

A slope that is bounded on  $\mathbb{Z}_+$  is bounded everywhere.

**lemma** (in int1) Int\_ZF\_2\_3\_L4:  
**assumes** A1:  $f \in \mathcal{S}$  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>*

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:  $f \in \mathcal{S}$  and A2:  $\text{IsBounded}(f(\mathbb{Z}_+), \text{IntegerOrder})$   
**shows**  $f \in \text{FinRangeFunctions}(\mathbb{Z}, \mathbb{Z})$   
*<proof>*

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**  $f \in \text{FinRangeFunctions}(\mathbb{Z}, \mathbb{Z}) \vee f \in \mathcal{S}_+$   
*<proof>*

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>*

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>*

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:  $f \in \mathcal{S}_+$  **and** A2:  $K \in \mathbb{Z}$   
**shows**  $\exists N \in \mathbb{Z}_+. \forall m. N \leq m \longrightarrow f(-m) \leq K$   
*<proof>*

A special case of Int\_ZF\_2\_3\_L5 where  $K = 1$ .

**corollary** (in int1) Int\_ZF\_2\_3\_L6: **assumes**  $f \in \mathcal{S}_+$   
**shows**  $\exists N \in \mathbb{Z}_+. \forall m. N \leq m \longrightarrow f(m) \in \mathbb{Z}_+$   
*<proof>*

A special case of Int\_ZF\_2\_3\_L5 where  $m = N$ .

**corollary** (in int1) Int\_ZF\_2\_3\_L6A: **assumes**  $f \in \mathcal{S}_+$  **and**  $K \in \mathbb{Z}$   
**shows**  $\exists N \in \mathbb{Z}_+. K \leq f(N)$   
*<proof>*

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>*

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>*

The sum of positive slopes is a positive slope.

**theorem** (in int1) sum\_of\_pos\_sls\_is\_pos\_sl:  
**assumes** A1:  $f \in \mathcal{S}_+$   $g \in \mathcal{S}_+$   
**shows**  $f+g \in \mathcal{S}_+$   
*<proof>*

The composition of positive slopes is a positive slope.

**theorem** (in int1) comp\_of\_pos\_sls\_is\_pos\_sl:  
**assumes** A1:  $f \in \mathcal{S}_+$   $g \in \mathcal{S}_+$   
**shows**  $f \circ g \in \mathcal{S}_+$   
*<proof>*

A slope equivalent to a positive one is positive.

**lemma** (in int1) Int\_ZF\_2\_3\_L9:  
**assumes** A1:  $f \in \mathcal{S}_+$  **and** A2:  $\langle f, g \rangle \in \text{A1EqRel}$  **shows**  $g \in \mathcal{S}_+$   
*<proof>*

The set of positive slopes is saturated with respect to the relation of equivalence of slopes.

**lemma** (in int1) pos\_slopes\_saturated: shows IsSaturated(AlEqRel, $\mathcal{S}_+$ )  
*<proof>*

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:  $f \in \mathcal{S}$   $g \in \mathcal{S}$   
 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>*

Identity function is a positive slope.

**lemma** (in int1) Int\_ZF\_2\_3\_L11: shows  $\text{id}(\mathbb{Z}) \in \mathcal{S}_+$   
*<proof>*

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>*

## 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 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:  $f \in \mathcal{S}_+$  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>*

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**  $f \in \mathcal{S}_+$  **and**  $p \in \mathbb{Z}_+$   
**shows**  
 $f^{-1}(p) \in \mathbb{Z}_+$   
 $p \leq f(f^{-1}(p))$   
 $\langle proof \rangle$

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**  $f \in \mathcal{S}_+$  **and**  $m \in \mathbb{Z}_+$   $p \in \mathbb{Z}_+$  **and**  $m \leq f(p)$   
**shows**  $f^{-1}(m) \leq p$   
 $\langle proof \rangle$

An upper bound  $f(f^{-1}(m) - 1)$  for positive slopes.

**lemma** (in int1) Int\_ZF\_2\_4\_L4:  
**assumes** A1:  $f \in \mathcal{S}_+$  **and** A2:  $m \in \mathbb{Z}_+$  **and** A3:  $f^{-1}(m) - 1 \in \mathbb{Z}_+$   
**shows**  $f(f^{-1}(m) - 1) \leq m$   $f(f^{-1}(m) - 1) \neq m$   
 $\langle proof \rangle$

The (candidate for) the inverse of a positive slope is nondecreasing.

**lemma** (in int1) Int\_ZF\_2\_4\_L5:  
**assumes** A1:  $f \in \mathcal{S}_+$  **and** A2:  $m \in \mathbb{Z}_+$  **and** A3:  $m \leq n$   
**shows**  $f^{-1}(m) \leq f^{-1}(n)$   
 $\langle proof \rangle$

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:  $f \in \mathcal{S}_+$  **and** A2:  $m \in \mathbb{Z}_+$   $n \in \mathbb{Z}_+$  **and**  
A3:  $f^{-1}(m) - 1 \in \mathbb{Z}_+$   
**shows**  $f^{-1}(m+n) - 1 \in \mathbb{Z}_+$   
 $\langle proof \rangle$

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**  
 $\exists U \in \mathbb{Z}. \forall m \in \mathbb{Z}_+. \forall n \in \mathbb{Z}_+. f(f^{-1}(m+n) - f^{-1}(m) - f^{-1}(n)) \leq U$   
 $\exists N \in \mathbb{Z}. \forall m \in \mathbb{Z}_+. \forall n \in \mathbb{Z}_+. N \leq f(f^{-1}(m+n) - f^{-1}(m) - f^{-1}(n))$   
 $\langle proof \rangle$

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>*

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>*

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>*

The (candidate for) the inverse of a positive slope is a slope.

**lemma** (in int1) Int\_ZF\_2\_4\_L11: **assumes** A1:  $f \in \mathcal{S}_+$  **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**  $\text{OddExtension}(\mathbb{Z}, \text{IntegerAddition}, \text{IntegerOrder}, g) \in \mathcal{S}$   
*<proof>*

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:  $f \in \mathcal{S}_+$  **and**  
A2:  $\forall m \in \mathbb{Z}_+. f^{-1}(m) - 1 \in \mathbb{Z}_+$   
**shows**  $\exists h \in \mathcal{S}. f \circ h \sim \text{id}(\mathbb{Z})$   
*<proof>*

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 workaroud: 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:  $f \in \mathcal{S}_+$   
**shows**  $\exists g \in \mathcal{S}. f \sim g \wedge (\exists h \in \mathcal{S}. g \circ h \sim \text{id}(\mathbb{Z}))$   
*<proof>*

### 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**

$\forall n \in \mathbb{Z}. (m^S)(n) = m \cdot n$

$m^S \in \mathcal{S}$

*<proof>*

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>*

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>*

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>*

The composition of embeddings is the embedding of the product.

**lemma** (in `int1`) `Int_ZF_2_5_L3B`: **assumes**  $A1: m \in \mathbb{Z} \quad k \in \mathbb{Z}$

**shows**  $(m^S) \circ (k^S) = ((m \cdot k)^S)$

*<proof>*

Embedding integers in slopes preserves order.

**lemma** (in `int1`) `Int_ZF_2_5_L4`: **assumes**  $A1: m \leq n$

**shows**  $(m^S) \sim (n^S) \vee (n^S) + (-m^S) \in \mathcal{S}_+$

*<proof>*

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  $m=0$   
*<proof>*

Embeddings of two integers are almost equal only if the integers are equal.

**lemma** (in int1) Int\_ZF\_2\_5\_L6:  
 assumes A1:  $m \in \mathbb{Z}$   $k \in \mathbb{Z}$  and A2:  $(m^S) \sim (k^S)$   
 shows  $m=k$   
*<proof>*

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>*

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:  $N \in \mathbb{Z}$   $M \in \mathbb{Z}$  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>*

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:  $N \in \mathbb{Z}$   $M \in \mathbb{Z}$  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>*

**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  $s : Z \rightarrow Z$  such that the set  $\{s(m+n) - s(m) - s(n)\}_{n,m \in Z}$  is finite ( $Z$  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  $s(Z)$  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)`

*<proof>*

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>*

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>

```

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 · 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  $\equiv \text{TheNeutralElement}(\text{RealNumbers},\text{RealMultiplication})$ 

  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( $\mathbb{R}, \text{RealAddition}, \text{RealMultiplication}$ )
  <proof>

```

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 $\in\mathbb{R}$ 
  <proof>

```

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**  
 $(-a) \in \mathbb{R}$   
 $(-(-a)) = a$   
 $a+0 = a$   
 $0+a = a$   
 $a \cdot 1 = a$   
 $1 \cdot a = a$   
 $a-a = 0$   
 $a-0 = a$   
*<proof>*

The lemma below lists some properties that require two real numbers to state.

**lemma** (in real0) Real\_ZF\_1\_L6: **assumes**  $a \in \mathbb{R} \quad b \in \mathbb{R}$   
**shows**  
 $a+b \in \mathbb{R}$   
 $a-b \in \mathbb{R}$   
 $a \cdot b \in \mathbb{R}$   
 $a+b = b+a$   
 $(-a) \cdot b = -(a \cdot b)$   
 $a \cdot (-b) = -(a \cdot b)$   
*<proof>*

Multiplication of reals is associative.

**lemma** (in real0) Real\_ZF\_1\_L6A: **assumes**  $a \in \mathbb{R} \quad b \in \mathbb{R} \quad c \in \mathbb{R}$   
**shows**  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$   
*<proof>*

Addition is distributive with respect to multiplication.

**lemma** (in real0) Real\_ZF\_1\_L7: **assumes**  $a \in \mathbb{R} \quad b \in \mathbb{R} \quad c \in \mathbb{R}$   
**shows**  
 $a \cdot (b+c) = a \cdot b + a \cdot c$   
 $(b+c) \cdot a = b \cdot a + c \cdot a$   
 $a \cdot (b-c) = a \cdot b - a \cdot c$   
 $(b-c) \cdot a = b \cdot a - c \cdot a$   
*<proof>*

A simple rearrangement with four real numbers.

**lemma** (in real0) Real\_ZF\_1\_L7A:  
**assumes**  $a \in \mathbb{R} \quad b \in \mathbb{R} \quad c \in \mathbb{R} \quad d \in \mathbb{R}$   
**shows**  $a-b + (c-d) = a+c-b-d$   
*<proof>*

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)
  <proof>
```

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
  <proof>
```

Zero is the class of any finite range function.

```
lemma (in real0) Real_ZF_1_L10:
  assumes A1: s ∈ Slopes
  shows SlopeEquivalenceRel{s} = 0 ↔ s ∈ BoundedIntMaps
  <proof>
```

We will need a couple of results from `Group_ZF_3.thy`. The first two 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)
  SlopeEquivalenceRel ⊆ Slopes × Slopes
  equiv(Slopes, SlopeEquivalenceRel)
  SlopeEquivalenceRel{id(int)} =
  TheNeutralElement(RealNumbers,RealMultiplication)
  BoundedIntMaps ⊆ Slopes
  <proof>
```

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**  $\text{SlopeEquivalenceRel}\{s\} = \mathbf{0}$   
*<proof>*

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:  $s \in \text{Slopes}$  **and**  
Dr:  $r = \text{QuotientGroupRel}(\text{Slopes}, \text{SlopeOp1}, \text{BoundedIntMaps})$   
**shows**  $r\{\text{GroupInv}(\text{int}, \text{IntegerAddition}) \ 0 \ s\} = -(\text{r}\{s\})$   
*<proof>*

Two classes are equal iff the slopes that represent them are almost equal.

**lemma** Real\_ZF\_1\_L13: **assumes**  $s \in \text{Slopes}$   $p \in \text{Slopes}$   
**and**  $r = \text{SlopeEquivalenceRel}$   
**shows**  $r\{s\} = r\{p\} \iff \langle s, p \rangle \in r$   
*<proof>*

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**  $\text{id}(\text{int}) \in \text{Slopes}$   
*<proof>*

**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 successful 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 ~ r ≡ ⟨s,r⟩ ∈ SlopeEquivalenceRel

fixes slope_add (infix + 70)
defines slope_add_def[simp]:
s + r ≡ SlopeOp1⟨s,r⟩

fixes slope_comp (infix ∘ 71)
defines slope_comp_def[simp]: s ∘ r ≡ SlopeOp2⟨s,r⟩

fixes slopes (S)
defines slopes_def[simp]: S ≡ AlmostHoms(int,IntegerAddition)

fixes posslopes (S+)
defines posslopes_def[simp]: S+ ≡ PositiveSlopes

fixes slope_class ([ _ ])
defines slope_class_def[simp]: [f] ≡ SlopeEquivalenceRel{f}

fixes slope_neg (-_ [90] 91)
defines slope_neg_def[simp]: -s ≡ GroupInv(int,IntegerAddition) 0 s

fixes lesseqr (infix ≤ 60)
defines lesseqr_def[simp]: a ≤ b ≡ ⟨a,b⟩ ∈ OrderOnReals

fixes sless (infix < 60)
defines sless_def[simp]: a < b ≡ a ≤ b ∧ a ≠ b

fixes positivereals (ℝ+)
defines positivereals_def[simp]: ℝ+ ≡ PositiveSet(ℝ,RealAddition,OrderOnReals)

fixes intembed (_R [90] 91)
defines intembed_def[simp]:
mR ≡ [{⟨n,IntegerMultiplication⟨m,n⟩}. n ∈ int]}

fixes floor ([ _ ])
defines floor_def[simp]:
⌊a⌋ ≡ Maximum(IntegerOrder,{m ∈ int. mR ≤ a})

fixes Γ
defines Γ_def[simp]: Γ(S,p) ≡ Maximum(IntegerOrder,{⌊pR.x⌋. x ∈ S})

fixes ia (infixl + 69)
defines ia_def[simp]: a+b ≡ IntegerAddition⟨ a,b⟩

fixes iminus (- _ 72)
defines iminus_def[simp]: -a ≡ GroupInv(int,IntegerAddition)(a)

```

```

fixes isub (infixl - 69)
defines isub_def[simp]: a-b  $\equiv$  a+ (- b)

fixes intpositives ( $\mathbb{Z}_+$ )
defines intpositives_def[simp]:
 $\mathbb{Z}_+ \equiv$  PositiveSet(int,IntegerAddition,IntegerOrder)

fixes zlesseq (infix  $\leq$  60)
defines lesseq_def[simp]: m  $\leq$  n  $\equiv$   $\langle m,n \rangle \in$  IntegerOrder

fixes imult (infixl  $\cdot$  70)
defines imult_def[simp]: a.b  $\equiv$  IntegerMultiplication(a,b)

fixes izero ( $0_{\mathbb{Z}}$ )
defines izero_def[simp]:  $0_{\mathbb{Z}} \equiv$  TheNeutralElement(int,IntegerAddition)

fixes ione ( $1_{\mathbb{Z}}$ )
defines ione_def[simp]:  $1_{\mathbb{Z}} \equiv$  TheNeutralElement(int,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)  $\equiv$  AbsoluteValue(int,IntegerAddition,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>

```

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>*

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>*

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>*

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  $[-f] = -[f]$

*<proof>*

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>*

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>*

Multiplication is commutative on reals.

**lemma** real\_mult\_commutative: shows  
RealMultiplication {is commutative on} RealNumbers  
*<proof>*

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  $[id(int)] = 1$   
*<proof>*

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  $[f] = 0$   
*<proof>*

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  $f \in \mathcal{S}$   $g \in \mathcal{S}$   
 shows  $[f] = [g] \iff f \sim g$   
*<proof>*

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  $f \sim g$   
 shows  $[f] = [g]$   
*<proof>*

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  $\text{id}(\text{int}) \in \mathcal{S}$   
*<proof>*

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  $A1: f \in \text{BoundedIntMaps}$   
 shows  $\neg(\text{id}(\text{int}) \sim f)$   
*<proof>*

Zero is not one.

**lemma** (in real1) real\_zero\_not\_one: shows  $1 \neq 0$   
*<proof>*

Negative of a real number is a real number. Property of groups.

**lemma** (in real1) Real\_ZF\_1\_1\_L8: assumes  $a \in \mathbb{R}$  shows  $(-a) \in \mathbb{R}$   
*<proof>*

An identity with three real numbers.

**lemma** (in real1) Real\_ZF\_1\_1\_L9: assumes  $a \in \mathbb{R}$   $b \in \mathbb{R}$   $c \in \mathbb{R}$   
 shows  $a \cdot (b \cdot c) = a \cdot c \cdot b$   
*<proof>*

### 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  $\subseteq$  Slopes
  PositiveReals  $\subseteq$  RealNumbers
<proof>
```

Positive reals are the same as classes of a positive slopes.

```
lemma (in real1) Real_ZF_1_2_L2:
  shows  $a \in \text{PositiveReals} \iff (\exists f \in \mathcal{S}_+. a = [f])$ 
<proof>
```

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  $f \in \mathcal{S}_+$   $g \in \mathcal{S}_+$ 
  shows
     $f+g \in \mathcal{S}_+$ 
     $f \circ g \in \mathcal{S}_+$ 
<proof>
```

Bounded integer maps are not positive slopes.

```
lemma (in real1) Real_ZF_1_2_L5:
  assumes  $f \in \text{BoundedIntMaps}$ 
  shows  $f \notin \mathcal{S}_+$ 
<proof>
```

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
   $0 \notin \text{PositiveReals}$ 
<proof>
```

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  $(f \in \mathcal{S}_+) \text{ Xor } ((-f) \in \mathcal{S}_+)$ 
<proof>
```

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  $([f] \in \text{PositiveReals}) \text{ Xor } ([g] \in \text{PositiveReals})$ 
<proof>

```

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>

```

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>

```

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>

```

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  $a \leq b$ 
<proof>

```

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>

```

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**  $(-b) \leq a$   
*<proof>*

Real order is antisymmetric.

**lemma** (in real1) real\_ord\_antisym:  
  **assumes** A1:  $a \leq b$   $b \leq a$  **shows**  $a = b$   
*<proof>*

Real order is transitive.

**lemma** (in real1) real\_ord\_transitive: **assumes** A1:  $a \leq b$   $b \leq c$   
  **shows**  $a \leq c$   
*<proof>*

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**  
   $a \cdot c \leq b \cdot c$   
   $c \cdot a \leq c \cdot b$   
*<proof>*

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**  $c \cdot a \leq c \cdot b$   
*<proof>*

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**  $a \in \mathbb{R}$   $b \in \mathbb{R}$   
*<proof>*

$a \leq b$  implies that  $0 \leq b - a$ .

**lemma** (in real1) Real\_ZF\_1\_2\_L16: **assumes**  $a \leq b$   
  **shows**  $0 \leq b - a$   
*<proof>*

A sum of nonnegative elements is nonnegative.

**lemma** (in real1) Real\_ZF\_1\_2\_L17: **assumes**  $0 \leq a$   $0 \leq b$   
  **shows**  $0 \leq a + b$   
*<proof>*

We can add sides of two inequalities

**lemma** (in real1) Real\_ZF\_1\_2\_L18: **assumes**  $a \leq b$   $c \leq d$   
  **shows**  $a + c \leq b + d$   
*<proof>*

The order on real is reflexive.

**lemma** (in real1) real\_ord\_refl: assumes  $a \in \mathbb{R}$  shows  $a \leq a$   
*<proof>*

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  $a+c \leq b+c$   
*<proof>*

We can put a number on the other side of an inequality, changing its sign.

**lemma** (in real1) Real\_ZF\_1\_2\_L19:  
assumes  $a \in \mathbb{R}$   $b \in \mathbb{R}$  and  $c \leq a+b$   
shows  $c-b \leq a$   
*<proof>*

What happens when one real number is not greater or equal than another?

**lemma** (in real1) Real\_ZF\_1\_2\_L20: assumes  $a \in \mathbb{R}$   $b \in \mathbb{R}$  and  $\neg(a \leq b)$   
shows  $b < a$   
*<proof>*

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  $a \in \mathbb{R}$   $b \in \mathbb{R}$  and  $c \leq a-b$   
shows  $c+b \leq a$   
*<proof>*

The order on reals is a relation on reals.

**lemma** (in real1) Real\_ZF\_1\_2\_L22: shows  $\text{OrderOnReals} \subseteq \mathbb{R} \times \mathbb{R}$   
*<proof>*

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:  $\text{IsBoundedAbove}(A, \text{OrderOnReals})$   
shows  $A \subseteq \mathbb{R}$   
*<proof>*

Properties of the maximum of three real numbers.

**lemma** (in real1) Real\_ZF\_1\_2\_L24:  
assumes A1:  $a \in \mathbb{R}$   $b \in \mathbb{R}$   $c \in \mathbb{R}$   
shows  
 $\text{Maximum}(\text{OrderOnReals}, \{a, b, c\}) \in \{a, b, c\}$   
 $\text{Maximum}(\text{OrderOnReals}, \{a, b, c\}) \in \mathbb{R}$   
 $a \leq \text{Maximum}(\text{OrderOnReals}, \{a, b, c\})$   
 $b \leq \text{Maximum}(\text{OrderOnReals}, \{a, b, c\})$   
 $c \leq \text{Maximum}(\text{OrderOnReals}, \{a, b, c\})$   
*<proof>*

A form of transitivity for the order on reals.

```
lemma (in real1) real_strict_ord_transit:  
  assumes A1:  $a \leq b$  and A2:  $b < c$   
  shows  $a < c$   
<proof>
```

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  $b \in \mathbb{R}_+$  and  $a \leq b$  and  $1 < c$   
  shows  $a < b \cdot c$   
<proof>
```

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  $a \in \mathbb{R}$   $b \in \mathbb{R}$  and  $a - b < c$   
  shows  $a < c + b$   
<proof>
```

Real order is translation invariant.

```
lemma (in real1) real_ord_transl_inv:  
  assumes  $a \leq b$  and  $c \in \mathbb{R}$   
  shows  $c + a \leq c + b$   
<proof>
```

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>
```

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  $\exists y \in A. x < y$   
<proof>
```

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>*

If a real number is less than another, then the second one can not be less or equal that the first.

**lemma** (in real1) Real\_ZF\_1\_2\_L29:  
 assumes  $a < b$  shows  $\neg(b \leq a)$   
*<proof>*

## 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  $\exists g \in \mathcal{S}. f \sim g \wedge (\exists h \in \mathcal{S}. g \circ h \sim \text{id}(\text{int}))$   
*<proof>*

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>*

Reals form a field.

**lemma** reals\_are\_field:  
 shows IsAfield(RealNumbers, RealAddition, RealMultiplication)  
*<proof>*

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)  
*<proof>*

If  $a$  is positive, then  $a^{-1}$  is also positive.

**lemma** (in real1) Real\_ZF\_1\_3\_L1: assumes  $a \in \mathbb{R}_+$   
 shows  $a^{-1} \in \mathbb{R}_+$   $a^{-1} \in \mathbb{R}$   
*<proof>*

A technical fact about multiplying strict inequality by the inverse of one of the sides.

**lemma** (in real1) Real\_ZF\_1\_3\_L2:  
**assumes**  $a \in \mathbb{R}_+$  and  $a^{-1} < b$   
**shows**  $1 < b \cdot a$   
*<proof>*

If  $a$  is smaller than  $b$ , then  $(b - a)^{-1}$  is positive.

**lemma** (in real1) Real\_ZF\_1\_3\_L3: **assumes**  $a < b$   
**shows**  $(b - a)^{-1} \in \mathbb{R}_+$   
*<proof>*

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:  $a \in \mathbb{R}$   $b \in \mathbb{R}_+$  and A2:  $a \cdot b < c$   
**shows**  $a < c \cdot b^{-1}$   
*<proof>*

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:  $b \in \mathbb{R}$   $c \in \mathbb{R}_+$  and A2:  $a < b \cdot c$   
**shows**  $a \cdot c^{-1} < b$   
*<proof>*

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:  $b \in \mathbb{R}$   $c \in \mathbb{R}_+$  and A2:  $a \leq b \cdot c$   
**shows**  $a \cdot c^{-1} \leq b$   
*<proof>*

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:  $a \in \mathbb{R}$   $b \in \mathbb{R}_+$  and A2:  $a \cdot b \leq c$   
**shows**  $a \leq c \cdot b^{-1}$   
*<proof>*

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**  $1 + a \cdot c < b \cdot c$   
*<proof>*

We can multiply an inequality by the inverse of a positive number.

**lemma** (in real1) Real\_ZF\_1\_3\_L6:  
**assumes**  $a \leq b$  **and**  $c \in \mathbb{R}_+$  **shows**  $a \cdot c^{-1} \leq b \cdot c^{-1}$   
*<proof>*

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**  $c \in \mathbb{R}_+$  **shows**  
 $a \cdot c < b \cdot c$   
 $c \cdot a < c \cdot b$   
 $a \cdot c^{-1} < b \cdot c^{-1}$   
*<proof>*

An identity with three real numbers, inverse and cancelling.

**lemma** (in real1) Real\_ZF\_1\_3\_L8: **assumes**  $a \in \mathbb{R}$   $b \in \mathbb{R}$   $b \neq 0$   $c \in \mathbb{R}$   
**shows**  $a \cdot b \cdot (c \cdot b^{-1}) = a \cdot c$   
*<proof>*

## 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**  $m \in \text{int}$   
**shows**  $m^R \in \mathbb{R}$   
*<proof>*

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**  $m \in \text{int}$   
**shows**  $(-m)^R = -(m^R)$   
*<proof>*

The embedding of sum of integers is the sum of embeddings.

**lemma** (in real1) Real\_ZF\_1\_4\_L1A: **assumes**  $m \in \text{int}$   $k \in \text{int}$   
**shows**  $m^R + k^R = ((m+k)^R)$   
*<proof>*

The embedding of a difference of integers is the difference of embeddings.

**lemma** (in real1) Real\_ZF\_1\_4\_L1B: **assumes** A1:  $m \in \text{int}$   $k \in \text{int}$   
**shows**  $m^R - k^R = (m-k)^R$   
*<proof>*

The embedding of the product of integers is the product of embeddings.

**lemma** (in real1) Real\_ZF\_1\_4\_L1C: **assumes**  $m \in \text{int}$   $k \in \text{int}$   
**shows**  $m^R \cdot k^R = (m \cdot k)^R$   
*<proof>*

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>*

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>*

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>*

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>*

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>*

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>*

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>*

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( $\{m \in \text{int. } m^R \leq a\}, \text{IntegerOrder}$ )  
 $\{m \in \text{int. } m^R \leq a\} \neq 0$   
 $\lfloor a \rfloor \in \text{int}$   
 $\lfloor a \rfloor^R \leq a$   
*<proof>*

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:  $m \in \text{int}$  and A2:  $m^R \leq a$   
**shows**  $m \leq \lfloor a \rfloor$   
*<proof>*

Integer zero and one embed as real zero and one.

**lemma** (in real1) int\_0\_1\_are\_real\_zero\_one:  
**shows**  $0_Z^R = 0$   $1_Z^R = 1$   
*<proof>*

Integer two embeds as the real two.

**lemma** (in real1) int\_two\_is\_real\_two: **shows**  $2_Z^R = 2$   
*<proof>*

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>*

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>*

Taking the floor function preserves the order.

**lemma** (in real1) Real\_ZF\_1\_4\_L9: **assumes** A1:  $a \leq b$   
**shows**  $\lfloor a \rfloor \leq \lfloor b \rfloor$   
*<proof>*

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( $S, \text{OrderOnReals}$ )  $S \neq 0$  and A2:  $p \in \mathbb{Z}_+$

**shows**  
 $\text{IsBoundedAbove}(\{\lfloor p^R \cdot x \rfloor. x \in S\}, \text{IntegerOrder})$   
 $\Gamma(S, p) \in \{\lfloor p^R \cdot x \rfloor. x \in S\}$   
 $\Gamma(S, p) \in \text{int}$   
*<proof>*

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:  $\text{IsBoundedAbove}(S, \text{OrderOnReals})$  and A2:  $x \in S$  and A3:  $p \in \mathbb{Z}_+$   
**shows**  $\lfloor p^R \cdot x \rfloor \leq \Gamma(S, p)$   
*<proof>*

The candidate for supremum is an integer mapping with values given by  $\Gamma$ .

**lemma** (in real1) Real\_ZF\_1\_4\_L12:  
**assumes** A1:  $\text{IsBoundedAbove}(S, \text{OrderOnReals})$   $S \neq 0$  and  
A2:  $g = \{\langle p, \Gamma(S, p) \rangle. p \in \mathbb{Z}_+\}$   
**shows**  
 $g : \mathbb{Z}_+ \rightarrow \text{int}$   
 $\forall n \in \mathbb{Z}_+. g(n) = \Gamma(S, n)$   
*<proof>*

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>*

Floor of (real) zero is (integer) zero.

**lemma** (in real1) floor\_01\_is\_zero\_one: **shows**  
 $\lfloor 0 \rfloor = 0_Z \quad \lfloor 1 \rfloor = 1_Z$   
*<proof>*

Floor of (real) two is (integer) two.

**lemma** (in real1) floor\_2\_is\_two: **shows**  $\lfloor 2 \rfloor = 2_Z$   
*<proof>*

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>*

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>*

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>*

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**  $\lfloor (m^R) + n^R \rfloor = m + n$   
*<proof>*

A lemma about adding one to floor.

**lemma** (in real1) Real\_ZF\_1\_4\_L17A: **assumes** A1:  $a \in \mathbb{R}$   
**shows**  $1 + \lfloor a \rfloor^R = (\mathbf{1}_Z + \lfloor a \rfloor)^R$   
*<proof>*

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**  
 $a - \lfloor a \rfloor^R < \mathbf{1}$   
 $a < (\mathbf{1}_Z + \lfloor a \rfloor)^R$   
*<proof>*

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>*

Some estimates for the homomorphism difference of the floor function.

**lemma** (in real1) Real\_ZF\_1\_4\_L18: **assumes** A1:  $x \in \mathbb{R}$   $y \in \mathbb{R}$   
**shows**  
 $\text{abs}(\lfloor x+y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor) \leq \mathbf{2}_Z$   
*<proof>*

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:  $\text{IsBoundedAbove}(S, \text{OrderOnReals})$   $S \neq \emptyset$  **and**  
A2:  $n \in \mathbb{Z}_+$   $x \in S$  **and**  
A3:  $\Gamma(S, n) = \lfloor n^R \cdot x \rfloor$  **and**  
A4:  $y \in S$   $x \leq y$   
**shows**  $\Gamma(S, n) = \lfloor n^R \cdot y \rfloor$   
*<proof>*

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 $\neq$ 0 and  
 A2: m $\in\mathbb{Z}_+$  n $\in\mathbb{Z}_+$   
 shows abs( $\Gamma(S,m+n)$  -  $\Gamma(S,m)$  -  $\Gamma(S,n)$ )  $\leq 2_Z$   
*<proof>*

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)  $\in \mathcal{S}$   
*<proof>*

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>*

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>*

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>*

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:  $x < y$   $y \in S$  and**  
**A4:  $N \in \mathbb{Z}_+$   $M \in \text{int}$  and**  
**A5:  $M^R < y \cdot N^R$  and A6:  $p \in \mathbb{Z}_+$**   
**shows  $p \cdot M \leq \Gamma(S, p \cdot N)$**   
*<proof>*

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)  $S \neq 0$  and A2:  $p \in \mathbb{Z}_+$**   
**and A3:**  
 **$h = \text{OddExtension}(\text{int}, \text{IntegerAddition}, \text{IntegerOrder}, \{p, \Gamma(S, p)\}. p \in \mathbb{Z}_+)$**   
**shows  $h(p) = \Gamma(S, p)$**   
*<proof>*

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:  $\neg \text{HasAmaximum}(\text{OrderOnReals}, S)$  and**  
**A3:  $x \in S$  and A4:**  
 **$h = \text{OddExtension}(\text{int}, \text{IntegerAddition}, \text{IntegerOrder}, \{p, \Gamma(S, p)\}. p \in \mathbb{Z}_+)$**   
**shows  $x \leq [h]$**   
*<proof>*

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:  $x \leq y$   $x \in S$  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>*

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)  $S \neq 0$  and**  
 **$h = \text{OddExtension}(\text{int}, \text{IntegerAddition}, \text{IntegerOrder}, \{p, \Gamma(S, p)\}. p \in \mathbb{Z}_+)$**   
**and  $p \in \mathbb{Z}_+$**   
**shows  $\exists x \in S. h(p) = \lfloor p^R \cdot x \rfloor$**   
*<proof>*

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:  $\forall x \in S. x \leq y$  and A3:
h = OddExtension(int,IntegerAddition,IntegerOrder,{p, $\Gamma(S,p)$ }. p $\in\mathbb{Z}_+$ )
shows [h]  $\leq y$ 
<proof>

```

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 HasAminimum(OrderOnReals, $\bigcap a \in S. \text{OrderOnReals}\{a\}$ )
<proof>

```

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)
<proof>

```

**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**

$$\begin{aligned} \text{CplxAdd}(R, A) \equiv \\ \{ \langle p, \langle \text{ReCxAdd}(R, A, \text{fst}(p), \text{snd}(p)), \text{ImCxAdd}(R, A, \text{fst}(p), \text{snd}(p)) \rangle \rangle \}. \\ p \in (R \times R) \times (R \times R) \} \end{aligned}$$

The expression representing the imaginary part of the product of complex numbers.

**definition**

$$\text{ImCxMul}(R, A, M, a, b) \equiv A \langle M(\text{fst}(a), \text{snd}(b)), M(\text{snd}(a), \text{fst}(b)) \rangle$$

The expression representing the real part of the product of complex numbers.

**definition**

$$\begin{aligned} \text{ReCxMul}(R, A, M, a, b) \equiv \\ A \langle M(\text{fst}(a), \text{fst}(b)), \text{GroupInv}(R, A)(M(\text{snd}(a), \text{snd}(b))) \rangle \end{aligned}$$

The function (set) that represents the binary operation of multiplication of complex numbers.

**definition**

$$\begin{aligned} \text{CplxMul}(R, A, M) \equiv \\ \{ \langle p, \langle \text{ReCxMul}(R, A, M, \text{fst}(p), \text{snd}(p)), \text{ImCxMul}(R, A, M, \text{fst}(p), \text{snd}(p)) \rangle \rangle \}. \\ p \in (R \times R) \times (R \times R) \} \end{aligned}$$

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 ( $\mathbf{1}_R$ )
defines rone_def[simp]:  $\mathbf{1}_R \equiv \text{TheNeutralElement}(R, M)$ 

fixes rzero ( $\mathbf{0}_R$ )
defines rzero_def[simp]:  $\mathbf{0}_R \equiv \text{TheNeutralElement}(R, A)$ 

fixes one (1)
defines one_def[simp]:  $\mathbf{1} \equiv \langle \mathbf{1}_R, \mathbf{0}_R \rangle$ 

fixes zero (0)
defines zero_def[simp]:  $\mathbf{0} \equiv \langle \mathbf{0}_R, \mathbf{0}_R \rangle$ 

fixes iunit (i)
defines iunit_def[simp]:  $i \equiv \langle \mathbf{0}_R, \mathbf{1}_R \rangle$ 

fixes creal ( $\mathbb{R}$ )
defines creal_def[simp]:  $\mathbb{R} \equiv \{ \langle r, \mathbf{0}_R \rangle . r \in \mathbb{R} \}$ 

fixes rmul (infixl · 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]:  $- a \equiv \text{GroupInv}(R, A)(a)$ 

fixes ca (infixl + 69)
defines ca_def[simp]:  $a + b \equiv \text{CplxAdd}(R, A)\langle a, b \rangle$ 

fixes cm (infixl · 71)
defines cm_def[simp]:  $a \cdot b \equiv \text{CplxMul}(R, A, M)\langle a, b \rangle$ 

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]:  $- a \equiv \mathbf{0} - a$ 

fixes lessr (infix < $\mathbb{R}$  68)
defines lessr_def[simp]:
 $a <_{\mathbb{R}} b \equiv \langle a, b \rangle \in \text{StrictVersion}(\text{CplxROrder}(R, A, r))$ 

```

```

fixes cpmf (+∞)
defines cpmf_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>*

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>*

Real and imaginary parts of sums and products of complex numbers are real.

**lemma** (in `complex0`) `cplx_mul_add_types`:

```
assumes A1:  $z_1 \in \mathbb{C}$   $z_2 \in \mathbb{C}$ 
shows
ReCxAdd(R,A, $z_1$ , $z_2$ )  $\in \mathbb{R}$ 
ImCxAdd(R,A, $z_1$ , $z_2$ )  $\in \mathbb{R}$ 
ImCxMul(R,A,M, $z_1$ , $z_2$ )  $\in \mathbb{R}$ 
ReCxMul(R,A,M, $z_1$ , $z_2$ )  $\in \mathbb{R}$ 
```

*<proof>*

Complex reals are complex. Recall the definition of  $\mathbb{R}$  in the `complex0` locale.

**lemma** (in `complex0`) `axresscn`: **shows**  $\mathbb{R} \subseteq \mathbb{C}$

*<proof>*

Complex 1 is not complex 0.

**lemma** (in `complex0`) `ax1ne0`: **shows**  $1 \neq 0$

*<proof>*

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>*

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>*

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:  $a \in \mathbb{R} \quad b \in \mathbb{R} \quad c \in \mathbb{R} \quad d \in \mathbb{R}$   
  **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>*

Complex multiplication is commutative.

**lemma** (in complex0) axmulcom: **assumes** A1:  $a \in \mathbb{C} \quad b \in \mathbb{C}$   
  **shows**  $a \cdot b = b \cdot a$   
*<proof>*

A sum of complex numbers is complex.

**lemma** (in complex0) axaddcl: **assumes**  $a \in \mathbb{C} \quad b \in \mathbb{C}$   
  **shows**  $a + b \in \mathbb{C}$   
*<proof>*

A product of complex numbers is complex.

**lemma** (in complex0) axmulcl: **assumes**  $a \in \mathbb{C} \quad b \in \mathbb{C}$   
  **shows**  $a \cdot b \in \mathbb{C}$   
*<proof>*

Multiplication is distributive with respect to addition.

**lemma** (in complex0) axdistr:  
  **assumes** A1:  $a \in \mathbb{C} \quad b \in \mathbb{C} \quad c \in \mathbb{C}$   
  **shows**  $a \cdot (b + c) = a \cdot b + a \cdot c$   
*<proof>*

Complex addition is commutative.

**lemma** (in complex0) axaddcom: **assumes**  $a \in \mathbb{C} \quad b \in \mathbb{C}$   
  **shows**  $a + b = b + a$   
*<proof>*

Complex addition is associative.

**lemma** (in complex0) axaddass: **assumes** A1:  $a \in \mathbb{C} \quad b \in \mathbb{C} \quad c \in \mathbb{C}$   
  **shows**  $a + b + c = a + (b + c)$   
*<proof>*

Complex multiplication is associative.

**lemma** (in complex0) axmulass: **assumes** A1:  $a \in \mathbb{C}$   $b \in \mathbb{C}$   $c \in \mathbb{C}$   
**shows**  $a \cdot b \cdot c = a \cdot (b \cdot c)$   
*<proof>*

Complex 1 is real. This really means that the pair  $\langle 1, 0 \rangle$  is on the real axis.

**lemma** (in complex0) ax1re: **shows**  $1 \in \mathbb{R}$   
*<proof>*

The imaginary unit is a "square root" of  $-1$  (that is,  $i^2 + 1 = 0$ ).

**lemma** (in complex0) axi2m1: **shows**  $i \cdot i + 1 = 0$   
*<proof>*

0 is the neutral element of complex addition.

**lemma** (in complex0) ax0id: **assumes**  $a \in \mathbb{C}$   
**shows**  $a + 0 = a$   
*<proof>*

The imaginary unit is a complex number.

**lemma** (in complex0) axicn: **shows**  $i \in \mathbb{C}$   
*<proof>*

All complex numbers have additive inverses.

**lemma** (in complex0) axnegex: **assumes** A1:  $a \in \mathbb{C}$   
**shows**  $\exists x \in \mathbb{C}. a + x = 0$   
*<proof>*

A non-zero complex number has a multiplicative inverse.

**lemma** (in complex0) axrecex: **assumes** A1:  $a \in \mathbb{C}$  **and** A2:  $a \neq 0$   
**shows**  $\exists x \in \mathbb{C}. a \cdot x = 1$   
*<proof>*

Complex 1 is a right neutral element for multiplication.

**lemma** (in complex0) ax1id: **assumes** A1:  $a \in \mathbb{C}$   
**shows**  $a \cdot 1 = a$   
*<proof>*

A formula for sum of (complex) real numbers.

**lemma** (in complex0) sum\_of\_reals: **assumes**  $a \in \mathbb{R}$   $b \in \mathbb{R}$   
**shows**  
 $a + b = \langle \text{fst}(a) + \text{fst}(b), 0_R \rangle$   
*<proof>*

The sum of real numbers is real.

**lemma** (in complex0) axaddrcl: **assumes** A1:  $a \in \mathbb{R}$   $b \in \mathbb{R}$   
**shows**  $a + b \in \mathbb{R}$

*<proof>*

The formula for the product of (complex) real numbers.

**lemma** (in complex0) prod\_of\_reals: assumes A1:  $a \in \mathbb{R}$   $b \in \mathbb{R}$   
shows  $a \cdot b = \langle \text{fst}(a) \cdot \text{fst}(b), \mathbf{0}_R \rangle$   
*<proof>*

The product of (complex) real numbers is real.

**lemma** (in complex0) axmulrcl: assumes  $a \in \mathbb{R}$   $b \in \mathbb{R}$   
shows  $a \cdot b \in \mathbb{R}$   
*<proof>*

The existence of a real negative of a real number.

**lemma** (in complex0) axrnegex: assumes A1:  $a \in \mathbb{R}$   
shows  $\exists x \in \mathbb{R}. a + x = \mathbf{0}$   
*<proof>*

Each nonzero real number has a real inverse

**lemma** (in complex0) axrrecex:  
assumes A1:  $a \in \mathbb{R}$   $a \neq \mathbf{0}$   
shows  $\exists x \in \mathbb{R}. a \cdot x = \mathbf{1}$   
*<proof>*

Our  $\mathbb{R}$  symbol is the real axis on the complex plane.

**lemma** (in complex0) real\_means\_real\_axis: shows  $\mathbb{R} = \text{ComplexReals}(R, A)$   
*<proof>*

The CplxROrder thing is a relation on the complex reals.

**lemma** (in complex0) cplx\_ord\_on\_cplx\_reals:  
shows  $\text{CplxROrder}(R, A, r) \subseteq \mathbb{R} \times \mathbb{R}$   
*<proof>*

The strict version of the complex relation is a relation on complex reals.

**lemma** (in complex0) cplx\_strict\_ord\_on\_cplx\_reals:  
shows  $\text{StrictVersion}(\text{CplxROrder}(R, A, r)) \subseteq \mathbb{R} \times \mathbb{R}$   
*<proof>*

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  $a \in \mathbb{R}$   $b \in \mathbb{R}$   
*<proof>*

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  
 $\langle x, \mathbf{0}_R \rangle <_{\mathbb{R}} \langle y, \mathbf{0}_R \rangle \iff \langle x, y \rangle \in r \wedge x \neq y$   
*<proof>*

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>*

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( $a <_{\mathbb{R}} b$ ,  $a = b$ ,  $b <_{\mathbb{R}} a$ )  
*<proof>*

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  $a <_{\mathbb{R}} b \iff \neg(a = b \vee b <_{\mathbb{R}} a)$   
*<proof>*

The strict order on complex reals is transitive.

**lemma** (in complex0) cplx\_strict\_ord\_trans:  
shows trans(StrictVersion(CplxROrder(R,A,r)))  
*<proof>*

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>*

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>*

The set of positive complex reals is closed with respect to multiplication.

**lemma** (in complex0) pre\_axmulgt0: assumes A1:  $\mathbf{0} <_{\mathbb{R}} a$   $\mathbf{0} <_{\mathbb{R}} b$   
shows  $\mathbf{0} <_{\mathbb{R}} a \cdot b$   
*<proof>*

The order on complex reals is linear and complete.

```

lemma (in complex0) cplx_reals_ord_lin_compl: shows
  CplxROrder(R,A,r) {is complete}
  IsLinOrder( $\mathbb{R}$ ,CplxROrder(R,A,r))
<proof>

```

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>

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**

$\text{IsATopology } (\_ \text{ \{is a topology\} } [90] 91)$  **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**

$\text{IsClosed } (\text{infixl } \text{\{is closed in\}} 90)$  **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**

`IsCompact (infixl \{is compact in\} 90) where`  
`K \{is compact in\} T  $\equiv (K \subseteq \bigcup T \wedge$`   
`( $\forall M \in \text{Pow}(T). K \subseteq \bigcup M \longrightarrow (\exists N \in \text{FinPow}(M). K \subseteq \bigcup N))$ )`

A basic example of a topology: the powerset of any set is a topology.

**lemma** `Pow_is_top: shows Pow(X) \{is a topology\}`  
`\langle proof \rangle`

Empty set is open.

**lemma** `empty_open:`  
`assumes T \{is a topology\} shows  $0 \in T$`   
`\langle proof \rangle`

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  $(\bigcup \mathcal{A}) \in T$  \langle proof \rangle`

Union of a indexed family of open sets is open.

**lemma** `union_indexed_open: assumes A1: T \{is a topology\} and A2:  $\forall i \in I. P(i) \in T$`   
`shows  $(\bigcup_{i \in I}. P(i)) \in T$  \langle proof \rangle`

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:  $\forall T \in \mathcal{M}. T \{is a topology\}$`   
`shows  $(\bigcap \mathcal{M}) \{is a topology\}$`   
`\langle proof \rangle`

We will now introduce some notation. In Isar, this is done by defining 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 `int(A)`. The closure of a set  $A \subseteq \bigcup T$  is denoted `cl(A)` and the boundary is  `$\partial A$` .

```

locale topology0 =
  fixes T
  assumes topSpaceAssum: T {is a topology}

  fixes int
  defines int_def [simp]: int(A)  $\equiv$  Interior(A,T)

  fixes cl
  defines cl_def [simp]: cl(A)  $\equiv$  Closure(A,T)

  fixes boundary ( $\partial_$  [91] 92)
  defines boundary_def [simp]:  $\partial A \equiv$  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  $\in$  FinPow(T)
  shows  $\bigcap N \in T$ 
  <proof>

```

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>

```

## 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 int(A)  $\subseteq$  A
  <proof>

```

Interior is open.

```

lemma (in topology0) Top_2_L2: shows int(A)  $\in$  T
  <proof>

```

A set is open iff it is equal to its interior.

```

lemma (in topology0) Top_2_L3: shows U $\in$ T  $\longleftrightarrow$  int(U) = U
  <proof>

```

Interior of the interior is the interior.

**lemma** (in topology0) Top\_2\_L4: shows  $\text{int}(\text{int}(A)) = \text{int}(A)$   
*<proof>*

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>*

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  $U \in \mathcal{T}$   
shows  $U \subseteq \text{int}(A)$   
*<proof>*

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  $\exists U \in \mathcal{T}. (x \in U \wedge U \subseteq A)$   
shows  $x \in \text{int}(A)$   
*<proof>*

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:  $V \in \mathcal{T}$   
shows  $\forall x \in V. \exists U \in \mathcal{T}. (x \in U \wedge U \subseteq V)$   
*<proof>*

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:  $\forall x \in V. \exists U \in \mathcal{T}. (x \in U \wedge U \subseteq V)$   
shows  $V \in \mathcal{T}$   
*<proof>*

### 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  $(\bigcup \mathcal{T})$  {is closed in}  $T$   
*<proof>*

Empty set is closed.

**lemma** (in topology0) Top\_3\_L2: shows 0 {is closed in} T  
 ⟨proof⟩

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 ClosedCovers(A,T)  $\neq 0$   
 ⟨proof⟩

Intersection of a nonempty family of closed sets is closed.

**lemma** (in topology0) Top\_3\_L4: assumes A1:  $K \neq 0$  and  
 A2:  $\forall D \in K. D$  {is closed in} T  
 shows  $(\bigcap K)$  {is closed in} T  
 ⟨proof⟩

The union and intersection of two closed sets are closed.

**lemma** (in topology0) Top\_3\_L5:  
 assumes A1:  $D_1$  {is closed in} T     $D_2$  {is closed in} T  
 shows  
 $(D_1 \cap D_2)$  {is closed in} T  
 $(D_1 \cup D_2)$  {is closed in} T  
 ⟨proof⟩

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:  $N \in \text{FinPow}(\{D \in \text{Pow}(\bigcup T). D$  {is closed in} T})  
 shows  $(\bigcup N)$  {is closed in} T  
 ⟨proof⟩

Closure of a set is closed.

**lemma** (in topology0) cl\_is\_closed: assumes  $A \subseteq \bigcup T$   
 shows  $\text{cl}(A)$  {is closed in} T  
 ⟨proof⟩

Closure of a bigger sets is bigger.

**lemma** (in topology0) top\_closure\_mono:  
 assumes A1:  $A \subseteq \bigcup T$      $B \subseteq \bigcup T$     and A2:  $A \subseteq B$   
 shows  $\text{cl}(A) \subseteq \text{cl}(B)$   
 ⟨proof⟩

Boundary of a set is closed.

**lemma** (in topology0) boundary\_closed:  
 assumes A1:  $A \subseteq \bigcup T$  shows  $\partial A$  {is closed in} T  
 ⟨proof⟩

A set is closed iff it is equal to its closure.

**lemma** (in topology0) Top\_3\_L8: **assumes** A1:  $A \subseteq \bigcup T$   
**shows** A {is closed in} T  $\longleftrightarrow$   $\text{cl}(A) = A$   
*<proof>*

Complement of an open set is closed.

**lemma** (in topology0) Top\_3\_L9:  
**assumes** A1:  $A \in T$   
**shows**  $(\bigcup T - A)$  {is closed in} T  
*<proof>*

A set is contained in its closure.

**lemma** (in topology0) cl\_contains\_set: **assumes**  $A \subseteq \bigcup T$  **shows**  $A \subseteq \text{cl}(A)$   
*<proof>*

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>*

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>*

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:  $B$  {is closed in} T  $A \subseteq B$   
**shows**  $\text{cl}(A) \subseteq B$   
*<proof>*

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:  $A \subseteq \bigcup T$   $\forall V \in T$  **and** A2:  $A \cap V = 0$   
**shows**  $\text{cl}(A) \cap V = 0$   
*<proof>*

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**  $A \subseteq \bigcup T$  **and**  $U \in T$  **and**  $x \in \text{cl}(A) \cap U$   
**shows**  $A \cap U \neq \emptyset$  *<proof>*

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**  $A3: \forall U \in T. x \in U \implies U \cap A \neq \emptyset$   
**shows**  $x \in \text{cl}(A)$   
*<proof>*

**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<sub>0</sub>**} [90] 91) **where**  
 $T$  {**is T<sub>0</sub>**}  $\equiv \forall x y. ((x \in \bigcup T \wedge y \in \bigcup T \wedge x \neq y) \longrightarrow (\exists U \in T. (x \in U \wedge y \notin U) \vee (y \in U \wedge x \notin U)))$

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<sub>1</sub>**} [90] 91) **where**  
 $T$  {**is T<sub>1</sub>**}  $\equiv \forall x y. ((x \in \bigcup T \wedge y \in \bigcup T \wedge x \neq y) \longrightarrow (\exists U \in T. (x \in U \wedge y \notin U)))$

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<sub>2</sub>**} [90] 91) **where**  
 $T$  {**is T<sub>2</sub>**}  $\equiv \forall x y. ((x \in \bigcup T \wedge y \in \bigcup T \wedge x \neq y) \longrightarrow (\exists U \in T. \exists V \in T. x \in U \wedge y \in V \wedge U \cap V = \emptyset))$

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 **isT0** condition and **isT1**.

**lemma** T1\_is\_T0: **assumes** A1:  $T$  {**is T<sub>1</sub>**} **shows**  $T$  {**is T<sub>0</sub>**}  
*<proof>*

If a topology is  $T_2$  then it is  $T_1$ .

**lemma** T2\_is\_T1: **assumes** A1:  $T$  {**is T<sub>2</sub>**} **shows**  $T$  {**is T<sub>1</sub>**}

*<proof>*

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>*

## 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>*

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**  $\exists A \in \text{Pow}(B). U = \bigcup A$   
*<proof>*

Elements of base are open.

**lemma** *base\_sets\_open*:  
**assumes**  $B$  {is a base for}  $T$  and  $U \in B$   
**shows**  $U \in T$   
*<proof>*

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**  $T = S$   
*<proof>*

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>*

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**  $A2$ :  $B \subseteq T$  and  $A3$ :  $\forall V \in T. \exists A \in \text{Pow}(B). V = \bigcup A$   
**shows**  $B$  {is a base for}  $T$   
*<proof>*

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**  $A1$ :  $\exists T. T$  {is a topology}  $\wedge B$  {is a base for}  $T$   
**and**  $A2$ :  $\forall B \ W \in B$   
**shows**  $\forall x \in V \cap W. \exists U \in B. x \in U \wedge U \subseteq V \cap W$   
*<proof>*

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>*

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:  $B$  {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>*

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:  $B$  {satisfies the base condition}  
**and** A2:  $T = \{\bigcup A. A \in \text{Pow}(B)\}$   
**shows**  $T$  {is a topology} **and**  $B$  {is a base for}  $T$   
*<proof>*

The carrier of the base and topology are the same.

**lemma** Top\_1\_2\_L5: **assumes**  $B$  {is a base for}  $T$   
**shows**  $\bigcup T = \bigcup B$   
*<proof>*

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>*

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**  $B = T$  *<proof>*

### 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>*

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>*

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`:  $U \in \text{ProductTopology}(T,S)$  **and** `A3`:  $x \in U$   
**shows**  $\exists V W. \forall T \wedge W \in S \wedge V \times W \subseteq U \wedge x \in V \times W$

*<proof>*

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`:  $U \in T$      $V \in S$   
**shows**  $U \times V \in \text{ProductTopology}(T,S)$

*<proof>*

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`:  $V \in \text{ProductTopology}(T,S)$   
**shows**  $V \subseteq \bigcup T \times \bigcup S$

*<proof>*

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>*

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×B)  
*<proof>*

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>*

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:  $V \in \text{ProductTopology}(T,S)$  and A3:  $y \in \bigcup TS$   
 shows  $\{x \in \bigcup T. \langle x,y \rangle \in V\} \in T$   
*<proof>*

**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⟩
```

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 `FinPow(A)` denotes the set of finite subsets of  $A$  in `IsarMathLib`.

```
theorem (in topology0) in_t2_compact_is_cl:
  assumes A1: T {is T2} and A2: K {is compact in} T
  shows K {is closed in} T
⟨proof⟩
```

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**

```
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( $\tau, \tau, \text{id}(\bigcup \tau)$ )` *<proof>*

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 cl1
defines cl1_def [simp]:  $cl_1(A) \equiv Closure(A, \tau_1)$ 

fixes cl2
defines cl2_def [simp]:  $cl_2(A) \equiv Closure(A, \tau_2)$ 

```

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( $\tau_2$ )
  <proof>

```

For continuous functions the inverse image of a closed set is closed.

```

lemma (in two_top_spaces0) Top_ZF_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>

```

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) Top_ZF_2_1_L2:
  assumes A1:  $\forall D. (D \{is\ closed\ in\} \tau_2) \longrightarrow f^{-1}(D) \{is\ closed\ in\} \tau_1$ 
  and A2:  $A \subseteq X_1$ 
  shows  $f(cl_1(A)) \subseteq cl_2(f(A))$ 
  <proof>

```

If  $f(\overline{A}) \subseteq \overline{f(A)}$  (the image of the closure is contained in the closure of the image), then  $f^{-1}(\overline{B}) \subseteq \overline{f^{-1}(B)}$  (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:  $\forall A. (A \subseteq X_1 \longrightarrow f(cl_1(A)) \subseteq cl_2(f(A)))$ 
  shows  $\forall B. (B \subseteq X_2 \longrightarrow cl_1(f^{-1}(B)) \subseteq \overline{f^{-1}(B)})$ 
  <proof>

```

If  $f^{-1}(\overline{B}) \subseteq \overline{f^{-1}(B)}$  (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>*

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:  $\forall U \in B. f^{-1}(U) \in \tau_1$   
**shows** f {is continuous}  
*<proof>*

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>*

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:  $\mathcal{B}$  {is a base for}  $\tau_1$  **and** A2:  $\forall B \in \mathcal{B}. f(B) \in \tau_2$  **and** A3:  
 $U \in \tau_1$   
**shows**  $f(U) \in \tau_2$   
*<proof>*

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)  
*<proof>*

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)  
*<proof>*

## 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)  $\equiv$   
 $f \in \text{bij}(\bigcup T, \bigcup S) \wedge \text{IsContinuous}(T,S,f) \wedge \text{IsContinuous}(S,T,\text{converse}(f))$

Inverse (converse) of a homeomorphism is a homeomorphism.

**lemma** `homeo_inv`: **assumes** `IsAhomeomorphism(T,S,f)`  
**shows** `IsAhomeomorphism(S,T,converse(f))`  
*<proof>*

Homeomorphisms are open maps.

**lemma** `homeo_open`: **assumes** `IsAhomeomorphism(T,S,f)` **and** `U∈T`  
**shows** `f(U) ∈ S`  
*<proof>*

A continuous bijection that is an open map is a homeomorphism.

**lemma** `bij_cont_open_homeo`:  
**assumes** `f ∈ bij(∪T,∪S)` **and** `IsContinuous(T,S,f)` **and** `∀U∈T. f(U) ∈ S`  
**shows** `IsAhomeomorphism(T,S,f)`  
*<proof>*

A continuous bijection that maps base to open sets is a homeomorphism.

**lemma** (**in** `two_top_spaces0`) `bij_base_open_homeo`:  
**assumes** `A1: f ∈ bij(X1,X2)` **and** `A2: B {is a base for} τ1` **and** `A3: C {is a base for} τ2` **and**  
`A4: ∀U∈C. f(U) ∈ τ1` **and** `A5: ∀V∈B. f(V) ∈ τ2`  
**shows** `IsAhomeomorphism(τ1,τ2,f)`  
*<proof>*

A bijections that maps base to base is a homeomorphisms.

**lemma** (**in** `two_top_spaces0`) `bij_base_homeo`:  
**assumes** `A1: f ∈ bij(X1,X2)` **and** `A2: B {is a base for} τ1` **and**  
`A3: {f(B). B∈B} {is a base for} τ2`  
**shows** `IsAhomeomorphism(τ1,τ2,f)`  
*<proof>*

Interior is a topological invariant.

**theorem** `int_top_invariant`: **assumes** `A1: A⊆∪T` **and** `A2: IsAhomeomorphism(T,S,f)`  
**shows** `f(Interior(A,T)) = Interior(f(A),S)`  
*<proof>*

### 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 ∈ bij(∪T,Y)`  
**shows**  
`{f(U). U∈T} {is a topology}` **and**

```

{ {f(x).x∈U}. U∈T} {is a topology} and
(⋃{f(U). U∈T}) = Y and
IsAhomeomorphism(T, {f(U). U∈T},f)
⟨proof⟩

```

#### 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⟩

```

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⟩

```

A combination of `restr_cont` and `restr_image_cont`.

```

lemma (in two_top_spaces0) restr_restr_image_cont:
  assumes A1: A ⊆ X1 and A2: f {is continuous} and
  A3: g = restrict(f,A) and
  A4: τ3 = τ1 {restricted to} A
  shows IsContinuous(τ3, τ2 {restricted to} g(A),g)
⟨proof⟩

```

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 τ1
  assumes tau1_is_top: τ1 {is a topology}

  fixes τ2
  assumes tau2_is_top: τ2 {is a topology}

```

```

fixes X1
defines X1_def [simp]: X1  $\equiv$   $\bigcup \tau_1$ 

```

```

fixes X2
defines X2_def [simp]: X2  $\equiv$   $\bigcup \tau_2$ 

```

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: IsContinuous( $\tau_1, \tau_2, g$ )
  shows  $A \in \tau_1$  and IsContinuous( $\tau_1$  {restricted to}  $A, \tau_2, g$ )
<proof>

```

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 IsContinuous( $\tau_1, \tau_2, g$ )  $\longleftrightarrow$ 
    IsContinuous( $\tau_1$  {restricted to}  $A, \tau_2, g$ )
<proof>

```

## 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 X1
  defines X1_def [simp]: X1  $\equiv$   $\bigcup \tau_1$ 

```

```

  fixes X2
  defines X2_def [simp]: X2  $\equiv$   $\bigcup \tau_2$ 

```

```

fixes X3
defines X3_def [simp]: X3  $\equiv$   $\bigcup \tau_3$ 

fixes  $\eta$ 
defines eta_def [simp]:  $\eta \equiv$  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( $\tau_2, \tau_3, \text{Fix1stVar}(f, x)$ )
  <proof>

```

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( $\tau_1, \tau_3, \text{Fix2ndVar}(f, y)$ )
  <proof>

```

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>

```

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>

```

## 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: restrict(f,A) {is continuous}
  shows  $A \in \tau_1$ 
<proof>
```

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 restrict(f, $\bigcup M$ ) {is continuous}
<proof>
```

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>
```

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  $\{U \in \tau_1. \text{restrict}(f,U) \text{ {is continuous}}\} \text{ {is a topology}}$ 
<proof>
```

0 is continuous.

```
corollary (in two_top_spaces0) zero_continuous: shows 0 {is continuous}
<proof>
```

**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:  $U \in \text{ProductTopBase}(I, T)$   $V \in \text{ProductTopBase}(I, T)$   
**shows**  $U \cap V \in \text{ProductTopBase}(I, T)$

*<proof>*

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**  $\text{ProductTopBase}(I, T)$  {satisfies the base condition}  
*<proof>*

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**  
 $\text{SeqProductTopology}(I, T)$  {is a topology} **and**  
 $\text{ProductTopBase}(I, T)$  {is a base for}  $\text{SeqProductTopology}(I, T)$  **and**  
 $\bigcup \text{SeqProductTopology}(I, T) = (I \rightarrow \bigcup T)$   
*<proof>*

## 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>*

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>*

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>*

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**  $\text{IsAHomeomorphism}(\text{SeqProductTopology}(1, \tau), \tau, \{ \langle x, x(0) \rangle \}. x \in 1 \rightarrow \bigcup \tau \})$

*<proof>*

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**  $(\bigcup \text{ProductTopology}(T, \tau)) = (n \rightarrow \bigcup \tau) \times \bigcup \tau$

*<proof>*

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>*

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>*

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 = {⟨x,⟨Init(x),x(n)⟩⟩. x ∈ succ(n)→⋃τ} and
A4: T = SeqProductTopology(n,τ) and
A5: S = SeqProductTopology(succ(n),τ)
shows IsAhomeomorphism(S,ProductTopology(T,τ),f)
⟨proof⟩

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 ≡ refl(D,r) ∧ trans(r) ∧ (∀x∈D. ∀y∈D. ∃z∈D.
⟨x,z⟩∈r ∧ ⟨y,z⟩∈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⟩
```

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 ≡ fst(N):domain(fst(N))→X ∧ (snd(N) {directs}
domain(fst(N))) ∧ domain(fst(N))≠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 (_ →N _ 90)
  where N {is a net on} ⋃T ⇒ NetConverges(N,x) ≡
(x∈⋃T) ∧ (∀U∈Pow(⋃T). (x∈int(U) → (∃t∈domain(fst(N)). ∀m∈domain(fst(N)).
(⟨t,m⟩∈snd(N) → fst(N)m∈U))))
```

One of the most important directed sets, is the neighborhoods of a point.

```
theorem (in topology0) directedset_neighborhoods:
```

```

fixes x
defines Neigh $\equiv\{U\in\text{Pow}(\bigcup T). x\in\text{int}(U)\}$ 
defines r $\equiv\{\langle U,V\rangle\in(\text{Neigh}\times\text{Neigh}). V\subseteq U\}$ 
shows r {directs} Neigh
<proof>

```

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 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>

```

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  $\mathfrak{F}$  {is a filter on} X  $\equiv (0\notin\mathfrak{F}) \wedge (X\in\mathfrak{F}) \wedge (\mathfrak{F}\subseteq\text{Pow}(X)) \wedge$ 
 $(\forall A\in\mathfrak{F}. \forall B\in\mathfrak{F}. A\cap B\in\mathfrak{F}) \wedge (\forall B\in\mathfrak{F}. \forall C\in\text{Pow}(X). B\subseteq C \longrightarrow C\in\mathfrak{F})$ 

```

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}  $\mathfrak{F} \equiv C\subseteq\mathfrak{F} \wedge \mathfrak{F}=\{A\in\text{Pow}(\bigcup\mathfrak{F}). (\exists D\in C. D\subseteq A)\}$ 

```

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 $\in\mathfrak{F}$  and C {is a base filter}  $\mathfrak{F}$ 
shows  $\exists D\in C. D\subseteq A$ 
<proof>

```

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}  $\mathfrak{F}$  and  $C$  {satisfies the filter base condition}  
 shows  $\mathfrak{F}$  {is a filter on}  $\bigcup \mathfrak{F}$   
*<proof>*

**theorem basic\_filter\_2:**

assumes  $C$  {is a base filter}  $\mathfrak{F}$  and  $\mathfrak{F}$  {is a filter on}  $\bigcup \mathfrak{F}$   
 shows  $C$  {satisfies the filter base condition}  
*<proof>*

**theorem basic\_filter:**

assumes  $C$  {is a base filter}  $\mathfrak{F}$   
 shows  $(C$  {satisfies the filter base condition})  $\longleftrightarrow$  ( $\mathfrak{F}$  {is a filter on}  $\bigcup \mathfrak{F}$ )  
*<proof>*

A base for a filter determines a filter up to the underlying set.

**theorem base\_unique\_filter:**

assumes  $C$  {is a base filter}  $\mathfrak{F}_1$  and  $C$  {is a base filter}  $\mathfrak{F}_2$   
 shows  $\mathfrak{F}_1 = \mathfrak{F}_2 \longleftrightarrow \bigcup \mathfrak{F}_1 = \bigcup \mathfrak{F}_2$   
*<proof>*

**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>*

**theorem base\_unique\_filter\_set2:**

assumes  $C \subseteq \text{Pow}(X)$  and  $C$  {satisfies the filter base condition}  
 shows  $((C$  {is a base filter}  $\mathfrak{F}) \wedge \bigcup \mathfrak{F} = X) \longleftrightarrow \mathfrak{F} = \{A \in \text{Pow}(X). \exists D \in C. D \subseteq A\}$   
*<proof>*

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>*

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**  $\mathfrak{F}$  {is a filter on}  $\bigcup T$  and  $C$  {is a base filter}  $\mathfrak{F}$  and  $\mathfrak{F} \rightarrow_F x$   
**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>*

**theorem** (in topology0) *convergence\_filter\_base2*:  
**assumes**  $\mathfrak{F}$  {is a filter on}  $\bigcup T$  and  $C$  {is a base filter}  $\mathfrak{F}$   
**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**  $\mathfrak{F} \rightarrow_F x$   
*<proof>*

**theorem** (in topology0) *convergence\_filter\_base\_eq*:  
**assumes**  $\mathfrak{F}$  {is a filter on}  $\bigcup T$  and  $C$  {is a base filter}  $\mathfrak{F}$   
**shows**  $(\mathfrak{F} \rightarrow_F x) \longleftrightarrow ((\forall U \in \text{Pow}(\bigcup T). x \in \text{int}(U) \longrightarrow (\exists D \in C. D \subseteq U)) \wedge x \in \bigcup T)$   
*<proof>*

### 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

**NetOfFilter** (*Net*(\_) 40) **where**  
 $\mathfrak{F}$  {is a filter on}  $\bigcup \mathfrak{F} \implies \text{NetOfFilter}(\mathfrak{F}) \equiv \langle \{ \langle A, \text{fst}(A) \rangle. A \in \{ \langle x, F \rangle \in (\bigcup \mathfrak{F}) \times \mathfrak{F}. x \in F \} \}, \{ \langle A, B \rangle \in \{ \langle x, F \rangle \in (\bigcup \mathfrak{F}) \times \mathfrak{F}. x \in F \} \times \{ \langle x, F \rangle \in (\bigcup \mathfrak{F}) \times \mathfrak{F}. x \in F \}. \text{snd}(B) \subseteq \text{snd}(A) \} \rangle$

**theorem** *net\_of\_filter\_is\_net*:  
**assumes**  $\mathfrak{F}$  {is a filter on}  $X$   
**shows**  $(\text{Net}(\mathfrak{F}))$  {is a net on}  $X$   
*<proof>*

**theorem** (in topology0) *filter\_conver\_net\_of\_filter\_conver*:  
**assumes**  $\mathfrak{F}$  {is a filter on}  $\bigcup T$  and  $\mathfrak{F} \rightarrow_F x$   
**shows**  $(\text{Net}(\mathfrak{F})) \rightarrow_N x$   
*<proof>*

**theorem** (in topology0) *net\_of\_filter\_conver\_filter\_conver*:  
**assumes**  $\mathfrak{F}$  {is a filter on}  $\bigcup T$  and  $(\text{Net}(\mathfrak{F})) \rightarrow_N x$

**shows**  $\mathfrak{F} \rightarrow_F x$   
*<proof>*

**theorem** (in topology0) filter\_conver\_iff\_net\_of\_filter\_conver:  
**assumes**  $\mathfrak{F}$  {is a filter on}  $\bigcup T$   
**shows**  $(\mathfrak{F} \rightarrow_F x) \longleftrightarrow ((\text{Net}(\mathfrak{F})) \rightarrow_N x)$   
*<proof>*

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  $\text{Net}\mathfrak{F}$  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**  
 $(N \text{ {is a net on} } X) \implies \text{FilterOfNet}(N, X) \equiv \{A \in \text{Pow}(X). \exists D \in \{\{\text{fst}(N)\text{snd}(s). s \in \{\text{snd}(N) \wedge \text{fst}(s)=t\}\}. t \in \text{domain}(\text{fst}(N))\}\}. D \subseteq A\}$

**theorem** filter\_of\_net\_is\_filter:

**assumes**  $N$  {is a net on}  $X$   
**shows** (Filter  $N..X$ ) {is a filter on}  $X$  **and**  $\{\{\text{fst}(N)\text{snd}(s). s \in \{\text{snd}(N) \wedge \text{fst}(s)=t\}\}. t \in \text{domain}(\text{fst}(N))\}\}$  {is a base filter} (Filter  $N..X$ )  
*<proof>*

**theorem** (in topology0) net\_conver\_filter\_of\_net\_conver:

**assumes**  $N$  {is a net on}  $\bigcup T$  **and**  $N \rightarrow_N x$   
**shows** (Filter  $N..(\bigcup T)$ )  $\rightarrow_F x$   
*<proof>*

**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>*

**theorem** (in topology0) filter\_of\_net\_conv\_iff\_net\_conv:

**assumes**  $N$  {is a net on}  $\bigcup T$   
**shows**  $((\text{Filter } N..(\bigcup T)) \rightarrow_F x) \longleftrightarrow (N \rightarrow_N x)$   
*<proof>*

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>*

**lemma** `topology0_filter`:  
 assumes  $\mathcal{F}$  {is a filter on}  $\bigcup \mathcal{F}$   
 shows `topology0` $(\mathcal{F} \cup \{0\})$   
*<proof>*

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` $(\mathcal{F}, x, T) \equiv \text{topology0.FilterConverges}(T, \mathcal{F}, x)$

**abbreviation** `NetConvTop` $(\_ \rightarrow N \_ \{in\} \_)$   
 where `NetConvTop` $(N, x, T) \equiv \text{topology0.NetConverges}(T, N, x)$

**lemma** `lim_filter_top_of_filter`:  
 assumes  $\mathcal{F}$  {is a filter on}  $\bigcup \mathcal{F}$  and  $x \in \bigcup \mathcal{F}$   
 shows  $\mathcal{F} \rightarrow F x \{in\} (\mathcal{F} \cup \{0\})$   
*<proof>*

**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>
```

**lemma** `Card_cases`:

```
  assumes Card (Q)
  obtains (0) Q=0 | (csucc) T where Card(T)  Q=csucc(T) | (limit) LimitC(Q)
<proof>
```

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>
```

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=nat  $\vee$  ( $\exists j$ . csucc(j) $\lesssim$ Q & InfCard(j))
  <proof>

```

```

lemma InfCard_cases:
  assumes InfCard (Q)
  obtains (nat) Q=nat | predecessor j where csucc(j) $\lesssim$ Q  $\wedge$  InfCard(j)
  <proof>

```

### 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 < csucc(m)  $\longleftrightarrow$  A  $\lesssim$  m
  <proof>

```

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>

```

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>

```

### 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 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  $A < \aleph$  and  $B < \aleph$  and  $\text{InfCard}(\aleph)$   
 shows  $A \cup B < \aleph$   
*<proof>*

## 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**  
 $\text{CoCardinal } X \ T \equiv \{F \in \text{Pow}(X). X - F < T\} \cup \{0\}$

For any set and any infinite cardinal; we prove that `CoCardinal`  $X \ \aleph$  forms a topology. The proof is done with an infinite cardinal, but it is obvious that the set  $\aleph$  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  $\aleph = 1$  which translates in the indiscrete topology.

**lemma** `CoCar_is_topology`:  
 assumes  $\text{InfCard } (\aleph)$   
 shows  $(\text{CoCardinal } X \ \aleph) \ \{\text{is a topology}\}$   
*<proof>*

**theorem** `topology0_CoCardinal`:  
 assumes  $\text{InfCard}(T)$   
 shows  $\text{topology0}(\text{CoCardinal } X \ T)$   
*<proof>*

It can also be proven that, if `CoCardinal`  $X \ T$  is a topology,  $X \neq 0$ ,  $\text{Card}(T)$  and  $T \neq 0$ ; then  $T$  is an infinite cardinal,  $X < T$  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` (`CoFinite`  $\_ 90$ ) **where**

$\text{CoFinite } X \equiv \text{CoCardinal } X \text{ nat}$

**definition**

$\text{Cocountable } (\text{CoCountable } \_ \ 90)$  where  
 $\text{CoCountable } X \equiv \text{CoCardinal } X \text{ csucc}(\text{nat})$

**48.2.2 Total set, Closed sets, Interior, Closure and Boundary**

There are several assertions that can be done to the  $\text{CoCardinal } X \ T$  topology. In each case, we will not assume sufficient conditions for  $\text{CoCardinal } X \ T$  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  $\bigcup (\text{CoCardinal } X \ T) = X$   
*<proof>*

The closed sets are the small subsets of  $X$  and  $X$  itself.

**lemma closed\_sets\_cocardinal:**  
 assumes  $T \neq 0$   
 shows  $D \{\text{is closed in}\} (\text{CoCardinal } X \ T) \iff (D \in \text{Pow}(X) \ \& \ D \prec T) \vee D = X$   
*<proof>*

The interior of a set is itself if it is open or 0 if it isn't open.

**lemma interior\_set\_cocardinal:**  
 assumes  $\text{noC}: T \neq 0$  and  $A \subseteq X$   
 shows  $\text{Interior}(A, (\text{CoCardinal } X \ T)) = (\text{if } ((X - A) \prec T) \text{ then } A \text{ else } 0)$   
*<proof>*

$X$  is a closed set that contains  $A$ . This lemma is necessary because we cannot use the lemmas proven in the  $\text{topology0}$  context since  $T \neq 0$  is too weak for  $\text{CoCardinal } X \ T$  to be a topology.

**lemma X\_closedcov\_cocardinal:**  
 assumes  $T \neq 0$  and  $A \subseteq X$   
 shows  $X \in \text{ClosedCovers}(A, (\text{CoCardinal } X \ T))$  *<proof>*

The closure of a set is itself if it is closed or  $X$  if it isn't closed.

**lemma closure\_set\_cocardinal:**  
 assumes  $T \neq 0$  and  $A \subseteq X$   
 shows  $\text{Closure}(A, (\text{CoCardinal } X \ T)) = (\text{if } (A \prec T) \text{ then } A \text{ else } X)$   
*<proof>*

The boundary of a set is 0 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**  $T \neq 0 \wedge A \subseteq X$   
**shows**  $\text{Boundary}(A, (\text{CoCardinal } X \ T)) = (\text{if } A \prec T \text{ then } (\text{if } (X-A) \prec T \text{ then } 0 \text{ else } A) \text{ else } (\text{if } (X-A) \prec T \text{ then } X-A \text{ else } X))$   
*<proof>*

### 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**  $X \prec T$   
**shows**  $(\text{CoCardinal } X \ T) = (\text{Pow } X)$   
*<proof>*

If the cardinal is taken as  $T = 1$  then the topology is indiscrete.

**lemma** `indiscrete_cocardinal`:  
**shows**  $(\text{CoCardinal } X \ 1) = \{0, X\}$   
*<proof>*

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>*

## 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**  
 $\text{ExcludedSet } (X \ U \ 50)$  **where**  
 $\text{ExcludedSet } X \ U \equiv \{F \in \text{Pow}(X). U \cap F = 0\} \cup \{X\}$

For any set; we prove that  $\text{ExcludedSet } X \ Q$  forms a topology.

**theorem** `excludedset_is_topology`:  
**shows**  $(\text{ExcludedSet } X \ Q) \{\text{is a topology}\}$   
*<proof>*

**theorem** `topology0_excludedset`:  
**shows**  $\text{topology0}(\text{ExcludedSet } X \ T)$   
*<proof>*

Choosing a singleton set, it is considered a point excluded topology.

**definition**

ExcludedPoint (ExcludedPoint \_ \_ 90) where  
 ExcludedPoint X p $\equiv$  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  $\bigcup$  (ExcludedSet X T)=X  
*<proof>*

The closed sets are those which contain the set  $X \cap T$  and  $0$ .

**lemma** closed\_sets\_excludedset:  
 shows  $D \{is\ closed\ in\} (ExcludedSet\ X\ T) \longleftrightarrow (D \in Pow(X) \ \& \ (X \cap T) \subseteq D) \vee D=0$   
*<proof>*

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  $Interior(A, (ExcludedSet\ X\ T)) = (if\ A=X\ then\ X\ else\ A-T)$   
*<proof>*

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  $Closure(A, (ExcludedSet\ X\ T)) = (if\ A=0\ then\ 0\ else\ A \cup (X \cap T))$   
*<proof>*

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  $Boundary(A, (ExcludedSet\ X\ T)) = (if\ A=0 \vee A=X\ then\ 0\ else\ X \cap T)$   
*<proof>*

### 48.3.3 Special cases and subspaces

The topology is equal in the sets  $T$  and  $X \cap T$ .

**lemma** smaller\_excludedset:  
 shows  $(ExcludedSet\ X\ T) = (ExcludedSet\ X\ (X \cap T))$   
*<proof>*

If the set which is excluded is disjoint with  $X$ , then the topology is discrete.

**lemma** empty\_excludedset:  
 assumes  $T \cap X = 0$   
 shows  $(ExcludedSet\ X\ T) = Pow(X)$   
*<proof>*

The topological subspaces of the ExcludedSet  $X$   $T$  topology are also ExcludedSet topologies.

**lemma** `subspace_excludedset:`

`shows (ExcludedSet  $X$   $T$ ) {restricted to}  $Y=(\text{ExcludedSet } (Y \cap X) T)$`   
*<proof>*

## 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 IncludedSet  $X$   $Q$  forms a topology.

**theorem** `includedset_is_topology:`

`shows (IncludedSet  $X$   $Q$ ) {is a topology}`  
*<proof>*

**theorem** `topology0_includedset:`

`shows topology0(IncludedSet  $X$   $T$ )`  
*<proof>*

Choosing a singleton set, it is considered a point excluded topology. In the following lemmas and theorems, when necessary it will be considered that  $T \neq 0$  and  $T \subseteq X$ . These cases will appear in the special cases section.

**definition**

`IncludedPoint (IncludedPoint _ _ 90) where`  
`IncludedPoint  $X$   $p \equiv \text{IncludedSet } X \{p\}$`

### 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>*

The closed sets are those which are disjoint with  $T$  and  $X$ .

**lemma** `closed_sets_includedset:`

`assumes  $T \subseteq X$`

**shows**  $D \{\text{is closed in}\} (\text{IncludedSet } X \ T) \longleftrightarrow (D \in \text{Pow}(X) \ \& \ (D \cap T) = 0) \vee D = X$   
*<proof>*

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>*

The closure of a set is itself if it is closed or  $X$  if it isn't.

**lemma** `closure_set_includedset`:  
**assumes**  $A \subseteq XT \subseteq X$   
**shows**  $\text{Closure}(A, (\text{IncludedSet } X \ T)) = (\text{if } T \cap A = 0 \text{ then } A \text{ else } X)$   
*<proof>*

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 a 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>*

### 48.4.3 Special cases and subspaces

The topology is discrete if  $T = 0$

**lemma** `smaller_includedset`:  
**shows**  $(\text{IncludedSet } X \ 0) = \text{Pow}(X)$   
*<proof>*

If the set which is included is not a subset of  $X$ , then the topology is trivial.

**lemma** `empty_includedset`:  
**assumes**  $\sim(T \subseteq X)$   
**shows**  $(\text{IncludedSet } X \ T) = \{0\}$   
*<proof>*

The topological subspaces of the `IncludedSet X T` topology are also `IncludedSet` topologies. The trivial case does not fit the idea in the demonstration; because if  $Y \subseteq X$  then `IncludedSet Y  $\cap$  X 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**  $T \subseteq X$   
**shows**  $(\text{IncludedSet } X \ T) \{\text{restricted to}\} Y = (\text{IncludedSet } (Y \cap X) \ (Y \cap T))$   
*<proof>*

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>
```

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>
```

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 Interior(A,T)= $\bigcup$ {T $\in$ U. T $\subseteq$ A}
<proof>
```

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 $\implies$ A $\cap$ T $\neq$  $\emptyset$ }
```

*<proof>*

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>*

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}T2B⊆B2`

`shows T⊆T2`

*<proof>*

### 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{is a base for}T ⇒ DualBase B T≡{∪T-U. U∈B}∪{∪T}`

**lemma** `closed_inter_dual_base:`

`assumes D{is closed in}TB{is a base for}T`

`obtains M where M⊆DualBase B TD=∩M`

*<proof>*

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⊆∪Q`

`shows Closure(A,Q)=∩{T∈DualBase U Q. A⊆T}`

*<proof>*

## 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 (_{is a partition of}_ 90) where`

`(U {is a partition of} X) ≡ (∪U=X ∧ (∀A∈U. ∀B∈U. A=B∨ A∩B=0) ∧ 0∉U)`

A subcollection of a partition is a partition of its union.

**lemma** subpartition:  
 assumes  $U$  {is a partition of}  $X$   $V \subseteq U$   
 shows  $V$  {is a partition of}  $\bigcup V$   
*<proof>*

A restriction of a partition is a partition. If the empty set appears it has to be removed.

**lemma** restriction\_partition:  
 assumes  $U$  {is a partition of}  $X$   
 shows  $((U$  {restricted to}  $Y) - \{0\})$  {is a partition of}  $(X \cap Y)$   
*<proof>*

Given a partition, the complement of a union of a subfamily is a union of a subfamily.

**lemma** diff\_union\_is\_union\_diff:  
 assumes  $R \subseteq P$   $P$  {is a partition of}  $X$   
 shows  $X - \bigcup R = \bigcup (P - R)$   
*<proof>*

### 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>*

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}  $X) \implies \text{PTopology } X \ U \equiv \text{TopologyBase } U$

**theorem** Ptopology\_is\_a\_topology:  
 assumes  $U$  {is a partition of}  $X$   
 shows  $(\text{PTopology } X \ U)$  {is a topology} and  $U$  {is a base for}  $(\text{PTopology } X \ U)$   
*<proof>*

**lemma** topology0\_ptopology:  
 assumes  $U$  {is a partition of}  $X$   
 shows  $\text{topology0}(\text{PTopology } X \ U)$   
*<proof>*

### 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  $\bigcup (\text{PTopology } X \ U) = X$   
*<proof>*

The closed sets are the open sets.

**lemma closed\_sets\_ptopology:**  
 assumes  $T$  {is a partition of}  $X$   
 shows  $D$  {is closed in}  $(\text{PTopology } X \ T) \iff D \in (\text{PTopology } X \ T)$   
*<proof>*

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}  $XA \subseteq X$   
 shows  $\text{Interior}(A, (\text{PTopology } X \ U)) = \bigcap \{T \in \text{DualBase } U \ (\text{PTopology } X \ U) . T = X \vee T \cup A \neq X\}$   
*<proof>*

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}  $XA \subseteq X$   
 shows  $\text{Closure}(A, (\text{PTopology } X \ U)) = \bigcup \{T \in U . T \cap A \neq \emptyset\}$   
*<proof>*

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}  $XA \subseteq X$   
 shows  $\text{Boundary}(A, (\text{PTopology } X \ U)) = \bigcup \{T \in U . T \cap A \neq \emptyset \wedge \sim(T \subseteq A)\}$   
*<proof>*

### 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  $\{\{x\} . x \in X\}$  {is a partition of}  $X$   
*<proof>*

**lemma indiscrete\_partition:**  
 assumes  $X \neq \emptyset$

**shows**  $\{X\}$  {is a partition of}  $X$   
*<proof>*

**theorem** discrete\_ptopology:  
**shows**  $(\text{PTopology } X \ \{\{x\}.x \in X\}) = \text{Pow}(X)$   
*<proof>*

**theorem** indiscrete\_ptopology:  
**assumes**  $X \neq 0$   
**shows**  $(\text{PTopology } X \ \{X\}) = \{0, X\}$   
*<proof>*

The topological subspaces of the  $\text{PTopology } X \ U$  are partition topologies.

**lemma** subspace\_ptopology:  
**assumes**  $U$ {is a partition of} $X$   
**shows**  $(\text{PTopology } X \ U) \ \{\text{restricted to}\} \ Y = (\text{PTopology } (X \cap Y) \ ((U \ \{\text{restricted to}\} \ Y) - \{0\}))$   
*<proof>*

## 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  $\text{Interval}$  is a closed interval; and open rays.

**definition**  
 $\text{Interval } X$  **where**  
 $\text{Interval } X(X, r, b, c) \equiv (\text{Interval}(r, b, c) \cap X) - \{b, c\}$

**definition**  
 $\text{LeftRay } X$  **where**  
 $\text{LeftRay } X(X, r, b) \equiv \{c \in X. \ \langle c, b \rangle \in r\} - \{b\}$

**definition**  
 $\text{RightRay } X$  **where**  
 $\text{RightRay } X(X, r, b) \equiv \{c \in X. \ \langle b, c \rangle \in r\} - \{b\}$

Intersections of intervals and rays.

**lemma** inter\_two\_intervals:  
**assumes**  $bu \in X, bv \in X, cu \in X, cv \in X, \text{IsLinOrder}(X, r)$   
**shows**  $\text{Interval } X(X, r, bu, cu) \cap \text{Interval } X(X, r, bv, cv) = \text{Interval } X(X, r, \text{GreaterOf}(r, bu, bv), \text{SmallerOf}(r, cu, cv))$   
*<proof>*

**lemma** inter\_rray\_interval:  
**assumes**  $bv \in X, bu \in X, cv \in X, \text{IsLinOrder}(X, r)$   
**shows**  $\text{RightRay } X(X, r, bu) \cap \text{Interval } X(X, r, bv, cv) = \text{Interval } X(X, r, \text{GreaterOf}(r, bu, bv), cv)$   
*<proof>*

**lemma** `inter_lray_interval`:  
 assumes  $bv \in X$   $cu \in X$   $cv \in X$   $\text{IsLinOrder}(X, r)$   
 shows  $\text{LeftRayX}(X, r, cu) \cap \text{IntervalX}(X, r, bv, cv) = \text{IntervalX}(X, r, bv, \text{SmallerOf}(r, cu, cv))$   
*<proof>*

**lemma** `inter_lray_rray`:  
 assumes  $bu \in X$   $cv \in X$   $\text{IsLinOrder}(X, r)$   
 shows  $\text{LeftRayX}(X, r, bu) \cap \text{RightRayX}(X, r, cv) = \text{IntervalX}(X, r, cv, bu)$   
*<proof>*

**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>*

**lemma** `inter_rray_rray`:  
 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>*

The open intervals and rays satisfy the base condition.

**lemma** `intervals_rays_base_condition`:  
 assumes  $\text{IsLinOrder}(X, r)$   
 shows  $\{\text{IntervalX}(X, r, b, c). \langle b, c \rangle \in X \times X\} \cup \{\text{LeftRayX}(X, r, b). b \in X\} \cup \{\text{RightRayX}(X, r, b). b \in X\}$  {satisfies the base condition}  
*<proof>*

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**  
 $\text{IsLinOrder}(X, r) \implies \text{OrdTopology } X \ r \equiv \text{TopologyBase } \{\text{IntervalX}(X, r, b, c). \langle b, c \rangle \in X \times X\} \cup \{\text{LeftRayX}(X, r, b). b \in X\} \cup \{\text{RightRayX}(X, r, b). b \in X\}$

**theorem** `Ordtopology_is_a_topology`:  
 assumes  $\text{IsLinOrder}(X, r)$   
 shows  $(\text{OrdTopology } X \ r)$  {is a topology} **and**  $\{\text{IntervalX}(X, r, b, c). \langle b, c \rangle \in X \times X\} \cup \{\text{LeftRayX}(X, r, b). b \in X\} \cup \{\text{RightRayX}(X, r, b). b \in X\}$  {is a base for}  $(\text{OrdTopology } X \ r)$   
*<proof>*

**lemma** `topology0_ordtopology`:  
 assumes  $\text{IsLinOrder}(X, r)$   
 shows  $\text{topology0}(\text{OrdTopology } X \ r)$   
*<proof>*

### 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)  $\exists x y. x \neq y \wedge x \in X \wedge y \in X$   
 shows  $\bigcup (\text{OrdTopology } X \text{ } r) = X$   
*<proof>*

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>*

**lemma** rightrays\_base\_condition:  
 assumes IsLinOrder(X,r)  
 shows {RightRayX(X,r,b).  $b \in X \cup \{X\}$  } {satisfies the base condition}  
*<proof>*

#### definition

LeftOrderTopology (LOrdTopology \_ \_ 50) **where**  
 $\text{IsLinOrder}(X,r) \implies \text{LOrdTopology } X \text{ } r \equiv \text{TopologyBase } \{\text{LeftRayX}(X,r,b). b \in X \cup \{X\}\}$

#### definition

RightOrderTopology (ROrdTopology \_ \_ 50) **where**  
 $\text{IsLinOrder}(X,r) \implies \text{ROrdTopology } X \text{ } r \equiv \text{TopologyBase } \{\text{RightRayX}(X,r,b). b \in X \cup \{X\}\}$

#### theorem LOrdtopology\_ROrdtopology\_are\_topologies:

assumes IsLinOrder(X,r)  
 shows (LOrdTopology X r) {is a topology} and {LeftRayX(X,r,b).  $b \in X \cup \{X\}$  }  
 {is a base for} (LOrdTopology X r)  
 and (ROrdTopology X r) {is a topology} and {RightRayX(X,r,b).  $b \in X \cup \{X\}$  }  
 {is a base for} (ROrdTopology X r)

*<proof>*

**lemma** topology0\_lordtopology\_rordtopology:  
  **assumes** IsLinOrder(X,r)  
  **shows** topology0(LOrdTopology X r) and topology0(ROrdTopology X r)  
*<proof>*

### 49.3.5 Total set

The topology is defined on the set  $X$

**lemma** union\_lordtopology\_rordtopology:  
  **assumes** IsLinOrder(X,r)  
  **shows**  $\bigcup (\text{LOrdTopology } X \text{ } r) = X$  and  $\bigcup (\text{ROrdTopology } X \text{ } r) = X$   
*<proof>*

## 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**  $\{\bigcap A. A \in \text{FinPow}(B)\}$  {satisfies the base condition}  
*<proof>*

**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>*

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**  $T = S$   
*<proof>*

**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 (*compact of cardinal*  $\kappa$ )  
**where**  $K$  *compact of cardinal*  $Q$   $\equiv$  ( $\text{Card}(Q) \wedge K \subseteq \bigcup T \wedge$   
 $(\forall M \in \text{Pow}(T). K \subseteq \bigcup M \longrightarrow (\exists N \in \text{Pow}(M). K \subseteq \bigcup N \wedge N \prec Q))$ )

The usual compact property is the one defined over the cardinal of the natural numbers.

**lemma** Compact\_is\_card\_nat:

**shows**  $K$  *compact in*  $T \iff (K$  *compact of cardinal*  $\text{nat}$  *in*  $T)$   
*<proof>*

Another property of this kind widely used is the Lindelof property; it is the one on the successor of the natural numbers.

**definition**

IsLindelof (*Lindelof in*  $\kappa$ ) **where**  
 $K$  *Lindelof in*  $T \equiv K$  *compact of cardinal*  $\text{csucc}(\text{nat})$  *in*  $T$

It would be natural to think that every countable set with any topology is Lindelof; 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*  $\kappa$  *choice holds for subsets*  $Q$ ) **where**  
*the axiom of*  $Q$  *choice holds for subsets*  $K \equiv \text{Card}(Q) \wedge (\forall M N. (M \lesssim Q \wedge$   
 $(\forall t \in M. \text{Nt} \neq 0 \wedge \text{Nt} \subseteq K)) \longrightarrow (\exists f. f: \text{Pi}(M, \lambda t. \text{Nt}) \wedge (\forall t \in M. ft \in \text{Nt})))$ )

**definition**

AxiomCardinalChoiceGen (*the axiom of*  $\kappa$  *choice holds*) **where**  
*the axiom of*  $Q$  *choice holds*  $\equiv \text{Card}(Q) \wedge (\forall M N. (M \lesssim Q \wedge (\forall t \in M.$   
 $\text{Nt} \neq 0)) \longrightarrow (\exists f. f: \text{Pi}(M, \lambda t. \text{Nt}) \wedge (\forall t \in M. ft \in \text{Nt})))$ )

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}  $\mathcal{Q}$  {choice holds}  $\iff$  (ALL  $K$ . {the axiom of}  $\mathcal{Q}$  {choice holds for subsets}  $K$ )  
*<proof>*

If a set is compact of cardinality  $\mathcal{Q}$  for some topology, it is compact of cardinality  $\mathcal{Q}$  for every coarser topology.

**theorem compact\_coarser:**  
 assumes  $T_1 \subseteq T$  and  $\bigcup T_1 = \bigcup T$  and  $(K)$  {is compact of cardinal}  $\mathcal{Q}$  {in}  $T$   
 shows  $(K)$  {is compact of cardinal}  $\mathcal{Q}$  {in}  $T_1$   
*<proof>*

A closed subspace of a compact space of any cardinality, is also compact of the same cardinality.

**theorem compact\_closed:**  
 assumes  $K$  {is compact of cardinal}  $\mathcal{Q}$  {in}  $T$   
 and  $R$  {is closed in}  $T$   
 shows  $(K \cap R)$  {is compact of cardinal}  $\mathcal{Q}$  {in}  $T$   
*<proof>*

## 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  
 $(T$  {is of first type of cardinal}  $\mathcal{Q}) \equiv \forall x \in \bigcup T. (\exists B. (B$  {is a base for}  $T) \wedge (\{b \in B. x \in b\} \prec \mathcal{Q}))$

**definition**  
 IsSecondOfCard ( $\_$  {is of second type of cardinal}  $\_ 90$ ) where  
 $(T$  {is of second type of cardinal}  $\mathcal{Q}) \equiv (\exists B. (B$  {is a base for}  $T) \wedge (B \prec \mathcal{Q}))$

**definition**  
 IsSeparableOfCard ( $\_$  {is separable of cardinal}  $\_ 90$ ) where  
 $T$  {is separable of cardinal}  $\mathcal{Q} \equiv \exists U \in \text{Pow}(\bigcup T). \text{Closure}(U, T) = \bigcup T \wedge U \prec \mathcal{Q}$

**definition**  
 IsFirstCountable ( $\_$  {is first countable}  $90$ ) where  
 $(T$  {is first countable})  $\equiv T$  {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}  $\text{csucc}(\text{nat}))$

**definition**  
 IsSeparable ( $\_$  {is separable}  $90$ ) where

$T\{\text{is separable}\} \equiv T\{\text{is separable of cardinality } \text{csucc}(\text{nat})\}$

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  $T\{\text{is of second type of cardinality } Q\}$   
 shows  $T\{\text{is of first type of cardinality } Q\}$   
*<proof>*

A set is dense iff it intersects all non-empty, open sets of the topology.

**lemma** `dense_int_open`:  
 assumes  $T\{\text{is a topology}\}$  and  $A \subseteq \bigcup T$   
 shows  $\text{Closure}(A, T) = \bigcup T \iff (\forall U \in T. U \neq \emptyset \implies A \cap U \neq \emptyset)$   
*<proof>*

### 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  $f: \text{surj}(A, B) \wedge A \subseteq \text{QOrd}(Q)$   
 shows  $B \lesssim A$   
*<proof>*

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  $f: \text{surj}(A, B) \wedge A \lesssim \text{QOrd}(Q)$   
 shows  $B \lesssim A$   
*<proof>*

### 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  $Q = \aleph_1$ , 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} $\text{csucc}(Q)$   
 and {the axiom of}  $Q$  {choice holds for subsets}  $\bigcup T$   
 and  $T$ {is a topology}  
 shows  $T$ {is separable of cardinal} $\text{csucc}(Q)$   
*<proof>*

The next theorem resolves that the axiom of  $Q$  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  $\forall T. (T$ {is a topology}  $\wedge (T$ {is of second type of cardinal} $\text{csucc}(Q))$ )  
 $\longrightarrow (T$ {is separable of cardinal} $\text{csucc}(Q))$   
 and  $\text{Card}(Q)$   
 shows {the axiom of}  $Q$  {choice holds}  
*<proof>*

Here is the equivalence from the two previous results.

**theorem** `Q_choice_eq_secon_imp_sepa`:  
 assumes  $\text{Card}(Q)$   
 shows  $(\forall T. (T$ {is a topology}  $\wedge (T$ {is of second type of cardinal} $\text{csucc}(Q))$ )  
 $\longrightarrow (T$ {is separable of cardinal} $\text{csucc}(Q))$ )  
 $\longleftrightarrow$ {the axiom of}  $Q$  {choice holds}  
*<proof>*

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  $B \lesssim_Q B$  {is a base for} $T$   
 shows  $\exists N. \{N_i. i \in Q\}$ {is a base for} $T$   
*<proof>*

### 50.3 Relation between numerability and compactness

If the axiom of  $Q$  choice holds, then any topology of second type of cardinal  $\text{csucc}(Q)$  is compact of cardinal  $\text{csucc}(Q)$

**theorem** `compact_of_cardinal_Q`:  
 assumes {the axiom of}  $Q$  {choice holds for subsets}  $(\text{Pow}(Q))$   
 $T$ {is of second type of cardinal} $\text{csucc}(Q)$   
 $T$ {is a topology}  
 shows  $((\bigcup T)$ {is compact of cardinal} $\text{csucc}(Q)$ {in} $T)$   
*<proof>*

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**  $\forall T. (T\{\text{is a topology}\} \wedge (T\{\text{is of second type of cardinal}\}\text{csucc}(Q)))$   
 $\longrightarrow ((\bigcup T)\{\text{is compact of cardinal}\}\text{csucc}(Q)\{\text{in}\}T)$   
**and**  $\text{InfCard}(Q)$   
**shows**  $\{\text{the axiom of}\} Q \{\text{choice holds for subsets}\} (\text{Pow}(Q))$   
*<proof>*

The two previous results, state the following equivalence:

**theorem**  $Q\_choice\_Pow\_eq\_secon\_imp\_comp$ :  
**assumes**  $\text{InfCard}(Q)$   
**shows**  $(\forall T. (T\{\text{is a topology}\} \wedge (T\{\text{is of second type of cardinal}\}\text{csucc}(Q))))$   
 $\longrightarrow ((\bigcup T)\{\text{is compact of cardinal}\}\text{csucc}(Q)\{\text{in}\}T)$   
 $\longleftrightarrow (\{\text{the axiom of}\} Q \{\text{choice holds for subsets}\} (\text{Pow}(Q)))$   
*<proof>*

In the next result we will prove that if the space  $(\kappa, \text{Pow}(\kappa))$ , 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**  $\text{InfCard}(Q) (Q)\{\text{is compact of cardinal}\}\text{csucc}(Q)\{\text{in}\}\text{Pow}(Q)$   
**shows**  $\forall T. (T\{\text{is a topology}\} \wedge (T\{\text{is of second type of cardinal}\}\text{csucc}(Q)))$   
 $\longrightarrow ((\bigcup T)\{\text{is compact of cardinal}\}\text{csucc}(Q)\{\text{in}\}T)$   
*<proof>*

**theorem**  $Q\_disc\_is\_second\_card\_csuccQ$ :  
**assumes**  $\text{InfCard}(Q)$   
**shows**  $\text{Pow}(Q)\{\text{is of second type of cardinal}\}\text{csucc}(Q)$   
*<proof>*

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**  $\text{InfCard}(Q)$   
**shows**  $(Q\{\text{is compact of cardinal}\}\text{csucc}(Q)\{\text{in}\}(\text{Pow}(Q))) \longleftrightarrow (\{\text{the axiom of}\}Q\{\text{choice holds for subsets}\}(\text{Pow}(Q)))$   
*<proof>*

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  $\aleph$ .

```
lemma (in topology0) T1_cocardinal_coarser:
  shows (T {is T1})  $\longleftrightarrow$  (Cofinite ( $\bigcup T$ ))  $\subseteq$  T  $\langle$ proof $\rangle$ 
```

Secondly, let's show that the CoCardinal  $\times$   $Q$  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  $\lesssim$  Q2
  shows (CoCardinal X Q1)  $\subseteq$  (CoCardinal X Q2)
 $\langle$ proof $\rangle$ 
```

```
corollary cocardinal_is_T1:
  fixes X
  assumes InfCard(K)
  shows (CoCardinal X K) {is T1}
 $\langle$ proof $\rangle$ 
```

In  $T_2$ -spaces, filters and nets have at most one limit point.

```
lemma (in topology0) T2_imp_unique_limit_filter:
  assumes T {is T2}  $\mathfrak{F}$  {is a filter on}  $\bigcup T$   $\mathfrak{F} \rightarrow F x$   $\mathfrak{F} \rightarrow F y$ 
  shows x=y
 $\langle$ proof $\rangle$ 
```

```
lemma (in topology0) T2_imp_unique_limit_net:
  assumes T {is T2} N {is a net on}  $\bigcup T$   $N \rightarrow N x$   $N \rightarrow N y$ 
  shows x=y
 $\langle$ proof $\rangle$ 
```

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  $\forall x \in \bigcup T. \forall y \in \bigcup T. \forall \mathfrak{F}. ((\mathfrak{F} \text{ {is a filter on}} \bigcup T) \wedge (\mathfrak{F} \rightarrow F x) \wedge (\mathfrak{F} \rightarrow F y)) \longrightarrow x=y$ 
  shows T {is T2}
 $\langle$ proof $\rangle$ 
```

```
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>*

This results make easy to check if a space is  $T_2$ .

The topology which comes from a filter as in  $\mathfrak{F} \text{ is a filter on } \bigcup \mathfrak{F} \implies (\mathfrak{F} \cup \{0\}) \text{ is a topology}$  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**  $(\mathfrak{F} \cup \{0\}) \text{ is } T_2$   $\mathfrak{F} \text{ is a filter on } \bigcup \mathfrak{F}$   $x \in \bigcup \mathfrak{F}$   
**shows**  $\bigcup \mathfrak{F} = \{x\}$   
*<proof>*

There are more separation axioms that just  $T_0$ ,  $T_1$  or  $T_2$

**definition**  
`IsRegular` ( $\_ \text{is regular}$ ) 90  
**where**  $T \text{ is regular} \equiv \forall A. A \text{ is closed in } T \longrightarrow (\forall x \in \bigcup T - A. \exists U \in T. \exists V \in T. A \subseteq U \wedge x \in V \wedge U \cap V = 0)$

**definition**  
`isT3` ( $\_ \text{is } T_3$ ) 90  
**where**  $T \text{ is } T_3 \equiv (T \text{ is } T_1) \wedge (T \text{ is regular})$

**definition**  
`IsNormal` ( $\_ \text{is normal}$ ) 90  
**where**  $T \text{ is normal} \equiv \forall A. A \text{ is closed in } T \longrightarrow (\forall B. B \text{ is closed in } T \wedge A \cap B = 0 \longrightarrow (\exists U \in T. \exists V \in T. A \subseteq U \wedge B \subseteq V \wedge U \cap V = 0))$

**definition**  
`isT4` ( $\_ \text{is } T_4$ ) 90  
**where**  $T \text{ is } T_4 \equiv (T \text{ is } T_1) \wedge (T \text{ is normal})$

**lemma** (`in topology0`) `T4_is_T3`:  
**assumes**  $T \text{ is } T_4$  **shows**  $T \text{ is } T_3$   
*<proof>*

**lemma** (`in topology0`) `T3_is_T2`:  
**assumes**  $T \text{ is } T_3$  **shows**  $T \text{ is } T_2$   
*<proof>*

### 51.1.1 Hereditability

A topological property is hereditary if whenever a space has it, every subspace also has it.

**definition** `IsHer` ( $\_ \text{is hereditary}$ ) 90

where  $P \text{ \{is hereditary\}} \equiv \forall T. T \text{ \{is a topology\}} \wedge P(T) \longrightarrow (\forall A \in \text{Pow}(\bigcup T). P(T \text{ \{restricted to\}} A))$

**lemma** `subspace_of_subspace`:

`assumes`  $A \subseteq B \subseteq \bigcup T$

`shows`  $T \text{ \{restricted to\}} A = (T \text{ \{restricted to\}} B) \text{ \{restricted to\}} A$

*\langle proof \rangle*

The separation properties  $T_0$ ,  $T_1$ ,  $T_2$  y  $T_3$  are hereditary.

**theorem** `regular_here`:

`assumes`  $T \text{ \{is regular\}} A \in \text{Pow}(\bigcup T)$  `shows`  $(T \text{ \{restricted to\}} A) \text{ \{is regular\}}$

*\langle proof \rangle*

**corollary** `here_regular`:

`shows` `IsRegular` `\{is hereditary\}` *\langle proof \rangle*

**theorem** `T1_here`:

`assumes`  $T \text{ \{is } T_1\}} A \in \text{Pow}(\bigcup T)$  `shows`  $(T \text{ \{restricted to\}} A) \text{ \{is } T_1\}}$

*\langle proof \rangle*

**corollary** `here_T1`:

`shows` `isT1` `\{is hereditary\}` *\langle proof \rangle*

**lemma** `here_and`:

`assumes`  $P \text{ \{is hereditary\}} Q \text{ \{is hereditary\}}$

`shows`  $(\lambda T. P(T) \wedge Q(T)) \text{ \{is hereditary\}}$  *\langle proof \rangle*

**corollary** `here_T3`:

`shows` `isT3` `\{is hereditary\}` *\langle proof \rangle*

**lemma** `T2_here`:

`assumes`  $T \text{ \{is } T_2\}} A \in \text{Pow}(\bigcup T)$  `shows`  $(T \text{ \{restricted to\}} A) \text{ \{is } T_2\}}$

*\langle proof \rangle*

**corollary** `here_T2`:

`shows` `isT2` `\{is hereditary\}` *\langle proof \rangle*

**lemma** `T0_here`:

`assumes`  $T \text{ \{is } T_0\}} A \in \text{Pow}(\bigcup T)$  `shows`  $(T \text{ \{restricted to\}} A) \text{ \{is } T_0\}}$

*\langle proof \rangle*

**corollary** `here_T0`:

`shows` `isT0` `\{is hereditary\}` *\langle proof \rangle*

## 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) ≡ ∀T. ((T{is a topology} ∧ ∪T≈K) → P(T))`

**lemma** `equipollent_spect`:  
 assumes `A≈B` `B` {is in the spectrum of} `P`  
 shows `A` {is in the spectrum of} `P`  
`<proof>`

**theorem** `eqpoll_iff_spec`:  
 assumes `A≈B`  
 shows `(B` {is in the spectrum of} `P) ↔ (A` {is in the spectrum of} `P)` `<proof>`

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) ↔ A ≲ 1`  
`<proof>`

If the topological properties are related, then so are the spectra.

**lemma** `P_imp_Q_spec_inv`:  
 assumes `∀T. T{is a topology} → (Q(T) → P(T))` `A` {is in the spectrum of} `Q`  
 shows `A` {is in the spectrum of} `P`  
`<proof>`

Since we already now the spectrum of `T4`; if we now the spectrum of `T0`, it should be easier to compute the spectrum of `T1`, `T2` and `T3`.

**theorem** `T0_spectrum`:  
 shows `(A` {is in the spectrum of} `isT0) ↔ A ≲ 1`  
`<proof>`

**theorem** `T1_spectrum`:  
 shows `(A` {is in the spectrum of} `isT1) ↔ A ≲ 1`  
`<proof>`

**theorem** T2\_spectrum:  
 shows (A {is in the spectrum of} isT2)  $\longleftrightarrow$   $A \lesssim 1$   
*<proof>*

**theorem** T3\_spectrum:  
 shows (A {is in the spectrum of} isT3)  $\longleftrightarrow$   $A \lesssim 1$   
*<proof>*

**theorem** compact\_spectrum:  
 shows (A {is in the spectrum of}  $(\lambda T. (\bigcup T) \text{ {is compact in} } T)) \longleftrightarrow$   
 Finite(A)  
*<proof>*

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}  $(\lambda T. ((\bigcup T) \text{ {is compact of cardinal} } csucc(K) \text{ {in} } T))) \longleftrightarrow (A \lesssim K)$   
*<proof>*

**theorem** compactK\_spectrum\_reverse:  
 assumes  $\forall A. (A \text{ {is in the spectrum of} } (\lambda T. ((\bigcup T) \text{ {is compact of cardinal} } csucc(K) \text{ {in} } T))) \longleftrightarrow (A \lesssim K) \text{ InfCard}(K)$   
 shows {the axiom of}K{choice holds for subsets}(Pow(K))  
*<proof>*

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 ( $\_ \text{ {is anti-} } \_ 50$ )  
 where  $T \text{ {is anti-} } P \equiv \forall A \in \text{Pow}(\bigcup T). P(T \text{ {restricted to} } A) \longrightarrow (A \text{ {is in the spectrum of} } P)$

**abbreviation**  
 ANTI(P)  $\equiv \lambda T. (T \text{ {is anti-} } P)$

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**  $\forall T. T\{\text{is a topology}\} \longrightarrow P(T) \longrightarrow Q(T) \forall A. (A\{\text{is in the spectrum of}\}Q) \longrightarrow (A\{\text{is in the spectrum of}\}P)$   
**and**  $T\{\text{is anti-}\}Q$   
**shows**  $T\{\text{is anti-}\}P$   
*<proof>*

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**  $Q\{\text{is hereditary}\}$   
**shows**  $\forall T. T\{\text{is a topology}\} \longrightarrow (Q(T) \longrightarrow (T\{\text{is anti-}\}P))$   
*<proof>*

**theorem** (in topology0)  $her\_P\_imp\_anti2P$ :  
**assumes**  $P\{\text{is hereditary}\} P(T)$   
**shows**  $T\{\text{is anti-}\}\text{ANTI}(P)$   
*<proof>*

The anti-properties are always hereditary

**theorem**  $anti\_here$ :  
**shows**  $\text{ANTI}(P)\{\text{is hereditary}\}$   
*<proof>*

**corollary** (in topology0)  $anti\_imp\_anti3$ :  
**assumes**  $T\{\text{is anti-}\}P$   
**shows**  $T\{\text{is anti-}\}\text{ANTI}(\text{ANTI}(P))$   
*<proof>*

In the article [5], we can find some results on anti-properties.

**theorem** (in topology0)  $anti\_T0$ :  
**shows**  $(T\{\text{is anti-}\}\text{is}T0) \longleftrightarrow T=\{0, \bigcup T\}$   
*<proof>*

**lemma**  $indiscrete\_spectrum$ :  
**shows**  $(A \{\text{is in the spectrum of}\}(\lambda T. T=\{0, \bigcup T\})) \longleftrightarrow A \lesssim 1$   
*<proof>*

**theorem** (in topology0)  $anti\_indiscrete$ :  
**shows**  $(T\{\text{is anti-}\}(\lambda T. T=\{0, \bigcup T\})) \longleftrightarrow T\{\text{is } T_0\}$   
*<proof>*

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{is anti-}isT1)  $\longleftrightarrow$  (IsLinOrder(T, { $\langle U, V \rangle \in \text{Pow}(\bigcup T) \times \text{Pow}(\bigcup T) . U \subseteq V$ }))  
  *<proof>*

**corollary** linordtop\_here:

**shows** ( $\lambda T . \text{IsLinOrder}(T, \{\langle U, V \rangle \in \text{Pow}(\bigcup T) \times \text{Pow}(\bigcup T) . U \subseteq V\})$ ){is hereditary}  
  *<proof>*

**theorem** (in topology0) anti\_T4:

**shows** (T{is anti-}isT4)  $\longleftrightarrow$  (IsLinOrder(T, { $\langle U, V \rangle \in \text{Pow}(\bigcup T) \times \text{Pow}(\bigcup T) . U \subseteq V$ }))  
  *<proof>*

**theorem** (in topology0) anti\_T3:

**shows** (T{is anti-}isT3)  $\longleftrightarrow$  (IsLinOrder(T, { $\langle U, V \rangle \in \text{Pow}(\bigcup T) \times \text{Pow}(\bigcup T) . U \subseteq V$ }))  
  *<proof>*

**theorem** (in topology0) anti\_T2:

**shows** (T{is anti-}isT2)  $\longleftrightarrow$  (IsLinOrder(T, { $\langle U, V \rangle \in \text{Pow}(\bigcup T) \times \text{Pow}(\bigcup T) . U \subseteq V$ }))  
  *<proof>*

**lemma** linord\_spectrum:

**shows** (A{is in the spectrum of})( $\lambda T . \text{IsLinOrder}(T, \{\langle U, V \rangle \in \text{Pow}(\bigcup T) \times \text{Pow}(\bigcup T) . U \subseteq V\})$ )  $\longleftrightarrow A \lesssim 1$   
  *<proof>*

**theorem** (in topology0) anti\_linord:

**shows** (T{is anti-})( $\lambda T . \text{IsLinOrder}(T, \{\langle U, V \rangle \in \text{Pow}(\bigcup T) \times \text{Pow}(\bigcup T) . U \subseteq V\})$ )  
   $\longleftrightarrow T\{\text{is } T_1\}$   
  *<proof>*

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>
```

### 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( $\tau_1, \tau_2, f$ )  $f \in (\bigcup \tau_1) \rightarrow (\bigcup \tau_2)$   $x \in \bigcup \tau_1$ 
  shows  $\forall U \in \tau_2. fx \in U \implies (\exists V \in \tau_1. x \in V \wedge fV \subseteq U)$ 
  <proof>
```

**lemma** ccontinuous\_all\_x\_imp\_cont\_global:

```
  assumes  $\forall x \in \bigcup \tau_1. \forall U \in \tau_2. fx \in U \implies (\exists V \in \tau_1. x \in V \wedge fV \subseteq U)$   $f \in (\bigcup \tau_1) \rightarrow (\bigcup \tau_2)$ 
   $\tau_1$  {is a topology}
  shows IsContinuous( $\tau_1, \tau_2, f$ )
  <proof>
```

### 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>

lemma (in two_top_spaces0) filter_conver_preserved_imp_cont:
  assumes  $\forall x \in \bigcup \tau_1. \forall \mathcal{F}. ((\mathcal{F} \text{ {is a filter on} } X_1) \wedge (\mathcal{F} \rightarrow F x \text{ {in} } \tau_1))$ 
   $\rightarrow ((f[\mathcal{F}]..X_2) \rightarrow F (fx) \text{ {in} } \tau_2)$ 
  shows  $f$ {is continuous}
  <proof>

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}
  <proof>
```

The anti-property of connectedness is called total-disconnectedness.

```
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>
```

The discrete space is a first example of totally-disconnected space.

```
lemma discrete_tot_dis:
  shows Pow(X) {is totally-disconnected}
  <proof>
```

An space is hyperconnected iff every two non-empty open sets meet.

```
definition IsHConnected (_{is hyperconnected}90)
  where T{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{is hyperconnected}
  shows T{is connected}
  <proof>
```

```
lemma Indiscrete_HConn:
  shows {0,X}{is hyperconnected}
  <proof>
```

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>*

**lemma** HConn\_spectrum:  
 shows (A{is in the spectrum of}IsHConnected)  $\longleftrightarrow$   $A \lesssim 1$   
*<proof>*

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>*

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  $T_1$ }  
*<proof>*

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 ( $\_$ {is sober}90)  
 where T{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{is anti-}IsHConnected  
 shows T{is sober}  
*<proof>*

Every sober space is  $T_0$ .

**lemma** (in topology0) sober\_imp\_T0:  
 assumes T{is sober}  
 shows T{is  $T_0$ }  
*<proof>*

Every  $T_2$  space is anti-hyperconnected.

**theorem** (in topology0) T2\_imp\_anti\_HConn:  
 assumes T{is T<sub>2</sub>}  
 shows T{is anti-}IsHConnected  
*<proof>*

Every anti-hyperconnected space is  $T_1$ .

**theorem** anti\_HConn\_imp\_T1:  
 assumes T{is anti-}IsHConnected  
 shows T{is T<sub>1</sub>}  
*<proof>*

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 ¬((CoFinite nat){is anti-}IsHConnected) and (CoFinite nat){is T<sub>1</sub>}  
*<proof>*

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>*

The previous topology is not  $T_2$ , but is anti-hyperconnected.

**theorem** join\_Cofinite\_ExclPoint\_not\_T2:  
 shows ¬((joinT {CoFinite nat, ExcludedSet nat {0,1}}){is T<sub>2</sub>}) and (joinT  
 {CoFinite nat, ExcludedSet nat {0,1}}){is anti-}IsHConnected  
*<proof>*

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<sub>1</sub>} and T{is sober}  
 shows T{is anti-}IsHConnected  
*<proof>*

**theorem** (in topology0) anti\_HConn\_iff\_T1\_sober:  
 shows (T{is anti-}IsHConnected)  $\longleftrightarrow$  (T{is sober}∧T{is T<sub>1</sub>})  
*<proof>*

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>`

Every ultraconnected space is connected.

**lemma** `UConn_imp_Conn`:  
 assumes `T`{is ultraconnected}  
 shows `T`{is connected}  
`<proof>`

**lemma** `UConn_spectrum`:  
 shows `(A`{is in the spectrum of}`)IsUConnected`  $\longleftrightarrow A \lesssim 1$   
`<proof>`

This time, anti-ultraconnected is an old property.

**theorem** `(in topology0) anti_UConn`:  
 shows `(T`{is anti-}`)IsUConnected`  $\longleftrightarrow T{is  $T_1$ }  
`<proof>`$

It 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`{is in the spectrum of}`)IsSober`  $\longleftrightarrow A \lesssim 1$   
`<proof>`

**theorem** `(in topology0)anti_sober`:  
 shows `(T`{is anti-}`)IsSober`  $\longleftrightarrow T = \{0, \bigcup T\}$   
`<proof>`

**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,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]:  $\mathbf{0} \equiv \text{TheNeutralElement}(G,f)$ 

fixes zerohoods ( $\mathcal{N}_0$ )
defines zerohoods_def [simp]:  $\mathcal{N}_0 \equiv \{A \in \text{Pow}(G). \mathbf{0} \in \text{int}(A)\}$ 

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)  
*<proof>*

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)  
*<proof>*

We can use the `group0` locale in the context of `topgroup`.

**lemma** (in topgroup) group0\_valid\_in\_tgroup: **shows** group0(G,f)  
*<proof>*

We can use `semigr0` locale in the context of `topgroup`.

**lemma** (in topgroup) semigr0\_valid\_in\_tgroup: **shows** semigr0(G,f)  
*<proof>*

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)  
*<proof>*

Negative of a group element is in group.

**lemma** (in topgroup) neg\_in\_tgroup: **assumes**  $g \in G$  **shows**  $(-g) \in G$   
*<proof>*

Zero is in the group.

**lemma** (in topgroup) zero\_in\_tgroup: **shows**  $0 \in G$   
*<proof>*

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  $\bigcup \tau = G \times G$   
*<proof>*

Let's recall that  $f$  is a binary operation on  $G$  in this context.

**lemma** (in topgroup) topgroup\_f\_binop: **shows**  $f : G \times G \rightarrow G$   
*<proof>*

A subgroup of a topological group is a topological group with relative topology and restricted operation. Relative topology is the same as `T {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>*

## 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  $A \subseteq G$   $B \subseteq G$  shows  
 $A+B \subseteq G$  and  $A+B = f(A \times B)$   $A+B = (\bigcup_{x \in A}. x+B)$   
*<proof>*

Right and left translations are continuous.

**lemma** (in topgroup) trans\_cont: assumes  $g \in G$  shows  
 $\text{IsContinuous}(T, T, \text{RightTranslation}(G, f, g))$  and  
 $\text{IsContinuous}(T, T, \text{LeftTranslation}(G, f, g))$   
*<proof>*

Left and right translations of an open set are open.

**lemma** (in topgroup) open\_tr\_open: assumes  $g \in G$  and  $V \in T$   
shows  $g+V \in T$  and  $V+g \in T$   
*<proof>*

Right and left translations are homeomorphisms.

**lemma** (in topgroup) tr\_homeo: assumes  $g \in G$  shows  
 $\text{IsAhomeomorphism}(T, T, \text{RightTranslation}(G, f, g))$  and  
 $\text{IsAhomeomorphism}(T, T, \text{LeftTranslation}(G, f, g))$   
*<proof>*

Translations preserve interior.

**lemma** (in topgroup) trans\_interior: assumes  $A_1: g \in G$  and  $A_2: A \subseteq G$   
shows  $g + \text{int}(A) = \text{int}(g+A)$   
*<proof>*

Inverse of an open set is open.

**lemma** (in topgroup) open\_inv\_open: assumes  $V \in T$  shows  $(-V) \in T$   
*<proof>*

Inverse is a homeomorphism.

**lemma** (in topgroup) inv\_homeo: shows  $\text{IsAhomeomorphism}(T, T, \text{GroupInv}(G, f))$   
*<proof>*

Taking negative preserves interior.

**lemma** (in topgroup) int\_inv\_inv\_int: assumes  $A \subseteq G$   
shows  $\text{int}(-A) = -(\text{int}(A))$   
*<proof>*

### 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 space is a neighborhood of zero.

**lemma** (in topgroup) zneigh\_not\_empty: shows  $G \in \mathcal{N}_0$   
*<proof>*

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>*

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>*

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>*

## 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>*

The next theorem provides a characterization of closure in topological groups in terms of neighborhoods of zero.

**theorem** (in topgroup) cl\_topgroup:  
 assumes  $A \subseteq G$  shows  $\text{cl}(A) = (\bigcap_{H \in \mathcal{N}_0} A+H)$   
*<proof>*

## 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⟩

```

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 ⟨proof⟩

```

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⟩

```

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⟩
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>
```

```
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](http://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 `C` and `{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  $\mathbb{R} \cap \{+\infty, -\infty\} = 0$   
<proof>
```

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>
```

Metamath defines the usual  $<$  and  $\leq$  ordering relations for the extended real line, including  $+\infty$  and  $-\infty$ .

**lemma** (in complex0) xrrebndt: **assumes** A1:  $x \in \mathbb{R}^*$   
**shows**  $x \in \mathbb{R} \iff (-\infty < x \wedge x < +\infty)$   
*<proof>*

A quite involved inequality.

**lemma** (in complex0) lt2mul2divt:  
**assumes** A1:  $a \in \mathbb{R} \quad b \in \mathbb{R} \quad c \in \mathbb{R} \quad d \in \mathbb{R}$  **and**  
A2:  $0 < b \quad 0 < d$   
**shows**  $a \cdot b < c \cdot d \iff a/d < c/b$   
*<proof>*

A real number is smaller than its half iff it is positive.

**lemma** (in complex0) halfpos: **assumes** A1:  $a \in \mathbb{R}$   
**shows**  $0 < a \iff a/2 < a$   
*<proof>*

One more inequality.

**lemma** (in complex0) ledivp1t:  
**assumes** A1:  $a \in \mathbb{R} \quad b \in \mathbb{R}$  **and**  
A2:  $0 \leq a \quad 0 \leq b$   
**shows**  $(a/(b + 1)) \cdot b \leq a$   
*<proof>*

## 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:  $n \in \mathbb{N} \quad k \in \mathbb{N}$   
**shows**  
 $n \leq k \iff n < k + 1$   
 $n < k \iff n + 1 \leq k$   
*<proof>*

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:  $\psi(1)$  **and**  
A2:  $\forall k \in \mathbb{N}. \psi(k) \implies \psi(k+1)$  **and**

A3:  $n \in \mathbb{N}$   
**shows**  $\psi(n)$   
*<proof>*

Some simple arithmetics.

**lemma** (in complex0) arith: **shows**  
 $2 + 2 = 4$   
 $2 \cdot 2 = 4$   
 $3 \cdot 2 = 6$   
 $3 \cdot 3 = 9$   
*<proof>*

### 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>*

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>*

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>*

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**  
 $\text{Infim}(A, \mathbb{R}, <) \in \mathbb{R}$   
 $\text{Infim}(A, \mathbb{R}, <) = ( -\text{Sup}(\{z \in \mathbb{R}. (-z) \in A \}, \mathbb{R}, <) )$   
*<proof>*

**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.