Queen Mary
University of London

MTHM024/MTH714U Group Theory

Revision Notes Autumn 2010

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).

These notes contain preliminary material for the course MTHM024/MTH714U, Group Theory (Masters/level 7) at Queen Mary. The preliminary material mostly occurs in the courses MTH4104 Introduction to Algebra, MTH5100 Algebraic Structures I, and MTH6104 Algebraic Structures II. You can find notes the first two of these courses on the lecturers' web pages (Dr Tomašić and Professor Wilson). Older versions of these notes are on my web page, while Professor Bailey has notes for Algebraic Structures II. You can also find the material in any algebra textbook, including my own book *Introduction to Algebra*, published by Oxford University Press.

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

The course 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, 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 $\equiv_R$ 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 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: $\mathrm{Im}(\theta) = \{b \in G_2 : b = a\theta \text{ for some } a \in G_1\}$;

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

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

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

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

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 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

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

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 $\langle a \rangle = \{1, a, a^2, \ldots, a^{n-1}\}$, and the order of $\langle a \rangle$ is equal to the order of a. An explicit realisation of this group is the set $\{e^{2\pi ik/n} : k = 0, 1, \ldots, n-1\}$ 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 $\langle a^{n/m} \rangle$. 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 is a 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 $i = 1, \ldots, r-1$; two groups of this form are isomorphic if and only if the numbers $m_1, \ldots, m_r$ 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.)

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 $\Omega = \{1, 2, \ldots, n\}$, 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 $\{1, \ldots, 7\}$, 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 $\sum ia_i = n$, 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 *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 is the least common multiple of the lengths of its 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 types $[3,1]$, $[2,2]$ 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 $\mathrm{GF}(q)$. 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

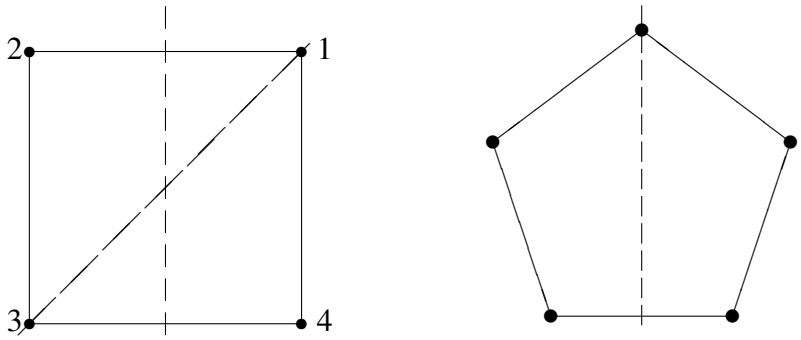
$$\det(AB) = \det(A)\det(B);$$

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 $\mathrm{SL}(n,q)$.

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 clockwise order from the top left 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 $0 \le m \le n-1$, so there are just $2n$ 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	$A_5 \times C_2$

3 Group actions

A group is an abstract object, and often we need to represent it in a more concrete way, for example, by permutations of a set, or by matrices over a field. We want the multiplication of the permutations or matrices to reflect the operation in the given group; that is to say, we want to have a homomorphism from the group to either a symmetric group or a general linear group. Using a homomorphism allows us a little extra flexibility: it is possible that the homomorphism is not injective, so that different group elements are represented by the same permutation or matrix.

In this chapter we look at representations by permutations, describe their structure, and look briefly at some other counting problems which are developed further in Enumerative Combinatorics.

3.1 Definition

An *action* of a group G on a set Ω is a homomorphism from G to the symmetric group $\mathrm{Sym}(\Omega)$. In other words, to each group element we associate a permutation, and the product of group elements is associated with the composition of the corresponding permutations. We will always have in mind a fixed action θ; so $g\theta$ is a permutation of Ω, and we can talk about $\alpha(g\theta)$ for $\alpha \in \Omega$. To simplify notation, we suppress the name of the action, and simply write αg for the image of α under the permutation corresponding to g.

Alternatively, we can define an action of G on Ω as a map μ from $\Omega \times G$ to Ω satisfying the two laws

(a) $\mu(\mu(\alpha,g),h) = \mu(\alpha,gh)$ for all $g,h \in G$, $\alpha \in \Omega$.

(b) $\mu(\alpha,1) = \alpha$ for all $\alpha \in \Omega$.

Again we simplify notation by suppressing the name μ: we write $\mu(\alpha,g)$ as αg. Then (a) says that $(\alpha g)h = \alpha(gh)$; it follows from (a) and (b) that the map $\alpha \mapsto \alpha g$ is a permutation of Ω (its inverse is $\alpha \mapsto \alpha g^{-1}$), and so we do indeed have a homomorphism from G to $\mathrm{Sym}(\Omega)$.

Example Let $G = S_4$, and let Ω be the set of three partitions of $\{1,2,3,4\}$ into two sets of size 2. Any permutation in G can be used to transform the partitions: for example, $g = (1,3,4)$ maps $12|34 \mapsto 23|14 \mapsto 13|24$. This gives an action of G on a set of size 3, that is, a homomorphism from S_4 to S_3. It is easily checked that this homomorphism is onto, and that its kernel is the Klein group V_4 consisting of the identity, $(1,2)(3,4)$, $(1,3)(2,4)$ and $(1,4)(2,3)$. Thus V_4 is a normal subgroup of S_4, and $S_4/V_4 \cong S_3$ (by the First Isomorphism Theorem).

Example There are several ways of making a group act on itself (that is, we take $\Omega = G$):

Right multiplication: $\mu(x,g) = xg$.

Left multiplication: $\mu(x,g) = g^{-1}x$ (the inverse is needed to ensure that acting with g and then with h is the same as acting with gh).

Conjugation: $\mu(x,g) = g^{-1}xg$.

The first of these actions has an important consequence. The action by right multiplication is *faithful*: if $\mu(x,g) = \mu(x,h)$ for all $x \in G$, then $g = h$. This means that the action homomorphism from G into $\mathrm{Sym}(G)$ is one-to-one (its kernel is the identity). By the First Isomorphism Theorem, the image of this map is a subgroup of $\mathrm{Sym}(G)$ which is isomorphic to G. Hence:

Theorem 3.1 (Cayley's Theorem) *Every group is isomorphic to a subgroup of some symmetric group.*

As well as motivating the study of symmetric groups and their subgroups, this theorem has historical importance. As noted earlier, group theory had existed as a mathematical subject for a century before the group laws were written down by Walther von Dyck in 1882. In those days the word "group" meant what we would now describe as a *permutation group* or *transformation group*, that is, a subgroup of the symmetric group. (In detail, a group was a set of transformations of a set which is closed under composition, contains the identity transformation, and contains the inverse of each of its elements. Since composition of transformations is associative, we see that every transformation group is a group in the modern sense. In the other direction, Cayley's theorem shows that every group is isomorphic to a transformation group; so, despite the change in foundations, the actual subject matter of group theory didn't change at all!

Finally, we note that the permutation group given by Cayley's Theorem can be written down from the Cayley table of G: the permutation of G corresponding to the element $g \in G$ is just the column labelled g of the Cayley table. Referring back to the two Cayley tables on page 2, we see that as permutation groups

$$\begin{aligned} C_4 &= \{1,(e,a,b,c),(e,b)(a,c),(e,c,b,a)\}, \\ V_4 &= \{1,(e,a)(b,c),(e,b)(a,c),(e,c)(a,b)\}. \end{aligned}$$

Both these groups are abelian so we could have used rows rather than columns to get the same result; but in general it makes a difference.

3.2 Orbits and stabilisers

Let G act on Ω. We define a relation $\equiv$ on Ω by the rule that $\alpha \equiv \beta$ if there is an element $g \in G$ such that $\alpha g = \beta$. Then $\equiv$ is an equivalence relation. (It is instructive to see how the reflexive, symmetric and transitive laws for $\equiv$ follow from the identity, inverse and closure laws for G.) The equivalence classes of this relation are called *orbits*; we say that the action is *transitive* (or that G acts *transitively* on Ω) if there is just one orbit.

We denote the orbit containing a point α by $\mathrm{Orb}_G(\alpha)$.

For example, the action of G on itself by right multiplication is transitive; in the action by conjugation, the orbits are the conjugacy classes.

Given a point α, the *stabiliser* of α is the set of elements of G which map it to itself:

$$\mathrm{Stab}_G(\alpha) = \{g \in G : \alpha g = \alpha\}.$$

Theorem 3.2 (Orbit-Stabiliser Theorem) *Let G act on Ω, and choose $\alpha \in \Omega$. Then $\mathrm{Stab}_G(\alpha)$ is a subgroup of G; and there is a bijection between the set of right cosets of $\mathrm{Stab}_G(\alpha)$ in G and the orbit $\mathrm{Orb}_G(\alpha)$ containing α.*

It follows from the Orbit-Stabiliser Theorem that $|\mathrm{Stab}_G(\alpha)| \cdot |\mathrm{Orb}_G(\alpha)| = |G|$.

The correspondence works as follows. Given $\beta \in \mathrm{Orb}_G(\alpha)$, by definition there exists $h \in G$ such that $\alpha h = \beta$. Now it can be checked that the set of all elements mapping α to β is precisely the right coset $(\mathrm{Stab}_G(\alpha))h$.

Every subgroup of G occurs as the stabiliser in a suitable transitive action of G. For let H be a subgroup of G. Let Ω be the set of all right cosets of H in G, and define an action of G on Ω by, formally, $\mu(Hx, g) = Hxg$. (Informally we would write $(Hx)g = Hxg$, but this conceals the fact that $(Hx)g$ means the result of acting on the point Hx with the element g, not just the product in the group, though in fact it comes to the same thing!) It is readily checked that this really is an action of G, that it is transitive, and that the stabiliser of the coset $H1 = H$ is the subgroup H.

So the Orbit-Stabiliser Theorem can be regarded as a refinement of Lagrange's Theorem.

3.3 The Orbit-Counting Lemma

The Orbit-Counting Lemma is a formula for the number of orbits of G on Ω, in terms of the numbers of fixed points of all the permutations in G. Given an action of G on Ω, and $g \in G$, let $\mathrm{fix}(g)$ be the number of fixed points of g (strictly, of the permutation of Ω induced by g). The Lemma says that the number of orbits is the average value of $\mathrm{fix}(g)$, for $g \in G$.

Theorem 3.3 (Orbit-Counting Lemma) *Let G act on Ω. Then the number of orbits of G on Ω is equal to*

$$\frac{1}{|G|}\sum_{g\in G}\mathrm{fix}(g).$$

The proof illustrates the Orbit-Stabiliser Theorem. We form a bipartite graph with vertex set $\Omega \cup G$; we put an edge between $\alpha \in \Omega$ and $g \in G$ if $\alpha g = \alpha$. Now we count the edges of this graph.

On one hand, every element $g \in G$ lies in $\mathrm{fix}(g)$ edges; so the number of edges is $\sum_{g\in G}\mathrm{fix}(g)$.

On the other hand, the point α lies in $|\mathrm{Stab}_G(\alpha)|$ edges; so the number of edges passing through points of $\mathrm{Orb}_G(\alpha)$ is $|\mathrm{Orb}_G(\alpha)| \cdot |\mathrm{Stab}_G(\alpha)| = |G|$, by the Orbit-Stabiliser Theorem. So each orbit accounts for $|G|$ edges, and the total number of edges is equal to $|G|$ times the number of orbits.

Equating the two expressions and dividing by $|G|$ gives the result.

Example The edges of a regular pentagon are coloured red, green and blue. How many different ways can this be done, if two colourings which differ by a rotation or reflection of the pentagon are regarded as identical?

The question asks us to count the orbits of the dihedral group D_{10} (the group of symmetries of the pentagon) on the set Ω of colourings with three colours. There are 3^5 colourings altogether, all fixed by the identity. For a colouring to be fixed by a non-trivial rotation, all the edges have the same colour; there are just three of these. For a colouring to be fixed by a reflection, edges which are images of each other under the reflection must get the same colour; three colours can be chosen independently, so there are 3^3 such colourings.

Since there are four non-trivial rotations and five reflections, the Orbit-Counting Lemma shows that the number of orbits is

$$\frac{1}{10}(1\cdot 243 + 4\cdot 3 + 5\cdot 27) = 39.$$

4 Sylow's Theorem

Sylow's Theorem is arguably the most important theorem about finite groups, so I am going to include a proof.

To begin, let's ask the question: is the converse of Lagrange's Theorem true? In other words, if G is a group of order n, and m is a divisor of n, does G necessarily contain a subgroup of order m? We note that this statement is true for cyclic groups. As an exercise, verify it for abelian groups (using the Fundamental Theorem of Abelian Groups).

In fact it is not true in general. Let G be the alternating group A_4. Then G is a group of order 12, containing the identity, three elements with cycle type $[2,2]$, and eight elements with cycle type $[3,1]$. We claim that G has no subgroup of order 6. Such a subgroup must contain an element of order 3, since there are only four elements not of order 3; also it must contain an element of order 2, since elements of order 3 come in inverse pairs, both or neither of which lie in any subgroup, so there are an even number of elements not of order 3, one of which is the identity. But it is not hard to show that, if you choose any element of order 2 and any element of order 3, together they generate the whole group.

4.1 Statement

Cauchy proved the first partial converse to Lagrange's Theorem:

Theorem 4.1 (Cauchy's Theorem) *Suppose that the prime p divides the order of the group G. Then G contains an element of order p.*

Sylow's Theorem is a far-reaching extension of Cauchy's. It is often stated as three separate theorems; but I will roll it into one here.

Theorem 4.2 (Sylow's Theorem) *Let G be a group of order $p^a \cdot m$, where p is a prime not dividing m. Then*

(a) G contains subgroups of order p^a, any two of which are conjugate;

(b) any subgroup of G of p-power order is contained in a subgroup of order p^a;

(c) the number of subgroups of order p^a is congruent to 1 mod p and divides m.

Subgroups of order p^a of G, that is, subgroups whose order is the largest power of p dividing $|G|$, are called *Sylow p-subgroups* of G.

The smallest positive integer which has a proper divisor whose order is not a prime power is 12; and we have seen that the group A_4 of order 12 has no subgroup of order 6. So Sylow's theorem cannot be improved in general!

4.2 Proof

This is quite a substantial proof; you may skip it at first reading. You can find different proofs discussed in some of the references. The crucial tool is the Orbit-Stabiliser Theorem, which is used many times, sometimes without explicit mention.

The proof uses two different actions of G. First, we consider the action on the set Ω consisting of all subsets of G of cardinality p^a, by right multiplication: $\mu(X,g) = Xg = \{xg : x \in X\}$. Each orbit consists of sets covering all elements of G. (For, if $x \in X$, and y is any element, then $y \in X(x^{-1}y)$.) So there are two kinds of orbits:

(A) orbits of size m, forming a partition of G;

(B) orbits of size greater than m.

Now by the Orbit-Stabiliser Theorem, the size of any orbit divides $|G|$; so an orbit of type (B) must have size divisible by p. But $|\Omega| = \binom{p^a m}{p^a}$ is not a multiple of p (this is a number-theoretic exercise); so there must be orbits of type (A). Again by the Orbit-Stabiliser Theorem, the stabiliser of a set in an orbit of type (A) is a subgroup of order p^a (and the orbit consists of its right cosets). This shows that subgroups of order p^a exist.

Now consider a different action of G, on the set Δ of all Sylow subgroups of G by conjugation (that is, $\mu(P,g) = g^{-1}Pg$).

We first observe that, if Q is a subgroup of G of p-power order which stabilises a Sylow subgroup P in this action, then $Q \leq P$; for otherwise PQ is a subgroup of order $|P| \cdot |Q|/|P \cap Q|$, a power of p strictly greater than p^a, which is not possible. (Further discussion of this point is at the end of this section.)

Take $P \in \Delta$. Then P stabilises itself, but no other Sylow subgroup (by the preceding remark), so all other orbits of P have size divisible by p. We conclude that $|\Delta|$, the number of Sylow p-subgroups, is congruent to 1 mod p.

Now G-orbits are unions of P-orbits, so the G-orbit containing P has size congruent to 1 mod p, and every other G-orbit has size congruent to 0 mod p. But P was arbitrary; so there is only a single orbit, whence all the Sylow p-subgroups are conjugate. The number of them is $|G : N|$, where $N = \mathrm{Stab}_G(P)$; since $P \leq N$, this number divides $|G : P| = m$.

Finally, if Q is any subgroup of p-power order, then the orbits of Q on Δ all have p-power size; since $|\Delta|$ is congruent to 1 mod p, there must be an orbit $\{P\}$ of size 1, and so $Q \leq P$ by our earlier remark.

All parts of the theorem are now proved.

Here is a two-part lemma which we made use of in the above proof. The proof is an exercise. If H is a subgroup of G, we say that the element $g \in G$ *normalises*

H if $g^{-1}Hg = H$; and we say that the subgroup K *normalises* H if all its elements normalise H. Thus H is a normal subgroup of G if and only if G normalises H. By HK we mean the *subset* $\{hk : h \in H, k \in K\}$ of G (not in general a subgroup).

Lemma 4.3 *Let H and K be subgroups of G. Then*

(a) $|HK| = |H| \cdot |K| / |H \cap K|$;

(b) if K normalises H, then HK is a subgroup of G.

4.3 Applications

There are many applications of Sylow's Theorem to the structure of groups. Here is one, the determination of all groups whose order is the product of two distinct primes.

Theorem 4.4 *Let G be a group of order pq, where p and q are primes with $p > q$.*

(a) If q does not divide $p-1$, then G is cyclic.

(b) If q divides $p-1$, then there is one type of non-cyclic group, with presentation

$$G = \langle a, b \mid a^p = 1, b^q = 1, b^{-1}ab = a^k \rangle$$

for some k satisfying $k^q \equiv 1$ mod p, $k \not\equiv 1$ mod p.

Proof Let P be a Sylow p-subgroup and Q a Sylow q-subgroup. Then P and Q are cyclic groups of prime orders p and q respectively. The number of Sylow p-subgroups is congruent to 1 mod p and divides q; since $q < p$, there is just one, so $P \lhd G$.

Similarly, the number of Sylow q-subgroups is 1 or p, the latter being possible only if $p \equiv 1 \bmod q$.

Suppose there is a unique Sylow q-subgroup. Let P and Q be generated by elements a and b respectively. Then $b^{-1}ab = a^k$ and $a^{-1}ba = b^l$ for some r, s. So $a^{k-1} = a^{-1}b^{-1}ab = b^{-l+1}$. This element must be the identity, since otherwise its order would be both p and q, which is impossible. So $ab = ba$. Then we see that the order of ab is pq, so that G is the cyclic group generated by ab.

In the other case, q divides $p-1$, and we have $b^{-1}ab = a^k$ for some k. Then an easy induction shows that $b^{-s}ab^s = a^{k^s}$. Since $b^q = 1$ we see that $k^q \equiv 1 \bmod p$. There are exactly q solutions to this equation; if k is one of them, the others are powers of k, and replacing b by a power of itself will have the effect of raising k to the appropriate power. So all these different solutions are realised within the same group.

In particular, the only non-cyclic group of order $2p$, where p is an odd prime, is the dihedral group $\langle a, b \mid a^p = 1, b^2 = 1, b^{-1}ab = a^{-1} \rangle$.

There are two groups of order 21, the cyclic group and the group

$$\langle a, b \mid a^7 = 1, b^3 = 1, b^{-1}ab = a^2 \rangle;$$

in this group, if we replace b by b^2, we replace the exponent 2 by 4 in the last relation.

5 Composition series

A non-trivial group G always has at least two normal subgroups: the whole group G, and the identity subgroup $\{1\}$. We call G *simple* if there are no other normal subgroups. Thus, a cyclic group of prime order is simple. We will see that there are other simple groups.

In this section we will discuss the Jordan–Hölder Theorem. This theorem shows that, in a certain sense, simple groups are the "building blocks" of arbitrary finite groups. In order to describe any finite group, we have to give a list of its "composition factors" (which are simple groups), and describe how these blocks are glued together to form the group.

5.1 The Jordan–Hölder Theorem

Suppose that the group G is not simple: then it has a normal subgroup N which is neither $\{1\}$ nor G, so the two groups N and G/N are smaller than G. If either or both of these is not simple, we can repeat the procedure. We will end up with a list of simple groups. These are called the *composition factors* of G.

More precisely, a *composition series* for G is a sequence of subgroups

$$\{1\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_r = G,$$

so that each subgroup is normal in the next (as shown), and the quotient group G_{i+1}/G_i is simple for $i = 0, 1, \ldots, r-1$.

We can produce a composition series by starting from the series $\{1\} \lhd G$ and refining it as follows. If we have $G_i \lhd G_{i+1}$ and G_{i+1}/G_i is not simple, let it have a normal subgroup N; then there is a subgroup N^* of G_{i+1} containing G_i by the Correspondence Theorem, with $G_i \lhd N^* \lhd G_{i+1}$, and we may insert another term in the sequence.

(The *Correspondence Theorem*, sometimes called the *Second Isomorphism Theorem*, asserts that, if A is a normal subgroup of B, then there is a bijection between subgroups of B/A and subgroups of B containing A, under which normal subgroups correspond to normal subgroups. The bijection works in the obvious way: if $C \leq B/A$, then elements of C are cosets of A, and the union of all these cosets gives the corresponding subgroup C^* of B containing A.)

Now, given a composition series for G, say

$$\{1\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_r = G,$$

we have r simple groups G_{i+1}/G_i. We are interested in them up to isomorphism; the *composition factors* of G are the isomorphism types. (We think of them as forming a list, since the same composition factor can occur more than once.)

For a simple example, let $G = C_{12}$. Here are three composition series:

$$\{1\} \lhd C_2 \lhd C_4 \lhd C_{12}$$
$$\{1\} \lhd C_2 \lhd C_6 \lhd C_{12}$$
$$\{1\} \lhd C_3 \lhd C_6 \lhd C_{12}$$

The composition factors are C_2 (twice) and C_3, but the order differs between series.

Theorem 5.1 (Jordan–Hölder Theorem) *Any two composition series for a finite group G give rise to the same list of composition factors.*

Note that the product of the orders of the composition factors of G is equal to the order of G.

5.2 Groups of prime power order

In this section, we will see that a group has order a power of the prime p if and only if all of its composition factors are the cyclic group of order p.

One way round this is clear, since the order of G is the product of the orders of its composition factors. The other depends on the following definition and theorem. The *centre* of a group G, denoted by $Z(G)$, is the set of elements of G which commute with everything in G:

$$Z(G) = \{g \in G : gx = xg \text{ for all } x \in G\}.$$

It is clearly a normal subgroup of G.

Theorem 5.2 *Let G be a group of order p^n, where p is prime and $n > 0$. Then*

(a) $Z(G) \neq \{1\}$;

(b) G has a normal subgroup of order p.

To prove this, we let G act on itself by conjugation. By the Orbit-Stabiliser Theorem, each orbit has size a power of p, and the orbit sizes sum to p^n. Now by definition, $Z(G)$ consists of all the elements which lie in orbits of size 1. So the number of elements not in $Z(G)$ is divisible by p, whence the number in $Z(G)$ is also. But there is at least one element in $Z(G)$, namely the identity; so there are at least p such elements.

Now, if g is an element of order p in $Z(G)$, then $\langle g \rangle$ is a normal subgroup of G of order p.

This proves the theorem, and also finds the start of a composition series: we take G_1 to be the subgroup given by part (b) of the theorem. Now we apply induction to G/G_1 to produce the entire composition series. We see that all the composition factors have order p.

We note in passing the following result:

Proposition 5.3 *Let p be prime.*

(a) Every group of order p^2 is abelian.

(b) There are just two such groups, up to isomorphism

For let $|G| = p^2$. If $|Z(G)| = p^2$, then certainly G is abelian, so suppose that $|Z(G)| = p$. Then $G/Z(G)$ is a cyclic group of order p, generated say by the coset $Z(G)a$; then every element of G has the form za^i, where $z \in Z(G)$ and $i = 0, 1, \ldots, p-1$. By inspection, these elements commute.

Finally, the Fundamental Theorem of Abelian Groups shows that there are just two abelian groups of order p^2, namely C_{p^2} and $C_p \times C_p$.

This theorem shows that the list of composition factors of a group does not determine the group completely, since each of these two groups has two composition factors C_p. So the "glueing" process is important too. In fact, worse is to come. The number of groups of order p^n grows very rapidly as a function of n. For example, it is known that the number of groups of order $1024 = 2^{10}$ is more than fifty billion; all of these groups have the same composition factors (namely C_2 ten times)!

Remark At this point, we have determined the structure of all groups whose order has at most two prime factors (equal or different); so we know all the groups of order less than 16 except for the orders 8 and 12.

5.3 Soluble groups

A finite group G is called *soluble* if all its composition factors are cyclic of prime order.

Historically, soluble groups arose in the work of Galois, who was considering the problem of solubility of polynomial equations by radicals (that is, the existence of formulae for the roots like the formula $(-b \pm \sqrt{b^2 - 4ac})/2a$ for the roots of a quadratic. It had already been proved by Ruffini and Abel that no such formula exists in general for polynomials of degree 5. Galois associated with each polynomial a group, now called the *Galois group* of the polynomial, and showed that the polynomial is soluble by radicals if and only if its Galois group is a soluble group. The result on degree 5 comes about because the smallest simple group which is not cyclic of prime order (and, hence, the smallest insoluble group) is the alternating group A_5, as we shall see.

I will not discuss soluble groups in detail here, but note just one theorem.

Theorem 5.4 *A finite group G is soluble if and only if it has a series of subgroups*

$$\{1\} < H_1 < H_2 < \cdots < H_s = G$$

such that each H_i is a normal subgroup of G, and each quotient H_{i+1}/H_i is abelian for $i = 0, 1, \ldots, s-1$.

(Note that in the definition of a composition series, each subgroup is only required to be normal in the next, not in the whole group.)

This theorem is important because the definition we gave of a soluble group makes no sense in the infinite case. So instead, we use the condition of the theorem as the *definition* of solubility in the case of infinite groups.

5.4 Simple groups

In the course, we will spend some time discussing simple groups other than cyclic groups of prime order. Here, for a starter, is the argument showing that they exist.

Theorem 5.5 *The alternating group A_5 is simple.*

The group $G = A_5$ consists of the even permutations of $\{1, \ldots, 5\}$. (Recall that even permutations are those for which the number of cycles is congruent to the degree mod 2.) Their cycle types and numbers are given in the following table.

Cycle type	Number
$[1,1,1,1,1]$	1
$[1,2,2]$	15
$[1,1,3]$	20
$[5]$	24

Since a normal subgroup must be made up of entire conjugacy classes, our next task is to determine these.

It is easy to see that all the elements of order 2 are conjugate, as are all those of order 3. The elements of order 5 are not all conjugate, but the subgroups of order 5 are (by Sylow's Theorem), and a potential normal subgroup must therefore either contain all or none of them.

So if N is a normal subgroup of A_5, then $|N|$ is the sum of some of the numbers 1, 15, 20, 24, certainly including 1 (since it must contain the identity), and must divide 60 (by Lagrange's Theorem).

It is straightforward to see that the only possibilities are $|N| = 1$ and $|N| = 60$. So A_5 is simple.

Exercise Show that there is no simple group of non-prime order less than 60.

In perhaps the greatest mathematical achievement of all time, all the finite simple groups have been determined. We will say more about this in the course. But, by way of introduction, they fall into four types:

(a) cyclic groups of prime order;

(b) alternating groups A_n (these are simple for all $n \geq 5$);

(c) the so-called *groups of Lie type*, which are closely related to certain matrix groups over finite fields — for example, if $G = \mathrm{SL}(n,q)$, then $G/Z(G)$ is simple for all $n \geq 2$ and all prime powers q except for $n = 2$ and $q = 2$ or $q = 3$;

(d) twenty-six so-called *sporadic groups*, most of which are defined as symmetry groups of various algebraic or combinatorial configurations.

The proof of this simply-stated theorem is estimated to run to about 10000 pages!

This theorem means that, if we regard the Jordan–Hölder theorem as reducing the description of finite groups to finding their composition factors and glueing them together, then the first part of the problem is solved, and only the second part remains open.