

## 4.5

## Groups



**Niels Henrik Abel** (1802–1829) of Norway was identified in childhood as a mathematical genius but never received in his lifetime the professional recognition his work deserved.

At 16, influenced by a perceptive teacher, he read the works of Newton, Euler, and Lagrange. One of Abel's achievements was the demonstration that a general formula for solving fifth-degree equations does not exist. The quadratic formula (for equations of degree 2) is well known, and formulas do exist for solving third- and fourth-degree equations. Abel's accomplishment ended a search that had lasted for years.

In the study of abstract algebra, groups which have the commutative property are referred to as **abelian** groups in honor of Abel. He died of tuberculosis at age 27.

We have considered some mathematical systems, most of which have satisfied some or all of the closure, associative, commutative, identity, inverse, and distributive properties. Systems are commonly classified according to which properties they satisfy. One important category is the mathematical group, which we define here.

**Group**

A mathematical system is called a **group** if, under its operation, it satisfies the closure, associative, identity, and inverse properties.

**EXAMPLE 1** Does the set  $\{-1, 1\}$  under the operation of multiplication form a group?

Check the necessary four properties.

**Closure** The given system leads to the multiplication table below. All entries in the body of the table are either  $-1$  or  $1$ ; the system is closed.

|          |      |      |
|----------|------|------|
| $\times$ | $-1$ | $1$  |
| $-1$     | $1$  | $-1$ |
| $1$      | $-1$ | $1$  |

**Associative** Both  $-1$  and  $1$  are integers, and multiplication of integers is associative.

**Identity** The identity for multiplication is  $1$ , an element of the set of the system  $\{-1, 1\}$ .

**Inverse** Both  $-1$  and  $1$  are their own inverses for multiplication.

All four of the properties are satisfied, so the system is a group. ■

**EXAMPLE 2** Does the set  $\{-1, 1\}$  under the operation of addition form a group?

The addition table below shows that closure is not satisfied, so there is no need to check further. The system is not a group.

|      |      |     |
|------|------|-----|
| $+$  | $-1$ | $1$ |
| $-1$ | $-2$ | $0$ |
| $1$  | $0$  | $2$ |

The system of Example 1 is a finite group. Let's look for an infinite group.



### Amalie ("Emmy") Noether

(1882–1935) was an outstanding mathematician in the field of abstract algebra. She studied and worked in Germany at a time when it was very difficult for a woman to do so. At the University of Erlangen in 1900, Noether was one of only two women. Although she could attend classes, professors could and did deny her the right to take the exams for their courses. Not until 1904 was Noether allowed to officially register. She completed her doctorate four years later.

In 1916 Emmy Noether went to Göttingen to work with David Hilbert on the general theory of relativity. But even with Hilbert's backing and prestige, it was three years before the faculty voted to make Noether a *Privatdozent*, the lowest rank in the faculty. In 1922 Noether was made an unofficial professor (or assistant). She received no pay for this post, although she was given a small stipend to lecture in algebra.

Noether's area of interest was abstract algebra, particularly structures called rings and ideals. (Groups are structures, too, with different properties.) One special type of ring bears her name; she was the first to study its properties.

**EXAMPLE 3** Does the set of integers  $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$  under the operation of addition form a group?

Check the required properties.

**Closure** The sum of any two integers is an integer; the system is closed.

**Associative** Try some examples:

$$2 + (5 + 8) = 2 + 13 = 15$$

and  $(2 + 5) + 8 = 7 + 8 = 15,$

so  $2 + (5 + 8) = (2 + 5) + 8.$

$$-4 + (7 + 14) = -4 + 21 = 17$$

and  $(-4 + 7) + 14 = 3 + 14 = 17,$

so  $-4 + (7 + 14) = (-4 + 7) + 14.$

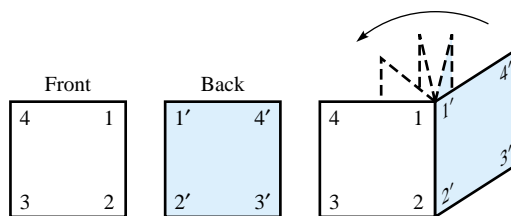
Apparently, addition of integers is associative.

**Identity** We know that  $a + 0 = a$  and  $0 + a = a$  for any integer  $a$ . The identity element for addition of integers is 0.

**Inverse** Given any integer  $a$ , its additive inverse,  $-a$ , is also an integer. For example, 5 and  $-5$  are inverses. The system satisfies the inverse property.

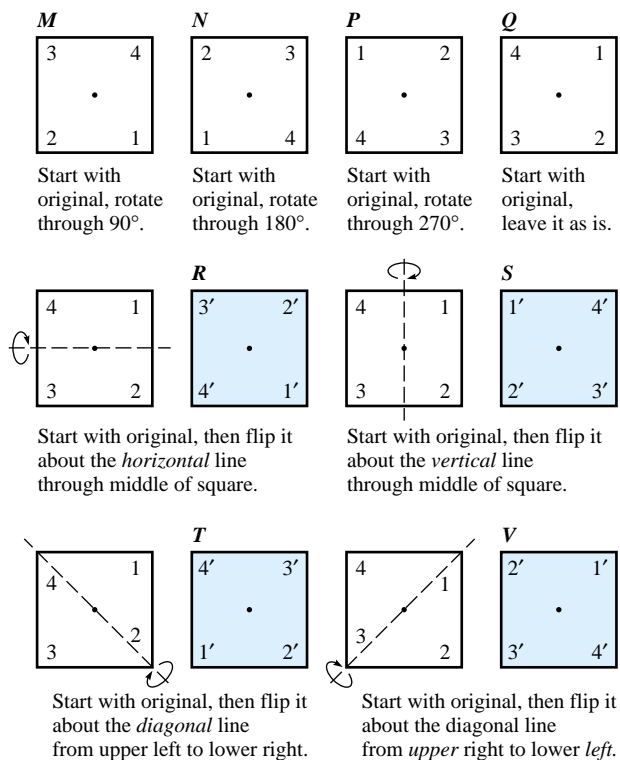
Since all four properties are satisfied, this (infinite) system *is* a group. ■

Group structure applies not only to sets of numbers. One common group is the group of **symmetries of a square**, which we now develop. First, cut out a small square, and label it as shown in Figure 5.



**FIGURE 5**

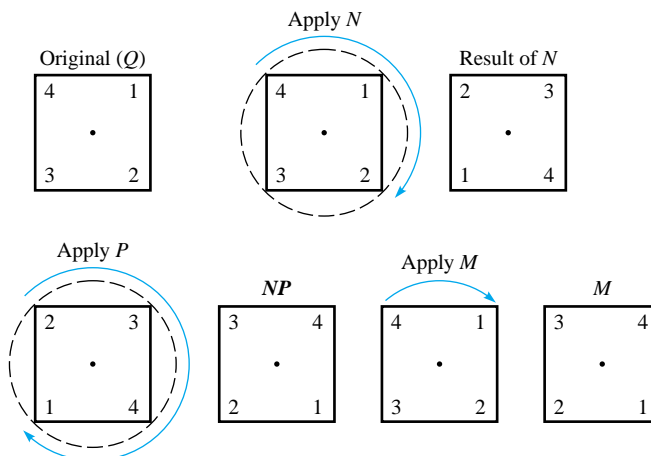
Make sure that 1 is in front of  $1'$ , 2 is in front of  $2'$ , 3 is in front of  $3'$ , and 4 is in front of  $4'$ . Let the letter  $M$  represent a clockwise rotation of  $90^\circ$  about the center of the square (marked with a dot in Figure 6). Let  $N$  represent a rotation of  $180^\circ$ , and so on. A list of the symmetries of a square is given in Figure 6 on the next page.



Symmetries of a square

**FIGURE 6**

Combine symmetries as follows: Let  $NP$  represent  $N$  followed by  $P$ . Performing  $N$  and then  $P$  is the same as performing just  $M$ , so that  $NP = M$ . See Figure 7.



Think of  $N$  as advancing each corner two quarter turns clockwise. Thus 4 goes from upper left to lower right. To this result apply  $P$ , which advances each corner three quarter turns. Thus 2 goes from upper left to lower left. The result,  $NP$ , is the same as advancing each (original) corner one quarter turn, which  $M$  does. Thus  $NP = M$ .

**FIGURE 7**



**Évariste Galois** (1811–1832), as a young Frenchman, agreed to fight a duel. He had been engaged in profound mathematical research for some time. Now, anticipating the possibility of his death, he summarized the essentials of his discoveries in a letter to a friend. The next day Galois was killed. He was not yet 21 years old when he died.

It was not until 1846 that Galois's theories were published. Mathematicians began to appreciate the importance of Galois's work, which centered on solving equations by using groups. Galois found a way to derive a group which corresponds to each equation. So-called Galois groups form an important part of modern abstract algebra.

**EXAMPLE 4** Find  $RT$ .

First, perform  $R$  by flipping the square about a horizontal line through the middle. Then, perform  $T$  by flipping the result of  $R$  about a diagonal from upper left to lower right. The result of  $RT$  is the same as performing only  $M$ , so that  $RT = M$ .

The method in Example 4 can be used to complete the following table for combining the symmetries of a square.

| $\square$ | $M$ | $N$ | $P$ | $Q$ | $R$ | $S$ | $T$ | $V$ |
|-----------|-----|-----|-----|-----|-----|-----|-----|-----|
| $M$       | $N$ | $P$ | $Q$ | $M$ | $V$ | $T$ | $R$ | $S$ |
| $N$       | $P$ | $Q$ | $M$ | $N$ | $S$ | $R$ | $V$ | $T$ |
| $P$       | $Q$ | $M$ | $N$ | $P$ | $T$ | $V$ | $S$ | $R$ |
| $Q$       | $M$ | $N$ | $P$ | $Q$ | $R$ | $S$ | $T$ | $V$ |
| $R$       | $T$ | $S$ | $V$ | $R$ | $Q$ | $N$ | $M$ | $P$ |
| $S$       | $V$ | $R$ | $T$ | $S$ | $N$ | $Q$ | $P$ | $M$ |
| $T$       | $S$ | $V$ | $R$ | $T$ | $P$ | $M$ | $Q$ | $N$ |
| $V$       | $R$ | $T$ | $S$ | $V$ | $M$ | $P$ | $N$ | $Q$ |

**EXAMPLE 5** Show that the system made up of the symmetries of a square is a group.

For the system to be a group, it must satisfy the closure, associative, identity, and inverse properties.

**Closure** All the entries in the body of the table come from the set  $\{M, N, P, Q, R, S, T, V\}$ . Thus, the system is closed.

**Associative** Try examples:

$$P(MT) = P(R) = T.$$

Also,  $(PM)T = (Q)T = T,$

so that  $P(MT) = (PM)T.$

Other similar examples also work. (See Exercises 25–28.) Thus, the system has the associative property.

**Identity** The column at the left in the table is repeated under  $Q$ . Check that  $Q$  is indeed the identity element.

**Inverse** In the first row,  $Q$  appears under  $P$ . Check that  $M$  and  $P$  are inverses of each other. In fact, every element in the system has an inverse. (See Exercises 29–34.)

Since all four properties are satisfied, the system is a group.

**EXAMPLE 6** Form a mathematical system by using only the set  $\{M, N, P, Q\}$  from the group of symmetries of a square. Is this new system a group?

The table for the elements  $\{M, N, P, Q\}$  (shown at the left) is just one corner of the table for the entire system. Verify that the system represented by this table satisfies all four properties and thus is a group. This new group is a *subgroup* of the original group of the symmetries of a square.

| $\square$ | $M$ | $N$ | $P$ | $Q$ |
|-----------|-----|-----|-----|-----|
| $M$       | $N$ | $P$ | $Q$ | $M$ |
| $N$       | $P$ | $Q$ | $M$ | $N$ |
| $P$       | $Q$ | $M$ | $N$ | $P$ |
| $Q$       | $M$ | $N$ | $P$ | $Q$ |

**Monster Groups** Much research in group theory now is devoted to “simple” groups (which are not at all simple). These groups are fundamental—other groups are built up from them. One of the largest of these simple groups has

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

different elements. This huge number of elements is why the group is called the “monster group.” If this “monster group” contains too many elements, how about the “baby monster” simple group, with only

$$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$$

different elements? (For more information, see “The Classification of the Finite Simple Groups,” by Michael Aschbacher in *The Mathematical Intelligencer*, Issue 2, 1981.)

**Permutation Groups** A very useful example of a group comes from studying the arrangements, or permutations, of a list of numbers. Start with the symbols 1-2-3, in that order.

There are several ways in which the order could be changed—for example, 2-3-1. This rearrangement is written:

1-2-3

2-3-1.

Replace 1 with 2, replace 2 with 3, and replace 3 with 1. In the same way,

1-2-3

3-1-2

means replace 1 with 3, 2 with 1, and 3 with 2, while

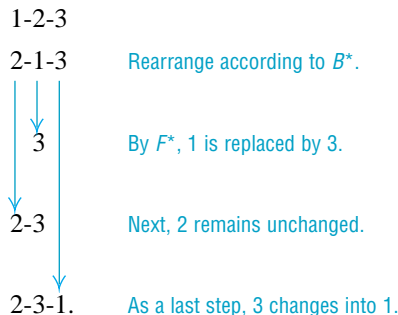
1-2-3

3-2-1

says to replace 1 with 3, leave the 2 unchanged, and replace 3 with 1. All possible rearrangements of the symbols 1-2-3 are listed below where, for convenience, a name has been given to each rearrangement.

A\*: 1-2-3    B\*: 1-2-3    C\*: 1-2-3    D\*: 1-2-3    E\*: 1-2-3    F\*: 1-2-3  
 2-3-1        2-1-3        1-2-3        1-3-2        3-1-2        3-2-1

Two rearrangements can be combined as with the symmetries of a square; for example, the symbol  $B^*F^*$  means to first apply  $B^*$  to 1-2-3 and then apply  $F^*$  to the result. Rearrangement  $B^*$  changes 1-2-3 into 2-1-3. Then apply  $F^*$  to this result: 1 becomes 3, 2 is unchanged, and 3 becomes 1. In summary:

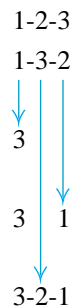


The net result of  $B^*F^*$  is to change 1-2-3 into 2-3-1, which is exactly what  $A^*$  does to 1-2-3. Therefore

$$B^*F^* = A^*.$$

**EXAMPLE 7** Find  $D^*E^*$ .

Use the procedure described above.



Apply  $D^*$ . To apply  $E^*$ , first replace 1 with 3. Next, replace 2 with 1. The last step is to replace 3 with 2. The result:  $D^*E^*$  converts 1-2-3 into 3-2-1, as does  $F^*$ , so

$$D^*E^* = F^*.$$

As further examples,  $A^*B^* = D^*$  and  $F^*E^* = B^*$ .

Once again, we see that we have encountered a mathematical system: the set  $\{A^*, B^*, C^*, D^*, E^*, F^*\}$  and the operation of the combination of two rearrangements. To see whether this system is a group, check the requirements.

**Closure** Combine any two rearrangements and the result is another rearrangement, so the system is closed.

**Associative** Try an example:

$$\begin{array}{ll}
 \text{First,} & (B^*D^*)A^* = E^*A^* = C^*, \\
 \text{while} & B^*(D^*A^*) = B^*B^* = C^*, \\
 \text{so that} & (B^*D^*)A^* = B^*(D^*A^*).
 \end{array}$$

Since other examples will work out similarly, the system is associative.

**Identity** The identity element is  $C^*$ . If  $x$  is any rearrangement, then  $xC^* = C^*x = x$ .

**Inverse** Does each rearrangement have an inverse rearrangement? Begin with the basic order 1-2-3 and then apply, say  $B^*$ , resulting in 2-1-3. The inverse of  $B^*$  must convert this 2-1-3 back into 1-2-3, by changing 2 into 1 and 1 into 2. But  $B^*$  itself will do this. Hence  $B^*B^* = C^*$  and  $B^*$  is its own inverse. By the same process,  $E^*$  and  $A^*$  are inverses of each other. Also, each of  $C^*$ ,  $D^*$ , and  $F^*$  is its own inverse.

Since all four requirements are satisfied, the system is a group. Rearrangements are also referred to as *permutations*, so this group is sometimes called the **permutation group on three symbols**. The total number of different permutations of a given number of symbols can be determined by methods described in the chapter on counting.