CHAPTER 11

Groups of Permutations

11.1 PERMUTATIONS AS GROUPS

In Problem 11 of Chapter 1 we asked, "What is the most effective way to shuffle a pack of cards?" To answer this question we need to return to the ideas about permutations that we introduced in Section 2.6 of Chapter 2 where we discussed permutations and cycles. We will see that permutations provide an example of a mathematical structure called a *group*. Groups play an important role in many areas of mathematics. Our interest in them is because of their relation to problems involving counting patterns. So the work in this chapter is also used later. In particular, we see that it underlies our answer to Problem 13B about the number of ways to color a cube using three colors. We expect that many readers will have met some group theory before. However, we will not assume any previous knowledge. All the ideas about groups that we use will be introduced as we need them.

You will recall from Chapter 2 that you may think of a permutation of a set, X, as a bijection $\sigma: X \to X$. Usually X will be a set of the form $\{1, 2, \ldots, n\}$ for some positive integer n. We let S_n be the set of all permutations of the set $\{1, 2, \ldots, n\}$. In Section 2.6 we introduced two notations for these permutations. In the *bracket notation* we describe a permutation by writing the numbers 1 to n in one row, with the numbers that σ maps them to in a second row, enclosing both rows in one pair of brackets. So, for example, if we write

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 3 & 5 & 2 \end{pmatrix},$$

this means that σ is the permutation of the set $\{1,2,3,4,5,6\}$ such that $\sigma(1) = 4$, $\sigma(2) = 6$, $\sigma(3) = 1$, $\sigma(4) = 3$, $\sigma(5) = 5$, and $\sigma(6) = 2$. In the alternative, *cycle notation*, we write $\sigma = (1\ 4\ 3)(2\ 6)(5)$ or, leaving out the cycle of length 1, just

$$\sigma = (1 \quad 4 \quad 3)(2 \quad 6).$$

TABLE 11.1

	(1 4 3)(2 6)			(1 5 2 4)(3 6)	
5	←	5		←	1
3	←	4		←	2
2	←	6		←	3
4	←	1		←	4
6	←	2		←	5
1	←	3		←	6

Since permutations are functions, we can compose them in the usual way. If σ and permutations of the same set we can define the composite permutation, $\sigma \circ \tau$, by

$$\sigma \circ \tau(x) = \sigma(\tau(x)).$$

Permutations that are given to us in cycle notation can be composed by worki what happens to each element in turn. When doing these calculations it is import remember that the composite permutation $\sigma \circ \tau$ means *first* τ, *then* σ. Here is an ex of how it works out in practice.

Let $\sigma = (1\ 4\ 3)(2\ 6)$ and let $\tau = (1\ 5\ 2\ 4)(3\ 6)$ be two permutations from S_6. We can late the composite permutation $\sigma \circ \tau$ by the method illustrated in Table 11.1.

We work from right to left as $\sigma \circ \tau$ means carrying out the permutation τ fir example, $\sigma \circ \tau(1) = \sigma(\tau(1)) = \sigma(5) = 5$ and $\sigma \circ \tau(4) = \sigma(\tau(4)) = \sigma(1) = 4$, as indicated table. Having worked out all the values of $\sigma \circ \tau$, we can read off from this table the t notation for $\sigma \circ \tau$, as

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 2 & 4 & 6 & 1 \end{pmatrix},$$

and we can then rewrite this in cycle notation as

$$\sigma \circ \tau = (1\ 5\ 6)(2\ 3).$$

After a bit of practice you will not find it necessary to write out the calculati composite permutation in full. The arrow diagram shown in Table 11.1 can be wor mentally, and it should be possible to write down the composite permutation in cyc tion without the need to write down any intermediate steps. If you think you nee practice with these calculations, attempt Exercises 11.1.1A and 11.1.1B, or swap e with a colleague, if possible.

The operation of *composition* of permutations has a number of important a properties that we now describe. Although we are mainly interested in permuta sets of the form $\{1, 2, \ldots, n\}$, these properties hold for arbitrary sets of permutation give general proofs of these properties.

First, we introduce some notation. We use $S(X)$ for the set of all permutations of the set X. The *identity* map on X is the function $\iota_X : X \to X$, given by

$$\text{for all } x \in X, \iota_X(x) = x.$$

It should be clear that ι_X is a permutation of X; that is, it is a bijection. Since permutations are bijections, they have inverses. We use the standard notation σ^{-1} for the inverse of a permutation σ.

We usually omit the symbol $\circ$ for composition and write $\sigma\iota$ for the composite permutation $\sigma \circ \tau$.

THEOREM 11.1

For each set X, the operation of composition on the set, $S(X)$, of permutations of X has the following properties.

a. For all $\sigma, \tau \in S(X)$, $\sigma\tau \in S(X)$.
b. For all $\sigma \in S(X)$, $\sigma\iota_X = \sigma = \iota_X\sigma$.
c. For all $\sigma \in S(X)$, $\sigma\sigma^{-1} = \iota_X = \sigma^{-1}\sigma$.
d. For all $\sigma, \tau, \rho \in S(X)$, $(\sigma\tau)\rho = \sigma(\tau\rho)$.

Proof

a. Suppose $\sigma, \tau \in S(X)$. Let $x, y \in X$ with $x \neq y$. Then, as τ is injective, $\tau(x) \neq \tau(y)$, and hence, as σ is injective, $\sigma(\tau(x)) \neq \sigma(\tau(y))$, that is, $\sigma\tau(x) \neq \sigma\tau(y)$. So $\sigma\tau$ is injective. Now suppose $z \in X$. Then, as σ is surjective, there is some $y \in X$ such that $\sigma(y) = z$, and as τ is surjective, there is some $x \in X$ such that $\tau(x) = y$. Thus there is some $x \in X$ such that $\sigma\tau(x) = \sigma(\tau(x)) = \sigma(y) = z$. So $\sigma\tau$ is surjective. We have therefore shown that $\sigma\tau$ is a bijection, and hence that $\sigma\tau \in S(X)$, as claimed.
b. For $x \in X$ $\sigma\iota_X(x) = \sigma(\iota_X(x)) = \sigma(x)$. Consequently, $\sigma\iota_X = \sigma$. Similarly, $\iota_X\sigma = \sigma$.
c. This follows immediately from the definition of σ^{-1}.
d. Suppose $\sigma, \tau, \rho \in S(X)$ and $x \in X$. Then $((\sigma\tau)\rho)(x) = (\sigma\tau)(\rho(x)) = (\sigma(\tau(\rho(x))) = \sigma(\tau\rho(x)) = (\sigma(\tau\rho))(x)$. Since the composite permutations $(\sigma\tau)\rho$ and $\sigma(\tau\rho)$ have the same effect on each $x \in X$, we deduce that $= (\sigma\tau)\rho = \sigma(\tau\rho)$.

We need to mention two more notational points. Expressed in terms of cycles the identity permutation $\iota \in S_n$ consists of n cycles of length 1. If we adopt our standard convention of not bothering to write down cycles of length 1, ι would simply be represented by an empty space! This is not always convenient, so usually we write either ι for the identity permutation, or often e (from the German *einheit*).

Because we usually omit the symbol $\circ$ when we are writing composite permutations, there can be an ambiguity. For example, if we write

$$(1\ 2\ 4)(3\ 5)(1\ 4\ 3\ 5),$$

this could mean

$$(1\,2\,4)(3\,5)\circ(1\,4\,3\,5) \text{ or } (1\,2\,4)\circ(3\,5)(1\,4\,3\,5) \text{ or}$$

$$((1\,2\,4)\circ(3\,5))\circ(1\,4\,3\,5) \text{ or } (1\,2\,4)\circ((3\,5)\circ(1\,4\,3\,5)).$$

However, it follows from Theorem 11.1d, that these different expressions all represent the same permutation, and so this ambiguity of notation does not cause us any problems.

The properties of permutations given in Theorem 11.1 are so important that we give a special name to any collection of mathematical objects that can be combined in a way that satisfies them. This is embodied in the following definition.

DEFINITION 11.1

A *group* is a pair $(G, \bullet)$, where G is a set and $\bullet$ is an operation defined on G that satisfies the following four properties.

THE GROUP PROPERTIES

G1. Closure: For all $x, y \in G$, $x \bullet y \in G$.
G2. Identity: There is an element $e \in G$, such that for all $x \in G$, $x \bullet e \in x$ and $e \bullet x = x$.
G3. Inverses: For each $x \in G$, there is an element $x^{-1} \in G$, such that $x \bullet x^{-1} = e$ and $x^{-1} \bullet x = e$.
G4. Associativity: For all $x, y, z \in G$, $(x \bullet y) \bullet z = x \bullet (y \bullet z)$.

The notation e used in this definition carries with it an implication that there is just one element of G satisfying the *identity* property. It is not difficult to prove this. Indeed, suppose, to the contrary, that we have two elements e_1, e_2 in G with this property. Then for all $x \in G$, $x \bullet e_2 = x$ and so, in particular, $e_1 \bullet e_2 = e_1$. Also, for all $x \in G$, $e_1 \bullet x = x$ and so $e_1 \bullet e_2 = e_2$. Consequently $e_1 = e_1 \bullet e_2 = e_2$. The unique element of G satisfying the identity property is called the *identity element* of the group. As shown in the definition, we often use e for the identity element of a group. If we need to emphasize that it is the identity element of G, we write this element as e_G.

In a similar way the use of x^{-1} carries with it the implication that for each $x \in G$ there is just one element satisfying the *inverse* property. This is also easy to prove, as if x_1^{-1}, x_2^{-1} were both inverses of x, we have x_1^{-1}, $x_1^{-1} \bullet e = x_1^{-1} \bullet (x \bullet x_2^{-1}) = (x_1^{-1} \bullet x) \bullet x_2^{-1} = e \bullet x_2^{-1} = x_2^{-1}$.

In cases where it is clear from the context which operation is involved in a particular group, we write xy instead of $x \bullet y$. Similarly in such cases, we often talk about "the group G" rather than "the group $(G, \bullet)$."

It follows from Theorem 11.1 that for each set X $(S(X),\circ)$ forms a group. Permutation groups form a very important class of groups. Indeed, in a sense explained at the end of Section 11.2, all groups can be viewed as permutation groups. However, the richness

of the group concept arises from the many other examples of groups that occur in mathematics. We list some of these examples, though they will not be of great interest to us in this book.

Examples of Groups

1. $(Z, +)$, the set of integers with the operation of addition, forms a group. Likewise, $(Q, +)$, the rational numbers; $(R, +)$, the real numbers; and $(C, +)$, the complex numbers, all with the operation of addition, form groups. In each case the identity element is the number 0, and the inverse of x is $-x$. It is easy to check that all these examples satisfy the definition of a group.
2. The sets Z, Q, R, and C do not form groups when the operation is multiplication. They are all closed under this operation, that is, *GI* holds. In each case the number 1 acts as an identity element. Also, multiplication satisfies the associativity property. However, there is a problem with the inverse property. When the operation is multiplication, the number 0 has no inverse, as, if there were any inverse, say z, it would have to satisfy $0 \times z = 1$, which is not possible. In the cases of Q, R, and C we can get around this difficulty by excluding 0. Thus, if we use Q^*, R^*, and C^* for the nonzero rational numbers, nonzero real numbers, and nonzero complex numbers, respectively, then $(Q^*, \times)$, $(R^*, \times)$, and $(C^*, \times)$ are all examples of groups, with 1 as the identity element and $1/x$ as the inverse of x. It is from these examples that we derive the general notation x^{-1} for the inverse of x. However, this does not work for the set, Z^*, of nonzero integers, since only for $x = 1$ and $x = -1$ is $1/x$ also an integer.
   The examples in the next category are much more important.
3. For each positive integer n, and each *field** of numbers, F, let $M_n(F)$ be the set of $n \times n$ invertible (also called nonsingular) matrices, with entries from F, and let $\times$ be the usual operation of matrix multiplication. Then $(M_n(F), \times)$ is a group.
4. For each positive integer n, $(Z_n, +_n)$ is a group where Z_n is the set $\{0, 1, 2, \ldots, n-1\}$, and $+_n$ is the operation of addition modulo n.

In these examples, the group elements are familiar mathematical objects, and the operations are natural ones for those particular objects. Although, in a philosophical sense, mathematical entities are abstract objects, they seem very real to the mathematicians who work with them. Accordingly, groups of these kinds are sometimes referred to as *concrete groups*. In contrast, with *abstract groups* we do not specify what the group elements actually are, but only how they are combined. When the number of elements is small, this can be conveniently displayed by giving a *multiplication table*.

Here is an example of this type. The set G is $\{e, a, b, c, h, v, r, s\}$. The operation $\bullet$ is defined by Table 11.2. The value of $x \bullet y$ is found by looking at the entry in the x-row and y-column. For example, we can see from the table that $v \bullet c = s$.

* A *field* of numbers is a set of numbers closed under the operations of addition and multiplication, and in which these operations have the standard properties. The rational numbers, Q; the real numbers, R; and the complex numbers, C, are all examples of fields. The integers, Z, do not form a field. For the details see, for example, R. B. J. T. Allenby, *Rings, Fields and Groups*, Arnold, London, 1983.

TABLE 11.2

•	e	a	b	c	h	v	r	s
e	e	a	b	c	h	v	r	s
a	a	b	c	e	r	s	v	h
b	b	c	e	a	v	h	s	r
c	c	e	a	b	s	r	h	v
h	h	s	v	r	e	b	c	a
v	v	r	h	s	b	e	a	c
r	r	h	s	v	a	c	e	b
s	s	v	r	h	c	a	b	e

A table of this kind is called either a *group table* or sometimes a *Cayley table.** It is not difficult to see from this table that the first three of the group properties are satisfied. To check *closure* we need only check that each entry in the table is one of the elements of the set G. The convention of using e for the identity element and putting it first in the table makes it easy to confirm that e acts as the identity element, but even if some differently named element had been the identity, and it had been placed somewhere else in the list, it would not have been difficult to spot from the table that it satisfies the $x \bullet e = x = e \bullet x$ property. To see that the inverse property $x \bullet x^{-1} = e = x^{-1} \bullet x$ holds, we need only check that the identity element, e, occurs once in each row and column and in positions that are symmetrical about the leading diagonal from the top left to the bottom right of the table.

We see, for example, that $a \bullet c = e = c \bullet a$, so that $a^{-1} = c$ and $c^{-1} = a$, and in fact all the other elements of this group are their own inverses.

To complete the check that Table 11.2 does indeed define a group, we need also to check that the operation • satisfies the associativity condition. Unfortunately, there is no very easy way to do this from the table, as this involves checking that $(x \bullet y) \bullet z = x \bullet (y \bullet z)$ for all choices of x, y, and z. In fact, it is not necessary to check the cases where at least one of x, y, and z is e, but this still leaves $7 \times 7 \times 7 = 343$ cases. If you are not willing to do all these calculations, we ask you take it on trust for the time being that the operation • is associative. We prove that it does have this property in the next section. Fortunately, as the proof of Theorem 11.1(d) shows, whenever the group elements are functions and the operation is composition, the associativity property always holds.

You may have noticed that in Table 11.2 each group element occurs exactly once in each row and each column. Tables of this kind are called *Latin squares.* In Exercise 11.1.2A you are asked to prove that a group table is always a Latin square. Latin squares are interesting and important combinatorial objects, but because of shortage of space we are not able to discuss them in this book.

Exercises

11.1.1A Evaluate the following compositions of permutations.

i. (1 5 4)(3 6 7 2)∘(4 6 2)(1 5)(3 7)
ii. (1 4 9 8 6)(2 3)∘(1 5 6)∘(7 1 3 2)

* After Arthur Cayley, whose biography is summarized in a footnote in Section 10.1.

11.1.1B Consider the permutations $\sigma = (1\ 5\ 8\ 2)(3\ 7)(4\ 6)$, $\tau = (1\ 7\ 3\ 5\ 2\ 4\ 8\ 6)$, and $\rho = (1\ 3\ 7)(4\ 6\ 8\ 2)$ from S_8. Find the permutations $\sigma \circ \tau$, $\tau \circ \rho$, $(\sigma \circ \tau) \circ \rho$ and $\sigma \circ (\tau \circ \rho)$ in cycle form, and hence verify that in this case $(\sigma \circ \tau) \circ \rho = \sigma \circ (\tau \circ \rho)$.

11.1.2A Prove that, if $(G,\bullet)$ is a group, then

i. For all $x, y, z, \in G$,

a. $x \bullet y = x \bullet z \Rightarrow y = z$ and

b. $y \bullet x = z \bullet x \Rightarrow y = z$.

ii. For all $x, y \in G$, there exist $w, z \in G$ such that $x \bullet w = y$ and $z \bullet x = y$.

[Note that it follows from (i) that in a Cayley table there are no repetitions in any row or any column. Also it follows from (ii) that each group element occurs at least once in each row and in each column. Thus together (i) and (ii) imply that each row and each column form a permutation of the elements of the group. Each Cayley table is, therefore, a Latin square. However, as Exercise 11.1.4B shows, the converse is not, in general, true.]

11.1.2B A group, $(G,\bullet)$, is said to be *commutative* (or *Abelian*) if for all $x, y \in G$, $x \bullet y = y \bullet x$. For which positive integers n is the group $(S_n,\circ)$ commutative?

11.1.3A Find a permutation $\sigma \in S_5$ such that $(4\ 3\ 5\ 2\ 1) \circ \sigma = (1\ 4)(2\ 3)$.

11.1.3B Show that there is no permutation $\sigma \in S_3$ such that $(1\ 2\ 3) \circ \sigma = \sigma \circ (1\ 2)$.

11.1.4A Show that the following table can be completed in just one way so as to form a Latin square, and that when so completed, it is the Cayley table of a group.

	e	a	b
e	e	a	b
a	a		
b	b		

11.1.4B Give a multiplication table for the operation $\bullet$ on the set $X = \{e,a,b,c,d\}$ that forms a Latin square in such a way that $\bullet$ satisfies the *closure*, *identity*, and *inverse* properties, with e as the identity element, but $(X,\bullet)$ is not a group.

11.2 SYMMETRY GROUPS

Groups are very useful when it comes to studying the symmetries of geometric figures. As we see in the next chapter, we need to take symmetries into account when it comes to counting different patterns. We explain the idea of geometric symmetry with a simple example, the symmetries of a square, shown in Figure 11.1.

A square is a symmetrical figure, but what exactly do we mean by this? One way of explaining symmetry is to say that the square occupies the same space and looks the same if we transform it in certain ways. For example, if we give the square a quarter turn clockwise (that is, if we rotate the square through an angle $\frac{1}{2}\pi$ clockwise about the axis through the center of the square, and perpendicular to the plane of the square),* it looks exactly the same as it did originally. We now need to make this idea more mathematically precise.

* We use radian measure for angles. So $\frac{1}{2}\pi$ radians = 90°.

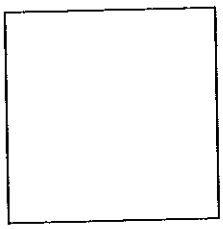


FIGURE 11.1

First, we need to be more precise about what transformations are allowed. If we want the figure to look the same after the transformation it must not distort either distances or angles. Since the angles in a triangle are determined once we know the lengths of its sides, a transformation that doesn't change distances also leaves angles unchanged. So all we need to specify in our definition is that the transformation leaves distances unchanged. As we want to consider both two- and three-dimensional figures, we frame our definition in terms of a space that could be either two-dimensional Euclidean space, R^2, or three-dimensional Euclidean space, R^3. In both these spaces we use $d(p,q)$ for the distance between two points p and q, measured in the standard way.* The *figures* that we mention in the following definition are subsets of either R^2 or R^3.

DEFINITION 11.2

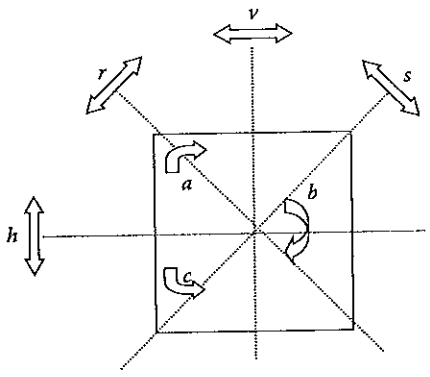
Let S be either R^2 or R^3. A mapping $f: S \to S$ is said to be an *isometry* if for all $p,q \in S$, $d(f(p), f(q)) = d(p,q)$. A *symmetry* of a figure F in the space S is an isometry $f: S \to S$ such that $f(F) = F$.

It should be noted that an isometry is automatically injective, as we have that for any two points p, q, $p \neq q \Rightarrow d(p,q) > 0 \Rightarrow d(f(p), f(q)) = d(p,q) > 0 \Rightarrow f(p) \neq f(q)$. It can be shown that the isometries of R^2 are either rotations, reflections, translations, or glide reflections.† However, a bounded figure, such as a square, cannot be mapped to itself by a translation or glide reflection, and so we need only consider rotations and reflections of bounded figures in R^2. In R^3 we may also need to consider symmetries that are compositions of a reflection and a rotation. We should also not forget the identity mapping, e, which satisfies Definition 11.2 and so counts as a symmetry of every figure.

It is important to note that because we regard symmetries as functions, two transformations of a figure that are physically different but have the same effect on all the points are regarded as being the same symmetry. For example, rotating a figure through an angle $\frac{1}{2}\pi$ clockwise about an axis is physically different from rotating it through an angle $\frac{3}{2}\pi$ counterclockwise about the same axis. However, these different operations have the same effect on each point, so they will count as being the same symmetry.

* That is, in R^2 we measure distances by $d((x_1, y_1),(x_2, y_2)) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$ and by the analogous formula in R^3. In fact, the definition that we give applies more generally, but we do not need to consider the more general context here.

† See, for example, David A. Brannan, Matthew F. Esplen, and Jeremy J. Gray, *Geometry*, Cambridge University Press, Cambridge, 1999.



The symmetries of a square

e	Identity
a	Rotation through ½π clockwise
b	Rotation through π clockwise
c	Rotation through ½π anticlockwise
h	Reflection in the horizontal axis
v	Reflection in the vertical axis shown
r	Reflection in the diagonal axis shown
s	Reflection in the diagonal axis shown

The rotations are about the axis through the centre of the square and perpendicular to it.

FIGURE 11.2

This is nothing more than our usual stipulation that if $f: D \to C$ and $g: D \to C$ are both functions with the same domain and codomain and for all $x \in D$, $f(x) = g(x)$ then we say that $f = g$.

Now that we have been careful to say what we mean by a symmetry of a figure we can see that a square has eight symmetries, as shown in Figure 11.2. The symbols used for these symmetries are somewhat arbitrary, but we will continue to use them.

We will use the notation $S(\square)$ for the group of symmetries of a square. It is now quite straightforward to work out the Cayley table for this group. We encourage you to do this. You might find it helpful to have an actual square to manipulate. Don't forget that in line with our usual convention for composing functions, when we compose two symmetries, say f and g, to obtain the composite fg this means *first* do g, *then* do f.

You should obtain exactly the same table as Table 11.2 in the previous section. Since the operation is composition of functions, we now know, without having to do lots of calculations, that the operation defined by Table 11.2 is associative. Hence it is the Cayley table of a group. In particular, we can also deduce that the symmetries of a square form a group. This is a special case of the more general result that the symmetries of any figure always form a group. This we now prove.

THEOREM 11.2

The set, G, of the symmetries of a figure, F, with the operation, denoted by $\circ$, of composition, forms a group.

Proof

We need to check that the four group properties are satisfied by $(G, \circ)$. Suppose that f and g are symmetries of F. Then as f and g are both isometries we have, for all points p and q (of the appropriate space),

$$d(fg(p), fg(q)) = d(f(g(p)), f(g(q))) = d(g(p), (g(q)) = d(p,q),$$

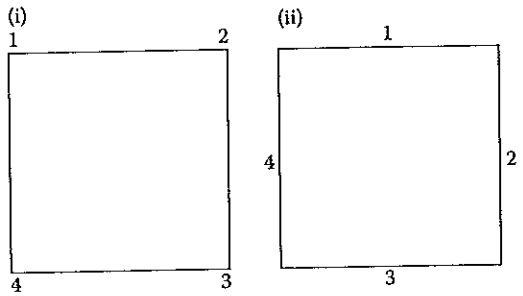


FIGURE 11.3

and hence fg is also an isometry. Since $f(F) = F$ and $g(F) = F$, $fg(F) = f(g(F)) = f(F) = F$. It follows that fg is also a symmetry of F. Thus the closure condition holds.

It is straightforward to check that the identity map is a symmetry of F, and hence that G has an identity element. Each symmetry is a bijection and so has an inverse. We leave as an exercise (Exercise 11.2.1A) to check that if f is an isometry of F then so also is f^{-1}, and hence that G satisfies the inverse condition. We already know that composition of symmetries is associative. Hence it follows that $(G, \circ)$ is a group.

Note that nothing in the above proof depended on the fact that we were dealing with figures in two- or three-dimensional space. The proof would work just as well in higher dimensional spaces. The only problem is that figures in four- and higher dimensional spaces are more difficult to picture!

We can relate groups of symmetries to permutation groups by adding numerical labels to the vertices or edges or, in three dimensions, the faces of a figure. For example, suppose we label the vertices of a square with 1, 2, 3, and 4 as shown in Figure 11.3i.

We can describe the symmetries of the square by specifying how the vertices move. For example, the symmetry h, which is the reflection in the horizontal axis of symmetry, moves the vertex in position 1 to position 4, the vertex in position 2 to position 3, and so on (notice that we regard the numbers as labeling positions that are fixed in space). Thus the permutation h corresponds to the permutation (1 4)(2 3) in S_4. You can readily see that each symmetry of the square corresponds to a permutation in S_4. In this way the eight symmetries of the square correspond to the eight permutations

$$e, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), (1\ 4)(2\ 3), (1\ 2)(3\ 4), (1\ 3), (2\ 4)$$

from S_4, which therefore, by themselves, form a group. This provides us with our first example of a *subgroup*, a concept that we describe in more detail in the next section. Notice that if we label the edges as shown in Figure 11.3ii, then we get a different correspondence between the symmetries of the square and permutations in S_4. For example, using the labeling of the edges, the symmetry h corresponds to the permutation (1 3).

In one sense the group of symmetries of a square is different from the group made up of the eight permutations listed above, since their elements are different, that is, symmetries in the first case and permutations in the second. However, in another sense they are different manifestations of the same group. We now make more precise what we mean by this.

In Figure 11.4 we show three Cayley tables; (i) is that of the rotational symmetries of a square, (ii) is the group Z_4 of the numbers 0, 1, 2, 3 with addition modulo 4,

(i)

o	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

(ii)

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

(iii)

o	e	(1 2 3 4)	(1 3)(2 4)	(1 4 3 2)
e	e	(1 2 3 4)	(1 3)(2 4)	(1 4 3 2)
(1 2 3 4)	(1 2 3 4)	(1 3)(2 4)	(1 4 3 2)	e
(1 3)(2 4)	(1 3)(2 4)	(1 4 3 2)	e	(1 2 3 4)
(1 4 3 2)	(1 4 3 2)	e	(1 2 3 4)	(1 3)(2 4)

FIGURE 11.4

and (iii) is the group of the corresponding permutations of the vertices of the square. Although the tables contain elements of different types, it is evident that the three tables display the same pattern. For example, the identity element occurs in the same positions in each table, and the element a occurs in the same position in the first Cayley table, as does the number 1 in the second table, and the permutation (1 2 3 4) in the third table.

We say that all three groups are *isomorphic* because they have the same structure in a sense that we now make precise. Note the similarities, and the differences, when this definition is compared with that of isomorphism of graphs (Definition 9.3).

DEFINITION 11.3 ***Isomorphism of Groups***

Let $(G, \bullet)$ and$(H,*)$ be groups. We say that these groups are *isomorphic* if there is a bijection $\theta : G \to H$ such that for all $g_1, g_2 \in G$, we have

$$\theta(g_1 \bullet g_2) = \theta(g_1) * \theta(g_2). \tag{11.1}$$

Such a mapping θ is called an *isomorphism* between the two groups.

For example, the mapping θ from the permutations corresponding to the rotations of a square and the numbers modulo 4 [given by iii and ii in Figure 11.4], namely,

$$\theta(e) = 0,\ \theta((1\ 2\ 3\ 4)) = 1,\ \theta((1\ 3)(2\ 4)) = 2, \text{ and } \theta((1\ 4\ 3\ 2)) = 3,$$

is an isomorphism between the two groups. We check just one case of the Equation 11.1. We have

$$\theta((1\ 3)(2\ 4) \circ (1\ 4\ 3\ 2)) = \theta((1\ 3)(2\ 4)) +_4 \theta((1\ 4\ 3\ 2))$$

since the left-hand side is $\theta((1\ 2\ 3\ 4)) = 1$ and the right-hand side is $2 +_4 3 = 1$.

Note that in, Definition 11.3, the equation $\theta(g_1 \bullet g_2) = \theta(g_1) * \theta(g_2)$ expresses the fact that combining elements in the group $(G,\bullet)$ and then mapping to $(H,*)$ produces the same result as first mapping to $(H,*)$ and then combining in $(H,*)$. This condition implies

that the Cayley tables of the two groups have the same pattern. As with isomorphisms between two graphs, an isomorphism between two groups is a *structure-preserving correspondence* of their elements. We regard two isomorphic groups as being essentially the same. So, for example, if we are asked, "How many different groups with four elements are there?" we are being asked to find the largest set, say X, of groups with four elements such that no two of the groups in X are isomorphic, but each group with 4 elements is isomorphic to one of the groups in X. Since the groups whose Cayley tables are shown in Figure 11.4 are isomorphic, any such set X can include at most one of them.

We have seen that each row of a Cayley table corresponds to a permutation of the group elements. For example, if we look at table (i) in Figure 11.4 we see from the a-row that a corresponds to the permutation that in bracket notation we can write as

$$\begin{pmatrix} e & a & b & c \\ a & b & c & e \end{pmatrix}$$

and in cycle notation as $(e\ a\ b\ c)$. A theorem due to Cayley says that this correspondence is always an isomorphism between a group $(G,\bullet)$ and the associated group of permutations of its elements. This is not difficult to prove once we notice that the permutation of G that corresponds to the element $g \in G$ is the permutation, θ_g, of G defined by $\theta_g(x) = g \bullet x$. Here is the proof.

THEOREM 11.3
Cayley's Theorem for Groups

Each group $(G,\bullet)$ is isomorphic to a group of permutations of its elements, with the operation of composition.

Proof

For each $g \in G$, we let $\theta_g : G \to G$ be the mapping defined by:

$$\text{for each } x \in G,\ \theta_g(x) = g \bullet x.$$

By Exercise 11.1.2A, each mapping θ_g is a permutation of the set G. We let G^* be the set of all these permutations, and we let $\Theta : G \to G^*$ be the mapping defined by $\Theta(g) = \theta_g$. Since $\Theta(g)(e) = \theta_g(e) = g \bullet e = g$, it follows that if $g \neq g'$, then $\Theta(g)(e) \neq \Theta(g')(e)$ and hence that $\Theta(g) \neq \Theta(g')$. Consequently, Θ is injective. By the definition of G^*, Θ is surjective, and hence Θ is a bijection.

We also have that, for all $g_1, g_2 \in G$, and all $x \in G$,

$$\Theta(g_1 \bullet g_2)(x) = \theta_{g_1 \bullet g_2}(x) = (g_1 \bullet g_2) \bullet x = g_1 \bullet (g_2 \bullet x) = \theta_{g_1}(\theta_{g_2}(x)) = \theta_{g_1} \circ \theta_{g_2}(x),$$

and therefore

$$\Theta(g_1 \bullet g_2) = \theta g_1 \circ \theta g_2 = \Theta(g_1) \circ \Theta(g_2).$$

Hence Θ is an isomorphism between the group $(G,\bullet)$ and the group $(G^*, \circ)$. This completes the proof.

In this sense every group may be viewed as a group of permutations. However, experience shows that this is not always a helpful way to think about groups. Note also that the group (G^*,o) is generally forms only a small subset of the group $(S(G), \circ)$ of all permutations of the set G. For, if G is a group of n elements, there are $n!$ elements in $S(G)$.

Exercises

11.2.1A Prove that if f is a symmetry of the figure F, then the inverse, f^{-1}, of f is also a symmetry of f.

11.2.1B Prove that if $f: R^2 \to R^2$ is an isometry, then f is surjective.

11.2.2A i. How many symmetries does an equilateral triangle have?
ii. Introduce some symbols for the symmetries of an equilateral triangle, and draw up the Cayley table for the group of these symmetries.
iii. Express the symmetries of an equilateral triangle as elements of S_3 by using the numbers 1, 2, and 3 to label its vertices.

11.2.2B i. How many symmetries does a regular pentagon have?
ii. How many symmetries does a regular n-gon (that is, a polygon with n sides, with all the sides equal and all the internal angles equal) have?

11.2.3A How many rotational symmetries does a cube have? Describe them.

11.2.3B Investigate the rotational symmetries of a regular tetrahedron.

11.2.4A Show that the group of rotational symmetries of an equilateral triangle is isomorphic to the group Z_3 of the integers 0, 1, 2 with addition modulo 3.

11.2.4B Show that every group with two elements is isomorphic to the group Z_2 and that every group with three elements is isomorphic to the group Z_3.

11.2.5A i. Show that each rectangle has four symmetries (note that we are taking "rectangle" to imply "not a square") and that the groups of symmetries of any two rectangles are isomorphic. It follows that we can talk about "*the* group of symmetries of a rectangle."
ii. Show that the group of isometries of a rectangle is not isomorphic to the group Z_4.

11.2.5B Prove that every group with four elements is isomorphic to either the group Z_4 or to the group of symmetries of a rectangle.

11.3 SUBGROUPS AND LAGRANGE'S THEOREM

Group theory is a large subject with an enormous literature. We are going to confine ourselves to those aspects of the subject that are relevant to the combinatorial problems we are interested in. The following definition is important.

DEFINITION 11.4

Suppose that G is a group. A subset H of G is said to be *subgroup* of G, if H itself forms a group with respect to the same operation that makes G a group.

Note: Here it is very convenient to be able to suppress mention of the group operation. If we were being really pedantic, we would have distinguish between the group operation for G, say $\bullet$, which, strictly speaking, is a mapping $\bullet: G \times G \to G$, and the operation on H, which is the restriction of $\bullet$ to the set H.

Since H is a subset of G and we are using the same operation as for the group G, it automatically follows that H satisfies the associativity property. Thus, for H to be a subgroup of G, H must be a subset of G that satisfies the following properties, labeled "SG" for "subgroup."*

THE SUBGROUP PROPERTIES

SG1. H itself is closed under the operation $\bullet$; that is, for all $x, y \in H$, $x \bullet y \in H$.
SG2. H contains the identity element, e_G, of G.
SG3. H contains inverses of all its elements; that is, for each $x \in H$, also $x^{-1} \in H$.

We now present some examples of subgroups.

Examples of Subgroups

1. We have seen that Z, Q, R, and C are all examples of groups, with the operation of addition in each case. Since $Z \subseteq Q \subseteq R \subseteq C$, it follows that Z is a subgroup of Q, Q is a subgroup of R, and R is a subgroup of C.
2. Each group, G, with more than one element has two *trivial* subgroups. The set $\{e_G\}$ containing just the identity element of G can easily be seen to satisfy the subgroup conditions. At the other extreme, the whole group G also counts as being a subgroup of itself.
3. The eight permutations from S_4 corresponding to the symmetries of a square form a subgroup of S_4.
4. We consider the group, S_3, of all the six permutations of the set {1, 2, 3}. Rather than write out these permutations in cycle form, we introduce the following symbols for them. We put $p = (1\ 2\ 3)$, $q = (1\ 3\ 2)$, $r = (1\ 2)$, $s = (2\ 3)$, $t = (1\ 3)$, and e is the identity element, as usual. The Cayley table for this group is shown in Table 11.3.

It can be seen that the top left-hand corner of the table, taken by itself, is also the Cayley table of a group. In other words the subset $\{e, p, q\}$ forms a subgroup of S_3. In this case it is rather easy to spot this. In general, it is rather difficult to find subgroups just by examining Cayley tables. Can you find any more subgroups from this Cayley table? In fact, apart from the two trivial subgroups, and the subgroup $\{e, p, q\}$, there are just three other subgroups, each containing just the identity and one other element.

TABLE 11.3

	e	p	q	r	s	t
e	e	p	q	r	s	t
p	p	q	e	t	r	s
q	q	e	p	s	t	r
r	r	s	t	e	p	q
s	s	t	r	q	e	p
t	t	r	s	p	q	e

* See, for example, Allenby, *Rings, Fields and Groups*, Theorem 5.6.5, for a proof that H is a subgroup if and only if it satisfies these subgroup properties.

Some theory comes to our aid when it comes to finding subgroups. This has to do with the number of elements in a subgroup compared with the number of elements in the group. Group theorists have special terminology for the number of elements in a group or a subgroup.

DEFINITION 11.5

The *order* of a group, or a subgroup, is the number of elements in it.

For example, the order of S_3 is 6, and the group of symmetries of a square has order 8. Group theorists often use the notation $o(G)$ for the order of a group, but we have already introduced the notation $\#(G)$ for the number of elements in any set G, and so we will keep to this notation.

The key idea in what follows is that given a group G and a subgroup H we can use H to partition G into sets, called, in this context, *cosets*, all having the same number of elements as does H. They are defined as follows. To make the general idea more concrete, we use the group S_3 as our example.

DEFINITION 11.6

Let G be a group and let H be a subgroup of G. For each $g \in G$, the *coset* gH is defined to be the set $\{gh : h \in H\}$.

We use the notation gH for the coset, as it is obtained by combining the fixed element g of G with all the elements of H in turn, and so the notation gH is rather suggestive and a good aid to memory. We now look at the specific example of the group S_3 to make these ideas more concrete.

PROBLEM 11.1

Find the cosets of the subgroup $\{e, r\}$ of the group S_3. (Recall that the Cayley table of S_3 is given in Table 11.3.)

Solution

We calculate the cosets as follows:

$$eH = \{ee, er\} = \{e, r\}, \quad qH = \{qe, qr\} = \{q, s\}, \quad sH = \{se, sr\} = \{s, q\},$$
$$pH = \{pe, pr\} = \{p, t\}, \quad rH = \{re, rr\} = \{r, e\}, \quad tH = \{te, tr\} = \{t, p\}.$$

We see that the cosets of different elements can turn out to be the same set. For example, the cosets pH and tH both consist of the set $\{p, t\}$. Note that as we are dealing with sets, the order in which their elements are listed in our calculation does not matter. In other cases the cosets are completely different. For example, there is no element that is in both pH and rH. Thus the different cosets partition G into three disjoint sets, namely, $G = \{e, r\} \cup \{p, t\} \cup \{q, s\}$. Furthermore each coset contains the same number of elements as the subgroup H. Thus $\#(G) = 3 \times \#(H)$, and it follows that $\#(H)$ is a divisor of $\#(G)$.

Of course, we do not need group theory to work out that 2 is a divisor of 6. However, the point of this example is that we can prove that the facts we have noticed about the cosets of H are true for all subgroups of all groups. This we now prove.

It is convenient first to prove a lemma that gives a useful criterion for when two cosets, g_1H and g_2H, are identical.

LEMMA 11.4

If G is a group, H is a subgroup of G, and $g_1, g_2 \in G$, then

$$g_1H = g_2H \Leftrightarrow g_2^{-1}g_1 \in H. \tag{11.2}$$

Proof

First, suppose $g_1H = g_2H$. Since H is a subgroup, $e \in H$, and hence $g_1 = g_1e \in g_1H$. Hence, as $g_1H = g_2H$, we deduce that $g_1 \in g_2H$, and so there is some $h' \in H$ such that $g_1 = g_2h'$. Therefore $g_2^{-1}g_1 = g_2^{-1}g_2h' = h'$ and hence $g_2^{-1}g_1 \in H$.

Second, suppose $g_2^{-1}g_1 \in H$. Let $h = g_2^{-1}g_1$. Then $g_1 = g_2h$. Now assume $x \in g_1H$. Then for some $h' \in H$, $x = g_1h' = g_2hh'$. As H is a subgroup of G, we have $hh' \in H$, and hence $x \in g_2H$. The argument to show that if $x \in g_2H$, then $x \in g_1H$ is similar. Therefore, $x \in g_1H \Leftrightarrow x \in g_2H$, and hence $g_1H = g_2H$.

We can now prove the main result of this section.

THEOREM 11.5

If G is a finite group and H is a subgroup of G, then the different cosets of H partition G into disjoint sets each containing the same number of elements as does H.

Proof

If $x \in G$, then as $e \in H$, $x = xe \in xH$. Thus each element of G is in at least one coset of H. Now suppose x is in two cosets, say $x \in g_1H$ and $x \in g_2H$. Then for some $h_1, h_2 \in H$, we have $x = g_1h_1 = g_2h_2$. It follows that $g_2^{-1}g_1 = h_2h_1^{-1}$. Now as $h_1, h_2 \in H$, and H is a subgroup of G, it follows that $h_2h_1^{-1} \in H$, and therefore $g_2^{-1}g_1 \in H$. It then follows from Lemma 11.4 that $g_1H = g_2H$. Therefore each element of G is in exactly one of the different cosets of H. Suppose $\#(H) = n$. Say that $H = \{h_1, \ldots, h_n\}$, where the elements h_i are all different. Then for each $g \in G$, $gH = \{gh_1, \ldots, gh_n\}$. Since $gh_i = gh_j$ implies $h_i = h_j$ (see Exercise 11.1.2A), the elements gh_i are all different. Therefore $\#(gH) = n = \#(H)$. Our key theorem is now an almost immediate consequence of Theorem 11.5.

THEOREM 11.6
Lagrange's Theorem*

If H is a subgroup of the finite group G, then the order of H is a divisor of the order of G.

* This theorem is named after Joseph Louis Lagrange (1736–1813), who was born in Turin in Italy. His mother was French and his father Italian. Eventually he moved to Paris, and in 1797 he became professor of mathematics at the École Polytechnique. Although Lagrange's theorem is now regarded as a fundamental result about finite groups, it was proved by Lagrange before the concept of a group had been isolated. Lagrange proved his theorem in a more special case dealing with the number of different polynomials that are obtained when its variables are permuted. For a good account of Lagrange's work, and the history of algebra more generally, see John Derbyshire, *Unknown Quantity, A Real and Imaginary History of Algebra*, John Henry Press, Washington DC, 2006, and Atlantic, London, 2007.

Proof

By Theorem 11.5, the different cosets of H completely partition G into disjoint sets each containing $\#(H)$ elements. So if there are k different cosets of H, we have that

$$k \times \#(H) = \#(G), \tag{11.3}$$

and it follows immediately that $\#(H)$ is a divisor of $\#(G)$.

Although we have stated Lagrange's theorem for finite groups, it can be extended to the cases where the group G is infinite and H is either finite or infinite. The proof that the cosets of H partition G is just the same in this case. It is possible to interpret Equation 11.3 in these cases using Cantor's theory of infinite sets, but this does not lead to any very interesting conclusions.

Note also that in the finite case Lagrange's theorem tells us only about the *possible* orders of the subgroups of a given group, G. They must be divisors of the order of G. However, not all these possible orders need be realized. There are cases where n is a divisor of the order of a group G, but G has no subgroup of order n. An example of this kind may be found in Exercise 11.3.2B. There is an extensive theory originated by the Norwegian mathematician Ludwig Sylow (1832–1918), which specifies cases where a group does have subgroups of certain orders, but this is beyond the scope of thisbook.*

Exercises

11.3.1A Determine which of the following sets form subgroups of the group, $S(\square)$, of symmetries of a square (whose Cayley table is given in Table 11.2).

i. $\{e,a,b,c\}$ ii. $\{e,a,b,c,h,v\}$ iii. $\{h,v,r,s\}$ iv. $\{e,r\}$

11.3.1B Which is the smallest subgroup of $S(\square)$ that contains both the symmetries b and h?

11.3.2A We have already noted that the set, Z, of integers forms a group with the operation of addition. Show that the subset, H, consisting of all integers that are multiples of 5, is a subgroup of Z. How many different cosets does H have?

11.3.2B Consider the following set, G, of 12 permutations from S_4:

$\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2\ 3), (1\ 3\ 2),$

$(1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\}.$

G forms a subgroup of S_4. This can be seen most easily by noticing that the permutations in G correspond to the rotational symmetries of a regular tetrahedron with its vertices labeled 1, 2, 3, and 4. Show that although G has order 12 and 6 is a divisor of 12, G does not have a subgroup of order 6. (You might find this easier after reading Section 11.4.)

* See, for example, Allenby, *Rings, Fields and Groups*, Chapter 6.

11.4 ORDERS OF GROUP ELEMENTS

Let G be a group, and let g be an element of G. Since G satisfies the closure condition, gg is also in G, and hence also $g(gg)$, and hence $g(g(gg))$, and so on. Because G satisfies the associativity condition, we can leave out the brackets, and write ggg and $gggg$ for these last two elements of G. At this point it is convenient to introduce the notation g^n for $\overbrace{gg...gg}^{n}$, that is, for the result of combining n g's together. Thus g^2 is gg, g^3 is ggg, and so on. We also use g^1 for g, and it will sometimes be convenient to write g^0 for the identity element e. It is immediately apparent that, when m and n are positive integers, $g^m g^n = g^{m+n}$, as both sides of this equation result from combining $m+n$ g's (but note that this index law depends on the associativity property). Also, if $g^m = g^n$ with $m > n$, then $g^{m-n} g^n = g^n$, and hence $g^{m-n} = e$. This observation will be useful in the sequel.

Now if G is a finite group, the elements g^n for $n = 0,1,2,\ldots$ cannot all be different. Suppose that $g^m = g^n$ with $m > n$. Then, as we have just noted, $g^{m-n} = e$, where $m - n$ is a positive integer. It follows that there is a smallest positive integer k, such that $g^k = e$. This integer k is given a special name.

DEFINITION 11.7

The least positive integer, k, if there is one, such that $g^k = e$, is called the *order* of the group element g, and is written $o(g)$. If there is no such k, we say that g is *an element of infinite order.*

PROBLEM 11.2

Calculate the orders of the elements of the group S_3, whose Cayley table is given in Table 11.3.

Solution

In each group $e^1 = e$, and so the identity element has order 1. It is, clearly, the only element of order 1. We see from the table that $r^2 = s^2 = t^2 = e$, and hence r, s, and t have order 2. We also have that $p^2 = q$, and hence $p^3 = p(p^2) = pq = e$. Thus $p \neq e$, $p^2 \neq e$, but $p^3 = e$, and so p has order 3. Similarly you can check that q has order 3.

We are now ready to explain the relationship between the meanings of *order* as used in Definitions 11.5 and 11.7. We first need a technical lemma.

LEMMA 11.7

Let G be a group and let g be an element of G of (finite) order k. Then for all integers m, n, we have

$$g^m = g^n \Leftrightarrow m \equiv n \pmod{k} \tag{11.4}$$

and, in particular,

$$g^n = e \Leftrightarrow n \equiv 0 \pmod{k}; \text{ that is, } k \text{ is a divisor of } n. \tag{11.5}$$

Proof

We first prove the equivalence 11.5. Then we show that we can deduce the equivalence in Equation 11.4.

Since g has order k, $g^k = e$, and hence, for each integer m, $g^{mk} = (g^k)^m = e^m = e$. So if n is a multiple of k, $g^n = e$. Conversely, suppose that $g^n = e$. Let r be the remainder when n is divided by k. Hence $0 \leq r < k$ and for some positive integer m, $n = mk + r$. Then $g^{mk+r} = e$ and hence $g^r = g^{mk}\, g^r = g^{mk+r} = g^n = e$. Since $0 \leq r < k$ and k is the least positive integer such that $g^k = e$, it follows that $r = 0$. So $n = mk$ and so k is a divisor of n. This proves the equivalence 11.5.

Now suppose m, n are positive integers with, say, $m \geq n$. Then using the equivalence 11.5, we have that $g^m = g^n \Leftrightarrow g^{m-n} = e \Leftrightarrow k$ is a divisor of $m - n \Leftrightarrow m \equiv n (\text{mod } k)$. This proves the equivalence 11.4.

It follows from this lemma that if g is an element of order k in a group G, there are only k different elements of the form g^n in G, namely, $e,g,g^2,\ldots,g^{k-1}$. It is not difficult to show that these elements form a subgroup of G (see Exercise 11.4.3A). This subgroup has order k.

In particular, in the case where G is finite, by Lagrange's theorem, k is a divisor of the order of G. We have thus proved the following useful consequence of Lagrange's theorem.

COROLLARY 11.8
Lagrange's Corollary

If G is a finite group, and $g \in G$, then the order of g is a divisor of the order of G.

As with Lagrange's theorem itself, this corollary only tells us about the possible orders of group elements. For example, you will see from the solution to Exercise 11.4.4B that in the group S_4, which has order 24, there are no elements of orders 6, 8, 12, or 24, even though these are all divisors of 24. We are now ready to give the first application of group theory to a combinatorial problem. We do this in the next section.

Exercises

11.4.1A Calculate the orders of the elements of
i. The group of symmetries of a square,
ii. The group of rotational symmetries of a cube.

11.4.1B Calculate the orders of the symmetries of a regular tetrahedron.

11.4.2A Calculate the orders of the elements of the group Z_{12} of the integers $\{0,1,\ldots, 11\}$ with addition modulo 12.

11.4.2B Show that in the group of rotational symmetries of a circle, for each positive integer k, there is a symmetry of order k, and also that this group contains elements of infinite order.

11.4.3A Show that if g is an element of (finite) order k in a group G, then the subset $H = \{e,g,g^2,\ldots,g^{k-1}\}$ is a subgroup of G.

11.4.3B Suppose that g is an element of order 5 in a group G. Draw up the Cayley table for the subgroup $\{e,g,g^2,g^3,g^4\}$. Is this group isomorphic to another group you have already met? (It might help to write e as g^0 and g as g^1.)

11.4.4A Find all the subgroups of the group of symmetries of a square. (You may find it useful to use the Cayley table of this group as given in Table 11.2.)

11.4.4B Find as many subgroups of S_4 as you can.

11.5 THE ORDERS OF PERMUTATIONS

Shuffling a pack of cards amounts to permuting the cards. Generally the method is roughly to divide the pack into two piles and then more or less interleave the cards in one pile with those in the other pile. With very great skill, a standard pack of 52 cards can be shuffled by dividing the pack into two equal piles of 26 cards, and then alternating the cards from the two piles. This can be done in two ways depending on whether the card that is originally on top stays on top or ends up as the second card in the permuted pack. These two shuffles are called *a top riffle shuffle* and a *bottom riffle shuffle*, respectively, or, alternatively, an *out shuffle* and an *in shuffle*, respectively. These two shuffles are illustrated in Figure 11.5.

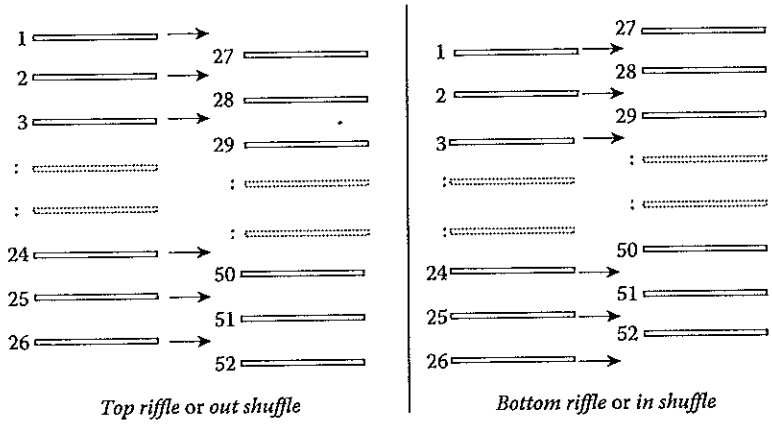
How many of these shuffles must take place before all the cards are restored to their original positions? It helps to answer this question if we write the relevant permutations in cycle notation. For example, we see that in the top riffle shuffle, the card originally in position 1 stays in position 1, the card originally in position 2 moves to position 3, ... the card in position 27 ends up in position 2, and so on. Thus this shuffle, which we denote by σ_T, corresponds to the permutation that is, in bracket notation,

$$\begin{pmatrix} 1 & 2 & 3 & . & . & 24 & 25 & 26 & 27 & 28 & 29 & . & . & 50 & 51 & 52 \\ 1 & 3 & 5 & . & . & 47 & 49 & 51 & 2 & 4 & 6 & . & . & 48 & 50 & 52 \end{pmatrix}.$$

In cycle notation this is

(1)(2 3 5 9 17 33 14 27)(4 7 13 25 49 46 40 28)(6 11 21 41 30 8 15 29)
(10 19 37 22 43 34 16 31) (12 23 45 38 24 47 42 32)(18 35)(20 39 26 51 50 48 44 36)(52).

We can now easily calculate the order of this permutation from its expression in cycle notation. We have already seen in Chapter 2, Section 2.6, that if we have a cycle of length n, then the numbers in the cycle are returned to their original positions after the permutation



Top riffle or *out shuffle* | *Bottom riffle* or *in shuffle*

FIGURE 11.5

has been carried out n times. We see that σ_T is made up of six cycles each of length 8, one cycle of length 2, and two cycles of length 1.

Thus we need to carry out this permutation only eight times before each card is returned to its original position. In the language of group theory, we say that σ_T has order 8. Thus, *if* you could carry out a perfect riffle shuffle eight times in succession (a very big "if"!), you could give the appearance of having shuffled the pack very well, while returning all the cards to their original positions. A very useful skill to have. The bottom riffle shuffle is rather different. We ask you to calculate its order in Exercise 11.5.4A.

Here is another example. Consider the permutation $\sigma = (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9)$ from S_9. Consider the effect of σ^k, that is, carrying out the permutation k times. The numbers 1 and 2 are returned to their original positions if k is a multiple of 2. To return 3, 4, and 5 to their original positions, k needs to be a multiple of 3, and to return 6, 7, 8, and 9 to their original positions, k must be a multiple of 4. So the least positive number k such that σ^k returns all of 1, 2, ..., 8, and 9 to their original positions is the least k that is a multiple of 2, 3, and 4. That is, the order of σ is the least common multiple of 2, 3, and 4, namely 12. It is easy to see how this generalizes. If a permutation in disjoint cycle form is made up of cycles of lengths $k_1,k_2,\ldots,k_s$, then the order of the permutation is the least common multiple of $k_1,k_2,\ldots,k_s$. We write this least common multiple as $lcm(k_1,\ldots,k_s)$.

Since the order of a permutation is determined by the structure of its disjoint cycle representation, it is useful to introduce some terminology and notation for this. We call this structure the *cycle type* of the permutation. We represent cycles of lengths 1, 2, 3, and so on, by the algebraic symbols x_1,x_2,x_3, and so on. We represent the number of cycles of a given length by writing these symbols with the appropriate exponents. So, for example, the cycle type of the permutation $\sigma = (1\ 2)(3\ 4)(5\ 6)(7\ 8\ 9\ 10\ 11)$ is $x_2^3x_5^1$, indicating that σ is made up of three cycles of length 2 and one cycle of length 5. Often the exponent 1 is omitted, so that the cycle type of σ could be written as $x_2^3x_5$.

In general, a permutation has cycle type $x_{k_1}^{r_1}x_{k_2}^{r_2}\ldots x_{k_s}^{r_s}$, where $k_1,k_2,\ldots,k_s$ is an increasing sequence of positive integers, and $r_1,\ldots,r_s$ are positive integers, if in disjoint cycle form it is made up of r_t cycles of length k_t, for $1 \le t \le s$. The usefulness of this notation will become apparent in Chapter 14.

Suppose σ is a permutation from S_n with cycle type $x_{k_1}^{r_1}\ldots x_{k_s}^{r_s}$. Then the total number of the positive integers in the cycles that make up σ is n. Hence we must have

$$r_1k_1 + \ldots + r_sk_s = n. \tag{11.6}$$

If we rewrite Equation 11.6 as

$$\overbrace{k_1+\ldots+k_1}^{r_1}+\overbrace{k_2+\ldots+k_2}^{r_2}+\ldots+\overbrace{k_s+\ldots+k_s}^{r_s}=n, \tag{11.7}$$

we see that Equation 11.6 corresponds to a *partition* of n, as described in Chapter 6. Thus the different cycle types of permutations in S_n correspond to the partitions of n. Since two

TABLE 11.4

Partition	Order
4	4
3+1	3
2+2	2
2+1+1	2
1+1+1+1+1	1

permutations that have the same cycle structure have the same order, if we want to find the orders of the elements of S_n, all we need do is list the partitions of n. So, for example, the orders of the elements of S_4 are as given in Table 11.4.

Thus, as we remarked in the previous section, S_4 is a group of order 24 in which there are no elements of orders 6, 8, 12, and 24 even though these are divisors of 24.

Exercises

11.5.1A Find the orders of the following permutations.
a. (1 2)(3 4 5)(6 7 8 9)(10 11 12 13 14)
b. (1 2 3)(4 5 6 7)(8 9 10 11 12 13)

11.5.1B Find the order of the permutation $\sigma \in S_{20}$, which in bracket notation is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ 7 & 8 & 14 & 1 & 2 & 6 & 11 & 16 & 10 & 17 & 4 & 15 & 20 & 9 & 12 & 18 & 13 & 5 & 3 & 19 \end{pmatrix}.$$

11.5.2A i. Find a permutation in S_{15} that has order 105.
ii. Show that for $n < 15$ there is no permutation in S_n of order 105.

11.5.2B i. Find a permutation in S_{31} that has order 1001.
ii. Show that for $n < 31$ there is no permutation in S_n of order 1001.

11.5.3A For $n = 4,5,6$, find the orders of the permutations in S_n.

11.5.3B For $1 \leq n \leq 10$ find the largest order of the permutations in S_n.

11.5.4A Express the permutation corresponding to a bottom riffle shuffle of 52 cards in disjoint cycle form, and use this to calculate its order.

11.5.4B Express the permutations corresponding to a bottom riffle shuffle and a top riffle shuffle of a pack of 40 cards, and calculate their orders.

11.5.5A Find the largest order of the permutations in S_{52}. (There are 281,589 partitions of 52, so that, without a computer, it is hardly practicable to answer this question by listing all the partitions and then calculating their least common multiples. Your search for a partition that corresponds to a permutation of the largest possible order should be guided by the fact that since for distinct primes p, q and positive integers k, l, $p^k + p^l < p^k p^l$, it is only necessary to consider partitions in which the parts are either powers of primes, or 1. We can regard the permutation of largest order in S_{52} as giving rise to the most effective way of shuffling a standard pack of 52 cards. Thus the answer to this exercise could be regarded as providing us with an answer to Problem 11 of Chapter 1.)

11.5.5B Find the largest order of the permutations in S_{50}.

CHAPTER 12

Group Actions

12.1 COLORINGS

In Chapter 1 we mentioned the following two problems.

PROBLEM 13A
Coloring a Chessboard
How many different ways are there to color the squares of a chessboard using two colors?

On a standard 8×8 chessboard, the squares are colored alternately black and white as shown in Figure 12.1i, but clearly they could be colored in many other ways. Alternative colorings are shown in Figure 12.1ii and iii. The problem is to decide exactly how many different colorings are possible.

PROBLEM 13B
Coloring a Cube
In how many different ways can you color a cube using three colors? One such coloring is shown in Figure 12.2.

These problems have a similar character. One difference is that the first problem is about a two-dimensional figure, and the second problem is about a three-dimensional figure. In this chapter we discuss only the first problem, as it is rather easier to work in two dimensions than in three. The solutions to both problems are given in the next chapter after we have described the ideas needed to solve them.

To make things as simple as possible for us, we begin by dealing with the case of a 2×2 chessboard; the case of a 1×1 chessboard is too simple for us to learn anything useful from it. A 2×2 chessboard has four squares, so with two choices of color for each square, there are altogether $2^4 = 16$ ways it can be colored. These 16 colorings are shown in Figure 12.3, where we have labeled them C1, C2, ..., C16, for future reference.

Are these colorings really all different? This depends on what we mean by "different." It seems reasonable to say that some of these colorings really are the same, and that they only look different because the chessboard has been rotated or reflected. For example, if we give the coloring C2 a quarter turn clockwise, it looks like C3. Also, the reflection in the vertical axis converts C2 into C3. From this point of view C2 and C3 are the same.

Indeed, in this light there are only six different patterns among these colorings. That is, we can put the colorings into the following six sets, with all the colorings in the same set having the same pattern.

{C1}, {C2, C3, C4, C5}, {C6, C7, C8, C9}, {C10, C11}, {C12, C13, C14, C15}, {C16}

Lurking in the background are the symmetries of the square. We have put two colorings in the same set if we can obtain one from the other by applying one of the symmetries of a square. As it happens, the case of a coloring of a 2×2 chessboard with two colors is so simple that it makes no difference whether we take into account reflections or not. In each case, whenever there is a reflectional symmetry taking one coloring to another coloring, there is also a rotational symmetry that does the same job. However, there is a difference as soon as we consider 3×3 and larger chessboards. Consider the two colorings in Figure 12.4. There is a reflectional symmetry that takes coloring (i) to coloring (ii), but no rotation of (i) produces coloring (ii).

We are free to choose whether we wish to regard these colorings as having the same pattern or not. This amounts to deciding which group of symmetries we are going to use, either the full group of all eight symmetries of the square, or just the subgroup consisting of only the identity and the rotational symmetries. The underlying theory turns out to be the same whichever group of symmetries we choose. The theory we are speaking about here deals with the interaction between a group and the members of some set. In the cases of interest to us the group will always be a group of symmetries of some figure, and the set will be a set of colorings of the same figure.

Exercises

12.1.1A How many colorings are there of
i. A standard 8×8 chessboard, using two colors
ii. The faces of a cube using three colors

12.1.1B How many colorings are there of an $n \times n$ chessboard using k colors?

12.1.2A Give an example of two colorings of a 2×2 chessboard, using *three* colors, such that one can be obtained from the other by a reflection but not by a rotation.

12.1.2B Are there two colorings of the faces of a cube using two colors such that one can be obtained from the other by a reflection but not by a rotation?

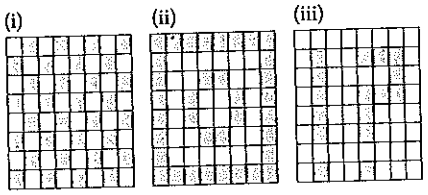


FIGURE 12.1

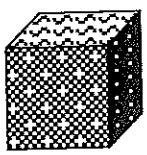


FIGURE 12.2

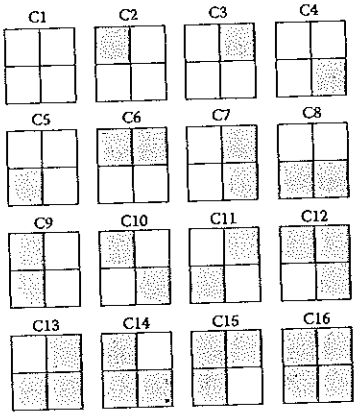


FIGURE 12.3

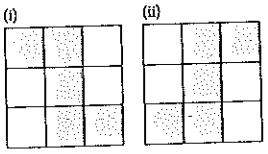


FIGURE 12.4

12.2 THE AXIOMS FOR GROUP ACTIONS

We wish to describe the general situation where we have an interaction between a group, say G, and a set, say X. In this abstract discussion you may find it helpful to keep in mind the particular example of the symmetries of a square and the colorings of a 2×2 chessboard, described in the previous section. We will often refer to this example.

The symmetries of a square in our example interact with each coloring to produce a (possibly) different coloring. For example, the quarter turn clockwise, for which we have used the symbol a, interacts with the coloring C2 to produce the coloring C3. We express this by writing $a \triangleright \mathrm{C2} = \mathrm{C3}$, and in general, we use $g \triangleright x$ for the result of g acting on x. In order to develop a general theory we require that this interaction satisfies a couple of simple and natural properties, as given in the following definition.

DEFINITION 12.1

Let $(G,\bullet)$ be a group and let X be a set. We say that G *acts on* X if for each $g \in G$ and each $x \in X$, there is defined an element $g \triangleright x \in X$, in such a way that the following properties hold:

THE GROUP ACTION CONDITIONS

GA1. For each $x \in X$, $e_G \triangleright x = x$, where e_G is the identity element of G.
GA2. For all $g_1, g_2 \in G$, and each $x \in X$, $g_1 \triangleright (g_2 \triangleright x) = (g_1 \bullet g_2) \triangleright x$.

Whenever a group acts on a set we say that we have a *group action*.

We stress that, in a group action, the elements of G are usually completely different from the elements of X. Thus the action of g on x to yield $g \triangleright x$ is very different from, for example, the combination of two group elements, which are objects of the same kind, to produce another group element. So, although we often omit the symbol for a group operation and write gh instead of $g \bullet h$, the symbol $\triangleright$ *should never be left out.* It helps to remind us of the disparity between g and x. [In those cases where the elements of the group G are functions with domain X, it may sometimes be appropriate to write $g(x)$ in place of $g \triangleright x$.]

It is not difficult to see that if G is a group of symmetries of a figure, and if X is the set of all colorings of the figure, then the action defined as in the previous section satisfies properties GA1 and GA2. In this case GA1 amounts to the fact that the identity element of G is the identity map, ι, and for each coloring x, $\iota \triangleright x = \iota(x) = x$, and GA2 to $g_1 \triangleright (g_2 \triangleright x) = g_1(g_2(x)) = g_1 \circ g_2(x) = (g_1 \circ g_2) \triangleright x$. Thus the examples of the previous section are group actions. For some examples of a different kind, see the exercises at the end of this section.

We conclude this section with a simple technical lemma about group actions that we need later on.

LEMMA 12.1

Let G be a group that acts on a set X. Then for each $g \in G$, and all x,y $\in X$,

$$g \triangleright x = y \Leftrightarrow g^{-1} \triangleright y = x.$$

Proof

Suppose that $g \triangleright x = y$. Then, $g^{-1} \triangleright y = g^{-1} \triangleright (g \triangleright x) = (g^{-1} \bullet g) \triangleright x$, by (GA2), $= e \triangleright x = x$, by GA1.

The converse implication, $g^{-1} \triangleright y = x \Rightarrow g \triangleright x = y$, is proved similarly.

Exercises

12.2.1A Let G be the group, $(\mathbb{R}, +)$, of real numbers with the operation of addition, and let X be the set, $\mathbb{R}^2$, of points in the plane. Suppose we define the action of $\mathbb{R}$ on $\mathbb{R}^2$ by specifying that for each $\theta \in \mathbb{R}$ and all $x \in \mathbb{R}^2$, $\theta \triangleright x =$ the point to which x is moved by a rotation through an angle θ counterclockwise about the origin. [Thus, $\theta \triangleright (x,y) = (x \cos\theta - y \sin\theta, x \sin\theta + y \cos\theta)$.] Show that this satisfies the group action conditions.

12.2.1B This question is about a more sophisticated example of a group action. Let G be any group. We define an action of the group G on G by: for $g \in G$ and $x \in G$, $g \triangleright x = gxg^{-1}$. Show that this satisfies the group action conditions. The action in this case is called *conjugation*, and gxg^{-1} is called the *conjugate of* x *by* g. This plays an important role in the theory of groups, but it is not greatly important from the point of view of this book.

12.2.2A Let n be a positive integer. We define the action of the group, S_n, of all permutations of the set $\{1,2,\ldots,n\}$ on the set of edges of the complete graph, $K_n = (V_n, E_n)$, with n vertices, say $V_n = \{v_1,\ldots, v_n\}$, by: for $\sigma \in S_n$ and $\{v_i, v_j\} \in E_n$, $\sigma \triangleright \{v_i, v_j\} = \{v_{\sigma(i)}, v_{\sigma(j)}\}$. Show that this satisfies the group

action conditions. This example of a group action plays an important role when it comes to counting the number of different simple graphs, as we do in Chapter 14.

12.2.2B Let G be a group, and let g_0 be a particular element of G. We define the action of the group, $(\mathbb{Z}, +)$, of the integers with addition, on G, as follows: For $n \in \mathbb{Z}$ and $g \in G$, $n \triangleright g = g_0^n g$, where we interpret g_0^0 as the identity element e_G of G, and for $n < 0$, we interpret g_0^n as $(g_0^{-n})^{-1}$. Show that this satisfies the group action conditions.

12.2.3A Suppose that the group G acts on the set X. Show that for all $g, h \in G$ and all $x \in X$, $g \triangleright x = h \triangleright x \Leftrightarrow g^{-1}h \triangleright x = x$.

12.2.3B Consider the group action of $\mathbb{R}$ on $\mathbb{R}^2$ as described in Exercise 12.2.1A. Determine the set

$$\{\theta \in \mathbb{R} : \theta \triangleright (1,0) = \frac{\pi}{4} \triangleright (1,0)\}.$$

12.3 ORBITS

We can now explain, in terms of group actions, what is meant by two colorings of some figure being regarded as "the same." We regard two colorings as being the same if some symmetry of the figure maps one to the other. Consequently, whether or not two colorings of a figure are regarded as being the same will depend heavily on which symmetries of the figure are taken into account. We can now explain this situation in general terms by using the language of group actions and giving a definition in this general context.

DEFINITION 12.2

Let G be a group that acts on a set X. We define the relation $\sim_G$ on X as follows:

$$\text{For all } x,y \in X,\ x \sim_G y \Leftrightarrow \text{there is some } g \in G \text{ such that } g \triangleright x = y.$$

The notation suggests that $\sim_G$ is an equivalence relation. We now prove that this is indeed the case. Recall that this means showing that the relation $\sim_G$ is *reflexive*, *symmetric*, and *transitive*. The proof uses the group action conditions, and it is notable that the proof that $\sim_G$ has these properties uses the identity, inverses, and closure properties of a group, respectively, to do this.

LEMMA 12.2

The relation $\sim_G$ is an equivalence relation on X.

Proof

We check that $\sim_G$ has the three necessary properties to be an equivalence relation.

Reflexive: Suppose $x \in X$. Since G is a group, it has an identity element e, and by GA1 $e \triangleright x = x$. It follows that $x \sim_G x$. Therefore $\sim_G$ is reflexive.

Symmetric: Suppose $x,y \in G$ and $x \sim_G y$. Then there is some $g \in G$ such that $g \triangleright x = y$. As G is a group, g has an inverse, g^{-1}, which is also in G. By Lemma 12.1, $g^{-1} \triangleright y = x$. Hence $y \sim_G x$. Therefore $\sim_G$ is symmetric.

Transitive: Suppose $x,y,z \in X$ and both $x \sim_G y$ and $y \sim_G z$. Then there are $g,h \in G$ such that $g \triangleright x = y$ and $h \triangleright y = z$. As G is a group, $hg \in G$, and using GA2, we have that $hg \triangleright x = h \triangleright (g \triangleright x) = h \triangleright y = z$. Hence $x \sim_G z$. Therefore $\sim_G$ is transitive.

Because $\sim_G$ is an equivalence relation, it partitions X into disjoint equivalence classes. When G is a group of symmetries acting on a set of colorings, these equivalence classes are the colorings that we are regarding as being the same. Thus our question about how many *different* colorings there are may be restated as asking how many different equivalence classes there are. In this context the standard term for the equivalence classes is *orbits*. Here is the formal definition.

DEFINITION 12.3

Let the group G act on a set X. The equivalence classes of the relation $\sim_G$ are called *orbits*. For each $x \in X$, we let $Orb(x)$ be the orbit to which x belongs.

Since $y \in Orb(x) \Leftrightarrow x \sim_G y \Leftrightarrow$ for some $g \in G$, $g \triangleright x = y$, it follows that $Orb(x) = \{g \triangleright x: g \in X\}$. That is, the orbit of x consists of all the elements of X that we obtain from x by letting each element of G act on x.

So we are now interested in how to calculate the number of different orbits when a group acts on a set. Before we can give the theorem that answers this question we need to develop one more theoretical idea. We do this in the next section.

Exercises

12.3.1A Consider the group action described in Exercise 12.2.1A. Find the orbits of the points (1,0) and (0,0).

12.3.1B Find a group action on R^2 whose orbits are ellipses.

12.3.2A Let G be the group, $(R,+)$, of real numbers with addition, and let $X = R^2$. The action of G of X is defined by: for $t \in R$, and $(x,y) \in R^2$, $t \triangleright (x,y) = (x + t, y + 2t)$. Show that this satisfies the group action conditions. Find the orbits of the points (0,0), (0,1), and (1,2).

12.3.2B Let G be the group, $S(\square)$, of symmetries of the square (recall that the Cayley table of this group is given in Table 11.2). Find the orbits of each element of G with respect to the group action of conjugation, as described in Exercise 12.2.1B.

12.4 STABILIZERS

Whenever a group G acts on a set X, each element of X is *fixed* by the identity element of G in the sense that $e \triangleright x = x$. This is built into the definition of a group action as condition GA1. Other elements of G may fix certain elements of X. For example, in our standard example of colorings of a 2×2 chessboard, the diagonal reflection r fixes each of the colorings C1, C2, C4, C10, C11, C13, C15, and C16, as these are symmetrical about the relevant diagonal. The type of symmetry of a particular coloring is determined by those symmetries that leave it unchanged. We give this set a special name.

DEFINITION 12.4

Let the group G act on a set X. For each $x \in X$, the set of elements of G that fix x is called the *stabilizer* of x. We let $Stab(x)$ be the stabilizer of x. Thus

$$Stab(x) = \{g \in G: g \triangleright x = x\}.$$

It can be seen that with our example of the group, $S(\square)$, of symmetries of a square acting on the colorings of a 2×2 chessboard, the stabilizer of C2 is $\{e,r\}$, and that of C10 is $\{e,b,r,s\}$. These are both subgroups of $S(\square)$. The next result tells us that this is not an accident.

LEMMA 12.3

If the group G acts on the set X, then for each $x \in X$, $Stab(x)$ is a subgroup of G.

Proof

We check that $Stab(x)$ satisfies the subgroup conditions.

Closure: Suppose $g,h \in Stab(x)$, then $g \triangleright x = x$ and $h \triangleright x = x$. Hence, by GA2, $gh \triangleright x = g \triangleright (h \triangleright x) = g \triangleright x = x$, and hence $gh \in Stab(x)$. So the closure condition is satisfied.

Identity: By GA1, $e \triangleright x = x$, and so $e \in Stab(x)$.

TABLE 12.1

Coloring	Orbit	Stabilizer
C1	{C1}	$\{e,a,b,c,h,v,r,s\}$
C2	{C2, C3, C4, C5}	$\{e,r\}$
C3		$\{e,s\}$
C4		$\{e,r\}$
C5		$\{e,s\}$
C6	{C6, C7, C8, C9}	$\{e,v\}$
C7		$\{e,h\}$
C8		$\{e,v\}$
C9		$\{e,h\}$
C10	{C10, C11}	$\{e,b,r,s\}$
C11		
C12	{C12, C13, C14, C15}	$\{e,s\}$
C13		$\{e,r\}$
C14		$\{e,s\}$
C15		$\{e,r\}$
C16	{C16}	$\{e,a,b,c,h,v,r,s\}$

Inverses: Suppose $g \in Stab(x)$. Then $g \triangleright x = x$, and so, by Lemma 12.1, $g^{-1} \triangleright x = x$. Hence $g^{-1} \in Stab(x)$, and the inverses condition is satisfied.

This completes the proof.

We are interested in stabilizers because, as we will soon see, they help us to count orbits. Group theorists are interested in stabilizers for other reasons. As Lemma 12.3 shows, they are useful in identifying subgroups. For example, the subgroup $\{e,b,r,s\}$ of $S(*)$ is not easy to find from the Cayley table (see Table 11.2), but can easily be identified as $Stab(C10)$.

Once again, it is instructive to return to our example of the group $S(\square)$ acting on the colorings of a 2×2 chessboard. In Table 12.1 we have listed the orbits and the stabilizers of the colorings.

We see that the larger the orbit then the smaller is the stabilizer. Indeed, in each case $\#(Orb(x)) \times \#(Stab(x)) = 8$, and 8 is the number of elements in the group $S(\square)$. This is not a coincidence, but an important result that is true in every case of a group action.

THEOREM 12.4
The Orbit-Stabilizer Theorem

If the group G acts on the set X, then for each $x \in X$,

$$\#(Orb(x)) \times \#(Stab(x)) = \#(G). \tag{12.1}$$

Proof

By Lemma 12.3, $Stab(x)$ is a subgroup of G. So Equation 12.1 is similar to the equation that occurs in our proof of Lagrange's theorem (Theorem 11.6), namely,

$$k \times \#(H) = \#(G), \tag{12.2}$$

where k is the number of different cosets of H.

Comparing Equations 12.1 and 12.2 we see that to prove Equation 12.1 it will be enough to prove that

$$\#(Orb(x)) = \text{the number of different cosets of } Stab(x).$$

Consequently, we need to show that there is a one–one correspondence between the elements of $Orb(x)$ and the cosets of $Stab(x)$. Now, $Orb(x) = \{g \triangleright x: g \in G\}$, and the set of cosets of $Stab(x)$ is $\{gStab(x): g \in G\}$. We now establish the required one–one correspondence between these sets as follows:

For $g_1, g_2 \in G$, we have that

$$g_1 \triangleright x = g_2 \triangleright x \Leftrightarrow g_2^{-1}g_1 \triangleright x = x, \text{ by the result of Exercise 12.2.3A,}$$

$$\Leftrightarrow g_2^{-1}g_1 \in Stab(x), \text{ by the definition of } Stab(x),$$

$$\Leftrightarrow g_1Stab(x) = g_2Stab(x), \text{ by Lemma 11.4.}$$

This establishes the desired correspondence, and so completes the proof of Theorem 12.4. We can immediately deduce the following corollary.

COROLLARY 12.5

Let G be a finite group that acts on a set X. Then the number of elements in each orbit is a divisor of the order of G.

In particular, in the case of the group action of conjugation of a group on itself, the number of elements in each orbit, which in this context are also called *conjugacy classes*, is a divisor of the number of elements in the group. This is a very useful result when it comes to analyzing the structure of groups.

As we now see, we can easily deduce from the orbit-stabilizer theorem the following result, which gives a formula for the number of orbits.

THEOREM 12.6
The Orbit-Counting Theorem

Let G be a finite group that acts on the set X. Then the number of different orbits is

$$\frac{1}{\#(G)}\sum_{x\in X}\#(Stab(x)).$$

Proof

Suppose that there are k different orbits, $Orb(y_1),Orb(y_2),\ldots,Orb(y_k)$. For $1 \le r \le k$ and for each $x \in Orb(y_r)$, $Orb(x) = Orb(y_r)$. Hence, by the orbit-stabilizer theorem,

$$\#(Stab(x))=\frac{\#(G)}{\#(Orb(x))}=\frac{\#(G)}{\#(Orb(y_r))}.$$

Hence

$$\sum_{x\in Orb(y_r)}\#(Stab(x))=\sum_{x\in Orb(y_r)}\frac{\#(G)}{\#(Orb(y_r))}. \tag{12.3}$$

In Equation 12.3 each term in the sum on the right-hand side has the same value, and there are $\#(Orb(y_r))$ terms in this sum. We therefore deduce from Equation 12.3 that

$$\sum_{x\in Orb(y_r)}\#(Stab(x))=\ \#(Orb(y_r))\times\frac{\#(G)}{\#(Orb(y_r))}=\ \#(G).$$

Therefore, as $X=\bigcup_{r=1}^{k}Orb(y_r)$, where for $1 \le r < s \le k$ the sets $Orb(y_r)$ and $Orb(y_s)$ are disjoint,

$$\sum_{x\in X}\#(Stab(x))=\sum_{r=1}^{k}\left(\sum_{x\in Orb(y_r)}\#(Stab(x))\right)=\sum_{r=1}^{k}\#(G)=k\#(G).$$

It follows that

$$k=\frac{1}{\#(G)}\sum_{x\in X}\#(Stab(x)).$$

This completes the proof.

TABLE 12.2

x	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16
$\#(Stab(x))$	8	2	2	2	2	2	2	2	2	4	4	2	2	2	2	8

Is the formula given by this theorem useful? It is easy to use it in our standard example of the group $S(\square)$ acting of the set of colorings of a 2×2 chessboard. From Table 12.1, we obtain Table 12.2 of values of $\#(Stab(x))$.
We thus see that in this case $\sum_{x \in X} \#(Stab(x)) = 48$, and hence, by the orbit-counting theorem, there are $\frac{1}{8} \times 48 = 6$ different orbits, which agrees with the value we have already found.

The calculation in this example is deceptively simple. We were able to use the orbit-counting theorem because we could easily list the 16 elements of X and work out the number of elements in their stabilizers. However, in the case we are really interested in, that of 8×8 chessboards, this method is completely impractical. There are 2^{64} colorings of an 8×8 chessboard using two colors, and there is no practical way we could list them all. If we could fit 50 colorings to a page, then we would need just over 10^{15} volumes with 360 pages each to list them all. However, although as we move from 2×2 chessboards to 8×8 chessboards the number of colorings becomes very large, the group of symmetries, $S(\square)$, remains the same and still has just eight elements. In the next chapter we show how this can be exploited.

Exercises

Note: In these exercises we show how the theory of group actions can be used to derive some combinatorial theorems about groups. They are not relevant for the rest of this book. We give only two applications. You will need to consult a book about groups for more.

12.4.1A We say that two elements, x, y, of a group, $(G, \bullet)$, *commute* if $x \bullet y = y \bullet x$, and that a group is a *commutative* group if all pairs of its elements commute. The *center* of a group, written $Z(G)$, is defined to be the set of all those elements of the group that commute with every element of the group. That is, $Z(G) = \{g \in G$: for all $x \in G$, $gx = xg\}$. Clearly, for every group G, we have $e_G \in Z(G)$. The example of the group of symmetries of an equilateral triangle (as given by Table 11.3) shows that it is possible to have $Z(G) = \{e\}$. The purpose of this exercise is to show that if $\#(G)$ is the power of a prime number, p, there are at least p elements in $Z(G)$.

a. Prove that $Z(G)$ is a subgroup of G.
b. Prove that $g \in Z(G) \Leftrightarrow$ the conjugacy class of g is $\{g\}$, that is, g is conjugate just to itself.
c. Prove that, if for some prime number p and some positive integer n, $\#(G) = p^n$, then $\#(Z(G)) \geq p$. (*Hint:* Make use of the remark after Corollary 12.5 that the number of elements in a conjugacy class divides the order of the group.)

12.4.1B We have noted in exercise 11.3.2B that the converse of Lagrange's theorem is not, in general, true. That is, if k divides the order of a group, there need not be an element of the group of order k (nor even a subgroup of order k). However, this converse is true when k is a prime number. In this exercise

you are asked to prove this result, which is due to the French mathematician Cauchy.*

We start with a group G and suppose that p is a prime number that is a divisor of $\#(G)$. We let X be the set of all ordered p-tuples of elements of G whose product is the identity element, e, of G. Thus

$$X = \{(g_1, g_2, \ldots, g_p): g_1, g_2, \ldots, g_p \in G \text{ and } g_1 g_2 \ldots g_p = e\}.$$

Recall that Z_p is the group of the integers $\{0,1,\ldots, p-1\}$ with addition modulo p. We define an action of this group on X by

$$k \triangleright (g_1, g_2, \ldots, g_p) = (g_{k+1}, g_{k+2}, \ldots, g_{k+p}), \tag{12.4}$$

where the addition in the suffices is carried out modulo p.

i. Given that $\#(G) = n$, how many elements are there in X?
ii. Prove that Equation 12.4 defines an action that satisfies the group action conditions.
iii. Prove that

$$k \triangleright (g_1, \ldots, g_p) = (g_1, \ldots, g_p), \text{ for all } k \in Z_p \Leftrightarrow g_1 = g_2 = \ldots = g_p.$$

It follows from (iii) that the only orbits containing just one element comprise those elements of X of the form $(g, g, \ldots, g)$. Such a p-tuple is in X, if and only if $g^p = 1$, and hence either $g = e$, or g is an element of order p. Thus to prove that G contains at least one element of order p you need only show that:

iv. There is more than one orbit that consists of a single element of X.

* Augustine-Louis Cauchy was born in Paris on August 21, 1789, and died at Sceaux, near Paris, on May 23, 1857. He was an extremely distinguished and prolific mathematician who made important contributions to both pure and applied mathematics. He is best remembered as the originator, along with Gauss, of complex analysis where many of the standard results, for example, the Cauchy–Riemann equations and Cauchy's residue theorem, bear his name.