Group Theory

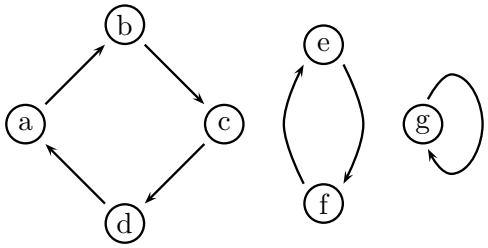
Group theory is the mathematical study of symmetry. This statement will be clarified somewhat shortly, but first we need a brief discussion of permutations.

Permutations

Definition. A *permutation* of a set of objects is a rule which assigns to each of the objects a unique successor, which is also an object in the set, in such a way that no two distinct objects have the same successor and every object in the set is the successor of some object in the set.

When discussing a particular permutation, we usually say "a goes to b" to indicate that b is the successor of a. When a goes to b we can also call a the predecessor of b. The definition implies that every object must have a unique predecessor as well as a unique successor.

Here is a representation of a permutation as a directed graph, where each arrow points from an object to its successor. Note that an object is allowed to be its own successor.



Suppose that we have a permutation of some finite set of objects. Choose one of them as a starting point, then move to its successor, then to the successor of that, and so on. Thus we obtain a sequence $(a_1, a_2, a_3, \dots)$, where a_1 is our starting point and a_{i+1} is the successor of a_i (for all $i \geq 1$). Since we have only a finite number of objects, at some stage we must encounter an object that we have encountered before. Choose the smallest value of k such that a_{k+1} is the same as a term that has already appeared in the sequence. Thus a_1, a_2, …, a_k are distinct from each other, and a_{k+1} is equal to to one of a_1, a_2, …, a_k. But if a_{k+1} were equal to a_2, say, then the predecessor of a_{k+1} would have to be the predecessor of a_2, which is impossible since a_k is not equal to a_1. In fact, a_{k+1} must be a_1, since if $2 \leq i \leq k$ then the predecessor of a_i is $a_{i-1} \neq a_k$. Thus we see that a_1, a_2, …, a_k form *k-cycle*; passing from object to successor leads us, in k steps, back to where we started.

The above reasoning shows that, in any given permutation, every object lies in a cycle of some length. The different cycles that make up a permutation clearly must be disjoint from one another. The permutation depicted in the diagram above is made up of a 4-cycle, a 2-cycle and a 1-cycle.

Notationally, we represent k-cycles as k-tuples $(a_1, a_2, \dots, a_k)$, where a_i goes to a_{i+1} for $1 \leq i \leq k-1$, and a_k goes to a_1. Thus, for example, $(2, 4, 1, 3)$ means 2 goes to 4, 4 goes to 1, 1 goes to 3 and 3 goes to 2. Note that $(4, 1, 3, 2)$ is exactly the same cycle: a cycle does not have any special starting point. So there are k different k-tuples that all represent the same k-cycle: $(2, 4, 1, 3) = (4, 1, 3, 2) = (1, 3, 2, 4) = (3, 2, 4, 1)$.

Our preferred notation for permutations is to write them as products of their disjoint cycles. Thus our example permutation above is written as (a,b,c,d)(e,f)(g).

A 2-cycle is sometimes called a *transposition*.

A 1-cycle is sometimes called a *fixed point* of a permutation.

In most of the examples of permutations that we shall consider from now on, the set of objects involved will be the set of integers from 1 to n, for some n. The set of all permutations of $\{1, 2, \ldots, n\}$ is denoted by $\mathrm{Sym}(n)$. Thus if $\sigma = (1, 5, 2, 7)(4)(3, 8)(6)$, a permutation of $\{1, 2, 3, 4, 5, 6, 7, 8\}$, then σ is an element of the set $\mathrm{Sym}(8)$.

The permutation σ just considered is made up of a 4-cycle, a 2-cycle and two 1-cycles. It is common practice when writing down permutations to omit the fixed points (1-cycles), it being understood that any element of the set that is not explicitly written down is a fixed point. Thus σ above could be written as $(1, 5, 2, 7)(3, 8)$ (or as $(2, 7, 1, 5)(3, 8)$, or $(8, 3)(7, 1, 5, 2)$, or thirteen other ways that do not mention 4 or 6). However, the 1-cycles still exist, even if they are not written down, and it is often a good idea not to leave them out, so that there can be no possible confusion.

Omitting fixed points creates a minor notational problem relating to the permutation all of whose cycles have length 1: if they are all omitted then there is no notation left! So we introduce the special notation id for the permutation of $\{1, 2, \ldots, n\}$ that fixes everything. (The value of n will always be clear from the context.) This permutation is called the *identity*.

Given a permutation $\sigma \in \mathrm{Sym}(n)$, for each $i \in \{1, 2, \ldots, n\}$ we let i^σ denote the successor of i. We say that σ takes i to i^σ (or i goes to i^σ under the action of σ).

An alternative notation for permutations that is sometimes used consists of writing the numbers from 1 to n in a row and, in a second row, writing i^σ below i (for each i). In this notation, the permutation $(1, 5, 2, 7)(3, 8) \in \mathrm{Sym}(8)$ is written as

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 8 & 4 & 2 & 6 & 1 & 3 \end{pmatrix}.$$

Because this notation is much longer, we shall not use it; however, it is as well to be aware of it since it is used in many books.

If $\sigma \in \mathrm{Sym}(n)$ then we can define a function $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ by the rule that $i \mapsto i^\sigma$ for all i. The definition of "permutation" as stated above has two components: no two distinct objects can have the same successor, and every object is the successor of some object. That is, $i^\sigma = j^\sigma$ is not possible unless $i = j$, and for every $k \in \{1, 2, \ldots, n\}$ there is an $i \in \{1, 2, \ldots, n\}$ with $k = i^\sigma$. In the standard terminology of mathematics, these two requirements say that the function defined by $i \mapsto i^\sigma$ is one-to-one and onto. (Recall that a function $f\colon A \to B$ is said to be one-to-one, or injective, if the following condition holds: for all a_1, $a_2 \in A$, if $f(a_1) = f(a_2)$ then $a_1 = a_2$. And $f\colon A \to B$ is said to be onto, or surjective, if the following holds: for every $b \in B$ there is an $a \in A$ such that $f(a) = b$.) In the two row notation described above, the fact that no two distinct objects have the same successor means that nothing appears twice in the second row; this says also that the function is one-to-one. The fact that every number is the successor of something means that every number appears somewhere in the second row; this says that the function is onto. Thus, if the two row notation is used, all the permutations of $\{1, 2, \ldots, n\}$ are obtained by arranging the numbers from 1 to n in all possible orders in the second row.

The above discussion shows that, effectively, a permutation of $\{1, 2, \ldots, n\}$ is the same as a function $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ that is one-to-one and onto. The only

difference is that we write i^σ instead of $\sigma(i)$ to indicate the effect of applying σ to the number i.

We now describe a method of multiplying permutations.

Definition. If σ and τ are permutations of $\{1, 2, \ldots, n\}$ then the *composite* or *product* $\sigma\tau$ is the permutation defined by the rule that $i^{\sigma\tau} = (i^\sigma)^\tau$ for all $i \in \{1, 2, \ldots, n\}$.

Note that MAGMA uses the notation $\sigma * \tau$ for the product.

To compute the product of two given permutations of $\{1, 2, \ldots, n\}$, choose any number $i_0 \in \{1, 2, \ldots, n\}$, find what i_0 goes to under the action of σ, and then find what that goes to under the action of τ. Call this number i_1. Then i_0 goes to i_1 under the action of $\sigma\tau$. Repeat the process for i_1: find what i_1 goes to under σ and what that goes to under τ. If we call this i_2 then i_1 goes to i_2 under $\sigma\tau$. Repeat again to find what i_2 goes to under $\sigma\tau$, and continue in this way until we get back to i_0, so that a complete cycle has been found. Choose any number that does not appear in this cycle and repeat the process to find another cycle. Continue in this way until there are no numbers left.

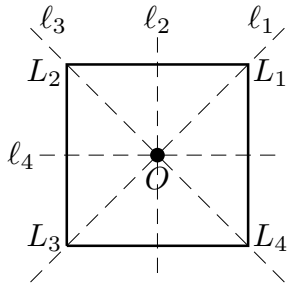
Example. Let $\sigma = (5, 2, 1, 7)(3, 8)$ and $\tau = (5, 1, 7, 3)(8, 6, 2, 4)$, elements of Sym(8). We calculate $\sigma\tau$. Since 1 goes to 7 under σ, and 7 to 3 under τ, we have 1 goes to 3 under $\sigma\tau$. So we can write $(1, 3$ as part of a cycle of $\sigma\tau$. Now 3 goes to 8 under σ, and 8 to 6 under τ; so 3 goes to 6 under $\sigma\tau$, and our partial cycle is now $(1, 3, 6$. Here is the complete calculation:

$$
\begin{array}{ll}
1 \overset{\sigma}{\mapsto} 7 \overset{\tau}{\mapsto} 3 & (1, 3 \\
3 \overset{\sigma}{\mapsto} 8 \overset{\tau}{\mapsto} 6 & (1, 3, 6 \\
6 \overset{\sigma}{\mapsto} 6 \overset{\tau}{\mapsto} 2 & (1, 3, 6, 2 \\
2 \overset{\sigma}{\mapsto} 1 \overset{\tau}{\mapsto} 7 & (1, 3, 6, 2, 7 \\
7 \overset{\sigma}{\mapsto} 5 \overset{\tau}{\mapsto} 1 & (1, 3, 6, 2, 7) \\
4 \overset{\sigma}{\mapsto} 4 \overset{\tau}{\mapsto} 8 & (1, 3, 6, 2, 7)(4, 8 \\
8 \overset{\sigma}{\mapsto} 3 \overset{\tau}{\mapsto} 5 & (1, 3, 6, 2, 7)(4, 8, 5 \\
5 \overset{\sigma}{\mapsto} 2 \overset{\tau}{\mapsto} 4 & (1, 3, 6, 2, 7)(4, 8, 5).
\end{array}
$$

Symmetry

A *symmetry* of an object is a transformation of the object that preserves its structure. Of course this is not a rigorous definition, since we have not said what it means to "preserve the structure" of something. Indeed, its meaning depends on the context. We start with two examples.

Consider a square in the Euclidean plane. We imagine detaching the square from the plane, turning it over or round somehow, and then reinserting it so that it occupies again the space from which it was removed. Let L_1, L_2, L_3 and L_4 be the points in the plane at which the corners of the square are placed. These points are not part of the square, but stay fixed when the square is removed and reinserted. Each possible removal and reinsertion of the square can be called a symmetry of the square. There are eight symmetries altogether: reflections in the lines ℓ_1, ℓ_2, ℓ_3 and ℓ_4 in the diagram, and anticlockwise rotations about O through $0°$, $90°$, $180°$ and $270°$.



The symmetries can be conveniently represented by permutations of $\{1, 2, 3, 4\}$. For example, the anticlockwise rotation through 90° moves one vertex of the square from L_1 to L_2, another from L_2 to L_3, a third from L_3 to L_4, and the remaining one from L_4 to L_1. So it is naturally represented by $(1, 2, 3, 4)$. The complete corresponce between symmetries of the square and permutations is as follows.

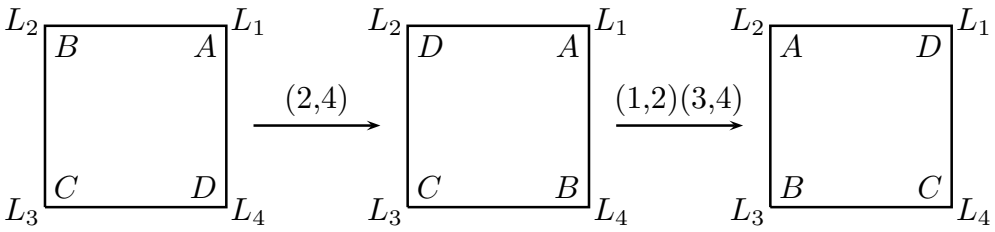
rotation through 0°	$\longleftrightarrow$	id
rotation through 90°	$\longleftrightarrow$	$(1, 2, 3, 4)$
rotation through 180°	$\longleftrightarrow$	$(1, 3)(2, 4)$
rotation through 270°	$\longleftrightarrow$	$(1, 4, 3, 2)$
reflection in ℓ_1	$\longleftrightarrow$	$(2, 4)$
reflection in ℓ_2	$\longleftrightarrow$	$(1, 2)(3, 4)$
reflection in ℓ_3	$\longleftrightarrow$	$(1, 3)$
reflection in ℓ_4	$\longleftrightarrow$	$(1, 4)(2, 3)$

Symmetries have two key properties:

(1) the composite effect of one symmetry followed by another is also a symmetry;

(2) for each symmetry there is an inverse symmetry, the composite effect of a symmetry followed by its inverse being the transformation that leaves everything fixed.

Our correspondence between symmetries of the square and permutations of $\{1, 2, 3, 4\}$ has been carefully arranged so that composition of symmetries agrees with multiplication of permutations. To illustrate this, consider the composite of the reflection in ℓ_1 followed by the reflection in ℓ_2, and the product of the corresponding permutations ($(2, 4)$ and $(1, 2)(3, 4)$ respectively). To keep track of what happens when composing the symmetries, we label the corners of the square A, B, C and D. The following diagram shows what happens.



The composite of the two given reflections is seen to be the anticlockwise rotation through 90°, corresponding to the permutation $(1, 2, 3, 4)$. It is left to the reader to check that $(2, 4)((1, 2)(3, 4)) = (1, 2, 3, 4)$.

Symmetry is perhaps most easily recognizable in geometrical situations like the one we have been considering above. But symmetry also exists in abstract contexts. We give an algebraic example.

Consider polynomial functions of four variables x_1, x_2, x_3 and x_4. For each such function f and each permutation $\sigma \in \mathrm{Sym}(4)$, let f^σ be the polynomial function defined by the following rule:

$$f^\sigma(x_1, x_2, x_3, x_4) = f(x_{1^\sigma}, x_{2^\sigma}, x_{3^\sigma}, x_{4^\sigma}).$$

That is to say, f^σ is obtained from f by replacing x_i by x_{i^σ} for each value of i. For example, suppose that f, g and h are given by

$$\begin{aligned} f(x_1, x_2, x_3, x_4) &= x_1 + x_2^2 - x_3 - x_4^2, \\ g(x_1, x_2, x_3, x_4) &= x_1 + x_4^2 - x_3 - x_2^2, \\ h(x_1, x_2, x_3, x_4) &= x_2 + x_3^2 - x_4 - x_1^2. \end{aligned}$$

Then $g = f^{(2,4)}$, since the expression for g is obtained from the expression for f by interchanging x_2 and x_4. Similarly, $h = g^{(1,2)(3,4)}$, since h is obtained from g by swapping x_1 with x_2 and x_3 with x_4. Again we have chosen things carefully so that if we first apply a permutation σ and then apply a permutation τ, the net effect is the same as applying the product $\sigma\tau$. In the above example, h is obtained from f by first applying $(2,4)$ (giving g) and then applying $(1,2)(3,4)$. Now $(2,4)((1,2)(3,4)) = (1,2,3,4)$, and we also observe that $h = f^{(1,2,3,4)}$, since f is transformed into h by replacing x_1 by x_2, x_2 by x_3, x_3 by x_4 and x_4 by x_1.

To prove this result generally, let f be any polynomial in x_1, x_2, x_3 and x_4, and let σ and τ be any permutations in $\mathrm{Sym}(4)$. For convenience, let us write $g = f^\sigma$. Then $(f^\sigma)^\tau = g^\tau$, and, by definition,

$$g^\tau(x_1, x_2, x_3, x_4) = g(x_{1^\tau}, x_{2^\tau}, x_{3^\tau}, x_{4^\tau}). \tag{1}$$

Furthermore, the definition also gives

$$g(x_1, x_2, x_3, x_4) = f(x_{1^\sigma}, x_{2^\sigma}, x_{3^\sigma}, x_{4^\sigma}).$$

This equation holds for all values of the variables; so we can put $x_i = y_i$ for each i, and deduce that

$$g(y_1, y_2, y_3, y_4) = f(y_{1^\sigma}, y_{2^\sigma}, y_{3^\sigma}, y_{4^\sigma}). \tag{2}$$

Now put $y_j = x_{j^\tau}$ for each j, and observe that this gives $y_{i^\sigma} = x_{(i^\sigma)^\tau} = x_{i^{\sigma\tau}}$ for each i. (Recall that permutation multiplication is defined by the rule that $i^{\sigma\tau} = (i^\sigma)^\tau$ for all i.) Thus Eq. (2) becomes

$$g(x_{1^\tau}, x_{2^\tau}, x_{3^\tau}, x_{4^\tau}) = f(x_{1^{\sigma\tau}}, x_{2^{\sigma\tau}}, x_{3^{\sigma\tau}}, x_{4^{\sigma\tau}}),$$

and combining this with Eq. (1) gives

$$(f^\sigma)^\tau(x_1, x_2, x_3, x_4) = f(x_{1^{\sigma\tau}}, x_{2^{\sigma\tau}}, x_{3^{\sigma\tau}}, x_{4^{\sigma\tau}}).$$

Since the right hand side of this equals $f^{\sigma\tau}(x_1, x_2, x_3, x_4)$, we conclude that $(f^\sigma)^\tau = f^{\sigma\tau}$, which is the result we wanted.

The above calculations have succeeded in making an easy idea appear hard. All we have said is that first replacing each x_i by x_{i^σ} and then replacing each x_j by x_{j^τ}, means that overall x_i is replaced by $x_{(i^\sigma)^\tau}$. It is reasonably clear.

Coming at last to an example of symmetry in this context, define

$$f(x_1, x_2, x_3, x_4) = x_1x_3 + x_2x_4,$$

and consider those permutations σ such that $f^\sigma = f$. These are called the permutations that *preserve* f; they can also be called the symmetries of the algebraic expression $x_1x_3 + x_2x_4$. The 4-cycle $(1, 2, 3, 4)$ is one such symmetry, since replacing x_1 by x_2, x_2 by x_3, x_3 by x_4 and x_4 by x_1 transforms $x_1x_3 + x_2x_4$ into $x_2x_4 + x_3x_1$, which is equal to $x_1x_3 + x_2x_4$. Similarly, interchanging x_1 with x_4 and x_2 with x_3 transforms $x_1x_3 + x_2x_4$ into $x_4x_2 + x_3x_1 = x_1x_3 + x_2x_4$. So $(1, 4)(2, 3)$ is another a symmetry of the expression. Clearly the transpositions $(1, 3)$ and $(2, 4)$ are also symmetries, as are $(1, 3)(2, 4)$, $(1, 2)(3, 4)$ and $(1, 4, 3, 2)$. And, of course, the identity transformation—the transformation that does nothing—is a symmetry. The permutations that correspond to symmetries of the algebraic expression $x_1x_3 + x_2x_4$ are thus the same as those that correspond to symmetries of the square. So in some sense the square and $x_1x_3 + x_2x_4$ have the same symmetries.

Binary operations

Definition. A *binary operation* on a set S is a function of two variables from S to itself.

In other words, a binary operation on S is a rule which accepts as input any ordered pair of elements of S and returns an element of S as output. Here are some examples.

- Addition is a binary operation on $\mathbb{R}$, the set of all real numbers. The input can be any pair (a, b), where a, $b \in \mathbb{R}$, and the output is $a + b$.
- Multiplication, $(a, b) \mapsto ab$, is another operation on $\mathbb{R}$.
- Matrix multiplication gives an operation on the set of all 2×2 matrices with integer entries.
- Permutation multiplication is an operation on $\mathrm{Sym}(n)$.
- Composition of symmetries is an operation on the set of all symmetries of an object.

We are now able to give the definition of the key concept of this section of the course.

Definition. A *group* is a set G equipped with a binary operation, $(a, b) \mapsto ab$, such that the following properties are satisfied:

G1) $(xy)z = x(yz)$, for all x, y, $z \in G$;

G2) there exists an element $e \in G$ such that

(a) $ex = x = xe$ for all $x \in G$, and

(b) for all $x \in G$ there exists a $y \in G$ such that $xy = e = yx$.

In the above definition we chose, for convenience, to write the operation as $(a, b) \mapsto ab$. However, it is not compulsory to use this notation. Indeed, we shall frequently encounter examples in which it is more natural to use additive notation, writing the operation as $(a, b) \mapsto a + b$. For example, the set of all real numbers forms a group under addition.

Before looking at examples of groups, there are some general observations we wish to make about binary operations. If a set is not too large, then a binary operation on the set

can be conveniently displayed by means of a "multiplication table". This is a table with rows and columns indexed by elements of the set, and the entry in the row indexed by a and the column indexed by b is the result of applying the operation to the pair (a, b). For example, consider Sym(3) and the operation of permutation multiplication. The reader can check the correctness of the following table.

	id	$(1,2,3)$	$(1,3,2)$	$(1,2)$	$(1,3)$	$(2,3)$
id	id	$(1,2,3)$	$(1,3,2)$	$(1,2)$	$(1,3)$	$(2,3)$
$(1,2,3)$	$(1,2,3)$	$(1,3,2)$	id	$(2,3)$	$(1,2)$	$(1,3)$
$(1,3,2)$	$(1,3,2)$	id	$(1,2,3)$	$(1,3)$	$(2,3)$	$(1,2)$
$(1,2)$	$(1,2)$	$(1,3)$	$(2,3)$	id	$(1,2,3)$	$(1,3,2)$
$(1,3)$	$(1,3)$	$(2,3)$	$(1,2)$	$(1,3,2)$	id	$(1,2,3)$
$(2,3)$	$(2,3)$	$(1,2)$	$(1,3)$	$(1,2,3)$	$(1,3,2)$	id

Definition. Let $*$ be an operation on a set S. An element $e \in S$ is said to be a *left identity element* for the operation $*$ if $e * x = x$ for all $x \in S$. An element $f \in S$ is said to be a *right identity element* for the operation $*$ if $x * e = x$ for all $x \in S$. An element that is both a left identity and a right identity is called an *identity element* for the operation $*$.

Observe that Part (a) of (G2) in the definition of a group says that the element e is an identity element for the group operation.

The following proposition is easy to prove, but nonetheless important.

Proposition. *If an operation $*$ on a set S has both a left identity element and a right identity element, then these elements coincide.*

Proof. Let e be a left identity and f a right identity. Then we have

$$e * x = x \qquad \text{for all } x \in S, \tag{3}$$
$$y * f = y \qquad \text{for all } y \in S. \tag{4}$$

Putting $x = f$ in Eq. (3) gives $e * f = f$, and putting $y = e$ in Eq. (4) gives $e * f = e$. Hence $e = f$, as required. □

In particular, this proposition tells us that an operation cannot have two distinct identity elements: if e and f are both identities, then, in particular, e is a left identity and f a right identity, whence $e = f$ by the proposition. Part (a) of (G2) tells us that a group has one identity element; we now know that it has only one.

Definition. Suppose that $*$ is an operation on the set S, and that $e \in S$ is an identity element for $*$. If x is an element of S then an element $y \in S$ is called a *left inverse* of x if $y * x = e$. Similarly, y is called a *right inverse* of x if $x * y = e$. And y is called an *inverse* of x if it is both a left inverse and a right inverse.

Definition. An operation $*$ on a set S is said to be *associative* if $(x * y) * z = x * (y * z)$ for all x, y, $z \in S$.

Note that (G1) says that group operations are always associative.

Proposition. *Let $*$ be an associative operation on the set S, and suppose that $e \in S$ is an identity element for $*$. If an element $x \in S$ has both a left inverse x' and a right inverse x'', then $x' = x''$.*

Proof. We have $x' * x = e$ and $x * x'' = e$. So

$$x'' = e * x'' = (x' * x) * x'' = x' * (x * x'') = x' * e = x',$$

the first equation by the fact that e is a left identity, the last by the fact that e is a right identity, and the middle one by the associative law. □

In particular, if $*$ is an associative operation on S then an element $x \in S$ cannot have two distinct inverses. If x' and x'' are both inverses of x, then x' is a left inverse and x'' a right inverse, and by the proposition it follows that $x' = x''$.

Part (b) of (G2) says that every element x in a group G must have an inverse. From what we have just shown it follows that x has exactly one inverse. Combining this with the uniqueness of the identity element, proved above, allows us to state the following result.

Proposition. *Let G be a group. Then G has a unique identity element, and each $x \in G$ has a unique inverse.*

We shall usually denote the identity element of a group by e, or by id. Alternatively, in cases when the operation is written as $+$, the identity will be denoted by 0, and called the *zero element* rather than the identity. The inverse of an element x will be denoted by x^{-1}, except that if the operation is $+$ then the inverse of x will be written as $-x$, and called the negative of x rather than the inverse of x.

Groups

The definition of the concept of a group, combined with the proposition proved above, enables us to give an equivalent formulation of the concept.

A group is a set G equipped with a binary operation that has the following properties.

- *The operation is associative: $x(yz) = x(yz)$ for all x, y, $z \in G$.*
- *There is a unique identity element: $ex = x = xe$ for all $x \in G$;*
- *Each $x \in G$ has a unique inverse: $xx^{-1} = e = x^{-1}x$ for all $x \in G$.*

There are a great many examples of groups. We list a few of them.

1) The set consisting of the two numbers 1 and -1 is a group under multiplication. The identity element is 1, and each element is its own inverse.
2) The set of $\{1, i, -1, -i\}$, a subset of $\mathbb{C}$ (the complex numbers) is a group under multiplication of complex numbers. It is clear that multiplication does define an operation on this set: the product of any pair of these four numbers is also one of the four. The operation is associative, since $\alpha(\beta\gamma) = (\alpha\beta)\gamma$ holds for all α, β, $\gamma \in \mathbb{C}$, and so it certainly holds for all α, β, $\gamma \in \{1, i, -1, -i\}$. The number 1 is an identity element for the operation. The elements i and $-i$ are inverses of each other, while and 1 and -1 are self-inverse.
3) The set of all nonzero real numbers is a group under multiplication. The product of two nonzero real numbers is a nonzero real number; so multiplication is an operation on the set. It is well known that $(ab)c = a(bc)$ for all a, b, $c \in \mathbb{R}$. The identity element is 1, and for each nonzero $a \in \mathbb{R}$ there is a nonzero $b \in \mathbb{R}$, namely $b = 1/a$, such that $ab = 1$.
4) The set of all integers, which we shall denote by $\mathbb{Z}$, is a group under addition. The sum of two integers is an integer; so we have an operation. It is well known that

addition is associative. Since $a + 0 = a = 0 + a$ for all $a \in \mathbb{Z}$, the number 0 is the zero element. And each $a \in \mathbb{Z}$ has a negative, $-a$ (which is in $\mathbb{Z}$), satisfying $a + (-a) = 0 = (-a) + a$.

5) The set $\mathbb{R}^n$, consisting of all n-component column vectors, is a group under the usual operation of addition for column vectors. The zero element is the column whose entries are all zero, and the negative of $\underline{a}$ is $-\underline{a}$, the column whose entries are the negatives of the entries of $\underline{a}$.

6) The set of all $m \times n$ matrices with integer entries is a group under matrix addition. The sum of a pair of such matrices is another; so we have an operation. Associativity of matrix addition is well-known (and follows easily from associativity of addition of numbers). The $m \times n$ matrix Z whose entries are all zero satisfies the requirements of a zero element: $A + Z = A = Z + A$ for all matrices A in the set, and for each A there is a negative, $-A$ (whose entries are the negatives of the entries of A), such that $A + (-A) = Z = (-A) + A$.

7) The set of all 2×2 matrices over $\mathbb{R}$ with nonzero determinant is a group under matrix multiplication. Since $\det(AB) = (\det A)(\det B)$ we see that $\det(AB)$ is nonzero whenever $\det A$ and $\det B$ are both nonzero; so matrix multiplication does yield an operation on the set of matrices with nonzero determinant. We know that matrix multiplication is associative. The usual 2×2 identity matrix is an identity element for matrix multiplication, and we also know that each matrix with nonzero determinant is invertible.

8) The set consisting of the following eight 2×2 matrices (over the complex field) is a group under matrix multiplication:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix},$$
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}.$$

To check that matrix multiplication does define an operation on this set it is necessary to check that the product of any pair of matrices in the list is another matrix in the list. Thus there are 64 products to check, and we shall not go through this. However, the reader who checks just a few of these products will soon be convinced that it is true. Associativity follows from the general fact that matrix multiplication is associative. The identity matrix is in the list; so there is an identity element. And it is not hard to check that the inverse of each matrix in the list is also in the list. For example,

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}^{-1} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix},$$
$$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$

and so on.

9) The eight permutations id, $(1,2,3,4)$, $(1,3)(2,4)$, $(1,4,3,2)$, $(1,3)$, $(1,2)(3,4)$, $(2,4)$ and $(1,4)(2,3)$ form a group under permutation multiplication. This is easiest to see by associating the permutations with symmetries of a square, in the manner we have

described. We have seen that multiplication of permutations and composition of the corresponding symmetries agree with each other, and since composites of symmetries are symmetries it follows that the product of any pair of permutations from the above list must also be a permutation in the list. So permutation multiplication defines an operation on this set. The fact that multiplication of permutations is associative will be proved later. However, in this example associativity is a consequence of the fact—which is not hard to see—that composition of symmetries is associative: if f, g and h are symmetries, then $(fg)h$ means fg followed by h, and since fg means f followed by g we see that $(fg)h$ is f followed by g, followed by h; similarly, $f(gh)$ is f followed by gh, and this is also f followed by g followed by h. The identity permutation corresponds to the identity symmetry, which, since it is the "do nothing" transformation, has the property that its composite with any symmetry f is the same as f (in whichever order the composition is performed). So the identity permutation also has the property required of an identity element. And since each symmetry has an inverse, each of the above permutations also has an inverse.

10) The set of all permutations of $\{1, 2, 3, 4\}$ is a group. This fact will be proved later. Note that there are 24 permutations of $\{1, 2, 3, 4\}$ altogether.

11) The set of all symmetries of any object is always a group. This is the basic reason why group theory is important.