

## 7 Group\_ZF\_1.thy

```
theory Group_ZF_1 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 "." 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

### 7.1 An alternative definition of group

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]:  $a \cdot b \equiv P\langle a, b \rangle$

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 -
  from A1 obtain a where D1:  $a \in G$  by auto
  with A3 obtain x where D2:  $x \in G$  and D3:  $a \cdot x = a$ 
    by auto
  from D1 A4 obtain y where D4:  $y \in G$  and D5:  $y \cdot a = a$ 
    by auto
  have T1:  $\forall b \in G. b = b \cdot x \wedge b = y \cdot b$ 
proof
  fix b assume A5:  $b \in G$ 
    with D1 A4 obtain  $y_b$  where D6:  $y_b \in G$ 
      and D7:  $y_b \cdot a = b$  by auto
    from A5 D1 A3 obtain  $x_b$  where D8:  $x_b \in G$ 
      and D9:  $a \cdot x_b = b$  by auto
    from D7 D3 D9 D5 have
       $b = y_b \cdot (a \cdot x)$   $b = (y \cdot a) \cdot x_b$  by auto
    moreover from D1 D2 D4 D8 D6 A2 have
       $(y \cdot a) \cdot x_b = y \cdot (a \cdot x_b)$   $y_b \cdot (a \cdot x) = (y_b \cdot a) \cdot x$ 
      using IsAssociative_def by auto
    moreover from D7 D9 have
       $(y_b \cdot a) \cdot x = b \cdot x$   $y \cdot (a \cdot x_b) = y \cdot b$ 
      by auto
    ultimately show  $b = b \cdot x \wedge b = y \cdot b$  by simp
  qed
moreover have  $x = y$ 
proof -
  from D2 T1 have  $x = y \cdot x$  by simp
  also from D4 T1 have  $y \cdot x = y$  by simp
  finally show  $x = y$  by simp
qed
ultimately have  $\forall b \in G. b \cdot x = b \wedge x \cdot b = b$  by simp
with D2 A2 have IsAmonoid( $G, P$ ) using IsAmonoid_def by auto
with A3 show IsAgroup( $G, P$ )
  using monoid0_def monoid0.unit_is_neutral IsAgroup_def
  by simp
qed

```

The converse of altgroup\_is\_group: in every (classically defined) group condition C holds. In informal mathematics we can say "Obviously condition C holds in any group." In formalized mathematics the word "obviously" is not in the language. The next theorem is proven in the context called group0

defined in the theory `Group_ZF.thy`. Similarly to the `group2` that context defines  $a \cdot b$  as  $P\langle a, b \rangle$  It also defines notation related to the group inverse and adds an assumption that the pair  $(G, P)$  is a group to all its theorems. This is why in the next theorem we don't explicitly assume that  $(G, P)$  is a group - this assumption is implicit in the context.

```

theorem (in group0) group_is_altgroup: shows
   $\forall a \in G. \forall b \in G. \exists x \in G. a \cdot x = b$  and  $\forall a \in G. \forall b \in G. \exists y \in G. y \cdot a = b$ 
proof -
  { fix a b assume A2:  $a \in G$   $b \in G$ 
    let x =  $a^{-1} \cdot b$ 
    let y =  $b \cdot a^{-1}$ 
    from A2 have
       $x \in G$   $y \in G$  and  $a \cdot x = b$   $y \cdot a = b$ 
      using inverse_in_group group_op_closed inv_cancel_two
      by auto
    hence  $\exists x \in G. a \cdot x = b$  and  $\exists y \in G. y \cdot a = b$  by auto
  } thus
     $\forall a \in G. \forall b \in G. \exists x \in G. a \cdot x = b$  and
     $\forall a \in G. \forall b \in G. \exists y \in G. y \cdot a = b$ 
    by auto
qed

end

```