2 Groups

A good stock of examples, as large as possible, is indispensable for a thorough understanding of any concept, and when I want to learn something new, I make it my first job to build one.

PAUL R. HALMOS

Definition and Examples of Groups

The term *group* was used by Galois around 1830 to describe sets of one-to-one functions on finite sets that could be grouped together to form a set closed under composition. As is the case with most fundamental concepts in mathematics, the modern definition of a group that follows is the result of a long evolutionary process. Although this definition was given by both Heinrich Weber and Walther von Dyck in 1882, it did not gain universal acceptance until the 20th century.

Definition Binary Operation
Let G be a set. A *binary operation* on G is a function that assigns each ordered pair of elements of G an element of G.

A binary operation on a set G, then, is simply a method (or formula) by which the members of an ordered pair from G combine to yield a new member of G. This condition is called *closure*. The most familiar binary operations are ordinary addition, subtraction, and multiplication of integers. Division of integers is not a binary operation on the integers because an integer divided by an integer need not be an integer.

The binary operations addition modulo n and multiplication modulo n on the set $\{0, 1, 2, \ldots, n - 1\}$, which we denote by Z_n, play an extremely important role in abstract algebra. In certain situations we will want to combine the elements of Z_n by addition modulo n only; in other situations we will want to use both addition modulo n and multiplication modulo n to combine the elements. It will be clear

from the context whether we are using addition only or addition and multiplication. For example, when multiplying matrices with entries from Z_n, we will need both addition modulo n and multiplication modulo n.

Definition Group

Let G be a set together with a binary operation (usually called multiplication) that assigns to each ordered pair (a, b) of elements of G an element in G denoted by ab. We say G is a *group* under this operation if the following three properties are satisfied.

1. ***Associativity.*** **The operation is associative; that is, $(ab)c = a(bc)$ for all a, b, c in G.**
2. ***Identity.*** **There is an element e (called the *identity*) in G such that $ae = ea = a$ for all a in G.**
3. ***Inverses.*** **For each element a in G, there is an element b in G (called an *inverse* of a) such that $ab = ba = e$.**

In words, then, a group is a set together with an associative operation such that there is an identity, every element has an inverse, and any pair of elements can be combined without going outside the set. Be sure to verify closure when testing for a group (see Example 5). Notice that if a is the inverse of b, then b is the inverse of a.

If a group has the property that $ab = ba$ for every pair of elements a and b, we say the group is *Abelian*. A group is *non-Abelian* if there is some pair of elements a and b for which $ab \neq ba$. When encountering a particular group for the first time, one should determine whether or not it is Abelian.

Now that we have the formal definition of a group, our first job is to build a good stock of examples. These examples will be used throughout the text to illustrate the theorems. (The best way to grasp the meat of a theorem is to see what it says in specific cases.) As we progress, the reader is bound to have hunches and conjectures that can be tested against the stock of examples. To develop a better understanding of the following examples, the reader should supply the missing details.

EXAMPLE 1 The set of integers Z (so denoted because the German word for numbers is *Zahlen*), the set of rational numbers Q (for quotient), and the set of real numbers $\mathbf{R}$ are all groups under ordinary addition. In each case, the identity is 0 and the inverse of a is $-a$. ∎

EXAMPLE 2 The set of integers under ordinary multiplication is not a group. Since the number 1 is the identity, property 3 fails. For example, there is no integer b such that $5b = 1$.

EXAMPLE 3 The subset $\{1, -1, i, -i\}$ of the complex numbers is a group under complex multiplication. Note that -1 is its own inverse, whereas the inverse of i is $-i$, and vice versa.

EXAMPLE 4 The set Q^+ of positive rationals is a group under ordinary multiplication. The inverse of any a is $1/a = a^{-1}$.

EXAMPLE 5 The set S of positive irrational numbers together with 1 under multiplication satisfies the three properties given in the definition of a group but is not a group. Indeed, $\sqrt{2} \cdot \sqrt{2} = 2$, so S is not closed under multiplication.

EXAMPLE 6 A rectangular array of the form $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is called a 2×2 *matrix*. The set of all 2×2 matrices with real entries is a group under componentwise addition. That is,

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix}$$

The identity is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, and the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$.

EXAMPLE 7 The set $Z_n = \{0, 1, \ldots, n - 1\}$ for $n \geq 1$ is a group under addition modulo n. For any $j > 0$ in Z_n, the inverse of j is $n - j$. This group is usually referred to as the *group of integers modulo n.*

As we have seen, the real numbers, the 2×2 matrices with real entries, and the integers modulo n are all groups under the appropriate addition. But what about multiplication? In each case, the existence of some elements that do not have inverses prevents the set from being a group under the usual multiplication. However, we can form a group in each case by simply throwing out the rascals. Examples 8, 9, and 11 illustrate this.

EXAMPLE 8 The set $\mathbf{R}^*$ of nonzero real numbers is a group under ordinary multiplication. The identity is 1. The inverse of a is $1/a$.

EXAMPLE 9† The *determinant* of the 2×2 matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is the number $ad - bc$. If A is a 2×2 matrix, $\det A$ denotes the determinant of A. The set

$$GL(2, \mathbf{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, c, d \in \mathbf{R}, ad - bc \neq 0 \right\}$$

of 2×2 matrices with real entries and nonzero determinants is a non-Abelian group under the operation

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix}.$$

The first step in verifying that this set is a group is to show that the product of two matrices with nonzero determinants also has a nonzero determinant. This follows from the fact that for any pair of 2×2 matrices A and B, $\det(AB) = (\det A)(\det B)$.

Associativity can be verified by direct (but cumbersome) calculations. The identity is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$; the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is

$$\begin{bmatrix} \dfrac{d}{ad - bc} & \dfrac{-b}{ad - bc} \\ \dfrac{-c}{ad - bc} & \dfrac{a}{ad - bc} \end{bmatrix}$$

(explaining the requirement that $ad - bc \neq 0$). This very important non-Abelian group is called the *general linear group* of 2×2 matrices over $\mathbf{R}$. ∎

EXAMPLE 10 The set of all 2×2 matrices with real entries is not a group under the operation defined in Example 9. Inverses do not exist when the determinant is 0. ∎

Now that we have shown how to make subsets of the real numbers and subsets of the set of 2×2 matrices into multiplicative groups, we next consider the integers under multiplication modulo n.

†For simplicity, we have restricted our matrix examples to the 2×2 case. However, readers who have had linear algebra can readily generalize to $n \times n$ matrices.

EXAMPLE 11 (L. EULER, 1761) By Exercise 11 in Chapter 0, an integer a has a multiplicative inverse modulo n if and only if a and n are relatively prime. So, for each $n > 1$, we define $U(n)$ to be the set of all positive integers less than n and relatively prime to n. Then $U(n)$ is a group under multiplication modulo n. (We leave it to the reader to check that this set is closed under this operation.)

For $n = 10$, we have $U(10) = \{1, 3, 7, 9\}$. The Cayley table for $U(10)$ is

mod 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

(Recall that ab mod n is the unique integer r with the property $a \cdot b = nq + r$, where $0 \leq r < n$ and $a \cdot b$ is ordinary multiplication.) In the case that n is a prime, $U(n) = \{1, 2, \ldots, n - 1\}$. ∎

In his classic book *Lehrbuch der Algebra*, published in 1895, Heinrich Weber gave an extensive treatment of the groups $U(n)$ and described them as the most important examples of finite Abelian groups.

EXAMPLE 12 The set $\{0, 1, 2, 3\}$ is not a group under multiplication modulo 4. Although 1 and 3 have inverses, the elements 0 and 2 do not. ∎

EXAMPLE 13 The set of integers under subtraction is not a group, since the operation is not associative. ∎

With the examples given thus far as a guide, it is wise for the reader to pause here and think of his or her own examples. Study actively! Don't just read along and be spoon-fed by the book.

EXAMPLE 14 The complex numbers $\mathbf{C} + \{a + bi \mid a, b \in \mathbf{R}, i^2 = -1\}$ are a group under the operation $(a + bi) + (c + di) = (a + c) + (b + d)i$. The inverse of $a + bi$ is $-a - bi$. The nonzero complex numbers $\mathbf{C}^*$ are a group under the operation $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$. The inverse of $a + bi$ is $\dfrac{1}{a + bi} = \dfrac{1}{a + bi}\dfrac{a - bi}{a - bi} = \dfrac{1}{a^2 + b^2}a - \dfrac{1}{a^2 + b^2}bi$. ∎

EXAMPLE 15 For all integers $n \geq 1$, the set of complex nth roots of unity

$$\left\{ \cos \frac{k \cdot 360^\circ}{n} + i \sin \frac{k \cdot 360^\circ}{n} \,\middle|\, k = 0, 1, 2, \ldots, n - 1 \right\}$$

(i.e., complex zeros of $x^n - 1$) is a group under multiplication. (See DeMoivre's Theorem—Example 10 in Chapter 0.) Compare this group with the one in Example 3.

Recall from Chapter 0 that the complex number $\cos \theta + i \sin \theta$ can be represented geometrically as the point $(\cos \theta, \sin \theta)$ in a plane coordinatized by a real horizontal axis and a vertical imaginary axis, where θ is the angle formed by the line segment joining the origin and the point $(\cos \theta, \sin \theta)$ and the positive real axis. Thus, the six complex zeros of $x^6 = 1$ are located at points around the circle of radius 1, 60° apart, as shown in Figure 2.1.

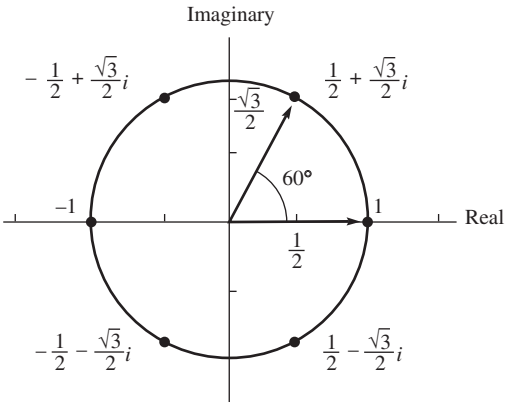


Figure 2.1

EXAMPLE 16 The set $\mathbf{R}^n = \{(a_1, a_2, \ldots, a_n) \mid a_1, a_2, \ldots, a_n \in \mathbf{R}\}$ is a group under componentwise addition [i.e., $(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$].

EXAMPLE 17 For a fixed point (a, b) in $\mathbf{R}^2$, define $T_{a,b}: \mathbf{R}^2 \to \mathbf{R}^2$ by $(x, y) \to (x + a, y + b)$. Then $G = \{T_{a,b} \mid a, b \in \mathbf{R}\}$ is a group under function composition. Straightforward calculations show that $T_{a,b}T_{c,d} = T_{a+c,b+d}$. From this formula we may observe that G is closed, $T_{0,0}$ is the identity, the inverse of $T_{a,b}$ is $T_{-a,-b}$, and G is Abelian. Function composition is always associative. The elements of G are called *translations.*

EXAMPLE 18 The set of all 2×2 matrices with determinant 1 with entries from Q (rationals), $\mathbf{R}$ (reals), $\mathbf{C}$ (complex numbers), or Z_p (p a prime) is a non-Abelian group under matrix multiplication. This group is called the *special linear group* of 2×2 matrices over Q, $\mathbf{R}$, $\mathbf{C}$, or Z_p, respectively. If the entries are from F, where F is any of the above, we denote this group by $SL(2, F)$. For the group $SL(2, F)$, the formula given in Example 9 for the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ simplifies to $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. When the matrix entries are from Z_p, we use modulo p arithmetic to compute determinants, matrix products, and inverses. To illustrate the case $SL(2, Z_5)$, consider the element $A = \begin{bmatrix} 3 & 4 \\ 4 & 4 \end{bmatrix}$. Then $\det A = (3 \cdot 4 - 4 \cdot 4) \bmod 5 = -4 \bmod 5 = 1$, and the inverse of A is $\begin{bmatrix} 4 & -4 \\ -4 & 3 \end{bmatrix} = \begin{bmatrix} 4 & 1 \\ 1 & 3 \end{bmatrix}$. Note that $\begin{bmatrix} 3 & 4 \\ 4 & 4 \end{bmatrix}\begin{bmatrix} 4 & 1 \\ 1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ when the arithmetic is done modulo 5. ∎

Example 9 is a special case of the following general construction.

EXAMPLE 19 Let F be any of Q, $\mathbf{R}$, $\mathbf{C}$, or Z_p (p a prime). The set $GL(2, F)$ of all 2×2 matrices with nonzero determinants and entries from F is a non-Abelian group under matrix multiplication. As in Example 18, when F is Z_p, modulo p arithmetic is used to calculate determinants, matrix products, and inverses. The formula given in Example 9 for the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ remains valid for elements from $GL(2, Z_p)$, provided we interpret division by $ad - bc$ as multiplication by the inverse of $(ad - bc)$ modulo p. For example, in $GL(2, Z_7)$, consider $\begin{bmatrix} 4 & 5 \\ 6 & 3 \end{bmatrix}$. Then the determinant $(ad - bc) \bmod 7$ is $(12 - 30) \bmod 7 = -18 \bmod 7 = 3$ and the inverse of 3 is 5 [since $(3 \cdot 5) \bmod 7 = 1$]. So, the inverse of $\begin{bmatrix} 4 & 5 \\ 6 & 3 \end{bmatrix}$ is $\begin{bmatrix} 3 \cdot 5 & 2 \cdot 5 \\ 1 \cdot 5 & 4 \cdot 5 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 5 & 6 \end{bmatrix}$. [The reader should check that $\begin{bmatrix} 4 & 5 \\ 6 & 3 \end{bmatrix}\begin{bmatrix} 1 & 3 \\ 5 & 6 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ in $GL(2, Z_7)$]. ∎

The group $GL(n, F)$ is called the *general linear group* of $n \times n$ matrices over F.

EXAMPLE 20 The set $\{1, 2, \ldots, n - 1\}$ is a group under multiplication modulo n if and only if n is prime. ∎

EXAMPLE 21 The set of all symmetries of the infinite ornamental pattern in which arrowheads are spaced uniformly a unit apart along

a line is an Abelian group under composition. Let T denote a translation to the right by one unit, T^{-1} a translation to the left by one unit, and H a reflection across the horizontal line of the figure. Then, every member of the group is of the form $x_1x_2 \cdot \cdot \cdot x_n$, where each $x_i \in \{T, T^{-1}, H\}$. In this case, we say that T, T^{-1}, and H *generate* the group. ∎

Table 2.1 summarizes many of the specific groups that we have presented thus far.

As the previous examples demonstrate, the notion of a group is a very broad one indeed. The goal of the axiomatic approach is to find properties general enough to permit many diverse examples having these properties and specific enough to allow one to deduce many interesting consequences.

The goal of abstract algebra is to discover truths about algebraic systems (that is, sets with one or more binary operations) that are independent of the specific nature of the operations. All one knows or needs to know is that these operations, whatever they may be, have

Table 2.1 Summary of Group Examples (F can be any of Q, $\mathbf{R}$, $\mathbf{C}$, or Z_p; L is a reflection)

Group	Operation	Identity	Form of Element	Inverse	Abelian
Z	Addition	0	k	$-k$	Yes
Q^+	Multiplication	1	m/n, $m, n > 0$	n/m	Yes
Z_n	Addition mod n	0	k	$n - k$	Yes
$\mathbf{R}^*$	Multiplication	1	x	$1/x$	Yes
$\mathbf{C}^*$	Multiplication	1	$a + bi$	$\frac{1}{a^2 + b^2}a - \frac{1}{a^2 - b^2}bi$	Yes
$GL(2, F)$	Matrix multiplication	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $ad - bc \neq 0$	$\begin{bmatrix} \frac{d}{ad - bc} & \frac{-b}{ad - bc} \\ \frac{-c}{ad - bc} & \frac{a}{ad - bc} \end{bmatrix}$	No
$U(n)$	Multiplication mod n	1	k, $\gcd(k, n) = 1$	Solution to $kx \bmod n = 1$	Yes
$\mathbf{R}^n$	Componentwise addition	$(0, 0, \ldots, 0)$	$(a_1, a_2, \ldots, a_n)$	$(-a_1, -a_2, \ldots, -a_n)$	Yes
$SL(2, F)$	Matrix multiplication	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $ad - bc = 1$	$\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$	No
D_n	Composition	R_0	R_α, L	$R_{360 - \alpha}$, L	No

certain properties. We then seek to deduce consequences of these properties. This is why this branch of mathematics is called *abstract* algebra. It must be remembered, however, that when a specific group is being discussed, a specific operation must be given (at least implicitly).

Elementary Properties of Groups

Now that we have seen many diverse examples of groups, we wish to deduce some properties that they share. The definition itself raises some fundamental questions. Every group has *an* identity. Could a group have more than one? Every group element has *an* inverse. Could an element have more than one? The examples suggest not. But examples can only suggest. One cannot prove that every group has a unique identity by looking at examples, because each example inherently has properties that may not be shared by all groups. We are forced to restrict ourselves to the properties that all groups have; that is, we must view groups as abstract entities rather than argue by example. The next three theorems illustrate the abstract approach.

Theorem 2.1 Uniqueness of the Identity

In a group G, there is only one identity element.

PROOF Suppose both e and e' are identities of G. Then,

1. $ae = a$ for all a in G, and
2. $e'a = a$ for all a in G.

The choices of $a = e'$ in (part 1) and $a = e$ in (part 2) yield $e'e = e'$ and $e'e = e$**.** Thus, e and e' are both equal to $e'e$ and so are equal to each other. ∎

Because of this theorem, we may unambiguously speak of "the identity" of a group and denote it by 'e' (because the German word for identity is *Einheit*).

Theorem 2.2 Cancellation

In a group G, the right and left cancellation laws hold; that is, $ba = ca$ implies $b = c$, and $ab = ac$ implies $b = c$.

PROOF Suppose $ba = ca$. Let a' be an inverse of a. Then multiplying on the right by a' yields $(ba)a' = (ca)a'$. Associativity yields $b(aa') = c(aa')$. Then $be = ce$ and, therefore, $b = c$ as desired. Similarly, one can prove that $ab = ac$ implies $b = c$ by multiplying by a' on the left. ∎

A consequence of the cancellation property is the fact that in a Cayley table for a group, each group element occurs exactly once in each row and column (see Exercise 31). Another consequence of the cancellation property is the uniqueness of inverses.

Theorem 2.3 Uniqueness of Inverses

For each element a in a group G, there is a unique element b in G such that ab = ba = e.

PROOF Suppose b and c are both inverses of a. Then $ab = e$ and $ac = e$, so that $ab = ac$. Canceling the a on both sides gives $b = c$, as desired. ∎

As was the case with the identity element, it is reasonable, in view of Theorem 2.3, to speak of "the inverse" of an element g of a group; in fact, we may unambiguously denote it by g^{-1}. This notation is suggested by that used for ordinary real numbers under multiplication. Similarly, when n is a positive integer, the associative law allows us to use g^n to denote the unambiguous product

$$\underbrace{gg \cdots g}_{n \text{ factors}}.$$

We define $g^0 = e$. When n is negative, we define $g^n = (g^{-1})^{|n|}$ [for example, $g^{-3} = (g^{-1})^3$]. Unlike for real numbers, in an abstract group we do not permit noninteger exponents such as $g^{1/2}$. With this notation, the familiar laws of exponents hold for groups; that is, for all integers m and n and any group element g, we have $g^m g^n = g^{m+n}$ and $(g^m)^n = g^{mn}$. Although the way one manipulates the group expressions $g^m g^n$ and $(g^m)^n$ coincides with the laws of exponents for real numbers, the laws of exponents fail to hold for expressions involving two group elements. Thus, for groups in general, $(ab)^n \neq a^n b^n$ (see Exercise 23).

The important thing about the existence of a unique inverse for each group element a is that for every element b in the group there is a unique solution in the group of the equations $ax = b$ and $xa = b$. Namely, $x = a^{-1}b$ in the first case and $x = ba^{-1}$ in the second case. In contrast,

in the set $\{0, 1, 2, 3, 4, 5\}$, the equation $2x = 4$ has the solutions $x = 2$ and $x = 5$ under the operation multiplication mod 6. However, this set is not a group under multiplication mod 6.

Also, one must be careful with this notation when dealing with a specific group whose binary operation is addition and is denoted by "+." In this case, the definitions and group properties expressed in multiplicative notation must be translated to additive notation. For example, the inverse of g is written as $-g$. Likewise, for example, g^3 means $g + g + g$ and is usually written as $3g$, whereas g^{-3} means $(-g) + (-g) + (-g)$ and is written as $-3g$. When additive notation is used, do not interpret "ng" as combining n and g under the group operation; n may not even be an element of the group! Table 2.2 shows the common notation and corresponding terminology for groups under multiplication and groups under addition. As is the case for real numbers, we use $a - b$ as an abbreviation for $a + (-b)$.

Table **2.2**

Multiplicative Group		Additive Group	
$a \cdot b$ or ab	Multiplication	$a + b$	Addition
e or 1	Identity or one	0	Zero
a^{-1}	Multiplicative inverse of a	$-a$	Additive inverse of a
a^n	Power of a	na	Multiple of a
ab^{-1}	Quotient	$a - b$	Difference

Because of the associative property, we may unambiguously write the expression abc, for this can be reasonably interpreted as only $(ab)c$ or $a(bc)$, which are equal. In fact, by using induction and repeated application of the associative property, one can prove a general associative property that essentially means that parentheses can be inserted or deleted at will without affecting the value of a product involving any number of group elements. Thus,

$$a^2(bcdb^2) = a^2b(cd)b^2 = (a^2b)(cd)b^2 = a(abcdb)b,$$

and so on.

Although groups do not have the property that $(ab)^n = a^nb^n$, there is a simple relationship between $(ab)^{-1}$ and a^{-1} and b^{-1}.

Theorem 2.4 Socks–Shoes Property

For group elements a and b, $(ab)^{-1} = b^{-1}a^{-1}$.

PROOF Since $(ab)(ab)^{-1} = e$ and $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$, we have by Theorem 2.3 that $(ab)^{-1} = b^{-1}a^{-1}$. ∎

Historical Note

We conclude this chapter with a bit of history concerning the noncommutativity of matrix multiplication. In 1925, quantum theory was replete with annoying and puzzling ambiguities. It was Werner Heisenberg who recognized the cause. He observed that the product of the quantum-theoretical analogs of the classical Fourier series did not necessarily commute. For all his boldness, this shook Heisenberg. As he later recalled [2, p. 94]:

> In my paper the fact that XY was not equal to YX was very disagreeable to me. I felt this was the only point of difficulty in the whole scheme, otherwise I would be perfectly happy. But this difficulty had worried me and I was not able to solve it.

Heisenberg asked his teacher, Max Born, if his ideas were worth publishing. Born was fascinated and deeply impressed by Heisenberg's new approach. Born wrote [1, p. 217]:

> After having sent off Heisenberg's paper to the *Zeitschrift für Physik* for publication, I began to ponder over his symbolic multiplication, and was soon so involved in it that I thought about it for the whole day and could hardly sleep at night. For I felt there was something fundamental behind it, the consummation of our endeavors of many years. And one morning, about the 10 July 1925, I suddenly saw light: Heisenberg's symbolic multiplication was nothing but the matrix calculus, well-known to me since my student days from Rosanes' lectures in Breslau.

Born and his student, Pascual Jordan, reformulated Heisenberg's ideas in terms of matrices, but it was Heisenberg who was credited with the formulation. In his autobiography, Born lamented [1, p. 219]:

> Nowadays the textbooks speak without exception of Heisenberg's matrices, Heisenberg's commutation law, and Dirac's field quantization.
>
> In fact, Heisenberg knew at that time very little of matrices and had to study them.

Upon learning in 1933 that he was to receive the Nobel Prize with Dirac and Schrödinger for this work, Heisenberg wrote to Born [1, p. 220]:

> If I have not written to you for such a long time, and have not thanked you for your congratulations, it was partly because of my rather bad conscience with respect to you. The fact that I am to receive the Nobel Prize alone, for work done in Göttingen in collaboration—you, Jordan, and I—this fact depresses me and I hardly know what to write to you. I am, of course, glad that our common efforts are now appreciated, and I enjoy the recollection of the beautiful time of collaboration. I also believe that all good physicists know how great was your and Jordan's contribution to the structure of quantum mechanics—and this remains unchanged by a wrong decision from outside. Yet I myself can do nothing but thank you again for all the fine collaboration, and feel a little ashamed.

The story has a happy ending, however, because Born received the Nobel Prize in 1954 for his fundamental work in quantum mechanics.

Exercises

"For example" is not proof.

JEWISH PROVERB

1. Which of the following binary operations are closed?
- **a.** subtraction of positive integers
- **b.** division of nonzero integers
- **c.** function composition of polynomials with real coefficients
- **d.** multiplication of 2×2 matrices with integer entries

2. Which of the following binary operations are associative?
- **a.** multiplication mod n
- **b.** division of nonzero rationals
- **c.** function composition of polynomials with real coefficients
- **d.** multiplication of 2×2 matrices with integer entries

3. Which of the following binary operations are commutative?
- **a.** substraction of integers
- **b.** division of nonzero real numbers
- **c.** function composition of polynomials with real coefficients
- **d.** multiplication of 2×2 matrices with real entries

4. Which of the following sets are closed under the given operation?
- **a.** $\{0, 4, 8, 12\}$ addition mod 16
- **b.** $\{0, 4, 8, 12\}$ addition mod 15
- **c.** $\{1, 4, 7, 13\}$ multiplication mod 15
- **d.** $\{1, 4, 5, 7\}$ multiplication mod 9

5. In each case, find the inverse of the element under the given operation.
- **a.** 13 in Z_{20}
- **b.** 13 in $U(14)$
- **c.** $n-1$ in $U(n)$ $(n > 2)$
- **d.** $3-2i$ in $\mathbf{C}^*$, the group of nonzero complex numbers under multiplication

6. In each case, perform the indicated operation.
- **a.** In $\mathbf{C}^*$, $(7 + 5i)(-3 + 2i)$
- **b.** In $GL(2, Z_{13})$, $\det \begin{bmatrix} 7 & 4 \\ 1 & 5 \end{bmatrix}$
- **c.** In $GL(2, \mathrm{R})$, $\begin{bmatrix} 6 & 3 \\ 8 & 2 \end{bmatrix}^{-1}$
- **d.** In $GL(2, Z_{13})$, $\begin{bmatrix} 6 & 3 \\ 8 & 2 \end{bmatrix}^{-1}$

7. Give two reasons why the set of odd integers under addition is not a group.

8. Referring to Example 13, verify the assertion that subtraction is not associative.

9. Show that $\{1, 2, 3\}$ under multiplication modulo 4 is not a group but that $\{1, 2, 3, 4\}$ under multiplication modulo 5 is a group.

10. Show that the group $GL(2, \mathbf{R})$ of Example 9 is non-Abelian by exhibiting a pair of matrices A and B in $GL(2, \mathbf{R})$ such that $AB \neq BA$.

11. Find the inverse of the element $\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}$ in $GL(2, Z_{11})$.

12. Give an example of group elements a and b with the property that $a^{-1}ba \neq b$.

13. Translate each of the following multiplicative expressions into its additive counterpart. Assume that the operation is commutative.

a. a^2b^3

b. $a^{-2}(b^{-1}c)^2$

c. $(ab^2)^{-3}c^2 = e$

14. For group elements a, b, and c, express $(ab)^3$ and $(ab^{-2}\,c)^{-2}$ without parentheses.

15. Let G be a group and let $H = \{x^{-1} \mid x \in G\}$. Show that $G = H$ as sets.

16. Show that the set $\{5, 15, 25, 35\}$ is a group under multiplication modulo 40. What is the identity element of this group? Can you see any relationship between this group and $U(8)$?

17. (From the GRE Practice Exam)* Let p and q be distinct primes. Suppose that H is a proper subset of the integers that is a group under addition that contains exactly three elements of the set $\{p, p + q, pq, p^q, q^p\}$. Determine which of the following are the three elements in H.

a. pq, p^q, q^p

b. $p + q, pq, p^q$

c. $p, p + q, pq$

d. p, p^q, q^p

e. p, pq, p^q

18. List the members of $H = \{x^2 \mid x \in D_4\}$ and $K = \{x \in D_4 \mid x^2 = e\}$.

19. Prove that the set of all 2×2 matrices with entries from $\mathbf{R}$ and determinant $+1$ is a group under matrix multiplication.

20. For any integer $n > 2$, show that there are at least two elements in $U(n)$ that satisfy $x^2 = 1$.

21. An abstract algebra teacher intended to give a typist a list of nine integers that form a group under multiplication modulo 91. Instead,

*GRE materials selected from the GRE Practice Exam, Question 9 by Educational Testing Service. Reprinted by permission of Educational Testing Service, the copyright owner.

one of the nine integers was inadvertently left out, so that the list appeared as 1, 9, 16, 22, 53, 74, 79, 81. Which integer was left out? (This really happened!)

22. Let G be a group with the property that for any x, y, z in the group, $xy = zx$ implies $y = z$. Prove that G is Abelian. ("Left-right cancellation" implies commutativity.)

23. (Law of Exponents for Abelian Groups) Let a and b be elements of an Abelian group and let n be any integer. Show that $(ab)^n = a^n b^n$. Is this also true for non-Abelian groups?

24. (Socks–Shoes Property) Draw an analogy between the statement $(ab)^{-1} = b^{-1}a^{-1}$ and the act of putting on and taking off your socks and shoes. Find distinct nonidentity elements a and b from a non-Abelian group such that $(ab)^{-1} = a^{-1}b^{-1}$. Find an example that shows that in a group, it is possible to have $(ab)^{-2} \neq b^{-2}a^{-2}$. What would be an appropriate name for the group property $(abc)^{-1} = c^{-1}b^{-1}a^{-1}$?

25. Prove that a group G is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all a and b in G.

26. Prove that in a group, $(a^{-1})^{-1} = a$ for all a.

27. For any elements a and b from a group and any integer n, prove that $(a^{-1}ba)^n = a^{-1}b^n a$.

28. If $a_1, a_2, \ldots, a_n$ belong to a group, what is the inverse of $a_1 a_2 \cdots a_n$?

29. The integers 5 and 15 are among a collection of 12 integers that form a group under multiplication modulo 56. List all 12.

30. Give an example of a group with 105 elements. Give two examples of groups with 44 elements.

31. Prove that every group table is a *Latin square*[†]; that is, each element of the group appears exactly once in each row and each column.

32. Construct a Cayley table for $U(12)$.

33. Suppose the table below is a group table. Fill in the blank entries.

	e	***a***	***b***	***c***	***d***
e	*e*	—	—	—	—
a	—	*b*	—	—	*e*
b	—	*c*	*d*	*e*	—
c	—	*d*	—	*a*	*b*
d	—	—	—	—	—

[†]Latin squares are useful in designing statistical experiments. There is also a close connection between Latin squares and finite geometries.

34. Prove that in a group, $(ab)^2 = a^2b^2$ if and only if $ab = ba$.

35. Let a, b, and c be elements of a group. Solve the equation $axb = c$ for x. Solve $a^{-1}xa = c$ for x.

36. Let a and b belong to a group G. Find an x in G such that $xabx^{-1} = ba$.

37. Let G be a finite group. Show that the number of elements x of G such that $x^3 = e$ is odd. Show that the number of elements x of G such that $x^2 \neq e$ is even.

38. Give an example of a group with elements a, b, c, d, and x such that $axb = cxd$ but $ab \neq cd$. (Hence "middle cancellation" is not valid in groups.)

39. Suppose that G is a group with the property that for every choice of elements in G, $axb = cxd$ implies $ab = cd$. Prove that G is Abelian. ("Middle cancellation" implies commutativity.)

40. Find an element X in D_4 such that $R_{90}VXH = D'$.

41. Suppose F_1 and F_2 are distinct reflections in a dihedral group D_n. Prove that $F_1F_2 \neq R_0$.

42. Suppose F_1 and F_2 are distinct reflections in a dihedral group D_n such that $F_1F_2 = F_2F_1$. Prove that $F_1F_2 = R_{180}$.

43. Let R be any fixed rotation and F any fixed reflection in a dihedral group. Prove that $R^kFR^k = F$.

44. Let R be any fixed rotation and F any fixed reflection in a dihedral group. Prove that $FR^kF = R^{-k}$. Why does this imply that D_n is non-Abelian?

45. In the dihedral group D_n, let $R = R_{360/n}$ and let F be any reflection. Write each of the following products in the form R^i or R^iF, where $0 \leq i < n$.

a. In D_4, $FR^{-2}FR^5$

b. In D_5, $R^{-3}FR^4FR^{-2}$

c. In D_6, $FR^5FR^{-2}F$

46. Prove that the set of all rational numbers of the form 3^m6^n, where m and n are integers, is a group under multiplication.

47. Prove that if G is a group with the property that the square of every element is the identity, then G is Abelian. (This exercise is referred to in Chapter 26.)

48. Prove that the set of all 3×3 matrices with real entries of the form

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

is a group. (Multiplication is defined by

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a + a' & b' + ac' + b \\ 0 & 1 & c' + c \\ 0 & 0 & 1 \end{bmatrix}.$$

This group, sometimes called the *Heisenberg group* after the Nobel Prize–winning physicist Werner Heisenberg, is intimately related to the Heisenberg Uncertainty Principle of quantum physics.)

49. Prove the assertion made in Example 20 that the set $\{1, 2, \ldots, n - 1\}$ is a group under multiplication modulo n if and only if n is prime.

50. In a finite group, show that the number of nonidentity elements that satisfy the equation $x^5 = e$ is a multiple of 5. If the stipulation that the group be finite is omitted, what can you say about the number of nonidentity elements that satisfy the equation $x^5 = e$?

51. List the six elements of $GL(2, Z_2)$. Show that this group is non-Abelian by finding two elements that do not commute. (This exercise is referred to in Chapter 7.)

52. Let $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} | a \in \mathbf{R}, a \neq 0 \right\}$. Show that G is a group under matrix multiplication. Explain why each element of G has an inverse even though the matrices have 0 determinants. (Compare with Example 10.)

53. Suppose that in the definition of a group G, the condition that there exists an element e with the property $ae = ea = a$ for all a in G is replaced by $ae = a$ for all a in G. Show that $ea = a$ for all a in G. (Thus, a one-sided identity is a two-sided identity.)

54. Suppose that in the definition of a group G, the condition that for each element a in G there exists an element b in G with the property $ab = ba = e$ is replaced by the condition $ab = e$. Show that $ba = e$. (Thus, a one-sided inverse is a two-sided inverse.)

Computer Exercises

Software for the computer exercises in this chapter is available at the website:

http://www.d.umn.edu/~jgallian

References

1. Max Born, *My Life: Recollections of a Nobel Laureate*, New York: Charles Scribner's Sons, 1978.
2. J. Mehra and H. Rechenberg, *The Historical Development of Quantum Theory*, Vol. 3, New York: Springer-Verlag, 1982.

Suggested Readings

Marcia Ascher, *Ethnomathematics*, Pacific Grove, CA: Brooks/Cole, 1991.

Chapter 3 of this book describes how the dihedral group of order 8 can be used to encode the social structure of the kin system of family relationships among a tribe of native people of Australia.

Arie Bialostocki, "An Application of Elementary Group Theory to Central Solitaire," *The College Mathematics Journal*, May 1998: 208–212.

The author uses properties of groups to analyze the peg board game central solitaire (which also goes by the name peg solitaire).

J. E. White, "Introduction to Group Theory for Chemists," *Journal of Chemical Education* 44 (1967): 128–135.

Students interested in the physical sciences may find this article worthwhile. It begins with easy examples of groups and builds up to applications of group theory concepts and terminology to chemistry.

3 Finite Groups; Subgroups

In our own time, in the period 1960–1980, we have seen particle physics emerge as the playground of group theory.

FREEMAN DYSON

Terminology and Notation

As we will soon discover, finite groups—that is, groups with finitely many elements—have interesting arithmetic properties. To facilitate the study of finite groups, it is convenient to introduce some terminology and notation.

Definition Order of a Group
The number of elements of a group (finite or infinite) is called its *order*. We will use $|G|$ to denote the order of G.

Thus, the group Z of integers under addition has infinite order, whereas the group $U(10) = \{1, 3, 7, 9\}$ under multiplication modulo 10 has order 4.

Definition Order of an Element
The *order* of an element g in a group G is the smallest positive integer n such that $g^n = e$. (In additive notation, this would be $ng = 0$.) If no such integer exists, we say that g has *infinite order*. The order of an element g is denoted by $|g|$.

So, to find the order of a group element g, you need only compute the sequence of products $g, g^2, g^3, \ldots$, until you reach the identity for the first time. The exponent of this product (or coefficient if the operation is addition) is the order of g. If the identity never appears in the sequence, then g has infinite order.

EXAMPLE 1 Consider $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ under multiplication modulo 15. This group has order 8. To find the order of

the element 7, say, we compute the sequence $7^1 = 7$, $7^2 = 4$, $7^3 = 13$, $7^4 = 1$, so $|7| = 4$. To find the order of 11, we compute $11^1 = 11$, $11^2 = 1$, so $|11| = 2$. Similar computations show that $|1| = 1$, $|2| = 4$, $|4| = 2$, $|8| = 4$, $|13| = 4$, $|14| = 2$. [Here is a trick that makes these calculations easier. Rather than compute the sequence 13^1, 13^2, 13^3, 13^4, we may observe that $13 = -2 \bmod 15$, so that $13^2 = (-2)^2 = 4$, $13^3 = -2 \cdot 4 = -8$, $13^4 = (-2)(-8) = 1$.][†] ∎

∎ **EXAMPLE 2** Consider Z_{10} under addition modulo 10. Since $1 \cdot 2 = 2$, $2 \cdot 2 = 4$, $3 \cdot 2 = 6$, $4 \cdot 2 = 8$, $5 \cdot 2 = 0$, we know that $|2| = 5$. Similar computations show that $|0| = 1$, $|7| = 10$, $|5| = 2$, $|6| = 5$. (Here $2 \cdot 2$ is an abbreviation for $2 + 2$, $3 \cdot 2$ is an abbreviation for $2 + 2 + 2$, etc.) ∎

∎ **EXAMPLE 3** Consider Z under ordinary addition. Here every nonzero element has infinite order, since the sequence a, $2a$, $3a$, . . . never includes 0 when $a \neq 0$. ∎

The perceptive reader may have noticed among our examples of groups in Chapter 2 that some are subsets of others with the same binary operation. The group $SL(2, \mathbf{R})$ in Example 18, for instance, is a subset of the group $GL(2, \mathbf{R})$ in Example 9. Similarly, the group of complex numbers $\{1, -1, i, -i\}$ under multiplication is a subset of the group described in Example 15 for n equal to any multiple of 4. This situation arises so often that we introduce a special term to describe it.

Definition Subgroup
If a subset H of a group G is itself a group under the operation of G, we say that H is a *subgroup* of G.

We use the notation $H \leq G$ to mean that H is a subgroup of G. If we want to indicate that H is a subgroup of G but is not equal to G itself, we write $H < G$. Such a subgroup is called a *proper subgroup*. The subgroup $\{e\}$ is called the *trivial subgroup* of G; a subgroup that is not $\{e\}$ is called a *nontrivial subgroup* of G.

Notice that Z_n under addition modulo n is *not* a subgroup of Z under addition, since addition modulo n is not the operation of Z.

Subgroup Tests

When determining whether or not a subset H of a group G is a subgroup of G, one need not directly verify the group axioms. The next

[†] The website **http://www.google.com** provides a convenient way to do modular arithmetic. For example, to compute 13^4 mod 15, just type "13^4 mod 15" in the search box.

three results provide simple tests that suffice to show that a subset of a group is a subgroup.

Theorem 3.1 One-Step Subgroup Test

Let G be a group and H a nonempty subset of G. If ab^{-1} is in H whenever a and b are in H, then H is a subgroup of G. (In additive notation, if $a - b$ is in H whenever a and b are in H, then H is a subgroup of G.)

PROOF Since the operation of H is the same as that of G, it is clear that this operation is associative. Next, we show that e is in H. Since H is nonempty, we may pick some x in H. Then, letting $a = x$ and $b = x$ in the hypothesis, we have $e = xx^{-1} = ab^{-1}$ is in H. To verify that x^{-1} is in H whenever x is in H, all we need to do is to choose $a = e$ and $b = x$ in the statement of the theorem. Finally, the proof will be complete when we show that H is closed; that is, if x, y belong to H, we must show that xy is in H also. Well, we have already shown that y^{-1} is in H whenever y is; so, letting $a = x$ and $b = y^{-1}$, we have $xy = x(y^{-1})^{-1} = ab^{-1}$ is in H. ∎

Although we have dubbed Theorem 3.1 the One-Step Subgroup Test, there are actually four steps involved in applying the theorem. (After you gain some experience, the first three steps will be routine.) Notice the similarity between the last three steps listed below and the three steps involved in the Second Principle of Mathematical Induction.

1. Identify the property P that distinguishes the elements of H; that is, identify a defining condition.
2. Prove that the identity has property P. (This verifies that H is nonempty.)
3. *Assume* that two elements a and b have property P.
4. Use the assumption that a and b have property P to show that ab^{-1} has property P.

The procedure is illustrated in Examples 4 and 5.

EXAMPLE 4 Let G be an Abelian group with identity e. Then $H = \{x \in G \mid x^2 = e\}$ is a subgroup of G. Here, the defining property of H is the condition $x^2 = e$. So, we first note that $e^2 = e$, so that H is nonempty. Now we assume that a and b belong to H. This means that $a^2 = e$ and $b^2 = e$. Finally, we must show that $(ab^{-1})^2 = e$. Since G is Abelian, $(ab^{-1})^2 = ab^{-1}ab^{-1} = a^2(b^{-1})^2 = a^2(b^2)^{-1} = ee^{-1} = e$. Therefore, ab^{-1} belongs to H and, by the One-Step Subgroup Test, H is a subgroup of G. ∎

In many instances, a subgroup will consist of all elements that have a particular form. Then the property P is that the elements have that particular form. This is illustrated in the following example.

EXAMPLE 5 Let G be an Abelian group under multiplication with identity e. Then $H = \{x^2 \mid x \in G\}$ is a subgroup of G. (In words, H is the set of all "squares.") Since $e^2 = e$, the identity has the correct form. Next, we write two elements of H in the correct form, say, a^2 and b^2. We must show that $a^2(b^2)^{-1}$ also has the correct form; that is, $a^2(b^2)^{-1}$ is the square of some element. Since G is Abelian, we may write $a^2(b^2)^{-1}$ as $(ab^{-1})^2$, which is the correct form. Thus, H is a subgroup of G. ∎

Beginning students often prefer to use the next theorem instead of Theorem 3.1.

Theorem 3.2 Two-Step Subgroup Test

Let G be a group and let H be a nonempty subset of G. If ab is in H whenever a and b are in H (H is closed under the operation), and a^{-1} is in H whenever a is in H (H is closed under taking inverses), then H is a subgroup of G.

PROOF By Theorem 3.1, it suffices to show that $a, b \in H$ implies $ab^{-1} \in H$. So, we suppose that $a, b \in H$. Since H is closed under taking inverses, we also have $b^{-1} \in H$. Thus, $ab^{-1} \in H$ by closure under multiplication. ∎

When applying the Two-Step Subgroup Test, we proceed exactly as in the case of the One-Step Subgroup Test, except we use the assumption that a and b have property P to prove that ab has property P and that a^{-1} has property P.

EXAMPLE 6 Let G be an Abelian group. Then $H = \{x \in G \mid |x| \text{ is finite}\}$ is a subgroup of G. Since $e^1 = e$, $H \neq \theta$. To apply the Two-Step Subgroup Test we assume that a and b belong to H and prove that ab and a^{-1} belong to H. Let $|a| = m$ and $|b| = n$. Then, because G is Abelian, we have $(ab)^{mn} = (a^m)^n(b^n)^m = e^n e^m = e$. Thus, ab has finite order (this does not show that $|ab| = mn$). Moveover, $(a^{-1})^m = (a^m)^{-1} = e^{-1} = e$ shows that a^{-1} has finite order. ∎

We next illustrate how to use the Two-Step Subgroup Test by introducing an important technique for creating new subgroups of Abelian

groups from existing ones. The method will be extended to some subgroups of non-Abelian groups in later chapters.

EXAMPLE 7 Let G be an Abelian group and H and K be subgroups of G. Then $HK = \{hk \mid h \in H, k \in K\}$ is a subgroup of G. First note that $e = ee$ belongs to HK because e is in both H and K. Now suppose that a and b are in HK. Then by definition of H there are elements h_1, $h_2 \in H$ and k_1, $k_2 \in K$ such that $a = h_1k_1$ and $b = h_2k_2$. We must prove that $ab \in HK$ and $a^{-1} \in HK$. Observe that because G is Abelian and H and K are subgroups of G, we have $ab = h_1k_1h_2k_2 = (h_1h_2)(k_1k_2) \in HK$. Likewise, $a^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} = h_1^{-1}k_1^{-1} \in HK$.

How do you prove that a subset of a group is *not* a subgroup? Here are three possible ways, any one of which guarantees that the subset is not a subgroup:

1. Show that the identity is not in the set.
2. Exhibit an element of the set whose inverse is not in the set.
3. Exhibit two elements of the set whose product is not in the set.

EXAMPLE 8 Let G be the group of nonzero real numbers under multiplication, $H = \{x \in G \mid x = 1 \text{ or } x \text{ is irrational}\}$ and $K = \{x \in G \mid x \geq 1\}$. Then H is not a subgroup of G, since $\sqrt{2} \in H$ but $\sqrt{2} \cdot \sqrt{2} = 2 \notin H$. Also, K is not a subgroup, since $2 \in K$ but $2^{-1} \notin K$.

When dealing with finite groups, it is easier to use the following subgroup test.

Theorem 3.3 Finite Subgroup Test

Let H be a nonempty finite subset of a group G. If H is closed under the operation of G, then H is a subgroup of G.

PROOF In view of Theorem 3.2, we need only prove that $a^{-1} \in H$ whenever $a \in H$. If $a = e$, then $a^{-1} = a$ and we are done. If $a \neq e$, consider the sequence a, a^2, ... By closure, all of these elements belong to H. Since H is finite, not all of these elements are distinct. Say $a^i = a^j$ and $i > j$. Then, $a^{i-j} = e$; and since $a \neq e$, $i - j > 1$. Thus, $aa^{i-j-1} = a^{i-j} = e$ and, therefore, $a^{i-j-1} = a^{-1}$. But $i - j - 1 \geq 1$ implies $a^{i-j-1} \in H$ and we are done.

Examples of Subgroups

The proofs of the next few theorems show how our subgroup tests work. We first introduce an important notation. For any element a from a group, we let $\langle a \rangle$ denote the set $\{a^n \mid n \in Z\}$. In particular, observe that the exponents of a include all negative integers as well as 0 and the positive integers (a^0 is defined to be the identity).

Theorem 3.4 $\langle a \rangle$ Is a Subgroup

Let G be a group, and let a be any element of G. Then, $\langle a \rangle$ is a subgroup of G.

PROOF Since $a \in \langle a \rangle$, $\langle a \rangle$ is not empty. Let a^n, $a^m \in \langle a \rangle$. Then, $a^n(a^m)^{-1} = a^{n-m} \in \langle a \rangle$; so, by Theorem 3.1, $\langle a \rangle$ is a subgroup of G. ∎

The subgroup $\langle a \rangle$ is called the *cyclic subgroup of G generated by a.* In the case that $G = \langle a \rangle$, we say that G is *cyclic* and a is a *generator of G.* (A cyclic group may have many generators.) Notice that although the list $\ldots, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots$ has infinitely many entries, the set $\{a^n \mid n \in Z\}$ might have only finitely many elements. Also note that, since $a^i a^j = a^{i+j} = a^{j+i} = a^j a^i$, every cyclic group is Abelian.

EXAMPLE 9 In $U(10)$, $\langle 3 \rangle = \{3, 9, 7, 1\} = U(10)$, for $3^1 = 3$, $3^2 = 9$, $3^3 = 7$, $3^4 = 1$, $3^5 = 3^4 \cdot 3 = 1 \cdot 3$, $3^6 = 3^4 \cdot 3^2 = 9, \ldots$; $3^{-1} = 7$ (since $3 \cdot 7 = 1$), $3^{-2} = 9$, $3^{-3} = 3$, $3^{-4} = 1$, $3^{-5} = 3^{-4} \cdot 3^{-1} = 1 \cdot 7$, $3^{-6} = 3^{-4} \cdot 3^{-2} = 1 \cdot 9 = 9, \ldots$. ∎

EXAMPLE 10 In Z_{10}, $\langle 2 \rangle = \{2, 4, 6, 8, 0\}$. Remember, a^n means na when the operation is addition. ∎

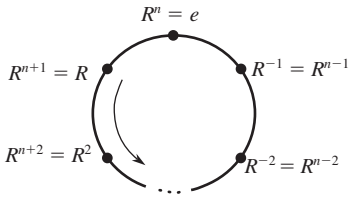
EXAMPLE 11 In Z, $\langle -1 \rangle = Z$. Here each entry in the list $\ldots, -2(-1), -1(-1), 0(-1), 1(-1), 2(-1), \ldots$ represents a distinct group element. ∎

EXAMPLE 12 In D_n, the dihedral group of order $2n$, let R denote a rotation of $360/n$ degrees. Then,

$$R^n = R_{360^\circ} = e, \qquad R^{n+1} = R, \qquad R^{n+2} = R^2, \ldots.$$

Similarly, $R^{-1} = R^{n-1}$, $R^{-2} = R^{n-2}, \ldots$, so that $\langle R \rangle = \{e, R, \ldots, R^{n-1}\}$. We see, then, that the powers of R "cycle back" periodically

with period n. Visually, raising R to successive positive powers is the same as moving counterclockwise around the following circle one node at a time, whereas raising R to successive negative powers is the same as moving around the circle clockwise one node at a time.



In Chapter 4 we will show that $|\langle a\rangle| = |a|$; that is, the order of the subgroup generated by a is the order of a itself. (Actually, the definition of $|a|$ was chosen to ensure the validity of this equation.)

For any element a of a group G, it is useful to think of $\langle a\rangle$ as the smallest subgroup of G containing a. This notion can be extended to any collection S of elements from a group G by defining $\langle S\rangle$ as the subgroup of G with the property that $\langle S\rangle$ contains S and if H is any subgroup of G containing S, then H also contains $\langle S\rangle$ Thus, $\langle S\rangle$ is the smallest subgroup of G that contains S. The set $\langle S\rangle$ is called *the subgroup generated by S*. We illustrate this concept in the next example. The verifications are left to the reader (Exercise 40).

EXAMPLE 13 In Z_{20}, $\langle 8,14\rangle = \{0, 2, 4,\ldots, 18\} = \langle 2\rangle$; in Z, $\langle 8, 13\rangle = Z$; in D_4, $\langle H, V\rangle = \{H, H^2, V, HV\} = \{R_0, R_{180}, H, V\}$; in D_4, $\langle R_{90}, V\rangle = \{R_{90}, R_{90}{}^2, R_{90}{}^3, R_{90}{}^4, V, R_{90}V, R_{90}{}^2V, R_{90}{}^3V\} = D_4$; in **C***, the group of nonzero complex numbers under multiplication, $\langle 1, i\rangle = \{1, -1, i, -i\} = \langle i\rangle$; in **C**, the group of complex numbers under addition, $\langle 1, i\rangle = \{a + bi \mid a, b \in Z\}$ (This group is called the "Gaussian integers"); in **R**, the group of real numbers under addition, $\langle 2, \pi, \sqrt{2}\rangle = \{2a + b\pi + c\sqrt{2} \mid a, b, c \in Z\}$; in a group in which a, b, c, and d commute, $\langle a, b, c, d\rangle = \{a^q b^r c^s d^t \mid q, r, s, t \in Z\}$.

We next consider one of the most important subgroups.

Definition Center of a Group

The *center*, $Z(G)$, of a group G is the subset of elements in G that commute with every element of G. In symbols,

$$Z(G) = \{a \in G \mid ax = xa \text{ for all } x \text{ in } G\}.$$

[The notation $Z(G)$ comes from the fact that the German word for center is *Zentrum*. The term was coined by J. A. de Séguier in 1904.]

Theorem 3.5 Center Is a Subgroup

The center of a group G is a subgroup of G.

PROOF For variety, we shall use Theorem 3.2 to prove this result. Clearly, $e \in Z(G)$, so $Z(G)$ is nonempty. Now, suppose $a, b \in Z(G)$. Then $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$ for all x in G; and, therefore, $ab \in Z(G)$.

Next, assume that $a \in Z(G)$. Then we have $ax = xa$ for all x in G. What we want is $a^{-1}x = xa^{-1}$ for all x in G. Informally, all we need do to obtain the second equation from the first one is simultaneously to bring the a's across the equals sign:

$$ax = xa$$

becomes $xa^{-1} = a^{-1}x$. (Be careful here; groups need not be commutative. The a on the left comes across as a^{-1} on the left, and the a on the right comes across as a^{-1} on the right.) Formally, the desired equation can be obtained from the original one by multiplying it on the left and right by a^{-1}, like so:

$$\begin{aligned} a^{-1}(ax)a^{-1} &= a^{-1}(xa)a^{-1}, \\ (a^{-1}a)xa^{-1} &= a^{-1}x(aa^{-1}), \\ exa^{-1} &= a^{-1}xe, \\ xa^{-1} &= a^{-1}x. \end{aligned}$$

This shows that $a^{-1} \in Z(G)$ whenever a is. ∎

For practice, let's determine the centers of the dihedral groups.

EXAMPLE 14 For $n \geq 3$,

$$Z(D_n) = \begin{cases} \{R_0, R_{180}\} & \text{when } n \text{ is even,} \\ \{R_0\} & \text{when } n \text{ is odd.} \end{cases}$$

To verify this, first observe that since every rotation in D_n is a power of $R_{360/n}$, rotations commute with rotations. We now investigate when a rotation commutes with a reflection. Let R be any rotation in D_n and let F be any reflection in D_n. Observe that since RF is a reflection we have $RF = (RF)^{-1} = F^{-1}R^{-1} = FR^{-1}$. Thus, it follows that R and F commute if and only if $FR = RF = FR^{-1}$. By cancellation, this holds if and only if $R = R^{-1}$. But $R = R^{-1}$ only when $R = R_0$ or $R = R_{180}$, and R_{180} is in D_n only when n is even. So, we have proved that $Z(D_n) = \{R_0\}$ when n is odd and $Z(D_n) = \{R_0, R_{180}\}$ when n is even. ∎

Although an element from a non-Abelian group does not necessarily commute with every element of the group, there are always some elements with which it will commute. For example, every element a commutes with all powers of a. This observation prompts the next definition and theorem.

Definition Centralizer of a in G

Let a be a fixed element of a group G. The *centralizer of a in G*, $C(a)$, is the set of all elements in G that commute with a. In symbols, $C(a) = \{g \in G \mid ga = ag\}$.

EXAMPLE 15 In D_4, we have the following centralizers:

$$\begin{aligned} C(R_0) &= D_4 = C(R_{180}), \\ C(R_{90}) &= \{R_0, R_{90}, R_{180}, R_{270}\} = C(R_{270}), \\ C(H) &= \{R_0, H, R_{180}, V\} = C(V), \\ C(D) &= \{R_0, D, R_{180}, D'\} = C(D'). \end{aligned}$$

Notice that each of the centralizers in Example 15 is actually a subgroup of D_4. The next theorem shows that this was not a coincidence.

Theorem 3.6 $C(a)$ Is a Subgroup

For each a in a group G, the centralizer of a is a subgroup of G.

PROOF A proof similar to that of Theorem 3.5 is left to the reader to supply (Exercise 41).

Notice that for every element a of a group G, $Z(G) \subseteq C(a)$. Also, observe that G is Abelian if and only if $C(a) = G$ for all a in G.

Exercises

The purpose of proof is to understand, not to verify.

ARNOLD ROSS

1. For each group in the following list, find the order of the group and the order of each element in the group. What relation do you see between the orders of the elements of a group and the order of the group?

$$Z_{12}, \qquad U(10), \qquad U(12), \qquad U(20), \qquad D_4$$