3. EXAMPLES OF GROUPS

§3.1. Abstract Groups and the Group Axioms

Before we surf the wide ocean of group theory let's review the definition of a group so that we'll easily recognise one when we come across it.

For Galois, a group involved the symmetry of certain algebraic expressions involving the zeros of a polynomial. After his death the concept was abstracted from its polynomial setting as the emphasis shifted to groups of 'substitutions' (as they were called at the time) or 'permutations' (as we refer to them now). The symbols being permuted could now can be anything, not just zeros of polynomials. This was the first stage in the process of abstraction.

A considerable body of theory was built up and many books were written on the subject until it was realised that almost every theorem could be derived from just four simple facts. That resulted in the process of abstraction being continued one stage further as groups and permutations were uncoupled. Now *any* algebraic system that behaves in a manner described by these four axioms could be called a group.

'Group' is the name given to a certain type of algebraic structure that satisfies four basic properties called the **group axioms** or **group laws**. On the basis of

these axioms it's possible to develop a considerable body of theory – group theory. We can prove theorems about groups without needing to know what they're groups of, just by basing the proofs on these four axioms.

The advantage of this abstract approach is that we can deal with countless algebraic systems all at once. A single theorem in group theory immediately becomes a theorem for groups of matrices, groups of numbers, groups of permutations, and so on.

A **binary operation** $*$ on a set G is a function that associates with every ordered pair of elements $a, b \in$ G, a unique element of G, denoted by $a * b$.

A **group** (G, $*$) is a set G together with a binary operation $*$ such that:

(1) Closure Law: $a * b \in$ G for all $a, b \in$ G.

(2) Associative Law:

$$(a * b) * c = a * (b * c) \text{ for all } a, b, c \in \text{G}.$$

(3) Identity Law: There exists $e \in$ G such that:

$$a * e = a = e * a \text{ for all } a \in \text{G}.$$

(4) Inverse Law: For all $a \in$ G there exists $b \in$ G such that $a * b = e = b * a$.

COMMENTS

(1) The closure law is redundant because it's implicit in the definition of a binary operation. However it's usually included for emphasis.

(2) The element e is called the **identity** for G. We'll show later that it must be unique, that is, a group can only have one identity for its operation.
(3) The element b in the last axiom is called the **inverse** of a (under $*$). It too is unique. Every element has exactly one inverse.
(4) The inverse of the inverse of an element is that element itself.

An **abelian** group G (so called to honour the Norwegian mathematician, Abel, whose work preceded Galois) is one that, in addition, satisfies the following:

Commutative Law: $a * b = b * a$ for all $a, b \in$ G.

§3.2. Subgroups

Groups are not isolated structures. Rather they're nested, one inside another, like a set of Russian dolls. Open up a group and you'll usually find lots of smaller groups living inside of it. They are called 'subgroups' of the larger group.

A subset H of G is a **subgroup** if:

(1) $a * b \in$ H for all $a, b \in$ H;

(2) e (the identity element of G) $\in$ H;

(3) the inverse of every element of H is in H.

Notation: H ≤ G.

NOTES:

(1) We often summarise these by saying that H is closed under the operation, under the identity and under inverses.

(2) These properties correspond to three of the four group axioms. The associative law doesn't have to be verified for a subgroup because it holds throughout all of the group. So subgroups are groups in their own right.

(3) The operations in H and G have to be the same. You can't have a subset of a group of numbers under addition being a subgroup under multiplication. For example the group of positive real numbers under multiplication is not a subgroup of the group of all real numbers under addition.

(4) Every group is a subgroup of itself.

The **order** of a group G is its number of elements. If this is **finite** we say that G is a **finite group**. Otherwise it's an **infinite** group. This distinction is important because the theories of finite groups and infinite groups use somewhat different methods. For example in finite group theory the divisibility properties of the natural numbers play an important role.

Notation: The **order** of the group G is denoted by **|G|**.

We're now ready to go hunting for groups and we'll find that they're native to practically every continent of the world of mathematics.

§3.3. Groups of Numbers

The easiest place to find groups is in the various number systems. Numbers can be both added and multiplied but if we focus our attention on just one of these we can produce examples of groups. And because the commutative law holds for addition and multiplication of numbers the groups we'll get will all be abelian.

Let's begin with $(\mathbb{Z}, +)$, the group of integers under addition. If you replace $*$ in the group axioms by $+$ you'll see that they all hold. The identity, e, in this case is the number 0 and the inverse of x is $-x$.

Now $(\mathbb{Z}, \times)$ is not a group. The problem lies with inverses under multiplication. Not only does 0 fail to have an inverse, numbers such as 2 have no inverse, not within the system of integers at any rate, since ½ is not an integer. It's not enough for an inverse to exist. It has to lie within the set under consideration. In fact the only integers which do have multiplicative inverses within $\mathbb{Z}$ are ± 1.

Within the group of integers under addition there's the subgroup $2\mathbb{Z}$ of even integers (even + even is even, 0 is even and minus an even is even). Other subgroups are $m\mathbb{Z}$ for any m, the multiples of a fixed integer m.

The rational numbers under addition form the group $(\mathbb{Q}, +)$ (for example rational plus rational is

rational) and $(\mathbb{Z}, +)$ is one of its many subgroups. Under multiplication $(\mathbb{Q}, \times)$ almost qualifies. Only zero fails to have an inverse under multiplication. If we exclude zero, and denote the set of non-zero rationals by $\mathbb{Q}^{\#}$, we do get a group. But note that we have to rethink the closure law. It's no longer enough that the product of two rationals is a rational. We need the product of two *non-zero* rationals to be a *non-zero* rational. Fortunately this is so by the cancellation law for rationals:

$xy = 0$ implies that $x = 0$ or $y = 0$.

One subgroup of $(\mathbb{Q}^{\#}, \times)$ is the set of all powers of 2: $\{2^n \mid n \in \mathbb{Z}\}$. This is because $2^m.2^n = 2^{m+n}$, the identity under multiplication is $1 = 2^0$ and $(2^n)^{-1} = 2^{-n}$.

A really small subgroup of $(\mathbb{Q}^{\#}, \times)$ consists just of ± 1. An even smaller one is $\{1\}$.

In fact for any group G the subset $\{e\}$, consisting of just the identity, is a subgroup known as the **trivial** subgroup of G. Check it:

(1) $e * e = e$;

(2) $\{e\}$ contains the identity;

(3) the inverse of e is e.

Things work for the real and complex numbers in very much the same way. The group $(\mathbb{C}, +)$ contains the subgroup $(\mathbb{R}, +)$. Another subgroup is the set of imaginary numbers (including 0). Within $(\mathbb{R}, +)$ you find $(\mathbb{Q}, +)$ and a subgroup of $(\mathbb{Q}, +)$ is $(\mathbb{Z}, +)$ etc.

The non-zero complex numbers under multiplication form the group $(\mathbb{C}^{\#}, \times)$ which in turn

contains $(\mathbb{R}^{\#}, \times)$. One of the many subgroups of $(\mathbb{R}^{\#}, \times)$ is $(\mathbb{Q}^{\#}, \times)$ and $(\mathbb{Q}^{\#}, \times)$ has within it the subgroup $(\mathbb{Q}^{+}, \times)$ of positive rationals.

For groups of numbers we usually omit the operation and just write $\mathbb{Q}$ or $\mathbb{Q}^{\#}$ etc. There's no ambiguity because there's a simple way to determine whether the operation is intended to be addition or multiplication, by a process of elimination. If the set contains zero, such as $\mathbb{R}$, it can't be a group under multiplication because zero doesn't have an inverse. But if zero is excluded it can't be a group under addition because zero is the identity under addition and so must be included.

So $0 \leq \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ and $1 \leq \mathbb{Q}^{+} \leq \mathbb{Q}^{\#} \leq \mathbb{R}^{\#} \leq \mathbb{C}^{\#}$. Notice that it's usual to denote the trivial subgroup by just 0 or 1 depending on the operation.

Of course if the operation is neither addition nor multiplication, and there's no reason why it has to be one or the other, then it must be spelt out explicitly.

Here's a group of numbers where the operation is neither addition nor multiplication.

Example 1: Let $G = \{x \in \mathbb{R} \mid x \neq -1\}$ and define

$$x * y = x + y + xy.$$

Then $(G, *)$ is a group.

Closure: If $x, y \in G$ then $x * y = (x + 1)(y + 1) - 1 \neq -1$ so $x * y \in G$.

Associative law: Since this is an operation we've never seen before we must check associativity:

$$(x * y) * z = (x * y) + z + (x * y)z$$
$$= (x + y + xy) + z + (x + y + xy)z$$
$$= x + y + z + xy + xz + yz + xyz$$

and $x * (y * z) = x + (y * z) + x(y * z)$

$$= x + y + z + yz + x(y + z + yz)$$
$$= x + y + z + xy + yz + xz + xyz.$$

Identity: The identity is 0.

Inverse: the inverse of $x \in G$ is $\frac{-x}{x+1}$ since

$$x + \frac{-x}{x+1} + x\left(\frac{-x}{x+1}\right) = 0.$$

Note that the denominator is non-zero since $x \neq -1$.

Moreover, $\frac{-x}{x+1} = -1 + \frac{1}{x+1} \neq -1.$

Another type of number is an integer-modulo-*m*, for some positive integer modulus *m*. Under addition these give the groups $(\mathbb{Z}_m, +)$. Because the operation is different to ordinary addition (eg. $1 + 1 = 0 \bmod 2$) they're not subgroups of $(\mathbb{Z}, +)$. In fact none of them is a subgroup of any of the others.

Under multiplication we may have to exclude more than just 0. Consider $\mathbb{Z}_{10}$ under multiplication. The numbers 2, 4, 5, 6 and 8 fail to have inverses under multiplication because they're not coprime to 10. For example if *y* was the inverse of 6 mod 10 then 6*y* would

have to be 1 plus a multiple of 10, which is clearly impossible.

Only 1, 3, 7 and 9 have inverses mod 10 and these inverses are 1, 7, 3 and 9 respectively. [Remember, for example, that $3.7 = 21 = 1 \bmod 10$.]

Moreover the set {1, 3, 7, 9} is closed under multiplication as can be seen if we write out the group table:

$\mathbb{Z}_{10}^{\#}$	**1**	**3**	**7**	**9**
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

The associative law holds because it holds for integers. So we get a group.

We denote the set of invertible elements of $\mathbb{Z}_m$ (the ones that have inverses, or equivalently, are coprime to m) by $\mathbb{Z}_m^{\#}$. This will always be a group because the product of two invertible elements is invertible.

Now the group $\mathbb{Z}_{12}^{\#}$ also has four elements {1, 5, 7, 11} and the group table is:

$\mathbb{Z}_{12}^{\#}$	**1**	**5**	**7**	**11**
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

In Chapter 1 we encountered the mattress group which also has order 4. Its table is:

	I	**A**	**B**	**C**
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

Which of the tables, the one for $\mathbb{Z}_{10}^{\#}$ or the one for $\mathbb{Z}_{12}^{\#}$ does this most resemble? The answer is $\mathbb{Z}_{12}^{\#}$. The mattress group and $\mathbb{Z}_{12}^{\#}$ follow the same pattern: everything squared is the identity and the product of any two of the non-identity elements is equal to the third. In fact we can turn one table into the other by the code

$$I \to 1,\ A \to 5,\ B \to 7,\ C \to 11.$$

The group $\mathbb{Z}_{10}^{\#}$ on the other hand is rather different. It can't be changed into the mattress group by any relabelling. The most obvious difference is that in $\mathbb{Z}_{10}^{\#}$ there are only 2 solutions to the equation $x^2 = 1$ while in both the mattress group and $\mathbb{Z}_{12}^{\#}$ all four elements satisfy this equation.

If two groups have essentially the same structure, meaning that the group table for one can be turned into the table for the other by a suitable renaming, we say that the groups are **isomorphic**. So $\mathbb{Z}_{12}^{\#}$ is isomorphic to the mattress group but neither of these is isomorphic to $\mathbb{Z}_{10}^{\#}$. (We'll define isomorphism a little more formally later.)

So there are at least two, essentially different, groups of order 4. In fact, as we'll see later, these are the only two. There are only finitely many groups with any given finite order (up to isomorphism) and one of the fundamental problems of finite group theory is to classify them.

§3.4. Groups of Permutations

The symmetric group, $\mathbf{S}_n$, is the group of all permutations on $\{1, 2, \ldots, n\}$. An important subgroup is the alternating group, $\mathbf{A}_n$, the group of all even permutations.

Another subgroup of $\mathbf{S}_n$ is the set H of all permutations that fix the symbol 1.

The elements of H permute the remaining elements 2, 3, ... , n in all the $(n - 1)!$ possible ways. By renumbering these symbols as 1, 2, ... , $n - 1$ we can turn this group into a copy of $\mathbf{S}_{n-1}$. In other words H is **isomorphic** to $\mathbf{S}_{n-1}$.

An important subgroup of S_4 is called the **Klein group** (after the mathematician Felix Klein) or the **Viergruppe** (German for the 'four-group'). It's often

denoted by $\mathbf{V_4}$ which is a bit silly in a way because both the V for 'vier' and the 4 tell us that there are four elements: $\mathbf{V}_4 = \{I, (12)(34), (13)(24), (14)(23)\}$.

Its group table is:

$\mathbf{V}_4$	**I**	**(12)(34)**	**(13)(24)**	**(14)(23)**
I	I	(12)(34)	(13)(24)	(14)(23)
(12)(34)	(12)(34)	I	(14)(23)	(13)(24
(13)(24)	(13)(24)	(14)(23)	I	(12)(34)
(14)(23)	(14)(23)	(13)(24)	(12)(34)	I

Notice that once again this has the same pattern as both $\mathbb{Z}_{12}^{\#}$ and the mattress group. $\mathbf{V}_4$ is a permutation group that's isomorphic to these other groups.

For many decades groups were only groups of permutations. Introducing the group axioms freed us from this connection and enabled us to look for groups anywhere. But in fact it didn't really lead us to find any extra groups, just different disguises for the same groups. This is because every group is isomorphic to a group of permutations. Multiplication of the elements of a group G by a fixed element is a permutation and these permutations form a group that's isomorphic to G.

This is known as Cayley's Theorem and we'll give a formal proof of it later once we've defined the word 'isomorphic' properly. But you can see it working in the following example.

Take the group $\mathbb{Z}_{12}^{\#}$:

$\mathbb{Z}_{12}^{\#}$	**1**	**5**	**7**	**11**
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Multiplication on the right by 5 permutes these four elements in a way that can be described in cycle notation as (1 5)(7 11). The corresponding permutations for all four elements are:

1	I
5	(1 5)(7 11)
7	(1 7)(5 11)
11	(1 11)(5 7)

Now relabelling the elements of $\mathbb{Z}_{12}^{\#}$ by the code: $1\to1$, $5\to2$, $7\to3$, $11\to4$ these four permutations become I, (12)(34), (13)(24), (14)(23), the elements of $\mathbf{V}_4$.

§3.5. Groups of Polynomials, Functions and Vectors

Polynomials can be added and subtracted, and the set of all polynomials in x over a field F forms an abelian group F[x]. Polynomials can also be multiplied but we

don't get a group, even if we exclude the zero polynomial, because expressions such as $\frac{1}{x+1}$ are not polynomials.

Functions $f: \mathbb{R} \to \mathbb{R}$ can be added, and again we get an abelian group. Multiplying functions, in the way that we might multiply the functions $f(x) = x^2$ and $g(x) = \sin x$ to get the function $f(x)g(x) = x^2 \sin x$, raises problems with inverses. For example g doesn't have an inverse. What about cosec $x = \frac{1}{\sin x}$? That's not a function from $\mathbb{R}$ to $\mathbb{R}$ since it's undefined when $x = n\pi$ for any integer n.

But there's another way of multiplying functions – function of a function. For any set X, if we have two functions f, g from X to X we can form their product fg, defined by $(fg)(x) = g(f(x))$, that is, we first apply f and then apply g. If $f(x) = x^2$ and $g(x) = \sin x$ then the product fg is the function $(fg)(x) = \sin(x^2)$, while gf is the function $(gf)(x) = (\sin x)^2$, which we normally write as $\sin^2 x$. Clearly, if we do get a group out of this it will be non-abelian.

In fact the groups we get out of this operation are the familiar groups of permutations on a set X. But X will be mostly infinite and in such cases the examples will look rather different to the usual permutation groups. Here's an example of a finite group of permutations on an infinite set.

Consider the functions:

$a(x) = x,$

$b(x) = 1 - x,$

$c(x) = \frac{1}{x},$

$d(x) = \frac{1}{1-x},$

$e(x) = \frac{x-1}{x},$

$f(x) = \frac{x}{x-1}.$

Since these are undefined for $x = 0$ and $x = 1$ we must exclude these values from the domain. So let's take X to be the set $\mathbb{R} - \{0, 1\}$, that is, the set of all real numbers excluding 0 and 1. Not only are all the above defined for every $x \in$ X, a quick check will reveal that their range is also X and that these are 1-1 and onto functions on X.

Now $d^2(x) = d(d(x)) = \frac{1}{1 - \frac{1}{1-x}} = \frac{x-1}{x} = e(x)$ and

$$(bd)(x) = \frac{1}{1-(1-x)} = \frac{1}{x} = c(x)$$

so that $d^2 = e$ and $bd = c$.

We can complete the group table for this group of order 6:

	a	***b***	***c***	***d***	***e***	***f***
a	*a*	*b*	*c*	*d*	*e*	*f*
b	*b*	*a*	*d*	*c*	*f*	*e*
c	*c*	*e*	*a*	*f*	*b*	*d*
d	*d*	*f*	*b*	*e*	*a*	*c*
e	*e*	*c*	*f*	*a*	*d*	*b*
f	*f*	*d*	*e*	*b*	*c*	*a*

Note that $d^3 = de = a$, the identity, so d has order 3, $b^2 = a$, and so d has order 2, and $bd = c = eb = d^{-1}b$. So this group is isomorphic to the dihedral group

$$D_6 = \langle A, B \mid A^3 = 1, B^2 = 1, BA = A^{-1}B \rangle,$$

with A corresponding to d and B corresponding to b.

Among the axioms for a vector space V, over a field F, are the group axioms for V to be a group under addition. In fact if we ignore scalar multiplication, vector spaces are just abelian groups. So we can produce examples of abelian groups by taking the set of all vectors $(x_1, x_2, \ldots, x_n)$ with each $x_i \in$ F, under the operation of addition.

If we want to get a finite group we'd need to take F to be a finite field, of which the best-known examples are the integers modulo a prime.

We denote the set of all vectors $(x_1, x_2, \ldots, x_n)$, with each $x_i \in \mathbb{Z}_p$ by

$$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p \ (n \text{ copies of } \mathbb{Z}_p).$$

We will explain the full meaning of the symbol $\oplus$ in a later chapter.

But since we're only adding these components there's no need for them to come from a field. In other words p need not be prime.

$\mathbb{Z}_6 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6$ is the set of all vectors of the form (x, y, z) where $x, y, z \in \mathbb{Z}_6$. With 6 choices for each component this gives a group of order $6^3 = 216$. It isn't even necessary for the modulus to be the same for each component. So $\mathbb{Z}_4 \oplus \mathbb{Z}_6$ is a group, under addition, of order 24, consisting of all vectors (x, y) where

$$x \in \mathbb{Z}_4 \text{ and } y \in \mathbb{Z}_6.$$

Here $(3, 5) + (2, 4) = (1, 3)$ since $3 + 2 = 1 \pmod 4$ and $5 + 4 = 3 \pmod 6$.

§3.6. Groups of Matrices

If F is a field **GL(n, F)** denotes the group of all invertible $n \times n$ matrices over F under multiplication. The phrase 'over F' means that the components come from F and 'under multiplication' means that the operation is matrix multiplication.

This group is called the **general linear group of degree n over F**. Checking the axioms needs a little non-trivial knowledge about matrices. We know that the associative law holds for matrix multiplication. Checking the closure law requires us to know that the product of two invertible matrices is invertible. And we need to know more than just the fact that every invertible matrix has an inverse. We need to observe that such an inverse is itself invertible.

An interesting subgroup of GL(n, F) is $\mathbf{T^+(n, F)}$ the set of all $n \times n$ **upper-triangular matrices** over F, that is, $n \times n$ matrices of the form:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & a_{22} & a_{23} & \dots & a_{2n} \\ 0 & 0 & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a_{nn} \end{pmatrix}$$

where each diagonal component is non-zero.

Check out for yourself that this set is closed under multiplication and that the inverse of any one of these matrices again has the same form.

Then there are the **lower triangular matrices** $\mathbf{T^-(n, F)}$ which are the transposes of the upper triangular ones. The intersection of these are the invertible **diagonal matrices D(n, F)**.

It's closed under multiplication, identity and inverses simply because each of $T^+(n, F)$ and $T^-(n, F)$ are. This is a special case of the general fact that:

The intersection of any collection of subgroups is itself a subgroup.

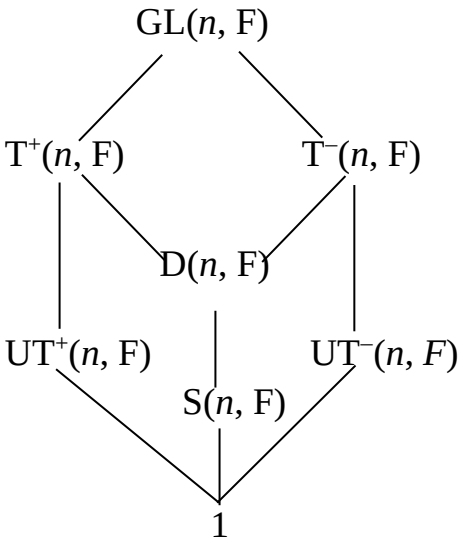
Within D(n, F) we have the non-zero **scalar matrices S(n, F)**. These are simply the diagonal matrices that have the same non-zero entry down the diagonal, that is, non-zero scalar multiples of the identity matrix.

Another interesting subgroup of $T^+(n, F)$ is the group of **uni-upper-triangular matrices $UT^+(n, F)$**. These are the upper-triangular matrices with 1's down the diagonal:

$$\begin{pmatrix} 1 & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & 1 & a_{23} & \dots & a_{2n} \\ 0 & 0 & 1 & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

And inside $T^-(n, F)$ we have the **uni-lower-triangular matrices $UT^-(n, F)$**.

We can summarise the connections between these subgroups in a so-called 'lattice diagram':



Here the lines indicate subgroup relationships, with the lower group being a subgroup of the group at the higher end of the line.

Another very important subgroup of GL(n, F) is **SL(n, F)** consisting of all the matrices with determinant 1. It's called **the special linear group of degree n over F**. We could incorporate this into our lattice of subgroups but including its intersections with the other subgroups would make the diagram very messy.

The **lattice of subgroups** of a group G is such a picture of *all* its subgroups. One subgroup is contained in another if and only if there is an ascending path in the diagram from the smaller to the larger. The intersection of two subgroups is the largest subgroup contained in them both and is easily picked out from the diagram.

If F is a finite field, such as $\mathbb{Z}_p$ we get a finite group. The group GL(n, $\mathbb{Z}_p$) is generally written as **GL(n, p)**.

Matrix groups provide a very rich source of examples of groups, both abelian and non-abelian. In fact, since every finite group is isomorphic to a group of permutations, and every permutation can be represented by a permutation matrix it follows that every finite group is isomorphic to some matrix group. This fact provides the basis for representation theory which we'll study in a later chapter.

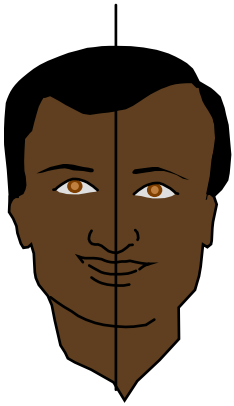
§3.7. Symmetry Groups

Symmetry can be found in many places, in art, graphic design, music, architecture, in the natural world and in science. And there are many types of symmetry.

There's the **mirror symmetry** we expect to find in the human face, there's the **rotational symmetry** such as you find in many flowers and the **translational symmetry** that's found in a repetitive piece of music or a recurring decimal expansion. Sometimes the symmetry is a combination of translational, rotational and mirror symmetry as in a honeycomb or a brick wall.

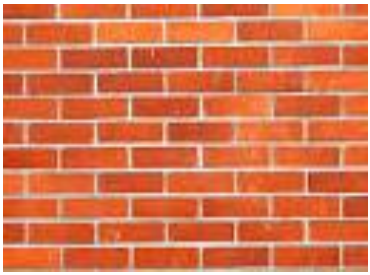
Poetry exhibits aspects of symmetry in its rhyming patterns and physical laws involve symmetry. Even asymmetry makes use of symmetry for its effect relies on our unsatisfied expectation of symmetry.

But what really is symmetry? The most useful definition is in terms of operations that keep something the same. The human face is never exactly symmetrical, but we imagine it to have mirror symmetry about a vertical axis of symmetry. If reflected left-to-right in this axis a face appears to be the same. The reflection operation is therefore a symmetry operation for the face.



So whenever we have an axis of symmetry we have a symmetry operation. In this case the symmetry is **mirror symmetry** (though for a 2-dimensional shape we can also think of it as a 180° rotation in a third dimension). But, as we saw with the square there's **rotational symmetry** as well.

The infinite pattern of bricks below exhibits two other forms of symmetry, **translational symmetry** and **glide symmetry**. A **translation** is a movement in a certain distance by a certain amount and if an infinite pattern is fixed by such a translation it is said to have translational symmetry. The brick pattern has horizontal translational symmetry through one brick length (or any integer multiple of this distance).



A **glide** is a reflection in an axis followed by a translation along that axis. The brick pattern has horizontal axes of symmetry running through the midpoints of the bricks but the lines which run between the rows of bricks are not mirror axes. Yet if you reflect in such a line and then translate by half a brick length, the pattern snaps back into place. So the pattern is fixed as a whole by this glide. A set of footprints only has glide symmetry.

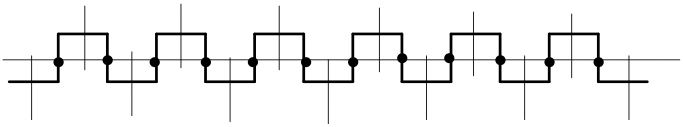
Isometries are distance-preserving functions. They include reflections, rotations, translations and glides (in two dimensions these are the only isometries). A **symmetry operation** for a shape is an isometry that fixes

the shape as a whole. While individual points are moved by the operation the whole shape occupies exactly the same region of space.

It's clear that if you multiply one symmetry operation by another (that is, follow one by another) you get a symmetry operation. The identity is always a symmetry operation and the inverse of a symmetry operation is a symmetry operation. So the set of all symmetry operations for a shape forms a group, called the **symmetry group** of the shape.

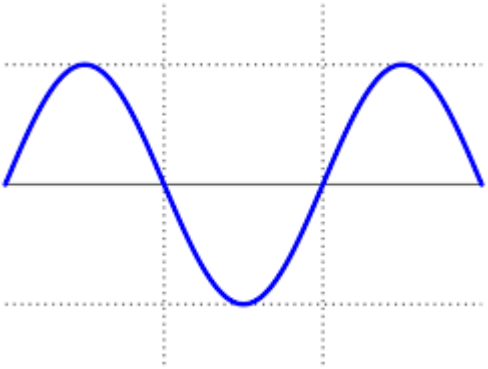
Castle Turrets:

The machicolations on a castle wall form the jagged outlines from which archers can fire their arrows. An infinitely long pattern of this type has **translational** symmetry in that if you translate the pattern through a certain distance it remains unchanged – each turret just gets moved on to the next.



There's also **reflectional** symmetry in the infinitely many vertical axes of symmetry (the horizontal axis is not an axis of symmetry). Then there's 180° **rotational** symmetry about the centres indicated by the dots. Finally there is what is called **glide** symmetry along the horizontal axis. Reflecting the pattern of turrets in the horizontal axis and then translating half a turret distance, every point on the pattern is moved to an equivalent one.

The sine curve also exhibits this same type of symmetry.



If T is the translation that takes each peak to the next on its right, R is the 180° rotation about one of the points where the curve cuts the *x*-axis, M is the reflection in the vertical axis immediately to the right of this point and G is the glide that takes each peak to the next trough to the right then:

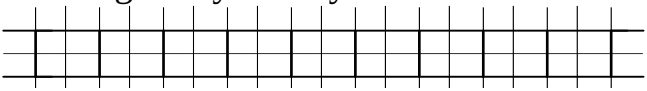
$$T = G^2,\ R = GM,\ M^2 = I \text{ and } GM = MG^{-1}.$$

The symmetry group of this pattern is generated by G and M alone and is in fact the infinite dihedral group

$$\langle G, M \mid M^2 = 1,\ GM = MG^{-1} \rangle.$$

Railway lines:

A set of railway tracks is another infinite repeating pattern. But unlike the sine curve or the castle turrets, the horizontal axis is an axis of reflectional symmetry and not just an axis of glide symmetry.



As well, there are infinitely many vertical axes of symmetry and infinitely many centres of 2-fold, that is 180°, rotational symmetry. And finally there are glides built up from these reflections and translations.

If T denotes the translation that takes each ‘railway sleeper’ to the next on the right, H the reflection in the horizontal axis and V the reflection in one of the vertical axes of symmetry then the group of symmetries is the infinite group

$$\langle T, H, V \mid H^2 = V^2 = 1, TH = HT, TV = VT^{-1}, HV = VH \rangle.$$

The people who are most interested in symmetry groups, particularly for 3 dimensional patterns, are crystallographers. Crystallography is the branch of chemistry that deals with the possible crystal lattices for various substances and the crystallographers long ago classified all possible symmetry groups in 2 and 3 dimensions.

§3.8. Group Tables

A finite group can be described by displaying its group table as follows:

$*$	y
	……..
x	... $x*y$ .....
	……..

The set $\{a, b, c\}$ becomes a group under the binary operation defined by the following table.

*	***a***	***b***	***c***
a	*a*	*b*	*c*
b	*b*	*c*	*a*
c	*c*	*a*	*b*

Given a table, however, it's not always easy to verify that it's a group table. The closure, identity and inverse axioms are easy to check but the associative law would involve a considerable amount of laborious checking. The quickest way to check the associative law is in fact to construct a group (where you know the associative law holds) and show that it's isomorphic to the one in the given table.

For example, to show that the above table is a group table we would need to check that $(xy)z = x(yz)$ for 27 combinations of x, y and z. But we can instead observe that $G = \{1, \omega, \omega^2\}$ is a group under multiplication, where $\omega = e^{2\pi i/3}$ is a non-real cube root of unity and that the code $1 \to a$, $\omega \to b$, $\omega^2 \to c$ transforms the group table for G to the one above.

§3.9. Group Presentations

The above group can be described very concisely by the notation $\langle A \mid A^3 = 1 \rangle$. This is called a **presentation** for the group with the first part being a list of generators (in this case there's just one). A **set of generators** is a subset of the group such that every element is a product of powers of the generators. The second part of the

description is a list of the relations that generate all the relations that hold between the generators.

The relation $A^3 = 1$ is not the only relation that holds in this group. We also have $A^6 = 1$, $A^9 = 1$, ... not to mention $A^{-3} = 1$, $A^{-6} = 1$, ... But all of these are consequences of the given one and so they may be omitted.

The trivial group also has a generator A such that $A^3 = 1$, so why doesn't this notation refer to that group as well? The assumption is not simply that the given relations hold in the group but that any relation which does hold is a consequence of the stated ones. In the trivial group we also have $A = 1$ and $A^2 = 1$, but these can't be deduced from the relation $A^3 = 1$.

This is only a fairly informal definition of presentations, but it will suffice for now. A more rigorous definition in terms of quotient groups of free groups will be given in a later chapter.

The relations can always be put in the form $R = 1$, though it's not always convenient to do so. When a relation is expressed in this form the expression R is called a **relator** and often just the relator is given. So the above group could be expressed as $\langle A \mid A^3 \rangle$.

It's even permissible to mix relators and relations in the same presentation. The **Klein group**, $\mathbf{V}_4$, has the presentation $\langle A, B \mid A^2, B^2, AB = BA \rangle$.

Other presentations for $\mathbf{V}_4$ are

$$\langle A, B \mid A^2, B^2, (AB)^2 \rangle \text{ and}$$
$$\langle A, B, C \mid A^2, B^2, C^2, AB = C = BA \rangle.$$

Here you see yet another small variation in the notation as a shortcut, that of having a chain of equalities.

A very common presentation for the dihedral group of order 8 is:

$$\mathbf{D}_8 = \langle A, B | A^4, B^2, BA = A^{-1}B \rangle.$$

More generally the dihedral group of order $2n$ can be defined by the presentation:

$$\mathbf{D}_{2n} = \langle A, B \mid A^n, B^2, BA = A^{-1}B \rangle.$$

In principle all the information about a group is locked up in such a compact presentation but it isn't always easy to release it. For many presentations, such as the one above for the dihedral group, we can argue that every element has the form A^rB^s for some integers r, s. That is because the relation $BA = A^{-1}B$ can be interpreted by saying that if we move a B past an A, the B doesn't change but the A is inverted.

Now a typical element of the group is a product of powers of the generators A and B, such as $A^5BA^{-2}B^3A$. Using the relation $BA = A^{-1}B$ we can move all the B's past all the A's to the back. The relation acts a bit like the commutative law, except that the power of A will not simply be the sum of all the powers scattered throughout the expression. For this example we'd have

$$A^5BA^{-2}B^3A = A^5A^2BB^3A = A^7B^4A = A^7AB^4$$

(the last A gets inverted 4 times by B^4 so remains as A)

$$= A^8B^4.$$

Of course since $B^2 = 1$ this simplifies further to A^8 and if n is 8 or less we could reduce this further. But

whenever you have a relation of the form $BA = A^kB$ anything generated by A and B can be expressed in the form A^rB^s.

For the dihedral group $\langle A, B \mid A^n, B^2, BA = A^{-1}B\rangle$ a typical element can be put in the form A^rB^s where:

$$0 \le r < n \text{ and } s = 0 \text{ or } 1.$$

Moreover these $2n$ expressions represent distinct elements so we can infer that the group has order $2n$.

With the elements written as:

$$1, A, A^2, \ldots, A^{n-1}, B, AB, A^2B, \ldots, A^{n-1}B$$

we can prepare a group table. To multiply any pair of elements we simply use the rule (valid for dihedral groups but not for groups in general) that **moving a B past an A inverts the A but leaves the B unchanged**. For example $A^5BA^3 = A^5A^{-3}B = A^2B$. And once we have the group table we can investigate the properties of the group fully.

Things are not always that easy. Given a very complicated presentation we may not even be able to decide whether the group is finite or infinite, or even whether the group has more than one element!

The Word Problem for groups asks the following:

WORD PROBLEM

Find an algorithm which can determine whether a given word in a group described by a given presentation is equal to the identity.

The Word Problem is unsolvable. It's not simply that nobody has yet found such an algorithm. No, a proof has been given that no such algorithm can possibly exist!

Fortunately in practice things are not quite so gloomy. There's an algorithm, called the Todd Coxeter algorithm which mostly works. (We'll visit it in a later chapter.) It's an algorithm that isn't completely deterministic in that at one place in each cycle a choice has to be made. Make a good choice each time and you'll get an answer. The algorithm is reliable in the sense that you'll never get a wrong answer. But it may fail to terminate.

An important class of groups are the **free groups**. These are groups with generators but no relators. The free group on one generator is $\langle A| \rangle$, which is isomorphic to $\mathbb{Z}$, with $A^n \rightarrow n$. It can be denoted by F_1.

The free group on 2 generators, F_2 can be presented as $\langle A, B| \rangle$. The elements are words on A, B and their inverses and every element is expressible as a unique **reduced word**, that is a word in which adjacent pairs of a generator and its inverse are removed. Multiplication is by concatenation followed by cancelling adjacent pairs of generators and inverses.

Example 2:

In $\langle A, B| \rangle$, $ABA^{-1}B \times B^{-1}ABBA^{-1} = ABBBA^{-1}$

EXERCISES FOR CHAPTER 3

EXERCISE 1: Which of the following subsets of $\mathbb{Z}$ are groups under addition?

A = the set of even integers;
B = the set of odd integers;
C = the set of non-negative integers;
D = {0};
E = the set of integers which are expressible as $42m + 1023n$ for integers m, n.

EXERCISE 2: Which of the following subsets of $\mathbb{C}$ are groups under multiplication?

A = the set of non-zero rational numbers;
B = the set of positive integers;
C = {1, –1, i, –i};
D = {1, ½, 2};
E = $\{a + b\mathrm{i} \mid a > 0\}$;
F = $\{1, \pi, \pi^2, \pi^3, \ldots\}$.

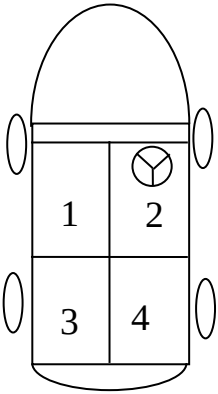
EXERCISE 3: Let $G = \{x \in \mathbb{R} \mid x \neq 1\}$ and define

$$x * y = xy - x - y + 2.$$

Prove that $(G, *)$ is a group.

EXERCISE 4:
Prove that {I, (12), (345), (354), (12)(345), (12)(354)} is a group.

EXERCISE 5:
Jack and Jill are going out together, as are Romeo and Juliet. Tonight they're going out on a double date, with Jack and Jill sitting in the front seat of their red convertible and with Romeo and Juliet cuddling in the back. It's a long drive and so every so often they stop and change drivers. But at all times Jack and Jill must sit together and so must Romeo and Juliet, so not every permutation on the set {Jack, Jill, Romeo, Juliet} is permitted. Show that the permutations that keep each couple together form a group.



EXERCISE 6: Which of the following are groups under polynomial addition:

(a) The set of all real polynomials that have $x - 1$ as a factor;

(b) The set of all real polynomials of even degree, together with 0;

(c) The set of all integer polynomials whose sum of coefficients is even;
(d) The set of all integer polynomials where every coefficient is odd.

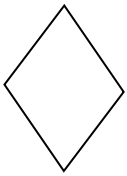
EXERCISE 7: In the group $\mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{10}$ perform the following additions:

(a) (3, 2, 7) + (2, 1, 8);
(b) (0, 4, 2) + (1, 4, 3);
(c) (2, 3, 4) + (2, 2, 6).

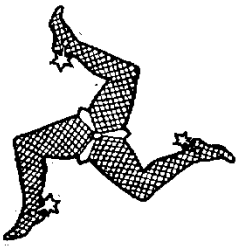
EXERCISE 8: Show that the set of all real matrices of the form $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ is a group under matrix multiplication. Does it satisfy the commutative law?

EXERCISE 9: Find the rotation group of a parallelogram:

EXERCISE 10: Find the rotation group of a diamond shape and write out its group table.



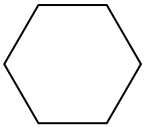
EXERCISE 11: Find the rotation group of the insignia of the Isle of Man:



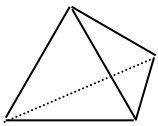
EXERCISE 12: Find the rotation groups of the letters of the alphabet (use the most symmetric possible way of writing each letter).

ABCDEFGHIJKLMNOPQRSTUVWXYZ

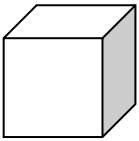
EXERCISE 13: Find the symmetry group of a regular hexagon.



EXERCISE 14: Find the order of the rotation group of a tetrahedron (triangular pyramid with four identical equilateral triangular faces).



EXERCISE 15: Find the order of the rotation group of a cube.



EXERCISE 16: Find the rotation group of the following shape:

EXERCISE 17: G is a group given by the following group table:

	A	**B**	**C**	**D**	**E**	**F**
A	A	B	C	D	E	F
B	B	A	D	C	F	E
C	C	E	A	F	B	D
D	D	F	B	E	A	C
E	E	C	F	A	D	B
F	F	D	E	B	C	A

Calculate the following:

(a) BD;
(b) FACE;
(c) E^{-1};
(d) $D^2B^3FE^{-1}$;
(e) $(BC)^{-2}BF$.

EXERCISE 18: Find all possible group tables on the set $\{1, a, b\}$ where 1 is the identity.

EXERCISE 19: Construct the group table for the group

$$\langle A \mid A^3 \rangle.$$

EXERCISE 20: In the group
$\langle A, B, C \mid A^7, B^3, C^2, BA = A^3B, CA = AC, CB = B^2C \rangle$
express each of the following in the form $A^qB^rC^s$

(a) $(BC)^2$;
(b) B^2A^3;
(c) C^3A^{-2};
(d) $(ABC)^{-1}$;
(e) $(AB)^3$.

EXERCISE 21
Let X be a set and let $\wp X$ denote the set of all subsets of X. For R, S $\in \wp X$ define R • S = (R ∪ S) – (R ∩ S).

(a) Prove that $(\wp X, \bullet)$ is an abelian group.
(b) What is the greatest order of any element of $\wp X$?

HINT: R • S = {x | x belongs to exactly one of R, S}.

SOLUTIONS FOR CHAPTER 3

EXERCISE 1:

A, D, E

EXERCISE 2:

A, C

EXERCISE 3:

Closure: Let $a, b \in G$, so $a \neq 1$ and $b \neq 1$.
Suppose $a * b = 1$.

Then $ab - a - b + 2 = 1$ and so $(a - 1)(b - 1) = 0$ which implies that $a = 1$ or $b = 1$, a contradiction.

Associative: Unlike the examples in exercise 1, this is a totally new operation that we have never encountered before. We must therefore carefully check the associative law.

$$\begin{aligned}(a * b) * c &= (a * b)c - (a * b) - c + 2 \\ &= (ab - a - b + 2)c - (ab - a - b + 2) - c + 2 \\ &= abc - ac - bc + 2c - ab + a + b - 2 - c + 2 \\ &= abc - ab - ac - bc + a + b + c\end{aligned}$$

Similarly $a * (b * c)$ has the same value (we can actually see this by the symmetry of the expression.

Identity: An identity, e, would have to satisfy: $e * x = x = x * e$ for all $x \in$ G, that is:

$ex - e - x + 2 = x$, or $(e - 2)(x - 1) = 0$ for all x.

Clearly $e = 2$ works. We can now check that 2 is indeed the identity.

Inverses: If $x * y = 2$, then $xy - x - y + 2 = 2$.

So $y(x - 1) = x + 2$ and hence $y = \dfrac{x + 2}{x - 1}$.

This exists for all $x \neq 1$, i.e. for all $x \in G$. But we must also check that it is itself an element of G. Clearly this is so because $\dfrac{x + 2}{x - 1} \neq 1$ for all $x \neq 1$.

EXERCISE 4:

The group table is

	I	**(12)**	**(345)**
I	I	(12)	(345)
(12)	(12)	I	(12)(345)
(345)	(345)	(12)(345)	(354)
(354)	(354)	(12)(354)	I
(12)(345)	(12)(345)	(345)	(12)(354)
(12)(354)	(12)(354)	(354)	(12)

	(354)	**(12)(345)**	**(12)(354)**
I	(354)	(12)(345)	(12)(354)
(12)	(12)(354)	(345)	(354)
(345)	I	(12)(354)	(12)
(354)	(345)	(12)	(12)(235)
(12)(345)	(12)	(354)	I
(12)(354)	(12)(345)	I	(345)

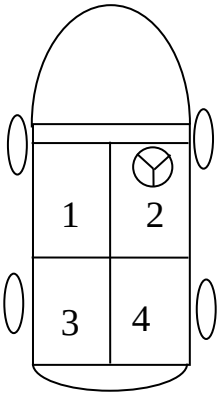
From this we can see that the set is closed under multiplication, and the fact that I appears in every row and

column shows that every element has an inverse. The set contains the identity permutation. Since multiplication of permutations is associative all four group axioms hold.

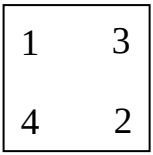
EXERCISE 5:

One way is to represent the four young people by real numbers x_{Jack}, x_{Jill}, x_{Romeo} and x_{Juliet} and to consider the algebraic expression $E = x_{Jack}.x_{Jill} + x_{Romeo}.x_{Juliet}$. The permissible permutations that are allowed are those that keep the value of E unchanged. This is clearly a group.

Or we can number the positions as follows:



The permissible permutations are: I, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423). These are the same permutations in the symmetry group of the square



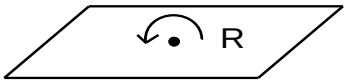
EXERCISE 6:
(a), (b), (c)

EXERCISE 7:
(a) (1, 3, 5), (b) (1, 3, 5), (c) (0, 0, 0).

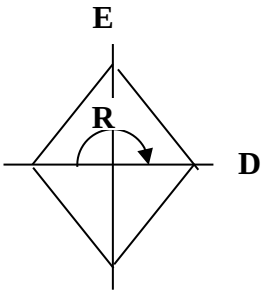
EXERCISE 8:
Closure: $\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & y\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & x+y\\ 0 & 1\end{pmatrix}$ so the set is closed under multiplication.
Identity: $I = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ belongs to this set.
Inverses: The inverse of $\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}$ is $\begin{pmatrix}1 & -x\\ 0 & 1\end{pmatrix}$, which belongs to this set.

The commutative law clearly holds, so this is an abelian group.

EXERCISE 9:
G = {I, R} where R is a 180° rotation.
NOTE: A parallelogram has *no* axes of symmetry unless it is a more symmetrical parallelogram such as a rhombus or a rectangle.



EXERCISE 10:
G = {I, R, D, E} where R is a 180° rotation about the centre and D, E are 180° rotations about the axes indicated.



The group table is:

	I	**R**	**E**	**D**
I	I	R	E	D
R	R	I	D	E
E	E	D	I	R
D	D	E	R	I

EXERCISE 11:
G = {I, R, R^2} where R is a 120° rotation about the centre and R^2 is a 240° rotation.

EXERCISE 12:
Each of **A, B, C, D, E, K, L, M, T, U, V, W** has one axis of symmetry (vertical for **A, M, T, U, V, W** diagonal for **L** assuming both arms have the same length, and horizontal for **B, C, D, E, K**) so their rotation groups are
{I, R} where R is a 180° flip about these axes.

The letters **N, S** and **Z** also have this group as their rotation group but this time R is a 180° rotation about the centre.

The letters **F, G, J, Q** and **R** have 'no symmetry', but since everything has the identity operation as a symmetry operation, their rotation group is just {I}.

The letters **H** and **I** have the same symmetry as a rectangle: {I, H, V and R} where H, V and R are a 180° rotations about the horizontal axis, the vertical axis and the centre, respectively.

The rotation group of the letter **X** (if the axes are at right angles) is the same as that of the square, that is, the dihedral group of order 8 and the rotation group of the letter **Y** (assuming the arms are 120 degrees apart) is $\mathbf{D}_6$.

The letter **O**, represented by a circle, has an infinite symmetry group. Any line through the centre is an axis of symmetry and *any* rotation about the centre is a symmetry operation.

EXERCISE 13:

G = {I, R, R^2, R^3, R^4, R^5, A, B, C, D, E, F} where R is a 60° rotation about the centre and A to F are 180° rotations about the six axes of symmetry.

EXERCISE 14:

There is 3-fold symmetry. Rotations through 120° and 240° about each of the four axes from a vertex to the midpoint of the opposite face are in the rotation group.

Less obvious is the 2-fold symmetry. Rotations through 180° about each of the three axes that join the midpoint of each edge to the midpoint of its opposite edge are in the rotation group.

The rotation group thus has order 12:

one identity
eight 3-fold rotations (2 about each of 4 axes)
three 2-fold rotations (1 about each of 3 axes)

EXERCISE 15: The most obvious symmetry is the 4-fold rotational symmetry about each of the three axes that join the centre of one face to the centre of the opposite face. For each such axis we have three rotations: 90°, 180° and 270°), giving us 9 rotations. Then there are the 2-fold rotations about the axes that join the midpoints of the edges. There are 6 such axes, each associated with one rotation. Finally there are the rotations about the three diagonals joining each vertex to the opposite vertex. If you examine the three edges that come out of each vertex you will see that there is 3-fold rotational symmetry about these diagonal axes. That is, a 120° or a 240° rotation about one of these axes returns the cube to a similar orientation. This gives 2 symmetry operations for each of 4 axes, a total of 8 symmetry operations altogether. We have identified $9 + 6 + 8 = 23$ operations, plus of course the identity giving a total of 24. This is the size of the rotational symmetry group of the cube. There are an additional 24 symmetry operations that arise from reflections.

EXERCISE 16:
The rotation group is {I, R, R^2, A, B, C} where R is a 120° rotation about the centre, and A, B, C are 180° rotations about the three axes of symmetry. This shape has the same rotation group as the equilateral triangle.

EXERCISE 17:
(a) C; (b) D; (c) D; (d) E; (e) B

EXERCISE 18: There is only one:

	1	***a***	***b***
1	1	*a*	*b*
a	*a*	*b*	1
b	*b*	1	*a*

EXERCISE 19:

	1	**A**	$\mathbf{A^2}$
1	1	A	A^2
A	A	A^2	1
$\mathbf{A^2}$	A^2	1	A

EXERCISE 20:
(a) $(BC)^2 = B(CB)C = BB^2CC = B^3C^2 = 1$;

(b) $B^2A^3 = B(BA)AA = BA^3(BA)A = BA^3A^3BA$
$= BA^6(BA) = BA^6A^3B = BA^9B$
$= BA^2B = BAAB = A^3BAB = A^3A^3BB = A^6B^2$;

(c) $C^3A^{-2} = CA^5 = A^5C$;

(d) $(ABC)^{-1} = C^{-1}B^{-1}A^{-1} = CB^2A^6 = (CB)BA^6$
$= B^2CBA^6 = B^2B^2CA^6 = B^4A^6C$
$= BAA^5C = A^3BAA^4C = \ldots$
$= (A^3)^6BC = A^{18}BC = A^4BC.$

EXERCISE 21:

(a) Associative:

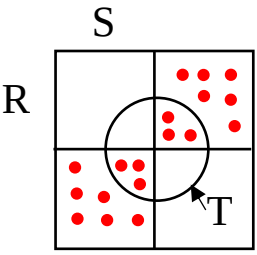
$x \in (R \bullet S) \bullet T$

$\leftrightarrow$ x belongs to exactly one of R, S and T

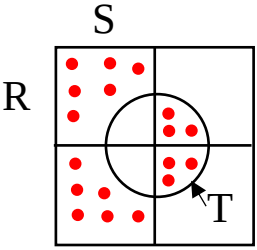
$\leftrightarrow x \in R \bullet (S \bullet T)$.

Alternatively we can use Venn Diagrams.

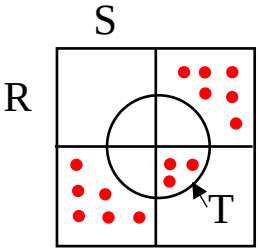
$R \bullet S$



$S \bullet T$



$(R \bullet S) \bullet T = R \bullet (S \bullet T)$



The empty set, $\varnothing$, is the identity.
Every set is its own inverse since $S \bullet S = \varnothing$.
$\wp X$ is abelian since both intersection and union are commutative.

(b) Every element, except the identity, has order 2. This is therefore the maximum order.