Queen Mary
University of London

MTHM024/MTH714U Group Theory

Peter Cameron's 2010 Revision Notes, Sections 1 and 2, slightly updated by LHS, 2014

Group theory is a central part of modern mathematics. Its origins lie in geometry (where groups describe in a very detailed way the symmetries of geometric objects) and in the theory of polynomial equations (developed by Galois, who showed how to associate a finite group with any polynomial equation in such a way that the structure of the group encodes information about the process of solving the equation).

The Revision Notes contain preliminary material for the module MTHM024/MTH714U, Group Theory (Masters/level-7) at Queen Mary. The preliminary material mostly occurs in the modules MTH4104 Introduction to Algebra and MTH6104 Algebraic Structures II. You can also find the material in most algebra textbooks, including my own book *Introduction to Algebra*, published by Oxford University Press.

Most of the material is given here without proof. I have included the proofs of Sylow's Theorem and the Jordan–Hölder Theorem because of their importance, and of the Fundamental Theorem of Finite Abelian Groups and the upper bound for the number of groups of order n since you may not have seen these before.

Material which is not in the above modules will be marked with $[***]$ in the text.

The module will begin with a review of this material.

1 Groups

This section defines groups, subgroups, homomorphisms, normal subgroups, and direct products: some of the basic ideas of group theory. The introduction to any kind of algebraic structure (e.g. rings) would look rather similar: we write down some axioms and make some deductions from them. But it is important to realise that mathematicians knew what was meant by a group long before they got around to writing down axioms. We return to this after discussing Cayley's Theorem.

1.1 Definition

A *group* consists of a set G with a binary operation $\circ$ on G satisfying the following four conditions:

Closure: For all $a, b \in G$, we have $a \circ b \in G$.

Associativity: For all $a, b, c \in G$, we have $(a \circ b) \circ c = a \circ (b \circ c)$.

Identity: There is an element $e \in G$ satisfying $e \circ a = a \circ e = a$ for all $a \in G$.

Inverse: For all $a \in G$, there is an element $a^* \in G$ satisfying $a \circ a^* = a^* \circ a = e$ (where e is as in the Identity Law).

The element e is the *identity element* of G. It is easily shown to be unique. In the Inverse Law, the element a^* is the *inverse* of a; again, each element has a unique inverse.

Strictly speaking, the Closure Law is not necessary, since a binary operation on a set necessarily satisfies it; but there are good reasons for keeping it in. The Associative Law is obviously the hardest to check from scratch.

A group is *abelian* if it also satisfies

Commutativity: For all $a, b \in G$, we have $a \circ b = b \circ a$.

Most of the groups in this course will be finite. The *order* of a finite group G, denoted $|G|$, is simply the number of elements in the group. A finite group can in principle be specified by a *Cayley table*, a table whose rows and columns are indexed by group elements, with the entry in row a and column b being $a \circ b$. Here are two examples.

$\circ$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

They are called the *cyclic group* and *Klein group* of order 4, and denoted by C_4 and V_4 respectively. Both of them are abelian.

Two groups $(G_1,\circ)$ and $(G_2,*)$ are called *isomorphic* if there is a bijective map f from G_1 to G_2 which preserves the group operation, in the sense that $f(a)*f(b) = f(a\circ b)$ for all $a,b \in G_1$. We write $(G_1,\circ) \cong (G_2,*)$, or simply $G_1 \cong G_2$, to denote that the groups G_1 and G_2 are isomorphic. From an algebraic point of view, isomorphic groups are "the same".

As an exercise, show that the two groups above are not isomorphic. The numbers of groups of orders $1,\ldots,8$ (up to isomorphism) are given in the following table:

Order	1	2	3	4	5	6	7	8
Number	1	1	1	2	1	2	1	5

We have given the definition rather formally. For most of the rest of the course, the group operation will be denoted by *juxtaposition* (that is, we write ab instead of $a\circ b$); the identity will be denoted by 1; and the inverse of a will be denoted by a^{-1}. Occasionally, the group operation will be $+$, the identity 0, and the inverse of a is $-a$.

If g and a are elements of a group G, we define the *conjugate* g^a of g by a to be the element $a^{-1}ga$. If we call two elements g,h conjugate if $h = g^a$ for some $a \in G$, then conjugacy is an equivalence relation (you should prove this as an exercise), and so the group is partitioned into *conjugacy classes*. (If a group is abelian, then two elements are conjugate if and only if they are equal.)

1.2 Subgroups

A subset H of a group G is called a *subgroup* if it forms a group in its own right (with respect to the same operation).

Since the associative law holds in G, it automatically holds in H; so we only have to check the closure, identity and inverse laws to ensure that H is a subgroup. (Since the associative law is the hardest to check directly, this observation means that, in order to show that a structure is a group, it is often better to identify it with a subgroup of a known group than to verify the group laws directly.)

We write "H is a subgroup of G" as $H \leq G$; if also $H \neq G$, we write $H < G$.

A subgroup H of a group G gives rise to two partitions of G:

Right cosets: sets of the form $Ha = \{ha : h \in H\}$;

Left cosets: sets of the form $aH = \{ah : h \in H\}$.

The easiest way to see that, for example, the right cosets form a partition of G is to observe that they are equivalence classes for the equivalence relation $\equiv$ defined by

$a \equiv b$ if and only if $ba^{-1} \in H$. In particular, this means that $Ha = Hb$ if and only if $b \in Ha$. In other words, any element of a coset can be used as its "representative".

The number of right cosets of H in G is called the *index* of H in G, written $|G : H|$. (The number of left cosets is the same.)

The cardinality of any right coset Ha of H is equal to $|H|$, since the map $h \mapsto ha$ is a bijection from H to Ha. So G is partitioned into classes of size $|H|$, and so $|G| = |G : H| \cdot |H|$. We conclude:

Theorem 1.1 (Lagrange's Theorem) *The order of a subgroup of a finite group G divides the order of G.*

The term "order" is also used with a different, though related, meaning in group theory. The *order* of an element a of a group G is the smallest positive integer m such that $a^m = 1$, if one exists; if no such m exists, we say that a has infinite order. Now, if a has order m, then the m elements $1, a, a^2, \ldots, a^{m-1}$ are all distinct and form a subgroup of G. Hence, by Lagrange's Theorem, we see that the order of any element of G divides the order of G.

Exercises

(a) Show that, if C is a right coset of H in G, then $C^{-1} = \{c^{-1} : c \in C\}$ is a left coset of H. Show also that the map $C \mapsto C^{-1}$ is a bijection between right and left cosets. Deduce that the numbers of left and right cosets are equal.

(b) Let H be a subgroup of G. Prove that $a^{-1}Ha = \{a^{-1}ha : h \in H\}$ is also a subgroup of G. (It is called a *conjugate* of H.)

(c) Prove that any right coset is a left coset (of a possibly different subgroup).

(d) Let H and K be subgroups of G, Show that $H \cap K$ is a subgroup. Give an example to show that $HK = \{hk : h \in H, k \in K\}$ is not always a subgroup.

1.3 Homomorphisms and normal subgroups

Let G_1 and G_2 be groups. A *homomorphism* from G_1 to G_2 is a map θ which preserves the group operation. We will write homomorphisms on the right of their arguments: the image of a under θ will be written as $a\theta$. Thus the condition for θ to be a homomorphism is

$$(ab)\theta = (a\theta)(b\theta) \text{ for all } a, b \in G_1,$$

where ab is calculated in G_1, and $(a\theta)(b\theta)$ in G_2.

With a homomorphism θ are associated two subgroups:

Image: $\text{Im}(\theta) = \{b \in G_2 : b = a\theta \text{ for some } a \in G_1\}$;

Kernel: $\text{Ker}(\theta) = \{a \in G_1 : a\theta = 1\}$.

A subgroup H of G is said to be a *normal subgroup* if it is the kernel of a homomorphism. Equivalently, H is a normal subgroup if its left and right cosets coincide: $aH = Ha$ for all $a \in G$. We write "H is a normal subgroup of G" as $H \trianglelefteq G$; if $H \neq G$, we write $H \triangleleft G$.

If H is a normal subgroup of G, we denote the set of (left or right) cosets by G/H. We define an operation on G/H by the rule

$$(Ha)(Hb) = Hab \text{ for all } a, b \in G.$$

It can be shown that the definition of this operation does not depend on the choice of the coset representatives, and that G/H equipped with this operation is a group, the *quotient group* or *factor group* of G by H.

Theorem 1.2 (First Isomorphism Theorem) *Let $\theta : G_1 \to G_2$ be a homomorphism. Then*

(a) $\text{Im}(\theta)$ *is a subgroup of* G_2*;*

(b) $\text{Ker}(\theta)$ *is a normal subgroup of* G_1*;*

(c) $G_1/\text{Ker}(\theta) \cong \text{Im}(\theta)$.

The moral of this theorem is: The best way to show that H is a normal subgroup of G (and to identify the quotient group) is to find a homomorphism from G to another group whose kernel is H.

There are two further isomorphism theorems which we will recall if and when we actually need them. This one is the most important!

1.4 Direct products

Here is a simple construction for producing new groups from old. We will see more elaborate versions later.

Let G_1 and G_2 be groups. We define the *direct product* $G_1 \times G_2$ to be the group whose underlying set is the Cartesian product of the two groups (that is, $G_1 \times G_2 = \{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$), with group operation given by

$$(g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2), \text{ for all } g_1, h_1 \in G_1, g_2, h_2 \in G_2.$$

It is not hard to verify the group laws, and to check that, if G_1 and G_2 are abelian, then so is $G_1 \times G_2$.

Note that $|G_1 \times G_2| = |G_1| \cdot |G_2|$. The Klein group V_4 is isomorphic to $C_2 \times C_2$.

The construction is easily extended to the direct product of more factors. The elements of $G_1 \times \cdots \times G_r$ are all r-tuples such that the ith component belongs to G_i; the group operation is "componentwise".

This is the "external" definition of the direct product. We also need to describe it "internally": given a group G, how do we recognise that G is isomorphic to a direct product of two groups G_1 and G_2?

The clue is the observation that, in the direct product $G_1 \times G_2$, the set

$$H_1 = \{(g_1, 1) : g_1 \in G_1\}$$

is a normal subgroup which is isomorphic to G_1; the analogously-defined H_2 is a normal subgroup isomorphic to G_2.

Theorem 1.3 *Let G_1, G_2, G be groups. Then G is isomorphic to $G_1 \times G_2$ if and only if there are normal subgroups H_1 and H_2 of G such that*

(a) $H_1 \cong G_1$ and $H_2 \cong G_2$;

(b) $H_1 \cap H_2 = \{1\}$ and $H_1 H_2 = G$.

(Here $H_1 H_2 = \{ab : a \in H_1, b \in H_2\}$.

There is a similar, but more complicated, theorem for recognising direct products of more than two groups.

1.5 Presentations[$***$]

Another method of describing a group is by means of a *presentation*, an expression of the form $G = \langle S \mid R \rangle$. Here S is a set of "generators" of the group, and R a set of "relations" which these generators must obey; the group G is defined to be the "largest" group (in a certain well-defined sense) generated by the given elements and satisfying the given relations.

An example will make this clear. $G = \langle a \mid a^4 = 1 \rangle$ is the cyclic group of order 4. It is generated by an element a satisfying $a^4 = 1$. While other groups (the cyclic group of order 2 and the trivial group) also have these properties, C_4 is the largest such group.

Similarly, $\langle a, b \mid a^2 = b^2 = 1, ab = ba \rangle$ is the Klein group of order 4.

While a presentation compactly specifies a group, it can be very difficult to get any information about the group from a presentation. To convince yourself of this, try to discover which group has the presentation

$$\langle a, b, c, d, e \mid ab = c, bc = d, cd = e, de = a, ea = b \rangle.$$

2 Examples of groups

In this section we consider various examples of groups: cyclic and abelian groups, symmetric and alternating groups, groups of units of rings, and groups of symmetries of regular polygons and polyhedra.

2.1 Cyclic groups

A group G is *cyclic* if it consists of all powers of some element $a \in G$. In this case we say that G is *generated* by a, and write $G = \langle a \rangle$.

If a has finite order n, then $\langle a \rangle = \{1, a, a^2, \dots, a^{n-1}\}$, and the order of $\langle a \rangle$ is equal to the order of a. An explicit realisation of this group is the set $\{e^{2\pi ik/n} : k = 0, 1, \dots, n-1\}$ of all complex nth roots of unity, with the operation of multiplication; another is the set $\mathbb{Z}/n\mathbb{Z}$ of integers mod n, with the operation of addition mod n. We denote the cyclic group of order n by C_n.

If a has infinite order, then $\langle a \rangle$ consists of all integer powers, positive and negative, of a. (Negative powers are defined by $a^{-m} = (a^{-1})^m$; the usual laws of exponents hold, for example, $a^{p+q} = a^p \cdot a^q$.) An explicit realisation consists of the set of integers, with the operation of addition. We denote the infinite cyclic group by C_∞.

The cyclic group C_n has a unique subgroup of order m for each divisor m of n; if $C_n = \langle a \rangle$, then the subgroup of order m is $\langle a^{n/m} \rangle$ (exercise). Similarly, $C_\infty = \langle a \rangle$ has a unique subgroup $\langle a^k \rangle$ of index k for each positive integer k.

A presentation for the cyclic group of order n is $C_n = \langle a \mid a^n = 1 \rangle$.

Proposition 2.1 *The only group of prime order p, up to isomorphism, is the cyclic group C_p.*

For if $|G| = p$, and a is a non-identity element of G, then the order of a divides (and so is equal to) p; so $G = \langle a \rangle$.

2.2 Abelian groups[$***$]

Cyclic groups are abelian; hence direct products of cyclic groups are also abelian. The converse of this is an important theorem, whose most natural proof uses concepts of rings and modules rather than group theory. We say that a group G is *finitely generated* if there is a finite set S which is contained in no proper subgroup of G (equivalently, every element of G can be written as some product of elements of S and their inverses).

Theorem 2.2 (Fundamental Theorem of Abelian Groups) *A finitely generated abelian group is a direct product of cyclic groups. More precisely, such a group can be written* *in the form*

$$C_{m_1} \times C_{m_2} \times \cdots \times C_{m_r} \times C_\infty \times \cdots \times C_\infty,$$

where $m_i \mid m_{i+1}$ for $i = 1, \dots, r-1$; two groups of this form are isomorphic if and only if the numbers $m_1, \dots, m_r$ and the numbers of infinite cyclic factors are the same for the two groups.

For example, there are three abelian groups of order 24 up to isomorphism:

$$C_{24}, \qquad C_2 \times C_{12}, \qquad C_2 \times C_2 \times C_6.$$

(Write 24 in all possible ways as the product of numbers each of which divides the next.)

The proof of this theorem for finite groups will be given in the appendix to this chapter.

2.3 Symmetric groups

Let Ω be a set. A *permutation* of Ω is a bijective map from Ω to itself. The set of permutations of Ω, with the operation of composition of maps, forms a group. (We write a permutation on the right of its argument, so that the composition $f \circ g$ means "first f, then g": that is, $\alpha(f \circ g) = (\alpha f)g$. Now as usual, we suppress the $\circ$ and simply write the composition as fg.)

The closure, identity and inverse laws hold because we have taken all the permutations; the associative law holds because composition of mappings is always associative: $\alpha(f(gh)) = \alpha((fg)h)$ (both sides mean "apply f, then g, then h"). The group of permutations of Ω is called the *symmetric group* on Ω, and is denoted by $\mathrm{Sym}(\Omega)$. In the case where $\Omega = \{1, 2, \dots, n\}$, we denote it more briefly by S_n. Clearly the order of S_n is $n!$.

A permutation of Ω can be written in *cycle notation*. Here is an example. Consider the permutation f given by

$$1 \mapsto 3, 2 \mapsto 6, 3 \mapsto 5, 4 \mapsto 1, 5 \mapsto 4, 6 \mapsto 2, 7 \mapsto 7$$

in the symmetric group S_7. Take a point of $\{1, \dots, 7\}$, say 1, and track its successive images under f; these are $1, 3, 5, 4$ and then back to 1. So we create a "cycle" $(1, 3, 5, 4)$. Since not all points have been considered, choose a point not yet seen, say 2. Its cycle is $(2, 6)$. The only point not visited is 7, which lies in a cycle of length 1, namely (7). So we write

$$f = (1, 3, 5, 4)(2, 6)(7).$$

If there is no ambiguity, we suppress the cycles of length 1. (But for the identity permutation, this would suppress everything; sometimes we write it as (1). The precise convention is not important.)

The *cycle structure* of a permutation is the list of lengths of cycles in its cycle decomposition. (A *list* is like a sequence, but the order of the entries is not significant; it is like a set, but elements can be repeated. The list [apple, apple, orange, apple, orange] can be summarised as "three apples and two oranges".)

Any permutation can be written in several different ways in cycle form:

- the cycles can be written in any order, so $(1,3,5,4)(2,6) = (2,6)(1,3,5,4)$.
- each cycle can start at any point, so $(1,3,5,4) = (3,5,4,1)$.

One can show that, if $a_1, a_2, \ldots$ are non-negative integers satisfying $\sum i a_i = n$, then the number of elements of S_n having a_i cycles of length i for $i = 1, 2, \ldots$ is

$$\frac{n!}{\prod i^{a_i} a_i!}$$

For if we write out the cycle notation with blanks for the entries, there are $n!$ ways of filling the blanks, and the denominator accounts for the ambiguities in writing a given notation in cycle form.

The significance of this number is the following:

Proposition 2.3 *Let Ω be a finite set. Then two elements of the symmetric group* $\mathrm{Sym}(\Omega)$ *are conjugate if and only if they have the same cycle structure.*

Hence the numbers just computed are the sizes of the conjugacy classes in S_n.

For example, the following list gives the cycle structures and conjugacy class sizes in S_4:

Cycle structure	Class size
$[4]$	6
$[3,1]$	8
$[2,2]$	3
$[2,1,1]$	6
$[1,1,1,1]$	1

The cycle structure of a permutation gives more information too.

Proposition 2.4 *The order of a permutation of a finite set is the least common multiple of the lengths of its disjoint cycles.*

Exercise What is the largest order of an element of S_{10}?

We define the *parity* of a permutation $g \in S_n$ to be the parity of $n - c(g)$, where $c(g)$ is the number of cycles of g (including cycles of length 1). We regard parity as an element of the group $\mathbb{Z}/2\mathbb{Z} = \{\text{even}, \text{odd}\}$ of integers mod 2 (the cyclic group of order 2).

Proposition 2.5 *For $n \geq 2$, parity is a homomorphism from S_n onto the group C_2.*

The kernel of this parity homomorphism is the set of all permutations with even parity. By the First Isomorphism Theorem, this is a normal subgroup of S_n with index 2 (and so order $n!/2$), known as the *alternating group*, and denoted by A_n. The above calculation shows that A_4 the set of permutations with cycle structures $[3,1]$, $[2,2]$ and $[1,1,1,1]$; there are indeed 12 such permutations.

2.4 General linear groups

The laws for abelian groups (closure, associativity, identity, inverse, and commutativity) will be familiar to you from other parts of algebra, notably ring theory and linear algebra. Any ring, or any vector space, with the operation of addition, is an abelian group.

More interesting groups arise from the multiplicative structure. Let R be a ring with identity. Recall that an element $u \in R$ is a *unit* if it has an inverse, that is, there exists $v \in R$ with $uv = vu = 1$. Now let $U(R)$ be the set of units of R. Since the product of units is a unit, the inverse of a unit is a unit, and the identity is a unit, and since the associative law holds for multiplication in a ring, we see that $U(R)$ (with the operation of multiplication) is a group, called the *group of units* of the ring R.

In the case where R is a field, the group of units consists of all the non-zero elements, and is usually called the *multiplicative group* of R, written $R^\times$.

A very interesting case occurs when R is the ring of linear maps from V to itself, where V is an n-dimensional vector space over a field $\mathbb{F}$. Then $U(R)$ consists of the invertible linear maps on V. If we choose a basis for V, then vectors are represented by n-tuples, so that V is identified with $\mathbb{F}^n$; and linear maps are represented by $n \times n$ matrices. So $U(R)$ is the group of invertible $n \times n$ matrices over $\mathbb{F}$. This is known as the *general linear group* of dimension n over $\mathbb{F}$, and denoted by $\mathrm{GL}(n, \mathbb{F})$.

Since we are interested in finite groups, we have to stop to consider finite fields here. The following theorem is due to Galois:

Theorem 2.6 (Galois' Theorem) *The order of a finite field is necessarily a prime power. If q is any prime power, then there is up to isomorphism a unique field of order q.*

For prime power q, this unique field of order q is called the *Galois field* of order q, and is usually denoted by $\mathrm{GF}(q)$ or $\mathbb{F}_q$. In the case where q is a prime number, $\mathrm{GF}(q)$ is the field of integers mod q. We shorten the notation $\mathrm{GL}(n,\mathrm{GF}(q))$ to $\mathrm{GL}(n,q)$.

For example, here are the addition and multiplication table of $\mathrm{GF}(4)$. We see that the additive group is the Klein group, while the multiplicative group is C_3.

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Exercise In the case $q = 2$, so that $\mathrm{GF}(2) = \{0,1\}$ is the field of integers mod 2, show that the invertible matrices are

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

Show that the group $\mathrm{GL}(2,2)$ of order 6 consisting of these matrices is isomorphic to the symmetric group S_3.

Note that $\mathrm{GL}(1,\mathbb{F})$ is just the multiplicative group $\mathbb{F}^\times$ of $\mathbb{F}$. From linear algebra, we recall that, for any $n \times n$ matrices A and B, we have

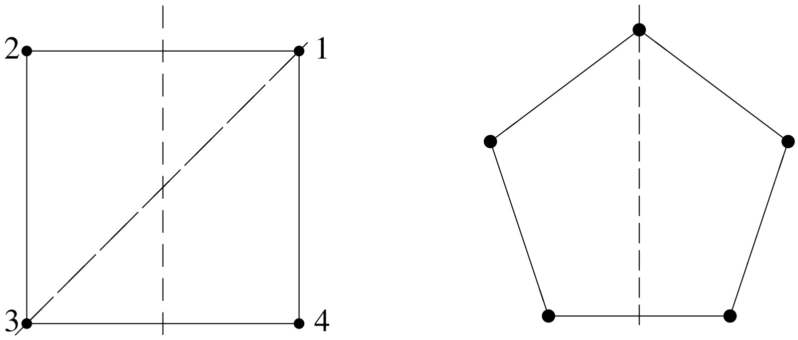
$$\det(AB) = \det(A)\det(B);$$

so the determinant map det is a homomorphism from $\mathrm{GL}(n,\mathbb{F})$ to $\mathbb{F}^\times$. The kernel of this homomorphism (the set of $n \times n$ matrices with determinant 1) is called the *special linear group*, and is denoted by $\mathrm{SL}(n,\mathbb{F})$. Again, if $\mathbb{F} = \mathrm{GF}(q)$, we abbreviate this to $\mathrm{SL}(n,q)$. Thus $\mathrm{SL}(n,q)$ is a normal subgroup of $\mathrm{GL}(n,q)$.

2.5 Dihedral and polyhedral groups

A *symmetry* of a figure in Euclidean space is a rigid motion (or the combination of a rigid motion and a reflection) of the space which carries the figure to itself. We can regard the rigid motion as a linear map of the real vector space, so represented by a matrix (assuming that the origin is fixed). Alternatively, if we number the vertices of the figure, then we can represent a symmetry by a permutation.

Let us consider the case of a regular polygon in the plane, say a regular n-gon. Here are drawings for $n = 4$ (the square) and $n = 5$ (the regular pentagon).



The n-gon has n rotational symmetries, through multiples of $2\pi/n$. In addition, there are n reflections about lines of symmetry. The behaviour depends on the parity of n. If n is even, there are two types of symmetry line; one joins opposite vertices, the other joins midpoints of opposite sides. If n is odd, then each line of symmetry joins a vertex to the midpoint of the opposite side.

The group of symmetries of the regular n-gon is called a *dihedral group*. We see that it has order $2n$, and contains a cyclic subgroup of order n consisting of rotations; every element outside this cyclic subgroup is a reflection, and has order 2. We denote this group by D_{2n} (but be warned that some authors call it D_n).

In the case $n = 4$, numbering the vertices $1,2,3,4$ in counterclockwise order from the top right as shown, the eight symmetries are

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

and the corresponding permutations are

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

(The ordering is: first the rotations, then the reflections in vertical, horizontal, and diagonal lines.)

The group D_{2n} has a presentation

$$D_{2n} = \langle a,b \mid a^n = 1, b^2 = 1, ba = a^{-1}b\rangle.$$

I won't prove this in detail (I haven't given a proper definition of a presentation!), but note that every product of as and bs can be reduced to the form a^m or $a^m b$ by using the relations, where $0 \leq m \leq n-1$, so there are at most $2n$ elements in the group given by the presentation. But the dihedral group does satisfy these relations.

There are only five regular polyhedra in three dimensions: the tetrahedron, cube, octahedron, dodecahedron, and icosahedron. Apart from the tetrahedron, they fall into two dual pairs: cube and octahedron, dodecahedron and icosahedron. If you take six vertices at the face centres of the cube, they are the vertices of an octahedron; and similarly the face centres of the octahedron are the vertices of a cube. A similar relation holds for the other pairs. So dual pairs have the same symmetry group. The following table describes the symmetry groups and the rotation groups (which are subgroups of index 2 in each case). As usual, C_n, S_n and A_n are the cyclic group of order n and the symmetric and alternating groups of degree n respectively.

Polyhedron	Rotation group	Symmetry group
Tetrahedron	A_4	S_4
Cube	S_4	$S_4 \times C_2$
Dodecahedron	A_5	$A_5 \times C_2$

2.6 Appendix: Finite abelian groups

Theorem 2.7 *Any finite abelian group G can be written in the form*

$$G \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r},$$

where $1 < n_1 \mid n_2 \mid \cdots \mid n_r$. Moreover, if also

$$G \cong C_{m_1} \times C_{m_2} \times \cdots \times C_{m_s},$$

where $1 < m_1 \mid m_2 \mid \cdots \mid m_s$, then $r = s$ and $n_i = m_i$ for $i = 1, 2, \ldots, r$.

Remark 1 We need the divisibility condition in order to get the uniqueness part of the theorem. For example,

$$C_2 \times C_6 \cong C_2 \times C_2 \times C_3;$$

the first expression, but not the second, satisfies this condition.

Remark 2 The proof given below is a kludge. There is an elegant proof of the theorem, which you should meet if you study Rings and Modules, or which you can read in a good algebra book. An abelian group can be regarded as a module over the ring $\mathbb{Z}$, and the Fundamental Theorem above is a special case of a structure theorem for finitely-generated modules over principal ideal domains.

We need a couple of preliminaries before embarking on the proof. The *exponent* of a group G is the smallest positive integer n such that $g^n = 1$ for all $g \in G$. Equivalently, it is the least common multiple of the orders of the elements of G. Note that the exponent of any subgroup or factor group of G divides the exponent of G; and, by Lagrange's Theorem, the exponent of a group divides its order.

For example, the symmetric group S_3 contains elements of orders 2 and 3, so its exponent is 6. However, it doesn't contain an element of order 6.

Lemma 2.8 *If G is abelian with exponent n, then G contains an element of order n.*

Proof Write $n = p_1^{a_1} \cdots p_r^{a_r}$, where $p_1, \ldots, p_r$ are distinct primes. Since n is the l.c.m. of orders of elements, there is an element with order divisible by $p_i^{a_i}$, and hence some power of it (say g_i) has order exactly $p_i^{a_i}$. Now in an abelian group, if two (or more) elements have pairwise coprime orders, then the order of their product is the product of their orders. So $g_1 \cdots g_r$ is the required element.

Proof of the Theorem We will prove the existence, but not the uniqueness. We use induction on $|G|$; so we suppose the theorem is true for abelian groups of smaller order than G.

Let n be the exponent of G; take a to be an element of order n, and let $A = \langle a \rangle$, so $A \cong C_n$. Let B be a subgroup of G of largest order subject to the condition that $A \cap B = \{1\}$. We *claim* that

$$AB = G.$$

Suppose this is proved. Since A and B are normal subgroups, it follows that $G = A \times B$. By induction, B can be expressed as a direct product of cyclic groups satisfying the divisibility condition; and the order of the largest one divides n, since n is the exponent of G. So we have the required decomposition of G.

Thus it remains to prove the claim. Suppose, for a contradiction, that $AB \neq G$. Then G/AB contains an element of prime order p dividing n; so an element x in this coset satisfies $x \notin AB$, $x^p \in AB$. Let $x^p = a^k b$ where $b \in B$.

Case 1: $p \mid k$. Let $k = pl$, and let $y = xa^{-l}$. Then $y \notin B$ (for if it were, then $x = ya^l \in AB$, contrary to assumption.) Now $B' = \langle B, y \rangle$ is a subgroup p times as large as B with $A \cap B' = \{1\}$, contradicting the definition of B. (If $A \cap B' \neq 1$, then $xa^{-l}b \in A$ for some $b \in B$, whence $x \in AB$.)

Case 2: If p does not divide k, then the order of x is divisible by a higher power of p than the order of a, contradicting the fact that the order of a is the exponent of G.

In either case we have a contradiction to the assumption that $AB \neq G$. So our claim is proved.

Using the uniqueness part of the theorem (which we didn't prove), we can in principle count the abelian groups of order n; we simply have to list all expressions for n as a product of factors each dividing the next. For example, let $n = 72$. The expressions are:

$$\begin{array}{l} 72 \\ 2\cdot 36 \\ 2\cdot 2\cdot 18 \\ 3\cdot 24 \\ 6\cdot 12 \\ 2\cdot 6\cdot 6 \end{array}$$

So there are six abelian groups of order 72, up to isomorphism.

Exercise Let $A(n)$ be the number of abelian groups of order n.

(a) Let p be a prime and a a positive integer. Prove that $A(p^a)$ is the number of *partitions* of a, that is, the number of expressions for a as a sum of positive integers, where order is not important).

(b) Show that $A(p^a) \le 2^{a-1}$ for $a \ge 1$ and p prime. [*Hint:* the number of expressions for a as a sum of positive integers, where order is important, is 2^{a-1}.]

(c) Let $n = p_1^{a_1} \cdots p_r^{a_r}$, where $p_1, \ldots, p_r$ are distinct primes and $a_1, \ldots, a_r$ are positive integers. Show that

$$A(n) = A(p_1^{a_1}) \cdots A(p_r^{a_r}).$$

(d) Deduce that $A(n) \le n/2$ for all $n > 1$.