1. The Axioms

A **binary operation** on a set is a correspondence that assigns to each ordered pair of elements of the set a uniquely determined element of the set. For example addition is a binary operation on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\{0\}$, and multiplication is a binary operation on $\mathbb{Q}$, $\mathbb{Q}^*$, $\mathbb{N}$, $\mathbb{Z}$, $\{-1,1\}$, and $\{0,1\}$; on the other hand, addition is neither a binary operation on $\{-1,1\}$ nor on $\{0,1\}$. Why?

A set G together with some binary operation, say "$\circ$" is a **group**, if the following axioms are satisfied:

(A0) For any $a,b,c \in G$ we have:

$$a \circ (b \circ c) = (a \circ b) \circ c\,.$$

This says that the operation "$\circ$" is **associative**.

(A1) There is an element $e \in G$ such that for all $a \in G$ we have:

$$e \circ a = a \circ e = a\,.$$

The element e is called a **neutral element** of $(G, \circ)$.

(A2) If e is a neutral element of $(G, \circ)$, then for each $a \in G$ there is an $\bar{a} \in G$ such that

$$a \circ \bar{a} = \bar{a} \circ a = e\,.$$

The element $\bar{a}$ is called an **inverse** of a.

Any binary operation on some set which satisfies (A0) is called associative. It is a consequence of (A0) that we can omit brackets. In particular, whenever "$\circ$" is a binary associative operation on some set S, then for any $a,b,c,d \in S$ we have (see Hw1.Q2):

$$(a \circ b) \circ (c \circ d) = \big(a \circ (b \circ c)\big) \circ d\,.$$

On the other, a binary operation must not be associative (see Hw1.Q3).

A binary operation "$\circ$" on some set S is called **commutative** if for all $x,y \in S$ we have

$$x \circ y = y \circ x\,.$$

Definition. A group $(G, \circ)$ is called **abelian**, if the binary operation "$\circ$" is commutative.

For example $(\mathbb{Z},+)$, $(\mathbb{Q}^*, \cdot)$, $\big(\{0\},+\big)$ and $\big(\{-1,1\}, \cdot\big)$ are abelian groups. On the other hand, as we will see later, not every group is abelian.

Let us now show that the neutral element of a group is unique and that each element has exactly one inverse.

Proposition 1.1. Let $(G, \circ)$ be a group, then there is exactly one neutral element and each element of G has exactly one inverse.

Proof. Let $e, \tilde{e} \in G$ be neutral elements of $(G, \circ)$. Thus, for every $x \in G$ we have $x \circ \tilde{e} = e \circ x = x$, and therefore,

$$e \underset{\substack{\uparrow \\ \tilde{e}\text{ neutral}}}{=} e \circ \tilde{e} \underset{\substack{\uparrow \\ e\text{ neutral}}}{=} \tilde{e}\,,$$

and hence, there is exactly one neutral element.

Let $a \in G$ be arbitrary and let $x, \tilde{x} \in G$ be such that $a \circ x = \tilde{x} \circ a = e$, where $e \in G$ is the unique neutral element of $(G, \circ)$. Now,

$$\tilde{x} \underset{\substack{\uparrow \\ e\text{ neutral}}}{=} \tilde{x} \circ e = \tilde{x} \circ (a \circ x) \underset{\substack{\uparrow \\ \text{“}\circ\text{” is associative}}}{=} (\tilde{x} \circ a) \circ x = e \circ x \underset{\substack{\uparrow \\ e\text{ neutral}}}{=} x\,,$$

and hence, a has exactly one inverse, and since $a \in G$ was arbitrary, this completes the proof. ⊣

Notation. For an “abstract” group we often write just G and instead of $(G, \circ)$, and for $a, b \in G$ we often write just ab instead of $a \circ b$. In other words, if the binary operation is not specified, we handle it like multiplication, and consequently, we usually denote the inverse of $a \in G$ by a^{-1}. Notice that in general, $(ab)^{-1} = b^{-1} a^{-1}$.

We can weaken the axioms (A1) and (A2) a little bit:

Proposition 1.2. G is a group if the following axioms hold:

(A0) The binary operation is associative.

(A1*) There is an element $e \in G$ such that for all $a \in G$ we have:

$$ea = a\,.$$

The element e is called a **left-neutral element** of G.

(A2*) If e is a left-neutral element of G, then for each $a \in G$ there is an $\bar{a} \in G$ such that

$$\bar{a}a = e\,.$$

The element $\bar{a}$ is called **left-inverse** of a.

Proof. We have to prove that e is also a right-neutral element of G and that $\bar{a}$ is also a right-inverse of a.

Let $a \in G$ be arbitrary and let $\bar{\bar{a}}$ be a left-inverse of $\bar{a}$, where $\bar{a}$ is a left-inverse of a. Now we have:

$$a\bar{a} \underset{\substack{\uparrow \\ e\text{ left-neutral}}}{=} e(a\bar{a}) = (\bar{\bar{a}}\bar{a})(a\bar{a}) \underset{\substack{\uparrow \\ \text{by associativity}}}{=} \bar{\bar{a}}\overbrace{(\bar{a}a)}^{e}\bar{a} = \bar{\bar{a}}\overbrace{(e\bar{a})}^{\bar{a}} = \bar{\bar{a}}\bar{a} = e\,.$$

Thus, $a\bar{a} = \bar{a}a = e$, which shows that each left-inverse of some $a \in G$ is also a right-inverse, hence an inverse of a.

Further, we have:

$$ae = a(\bar{a}a) \underset{\substack{\uparrow \\ \text{by associativity}}}{=} \overbrace{(a\bar{a})}^{e}a = ea \underset{\substack{\uparrow \\ e\text{ left-neutral}}}{=} a\,.$$

Thus, since $a \in G$ was arbitrary, e is also a right-neutral element, hence, a neutral element of G. ⊣

In (A1*) and (A2*) we can replace "left-neutral" and "left-inverse" by "right-neutral" and "right-inverse" respectively (see Hw2.Q9), but we cannot mix left and right:

Proposition 1.3. If a set S with an associative operation has a left-neutral element and each element of S has a right-inverse, then S must not be a group.

Proof. Let $S = \{0, 1\}$ and for $x, y \in S$ define $x * y := y$. Now, the binary operation "$*$" is associative and 0 is a left-neutral element of $(S, *)$, 0 is the right-inverse of 0 as well as of 1, so, each element of S has a right-inverse. On the other hand, there is no $x \in S$ such that $x * 1 = 0$, or in other words, 1 has no left-inverse. Hence, $(S, *)$ is not a group. ⊣

Of course, in Proposition 1.3, we can swap "left" and "right" (see Hw2.Q10). However, the situation is different, if the left-neutral element is unique:

Proposition 1.4. If a set G with an associative operation has a unique left-neutral element and each element of G has a right-inverse, then G is a group.

Proof. Let e be the unique left-neutral element of G. Let

$$E(G) = \{a \in G : aa = a\}.$$

First we show that $E(G) = \{e\}$. Take any $a \in E(G)$ and $b \in G$, then

$$ab = a(eb) = a(aa^{-1})b = (aa)(a^{-1}b) = a(a^{-1}b) = (aa^{-1})b = eb = b.$$

Therefore, since b was arbitrary, a is a left-neutral element, and since the left-neutral element is unique, we have $a = e$.

Consider $Ge = \{ge : g \in G\}$, and let us show that Ge is a group. By definition of Ge, any $x \in Ge$ is of the form $x = ge$ (for some $g \in G$). Now, $xe = (ge)e = g(ee) = ge = x$, and therefore, e (or more precisely ee) is a right-neutral element of Ge. Further, let g^{-1} be a right-inverse element of g, then $g^{-1}e \in Ge$ is a right-inverse of $x = ge$. Indeed,

$$x(g^{-1}e) = (ge)(g^{-1}e) = g(eg^{-1})e = (gg^{-1})e = ee = e.$$

So, Ge has a right-neutral element and each element of Ge has a right inverse, which implies (by the "right-version" of Proposition 1.2) that Ge is a group.

In order to show that G is a group, by Proposition 1.2 it is enough to show that each element in G has a left-inverse.

Let g be any element of G, and let $x \in Ge$ be such that $x(ge) = (ge)x = e$ (such an x exists since Ge is a group). We claim that $xg \in E(G)$:

$$\begin{aligned}(xg)(xg) &= (xg)e(xg) && \text{(since } x \in Ge,\ ex = x\text{)}\\ &= xeg \\ &= xg && \text{(since } x \in Ge,\ xe = x\text{).}\end{aligned}$$

Thus, $xg \in E(G) = \{e\}$, or in other words, $xg = e$. Since $g \in G$ was arbitrary, each element of G has a left-inverse, which implies (by Proposition 1.2) that G is a group. ⊣

Definition. The **order** of a group $(G, \circ)$, denoted by $|G|$, is the cardinality (or size) of the underlying set G.

If G has finitely many elements, then $|G| = n$ for some positive integer n (why there is no group with 0 elements?) and if G is infinite, then we set $|G| = \infty$.

To state the next result we have first to give some definitions.

Definition. A set S with a binary operation is **left cancellative** if whenever $x, y, z \in S$ and $xy = xz$, one has $y = z$. The notion **right cancellative** is defined similarly. Further, S is **cancellative** if S is both, left cancellative as well as right cancellative.

If the binary operation on S is commutative and S is left cancellative, then S is also right cancellative. But on the other hand, if S is cancellative, then this does not imply that the binary operation on S must be commutative, as we will see later.

However, it is easy to see that every group is cancellative. Moreover, for finite sets, axioms (A1) and (A2) can be replaced by just one axiom:

Proposition 1.5. Let G be a finite set with an associative operation. If G is cancellative, then G is a group.

Proof. Let $a \in G$ be arbitrary. Consider the set $aG = \{ax : x \in G\}$. It is easy to see that $|aG| \leq |G|$. On the other hand, if $|aG| < |G|$, then would find two distinct $x, y \in G$ such that $ax = ay$, and since G is left cancellative, this would imply that $x = y$, a contradiction. So, $|aG| = |G|$, which implies that $aG = G$.

Now, there must be an element $e \in G$ such that $ae = a$. Further, we have $ae = (ae)e = a(ee)$, which implies, since G is left cancellative, that $e = ee$. Let now $b \in G$ be arbitrary. We get $be = b(ee) = (be)e$, and since G is right cancellative, $be = b$, and hence, e is a right-neutral element of G.

Let $b \in G$ be arbitrary. Again, we have $bG = G$, which implies that there is a $\bar{b} \in G$ such that $b\bar{b} = e$, thus, the element $b \in G$ has a right-inverse, and since $b \in G$ was arbitrary, every element of G has a right-inverse. By Proposition 1.2 (replacing "left" by "right"), this proves that G is a group. ⊣

Notice that in the proof of Proposition 1.5 we used that G is both, left and right cancellative and that G is finite. In fact, we cannot do better:

Proposition 1.6.

(a) A finite set S with an associative operation which is right cancellative must not be a group.

(b) An infinite set S with an associative operation which is cancellative must not be a group.

Proof. (a) Let $S = \{0, 1\}$ and for $x, y \in S$ define $x * y := x$. Then the operation "$*$" is associative and S is right cancellative (since $y * x = z * x$ implies $y = z$). But S is obviously not a group (see also the proof of Proposition 1.3).

(b) Consider $(\mathbb{N}, +)$, where $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ denotes the set of natural numbers. The operation "$+$" is associative and $\mathbb{N}$ is cancellative (since $x + y = x + z \Leftrightarrow y = z \Leftrightarrow y + x = z + x$). But $(\mathbb{N}, +)$ is not a group, since for example 1 does not have an inverse. ⊣