Note that all three of these presentations can give groups of order at most 10, since the last relation $ba = a^i b$ enables us to express every product of a's and b's in G in the form $a^s b^t$. Then $a^5 = 1$ and $b^2 = 1$ show that the set

$$S = \{a^0b^0, a^1b^0, a^2b^0, a^3b^0, a^4b^0, a^0b^1, a^1b^1, a^2b^1, a^3b^1, a^4b^1\}$$

includes all elements of G.

It is not yet clear that all these elements in S are distinct, so that we have in all three cases a group of order 10. For example, the group presentation

$$(a, b : a^5 = 1, b^2 = 1, ba = a^2b)$$

gives a group in which, using the associative law, we have

$$\begin{aligned} a &= b^2a = (bb)a = b(ba) = b(a^2b) = (ba)(ab) \\ &= (a^2b)(ab) = a^2(ba)b = a^2(a^2b)b = a^4b^2 = a^4 \end{aligned}$$

Thus in this group, $a = a^4$, so $a^3 = 1$, which, together with $a^5 = 1$, yields $a^2 = 1$. But $a^2 = 1$, together with $a^3 = 1$, means that $a = 1$. Hence every element in the group with presentation

$$(a, b : a^5 = 1, b^2 = 1, ba = a^2b)$$

is equal to either 1 or b; that is, this group is isomorphic to $\mathbb{Z}_2$. A similar study of

$$(bb)a = b(ba)$$

for

$$(a, b : a^5 = 1, b^2 = 1, ba = a^3b)$$

shows that $a = a^4$ again, so this also yields a group isomorphic to $\mathbb{Z}_2$.

This leaves just

$$(a, b : a^5 = 1, b^2 = 1, ba = a^4b)$$

as a candidate for a nonabelian group of order 10. As in Example 21.4 this is a presentation of the dihedral group D_5.

If we were unaware of the dihedral group, how would we show that the presentation gives a group with 10 elements? One attack is as follows. Let us try to make S into a group by defining $(a^s b^t)(a^u b^v)$ to be $a^x b^y$, where x is the remainder of $s + u(4^t)$ when divided by 5, and y is the remainder of $t + v$ when divided by 2, in the sense of the division algorithm (Theorem 6.2). The formula $s + u(4)^t$ is counting what the power of a should be after moving u copies of a by t copies of b. In other words, we use the relation $ba = a^4b$ as a guide in defining the product $(a^s b^t)(a^u b^v)$ of two elements of S. We see that a^0b^0 acts as identity, and that given $a^u b^v$, we can determine t and s successively by letting

$$t \equiv -v \pmod 2$$

and then

$$s \equiv -u(4^t) \pmod 5,$$

giving $a^s b^t$, which is a left inverse for $a^u b^v$. We will then have a group structure on S if and only if the associative law holds. Exercise 13 asks us to carry out the straightforward computation for the associative law and to discover a condition for S to be a group under such a definition of multiplication. The criterion of the exercise in this case amounts to the valid congruence

$$4^2 \equiv 1 \pmod 5.$$

Thus we do get a group of order 10. Note that

$$2^2 \not\equiv 1 \pmod 5$$

and

$$3^2 \not\equiv 1 \pmod 5,$$

so Exercise 13 also shows that

$$(a, b : a^5 = 1, b^2 = 1, ba = a^2b)$$

and

$$(a, b : a^5 = 1, b^2 = 1, ba = a^3b)$$

do not give groups of order 10. ▲

21.7 Example Let us determine all groups of order 8 up to isomorphism. We know the three abelian ones:

$$\mathbb{Z}_8, \qquad \mathbb{Z}_2 \times \mathbb{Z}_4, \qquad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Using generators and relations, we shall give presentations of the nonabelian groups.

Let G be nonabelian of order 8. Since G is nonabelian, it has no elements of order 8, so each element but the identity is of order either 2 or 4. If every element were of order 2, then for $a, b \in G$, we would have $(ab)^2 = 1$, that is, $abab = 1$. Then since $a^2 = 1$ and $b^2 = 1$ also, we would have

$$ba = a^2bab^2 = a(ab)^2b = ab,$$

contrary to our assumption that G is not abelian. Thus G must have an element of order 4.

Let $\langle a \rangle$ be a subgroup of G of order 4. If $b \notin \langle a \rangle$, the cosets $\langle a \rangle$ and $b\langle a \rangle$ exhaust all of G. Hence a and b are generators for G and $a^4 = 1$. Since $\langle a \rangle$ is normal in G (by Sylow theory, or because it is of index 2), $G/\langle a \rangle$ is isomorphic to $\mathbb{Z}_2$ and we have $b^2 \in \langle a \rangle$. If $b^2 = a$ or $b^2 = a^3$, then b would be of order 8. Hence $b^2 = 1$ or $b^2 = a^2$. Finally, since $\langle a \rangle$ is normal, we have $bab^{-1} \in \langle a \rangle$, and since $b\langle a \rangle b^{-1}$ is a subgroup conjugate to $\langle a \rangle$ and hence isomorphic to $\langle a \rangle$, we see that bab^{-1} must be an element of order 4. Thus $bab^{-1} = a$ or $bab^{-1} = a^3$. If bab^{-1} were equal to a, then ba would equal ab, which would make G abelian. Hence $bab^{-1} = a^3$, so $ba = a^3b$. Thus we have two possibilities for G, namely,

$$G_1 : (a, b : a^4 = 1, b^2 = 1, ba = a^3b)$$

and

$$G_2 : (a, b : a^4 = 1, b^2 = a^2, ba = a^3b).$$

Note that $a^{-1} = a^3$, and that b^{-1} is b in G_1 and b^3 in G_2. These facts, along with the relation $ba = a^3b$, enable us to express every element in G_i in the form a^mb^n, as in Examples 21.3 and 21.6. Since $a^4 = 1$ and either $b^2 = 1$ or $b^2 = a^2$, the possible elements in each group are

$$1, \quad a, \quad a^2, \quad a^3, \quad b, \quad ab, \quad a^2b, \quad a^3b.$$

Thus G_1 and G_2 each have order at most 8. The first group G_1 is sometimes called the **octic** group, but as we saw in Example 21.4 it is isomorphic with our old friend D_4, the dihedral group. For the second we can make S into a group by defining $(a^ib^j)(a^rb^s)$ to be a^xb^y where y is $j + s$ modulo 2 and if $j + s < 2$, then x is the remainder of $i + r(2j + 1)$ when divided by 4 and if $j + s = 2$, then x is the remainder when $i + 2 + r(2j + 1)$ is divided by 4. We leave it as an exercise to show that this operation makes S a group, which shows that G_2 is a presentation of a group of order 8.

Since $ba = a^3b \neq ab$, we see that both G_1 and G_2 are nonabelian. That the two groups are not isomorphic follows from the fact that a computation shows that G_1 has only two elements of order 4, namely, a and a^3. On the other hand, in G_2 all elements but 1 and a^2 are of order 4. We leave the computations of the tables for these groups

to Exercise 3. To illustrate suppose we wish to compute $(a^2b)(a^3b)$. Using $ba = a^3b$ repeatedly, we get

$$(a^2b)(a^3b) = a^2(ba)a^2b = a^5(ba)ab = a^8(ba)b = a^{11}b^2.$$

Then for G_1, we have

$$a^{11}b^2 = a^{11} = a^3,$$

but if we are in G_2, we get

$$a^{11}b^2 = a^{13} = a.$$

The group G_2 is called the **quaternion group**. We shall encounter the quaternion group again in Section 32. ▲

EXERCISES 21

Computations

1. Give a presentation of $\mathbb{Z}_4$ involving one generator; involving two generators; involving three generators.

2. Give a presentation of S_3 involving three generators.

3. Give the tables for both the octic group

$$(a, b : a^4 = 1, b^2 = 1, ba = a^3b)$$

and the quaternion group

$$(a, b : a^4 = 1, b^2 = a^2, ba = a^3b).$$

In both cases, write the elements in the order $1, a, a^2, a^3, b, ab, a^2b, a^3b$. (Note that we do not have to compute *every* product. We know that these presentations give groups of order 8, and once we have computed enough products the rest are forced so that each row and each column of the table has each element exactly once.)

4. Determine all groups of order 14 up to isomorphism. [*Hint:* Follow the outline of Example 21.6 and use Exercise 13, part (b).]

5. Determine all groups of order 21 up to isomorphism. [*Hint:* Follow the outline of Example 21.6 and use Exercise 13, part (b). It may seem that there are two presentations giving nonabelian groups. Show that they are isomorphic.]

Concepts

In Exercises 6 and 7, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

6. A *consequence* of the set of relators is any finite product of relators raised to powers.

7. Two group presentations are *isomorphic* if and only if there is a one-to-one correspondence of the generators of the first presentation with the generators of the second that yields, by renaming generators, a one-to-one correspondence of the relators of the first presentation with those of the second.

8. Determine whether each of the following is true or false.

a. Every group has a presentation.

b. Every group has many different presentations.

c. Every group has two presentations that are not isomorphic.

d. Every group has a finite presentation.

e. Every group with a finite presentation is of finite order.

f. Every cyclic group has a presentation with just one generator.

g. Every conjugate of a relator is a consequence of the relator.

h. Two presentations with the same number of generators are always isomorphic.

i. In a presentation of an abelian group, the set of consequences of the relators contains the commutator subgroup of the free group on the generators.

j. Every presentation of a free group has 1 as the only relator.

Theory

9. Use the methods of this section and Exercise 13, part (b), to show that there are no nonabelian groups of order 15.

10. Show, using Exercise 13, that

$$(a, b : a^3 = 1, b^2 = 1, ba = a^2b)$$

gives a group of order 6. Show that it is nonabelian.

11. Show that the presentation

$$(a, b : a^3 = 1, b^2 = 1, ba = a^2b)$$

of Exercise 10 gives (up to isomorphism) the only nonabelian group of order 6, and hence gives a group isomorphic to S_3.

12. We showed in Example 13.6 that A_4 has no subgroup of order 6. The preceding exercise shows that such a subgroup of A_4 would have to be isomorphic to either $\mathbb{Z}_6$ or S_3. Show again that this is impossible by considering orders of elements.

13. Let

$$S = \{a^i b^j \mid 0 \leq i < m, 0 \leq j < n\},$$

that is, S consists of all formal products $a^i b^j$ starting with $a^0 b^0$ and ending with $a^{m-1} b^{n-1}$. Let r be a positive integer, and define multiplication on S by

$$(a^s b^t)(a^u b^v) = a^x b^y,$$

where x is the remainder of $s + u(r^t)$ when divided by m, and y is the remainder of $t + v$ when divided by n, in the sense of the division algorithm (Theorem 6.2).

a. Show that a necessary and sufficient condition for the associative law to hold and for S to be a group under this multiplication is that $r^n \equiv 1 \pmod{m}$.

b. Deduce from part (a) that the group presentation

$$(a, b : a^m = 1, b^n = 1, ba = a^r b)$$

gives a group of order mn if and only if $r^n \equiv 1 \pmod{m}$. (See the Historical Note in this section.)

14. Without using Exercise 13, prove that $(a, b : a^5 = 1, b^2 = 1, ba = a^3 b)$ is a presentation for the group $\mathbb{Z}_2$.

15. Is the group obtained from the group presentation with the letters a through z as generators and the words in a standard English dictionary as relators the trivial group? Prove your answer.

PART V

Rings and Fields

SECTION 22 RINGS AND FIELDS

All our work thus far has been concerned with sets on which a single binary operation has been defined. Our years of work with the integers and real numbers show that a study of sets on which two binary operations have been defined should be of great importance. Algebraic structures of this type are introduced in this section. In one sense, this section seems more intuitive than those that precede it, for the structures studied are closely related to those we have worked with for many years. However, we will be continuing with our axiomatic approach. So, from another viewpoint this study is more complicated than group theory, for we now have two binary operations and more axioms to deal with.

Definitions and Basic Properties

The most general algebraic structure with two binary operations that we shall study is called a *ring*. As Example 22.2 following Definition 22.1 indicates, we have all worked with rings since elementary school.

22.1 Definition A **ring** $\langle R, +, \cdot \rangle$ is a set R together with two binary operations $+$ and $\cdot$, which we call *addition* and *multiplication,* defined on R such that the following axioms are satisfied:

$\mathscr{R}_1$. $\langle R, + \rangle$ is an abelian group.

$\mathscr{R}_2$. Multiplication is associative.

$\mathscr{R}_3$. For all $a, b, c \in R$, the **left distributive law**, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and the **right distributive law** $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ hold. ■

22.2 Example We are well aware that axioms $\mathscr{R}_1, \mathscr{R}_2$, and $\mathscr{R}_3$ for a ring hold in any subset of the complex numbers that is a group under addition and that is closed under multiplication. For example, $\langle \mathbb{Z}, +, \cdot \rangle$, $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$, and $\langle \mathbb{C}, +, \cdot \rangle$ are rings. ▲

Historical Note

The theory of rings grew out of the study of two particular classes of rings, polynomial rings in n variables over the real or complex numbers (Section 27) and the "integers" of an algebraic number field. It was David Hilbert (1862–1943) who first introduced the term *ring,* in connection with the latter example, but it was not until the second decade of the twentieth century that a fully abstract definition appeared. The theory of commutative rings was given a firm axiomatic foundation by Emmy Noether (1882–1935) in her monumental paper "Ideal Theory in Rings," which appeared in 1921. A major concept of this paper is the ascending chain condition for ideals. Noether proved that in any ring in which every ascending chain of ideals has a maximal element, every ideal is finitely generated.

Emmy Noether received her doctorate from the University of Erlangen, Germany, in 1907. Hilbert invited her to Göttingen in 1915, but his efforts to secure her a paid position were blocked because of her sex. Hilbert complained, "I do not see that the sex of the candidate is an argument against her admission [to the faculty]. After all, we are a university, not a bathing establishment." Noether was, however, able to lecture under Hilbert's name. Ultimately, after the political changes accompanying the end of the First World War reached Göttingen, she was given in 1923 a paid position at the University. For the next decade, she was very influential in the development of the basic concepts of modern algebra. Along with other Jewish faculty members, however, she was forced to leave Göttingen in 1933. She spent the final two years of her life at Bryn Mawr College near Philadelphia.

It is customary to denote multiplication in a ring by juxtaposition, using ab in place of $a \cdot b$. We shall also observe the usual convention that multiplication is performed before addition in the absence of parentheses, so the left distributive law, for example, becomes

$$a(b + c) = ab + ac,$$

without the parentheses on the right side of the equation. Also, as a convenience analogous to our notation in group theory, we shall somewhat incorrectly refer to a *ring* R in place of a *ring* $\langle R, +, \cdot \rangle$, provided that no confusion will result. In particular, from now on $\mathbb{Z}$ will always be $\langle \mathbb{Z}, +, \cdot \rangle$, and $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ will also be the rings in Example 22.2. We may on occasion refer to $\langle R, + \rangle$ as *the additive group of the ring* R.

22.3 Example Let R be any ring and let $M_n(R)$ be the collection of all $n \times n$ matrices having elements of R as entries. The operations of addition and multiplication in R allow us to add and multiply matrices in the usual fashion, explained in the appendix. We can quickly check that $\langle M_n(R), + \rangle$ is an abelian group. The associativity of matrix multiplication and the two distributive laws in $M_n(R)$ are more tedious to demonstrate, but straightforward calculations indicate that they follow from the same properties in R. We will assume from now on that we know that $M_n(R)$ is a ring. In particular, we have the rings $M_n(\mathbb{Z}), M_n(\mathbb{Q}), M_n(\mathbb{R})$, and $M_n(\mathbb{C})$. Note that multiplication is not a commutative operation in any of these rings for $n \geq 2$. ▲

22.4 Example Let F be the set of all functions $f : \mathbb{R} \to \mathbb{R}$. We know that $\langle F, + \rangle$ is an abelian group under the usual function addition,

$$(f + g)(x) = f(x) + g(x).$$

We define multiplication on F by

$$(fg)(x) = f(x)g(x).$$

That is, fg is the function whose value at x is $f(x)g(x)$. It is readily checked that F is a ring; we leave the demonstration to Exercise 36. We have used this juxtaposition

notation $\sigma\mu$ for the composite function $\sigma(\mu(x))$ when discussing permutation multiplication. If we were to use both function multiplication and function composition in F, we would use the notation $f \circ g$ for the composite function. However, we will use composition of functions almost exclusively with homomorphisms, which we will denote by Greek letters, and the usual product defined in this example chiefly when multiplying polynomial function's $f(x)g(x)$, so no confusion should result. ▲

22.5 Example Recall that in group theory, $n\mathbb{Z}$ is the cyclic subgroup of $\mathbb{Z}$ under addition consisting of all integer multiples of the integer n. Since $(nr)(ns) = n(nrs)$, we see that $n\mathbb{Z}$ is closed under multiplication. The associative and distributive laws that hold in $\mathbb{Z}$ then assure us that $\langle n\mathbb{Z}, +, \cdot\rangle$ is a ring. From now on in the text, we will consider $n\mathbb{Z}$ to be this ring. ▲

22.6 Example Consider the cyclic group $\langle \mathbb{Z}_n, +\rangle$. If we define for $a, b \in \mathbb{Z}_n$ the product ab as the remainder of the usual product of integers when divided by n, it can be shown that $\langle \mathbb{Z}_n, +, \cdot\rangle$ is a ring. We shall feel free to use this fact. For example, in $\mathbb{Z}_{10}$ we have $(3)(7) = 1$. This operation on $\mathbb{Z}_n$ is **multiplication modulo** n. We do not check the ring axioms here, for they will follow in Section 30 from some of the theory we develop there. From now on, $\mathbb{Z}_n$ will always be the ring $\langle \mathbb{Z}_n, +, \cdot\rangle$. ▲

22.7 Example If $R_1, R_2, \cdots, R_n$ are rings, we can form the set $R_1 \times R_2 \times \cdots \times R_n$ of all ordered n-tuples $(r_1, r_2, \cdots, r_n)$, where $r_i \in R_i$. Defining addition and multiplication of n-tuples by components (just as for groups), we see at once from the ring axioms in each component that the set of all these n-tuples forms a ring under addition and multiplication by components. The ring $R_1 \times R_2 \times \cdots \times R_n$ is the **direct product** of the rings R_i. ▲

Continuing matters of notation, we shall always let 0 be the additive identity of a ring. The additive inverse of an element a of a ring is $-a$. We shall frequently have occasion to refer to a sum

$$a + a + \cdots + a$$

having n summands. We shall let this sum be $n \cdot a$, always using the dot. However, $n \cdot a$ *is not to be interpreted as a multiplication of n and a in the ring, for the integer n may not be in the ring at all*. If $n < 0$, we let

$$n \cdot a = (-a) + (-a) + \cdots + (-a)$$

for $|n|$ summands. Finally, we define

$$0 \cdot a = 0$$

for $0 \in \mathbb{Z}$ on the left side of the equations and $0 \in R$ on the right side. Actually, the equation $0a = 0$ holds also for $0 \in R$ on both sides. The following theorem proves this and various other elementary but important facts. Note the strong use of the distributive laws in the proof of this theorem. Axiom $\mathscr{R}_1$ for a ring concerns only addition, and axiom $\mathscr{R}_2$ concerns only multiplication. This shows that in order to prove anything that gives a relationship between these two operations, we are going to have to use axiom $\mathscr{R}_3$. For example, the first thing that we will show in Theorem 22.8 is that $0a = 0$ for any element a in a ring R. Now this relation involves both addition and multiplication. The multiplication $0a$ stares us in the face, and 0 is an *additive* concept. Thus we will have to come up with an argument that uses a distributive law to prove this.

22.8 Theorem If R is a ring with additive identity 0, then for any $a, b \in R$ we have

1. $0a = a0 = 0$,
2. $a(-b) = (-a)b = -(ab)$,
3. $(-a)(-b) = ab$.