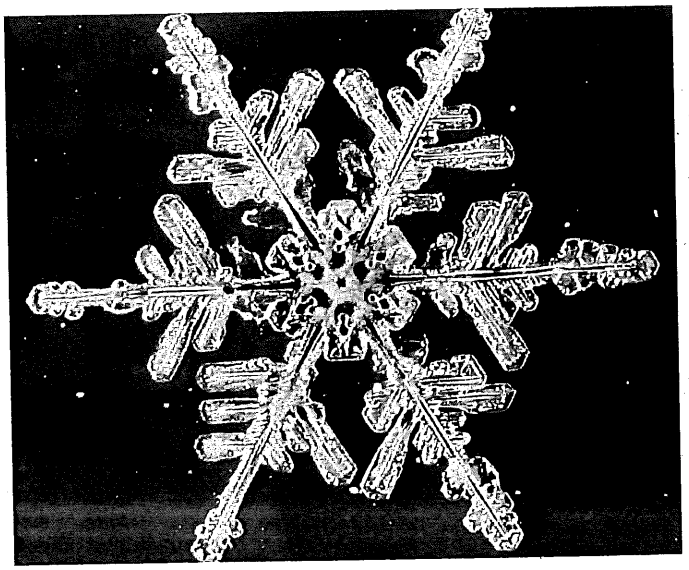
Symmetry Groups

The mathematical study of symmetry is carried out by looking at *transformations* of objects. To the mathematician, a transformation is a special kind of function. Examples of transformations are rotations, translations, reflections, stretchings, or shrinkings of an object. A *symmetry* of some figure is a transformation that leaves the figure invariant, in the sense that, taken as a whole, it looks the same after the transformation as it did before, although individual points of the figure may be moved by the transformation.

An obvious example of a symmetrical figure is the circle. The transformations that leave the circle invariant are rotations about the center (through any angle, in either direction), reflections in any diameter, or any finite combination of rotations and reflections. Of course, a point marked on the circumference may well end up at a different location: a *marked* circle may possess symmetry neither for rotation nor for reflection. But the circle itself, ignoring any marks, does have such symmetry.



The sixfold symmetry of the snowflake. If you rotate a snowflake by any multiple of 60° (one sixth of a complete rotation), it always will look the same.

Given any figure, the *symmetry group* of that figure is the collection of all transformations that leave that figure invariant. A transformation in the symmetry group leaves the figure looking exactly the same, in shape, position, and orientation, as it did before.

The symmetry group of the circle consists of all possible combinations of rotations about the center (through any angle, in either direction) and reflections in any diameter. Invariance of the circle under rotations about the center is referred to as rotational symmetry; invariance with respect to reflection in a diameter is called reflectional symmetry. Both kinds of symmetry are recognizable by sight.

If S and T are any two transformations in the circle's symmetry group, then the result of applying first S and then T is also a member of the symmetry group—since both S and T leave the circle invariant, so does the combined application of both transformations. It is common to denote this double transformation by $T \circ S$. (There is a good reason for the rather perverse looking order here, having to do with an abstract pattern that connects groups and functions, but I shall not go into that connection here.)

This method of combining two transformations to give a third is reminiscent of addition and multiplication, which combine any pair of integers to give a third. To the mathematician, ever on the lookout for patterns and structure, it is natural to see what kind of properties are exhibited by this operation of combining two transformations in the circle's symmetry group to give a third.

First, the operation is associative: if S, T, W are transformations in the symmetry group, then

$$(S \circ T) \circ W = S \circ (T \circ W).$$

In this respect, this new operation is very much like addition and multiplication of integers.

Second, the combination operation has an identity element that leaves unchanged any transformation it is combined with: the 'null rotation', the rotation through angle 0. The null rotation, call it I,

can be applied along with any other transformation T, to yield

$$T \circ I = I \circ T = T.$$

The rotation I obviously plays the same role here as the integer 0 does in addition and the integer 1 in multiplication.

Third, every transformation has an inverse: if T is any transformation, there is another transformation S such that

$$T \circ S = S \circ T = I.$$

The inverse of a rotation is a rotation through the same angle in the opposite direction. The inverse of any reflection is that very same reflection. To obtain the inverse for any finite combination of rotations and reflections, you take the combination of backward rotations and re-reflections that exactly undoes its effect: start with the last one, undo it, then undo the previous one, then its predecessor, and so on.

The existence of inverses is a property shared with addition for integers: for every integer m there is an integer n such that

$$m + n = n + m = 0 \text{ (the identity for addition)},$$

namely $n = -m$. The same is not true for multiplication of integers, of course: it is not the case that for every integer m there is an integer n such that

$$m \times n = n \times m = 1 \text{ (the identity for multiplication)}.$$

In fact, only for the integers $m = 1$ and $m = -1$ is there another integer n that satisfies the above equation.

To summarize, any two symmetry transformations of a circle can be combined by the combination operation to give a third symmetry transformation, and this operation has the three 'arithmetic' properties associativity, identity, and inverses.

A similar analysis can be carried out for other symmetrical figures. In fact, the properties of symmetry transformations we have just observed in the case of the circle turn out to be sufficiently common in mathematics to be given a name—indeed, I have already used that name in referring to the 'symmetry *group*'. In general, whenever mathematicians have some set, G, of entities and an operation $*$ that combines any two elements x and y in G to give a further element $x * y$ in G, they call this collection a group if the following three conditions are met:

G1. for all x, y, z in G,
$(x * y) * z = x * (y * z)$;

G2. there is an element e in G such that
$x * e = e * x = x$, for all x in G;

G3. for each element x in G there is an element y in G such that $x * y = y * x = e$, where e is as in condition G2.

Thus, the collection of all symmetry transformations of a circle is a group. In fact, you should have no difficulty in convincing yourself that if G is the collection of all symmetry transformations of *any* figure, and $*$ is the operation of combining two symmetry transformations, then the result is a group.

From the remarks made earlier, it should also be clear that if G is the set of integers and the operation $*$ is addition, then the resulting structure is a group. The same is not true for the integers and multiplication, however. But if G is the set of all rational numbers *apart from zero,* and $*$ is multiplication, then the result is a group.

A different example of a group is provided by the finite arithmetics discussed in Chapter 1. The integers $0, 1, \ldots, n-1$ with the operation of addition modulo n is a group for any integer n. And if n is a prime number, then the integers $1, 2, \ldots, n-1$ constitute a group under the operation of multiplication modulo n.

In fact, the three kinds of examples just described barely scratch the surface. The group concept turns out to be ubiquitous in modern mathe-

element of your group has a single inverse. In fact, you will know that your newly discovered structure possesses every property that can be established—in abstract form—on the basis of the group axioms alone.

The more examples there are of a given abstract structure, such as a group, the more widespread the applications of any theorems proved about that abstract structure. The cost of this greatly increased efficiency is that one has to learn to work with highly abstract structures, with abstract patterns of abstract entities. In group theory, it does not matter, for the most part, *what* the elements of a group are, or *what* the group operation is. Their nature plays no role. The elements could be numbers, transformations, or other kinds of entities, and the operation could be addition, multiplication, composition of transformations, or whatever. All that matters is that the objects together with the operation satisfy the group axioms G1, G2, and G3.

One final remark concerning the group axioms is in order. In both G2 and G3, the combinations were written two ways. Anyone familiar with the commutative laws of arithmetic might well ask why the axioms were written this way. Why don't mathematician simply write them one way, say

$$x * e = x$$

in G2 and

$$x * y = e$$

in G3, and add one further axiom, the commutative law:

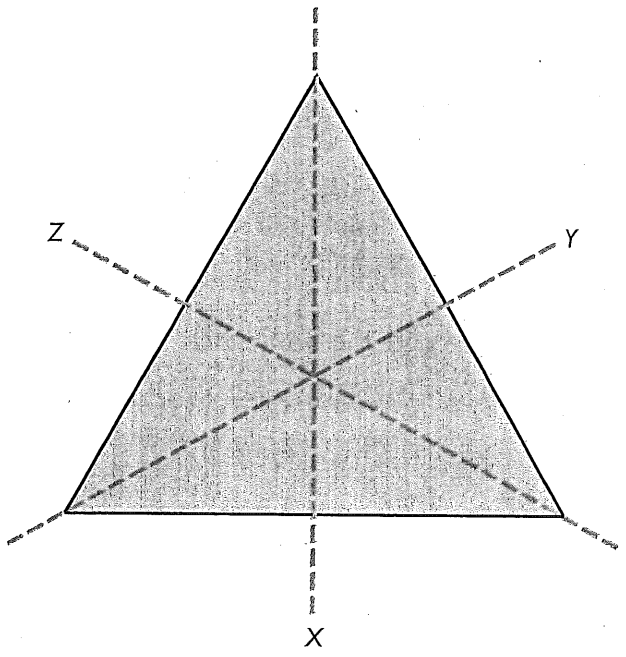
G4. for all x, y in G, $x * y = y * x$.

The answer is that this additional requirement would exclude many of the examples of groups that mathematicians wish to consider.

Though many other symmetry groups do not satisfy the commutativity condition G4, a great many other kinds of groups do. Consequently, groups that satisfy the additional condition G4 are given a special name: they are called abelian groups, after the Norwegian mathematician Niels Henrik Abel. The study of abelian groups constitutes an important subfield of group theory.

For a further example of a symmetry group, consider the equilateral triangle shown on this page. This figure has precisely six symmetries. There is the identity transformation, I, counterclockwise rotations v and w through 120° and 240°, and reflections x, y, z in the lines X, Y, Z, respectively. (The lines X, Y, Z stay fixed as the triangle moves.) There is no need to list any clockwise rotations, since a clockwise rotation of 120° is equivalent to a counterclockwise rotation of 240° and a clockwise rotation of 240° has the same effect as a counterclockwise rotation of 120°.

There is also no need to include any combinations of these six transformations, since the result of any such combination is equivalent to one of the six given. The table on the next page gives the basic



The symmetries of an equilateral triangle.

matics, both pure and applied. Indeed, the notion of a group was first formulated, in the early nineteenth century, not in connection with arithmetic or with symmetry transformations, but as part of an investigation of polynomial equations in algebra. The key ideas may be found in the work of Evariste Galois, described later in this chapter.

The symmetry group of a figure is a mathematical structure that in some sense captures the degree of visual symmetry of that figure. In the case of a circle, the symmetry group is infinite, since there are infinitely many possible angles through which a circle may be rotated and infinitely many possible diameters in which it may be reflected. It is the richness of the circle's group of symmetry transformations that corresponds to the high degree of visual symmetry—the 'perfect symmetry'—that we observe when we look at a circle.

At the other end of the spectrum, a figure that is completely unsymmetric will have a symmetry group that consists only of a single transformation, the identity (or 'do nothing') transformation. It is easy to check that this special case does satisfy the requirements of a group, as does the single integer 0 with the operation of addition.

Before looking at a further example of a group, it is worth spending a few moments reflecting on the three conditions G1, G2, and G3 that determine whether a given collection of entities and an operation constitute a group or not.

The first condition, G1, the associativity condition, is already very familiar to us in the case of the arithmetic operations of addition and multiplication (though not subtraction or division).

Condition G2 asserts the existence of an identity element. Such an element has to be unique. For if e and i both have the property expressed by G2, then, applying this property twice in succession, you would have

$$e = e * i = i,$$

so e and i are in fact one and the same.

This last observation means that there is only one element e that can figure in condition G3. Moreover, for any given element x in G, there is only one element y in G that satisfies the requirement imposed by G3. This is also quite easy to demonstrate. Suppose y and z are both related to x as in G3. That is, suppose that:

$$(1) \qquad x * y = y * x = e,$$

$$(2) \qquad x * z = z * x = e.$$

Then:

$$\begin{aligned} y &= y * e && \text{(by the property of } e\text{)} \\ &= y * (x * z) && \text{(by equation (2))} \\ &= (y * x) * z && \text{(by G1)} \\ &= e * z && \text{(by equation (1))} \\ &= z && \text{(by the property of } e\text{)}, \end{aligned}$$

so in fact y and z are one and the same. Since there is precisely one y in G related to a given x as in G3, that y may be given a name: it is called the (group) inverse of x, and is often denoted by x^{-1}. And with that, I have just proved a theorem in the mathematical subject known as group theory: the theorem that says that, in any group, every element has a unique inverse. I proved that uniqueness by deducing it logically from the group axioms, the three initial conditions G1, G2, G3.

Though this particular theorem is an extremely simple one, both to state and to prove, it does illustrate the enormous power of abstraction in mathematics. There are many, many examples of groups in mathematics; in writing down the group axioms, mathematicians are capturing a highly abstract pattern that arises in many instances. Having proved, *using only the group axioms,* that group inverses are unique, this fact will apply to every single example of a group. No further work is required. If tomorrow you come across a quite new kind of mathematical structure, and you determine that what you have is a group, you will know at once that every

The Triangle Symmetry Group

$\circ$	I	v	w	x	y	z
I	I	v	w	x	y	z
v	v	w	I	z	x	y
w	w	I	v	y	z	x
x	x	y	z	I	v	w
y	y	z	x	w	I	v
z	z	x	y	v	w	I

transformation that results from applying any two basic transformations. To read off the value of the combination $x \circ v$ from the table, look along the row labeled x and locate the entry in the column labeled v, namely y. Thus,

$$x \circ v = y$$

in this group. Again, the result of applying first w and then x, namely the group element $x \circ w$, is z, and the result of applying v twice in succession, namely $v \circ v$, is w. The group table also shows that v and w are mutual inverses and x, y, z are each self-inverse.

Since the combination of any two of the given six transformations is another such transformation, it follows that the same is true for any finite combination. You simply apply the pairing rule successively. For example, the combination $(w \circ x) \circ y$ is equivalent to $y \circ y$, which in turn is equivalent to I.

Evariste Galois

It is to a brilliant young Frenchman by the name of Evariste Galois that the world owes its gratitude for the introduction of the group concept. Killed in a duel on 30 May, 1832, at the age of 21, Galois himself never lived to see the mathematical revolution ushered in by his work. In fact, an entire decade was to go by before the true magnitude of his accomplishment was recognized.

Galois was led to formulate the notion of a group by his attempt to solve a specific problem: that of finding simple, algebraic formulas for the solution of polynomial equations. Every high-school student is familiar with the formula for the solution of a quadratic equation. The roots of the quadratic equation

$$ax^2 + bx + c = 0$$

are given by the formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Evariste Galois (1811–1832).