Groups – minimal axiomatisation

Definition 1 (Group (informal))**.**

A **group** is a set equipped with an *associative binary operation*, for that exists a *right-neutral element*, and for any element a *right-inverse*.

For convenience I will use a rather large non-logical[1] signature, i.e. $\langle e, \circ, ^{-1} \rangle$, where '$e$' is a constant (or 0-ary function symbol), '$\circ$' is a binary function symbol (using the usual infix-notation rather then prefix), and '$^{-1}$' is a unary function symbol (as a postfix-operator, as is usual for this symbol); further the convention, that the binding strength of '$^{-1}$' is greater than that of '$\circ$' is employed.[2] Then we get the following three axioms:

Definition 2 (Group (axiomatic))**.**

In the language of groups with the signature explained above we have the following axioms:

1. $(\forall x.\forall y.\forall z.(x \circ y) \circ z = x \circ (y \circ z))$
2. $(\forall x.x \circ e = x)$
3. $(\forall x.x \circ x^{-1} = e)$

Lemma 1.
In a group any element a for which we have $a \circ a = a$ is the right-neutral element.

Proof. $a = a \circ e = a \circ (a \circ a^{-1}) = (a \circ a) \circ a^{-1} = a \circ a^{-1} = e$ □

Theorem 1.
In a group the right-neutral element is also the unique neutral element, and a right-inverse is also left-inverse, i.e. inverse; for any element there is exactly one inverse element.

Proof. Firstly, we show that the right-inverse $b := a^{-1}$ for an arbitrary element a is also left-inverse, by using associativity and – in the very last step – Lemma 1:

$$(b \circ a) \circ (b \circ a) = b \circ (a \circ (b \circ a)) = b \circ ((a \circ b) \circ a) = b \circ (e \circ a) = (b \circ e) \circ a = b \circ a = e$$

Then, further employing our convention $b := a^{-1}$ and last result $a \circ b = b \circ a$ we show, that the right-neutral is also left-neutral:

$$a = a \circ e = a \circ (a \circ b) = a \circ (b \circ a) = (a \circ b) \circ a = e \circ a$$

To prove uniqueness of the neutral element, assume that e' is a(nother) left-neutral one: $e' = e' \circ e = e$. In particular, a neutral element is automatically unique!

To prove uniqueness of the inverse element assume that b' is a(nother) left-inverse to a.

$$b' = b' \circ e = b' \circ (a \circ b) = (b' \circ a) \circ b = e \circ b = b$$

Again, in particular, inverse elements are automatically unique (which is also true in monoids for those element who have inverses). □

[1] The logical signature will contain, amongst symbols for the boolean connectives and quantifiers especially identity!

[2] Of course, the situation is different, if one sticks to the formal setup given in the lecture: using prefix notation with fixed arity is akin to Polish notation one can dispense with brackets and binding strength.