

# CHAPTER 2

## Groups

### §7

#### Basic Definitions

Before giving the formal definition of a group, we would rather present some concrete examples.

**7.1 Examples: (a)** Consider the addition of integers. From the numerous properties of this binary operation, we single out the following ones.

(i)  $+$  is a binary operation on  $\mathbb{Z}$ , so, for any  $a, b \in \mathbb{Z}$ , we have  $a + b \in \mathbb{Z}$ .

(ii) For all  $a, b, c \in \mathbb{Z}$ , we have  $(a + b) + c = a + (b + c)$ .

(iii) There is an integer, namely  $0 \in \mathbb{Z}$ , which has the property

$$a + 0 = a \quad \text{for all } a \in \mathbb{Z}.$$

(iv) For all  $a \in \mathbb{Z}$ , there is an integer, namely  $-a$ , such that

$$a + (-a) = 0.$$

**(b)** Consider the multiplication of positive real numbers. Let  $\mathbb{R}^+$  be the set of positive real numbers. Here the multiplication enjoys properties analogous to the ones above.

(i)  $\cdot$  is a binary operation on  $\mathbb{R}^+$ , so, for any  $a, b \in \mathbb{R}^+$ , we have  $a \cdot b \in \mathbb{R}^+$ .

(ii) For all  $a, b, c \in \mathbb{R}^+$ , we have  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ .

(iii) There is a positive real number, namely  $1 \in \mathbb{R}^+$ , which has the property

$$a \cdot 1 = a \text{ for all } a \in \mathbb{R}^+.$$

(iv) For all  $a \in \mathbb{R}^+$ , there is a positive real number, namely  $1/a$ , such that

$$a \cdot \frac{1}{a} = 1.$$

**(c)** Let  $n$  be a natural number and consider the addition in  $\mathbb{Z}_n$ , which we introduced in §6.

(i)  $+$  is a binary operation on  $\mathbb{Z}_n$ , so, for any  $\bar{a}, \bar{b} \in \mathbb{Z}_n$ , we have  $\bar{a} + \bar{b} \in \mathbb{Z}_n$ .

(ii) For all  $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$ , we have  $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$ .

(iii) There is an integer mod  $n$ , namely  $\bar{0} \in \mathbb{Z}_n$ , which has the property

$$\bar{a} + \bar{0} = \bar{a} \text{ for all } \bar{a} \in \mathbb{Z}_n.$$

(iv) For all  $\bar{a} \in \mathbb{Z}_n$ , there is an integer mod  $n$ , namely  $\overline{-a}$ , such that

$$\bar{a} + (\overline{-a}) = \bar{0}.$$

**(d)** Let  $X$  be a nonempty set and let  $S_X$  be the set of all one-to-one mappings from  $X$  onto  $X$ . Consider the composition  $\circ$  of mappings in  $S_X$ .

(i)  $\circ$  is a binary operation on  $S_X$ , for if  $\sigma$  and  $\tau$  are one-to-one mappings from  $X$  onto  $X$ , so is  $\sigma \circ \tau$  by Theorem 3.13.

(ii) For all  $\sigma, \tau, \mu \in S_X$ , we have  $(\sigma \circ \tau) \circ \mu = \sigma \circ (\tau \circ \mu)$  (Theorem 3.10).

(iii) There is a mapping in  $S_X$ , namely  $\iota_X \in S_X$ , such that

$$\sigma \circ \iota_X = \sigma \text{ for all } \sigma \in S_X \quad (\text{Example 3.9(a)}).$$

(iv) For all  $\sigma \in S_X$ , there is a mapping in  $S_X$ , namely  $\sigma^{-1}$ , such that

$$\sigma \circ \sigma^{-1} = \iota_X.$$

(See Theorem 3.14 and Theorem 3.16. That  $\sigma^{-1} \in S_X$  follows from Theorem 3.17(1).)

These are examples of groups. In each case, we have a nonempty set and a binary operation on that set which enjoys some special properties. A group will be defined as a nonempty set and a binary operation on

that set having the same properties as in the examples above. A group will thus consist of two parts: a set and a binary operation. Formally, a group is an ordered pair whose components are the set and the operation in question.

**7.2 Definition:** An ordered pair  $(G, \circ)$ , where  $G$  is a nonempty set and  $\circ$  is a binary operation on  $G$ , is called a *group* provided the following hold.

(i)  $\circ$  is a (well defined) binary operation on  $G$ . Thus, for any  $a, b \in G$ ,  $a \circ b$  is a uniquely determined element of  $G$ .

(ii) For all  $a, b, c \in G$ , we have  $(a \circ b) \circ c = a \circ (b \circ c)$ .

(iii) There is an element  $e$  in  $G$  such that

$$a \circ e = a \text{ for all } a \in G$$

and which is furthermore such that

(iv) for all  $a \in G$ , there is an  $x$  with

$$a \circ x = e.$$

When  $(G, \circ)$  is a group, we also say that  $G$  is (or builds, or forms) a group with respect to  $\circ$  (or under  $\circ$ ). Since a group is an ordered pair, two groups  $(G, \circ)$  and  $(H, *)$  are equal if and only if  $G = H$  and the binary operation  $\circ$  on  $G$  is equal to the binary operation  $*$  on  $G$  (i.e.,  $\circ$  and  $*$  are identical mappings from  $G \times G$  into  $G$ ). On one and the same set  $G$ , there may be distinct binary operations  $\circ$  and  $*$  under which  $G$  is a group. In this case, the groups  $(G, \circ)$  and  $(G, *)$  are distinct.

The four conditions (i)-(iv) of Definition 7.2 are known as the *group axioms*. The first axiom (i) is called the *closure axiom*. When (i) is true, we say  $G$  is *closed under*  $\circ$ .

A binary operation  $\circ$  on a nonempty set  $G$  is said to be *associative* when (ii) holds. The associativity of  $\circ$  enables us to write  $a \circ b \circ c$  without ambiguity. Indeed,  $a \circ b \circ c$  has first no meaning at all. We must write either  $(a \circ b) \circ c$  or  $a \circ (b \circ c)$  to denote a meaningful element in  $G$ . By associativity, we may and do make the convention that  $a \circ b \circ c$  will mean

$(a \circ b) \circ c = a \circ (b \circ c)$ , for whether we read it as  $(a \circ b) \circ c$  or  $a \circ (b \circ c)$  does not make any difference. This would be wrong if  $\circ$  were not associative. For instance,  $:$  (division) is not an associative operation on  $\mathbb{Q} \setminus \{0\}$  and  $(a:b):c \neq a:(b:c)$  unless  $c = 1$  (here  $a, b, c \in \mathbb{Q} \setminus \{0\}$ ). Thus  $a:b:c$  is ambiguous.

An element  $e$  of a set  $G$ , on which there is a binary operation  $\circ$ , is called a *right identity element* or simply a *right identity* if  $a \circ e = a$  for all  $a$  in  $G$ . The third group axiom (iii) ensures that group  $G$  has a right identity element. We will show presently that group has precisely one identity element, but we have not proved it yet and we must be careful not to use the uniqueness of the right identity before we prove it. All we know at this stage is that a group has at least one right identity for which (iv) holds. As it is, there may be many right identities. In addition, there may be some right identities for which (iv) is true and also some for which (iv) is false. For the time being, these possibilities are not excluded.

They will be excluded in Lemma 7.3, where we will prove further that our unique right identity is also a left identity. A *left identity element* or a *left identity of  $G$* , where  $G$  is a nonempty set with a binary operation  $\circ$  on it, is by definition an element  $f$  of  $G$  such that  $f \circ a = a$  for all  $a \in G$ . The group axioms say nothing about left identities. If  $(G, \circ)$  is a group, we do not yet know if there is a left identity in  $G$  at all, nor do we know any relation between right and left identities. For the time being, there may be no or one or many left identities in  $G$ . If there is only one left identity, it may or may not be right identity. If there are many left identities, some or one or none of them may be right identities.

We mention all these possibilities so that the reader does not read in the axioms more than what they really say. The group axioms say nothing about left identities or about the uniqueness of the right identity.

The group axioms do say something about right inverses. If  $G$  is a nonempty set with a binary operation  $\circ$  on it, and if  $e$  is a right identity in  $G$ , and  $a \in G$ , an element  $x \in G$  is called a *right inverse* of  $a$  (with respect to  $e$ ) when  $a \circ x = e$ . The group axioms state that, in case  $(G, \circ)$  is a group, there is a right identity  $e$  in  $G$  with respect to which each element of  $G$  has at least one right inverse. Until we prove Lemma 7.3, there may be many right identities with this property. Also, some of the right identity elements may and some of the right identity elements may not have this property. Furthermore, some (or all) of the elements may have more than one right inverses with respect to some (or all) of the right identities. The group axioms make no uniqueness assertion about the right inverses.

Before we lose ourselves in chaos, we had better prove our lemma.

**7.3 Lemma:** Let  $(G, \circ)$  be a group and let  $e$  be a right identity element of  $G$  such that, for all  $a \in G$ , there exists a suitable  $x$  in  $G$  with  $a \circ x = e$ . The existence of  $e$  is assured by the group axioms (iii) and (iv).

- (1) If  $g \in G$  is such that  $g \circ g = g$ , then  $g = e$ .
- (2)  $e$  is the unique right identity in  $G$ .
- (3) A right inverse of an element in  $G$  is also a left inverse of the same element. In other words, if  $a \circ x = e$ , then  $x \circ a = e$ .
- (4)  $e$  is a left identity in  $G$ . That is,  $e \circ a = a$  for all  $a \in G$ .
- (5)  $e$  is the unique left identity in  $G$ .
- (6) Each element has a unique right inverse in  $G$ .
- (7) Each element has a unique left inverse in  $G$ .
- (8) The unique right inverse of any  $a \in G$  is equal to the unique left inverse of  $a$ .

**Proof:** (1) Let  $g \in G$  be such that  $g \circ g = g$ . We choose a right inverse of  $g$  with respect to  $e$ . This is possible by the axiom (iv). Let us call it  $h$ . Thus  $g \circ h = e$ . Then

$$\begin{aligned} (g \circ g) \circ h &= g \circ h && \text{(by associativity),} \\ g \circ (g \circ h) &= g \circ h && \text{(since } g \circ h = e\text{),} \\ g \circ e &= e && \text{(since } e \text{ is a right identity).} \\ g &= e \end{aligned}$$

This proves part (1).

(2) The claim is that  $e$  is the unique right identity in  $G$ . This means: if  $f \in G$  is a right identity, that is, if  $a \circ f = a$  for all  $a \in G$ , then  $f = e$ . Suppose  $f$  is a right identity. Then  $a \circ f = a$  for all  $a \in G$ . Writing  $f$  for  $a$  in particular, we see  $f \circ f = f$ . Hence  $f = e$  by part (1).

(3) A right inverse  $x$  of an arbitrary element  $a \in G$  is also a left inverse of  $a$ . This is what we are to prove. So we assume  $a \circ x = e$  and try to derive  $x \circ a = e$ . We use part (1). If  $a \circ x = e$ , then

$$\begin{aligned} (x \circ a) \circ (x \circ a) &= [(x \circ a) \circ x] \circ a && \text{(by associativity)} \\ &= [x \circ (a \circ x)] \circ a && \text{(by associativity)} \\ &= [x \circ e] \circ a \\ &= x \circ a. \end{aligned}$$

So  $g := (x \circ a)$  is such that  $g \circ g = g$ . By part (1),  $g = e$ . So  $x \circ a = e$ .

(4) We are to prove that  $e$  is a left identity. So we must show  $e \circ a = a$  for all  $a \in G$ . Let  $a \in G$  and let  $x$  be a right inverse of  $a$ . Then

$$a \circ x = e$$

$$\begin{aligned}
a \circ x &= x \circ a && \text{(by part (3))} \\
(a \circ x) \circ a &= (x \circ a) \circ a \\
a \circ (x \circ a) &= (x \circ a) \circ a \\
a \circ e &= e \circ a \\
a &= e \circ a.
\end{aligned}$$

Therefore,  $e$  is a left identity as well. This proves part (4).

(5) The claim is that  $e$  is the unique left identity in  $G$ . This means: if  $f$  is a left identity in  $G$  so that  $f \circ a = a$  for all  $a \in G$ , then  $f = e$ . We know that the right identity  $e$  is a left identity (part (4)), and that  $e$  is the unique right identity (part (2)). So we conclude that  $e$  is the unique left identity. Is this correct? No, this is wrong. This would be correct if we knew that any left identity is also a right identity (and so the unique right identity by part (2)), which is not what part (4) states. For all we proved up to now, there may very well be a unique right identity and many left identities (among them the right identity). We are to show in part (5) that this is impossible.

After so much fuss, now the correct proof, which is very short. Suppose  $f \circ a = a$  for all  $a \in G$ . Write in particular  $f$  for  $a$ . Then  $f \circ f = f$  and part (1) yields  $f = e$ .

(6) The claim is that each element  $a \in G$  has a unique right inverse in  $G$ . We know that  $a$  has at least one right inverse, say  $x$ . We have  $a \circ x = e$ . We are to show: if  $a \circ y = e$ , then  $y = x$  (here  $y \in G$ ). Suppose then  $a \circ x = e$  and  $a \circ y = e$ . We obtain

$$\begin{aligned}
x \circ a &= e && \text{(by part (3))} \\
(x \circ a) \circ y &= e \circ y \\
x \circ (a \circ y) &= e \circ y \\
x \circ e &= e \circ y \\
x &= e \circ y \\
x &= y && \text{(by part (4)).}
\end{aligned}$$

This proves part (6).

(7) and (8) Let  $a \in G$  and let  $x$  be the unique right inverse of  $a$ . From part (3), we know that  $x$  is a left inverse of  $a$ , so that  $x \circ a = e$ . We must prove: if  $x \circ a = e$  and  $y \circ a = e$ , then  $y = x$ . Suppose then  $x \circ a = e$  and  $y \circ a = e$ . Then

$$\begin{aligned}
a \circ x &= e \\
y \circ (a \circ x) &= y \circ e
\end{aligned}$$

$$\begin{aligned}
(y \circ a) \circ x &= y \\
e \circ x &= y \\
x &= y.
\end{aligned}$$

This completes the proof. □

According to Lemma 7.3, a group  $(G, \circ)$  has one and only one right identity, which is also the unique left identity. Therefore, we can refer to it as *the* identity of the group, without mentioning right or left. Similarly, since any  $a \in G$  has a unique right inverse, which is also the unique left inverse of  $a$ , we may call it *the* inverse of  $a$ . The inverse of  $a$  is uniquely determined by  $a$ ; for this reason, we introduce a notation displaying the fact that it depends on  $a$  alone. We write  $a^{-1}$  for the inverse of  $a$  (read:  $a$  inverse). Thus  $a^{-1}$  is the unique element of  $G$  such that  $a \circ a^{-1} = a^{-1} \circ a = e$ , where  $e$  is the identity of the group.

The group axioms, as presented in Definition 7.2, assert the existence of a right identity, and a right inverse of each element. We proved in Lemma 7.3 that a right identity is also a left identity and a right inverse of an element is also a left inverse of the same element. One could give an alternative definition of a group by so modifying the axioms that they assert the existence of a left identity, and a left inverse of each element. A lemma analogous to Lemma 7.3 would prove then that there is a unique left identity, which is also a unique right identity and that each element has a unique left inverse, which is also a unique right inverse of that element. Thus the existence of a right identity plus right inverses lead to the same algebraic structure (group) as the existence of a left identity plus left inverses.

However, existence of a right identity and the existence of left inverses do not always produce a group. For example, consider the set  $\mathbb{Z} \times \mathbb{Z}$ . For any  $(a,b), (c,d) \in \mathbb{Z} \times \mathbb{Z}$ , we put  $(a,b) \Delta (c,d) = (a, b + d)$ . Let us check if  $(\mathbb{Z} \times \mathbb{Z}, \Delta)$  is a group.

(i)  $\Delta$  is a binary operation on  $\mathbb{Z} \times \mathbb{Z}$  since  $a \in \mathbb{Z}, b + d \in \mathbb{Z}$  whenever  $a,b,c,d \in \mathbb{Z}$ . So  $\mathbb{Z} \times \mathbb{Z}$  is closed under  $\Delta$ .

(ii) Is  $\Delta$  associative? For any  $(a,b), (c,d), (e,f) \in \mathbb{Z} \times \mathbb{Z}$ , we ask

$$\begin{aligned}
[(a,b) \Delta (c,d)] \Delta (e,f) &\stackrel{?}{=} (a,b) \Delta [(c,d) \Delta (e,f)] \\
(a,b + d) \Delta (e,f) &\stackrel{?}{=} (a,b) \Delta (c,d + f) \\
(a, (b + d) + f) &\stackrel{?}{=} (a, b + (d + f))
\end{aligned}$$

Yes, this is true since  $+$  is an associative operation on  $\mathbb{Z}$ . Hence  $\Delta$  is associative.

(iii) Is there an element in  $\mathbb{Z} \times \mathbb{Z}$ ,  $(a_0, b_0)$  say, such that

$$(a, b) \Delta (a_0, b_0) = (a, b) \text{ for all } (a, b) \in \mathbb{Z} \times \mathbb{Z}?$$

Well, this is true if and only if  $(a, b + b_0) = (a, b)$ , which is equivalent to  $b_0 = 0$ . There is no condition on  $a_0$ . For example,

$$(a, b) \Delta (0, 0) = (a, b + 0) = (a, b)$$

$$(a, b) \Delta (1, 0) = (a, b + 0) = (a, b)$$

for all  $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ , so  $(0, 0)$  and  $(1, 0)$  are right identities. In fact, any  $(n, 0) \in \mathbb{Z} \times \mathbb{Z}$  is a right identity.

From Lemma 7.3, we know that a group has one and only one right identity. so  $\mathbb{Z} \times \mathbb{Z}$  is not a group under  $\Delta$ . On the other hand, with respect to  $(0, 0)$  for example (in fact, with respect to any right identity), each element  $(a, b)$  of  $\mathbb{Z} \times \mathbb{Z}$  has a left inverse  $(0, -b)$ :

$$(0, -b) \Delta (a, b) = (0, -b + b) = (0, 0)$$

(with respect to  $(n, 0)$ , a left inverse of  $(a, b)$  is  $(n, -b)$ ).

So  $(\mathbb{Z} \times \mathbb{Z}, \Delta)$  is a system in which a right identity exists, plus a left inverse of each element; nevertheless, it fails to be a group. Likewise, fulfilling the existence of a left identity and right inverses is not enough for building a group.

We could define a group by including the claims of Lemma 7.3 directly into the definition. Then we would have

(iii)' there is a unique  $e \in G$  such that

$$a \circ e = e \circ a = a \text{ for all } a \in G$$

and

(iv)' for all  $a \in G$ , there is a unique  $a^{-1} \in G$  such that

$$a \circ a^{-1} = e = a^{-1} \circ a$$

in place of (iii) and (iv) of Definition 7.2. Some textbooks define groups in this way. This would save us from the trouble of proving Lemma 7.3. Why, then, did we not use this definition? Because we do not want to do unnecessary work. If we defined groups by (iii)' and (iv)' instead of (iii) and (iv), then, each time when we wanted to show that a set  $G$  builds a group under a binary operation  $\circ$  on  $G$ , we had to check

- 1) that there is an  $e \in G$  such that  $a \circ e = a$  for all  $a \in G$ ,
- 2) that this  $e$  is also such that  $e \circ a = a$  for all  $a \in G$ ,
- 3) that  $e$  is the unique element of  $G$  with these two properties,

4) that for each  $a \in G$ , there is an  $a^{-1} \in G$  such that  $a \circ a^{-1} = e$ ,

5) that  $a^{-1} \circ a = e$  as well,

6) that this  $a^{-1}$  is the unique element of  $G$  with  $a \circ a^{-1} = e = a^{-1} \circ a$ ,

which more than doubles our work. With our Definition 7.2, we need check only 1) and 4). The other items 2),3),5),6) follow from 1) and 4) automatically. We pay for our comfort by having to prove Lemma 7.3, but, once this is over, we have less work to do in order to see whether a given set  $G$  forms a group under a given operation  $\circ$  on it, as in the following examples.

**7.4 Examples: (a)** For any two elements  $a, b$  of  $\mathbb{Q} \setminus \{1\}$ , we put  $a \circ b = ab - a - b + 2$ . We ask if  $\mathbb{Q} \setminus \{1\}$  is a group under  $\circ$ . Let us check the group axioms.

(i) For all  $a, b \in \mathbb{Q} \setminus \{1\}$ , we observe  $a \circ b = ab - a - b + 2 \in \mathbb{Q}$ , but this is not enough. We must prove  $a \circ b \neq 1$  also. Let  $a, b \in \mathbb{Q}$ ,  $a \neq 1 \neq b$ . We suppose  $a \circ b = 1$  and try to reach a contradiction. If  $a \circ b = 1$ , then

$$\begin{aligned} ab - a - b + 2 &= 1 \\ ab - a - b + 1 &= 0 \\ (a - 1)(b - 1) &= 0 \\ a - 1 = 0 \text{ or } b - 1 &= 0 \\ a = 1 \text{ or } b = 1, \end{aligned}$$

a contradiction. So  $a \circ b \in \mathbb{Q} \setminus \{1\}$  and  $\circ$  is a binary operation on  $\mathbb{Q} \setminus \{1\}$ .

(ii) For all  $a, b, c \in \mathbb{Q} \setminus \{1\}$ , we ask if  $(a \circ b) \circ c = a \circ (b \circ c)$ .

$$\begin{aligned} (ab - a - b + 2) \circ c &\stackrel{?}{=} a \circ (bc - b - c + 2) \\ (ab - a - b + 2)c - (ab - a - b + 2) - c + 2 &\stackrel{?}{=} a(bc - b - c + 2) - a - (bc - b - c + 2) + 2 \\ abc - ac - bc + 2c - ab + a + b - 2 - c + 2 &\stackrel{?}{=} abc - ab - ac + 2a - a - bc + b + c - 2 + 2 \end{aligned}$$

The answer is "yes." So  $\circ$  is associative.

(iii) We are looking for an  $e \in \mathbb{Q} \setminus \{1\}$  such that  $a \circ e = a$  for all  $a \in \mathbb{Q} \setminus \{1\}$ . Assuming such an  $e$  exists, we get

$$\begin{aligned} ae - a - e + 2 &= a \\ ae - e &= 2a - 2 \\ (a - 1)e &= 2(a - 1) \\ e &= 2 \quad (\text{since } a - 1 \neq 0). \end{aligned}$$

We have not proved that  $2 \in \mathbb{Q} \setminus \{1\}$  is a right identity element. We showed only that a right identity element, if it exists at all, has to be 2. Let us see if 2 is really a right identity. We observe

$$a \circ 2 = a2 - a - 2 + 2 = 2a - a = a$$

for all  $a \in \mathbb{Q} \setminus \{1\}$ . Since  $2 \in \mathbb{Q} \setminus \{1\}$ , 2 is indeed a right identity in  $\mathbb{Q} \setminus \{1\}$ .

(iv) For all  $a \in \mathbb{Q} \setminus \{1\}$ , we must find an  $x \in \mathbb{Q} \setminus \{1\}$  such that  $a \circ x = 2$ . Well, this gives

$$\begin{aligned} ax - a - x + 2 &= 2 \\ ax - a - x + 1 &= 1 \\ (a - 1)(x - 1) &= 1 \\ x - 1 &= 1/(a - 1) \\ x &= a/(a - 1), \end{aligned}$$

which is meaningful since  $a \neq 1$ . We have not proved yet that  $a/(a - 1)$  is a right inverse of  $a$ . We showed only that a right inverse of  $a \in \mathbb{Q} \setminus \{1\}$ , if it exists at all, has to be  $a/(a - 1)$ . We must now show that  $a \circ a/(a - 1) = 2$  for all  $a \in \mathbb{Q} \setminus \{1\}$  and also that  $a/(a - 1) \in \mathbb{Q} \setminus \{1\}$ . Good. We have

$$\begin{aligned} a \circ a/(a - 1) &= a(a/(a - 1)) - a - (a/(a - 1)) + 2 \\ &= (a - 1)(a/(a - 1)) - a + 2 \\ &= 2, \end{aligned}$$

and also  $a/(a - 1) \neq 1$ , for  $a/(a - 1) \in \mathbb{Q}$  and  $a/(a - 1) = 1$  would imply that  $a = a - 1$ , hence  $0 = 1$ , which is absurd.

Since all the group axioms hold,  $\mathbb{Q} \setminus \{1\}$  is a group under  $\circ$ .

**(b)** Let us define an operation  $*$  on  $\mathbb{Z}$  by putting  $a * b = a + b + 2$  for all  $a, b \in \mathbb{Z}$ . Does  $\mathbb{Z}$  form a group under  $*$ ?

(i) For any  $a, b \in \mathbb{Z}$ ,  $a * b = a + b + 2$  is an integer. So  $\mathbb{Z}$  is closed under  $*$ .

(ii) For all  $a, b, c \in \mathbb{Z}$ , we ask if  $(a * b) * c = a * (b * c)$ . We have

$$\begin{aligned} (a * b) * c &= (a + b + 2) * c \\ &= (a + b + 2) + c + 2 \\ &= a + (b + 2 + c) + 2 \\ &= a + (b + c + 2) + 2 \\ &= a + (b * c) + 2 \\ &= a * (b * c). \end{aligned}$$

So  $*$  is associative.

(iii) Is there an integer  $e \in \mathbb{Z}$  such that  $a * e = a$  for all  $a \in \mathbb{Z}$ ? Well, this gives  $a + e + 2 = a$  and  $e = -2$ . Let us check whether  $-2$  is really a right identity element. We observe that  $a * -2 = a + (-2) + 2 = a$  for all  $a \in \mathbb{Z}$ . So  $-2$  is a right identity element.

(iv) Does each integer  $a$  have a right inverse in  $\mathbb{Z}$ ? The condition  $a * x = -2$  yields

$$a + x + 2 = -2$$

$$x = -4 - a \in \mathbb{Z}.$$

$-4 - a$  is indeed a right inverse of  $a$  since  $a * (-4 - a) = a + (-4 - a) + 2 = -2$ .

Therefore  $\mathbb{Z}$  is a group with respect to  $*$ .

(c) Let  $A$  be a nonempty set and let  $\mathfrak{X}$  be the set of all subsets of  $A$ . The elements of  $\mathfrak{X}$  are thus subsets of  $A$ . Consider the forming of symmetric differences (§1, Ex.7).  $\mathfrak{X}$  is a group under  $\Delta$ :

(i) For all  $S, T \in \mathfrak{X}$ ,  $S \Delta T$  is a subset of  $A$ , so  $S \Delta T \in \mathfrak{X}$  and  $\mathfrak{X}$  is closed under  $\Delta$ .

(ii)  $\Delta$  is associative (§1, Ex.8).

(iii)  $\emptyset$  is a right identity (§1, Ex.8).

(iv) Each element  $S$  of  $\mathfrak{X}$  has a right inverse, namely  $S$  itself, as  $S \Delta S = \emptyset$  for all  $S \in \mathfrak{X}$  (§1, Ex.8).

So  $\mathfrak{X}$  is a group under  $\Delta$ .

We have seen many examples of groups. In some of the groups  $(G, \circ)$ , the underlying set  $G$  is infinite, in some finite. The number of elements of  $G$ , more precisely the cardinality of  $G$ , is called the *order* of the group  $(G, \circ)$ . We denote the order of  $(G, \circ)$  by  $|G|$ . A group  $(G, \circ)$  is called a *finite* group if  $|G|$  is finite, and an *infinite* group if  $|G|$  is infinite. One might distinguish between various infinite cardinalities, but we will not do so in this book. When the order of a group  $(G, \circ)$  is infinite, we write  $|G| = \infty$ . The symbol  $\infty$  will stand for all types of infinities.

A. Cayley (1821-1895) introduced a convenient device for investigating groups. Let  $(G, \circ)$  be a finite group. We make a table that displays  $a \circ b$  for each  $a, b \in G$ . We divide a square into  $|G|^2$  parts by dividing the sides into  $|G|$  parts. Each one of the rows will be indexed by an element of the group, usually written on the left of the row. Likewise, each one of the columns will be indexed by an element of the group, usually written above the column. Each element will index only one row and only one column. It is customary to use the same ordering of the elements to index the rows and columns. Also, the first row and the first column are customarily indexed by the identity element of the group. In the cell where the row of  $a \in G$  and  $b \in G$  meet, we write down  $a \circ b$ . This

square is known as the *Cayley table* or the *operation table* (*multiplication* or *addition table*, as the case may be) of the group  $(G, \circ)$ .

As an illustration, we give the addition table of  $(\mathbb{Z}_4, +)$  below.  $(\mathbb{Z}_4, +)$  is a group by Example 7.1(c). We drop the bars for convenience.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

We observe in this table that every element of  $\mathbb{Z}_4$  appears once in each row and also in each column. This is a general property of groups: if  $(G, \circ)$  is a group, then every element  $b$  of  $G$  appears once and only once in the row of any  $a \in G$ , say in the cell where the row of  $a$  and the column of  $x \in G$  meet. A similar assertion holds for columns. This is the content of the next lemma.

**7.5 Lemma:** *Let  $(G, \circ)$  be a group and  $a, b \in G$ .*

- (1) *There is one and only one  $x \in G$  such that  $a \circ x = b$ .*
- (2) *There is one and only one  $y \in G$  such that  $y \circ a = b$ .*

**Proof:** (1) We prove first that there can be at most one  $x \in G$  such that  $a \circ x = b$ . Let  $a \circ x = b = a \circ x_1$ . We prove  $x = x_1$ . We have

$$\begin{aligned}
 a \circ x &= a \circ x_1 \\
 a^{-1} \circ (a \circ x) &= a^{-1} \circ (a \circ x_1) \\
 (a^{-1} \circ a) \circ x &= (a^{-1} \circ a) \circ x_1 \\
 e \circ x &= e \circ x_1 \\
 x &= x_1
 \end{aligned}$$

by Lemma 7.3. So there can be at most one  $x$  with  $a \circ x = b$ .

The existence of at least one such  $x$  is easily seen when we put  $x = a^{-1} \circ b$ . Indeed,  $a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b = e \circ b = b$ .

So there is one and only one element  $x$  of  $G$ , namely  $x = a^{-1} \circ b$ , such that  $a \circ x = b$ . This proves (1).

The proof of (2) is similar and is left to the reader. □

We give an application of Lemma 7.5. We determine the Cayley table of groups of order 3. Let  $(\{e,a,b\}, \circ)$  be a group of order 3, where  $e$  is the identity. The Cayley table of this group contains the information given in Figure 1. Now we fill the remaining four cells. What is  $a \circ a$ ? The cell  $*$  cannot contain  $a$ , for  $a$  would otherwise appear more than once in the

	$e$	$a$	$b$
$e$	$e$	$a$	$b$
$a$	$a$	*	
$b$	$b$		

Figure 1

	$e$	$a$	$b$
$e$	$e$	$a$	$b$
$a$	$a$	$b$	
$b$	$b$		

Figure 2

	$e$	$a$	$b$
$e$	$e$	$a$	$b$
$a$	$a$	$b$	$e$
$b$	$b$	$e$	$a$

Figure 3

second row (or column). So the cell  $*$  contains  $e$  or  $b$ . If it contained  $e$ , then the third entry in the second row had to be  $b$  and  $b$  would appear at least twice in the third column, contrary to Lemma 7.5. This leaves only the possibility  $a \circ a = b$ . Then we have the table in Figure 2. The remaining cells are necessarily filled in as in Figure 3.

We did not prove that Figure 3 is a Cayley table of a group of order 3. At this stage, we do not even know whether a group of order 3 exists. We proved: if there is a group of order 3 at all, then its Cayley table is the table of Figure 3. We now prove the existence of a group of order 3. We use Figure 3. Let  $\{e,a,b\}$  be a set of 3 elements, and let the binary operation  $\circ$  on this set be *defined* as in Figure 3. It is easy to check the group axioms (i),(iii),(iv). It remains to check associativity. We must verify  $3 \cdot 3 \cdot 3 = 27$  equations  $(x \circ y) \circ z = x \circ (y \circ z)$ , where  $x,y,z \in \{e,a,b\}$ . An equation of this type is true when one of  $x,y,z$  is equal to  $e$ . So we are left with  $2 \cdot 2 \cdot 2 = 8$  equations

$$\begin{array}{ll}
 (a \circ a) \circ a = a \circ (a \circ a) & (b \circ a) \circ a = b \circ (a \circ a) \\
 (a \circ a) \circ b = a \circ (a \circ b) & (b \circ a) \circ b = b \circ (a \circ b) \\
 (a \circ b) \circ a = a \circ (b \circ a) & (b \circ b) \circ a = b \circ (b \circ a)
 \end{array}$$

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

and these are verified easily. Hence  $(\{e,a,b\}, \circ)$  is a group. There is a group of order 3. Any two groups of order 3 have essentially the same Cayley table, namely the table in Figure 3. This statement will be made precise in §20.

The Cayley tables of  $(\mathbb{Z}_4,+)$  and  $(\{e,a,b\}, \circ)$  are symmetric about the principal diagonal (that joins the upper-left and lower-right cells). What does this signify? The symmetry of the Cayley table of a group  $(G, \circ)$  means that the cell where the  $i$ -th row and  $j$ -th column meet has the same entry as the cell where the  $j$ -th row and  $i$ -th column meet, and this for all  $i,j = 1,2, \dots, |G|$ . Assuming the  $i$ -th row is the row of  $a \in G$  and the  $j$ -th column is the column of  $b \in G$  (and assuming we index the rows and columns by the elements of  $G$  in the same order), this means:  $a \circ b = b \circ a$  for all  $a,b \in G$ . So the group is commutative in the following sense.

**7.6 Definition:** A group  $(G, \circ)$  is called a *commutative* group or an *abelian* group, if, in addition to the group axioms (i)-(iv), a fifth axiom

$$(v) \ a \circ b = b \circ a \text{ for all } a,b \in G$$

holds.

A binary operation on a set  $G$  is called *commutative* when  $a \circ b = b \circ a$  for all  $a,b \in G$ . So a commutative group is one where the operation is commutative. The term "abelian" is used in honor of N. H. Abel, a Norwegian mathematician (1802-1829).

We close this paragraph with some comments on the group axioms. The reader might ask why we should study the structures  $(G, \circ)$  where  $\circ$  satisfies the axioms (i),(ii),(iii),(iv). Why do we not study structures  $(G, \circ)$  where  $\circ$  satisfies the axioms (i),(iii),(iv),(v) or (i),(ii),(iii),(v)? What is the reason for preferring the axioms (i),(ii),(iii),(iv) to some other combination of (i),(ii),(iii),(iv),(v)? There is of course no reason why other combinations ought to be excluded from study. As a matter of fact, all combinations have a proper name and there are theories about them. However, they

are very far from having the same importance as the combination (i),(ii), (iii),(iv).

A mathematical theory, if it deserves to be considered important, has to possess both generality and informative significance. Clearly, a theory whose axioms are too restrictive to hold in a variety of cases is bound to be insignificant for those who cannot fulfill them in their area of study, and the theory will have limited interest. An interesting theory is a general one. But generality costs content. When we wish that the axioms of a theory be fulfilled in diverse areas and in many contexts, we must also realize that the theory can only deal with what is common in these diverse areas, and this might be nil. There we have the danger that the theory will degenerate into a list of uninformative paraphrases of the axioms without substance. Imposing restrictions on the axioms diminishes the use and interest of a theory, and lifting restrictions tends to make the theory void. The balance of generality against content is very delicate. Group theory is one of the cases where this balance is attained successfully. Group theory has applications in literally every branch of mathematics, both pure and applied, as well as in theoretical physics and other sciences, and it is a theory full of deep, interesting, beautiful results. This is why the choice (i),(ii),(iii),(iv) is judicious. Other combinations of the axioms are not as fruitful as (i),(ii),(iii),(iv).

## Exercises

1. Determine whether the following sets build groups with respect to the operations given. In each case, state which group axioms are satisfied.

- (a)  $\mathbb{R}$  under subtraction, multiplication and division.
- (b)  $\mathbb{R} \setminus \{0\}$ ,  $\mathbb{Q} \setminus \{0\}$ ,  $\mathbb{C} \setminus \{0\}$  under multiplication.
- (c)  $\{0,1\}$ ,  $\{-1,1\}$  under multiplication.
- (d)  $\{z \in \mathbb{C} : |z| \leq 1\}$  under multiplication.
- (e)  $\{z \in \mathbb{C} : |z| = 1\}$  under multiplication.

(f)  $5\mathbb{Z} = \{5z \in \mathbb{Z} : z \in \mathbb{Z}\}$  under multiplication and addition.

(g)  $\{x\}$  under  $\circ$ , where  $x \circ x = x$ .

(h)  $\{(t,u) \in \mathbb{Z} \times \mathbb{Z} : t^2 - 5u^2 = 4\}$  under  $*$ , where  $*$  is defined by

$$(t_1, u_1) * (t_2, u_2) = \left( \frac{t_1 t_2 + 5u_1 u_2}{2}, \frac{t_1 u_2 + t_2 u_1}{2} \right)$$

for all  $(t_1, u_1), (t_2, u_2)$  in this set.

(i)  $\mathbb{Z}_6$  and  $\mathbb{Z}_8$  under multiplication and addition.

(j)  $\mathbb{Z}_7$  and  $\mathbb{Z}_7 \setminus \{\bar{0}\}$  under multiplication.

(k)  $\{f, g\}$  under the composition of mappings, where  $f: x \rightarrow x$  and  $g: x \rightarrow 1/(1-x)$  are functions from  $\mathbb{R} \setminus \{1\}$  into  $\mathbb{R} \setminus \{1\}$ .

(l)  $\{f, g, h\}$  under the composition of mappings, where  $f: x \rightarrow x$  and  $g: x \rightarrow 1/(1-x)$  and  $h: x \rightarrow (x-1)/x$  are functions from  $\mathbb{R} \setminus \{1, 0\}$  into  $\mathbb{R} \setminus \{1, 0\}$ .

(m)  $\{f_{a,b} : a, b \in \mathbb{R}, a \neq 0\}$  under the composition of mappings, where  $f_{a,b}$  is defined by  $f_{a,b}(x) = ax + b$  as a function from  $\mathbb{R}$  into  $\mathbb{R}$ .

2. For which  $m \in \mathbb{N}$  is the set  $\mathbb{Z}_m \setminus \{0\}$  a group under multiplication?