Chapter 3
Introduction to Groups

We now begin our study of abstract algebra in earnest! A group is one of the simplest algebraic structures; we take a set, assign an operation to it, impose four basic rules, and see what we can deduce. And yet, the possibilities are endless. Groups show up everywhere, and not just in mathematics. Indeed, it would be difficult to study physics or chemistry without an understanding of group theory. The solution to the famous Rubik's cube is also a problem in groups.

In this chapter, we will define the notion of a group, and give a number of examples. We will also prove several basic properties of groups and subgroups.

3.1 An Important Example

In the next section, we will give the definition of a group. For now, we will look at a motivating example.

Let A be the set $\{1, 2, 3\}$. We would like to consider all of the permutations of A; that is, all the ways of rearranging the numbers 1, 2 and 3. For example, we have the permutation σ, where $\sigma(1) = 2$, $\sigma(2) = 1$ and $\sigma(3) = 3$. We can easily see that there are going to be exactly 6 such permutations, as there are 3 choices for $\sigma(1)$, then 2 remaining choices for $\sigma(2)$, and once those are known, $\sigma(3)$ is determined.

A bit of notation would be helpful. Let us denote a permutation σ by writing two rows. The elements of A go in the first row, and the numbers to which each of them is sent in the second; that is, we take

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ a & b & c \end{pmatrix}$$

to mean that $\sigma(1) = a$, $\sigma(2) = b$ and $\sigma(3) = c$. Then the permutation we mentioned above would be denoted

G. T. Lee, *Abstract Algebra*, Springer Undergraduate Mathematics Series,
https://doi.org/10.1007/978-3-319-77649-1_3

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

In fact, the complete list of permutations is

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Let us now discuss the composition of two permutations. For instance, if

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ and } \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

then we see that $(\sigma \circ \tau)(1) = \sigma(\tau(1)) = \sigma(3) = 3, (\sigma \circ \tau)(2) = \sigma(\tau(2)) = \sigma(1) = 2$ and $(\sigma \circ \tau)(3) = \sigma(\tau(3)) = \sigma(2) = 1$. Thus,

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

(It is worth noting here that we apply τ first, then σ.)

We can now consider some properties that these permutations enjoy with respect to this composition operation. As we discuss them, please compare with the properties of $\mathbb{Z}$ or $\mathbb{Z}_n$, under addition, with which we are already familiar.

First of all, we have **closure**. That is, if we take two permutations of A and compose them, we obtain another permutation of A. In fact, we proved this in Theorem 1.2, where we saw that the composition of two bijections is a bijection.

Next, we have **associativity**; that is, for any permutations ρ, σ and τ, we have $\rho \circ (\sigma \circ \tau) = (\rho \circ \sigma) \circ \tau$. We have seen this before as well; by Theorem 1.2, the composition of functions is always associative.

Also, we have an **identity**. In particular, if σ is any permutation of A, then

$$\sigma \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \circ \sigma = \sigma.$$

Composing with the permutation that moves nothing cannot change a function.

Finally, we have **inverses**; that is, for each permutation σ, there is another permutation τ such that

$$\sigma \circ \tau = \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},$$

the identity. This is easy enough to calculate directly; for instance,

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

However, the existence of such an inverse is guaranteed by Theorem 1.3.

Given our discussion in Sections 2.4 and 2.5, we can agree that all of these properties are shared by $\mathbb{Z}$ and $\mathbb{Z}_n$ under addition. However, we also noted that the addition operation is **commutative**. Not so here! For instance,

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\circ\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},$$

whereas

$$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\circ\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

Thus, in general, $\sigma\circ\tau\neq\tau\circ\sigma$.

These permutations under the composition operation give us a nice example of a group, as we shall see momentarily. There is, of course, nothing very magical about the set $A=\{1,2,3\}$ here. Indeed, we could just as easily have used $\{1,2,3,\ldots,n\}$, for any positive integer n. The set of all permutations of this set, under the composition operation, is called the **symmetric group** on n letters, and is denoted S_n.

Exercises

3.1. In S_4, let $\sigma=\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}$ and $\tau=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$. Calculate the following.

1. $\sigma\tau$
2. $\tau\sigma$
3. the inverse of σ

3.2. In S_5, let $\sigma=\begin{pmatrix}1&2&3&4&5\\5&3&2&1&4\end{pmatrix}$ and $\tau=\begin{pmatrix}1&2&3&4&5\\2&4&1&3&5\end{pmatrix}$. Calculate the following.

1. $\sigma\tau\sigma$
2. $\sigma\sigma\tau$
3. the inverse of σ

3.3. How many permutations are there in S_n? In S_5, how many permutations α satisfy $\alpha(2)=2$?

3.4. Let H be the set of all permutations $\alpha\in S_5$ satisfying $\alpha(2)=2$. Which of the properties we have discussed (closure, associativity, identity, inverses) does H enjoy under composition of functions?

3.5. Consider the set of all functions from $\{1,2,3,4,5\}$ to $\{1,2,3,4,5\}$. Which of the properties (closure, associativity, identity, inverses) does this set enjoy under composition of functions?

3.6. Let G be the set of all permutations of $\mathbb{N}$. Which of the properties (closure, associativity, identity, inverses) does G enjoy under composition of functions?

3.2 Groups

We can now give the general definition of a group.

Definition 3.1. A **group** is a set G, together with a binary operation $*$, satisfying the following conditions:

1. $a * b \in G$ for all $a, b \in G$ (closure);
2. $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$ (associativity);
3. there exists an $e \in G$ such that $a * e = e * a = a$ for all $a \in G$ (existence of identity); and
4. for each $a \in G$, there exists a $b \in G$ such that $a * b = b * a = e$ (existence of inverses).

We will refer to G as a group **under** $*$.

The element e is called the **identity** of the group. If $a \in G$, and $a * b = b * a = e$, then b is called the **inverse** of a, and we write $b = a^{-1}$.

As we discussed in the previous section, the group operation does not have to be commutative. We have a special term for groups that do have this property, named after mathematician Niels H. Abel.

Definition 3.2. A group G is said to be **abelian** if $a * b = b * a$ for all $a, b \in G$.

We devote the remainder of this section to examples of groups.

Example 3.1. As we saw in Sections 2.4 and 2.5, $\mathbb{Z}$ and $\mathbb{Z}_n$ (for any integer $n \geq 2$) are abelian groups under addition. Indeed, 0 is the identity, and the inverse of a is $-a$. In fact, the same can be said for $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ under addition.

When a group G has only finitely many elements, we can represent it with a **group table**. We write the elements of G down the first column and along the first row of the table. Then the entry in the row headed by a and the column headed by b is $a * b$. For instance, the group table for $\mathbb{Z}_5$ is given in Table 3.1.

Table 3.1 Group table for the additive group $\mathbb{Z}_5$

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Example 3.2. Let G be the set of nonzero rational numbers. Then G is an abelian group under multiplication. Indeed, we see that the product of two nonzero rationals is a nonzero rational, hence closure is satisfied. Also, multiplication of rationals is both

associative and commutative. Clearly, $a \cdot 1 = a$, for all $a \in G$, so 1 is the identity. Finally, if $a = m/n \in G$, with m and n nonzero integers, then $a^{-1} = n/m \in G$, since $(m/n)(n/m) = 1$.

This last example merits a second look. In particular, it is worth noting that we cannot do the same thing with the set of nonzero integers. To be sure, the product of two nonzero integers is a nonzero integer, and the multiplication is associative. Also, 1 is the identity. But 2 has no inverse; that is, there is no integer a such that $2a = 1$. In fact, the only integers that would have inverses in this set are 1 and -1. The set $\{1, -1\}$ is easily seen to be a group under multiplication.

Let us see how the integers modulo n compare.

Example 3.3. Let $n \geq 2$ be a positive integer. Let $U(n)$ denote the set of all elements $a \in \mathbb{Z}_n$ such that $(a, n) = 1$. (For instance, $U(10) = \{1, 3, 7, 9\}$.) Let us ensure that this makes sense. That is, if $a \equiv b \pmod{n}$, and $(a, n) = 1$, then it had also better be the case that $(b, n) = 1$. But $a = b + nk$, for some integer k. Then, if c divides both b and n, then c divides a as well. We claim that $U(n)$ is an abelian group under the multiplication operation in $\mathbb{Z}_n$. First, closure. By Corollary 2.5, if $(a, n) = 1$ and $(b, n) = 1$, then $(ab, n) = 1$. We also know that multiplication in $\mathbb{Z}_n$ is associative and commutative, and 1 (which obviously lies in $U(n)$) is the identity. What about inverses? If $a \in U(n)$, then since $(a, n) = 1$, there exist integers u and v such that $au + nv = 1$. That is, in $\mathbb{Z}_n$, $au = ua = 1$. The group table of $U(10)$ is given in Table 3.2.

Table 3.2 Group table for the multiplicative group $U(10)$

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Note that we will use the notation $U(n)$ from the above example throughout the book.

Example 3.4. Let n be a positive integer, and let G be the set of all complex numbers w satisfying $w^n = 1$. Then we claim that G is an abelian group under multiplication. Of course, we know that the multiplication is both associative and commutative, and $1 \in G$ will serve as a multiplicative identity. If $v, w \in G$, then $(vw)^n = v^n w^n = 1$, so $vw \in G$, and we have closure. Also, if $w \in G$, then we know that $1/w \in \mathbb{C}$. But $(1/w)^n = 1/(w^n) = 1$, and therefore $1/w \in G$.

In particular, if $n = 4$ in the above example, then we get the group $\{1, -1, i, -i\}$. Also, if $n = 1$, then we just get the group consisting of the identity. This is known as the **trivial group**.

Of course, not all groups are abelian. Two useful examples follow.

Example 3.5. As we illustrated in the previous section, S_n is a group under composition. If $n \geq 3$, then the group is nonabelian.

Example 3.6. The set of all invertible 2×2 matrices with entries in $\mathbb{R}$ is called the **general linear group** over $\mathbb{R}$, and denoted $GL_2(\mathbb{R})$. It is a group under matrix multiplication. The identity matrix I_2 is the identity of $GL_2(\mathbb{R})$. Also, if $A, B \in GL_2(\mathbb{R})$, then

$$AB(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_2A^{-1} = AA^{-1} = I_2$$

and, similarly, $(B^{-1}A^{-1})AB = I_2$. Thus, AB is invertible as well, so $GL_2(\mathbb{R})$ is closed under multiplication. Also, matrix multiplication is associative. By definition of $GL_2(\mathbb{R})$, every element A has an inverse, and since $(A^{-1})^{-1} = A$, we know that $A^{-1} \in GL_2(\mathbb{R})$. Thus, $GL_2(\mathbb{R})$ is indeed a group. However, the group is nonabelian. For instance,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix},$$

whereas

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

By changing the entries in the matrices, we can obtain other general linear groups, such as $GL_2(\mathbb{Q})$. We can also use invertible $n \times n$ matrices and obtain $GL_n(\mathbb{R})$.

Let us also present a useful way of obtaining new groups from old ones.

Definition 3.3. Let G be a group with operation $*$ and H a group with operation $\bullet$. On the Cartesian product $G \times H$, define an operation $\diamond$ via

$$(g_1, h_1) \diamond (g_2, h_2) = (g_1 * g_2, h_1 \bullet h_2),$$

for all $g_i \in G$, $h_i \in H$. Under this operation, we call $G \times H$ the **direct product** of G and H.

Theorem 3.1. *The direct product of two groups is a group.*

Proof. Let us adopt the same notation as in the definition. First, we must check that the direct product is closed. But if $g_1, g_2 \in G, h_1, h_2 \in H$, then $(g_1, h_1) \diamond (g_2, h_2) = (g_1 * g_2, h_1 \bullet h_2) \in G \times H$, since $g_1 * g_2 \in G, h_1 * h_2 \in H$. The associativity of $\diamond$ follows from the associativity of $*$ and $\bullet$. Indeed, if $g_1, g_2, g_3 \in G, h_1, h_2, h_3 \in H$, then

$$\begin{aligned} ((g_1, h_1) \diamond (g_2, h_2)) \diamond (g_3, h_3) &= (g_1 * g_2, h_1 \bullet h_2) \diamond (g_3, h_3) \\ &= ((g_1 * g_2) * g_3, (h_1 \bullet h_2) \bullet h_3) \\ &= (g_1 * (g_2 * g_3), h_1 \bullet (h_2 \bullet h_3)) \\ &= (g_1, h_1) \diamond ((g_2, h_2) \diamond (g_3, h_3)). \end{aligned}$$

Let e_G and e_H be the identities of G and H respectively. Then for any $g \in G$, $h \in H$, we have

$$(g, h) \diamond (e_G, e_H) = (g * e_G, h \bullet e_H) = (g, h)$$

and, similarly, $(e_G, e_H) \diamond (g, h) = (g, h)$. Thus, (e_G, e_H) is the identity for $G \times H$. Furthermore, $(g, h) \diamond (g^{-1}, h^{-1}) = (g * g^{-1}, h \bullet h^{-1}) = (e_G, e_H)$ and, similarly, $(g^{-1}, h^{-1}) \diamond (g, h) = (e_G, e_H)$. Thus, $(g, h)^{-1} = (g^{-1}, h^{-1})$. The proof is complete. □

Example 3.7. Suppose that $G = \mathbb{Z}_5$ and $H = S_3$. Then in $G \times H$,

$$\left(4, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\right) \diamond \left(3, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\right) = \left(4 + 3, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\right) = \left(2, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\right).$$

Before concluding this section, it seems to be worth mentioning that part of the definition of a group is redundant. We specify that $*$ is a binary operation on G, and then require closure. But closure is part of the definition of a binary operation! Nevertheless, it is a good idea to emphasize this point, as closure must be checked whenever a new group is defined, and it is easy to forget about it if it is buried inside another definition.

Exercises

3.7. Give group tables for the following additive groups.

1. $\mathbb{Z}_3$
2. $\mathbb{Z}_3 \times \mathbb{Z}_2$

3.8. Give group tables for the following groups.

1. $U(12)$
2. S_3

3.9. Show that $G \times H$ is abelian if and only if G and H are abelian.

3.10. Let G be a group containing at most three elements. Show that G is abelian.

3.11. Explain why neither of the following is a group.

1. the set of positive rational numbers under division
2. the set of rational numbers $q \geq 1$ under multiplication

3.12. Is either of the following a group under addition?

1. the set of even integers
2. the set of odd integers

3.13. Let $G = \{a + bi \in \mathbb{C} : a^2 + b^2 = 1\}$. Is G a group under multiplication?

3.14. Let G be the following subset of $\mathbb{Z}_{15}$, namely $\{3, 6, 9, 12\}$. Show that G is a group under multiplication in $\mathbb{Z}_{15}$. Find the identity, and the inverse of each group element.

3.15. Let p be a prime and $G = \{a/p^n : a \in \mathbb{Z}, n \in \mathbb{N}\}$. Is G a group under addition?

3.16. Let G be the set of all matrices of the form $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$, with $a, b, c \in \mathbb{Z}$. Show that G is a group under matrix multiplication. Is it abelian?

3.3 A Few Basic Properties

Let us begin with a small notational change. Usually, when we are working inside a group, we suppress the symbol for the group operation. That is, we write ab instead of $a * b$. The major exception is where the operation is addition, in which case this **multiplicative notation** would be confusing. In that case, we will use **additive notation** and continue to write $a + b$ instead of ab, 0 instead of e and $-a$ instead of a^{-1} .

In the preceding section, we glossed over the uniqueness of the group identity and inverses of group elements. These are important points, if we are to speak of "the" identity, or write a^{-1} and have it mean something. Let us take care of this problem.

Theorem 3.2. *Let G be a group. Then*

1. *the identity of G is unique; and*
2. *if $a \in G$, then a^{-1} is unique.*

Proof. (1) Suppose that e and f are both identities in G. Then as f is an identity, $ef = e$. But as e is an identity, we also have $ef = f$. Therefore, $e = f$.

(2) Suppose that b and c are both inverses of a. Then as b is an inverse of a, $(ba)c = ec = c$. However, as c is an inverse of a, we have $b(ac) = be = b$. Given that our group operation is associative, $b = b(ac) = (ba)c = c$. □

We know that in any group, $(ab)c = a(bc)$. Thus, we can write abc without worrying about ambiguity. But we would like to be able to write $abcd$, for instance. To that end, we have the following result.

Theorem 3.3. *Let G be any group, and $a_1, a_2, \ldots, a_n \in G$. Then regardless of how the product $a_1 a_2 \cdots a_n$ is bracketed, the result equals $(\cdots(((a_1 a_2)a_3)a_4)\cdots a_{n-1})a_n$.*

Proof. Our proof is by strong induction upon n. If n is 1 or 2, no bracketing is needed, so there is nothing to do. When $n = 3$, this is the associativity from the definition of a group. Therefore, let $n \geq 4$, and suppose that the theorem is true for any product of fewer than n group elements. Take any bracketing of $w = a_1 \cdots a_n$, and look at the

last operation to be performed. Then $w = xy$, where x is the product $a_1 \cdots a_m$ and y is the product $a_{m+1} \cdots a_n$, each with some bracketing. By our inductive hypothesis, $x = (\cdots((a_1a_2)a_3) \cdots a_{m-1})a_m$ and $y = (\cdots((a_{m+1}a_{m+2})a_{m+3}) \cdots a_{n-1})a_n$. If $m = n - 1$, then writing xy in this way, we have our desired conclusion. If not, then by associativity,

$$xy = ((\cdots((a_1a_2)a_3) \cdots a_m)(\cdots((a_{m+1}a_{m+2})a_{m+3}) \cdots a_{n-1}))a_n.$$

Now applying our inductive hypothesis to the product of the first $n - 1$ terms, we obtain the desired bracketing. □

Therefore, we do not have to use brackets when we write a product of group elements. However, we must always remember that unless our group is abelian, we cannot rearrange terms at will. For instance, $(ab)(cd) = (a(bc))d$, and we can write both as $abcd$, but we cannot write $abcd = cdba$.

Let us also prove a couple of useful facts about inverses.

Theorem 3.4. *Let G be a group, with $a, b \in G$. Then*

1. $(a^{-1})^{-1} = a$; *and*
2. $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. (1) Since $aa^{-1} = a^{-1}a = e$, we see from the definition of inverses that the inverse of a^{-1} is a.

(2) Notice that $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$ and, similarly, $(b^{-1}a^{-1})(ab) = e$. Therefore, $b^{-1}a^{-1}$ is the inverse of ab. □

Do not make the mistake of thinking that the inverse of ab is $a^{-1}b^{-1}$!

In ordinary arithmetic with real numbers, we know that if $ab = ac$, and $a \neq 0$, then $b = c$. We have something similar for groups.

Theorem 3.5. (Cancellation Law). *Let G be a group and $a, b, c \in G$. If either $ab = ac$ or $ba = ca$, then $b = c$.*

Proof. If $ab = ac$, then $a^{-1}ab = a^{-1}ac$. As $a^{-1}a = e$, we have $eb = ec$, and therefore $b = c$. The proof is similar if $ba = ca$. □

When our group has finitely many elements, the cancellation law has important implications for the group table. Suppose that, in the row headed by a, the group element b occurs twice. Then there exist group elements c and d such that $ac = b = ad$. But then we know that $c = d$. Therefore, a group element can occur only once in each row. In the same way, there will be no repetitions in any column.

Corollary 3.1. *Let G be a group and $a, b \in G$. Then there exists exactly one $c \in G$ such that $ac = b$, and exactly one $d \in G$ such that $da = b$.*

Proof. We showed the uniqueness of c and d above. To show the existence of c and d, let $c = a^{-1}b$ and $d = ba^{-1}$. Then $ac = aa^{-1}b = eb = b$, and $da = ba^{-1}a = be = b$. □

Example 3.8. Suppose G is a group with four elements, a, b, c and d. If we are given the partial group table shown in Table 3.3, we can fill in the missing elements. Indeed, examining the first row, we see that ad cannot be b or d. The last column tells us that it also cannot be a, so $ad = c$. As there must be an a in the first row, $ab = a$. Filling in the rest of the table is left as an exercise.

Table 3.3 Incomplete group table

	a	b	c	d
a	d		b	
b		b		
c				a
d			a	

Exercises

3.17. Simplify each of the following expressions as far as possible in an arbitrary group G, leaving no brackets.

1. $(acb)(cbab)^{-1}$
2. $(a^{-1}bca)^{-1}$

3.18. Repeat the preceding exercise, assuming that G is abelian.

3.19. Fill in the rest of Table 3.3.

3.20. Let $G = \{v, w, x, y, z\}$ be a group with five elements. Further suppose that $vw = y$, $vy = v$, $wx = z$, $xv = w$ and $zw = v$. Fill in the group table for G.

3.21. Show that the following are equivalent for a group G:

1. for every $a, b, c \in G$ satisfying $ab = ca$, we have $b = c$; and
2. G is abelian.

3.22. Suppose that in the definition of a group, we replace the third part with the following weaker condition:

(3') There exists an $e \in G$ such that for every $a \in G$, $ae = a$.

(That is, we do not insist that $ea = a$.) Show that we still get a group.

3.4 Powers and Orders

In group theory, the word *order* is used in two different, but related, ways. One is easy.

Definition 3.4. If G is a group, then its **order**, $|G|$, is the number of elements in the set G. We say that G is a **finite group** if its order is finite; otherwise, it is an **infinite group**.

Example 3.9. If $G = \mathbb{Z}_5$, then $|G| = 5$, and therefore G is a finite group. On the other hand, $\mathbb{Z}$ is an infinite group.

To understand the other use of the word, we need to know about **powers** of group elements. Let G be any group, and $a \in G$. Then for any positive integer n, we let

$$a^n = \underbrace{aa \cdots a}_{n \text{ times}}.$$

(Alternatively, we could define the powers recursively. That is, let $a^1 = a$, and for each positive integer n, let $a^{n+1} = a^n a$.) Also, let $a^0 = e$ and, for each positive integer n, let $a^{-n} = (a^n)^{-1}$.

Example 3.10. In $U(20)$, we calculate $7^3 = 7 \cdot 7 \cdot 7 = 9 \cdot 7 = 3$. If we wanted to know 7^{-3}, then we would calculate $(7^3)^{-1} = 3^{-1} = 7$, since $3 \cdot 7 = 1$.

Powers behave in a rather nice manner, as the following theorem tells us.

Theorem 3.6. *Let G be a group, with $a \in G$, and let m and n be any integers. Then*

1. $a^m a^n = a^{m+n}$;
2. $(a^m)^n = a^{mn}$; *and, in particular,*
3. $a^{-n} = (a^{-1})^n$.

Proof. Exercise 3.26. □

We know that if the group operation is addition, then we will use additive notation, rather than multiplicative. In this case, our exponentiation notation would be confusing, so we will write things in a more familiar manner. Instead of a^n, we will write na (that is, add a to itself n times).

Example 3.11. In $\mathbb{Z}_{12}$, since our operation is addition, instead of writing 5^4, we would write $4 \cdot 5 = 5 + 5 + 5 + 5 = 8$.

Sometimes, a group will consist only of powers of a specific group element.

Definition 3.5. A group G is said to be **cyclic** if there exists an element a such that every element of G is a power of a. In particular, we say that G is **generated** by a, and write $G = \langle a \rangle$.

Example 3.12. The additive group $\mathbb{Z}$ is cyclic; indeed, $\mathbb{Z} = \langle 1 \rangle$. (Remember, in an additive group, the powers are integer multiples, so if $a \in \mathbb{Z}$, then $a = a \cdot 1$.) In fact, $\mathbb{Z} = \langle -1 \rangle$ as well, so the generator of the cyclic group is not unique. In the same way, $\mathbb{Z}_n$ is cyclic.

Example 3.13. Consider the multiplicative group of complex fourth roots of unity discussed in Example 3.4, namely $G = \{1, -1, i, -i\}$. Then G is cyclic. Indeed, $G = \langle i \rangle$ since the powers of i are i, -1, $-i$ and 1.

Not every group is cyclic. For one thing, we have the following fact.

Theorem 3.7. *Every cyclic group is abelian.*

Proof. Let $G = \langle a \rangle$. If $b, c \in G$, then $b = a^m$ and $c = a^n$, for some $m, n \in \mathbb{Z}$. Then $bc = a^m a^n = a^{m+n}$, but $cb = a^n a^m = a^{m+n}$ as well. □

However, abelian groups need not be cyclic.

Example 3.14. The group $U(10)$ is cyclic, but $U(8)$ is not. To see this, observe that $U(10) = \{1, 3, 7, 9\}$. But the powers of 3 are 3, 9, 7 and 1, so $U(10) = \langle 3 \rangle$. On the other hand, $U(8) = \{1, 3, 5, 7\}$. But the powers of 1 are all 1, the powers of 3 are 1 and 3, the powers of 5 are 1 and 5, and the powers of 7 are 1 and 7. Therefore, no element generates $U(8)$.

Now, let us discuss the order of a group element.

Definition 3.6. Let G be a group and $a \in G$. The **order** of a, denoted $|a|$, is the smallest positive integer n such that $a^n = e$, assuming that such an n exists, in which case a has **finite order**. If no such n exists, then a has **infinite order**.

Example 3.15. The identity of a group is the only element having order 1.

Example 3.16. In S_3, the element $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ has order 3; indeed, $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, whereas σ^3 is the identity.

Example 3.17. In $\mathbb{Z}$, every element other than 0 has infinite order. For instance, no matter how many times we add 8 to itself, we will never get 0.

Example 3.18. In $\mathbb{Z}_6$, we have $|0| = 1$, $|1| = |5| = 6$, $|2| = |4| = 3$ and $|3| = 2$. For instance, $1 \cdot 4 = 4 \neq 0$ and $2 \cdot 4 = 2 \neq 0$, but $3 \cdot 4 = 0$, so $|4| = 3$.

The order of an element tells us a great deal about its powers.

Theorem 3.8. *Let G be a group and $a \in G$. Suppose $i, j \in \mathbb{Z}$. Then*

1. *if a has infinite order, then $a^i = a^j$ if and only if $i = j$; and*
2. *if $|a| = n < \infty$, then $a^i = a^j$ if and only if $i \equiv j \pmod{n}$.*

Proof. (1) Suppose that $a^i = a^j$, but $i \neq j$. Without loss of generality, say $i > j$. Then $a^i (a^j)^{-1} = a^j (a^j)^{-1} = e$. That is, $a^{i-j} = e$. But $i - j$ is a positive integer, and this contradicts the assumption that a has infinite order.

(2) Suppose that $a^i = a^j$. Once again, $a^{i-j} = e$. Using the division algorithm, write $i - j = nq + r$, with $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then

$$e = a^{i-j} = a^{nq+r} = (a^n)^q a^r.$$

But $a^n = e$. Thus, $a^r = e$. But n is the smallest positive integer having this property, and $r < n$. Therefore, $r = 0$. That is, $n|(i - j)$, as required.

Conversely, suppose that $i \equiv j \pmod{n}$. Then let us write $i - j = nk$, for some $k \in \mathbb{Z}$. But we now have

$$a^{i-j} = a^{nk} = (a^n)^k = e^k = e.$$

Thus, $a^{i-j}a^j = ea^j$, and hence $a^i = a^j$. □

Example 3.19. In $U(10)$, we see that $|3| = 4$. Thus, $3^i = 3^j$ if and only if $4|(i - j)$. That is, $3^6 = 3^{14}$, but $3^2 \neq 3^{11}$.

Example 3.20. In $\mathbb{Z}$, all the integer multiples of 5 are distinct, because 5 has infinite order.

Corollary 3.2. *Let G be a group, and let $a \in G$ have order $n < \infty$. Then, for any integer i,*

1. *$a^i = e$ if and only if $n|i$; and*
2. *$|a^i| = n/(i, n)$.*

Proof. (1) By the preceding theorem, $a^i = e = a^0$ if and only if $i \equiv 0 \pmod{n}$. (2) Suppose that, for some positive integer j, we have $(a^i)^j = e$. We see from (1) that since $a^{ij} = e$, we have $n|ij$. Write $ij = nk$, with $k \in \mathbb{Z}$. Letting $d = (n, i)$, we have $j(i/d) = k(n/d)$. Now, $(n/d, i/d) = 1$. Thus, by Corollary 2.2, since $n/d|j(i/d)$, we must have $n/d|j$. Therefore, $|a^i| \geq n/d$. But $(a^i)^{n/d} = a^{in/d} = a^{n(i/d)}$. As i/d is an integer, this is $(a^n)^{i/d} = e^{i/d} = e$. Thus, $|a^i| = n/d$, as required. □

Example 3.21. Again considering 3 in $U(10)$, we note that $3^i = 1$ if and only if i is a multiple of 4. Also, $|3^{14}| = 4/(4, 14) = 4/2 = 2$.

If G is a group, and $a, b \in G$, then we say that b is a **conjugate** of a if there exists a $c \in G$ such that $b = c^{-1}ac$.

Theorem 3.9. *In any group, conjugate elements have the same order.*

Proof. Suppose that $b = c^{-1}ac$ and that $a^n = e$, for some positive integer n. Then

$$\begin{aligned} b^n = (c^{-1}ac)^n &= c^{-1}acc^{-1}acc^{-1} \cdots cc^{-1}ac \\ &= c^{-1}aeae \cdots ac = c^{-1}a^n c = c^{-1}ec = e. \end{aligned}$$

That is, $|b| \leq |a|$. But since $b = c^{-1}ac$, we have $a = (c^{-1})^{-1}bc^{-1}$. Thus, by the same argument, $|a| \leq |b|$. Therefore, $|a| = |b|$. □

Exercises

3.23. Find the order of each group, and the order of every element of each group.

1. $\mathbb{Z}_{12}$
2. $\mathbb{Z}_2 \times \mathbb{Z}_4$

3.24. Find the order of every element of each group. Is the group cyclic? If so, list all generators.

1. $U(14)$
2. S_3

3.25. Let $G = \langle a \rangle$ be a cyclic group of order 20. Find the orders of a^3, a^{12} and a^{15}.

3.26. Prove Theorem 3.6.

3.27. Let $a \in G$ and $b \in H$. Suppose that $|a| = 12$ and $|b| = 18$. Find the order of (a, b) in $G \times H$.

3.28. Let a and b be elements of odd order in a group. Show that a^2 and b^2 commute if and only if a and b commute. Also show that this does not have to hold if a and b have even order.

3.29. Let a and b be elements of a group. Show that the following pairs of elements have the same order:

1. a and a^{-1}; and
2. ab and ba.

3.30. Let $G = \{a_1, \ldots, a_k\}$ be a finite abelian group. Show that $a_1 a_2 \cdots a_k$ has order 1 or 2.

3.31. Show that it is possible for an abelian group to have exactly three elements of order 2, but not exactly four elements of order 2.

3.32. Suppose that G is a group in which every element has order 1 or 2. Show that G must be abelian.

3.5 Subgroups

One of the most important ways of obtaining new groups is to consider subgroups of a particular group.

Definition 3.7. Let G be a group with operation $*$. Then a subset H of G is called a **subgroup** of G if H is a group under the same operation $*$. In this case, we write $H \leq G$.

Example 3.22. Every group is a subgroup of itself, and $\{e\}$ is a subgroup of every group.

When we refer to a **proper** subgroup of G, we mean any subgroup other than G itself.

Example 3.23. We can see that $\mathbb{Z}$ is a subgroup of $\mathbb{Q}$, and both are subgroups of $\mathbb{R}$.

We do not have to check the entire definition of a group to see if a subset is a subgroup. For instance, we know that the group operation is associative on the entire group, so it is surely associative on every subset. The following theorem will save us some time.

Theorem 3.10. *Let G be a group and H a subset of G. Then H is a subgroup of G if and only if*

1. *$e \in H$ (the subset contains the identity);*
2. *$ab \in H$ for all $a, b \in H$ (the subset is closed); and*
3. *$a^{-1} \in H$ for all $a \in H$ (the subset contains all inverses).*

Proof. Let H be a subgroup of G. Then H has an identity, f. Thus, $ff = f$. But also, $ef = f$. By cancellation, $f = e$, giving (1). Then, by definition of a group, (2) and (3) must hold.

Conversely, suppose that (1)–(3) hold. We must check that H is a group. But by (2), H is closed. As the group operation is associative on G, it is associative on H. By (1) and (3), we have an identity and inverses as well. Therefore, H is a subgroup of G. □

A remark is in order here. To wit, we could replace condition (1) in the above theorem with the weaker condition

(1') H is not the empty set.

Indeed, if $a \in H$, then we see from (3) that $a^{-1} \in H$, and then (2) tells us that $e = aa^{-1} \in H$. So why not express it that way? Because sometimes, the subset we are checking is not a subgroup. And we can tell immediately that that is the case if the subset does not contain e.

Example 3.24. The set of all even integers, $2\mathbb{Z}$, is a subgroup of $\mathbb{Z}$. Indeed, we certainly have $0 = 2 \cdot 0 \in 2\mathbb{Z}$. If $2m, 2n \in 2\mathbb{Z}$, then $2m + 2n = 2(m + n) \in 2\mathbb{Z}$, so we have closure. Finally, if $2m \in 2\mathbb{Z}$, then its inverse is $-(2m) = 2(-m) \in 2\mathbb{Z}$, and we have inverses. Of course, there is nothing magical about the number 2 here. If a is an integer, than $a\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

In fact, this last example is a specific case of a more general phenomenon. We have already encountered cyclic groups.

Definition 3.8. Let G be a group and $a \in G$. Then the **cyclic subgroup generated by** a is the set of all powers of a in G, and we write

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\}.$$

Of course, the group G is cyclic if and only if there exists an $a \in G$ such that $G = \langle a \rangle$.

Theorem 3.11. *If G is a group and $a \in G$, then $\langle a \rangle$ is a subgroup of G.*

Proof. Certainly $e = a^0 \in \langle a \rangle$. Take any $a^m, a^n \in \langle a \rangle$. Then $a^m a^n = a^{m+n} \in \langle a \rangle$. Finally, if $a^m \in \langle a \rangle$, then $(a^m)^{-1} = a^{-m} \in \langle a \rangle$. Now apply Theorem 3.10. □

Example 3.25. In $U(10)$, the powers of 3 are 1, 3, 9 and 7, so $\langle 3 \rangle = \{1, 3, 7, 9\} = U(10)$. Similarly, $\langle 7 \rangle = U(10)$. But the only powers of 9 are 1 and 9, so $\langle 9 \rangle = \{1, 9\}$. Also, $\langle 1 \rangle = \{1\}$.

Example 3.26. In $\mathbb{Z}_{12}$, the multiples of 8 are $1 \cdot 8 = 8, 2 \cdot 8 = 4$ and $3 \cdot 8 = 0$. Thus, we have $\langle 8 \rangle = \{0, 4, 8\}$.

Of course, we do not insist upon commutativity in groups, but it can be useful to know which elements commute with everything.

Definition 3.9. If G is a group, then the **centre** of G, denoted $Z(G)$, is the set of elements of G that commute with everything in G. That is, $Z(G) = \{z \in G : az = za \text{ for all } a \in G\}$.

Example 3.27. If G is abelian, then $Z(G) = G$.

Example 3.28. The centre of S_3 is the trivial subgroup, $\{e\}$. Verifying this is a matter of considering each element of S_3 other than the identity, and finding another element that does not commute with it.

Example 3.29. The centre of $GL_2(\mathbb{R})$ is the set of all matrices $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, where $0 \neq a \in \mathbb{R}$. We leave the proof as Exercise 3.36.

Theorem 3.12. *If G is a group, then $Z(G)$ is a subgroup of G.*

Proof. Certainly $ea = a = ae$ for all $a \in G$, so $e \in Z(G)$. If $y, z \in Z(G)$ and $a \in G$, then $yza = yaz = ayz$; thus, $yz \in Z(G)$. Also, if $z \in Z(G)$ and $a \in G$, then $a^{-1}z = za^{-1}$. Inverting both sides, we get $z^{-1}a = az^{-1}$. Thus, $z^{-1} \in Z(G)$. The proof is complete. □

Some shortcuts are possible when it comes to testing whether a subset is a subgroup.

Theorem 3.13. *Let G be a group and H a subset of G. Then H is a subgroup if and only if*

1. $e \in H$; *and*
2. $ab^{-1} \in H$ *whenever* $a, b \in H$.

Proof. Suppose that H is a subgroup. By Theorem 3.10, we know that $e \in H$ and if $a, b \in H$, then $b^{-1} \in H$, and therefore $ab^{-1} \in H$.

Conversely, suppose that H satisfies (1) and (2). Take any $a, b \in H$. Then since $e \in H$, we have $ea^{-1} = a^{-1} \in H$ and, similarly, $b^{-1} \in H$. Therefore, $a(b^{-1})^{-1} = ab \in H$. In view of Theorem 3.10, H is a subgroup. □

Once again, instead of checking that $e \in H$, it is enough to verify that H is not empty. We can even make things simpler if H is a finite set.

Theorem 3.14. *Let G be a group and H a finite subset of G. Then $H \leq G$ if and only if*

1. $e \in H$; *and*
2. $ab \in H$ *whenever* $a, b \in H$.

Proof. If H is a subgroup of G, then Theorem 3.10 tells us that (1) and (2) hold. Conversely, suppose that (1) and (2) are true. By Theorem 3.10, we only need to show that if $a \in H$ then $a^{-1} \in H$. In view of (2), we have $aa = a^2 \in H$, and hence $a^2a = a^3 \in H$, and so on; thus, $a^n \in H$ for all positive integers n. But there are infinitely many such powers, and H is finite. Thus, there exist positive integers m and n, with $m > n$, such that $a^m = a^n$. Then $a^{m-n} = e$. If $m - n = 1$, then $a = e$, in which case $a^{-1} = e \in H$. So, suppose that $m - n > 1$. Then $aa^{m-n-1} = a^{m-n-1}a = a^{m-n} = e$. That is, $a^{m-n-1} = a^{-1}$. But $m - n - 1$ is a positive integer, and therefore $a^{m-n-1} \in H$, as required. □

We must be careful only to use the above theorem when H is finite. To see why, let G be the additive group of integers, and let H be the set of nonnegative integers. Then H contains 0 and is closed under addition, but H is not a subgroup of G, since 1 has no additive inverse.

Example 3.30. Let $G = \mathbb{Z}_8 \times \mathbb{Z}_8$, and let $H = \{(a, b) \in G : 4a = 0\}$. We claim that H is a subgroup of G. Clearly, $(0, 0) \in H$. Also, if $(a, b), (c, d) \in H$, then $(a, b) + (c, d) = (a + c, b + d)$, where $4(a + c) = 4a + 4c = 0 + 0 = 0$. Therefore, H is closed, and hence a subgroup.

We conclude the section with an extended, and important, example. Suppose we have a floor consisting of featureless square ceramic tiles. Let us pry up one of the tiles, and then consider all of the ways in which we can move the tile around in three-dimensional space, and then replace it so that it looks exactly as it did when we began. For convenience, let us label the vertices of the square 1, 2, 3 and 4. Then we can see that each vertex moves to the position of some vertex. Also, two vertices will not move to the same place. Once we have positioned the vertices, we

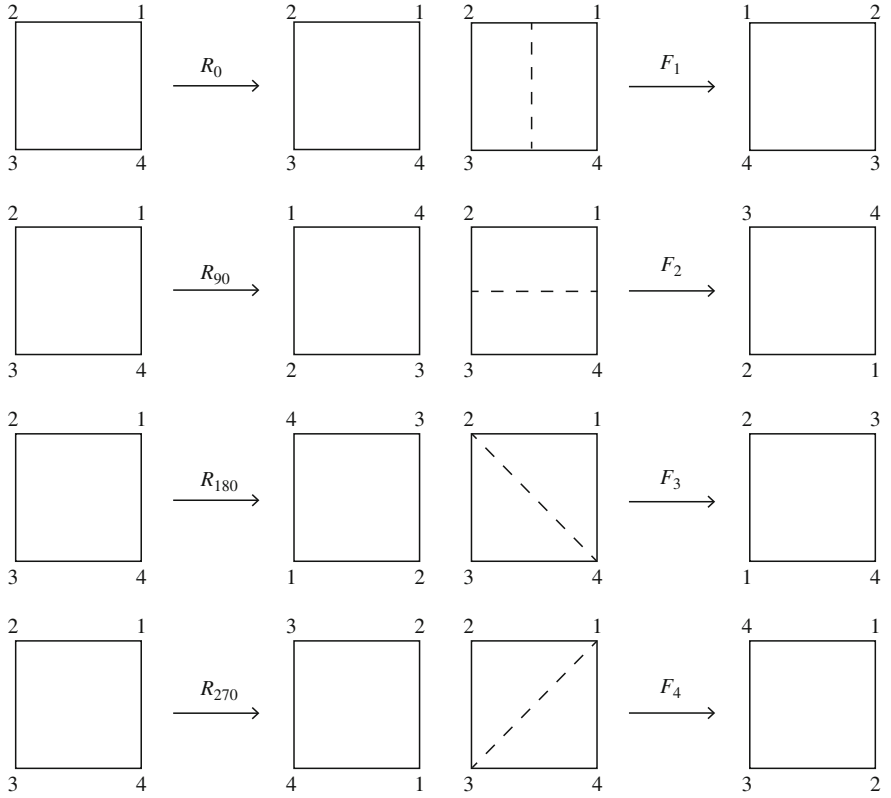

Fig. 3.1 The symmetries in the dihedral group D_8

are done. Therefore, these **symmetries** of a square can be regarded as permutations of the set $\{1, 2, 3, 4\}$; that is, as elements of S_4. Of course, the identity of S_4 is such a symmetry, and if we compose two of these symmetries, then we get another. Thus, by Theorem 3.14, they form a subgroup of S_4, known as the **dihedral group** of order 8, and denoted D_8.

What are the elements of D_8? They are illustrated in Figure 3.1. There are four **rotations**, R_0, R_{90}, R_{180} and R_{270}, where R_α is a counterclockwise rotation by α degrees. We also have four **flips**, F_1 through F_4, about the lines shown in the diagram.

And that is all! Indeed, vertex 1 can go to any of the 4 vertices, but then vertex 2 must be adjacent to it, not diagonally opposite. Once vertices 1 and 2 are positioned, the others fall into place. Therefore, $|D_8| = 8$. The group table of D_8 is shown in Table 3.4.

Remember that when we write $R_{90}F_1 = F_3$, we mean perform F_1 first, then R_{90}. We note that $R_{90}F_1 \neq F_1R_{90}$, and therefore D_8 is a nonabelian group of order 8. In fact, a quick glance through the table tells us that the centre of D_8 is $\{R_0, R_{180}\}$.

Table 3.4 Group table for the dihedral group D_8

	R_0	R_{90}	R_{180}	R_{270}	F_1	F_2	F_3	F_4
R_0	R_0	R_{90}	R_{180}	R_{270}	F_1	F_2	F_3	F_4
R_{90}	R_{90}	R_{180}	R_{270}	R_0	F_3	F_4	F_2	F_1
R_{180}	R_{180}	R_{270}	R_0	R_{90}	F_2	F_1	F_4	F_3
R_{270}	R_{270}	R_0	R_{90}	R_{180}	F_4	F_3	F_1	F_2
F_1	F_1	F_4	F_2	F_3	R_0	R_{180}	R_{270}	R_{90}
F_2	F_2	F_3	F_1	F_4	R_{180}	R_0	R_{90}	R_{270}
F_3	F_3	F_1	F_4	F_2	R_{90}	R_{270}	R_0	R_{180}
F_4	F_4	F_2	F_3	F_1	R_{270}	R_{90}	R_{180}	R_0

We do not have to begin with a square. Indeed, let us consider any regular n-gon, with $n \geq 3$. Then the symmetries of this n-gon form a subgroup of S_n. By precisely the same arguments as above, it will consist of n rotations and n flips. (There are n possible locations for a given vertex, and once it is fixed, 2 choices for an adjacent vertex. After fixing those vertices, there are no choices remaining.) We call this group of symmetries the dihedral group of order $2n$, and denote it by D_{2n}. In particular, if $n = 3$, we note that D_6 consists of all of S_3, but for larger n, D_{2n} is a proper subgroup of S_n. In any case, we now have an example of a nonabelian group of every even order except 2 and 4.

Exercises

3.33. In each case, is H a subgroup of G?

1. $G = GL_2(\mathbb{R})$, H is the set of matrices with determinant 1
2. $G = D_{10}$, H is the set of flips
3. $G = \mathbb{Q}$, $H = \{a/b : a, b \in \mathbb{Z}, 2 \nmid b\}$

3.34. In each case, is H a subgroup of G?

1. $G = D_{10}$, H is the set of rotations
2. $G = \mathbb{Q}$, H is the set of nonnegative rational numbers
3. G is the multiplicative group of nonzero rational numbers, H is the set of positive rational numbers

3.35. For each positive integer $n \geq 3$, determine the centre of D_{2n}.

3.36. Show that the centre of $GL_2(\mathbb{R})$ consists of the matrices $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, for all $0 \neq a \in \mathbb{R}$.

3.37. Show that the intersection of two subgroups of G is also a subgroup. Then extend this to show that if N_i is a subgroup of G for every i in some set T, then $\bigcap_{i \in T} N_i$ is a subgroup of G.

3.38. Let H and K be subgroups of G. Show that $H \cup K$ is a subgroup of G if and only if either $H \subseteq K$ or $K \subseteq H$.

3.39. Find every cyclic subgroup of each of the following groups.

1. $\mathbb{Z}_{20}$
2. $U(16)$

3.40. Let G be an abelian group and $n \in \mathbb{N}$. Let $H = \{a \in G : a^n = e\}$ and $K = \{a^n : a \in G\}$. Show that H and K are subgroups of G.

3.41. In any dihedral group, show that a rotation followed by a rotation, or a flip followed by a flip, is a rotation, whereas a rotation followed by a flip or a flip followed by a rotation is a flip.

3.42. Let G be the set of all sequences of integers $(a_1, a_2, a_3, \ldots)$.

1. Show that G is a group under $(a_1, a_2, \ldots) + (b_1, b_2, \ldots) = (a_1 + b_1, a_2 + b_2, \ldots)$.
2. Let H be the set of all elements $(a_1, a_2, \ldots)$ of G such that only finitely many a_i are different from 0 (and $(0, 0, 0, \ldots) \in H$). Show that H is a subgroup of G.

3.6 Cyclic Groups

Cyclic groups have a very straightforward structure. Let us prove a few basic facts. First, we can illustrate the link between the order of an element and the order of a group.

Theorem 3.15. *Let $G = \langle a \rangle$ be cyclic. If a has infinite order, then all powers of a are distinct. If $|a| = n < \infty$, then the distinct elements of G are $e, a, a^2, \ldots, a^{n-1}$. In particular, $|a| = |\langle a \rangle|$.*

Proof. If a has infinite order, then we can use Theorem 3.8. Suppose $|a| = n < \infty$. If $m \in \mathbb{Z}$, then write $m = nq + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then as $m \equiv r \pmod{n}$, Theorem 3.8 tells us that $a^m = a^r$. In particular, every element of G is equal to some a^i $(0 \leq i < n)$. Now, suppose that $a^i = a^j$, with $0 \leq i < j < n$. Then by Theorem 3.8, $i \equiv j \pmod{n}$. But given the range of values for i and j, this is impossible. □

The subgroups of cyclic groups are also easy to determine.

Theorem 3.16. *Every subgroup of a cyclic group is cyclic.*

Proof. Let $G = \langle a \rangle$, and let $H \leq G$. If $H = \{e\}$, then $H = \langle e \rangle$, and we are done, so assume that H is not the trivial subgroup. Then H contains a^m, for some nonzero integer m. If $m < 0$, then H also contains $(a^m)^{-1} = a^{-m}$, so H contains a positive power of a. Let n be the smallest positive integer such that $a^n \in H$. We claim that $H = \langle a^n \rangle$. Surely H contains every power of a^n, so $\langle a^n \rangle \leq H$. But suppose $a^k \in H$. Then write $k = nq + r$, with $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Now, H contains a^k and $(a^n)^{-q}$, and therefore $a^k(a^n)^{-q} = a^{k-nq} = a^r$. But n is the smallest positive integer such that $a^n \in H$. As $r < n$, we can only have $r = 0$. Thus, $a^k = (a^n)^q \in \langle a^n \rangle$. That is, $H \leq \langle a^n \rangle$, proving the claim. We are done. □

Actually, we can say more.

Corollary 3.3. *Let $G = \langle a \rangle$, where $|a| = n < \infty$. Then the order of every subgroup of G is a divisor of n. Furthermore, if m is a positive divisor of n, then G has exactly one subgroup of order m, namely $\langle a^{n/m} \rangle$.*

Proof. By the preceding theorem, every subgroup is of the form $\langle a^k \rangle$, for some $k \in \mathbb{Z}$. But Corollary 3.2 tells us that the order of every power of a is a divisor of n.

Let m be a positive divisor of n. Again using Corollary 3.2, we see that $|a^{n/m}| = n/(n, n/m) = n/(n/m) = m$. Thus, $\langle a^{n/m} \rangle$ is indeed a subgroup of order m. Let us check that it is unique. Suppose that $\langle a^k \rangle$ is a subgroup of order m. Then $|a^k| = m$, and so $(a^k)^m = e$. That is, $a^{km} = e$, hence $n|km$. But then $n/m|k$. Writing $k = (n/m)i$, with $i \in \mathbb{Z}$, we have $a^k = (a^{n/m})^i \in \langle a^{n/m} \rangle$. Thus, $\langle a^k \rangle \leq \langle a^{n/m} \rangle$. But these two subgroups have the same order. Therefore, they are equal. □

Example 3.31. Let $G = \langle a \rangle$, where $|a| = 20$. Then G has exactly one subgroup of order 5, namely $\langle a^4 \rangle = \{e, a^4, a^8, a^{12}, a^{16}\}$.

Thus, a cyclic group can only have one subgroup of any given order. This is a special property of cyclic groups; indeed, D_8 and $U(8)$ are easily seen to have several different cyclic subgroups of order 2.

We can also discuss the number of elements of a particular order in a cyclic group. Some notation will be helpful. The following function is named after Leonhard Euler.

Definition 3.10. The **Euler phi-function** is a function $\varphi : \mathbb{N} \to \mathbb{N}$, where $\varphi(n)$ is the number of positive integers less than or equal to n that are relatively prime to n.

Example 3.32. Of the integers from 1 to 10, only 1, 3, 7 and 9 are relatively prime to 10, so $\varphi(10) = 4$. The first few values of φ are given in Table 3.5.

From the definition of the group $U(n)$, we immediately obtain the following.

Theorem 3.17. *For any positive integer n, $|U(n)| = \varphi(n)$.*

But we can also use the Euler function to count the elements of a particular order in a finite cyclic group.

Theorem 3.18. *Let $G = \langle a \rangle$ be a cyclic group of order n. Let m be a positive divisor of n. Then the number of elements of order m in G is $\varphi(m)$.*

Proof. If b is an element of order m in G, then $\langle b \rangle$ must be the unique cyclic subgroup of order m. That is, all of the elements of order m in G are in the cyclic subgroup of order m. Thus, we may as well assume that G is cyclic of order m. We must

Table 3.5 Values of the Euler phi-function

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8

therefore decide which elements of this group have order m. But by Corollary 3.2, the order of a^k is m if and only if $(k, m) = 1$. By definition, the number of such k, with $1 \leq k \leq m$, is $\varphi(m)$. (By Theorem 3.15, the elements of $\langle a \rangle$ are precisely a^i, with $0 \leq i < m$, but as $a^0 = a^m = e$, this is the same as considering a^i with $1 \leq i \leq m$.) □

Example 3.33. Let $G = \langle a \rangle$ be cyclic of order 50. Then we know that there are $\varphi(10) = 4$ elements of order 10 in G. They lie in the subgroup of order 10, namely $\langle a^{50/10} \rangle = \langle a^5 \rangle$. Indeed, the precise elements will be $(a^5)^k$, where $(k, 10) = 1$. This means that $k \in \{1, 3, 7, 9\}$, so the elements of order 10 are a^5, a^{15}, a^{35} and a^{45}. It is worth noting that the number of elements of order 10 in a cyclic group of order one million is also $\varphi(10) = 4$.

For relatively small numbers, $\varphi(n)$ is easy to determine, but for large n, it would be tedious to go through all the numbers from 1 to n in order to see if they are relatively prime to n. Happily, there is a shortcut. The first part of the following theorem is Exercise 3.45. It will make more sense if we postpone the proof of the second part until Section 4.4.

Theorem 3.19. *Let p be a prime number, and let m and n be positive integers. Then*

1. $\varphi(p^n) = p^n - p^{n-1}$; *and*
2. *if* $(m, n) = 1$, *then* $\varphi(mn) = \varphi(m)\varphi(n)$.

Thus, we can determine $\varphi(n)$ by writing n as a product of powers of primes and then using the above theorem.

Example 3.34. We have $\varphi(81) = 81 - 27 = 54$ and $\varphi(540) = \varphi(4)\varphi(27)\varphi(5) = (4 - 2)(27 - 9)(5 - 1) = 144$.

Exercises

3.43. 1. Let $G = \langle a \rangle$ be a cyclic group of order 12. List every subgroup of G.
2. List every subgroup of $\mathbb{Z}_{12}$.

3.44. 1. Let $G = \langle a \rangle$ be a cyclic group of order 120. List all of the elements of order 12 in G.
2. How many elements of order 12 are there in a cyclic group of order 1200?

3.45. Let p be a prime and n a positive integer. Show that $\varphi(p^n) = p^n - p^{n-1}$.

3.46. Find all positive integers n such that $|U(n)| = 24$.

3.47. Let G be a nonabelian group. If H and K are cyclic subgroups of G, does it follow that $H \cap K$ is also a cyclic subgroup? Prove that it does, or provide a counterexample.

3.48. Let $G = \langle a \rangle$ be infinite cyclic. If m and n are positive integers, find a generator for $\langle a^m \rangle \cap \langle a^n \rangle$.

3.49. Let n be a positive integer and let T be the set of positive integers that divide n. Show that $\sum_{k\in T} \varphi(k) = n$.

3.50. For precisely which positive integers n is $U(2^n)$ cyclic?

3.51. Let G be any group and n a positive integer.

1. If H and K are subgroups of order n in G, and $H \neq K$, show that $H \cap K$ does not contain any elements of order n.
2. Show that the number of elements of order n in G is either a multiple of $\varphi(n)$ or infinite.

3.52. Show that a nontrivial group G has no nontrivial proper subgroups if and only if G is cyclic of prime order. (Do not assume, to begin with, that G is finite.)

3.7 Cosets and Lagrange's Theorem

One important fact we learned in the preceding section is that if G is a finite cyclic group, then the order of every subgroup of G divides the order of G. As it turns out, this is true for all finite groups, but a different proof will be required. To this end, we need some new terminology.

Definition 3.11. Let G be a group and H a subgroup. If $a, b \in G$, we say that a is **congruent to** b **modulo** H, and we write $a \equiv b \pmod{H}$, if $a^{-1}b \in H$ (or, in the case of an additive group, if $-a + b \in H$).

Example 3.35. Let $G = \mathbb{Z}$ and $H = 5\mathbb{Z}$. Then as $-1 + 16 = 15 \in H$, we see that $1 \equiv 16 \pmod{H}$. In this particular case, the notion is identical to congruence modulo 5.

Example 3.36. Let $G = U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$, and let $H = \langle 3\rangle$; namely, $H = \{1, 3, 7, 9\}$. Then we note that $13^{-1} \cdot 19 = 17 \cdot 19 = 3 \in H$. Thus, $13 \equiv 19 \pmod{H}$.

Lemma 3.1. *Let G be a group and H a subgroup. Then congruence modulo H is an equivalence relation on G.*

Proof. Reflexivity: If $a \in G$, then $a^{-1}a = e \in H$, and therefore $a \equiv a \pmod{H}$. Symmetry: If $a, b \in G$ and $a \equiv b \pmod{H}$, then $a^{-1}b \in H$, and therefore $(a^{-1}b)^{-1} = b^{-1}a$ lies in H as well. But this means that $b \equiv a \pmod{H}$. Transitivity: Suppose that $a, b, c \in G$, where $a \equiv b \pmod{H}$ and $b \equiv c \pmod{H}$. Then $a^{-1}b, b^{-1}c \in H$. But in this case, H contains their product, $a^{-1}bb^{-1}c = a^{-1}c$. Thus, $a \equiv c \pmod{H}$. We are done. □

What are the equivalence classes?

Lemma 3.2. *Let G be a group and H a subgroup. If $a \in G$, then its equivalence class with respect to congruence modulo H is the set $\{ah : h \in H\}$.*

Proof. If $a \equiv b \pmod{H}$, then $a^{-1}b \in H$, so $a^{-1}b = h$, for some $h \in H$. Thus, $b = ah$, which is in our set. Conversely, if $b = ah$, for some $h \in H$, then $a^{-1}b = h \in H$, and therefore $a \equiv b \pmod{H}$. □

We need a name for this set.

Definition 3.12. Let G be a group, $H \leq G$ and $a \in G$. Then the **left coset** of a with respect to H is the set $\{ah : h \in H\}$, which is denoted aH. (Note: If the group operation is addition, then we will write $a + H = \{a + h : h \in H\}$.)

Example 3.37. If $G = U(20)$, let $H = \langle 9 \rangle = \{1, 9\}$. Then $3H = \{3 \cdot 1, 3 \cdot 9\} = \{3, 7\}$. Also, $7H = \{7 \cdot 1, 7 \cdot 9\} = \{3, 7\}$, so $3H = 7H$. Furthermore, $1H = 9H = H$, $11H = 19H = \{11, 19\}$ and $13H = 17H = \{13, 17\}$. Note that these left cosets partition G.

Example 3.38. Let $G = \mathbb{Z}$ and $H = 3\mathbb{Z}$. Then there are three left cosets: $0 + H = H$, $1 + H = \{\cdots, -5, -2, 1, 4, 7, \ldots\}$ and $2 + H = \{\cdots, -4, -1, 2, 5, 8, \ldots\}$. Note that $2 + H = 5 + H = -13 + H$, and so on. Again, the left cosets partition G.

In general, we know that equivalence classes always partition a set. Therefore, we can record the following result.

Theorem 3.20. *Let G be a group and H a subgroup. Then the left cosets of H in G partition G. In particular,*

1. *each $a \in G$ is in exactly one left coset, namely aH; and*
2. *if $a, b \in G$, then either $aH = bH$ or $aH \cap bH = \varnothing$.*

Two points should be kept in mind here. First, left cosets are not subgroups! Remember, the left cosets partition G, and therefore the identity can only be in one of them, namely, $eH = H$. The rest cannot possibly be subgroups. Second, as we have already seen, when we write aH, the element a is not unique. Indeed, since the left cosets are equivalence classes, we have $aH = bH$ if and only if $a^{-1}b \in H$.

We can now prove our first big result on finite groups, due to Joseph-Louis Lagrange.

Theorem 3.21. (Lagrange's Theorem). *Let G be a finite group and H a subgroup. Then $|H|$ divides $|G|$.*

Proof. We have already seen that G is partitioned into left cosets; in particular, $|G|$ is the sum of the sizes of these left cosets. But for any $a \in G$, $aH = \{ah : h \in H\}$. Now, if $ah_1 = ah_2$, with $h_1, h_2 \in H$, then by the cancellation law, $h_1 = h_2$. Therefore, aH consists of precisely $|H|$ distinct elements. It now follows that the order of G is $|H|$ multiplied by the number of left cosets. In particular, $|H|$ divides $|G|$. □

Definition 3.13. Let G be a group and $H \leq G$. Then the **index** of H in G, denoted $[G : H]$, is the number of left cosets of H in G.

Corollary 3.4. *If G is a finite group and H is a subgroup, then $[G : H] = |G|/|H|$.*

Proof. This is immediate from the proof of the above theorem. □

Example 3.39. Let $G = D_8$ and $H = \langle R_{90} \rangle = \{R_0, R_{90}, R_{180}, R_{270}\}$. Then $[G : H] = |G|/|H| = 8/4 = 2$. Thus, there are two left cosets. One is $R_0 H = H$. The other must be $F_1 H = \{F_1, F_2, F_3, F_4\}$. If $K = \langle F_1 \rangle = \{R_0, F_1\}$, then it must have $8/2 = 4$ left cosets. One is $R_0 K = K$. To find another, just choose an element of G that we have not yet found, say R_{90}. Then we get $R_{90} K = \{R_{90}, F_3\}$. We haven't yet used F_2, so take $F_2 K = \{F_2, R_{180}\}$. Finally, we can take $R_{270} K = \{R_{270}, F_4\}$.

Example 3.40. Note that the subgroups of an infinite group can be of finite or infinite index. For instance, we saw above that $0 + 3\mathbb{Z}$, $1 + 3\mathbb{Z}$ and $2 + 3\mathbb{Z}$ are the distinct left cosets of $3\mathbb{Z}$ in $\mathbb{Z}$. Thus, $[\mathbb{Z} : 3\mathbb{Z}] = 3$. On the other hand, $\mathbb{Z}$ has infinite index in $\mathbb{Q}$. To see this, observe that for all positive integers n, the left cosets $1/n + \mathbb{Z}$ are distinct. And there are still more!

Lagrange's theorem has a beautiful consequence.

Corollary 3.5. *Let G be a finite group, and $a \in G$. Then the order of a divides the order of G.*

Proof. The order of a is the order of the cyclic subgroup generated by a, and that must divide the order of G. □

Example 3.41. Note that $|D_8| = 8$, the identity has order 1, R_{180} and the flips all have order 2 and $|R_{90}| = |R_{270}| = 4$. All of the orders are divisors of 8.

Of course, it does not follow that because a number n divides the order of a group, then the group has an element of that order. Indeed, if that were always true, then a group of order n would have to have an element of order n, and therefore every finite group would be cyclic, which is not the case.

One important thing that we can do is to try to classify all the groups of some particular order. We can now make a step in that direction.

Corollary 3.6. *Every group of prime order is cyclic.*

Proof. Take $e \neq a \in G$, where $|G|$ is a prime. As $|a|$ divides $|G|$, and $|a| \neq 1$, we must have $|a| = |G|$. But then $|G| = |\langle a \rangle|$, and therefore $G = \langle a \rangle$. □

Not surprisingly, there is also such a thing as a right coset. Indeed, if we had defined $a \equiv b \pmod{H}$ to mean that $ab^{-1} \in H$, then we would have found that this is still an equivalence relation, and the equivalence classes would have been as follows.

Definition 3.14. Let G be a group and $H \leq G$. Then for any $a \in G$, the **right coset** of a with respect to H is $Ha = \{ha : h \in H\}$. (If G is an additive group, then we write $H + a = \{h + a : h \in H\}$.)

If G is abelian, then there is no distinction between left and right cosets. In nonabelian groups, right cosets also partition G, but possibly in a different way.

Example 3.42. Take G, H and K as in Example 3.39. Then we can see that one right coset of H in G is $HR_0 = H = R_0H$ and the other must be $HF_1 = \{F_1, F_2, F_3, F_4\} = F_1H$. Here, the left and right cosets agree. But it is not the same for K. For instance, $R_{90}K = \{R_{90}, F_3\}$, but $KR_{90} = \{R_{90}, F_4\}$.

Would it have made a difference if we had defined the index of H in G using right cosets instead of left? Fortunately, no. This is clear if G is finite, as Lagrange's theorem works equally well using right cosets. But what if G is an infinite group having a subgroup H of index $n < \infty$? Then notice that $aH = bH$ if and only if $a^{-1}b \in H$, but also $Ha^{-1} = Hb^{-1}$ if and only if $a^{-1}b \in H$. Thus, if the distinct left cosets of H in G are $a_1H, a_2H, \ldots, a_nH$, then the distinct right cosets are $Ha_1^{-1}, Ha_2^{-1}, \ldots, Ha_n^{-1}$.

Exercises

3.53. For each group G and subgroup H, find all the left cosets and right cosets of H in G.

1. $G = \mathbb{Z}$, $H = 4\mathbb{Z}$
2. $G = D_8$, $H = \langle F_2 \rangle$

3.54. For each group G and subgroup H, find all the left cosets and right cosets of H in G.

1. $G = U(13)$, $H = \langle 8 \rangle$
2. $G = S_3$, $H = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\rangle$

3.55. Let G be a group whose order is the product of two (not necessarily distinct) primes. Show that every proper subgroup of G is cyclic.

3.56. Let G be a group of order p^n, for some prime p and positive integer n. Show that G has an element of order p.

3.57. Let G be a group having a subgroup H of order 28 and a subgroup K of order 65. Show that $H \cap K = \{e\}$.

3.58. Let G be a finite group having an element of order k, for each $1 \leq k \leq 10$. What is the smallest possible order of G? Show that a group of that order exists having this property.

3.59. Let $G = \{a_1, \ldots, a_k\}$ be an abelian group of odd order k. Show that $a_1a_2 \cdots a_k = e$.

3.60. Show that every group of order 55 contains an element of order 5 and an element of order 11.

3.61. Let G be a group with subgroups H and K. If $[G : K] = n$, show that $[H : H \cap K] \leq n$.

3.62. Let G be a group with subgroups H and K such that $K \leq H$. Suppose that $[G : H] = m$ and $[H : K] = n$. Show that $[G : K] = mn$. (Do not assume that G is finite.)