# Notes on finite group theory

Peter J. Cameron

October 2013

# Preface

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 are based on a Masters course I gave at Queen Mary, University of London. Of the two lecturers who preceded me, one had concentrated on finite soluble groups, the other on finite simple groups; I have tried to steer a middle course, while keeping finite groups as the focus. The notes do not in any sense form a textbook, even on finite group theory.

Finite group theory has been enormously changed in the last few decades by the immense Classification of Finite Simple Groups. The most important structure theorem for finite groups is the Jordan–Hölder Theorem, which shows that any finite group is built up from finite simple groups. If the finite simple groups are the building blocks of finite group theory, then extension theory is the mortar that holds them together, so I have covered both of these topics in some detail: examples of simple groups are given (alternating groups and projective special linear groups), and extension theory (via factor sets) is developed for extensions of abelian groups.

In a Masters course, it is not possible to assume that all the students have reached any given level of proficiency at group theory. So the first chapter of these notes, "Preliminaries", takes up nearly half the total. This starts from the definition of a group and includes subgroups and homomorphisms, examples of groups, group actions, Sylow's theorem, and composition series. This material is mostly without proof, but I have included proofs of some of the most important results, including the theorems of Sylow and Jordan–Hölder and the Fundamental Theorem of Finite Abelian Groups.

The fourth chapter gives some basic information about nilpotent and soluble groups. Much more could be said here; indeed, it could be argued that a goal of finite group theory is to understand general finite groups as well as we now understand finite soluble groups.

The final chapter contains solutions to some of the exercises.

I am grateful to students and colleagues for many helpful comments, and especially to Jiajie Wang, whose project on Sylow's Theorem led me to realise that Sylow's original proof of his first theorem is still the best!

# Contents

# Chapter 1

# Preliminaries

## 1.1 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.

### 1.1.1 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”.

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 $a^{-1}$. Sometimes the group operation will be $+$, the identity 0, and the inverse of $a$ is $-a$. (This convention is particularly used when studying abelian groups.)

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.)

### 1.1.2 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 1.1.1 (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 $1, a, a^2, \dots, a^{m-1}$ 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 $G$.

### 1.1.3 Homomorphisms and normal subgroups

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

*Image*: $\mathrm{Im}(\theta) = \{b \in G_2 : b = a\theta$ 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 1.1.2 (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!

### 1.1.4 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 $i$th 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 1.1.3** *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.

## 1.1.5 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

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

## 1.2 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.

### 1.2.1 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 $\{\mathrm{e}^{2\pi\mathrm{i}k/n} : k = 0, 1, \dots, n-1\}$ of all complex $n$th 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 $C_\infty$.

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 1.2.1** *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 $G = \langle a \rangle$.

### 1.2.2 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 1.2.2 (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.)

**Proof of the FTAG** We prove the theorem in the special case of finite abelian groups.

**Theorem 1.2.3** *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 1.2.4** *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.

### 1.2.3 Symmetric groups

Let $\Omega$ be a set. A *permutation* of $\Omega$ is a bijective map from $\Omega$ to itself. The set of permutations of $\Omega$, 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 $\Omega$ is called the *symmetric group* on $\Omega$, 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 $\Omega$ 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 $[\text{apple}, \text{apple}, \text{orange}, \text{apple}, \text{orange}]$ 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 permutation in cycle form.

The significance of this number is the following:

**Proposition 1.2.5** *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 1.2.6** *The order of a permutation is the least common multiple of the lengths of its cycles.*

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 1.2.7** *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.

### 1.2.4 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 1.2.8 (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 GF$(4)$. We see that the additive group is the Klein group, while the multiplicative group is $C_3$.

| $+$ | $0$ | $1$ | $\alpha$ | $\beta$ |
|---|---|---|---|---|
| $0$ | $0$ | $1$ | $\alpha$ | $\beta$ |
| $1$ | $1$ | $0$ | $\beta$ | $\alpha$ |
| $\alpha$ | $\alpha$ | $\beta$ | $0$ | $1$ |
| $\beta$ | $\beta$ | $\alpha$ | $1$ | $0$ |

| $\cdot$ | $0$ | $1$ | $\alpha$ | $\beta$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $\alpha$ | $\beta$ |
| $\alpha$ | $0$ | $\alpha$ | $\beta$ | $1$ |
| $\beta$ | $0$ | $\beta$ | $1$ | $\alpha$ |

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

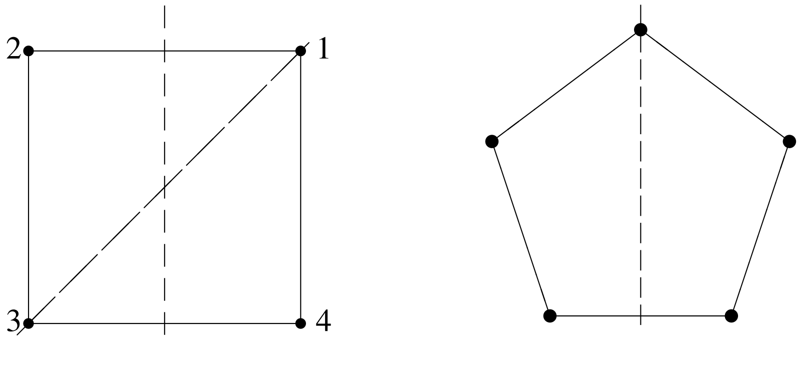
$$\det(AB) = \det(A)\det(B);$$

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

### 1.2.5 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 $a$s and $b$s 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 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 | $A_5$ | $A_5 \times C_2$ |

### 1.2.6 Small groups

We have seen in Proposition 1.2.1 a proof that there is a unique group of prime order (up to isomorphism). Here are proofs that the numbers of groups of orders 4, 6, 8 are 2, 2 and 5 respectively.

**Order** 4**:** Let $G$ be an element of order 4. If $G$ contains an element of order 4, then it is cyclic; otherwise all its elements apart from the identity have order 2. Let $G = \{1,x,y,z\}$. What is $xy$? By the cancellation laws, $xy$ cannot be 1 (since $xx = 1$), or $x$, or $y$; so $xy = z$. Similarly the product of any two of $x,y,z$ is the third, and the multiplication table is determined. So there is at most one type of non-cyclic group. But the group $C_2 \times C_2$ realises this case.

**Order** 6**:** Again suppose that there is no element of order 6, so that elements of $G$ have orders 1, 2 and 3 only. All these orders actually appear [why?]. Let $a$ have order 3 and $b$ order 2. Then it is easy to see that $G = \{1,a,a^2,b,ab,a^2b\}$. We cannot have $ba = ab$, since then we would find that this element has order 6. All other possibilities for $ba$ except $ba = a^2b$ are eliminated by the cancellation laws. So $ba = a^2b$, and then the multiplication table is determined. This case is realised by the symmetric group $S_3$.

**Order** 8**:** If there is an element of order 8, then $G$ is cyclic; if no element has order greater than 2, then $G = C_2 \times C_2 \times C_2$ (this is a bit harder). So assume that $a$ is an element of order 4, and let $b$ be an element which is not a power of $a$. Then $G = \{1,a,a^2,a^3,b,ab,a^2b,a^3b\}$. This time we need to know which of these eight elements is $b^2$, and which is $ba$, in order to determine the group. We find that $b^2 = 1$ or $b^2 = a^2$, and that $ba = ab$ or $ba = a^3b$. There seem to be four different possibilities; but two of these turn out to be isomorphic (namely, the cases $b^2 = 1, ba = ab$ and $b^2 = a^2, ba = ab$). So there are three different groups of this form. All of them actually occur: they are $C_4 \times C_2$ and the dihedral and quaternion groups. These together with the two we already found make five altogether.

## 1.3 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.

### 1.3.1 Definition

An *action* of a group $G$ on a set $\Omega$ 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 $\theta$; so $g\theta$ is a permutation of $\Omega$, 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 $\alpha g$ for the image of $\alpha$ under the permutation corresponding to $g$.

Alternatively, we can define an action of $G$ on $\Omega$ as a map $\mu$ from $\Omega \times G$ to $\Omega$ 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 $\mu$: we write $\mu(\alpha,g)$ as $\alpha g$. 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 $\Omega$ (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 $\Omega$ 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 1.3.1 (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 6, 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.

### 1.3.2 How many groups?

The number of $n \times n$ arrays with entries chosen from a set of size $n$ is $n^{n^2}$. So certainly this is an upper bound for the number of groups of order $n$.

In fact one can do much better, using two results we have met: the theorems of Lagrange and Cayley.

**Theorem 1.3.2** *The number of groups of order $n$ is at most $n^{n \log_2 n}$.*

**Proof** By Cayley's Theorem, every group of order $n$ is isomorphic to a subgroup of the symmetric group $S_n$. So if we can find an upper bound for the number of such subgroups, this will certainly bound the number of groups up to isomorphism.

We use Lagrange's Theorem in the following way. We say that a set $\{g_1, \ldots, g_k\}$ of elements of a group $G$ *generates* $G$ if no proper subgroup of $G$ contains all these elements. Equivalently, every element of $G$ can be written as a product of these elements and their inverses.

Now we have the following:

**Proposition 1.3.3** *A group of order n can be generated by a set of at most* $\log_2 n$ *elements.*

To see this, pick a non-identity element $g_1$ of $G$, and let $G_1$ be the subgroup generated by $g_1$. If $G_1 = G$, stop; otherwise choose an element $g_2 \notin G_1$, and let $G_2$ be the subgroup generated by $g_1$ and $g_2$. Continue in this way until we find $g_1, \ldots, g_k$ which generate $G$.

We claim that $|G_i| \geq 2^i$ for $i = 1, \ldots, k$. The proof is by induction on $i$. The assertion is clear for $i = 1$, since by assumption $|G_1| > 1$, so $|G_1| \geq 2$. Now suppose that $|G_i| \geq 2^i$. Now $G_i$ is a subgroup of $G_{i+1}$, and so $|G_i|$ divides $|G_{i+1}|$, by Lagrange's Theorem; since $G_i \neq G_{i+1}$, we have that $|G_{i+1}| \geq 2|G_i| \geq 2^{i+1}$. So the assertion is proved by induction.

Finally, $n = |G| = |G_k| \geq 2^k$, so $k \leq \log_2 n$.

Thus, to specify a subgroup $G$ of order $n$ of $S_n$, we only have to pick $k = \lfloor \log_2 n \rfloor$ elements which generate $G$. There are at most $n!$ choices for each element, so the number of subgroups is at most

$$(n!)^k \leq (n^n)^{\log_2 n} = n^{n \log_2 n},$$

since clearly $n! \leq n^n$.

### 1.3.3 Orbits and stabilisers

Let $G$ act on $\Omega$. We define a relation $\equiv$ on $\Omega$ 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 $\Omega$) if there is just one orbit.

We denote the orbit containing a point $\alpha$ 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 $\alpha$, the *stabiliser* of $\alpha$ is the set of elements of $G$ which map it to itself:

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

**Theorem 1.3.4 (Orbit-Stabiliser Theorem)** *Let $G$ act on $\Omega$, 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 $\alpha$.*

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 $\alpha$ to $\beta$ 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 $\Omega$ be the set of all right cosets of $H$ in $G$, and define an action of $G$ on $\Omega$ 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.

### 1.3.4 The Orbit-Counting Lemma

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

**Theorem 1.3.5 (Orbit-Counting Lemma)** *Let $G$ act on $\Omega$. Then the number of orbits of $G$ on $\Omega$ 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 $\alpha$ 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 $\Omega$ 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

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

## 1.4 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.

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.

### 1.4.1 Statement

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

**Theorem 1.4.1 (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 1.4.2 (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!

### 1.4.2 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 $\Omega$ 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 $\Delta$ 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 $\Delta$ 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 1.4.3** *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 $G$.*

### 1.4.3 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 1.4.4** *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 $k^q \equiv 1 \bmod p$, $k \not\equiv 1 \bmod p$.*

**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.

## 1.4.4 Another proof

Since writing the first version of these notes, I have changed my mind about which is the best proof of the first part of Sylow's Theorem (the existence of Sylow subgroups). The following proof is a translation of Sylow's original proof.

We begin with the following observation:

> The group $G$ has a Sylow $p$-subgroup if and only if it has an action in which all stabilisers have $p$-power order and there is an orbit of size coprime to $p$.

For, if $P$ is a Sylow $p$-subgroup, then the action on the right cosets of $P$ by right multiplication has the stated properties; conversely, if such an action exists, then the stabiliser of a point in an orbit of size coprime to $p$ is the required Sylow $p$-subgrop.

Now the heart of the argument is the following result.

**Proposition 1.4.5** *If a group $G$ has a Sylow $p$-subgroup, then so does every subgroup of $G$.*

**Proof** Suppose that $G$ has a Sylow $p$-subgroup. Take an action with the properties noted above, which we may assume to be transitive; thus the number of points is coprime to $p$, and all the stabilisers have $p$-power order. Now restrict the action to an arbitrary subgroup $H$. It is clear that all the stabilisers in $H$ have $p$-power order; and at least one orbit has size coprime to $p$, since if $p$ divided all orbit sizes it would divide the total number of points.

Now the existence of Sylow $p$-subgroups in a group $G$ of order $n$ follows immediately from two facts:

- $G$ is isomorphic to a subgroup of $S_n$;
- $S_n$ has Sylow $p$-subgroups.

The first statement is Cayley's Theorem; the second can be proved directly (see Exercise 1.17). But another application of the principle saves even this small amount of work:

- $S_n$ is a subgroup of $\mathrm{GL}(n,p)$;
- $\mathrm{GL}(n,p)$ has Sylow $p$-subgroups.

For the first fact, represent elements of $S_n$ by *permutation matrices*, zero-one matrices with a unique 1 in each row and column: the $(i,j)$ entry of the matrix corresponding to $g$ is equal to 1 if $ig = j$, and 0 otherwise. For the second fact, let $P$ be the set of *upper unitriangular* matrices in $\mathrm{GL}(n,p)$ (upper triangular matrices with 1 on the diagonal). It is straightforward to show that the order of $P$ is $p^{n(n-1)/2}$, which is exactly the power of $p$ dividing the order of $\mathrm{GL}(n,p)$; so it is indeed a Sylow subgroup.

## 1.5 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.

### 1.5.1 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:

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

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

**Theorem 1.5.1 (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 $G$.

### 1.5.2 Proof of the Jordan–Hölder Theorem

Recall that we are proving that any two composition series for a group $G$ have the same length and give rise to the same list of composition factors.

The proof is by induction on the order of $G$. We suppose the theorem true for groups smaller than $G$. Let

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

and

$$G = H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_s = \{1\}$$

be two composition series for $G$.

**Case 1:** $G_1 = H_1$. Then the parts of the series below this term are composition series for $G_1$ and so have the same length and composition factors. Adding in the composition factor $G/G_1$ gives the result for $G$.

**Case 2:** $G_1 \neq H_1$. Let $K_2 = G_1 \cap H_1$, a normal subgroup of $G$, and take a composition series

$$K_2 \rhd K_3 \rhd \cdots \rhd K_t = \{1\}$$

for $K_2$.

We claim that $G_1/K_2 \cong G/H_1$ and $H_1/K_2 \cong G/G_1$. If we can prove this, then the two composition series

$$G_1 \rhd G_2 \rhd \cdots \rhd \{1\}$$

and

$$G_1 \rhd K_2 \rhd K_3 \rhd \cdots \rhd \{1\}$$

for $G_1$ have the same length and composition factors; the composition factors of $G$ using the first series are these together with $G/G_1$. A similar remark holds for $H_1$. So each of the given composition series for $G$ has the composition factors in the series for $K_2$ together with $G/G_1$ and $G/H_1$, and the theorem is proved. So it only remains to establish the claim.

Now $G_1H_1$ is a normal subgroup of $G$ properly containing $G_1$; so $G_1H_1 = G$. Thus, by the Third Isomorphism Theorem,

$$G/G_1 = G_1H_1/G_1 \cong H_1/G_1 \cap H_1 = H_1/K_2,$$

and similarly $G/H_1 \cong G_1/K_2$. Thus the claim is proved.

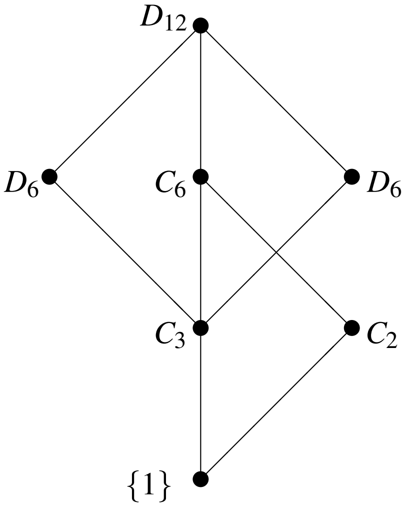
**Example** Find all composition series for the dihedral group $D_{12}$.

This group consists of the symmetries of a regular hexagon. It has three subgroups of order 6: a cyclic group consisting of the six rotations; and two dihedral groups, each containing three rotations (through multiples of $2\pi/3$) and three reflections. (In one case the reflections are in the diagonals; in the other, in the lines joining midpoints of opposite edges.) Also, there is no normal subgroup of order 4: the three subgroups of order 4 each consist of two rotations and two reflections through perpendicular axes, and they are conjugate.

Assuming that we know the composition series for cyclic and dihedral groups of order 6, we can now write down all composition series for the whole group. They are

- $D_{12} \rhd C_6 \rhd C_3 \rhd \{1\}$;
- $D_{12} \rhd C_6 \rhd C_2 \rhd \{1\}$;
- $D_{12} \rhd D_6 \rhd C_3 \rhd \{1\}$ (two such series).

Here is a diagram of the subgroups occurring in the composition series.



Both cases in the proof of the Jordan–Hölder theorem are exhibited here.

**Example** Among groups with composition factors $C_2$ and $A_5$, the factors can come in both orders or in one but not the other in composition series.

- If $G$ has two composition series with the factors in the two different orders, then it has normal subgroups $H$ and $K$ isomorphic to $C_2$ and $A_5$ respectively; clearly $HK = G$ and $H \cap K = \{1\}$. So $G \cong C_2 \times A_5$.
- The symmetric group $S_5$ has a normal subgroup $A_5$ with quotient $C_2$, but has no normal subgroup isomorphic to $C_2$.
- We will see later that the special linear group $\mathrm{SL}(2,5)$ has a normal subgroup isomorphic to $C_2$ (consisting of the matrices $I$ and $-I$) with quotient isomorphic to $A_5$; but it has no normal subgroup isomorphic to $A_5$ (since calculation shows that it contains a unique element of order 2, namely $-I$). (See Exercise 1.12.)

### 1.5.3 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 1.5.2** *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 1.5.3** *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.

### 1.5.4 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.

**Theorem 1.5.4** *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.

### 1.5.5 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 1.5.5** *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.

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 $q = 3$;

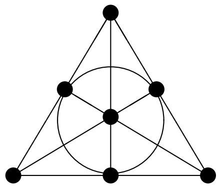
(d) twenty-six so-called *sporadic groups*, most of which are defined as symmetry groups of various algebraic or combinatorial configurations.

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.

# Exercises

**1.1** The figure below is the *Fano plane*, a configuration of seven points and seven lines. A *symmetry* is a permutation of the seven points which carries lines to lines.



(a) Let $a,b,c$ and $A,B,C$ be two triples of distinct points, neither of which forms a line. Show that there is a unique symmetry of the Fano plane carrying the first to the second.

(b) Show that the symmetries of the Fano plane form a group $G$ of order 168.

(c) Describe the Sylow subgroups of $G$.

(d) Show that $G$ is simple.

(e) Show that $G$ is isomorphic to $\mathrm{PSL}(3,2)$.

**1.2** Show that the two groups whose Cayley tables are given on page 6 are not isomorphic.

**1.3** Let $G$ be a group with the property that every element $g \in G$ satisfies $g^2 = 1$. Prove that $G$ is abelian.

**1.4** Facts about cosets.

(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).

**1.5** Let $H$ and $K$ be subgroups of a group $G$.

(a) Show that $H \cap K$ is a subgroup.

(b) Show that

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|},$$

where $HK = \{hk : h \in H, k \in K\}$. [*Hint:* given $x \in HK$, in how many different ways can we write it in the form $hk$ with $h \in H$ and $k \in K$?]

(c) Show that, if $H$ is a normal subgroup of $G$, then $HK$ is a subgroup of $G$.

(d) Give an example of subgroups $H$ and $K$ for which $HK$ is not a subgroup.

**1.6** Use the Fundamental Theorem of Abelian Groups to show that the converse of Lagrange's Theorem is true for abelian groups: that is, if $G$ is an abelian group of order $n$, and $m \mid n$, then $G$ has a subgroup of order $m$.

**1.7** What is the largest order of an element of $S_{10}$?

**1.8** Recall that that $\mathrm{GF}(2) = \{0,1\}$ is the field of integers mod 2. Show that the invertible $2 \times 2$ matrices over $\mathrm{GF}(2)$ 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 $S_3$.

**1.9** 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 $A(p^a) \leq 2^{a-1}$ for $a \geq 1$ 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 $A(n) \leq n/2$ for all $n > 1$.

**1.10** Show that there is no simple group of non-prime order less than 60. Show also that there is no simple group of order 120.

**1.11** Let $G$ be a group of order $2m$, where $m$ is odd and $m > 1$. Prove that $G$ is not simple. [Hint: Consider the action of $G$ on itself by right multiplication; show that this action contains an odd permutation.]

**1.12** Let $F$ be a field of characteristic different from 2. Show that $\mathrm{SL}(2,F)$ contains a unique element of order 2.

**1.13** Show directly that, if $p$ is a prime not dividing $m$, then $\binom{p^a m}{p}$ is not divisible by $p$. Harder: show that

$$\binom{p^a m}{p^a} \equiv m \pmod{p}.$$

**1.14** Prove Lemma 1.4.3.

**1.15** Let $A$ be the group of all complex roots of unity, with the operation of multiplication. Let $\mathbb{Q}$ be the group of rational numbers, with the operation of addition. Let $\theta : \mathbb{Q} \to A$ be the map given by

$$q\theta = \mathrm{e}^{2\pi \mathrm{i} q}.$$

Prove that $\theta$ is a homomorphism, with image $A$ and kernel $\mathbb{Z}$. Hence show that $\mathbb{Q}/\mathbb{Z} \cong A$.

Is $A$ isomorphic to the infinite cyclic group $C_\infty$?

**1.16** Verify the isomorphisms between polyhedral groups and symmetric or alternating groups in the table on page 17.

**1.17** Let $n = a_0 + a_1 p + \cdots + a_r p^r$, where $p$ is prime and $0 \le a_i \le p-1$ for $i = 0, \ldots, r$, be the expression for $n$ in base $p$.

(a) Show that the symmetric group $S_n$ contains a subgroup which is the direct product of $a_i$ symmetric groups of degree $p^i$, for $i = 0, \ldots, r$.

(b) Show that a Sylow $p$-subgroup of $S_{p^i}$ has order $p^m$, where $m = 1 + p + \cdots + p^{i-1}$, and construct such a subgroup.

(c) Hence show that $S_n$ has a Sylow $p$-subgroup.

**1.18** A *transposition* is a permutation which interchanges two points and fixes the others.

(a) Show that the symmetric group $S_n$ is generated by its transpositions for $n \geq 2$.

(b) Let $G$ be a subgroup of $S_n$ containing a transposition. Define a relation $\sim$ on the set $\{1,2,\ldots,n\}$ by the rule that $i \sim j$ if either $i = j$ or the transposition $(i,j)$ belongs to $G$. Prove that $\sim$ is an equivalence relation. Show that the transpositions contained in any equivalence class generate the symmetric group on that class.

(c) Hence show that $G$ has a normal subgroup which is the direct product of symmetric groups on the equivalence classes of $\sim$.

**1.19** Let $G$ be the symmetric group $S_5$.

(a) For each prime $p$ dividing $|G|$, find a Sylow $p$-subgroup of $G$ and determine its structure; find also the number of Sylow $p$-subgroups.

(b) Find all the normal subgroups of $G$.

**1.20** (a) Show that a group of order 40 has a normal Sylow subgroup.

(b) Do the same for a group of order 84.

**1.21** (a) Show that every subgroup of a cyclic group is cyclic.

(b) Show that every subgroup of a dihedral group is cyclic or dihedral.

(c) Let $G$ be the dihedral group of order 12. Find all subgroups of $G$, indicating which are normal.

(d) Find all the composition series for the dihedral group of order 12.

**1.22** Suppose that $a$ and $b$ are elements of a finite group $G$ satisfying $a^2 = b^2 = 1$.

(a) Show that $\langle a,b \rangle$ is a dihedral group $D_{2m}$ for some $m$.

(b) If $m$ is odd, show that $a$ and $b$ are conjugate in $G$.

(c) If $m$ is even, show that $G$ contains an element $c$ satisfying $c^2 = 1$ which commutes with both $a$ and $b$.

**1.23** Find all the composition series for the symmetric group $S_4$.

**1.24** Let $p$ be a prime number. An *elementary abelian p-group* is a group $G$ such that $G$ is abelian and $g^p = 1$ for all $g \in G$.

(a) Show that an elementary abelian $p$-group has order a power of $p$.

(b) Show that if $G$ is an elementary abelian group of order $p^n$, then

$$G \cong C_p \times C_p \times \cdots \times C_p \qquad (n \text{ factors}).$$

**1.25** Don't tackle parts (b) and (c) of this question unless you have met primitive roots (e.g. in a number theory course). Let $U(n)$ be the group of units of the ring $Z_n$ of integers mod $n$.

(a) Prove that, if $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, then

$$U(n) \cong U(p_1^{a_1}) \times U(p_2^{a-2}) \times \cdots \times U(p_r^{a_r}).$$

[Hint: Chinese Remainder Theorem.]

(b) Prove that, if $p$ is prime, then $U(p) \cong C_{p-1}$.

(c) Prove that, if $p$ is prime and $a \geq 1$, then $U(p^a) \cong C_{(p-1)p^{a-1}}$.

(d) Prove that $U(2^a) \cong C_2 \times C_{2^{a-2}}$ for $a \geq 2$. [Hint: the factors are generated by the units $-1$ and 5.]

# Chapter 2

# Simple groups

## 2.1 More on group actions

We saw when we considered group actions before that any action of a group can be "decomposed" into orbits, so that the group has a transitive action on each orbit. In this section we look further at transitive actions, and show that all the different transitive actions of a group can be recognised in terms of the subgroup structure of the group. We define primitivity of an action, and examine how to recognise this in group-theoretic terms and its consequences for normal subgroups. We also look at the stronger notion of double transitivity. After some examples, we turn to *Iwasawa's Lemma*, which will enable us to show that certain groups are simple.

### 2.1.1 Coset actions

Let $H$ be a subgroup of the group $G$. We will consider the set of right cosets of $H$ in $G$:

$$\cos(H,G) = \{Hg : g \in G\}.$$

Sometimes this is written as $H\backslash G$, but this is too close to the notation $H \setminus G$ for set difference so I will avoid it. Sometimes it is written $[G{:}H]$.

Now $G$ acts on $\cos(H,G)$ by right multiplication. Formally, using $\mu(x,g)$ for the action of the permutation corresponding to $g$ on the element $x$, the action is given by

$$\mu(Hx,g) = H(xg).$$

Fortunately, we can write this in the briefer form $(Hx)g = H(xg)$ without risk of too much confusion.

Note that the action of $G$ on $\cos(H,G)$ is transitive; for given any two cosets $Hx$ and $Hy$, we have $(Hx)(x^{-1}y) = Hy$. The important thing is that every transitive action can be realised in this way, in a sense which we now explore.

Let $G$ have actions on two sets $\Omega_1$ and $\Omega_2$. An *isomorphism* between these actions is a bijection $f : \Omega_1 \to \Omega_2$ such that $(\alpha g)f = (\alpha f)g$ for all $g \in G$. Here the left-hand side means "apply the group element $g$ to $\alpha$, in the given action on $\Omega_1$, and then map across to $\Omega_2$ using $f$", while the right-hand side means "map to $\Omega_2$ using $f$, and then apply $g$ using the action on $\Omega_2$". Another way that this is commonly expressed is that the following diagram *commutes*, in the sense that all routes through the diagram following the arrows give the same result:

$$\begin{tikzcd}
\Omega_1 \arrow[r, "f"] \arrow[d, "g"'] & \Omega_2 \arrow[d, "g"] \\
\Omega_1 \arrow[r, "f"] & \Omega_2
\end{tikzcd}$$

The $g$s on left and right refer to the two actions.

Recall that, if $G$ acts on $\Omega$, then the *stabiliser* $\mathrm{Stab}(\alpha)$ of a point $\alpha$ is

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

**Theorem 2.1.1** *(a) Any transitive action of a group $G$ on a set $\Omega$ is isomorphic to the action of $G$ on the coset space* $\cos(H,G)$*, where $H =$* $\mathrm{Stab}(\alpha)$ *for some $\alpha \in \Omega$.*

*(b) The actions of $G$ on the coset spaces* $\cos(H,G)$ *and* $\cos(K,G)$ *are isomorphic if and only if the subgroups $H$ and $K$ are conjugate (that is, $K = g^{-1}Hg$ for some $g \in G$).*

**Proof** I will prove the first part; the second is an exercise. The proof is just an adaptation of the proof of the Orbit-Stabiliser Theorem. If $G$ acts transitively on $\Omega$, we saw that there is a bijection between $\Omega$ and the set of subsets $X(\alpha,\beta)$ of $G$ for fixed $\alpha$ (as $\beta$ ranges over $\Omega$), where

$$X(\alpha,\beta) = \{g \in G : \alpha g = \beta\}.$$

We saw, furthermore, that $X(\alpha,\beta)$ is a right coset of $\mathrm{Stab}(\alpha)$, and that every right coset arises in this way. Now it is a fairly routine exercise to check that the bijection from $\Omega$ to $\cos(\mathrm{Stab}(\alpha),G)$ taking $\beta$ to $X(\alpha,\beta)$ is an isomorphism.

**Example** Let $G$ be the dihedral group $D_6$ of symmetries of an equilateral triangle. Let $\Omega_1$ be the set of three vertices of the triangle, and $\Omega_2$ the set of three edges. Show that $G$ acts transitively on both these sets, and that the map $f$ which takes each vertex to the opposite edge is an isomorphism of actions.

### 2.1.2 Primitivity

Let $G$ act transitively on a set $\Omega$, with $|\Omega| > 1$. A *congruence*, or *G-congruence*, on $\Omega$ is an equivalence relation on $\Omega$ which is preserved by $G$ (that is, if $\alpha \equiv \beta$, then $(\alpha g) \equiv (\beta g)$ for all $g \in G$). An equivalence class of a congruence is called a *block*. Note that, if $B$ is a block, then so is $Bg$ for any $g \in G$.

There are always two trivial congruences:

*equality*: $\alpha \equiv \beta$ if and only if $\alpha = \beta$;

the *universal* relation: $\alpha \equiv \beta$ for all $\alpha, \beta \in \Omega$.

The action is called *imprimitive* if there is a non-trivial congruence, and *primitive* if not.

**Example** Let $G$ be the symmetry group of a square (the dihedral group of order 8), acting on $\Omega$, the set of four vertices of the square. The relation $\equiv$ defined by $\alpha \equiv \beta$ if $\alpha$ and $\beta$ are equal or opposite is a congruence, with two blocks of size 2.

**Proposition 2.1.2** *Let $G$ act transitively on $\Omega$. A non-empty subset $B$ of $\Omega$ is a block if and only if, for all $g \in G$, either $Bg = B$ or $B \cap Bg = \emptyset$.*

**Proof** If $B$ is a block, then so is $Bg$; and equivalence classes are equal or disjoint.

Conversely, suppose that $B$ is a non-empty set such that $B = Bg$ or $B \cap Bg = \emptyset$ for all $g$. Then for any $h, k \in G$, we have $Bh = Bk$ or $Bh \cap Bk = \emptyset$. (For $Bh \cap Bk = (B \cap Bkh^{-1})h$.) So the images of $B$ are pairwise disjoint. By transitivity, every point of $\Omega$ is covered by these images. So they form a partition, which is the set of equivalence classes of a congruence.

We saw that every transitive action is isomorphic to a coset space: how do we recognise primitive actions? A subgroup $H$ of $G$ is *maximal* if $H < G$ but there is no subgroup $K$ satisfying $H < K < G$.

**Proposition 2.1.3** *Let $H$ be a proper subgroup of $G$. Then the action of $G$ on $\cos(H,G)$ is primitive if and only if $H$ is a maximal subgroup of $G$.*

**Proof** Suppose that $H < K < G$, and let $B$ be the set of cosets of $H$ which are contained in $K$. Then $B$ satisfies the conditions of the previous proposition. For take a coset $Hk$ with $k \in K$. For any $g \in G$,

- if $g \in K$, then $Hkg \in B$, so $Bg = B$;
- if $g \notin K$, then $Hkg \notin B$, so $B \cap Bg = \emptyset$.

Conversely, suppose that $G$ acts imprimitively on $\cos(H,G)$; let $B$ be a block containing the coset $H$, and $K = \{g \in G : Bg = B\}$. Then $K$ is a subgroup of $G$, and $H < K < G$.

One of the important properties of primitive actions is the following strong restriction on normal subgroups:

**Proposition 2.1.4** *Let $G$ act primitively on $\Omega$, and let $N$ be a normal subgroup of $G$. Then either $N$ acts trivially on $\Omega$ (that is, $N$ lies in the kernel of the action), or $N$ acts transitively on $\Omega$.*

**Proof** We show that, for any transitive action of $G$, the orbit relation of the normal subgroup $N$ is a congruence. It follows that, if the action is primitive, then either all orbits have size 1, or there is a single orbit.

So let $\alpha \equiv \beta$ if $\alpha h = \beta$ for some $h \in N$. Then for any $g \in G$, $(\alpha g)(g^{-1}hg) = \beta g$, and $g^{-1}hg \in N$ by normality; so $\alpha g \equiv \beta g$. Thus $\equiv$ is indeed a congruence.

**Example** If $G$ is the group of symmetries of a square, then the subgroup of order 2 generated by the 180° rotation is normal; its orbit relation is the congruence we found earlier.

**Remark** Let $G$ act transitively on an $n$-element set. If $\equiv$ is a congruence with $l$ classes, then each class has the same size $k$, and $kl = n$. If $n$ is prime, then necessarily $k = 1$ or $k = n$. So:

> A transitive action on a prime number of points is primitive.

### 2.1.3 Digression: Minimal normal subgroups

A *minimal normal subgroup* of a group $G$ is a normal subgroup $N \trianglelefteq G$ with $N \neq \{1\}$ such that, if $M \trianglelefteq G$ with $M \leq N$, then either $M = N$ or $M = \{1\}$.

There is an important result which says:

**Theorem 2.1.5** *A minimal normal subgroup of a finite group is isomorphic to the direct product of a number of copies of a simple group.*

Since I haven't given in detail the result for recognising the direct product of more than two factors, I won't prove this theorem in general; but I will prove a special case as an illustration.

Let $p$ be a prime number. An *elementary abelian $p$-group* is an abelian group in which every element different from the identity has order $p$. By the Fundamental Theorem of Abelian Groups, such a group is a direct product of cyclic groups of order $p$.

**Proposition 2.1.6** *An abelian minimal normal subgroup of a finite group is elementary abelian.*

**Proof** Let $N$ be such a subgroup, and let $p$ be a prime dividing $|N|$. There is an element of order $p$ in $N$. Let $M$ be the set of elements of $N$ with order dividing $p$. Then $M \neq \{1\}$, and $M$ is a normal subgroup of $G$ (since conjugation preserves both order and membership in $N$). So $M = N$.

Any minimal normal subgroup of a soluble group is abelian. For let $G$ be soluble, and $N$ a minimal normal subgroup. Then $N$ is soluble, so its derived group $N'$ satisfies $N' \neq N$; and $N' \trianglelefteq G$, since conjugation preserves both commutators and members of $N$. So $N' = \{1\}$, that is, $N$ is abelian.

Here is a slightly unexpected corollary.

**Proposition 2.1.7** *Let G be a finite soluble group. Then any maximal subgroup of G has prime power index.*

**Proof** Let $H$ be a maximal subgroup, and consider the (primitive) action of $G$ on $\cos(H,G)$. The image of this action is a quotient of $G$, hence is soluble. So we may assume that the action is faithful.

Let $N$ be a minimal normal subgroup of $G$. Then $N$ is abelian, and hence an elementary abelian $p$-group for some prime $p$; and $N$ is transitive, since $G$ is primitive and $N \neq \{1\}$. So by the Orbit-Stabiliser Theorem, $|\cos(H,G)|$ (the index of $H$ in $G$) is a power of $p$.

### 2.1.4 Regular actions

In this section we consider only faithful actions.

An action of $G$ on $\Omega$ is *regular* if it is transitive and the point stabiliser is trivial.

If $H$ is the trivial subgroup, then each coset of $H$ consists of a single element; so the set $\cos(H,G)$ is "essentially" just $G$. Thus, a regular action of $G$ is isomorphic to the action on itself by right multiplication.

(If we did not require the action to be faithful, then we could say that an action is regular if it is transitive and the point stabiliser $H$ is a normal subgroup of $G$; such an action is isomorphic to the action of $G/H$ on itself by right multiplication. In particular, since every subgroup of an abelian group is normal, we see that every transitive action of an abelian group is regular.)

We need to look at a fairly technical situation. Let $G$ be a group with a faithful action on $\Omega$, and $N$ a normal subgroup of $G$ whose action on $\Omega$ is regular. Then we can "identify" $\Omega$ with $N$ so that $N$ acts by right multiplication. More precisely, we choose a fixed reference point $\alpha \in \Omega$; then there is a bijection between $N$ and $\Omega$, under which $h \in N$ corresponds to $\alpha h \in \Omega$; this is an isomorphism between the action of $N$ on itself by right multiplication and the given action.

Can we describe the entire action of $G$ on $N$? It turns out that there is a nice description of the subgroup $\mathrm{Stab}(\alpha)$ of $G$:

> Under the above bijection, the action of $\mathrm{Stab}(\alpha)$ on $N$ by conjugation corresponds to the given action on $\Omega$.

To show this, take $g \in \mathrm{Stab}(\alpha)$ and suppose that $g$ maps $\beta$ to $\gamma$. Let $h$ and $k$ be the elements of $N$ corresponding to $\beta$ and $\gamma$ under the bijection: that is, $\alpha h = \beta$ and $\alpha k = \gamma$. Now

$$\alpha(g^{-1}hg) = \alpha hg = \beta g = \gamma,$$

since $g^{-1}$ fixes $\alpha$. Since there is a unique element of $N$ mapping $\alpha$ to $\gamma$, namely $k$, we have $g^{-1}hg = k$, as required.

We will use this analysis when we come to showing the simplicity of the alternating group.

### 2.1.5 Double transitivity

Let $G$ act on $\Omega$, with $|\Omega| > 1$. We say that the action is *doubly transitive* if, given any two ordered pairs $(\alpha_1, \alpha_2)$ and $(\beta_1, \beta_2)$ of *distinct* elements of $\Omega$, there is an element $g \in G$ satisfying $\alpha_1 g = \beta_1$ and $\alpha_2 g = \beta_2$.

Here "distinct" means that $\alpha_1 \neq \alpha_2$ and $\beta_1 \neq \beta_2$, but we don't say anything about the relation between $\alpha_1$ and $\beta_1$, for example. (A permutation cannot map distinct points to equal points or *vice versa*.)

**Examples** 1. The symmetric group $S_n$ acts doubly transitively on the set $\{1, 2, \ldots, n\}$ for $n \geq 2$.

2. The automorphism group of the Fano plane, the group of order 168 in Exercise 1.1, acts doubly transitively on the seven points of the plane.

**Proposition 2.1.8** *A doubly transitive action is primitive.*

**Proof** Let $\equiv$ be a congruence. By the reflexive property, $\alpha \equiv \alpha$ for all $\alpha$. If $\alpha_1 \equiv \alpha_2$ for any single pair $(\alpha_1, \alpha_2)$ of distinct elements, then $\beta_1 \equiv \beta_2$ for all distinct pairs, and $\equiv$ is the universal congruence; otherwise, it is the relation of equality.

**Remark** In a similar way, we can define $t$-transitivity of an action, for any $t \geq 1$.

### 2.1.6 Iwasawa's Lemma

Iwasawa's Lemma is a technique for proving the simplicity of a group. It looks rather technical, but we will use it to show that the group $\mathrm{PSL}(d,F)$ is simple in most cases. Though it is technical, fortunately the proof is quite straightforward.

The *derived group*, or *commutator subgroup*, of $G$ is the subgroup $G'$ generated by all *commutators* $[g,h] = g^{-1}h^{-1}gh$ for $g,h \in G$. It has the following properties:

- $G'$ is a normal subgroup of $G$;
- $G/G'$ is abelian;
- if $N$ is a normal subgroup of $G$ such that $G/N$ is abelian, then $G' \leq N$.

**Theorem 2.1.9** *Let G be a group with a faithful primitive action on* $\Omega$. *Suppose that there is an abelian normal subgroup A of* $\mathrm{Stab}(\alpha)$ *with the property that the conjugates of A generate G. Then any non-trivial normal subgroup of G contains* $G'$. *In particular, if* $G = G'$, *then G is simple.*

**Proof** Suppose that $N$ is a non-trivial normal subgroup of $G$. Then $N$ is transitive, so $N \not\leq \mathrm{Stab}(\alpha)$. Since $\mathrm{Stab}(\alpha)$ is a maximal subgroup of $G$, we have $N\,\mathrm{Stab}(\alpha) = G$.

Let $g$ be any element of $G$. Write $g = nh$, where $n \in N$ and $h \in \mathrm{Stab}(\alpha)$. Then

$$gAg^{-1} = nhAh^{-1}n^{-1} = nAn^{-1},$$

since $A$ is normal in $\mathrm{Stab}(\alpha)$. Since $N$ is normal in $G$ we have $gAg^{-1} \leq NA$. Since the conjugates of $A$ generate $G$ we see that $G = NA$.

Hence

$$G/N = NA/N \cong A/(A \cap N)$$

is abelian, whence $N \geq G'$, and we are done.

## 2.2 Symmetric and alternating groups

In this section we examine the alternating groups $A_n$ (which are simple for $n \geq 5$), prove that $A_5$ is the unique simple group of its order, and study some further properties, including the remarkable outer automorphism of the symmetric group $S_6$.

Let us remind ourselves at the start of the test for conjugacy in $S_n$. The *cycle structure* of permutation is the list of cycle lengths.

**Proposition 2.2.1** *Two elements of $S_n$ are conjugate if and only if they have the same cycle structure.*

Using this, it is possible to calculate the size of any conjugacy class in $S_n$:

**Proposition 2.2.2** *If a permutation has $a_i$ cycles of length $i$ for $i = 1, 2, \ldots, n$, then the size of its conjugacy class in $S_n$ is*

$$\frac{n!}{1^{a_1} a_1! \, 2^{a_2} a_2! \cdots n^{a_n} a_n!}.$$

**Proof** Write down brackets and spaces for a permutation with the given cycle structure. There are $n!$ ways of writing the numbers $1, 2, \ldots, n$ into the gaps. But we get the same permutation if we start any cycle at a different point, or if we rearrange the cycles of the same length in any order. The number of different representations of a permutation is thus the denominator in the above expression.

We saw that every permutation is a product of transpositions; that is, the transpositions generate $S_n$. Similarly, we have:

**Proposition 2.2.3** *The alternating group $A_n$ is generated by the 3-cycles.*

**Proof** First, note that 3-cycles are even permutations, so they lie in $A_n$.

Now take an arbitrary even permutation $g \in A_n$; say

$$g = t_1 t_2 \cdots t_{2k-1} t_{2k}.$$

We have to express $g$ as a product of 3-cycles. Clearly it suffices to write each consecutive pair of transpositions $t_{2i-1} t_{2i}$ in the product in terms of 3-cycles. There are three cases for a product of two transpositions:

- $(a,b)(a,b) = 1$;
- $(a,b)(a,c) = (a,b,c)$;
- $(a,b)(c,d) = (a,b,c)(a,d,c)$.

### 2.2.1 The group $A_5$

Recall that $A_n$ is the group of all even permutations on $\{1,\ldots,n\}$. (A permutation is even if the number of disjoint cycles is congruent to $n$ mod 2, or if it is the product of an even number of transpositions.) It is a group of order $(n!)/2$.

$A_2$ is the trivial group, and $A_3$ the cyclic group of order 3. $A_4$ is a group of order 12. It consists of the identity, three conjugate elements of order 2, and eight elements of order 3 (falling into two conjugacy classes each of size 4). The identity and the three elements of order 2 form a normal subgroup of order 4, the *Klein group* $V_4$. It is the only non-trivial proper normal subgroup of $A_4$. (We use "non-trivial" to mean "not the identity subgroup", and "proper" to mean "not the whole group".)

**Proposition 2.2.4** *$A_5$ is simple.*

There are several ways to prove this theorem. Here are two. They both start by describing the conjugacy classes. First, note that any conjugacy class in $S_n$ must be a union of conjugacy classes in $A_n$; since the index is 2, either it is a single $A_n$-class, or it splits into two $A_n$-classes of equal sizes. We need to know which classes split.

**Proposition 2.2.5** *The following are equivalent for a permutation $g \in A_n$:*

*(a) the $S_n$-conjugacy class of $g$ splits into two $A_n$-classes;*

*(b) there is no odd permutation which commutes with $g$;*

*(c) $g$ has no cycles of even length, and all its cycles have distinct lengths.*

**Proof** $S_n$ acts transitively by conjugation, and the stabiliser of an element $g$ is its *centraliser* (the set of elements which commute with $g$). Now if $C(g)$ and $C'(g)$ are the centralisers of $g$ in $S_n$ and $A_n$, then $C'(g) = C(g) \cap A_n$, so $C'(g) = C(g)$ if condition (b) holds, and $|C'(g)| = |C(g)|/2$ otherwise. Now the sizes of the conjugacy classes in $S_n$ and $A_n$ are $|S_n|/|C(g)|$ and $|A_n|/|C'(g)|$, from which we see that (a) is equivalent to (b).

If $g$ has a cycle of even length, then this cycle is an odd permutation commuting with $g$; if $g$ has two cycles of equal odd length $l$, then a permutation interchanging them is a product of $l$ transpositions and commutes with $g$. On the other hand, if neither possibility holds, then any permutation commuting with $g$ must fix each of its cycles and act on it as a power of the corresponding cycle of $g$, hence is an even permutation. So (b) and (c) are equivalent.

Using this, we can calculate the conjugacy classes in $A_5$:

| Cycle structure | Class size | Splits in $A_5$? |
|---|---|---|
| $[1,1,1,1,1]$ | 1 | No |
| $[1,2,2]$ | 15 | No |
| $[1,1,3]$ | 20 | No |
| $[5]$ | 24 | Yes |

So the class sizes are $1,15,20,12,12$.

A normal subgroup is a union of conjugacy classes, containing the identity, and having order dividing 60 (the order of $A_5$). It is easy to see that there is no such divisor.

Here is a rather different proof. We know that $A_5$ acts doubly transitively, and hence primitively, on $\{1,2,3,4,5\}$. (Alternatively it is primitive because 5 is prime.) So, if $N$ is a non-trivial normal subgroup, then $N$ is transitive. Then $|N| = 5 \cdot |N \cap A_4|$, and $N \cap A_4$ is a normal subgroup of $A_4$, hence is $\{1\}$, $V_4$ or $A_4$. So $|N| = 5, 20$ or 60. We can ignore the last case.

Since 5 divides $|N|$, we see that $N$ contains a Sylow 5-subgroup of $A_5$. Since they are all conjugate, it contains all six Sylow 5-subgroups. But they contain 24 elements of order 5; these cannot fit into a group of order 5 or 20.

### 2.2.2 Simplicity of $A_n$

**Theorem 2.2.6** *$A_n$ is simple for all $n \geq 5$.*

**Proof** The proof is by induction, starting at $n = 5$ (the case we have just done). Suppose that $N$ is a non-trivial normal subgroup of $A_n$. Then $N$ is transitive, so contains a set of coset representatives for the stabiliser $A_{n-1}$; thus $NA_{n-1} = A_n$. Also, $N \cap A_{n-1}$ is a normal subgroup of $A_{n-1}$, so by the inductive hypothesis either $N \cap A_{n-1} = A_{n-1}$ (in which case we have

$$A_n/N = NA_{n-1}/N \cong A_{n-1}/N \cap A_{n-1} = \{1\},$$

so that $N = A_n$) or $N \cap A_{n-1} = \{1\}$, in which case $N$ acts regularly and $|N| = n$.

Now there are many ways to proceed. Here are three different proofs.

- We have a formula for the size of conjugacy classes in $A_{n-1}$. Using this, and some hard labour, it is possible to show that there cannot be a conjugacy class of size $n-1$ or smaller. So the existence of a normal subgroup of order $n$ is impossible.

- Use the analysis of regular normal subgroups we gave in the last section. The action of $A_{n-1}$ on $N \setminus \{1\}$ by conjugation is isomorphic to its action on $\{1,2,\ldots,n-1\}$. This implies

(a) all non-identity elements of $N$ are conjugate, so all have the same order, necessarily a prime number $p$;

(b) now $N$ is a $p$-group, so $Z(N) \neq \{1\}$; but $Z(N)$ is fixed by conjugation, so $Z(N) = N$, and $N$ is elementary abelian;

(c) suppose that $p > 2$, and let $a, b \in N$ such that $b \neq a, a^2$; then since $A_{n-1}$ is 2-transitive, there is an element $g \in A_{n-1}$ satisfying $g^{-1}ag = a$ and $g^{-1}a^2g = b$, which is impossible;

(d) suppose that $p = 2$, and choose $a, b, c \in N$ generating a subgroup of order 8; since $N$ is triply transitive, there is an element $g \in N$ satisfying $g^{-1}ag = 1$, $g^{-1}bg = b$ and $g^{-1}(ab)g = c$, which is impossible.

The contradiction shows that no normal subgroup of order $n$ can exist.

- We have seen that $N$ is generated by at most $\lfloor \log_2 n \rfloor$ elements. An automorphism is determined by the images of the generators, so $|\operatorname{Aut}(N)| \leq n^{\log_2 n}$. But $A_{n-1}$ acts faithfully on $N$ by conjugation, so $(n-1)! \leq n^{\log_2 n}$. Some easy checking shows that this is impossible for $n \geq 6$.

### 2.2.3 Normal subgroups of $S_n$

**Theorem 2.2.7** *The only normal subgroups of $S_n$ for $n \geq 5$ are $\{1\}$, $A_n$ and $S_n$.*

**Proof** Let $N$ be a normal subgroup of $S_n$. Then $N \cap A_n$ is a normal subgroup of $A_n$, so $N \cap A_n = \{1\}$ or $A_n$.

If $N \cap A_n = A_n$, then $N \geq A_n$, so $N = A_n$ or $S_n$.

if $N \cap A_n = \{1\}$, then

$$N = N/(N \cap A_n) \cong NA_n/A_n = S_n/A_n \text{ or } A_n/A_n,$$

So $|N| = 1$ or 2. But $|N| = 2$ is impossible, since then there would have to be a non-identity element of $S_n$ in a conjugacy class of size 1. So $N = \{1\}$ in this case.

### 2.2.4 The uniqueness of $A_5$

**Proposition 2.2.8** *A simple group of order* 60 *is isomorphic to* $A_5$.

**Proof** Let $G$ be a simple group of order 60.

The number of Sylow 5-subgroups of $G$ is congruent to 1 (mod 5) and divides 12, but is not 1 (else the unique Sylow subgroup would be a normal subgroup of $G$). So there are six Sylow 5-subgroups.

Consider the action of $G$ on the set $\Omega$ of six Sylow 5-subgroups by conjugation. By Sylow's Theorem, the action is transitive. Since $G$ is simple, the kernel of the action is $\{1\}$; that is, the action is faithful. So the image of the action is a subgroup of $S_6$ isomorphic to $G$; let us call it $H$.

Now $H \leq A_6$, since otherwise $H \cap A_6$ would be a normal subgroup of $H$, contradicting the simplicity of $H$. Also, $|H| = 60$, and $|A_6| = 360$, so $H$ has index 6 in $H$.

Consider the action of $K = A_6$ on the set $\cos(H,K)$ of six cosets of $H$. This action is faithful, so $K$ is a subgroup of the symmetric group $S$ on the set $\cos(H,K)$. Clearly $K$ has index 2 in $S$, and so is a normal subgroup. Thus $K = A_6$ in its usual action on six objects. But then $H$ is the stabiliser of one of these objects, so $H \cong A_5$.

Since $G \cong H$ we have $G \cong A_5$ as required.

### 2.2.5 Automorphisms

You may have got lost in the above proof because the group $A_6$ was acting on a set of six objects which were not the original $\{1,\ldots,6\}$ on which the group is defined. We can put this confusion to constructive use. In the next section we see a remarkable property of the number 6, which is shared by no other positive integer, finite or infinite.

First some definitions. Let $G$ be a group.

- An *automorphism* of $G$ is an isomorphism from $G$ to $G$.
- An *inner automorphism* is a map of the form $c_g : x \mapsto g^{-1}xg$ from the group $G$ to itself.

In what follows, maps will be composed from left to right, so to avoid confusion, we write a map on the right of its argument.

**Theorem 2.2.9** *Let G be a group.*

*(a) The set of automorphisms of G forms a group under the operation of composition. This is the* automorphism group *of G, denoted by* $\mathrm{Aut}(G)$.

*(b) An inner automorphism of G is an automorphism of G (as the name suggests).*

*(c) The inner automorphisms comprise a normal subgroup of* $\mathrm{Aut}(G)$*, denoted by* $\mathrm{Inn}(G)$*; it is isomorphic to* $G/Z(G)$*, where* $Z(G)$ *is the centre of G.*

**Proof** (a) It is straightforward to show that the composition of automorphisms is an automorphism, and the inverse map of an automorphism is an automorphism.

(b) First, $c_g$ is a bijective map, since it has an inverse, namely $c_{g^{-1}}$. Next,

$$(xy)c_g = g^{-1}(xy)g = g^{-1}xg \cdot g^{-1}yg = (xc_g)(yc_g),$$

so $c_g$ is a homomorphism, and hence an automorphism.

There is a map from $G$ to $\mathrm{Aut}(G)$ given by $g \mapsto c_g$. We show that this map is a homomorphism.

$$\begin{aligned}(xc_g)c_h &= (g^{-1}xg)c_h = h^{-1}(g^{-1}xg)h,\\ xc_{gh} &= (gh)^{-1}x(gh) = (h^{-1}g^{-1})x(gh),\end{aligned}$$

and the right-hand sides are equal.

So the First Isomorphism Theorem tells us that $\mathrm{Inn}(G)$, the image of this map, is a subgroup of $\mathrm{Aut}(G)$. To show that it is normal, let $\phi$ be any automorphism of $G$, and calculate the effect of $\phi^{-1}c_g\phi$:

$$\begin{aligned}x(\phi^{-1}c_g\phi) &= ((x\phi^{-1})c_g)\phi\\ &= (g^{-1}(x\phi^{-1})g)\phi\\ &= (g\phi)^{-1}x(g\phi),\end{aligned}$$

where we used the fact that automorphisms map inverses to inverses to say that $(g^{-1})\phi = (g\phi)^{-1}$. So $\phi^{-1}c_g\phi = c_{g\phi}$, an inner automorphism. Thus $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

The kernel of the map $g \mapsto c_g$ is the set

$$\begin{aligned}\{g \in G : c_g = 1\} &= \{g \in G : xc_g = x \text{ for all } x \in G\}\\ &= \{g \in G : g^{-1}xg = x \text{ for all } x \in G\}\\ &= \{g \in G : xg = gx \text{ for all } x \in G\}\\ &= Z(G).\end{aligned}$$

So $G/Z(G) \cong \mathrm{Inn}(G)$.

An automorphism which is not inner is called *outer*. However, by abuse of language, the *outer automorphism group* of $G$ is not the group of outer automorphisms — they do not form a group [WHY?] — but is defined to be the quotient group $\mathrm{Aut}(G)/\mathrm{Inn}(G)$. Thus, the outer automorphism group of $G$ is trivial if and only if $G$ has no outer automorphisms.

### 2.2.6 Outer automorphisms of $S_6$

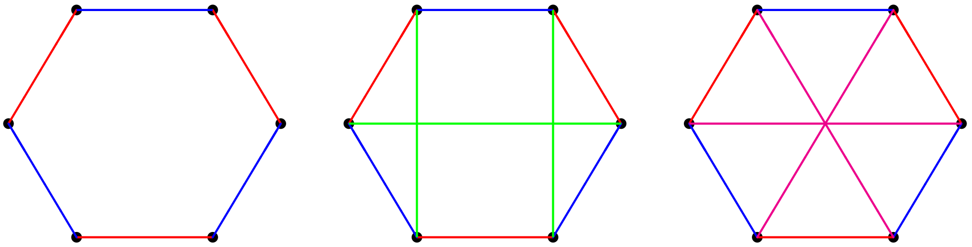
For $n \geq 3$, $Z(S_n) = \{1\}$, so $\mathrm{Inn}(S_n) \cong S_n$. It turns out that, except for the single value $n = 6$, we actually have $\mathrm{Aut}(S_n) = S_n$, so that $S_n$ has no outer automorphisms. We will not prove that, but will construct outer automorphisms of $S_6$ in two different ways, and hence show that $|\mathrm{Out}(S_6)| = 2$.

First, we can find such a subgroup directly. Let $G = S_5$. It is easy to check that $G$ has six Sylow 5-subgroups. (The only divisors of 24 which are congruent to 1 (mod 6) are 1 and 6, and we know that $S_5$ does not have a normal Sylow 5-subgroup.) So $S_5$ acts faithfully and transitively on the set of six Sylow 5-subgroups by conjugation, giving a transitive subgroup of $S_6$ isomorphic to $S_5$ but not conjugate to the stabiliser of a point. By our previous analysis, this shows that there is an outer automorphism.

For the second approach, we follow Sylvester, including his rather odd terminology. Let $A = \{1,2,\ldots,6\}$. A *duad* is a 2-element subset of $A$; there are $(6\cdot 5)/2 = 15$ duads. A *syntheme* is a partition of $A$ into three duads. Each duad is contained in three synthemes (the number of ways of partitioning the remaining four points into two duads), so there are $(15\cdot 3)/3 = 15$ synthemes. Finally, a *synthematic total* is a partition of the 15 duads into five synthemes. It is a little harder to count this; we argue as follows.

Consider two disjoint synthemes; think of them as having two different colours, say red and blue (see the left-hand figure below). The red and blue duads form the edges of a hexagon, and the remaining nine duads are of two types; six "short diagonals" of the hexagon, and three "long diagonals".

It is easy to see that there are two different ways to pick three disjoint duads from these nine: either take the three long diagonals (magenta on the right), or one long diagonal and the two short diagonals perpendicular to it (green in the middle). So the only way to partition these nine duads into three synthemes is to take the three synthemes of the second type.



Thus, any two disjoint synthemes are contained in a unique synthematic total. There are eight synthemes disjoint from a given one; so the number of synthematic totals is $(15\cdot 8)/(5\cdot 4) = 6$. The six synthematic totals are all isomorphic, and so

$S_6$ permutes them transitively. Thus, the stabilisers of synthemes form a conjugacy class of subgroups of index 6, not conjugate to the point stabilisers. Hence we get our outer automorphism.

Using this approach, we can show that the outer automorphism group has order 2: all that is required is to show that any subgroup of index 6 stabilises either a point or a syntheme.

It is an instructive exercise to repeat the construction. Let $X$ be the set of synthemes. Then

- any two synthematic totals share a unique syntheme, so the "duads of $X$" correspond to synthemes of $A$;

- three synthemes containing a given duad lie between them in all the synthematic totals, so the "synthemes of $X$" correspond to duads of $A$;

- the five duads through a point lie between them in all fifteen synthemes, so the "synthematic totals of $X$ correspond to the points of $A$.

Thus, the square of our automorphism is the identity.

## 2.3 Linear groups

In this section we study the next important family of linear groups, the "projective special linear groups" $\mathrm{PSL}(n,F)$. The proof of their simplicity is an application of Iwasawa's Lemma.

### 2.3.1 Finite fields

Our constructions of simple groups in this chapter work over any field, and give finite groups if and only if the field is finite.

The finite fields were classified by Galois (this was one of the few pieces of work published in his lifetime). His theorem is:

**Theorem 2.3.1** *The order of a finite field is a prime power. Conversely, for any prime power $q > 1$, there is a field with $q$ elements, unique up to isomorphism.*

We will not prove this theorem here, since the techniques come from ring theory rather than group theory. Here is a simple example, a field of four elements. We construct it by adjoining to the field $\mathbb{Z}_2$ a root of an irreducible polynomial of degree 2. Of the four polynomials of degree 2 over $\mathbb{Z}_2$, namely,

$$x^2, \quad x^2+1=(x+1)^2, \quad x^2+x=x(x+1), \quad x^2+x+1,$$

only the last is irreducible, so we add an element $\alpha$ satisfying $\alpha^2 = \alpha + 1$. (Remember that, since $-1 = 1$ in $\mathbb{Z}_2$, we have $-u = u$ for any element $u$ in the field we are constructing.) Thus the addition and multiplication tables of our field are the following, where we have put $\beta = \alpha + 1 = \alpha^2$:

| $+$ | $0$ | $1$ | $\alpha$ | $\beta$ |
|---|---|---|---|---|
| $0$ | $0$ | $1$ | $\alpha$ | $\beta$ |
| $1$ | $1$ | $0$ | $\beta$ | $\alpha$ |
| $\alpha$ | $\alpha$ | $\beta$ | $0$ | $1$ |
| $\beta$ | $\beta$ | $\alpha$ | $1$ | $0$ |

| $\cdot$ | $0$ | $1$ | $\alpha$ | $\beta$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $\alpha$ | $\beta$ |
| $\alpha$ | $0$ | $\alpha$ | $\beta$ | $1$ |
| $\beta$ | $0$ | $\beta$ | $1$ | $\alpha$ |

Finite fields are called *Galois fields*. The unique Galois field of given prime power order $q$ is denoted by $\mathbb{F}_q$ or $\mathrm{GF}(q)$. Note that $\mathbb{F}_q \cong \mathbb{Z}_q$ if and only if $q$ is prime.

Note that the additive group of $\mathbb{F}_4$ is the Klein group, while the multiplicative group is cyclic of order 3. This is an instance of a general fact.

**Theorem 2.3.2** *Let $q = p^n$, where $p$ is prime. Then:*

*(a) The additive group of $\mathbb{F}_q$ is elementary abelian of order $q$.*

*(b) The multiplicative group of $\mathbb{F}_q$ is cyclic of order $q - 1$.*

*(c) The automorphism group of $\mathbb{F}_q$ is cyclic of order $n$.*

**Proof** (a) For $n \in \mathbb{N}$ and $u \in \mathbb{F}_q$, let $nu = u + \cdots + u$ ($n$ terms). This is the additive analogue of raising $u$ to the $n$th power.

Since the additive group has order $p^n$, there is an element $u \neq 0$ with order $p$, thus $pu = 0$. But then $pv = (pu)(u^{-1}) = 0$ for all $v \in \mathbb{F}_q$. Thus the additive group is elementary abelian.

(b) Let $k$ be the exponent of the multiplicative group of $\mathbb{F}_q$ (the smallest positive integer such that $u^k = 1$ for all $u \neq 0$). Then $k$ divides the order $q - 1$ of the multiplicative group. But the equation $x^k - 1 = 0$ has at most $k$ solutions. So we must have $k = q - 1$. Now in our proof of the Fundamental Theorem of Finite Abelian Groups, we saw that there is an element whose order is equal to the exponent. So the multiplicative group is cyclic.

(c) We will not prove this, but simply describe an automorphism of the field which generates the automorphism group. This is the *Frobenius map $u \mapsto u^p$*. To show that it is a homomorphism:

$$\begin{aligned}
(u+v)^p &= \sum_{i=0}^{p} \binom{p}{i} u^{p-i} v^i = u^p + v^p, \\
(uv)^p &= u^p v^p.
\end{aligned}$$

In the first line we use the fact that the binomial coefficient $\binom{p}{i}$ is divisible by $p$ for $i = 1, \ldots, p-1$, so that $\binom{p}{i}x = 0$ in $\mathbb{F}_q$.

Now a field has no non-trivial ideals, so the kernel of the Frobenius map is $\{0\}$, that is, it is one-to-one. Since $\mathbb{F}_q$ is a finite set, this implies that the Frobenius map is a bijection, that is, an automorphism.

### 2.3.2 Linear groups

Let $F$ be any field. We denote by $\mathrm{GL}(n,F)$ the group of all invertible $n \times n$ matrices over $F$; this group is the *general linear group* of dimension $n$ over $F$. For brevity, we write $\mathrm{GL}(n,q)$ instead of $\mathrm{GL}(n,\mathbb{F}_q)$. We always assume that $n \geq 2$; for $\mathrm{GL}(1,F)$ is simply the multiplicative group $F^\times$ of $F$, and is abelian (and cyclic if $F$ is finite).

**Proposition 2.3.3**

$$|\mathrm{GL}(n,q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}).$$

**Proof** A matrix is invertible if and only if its rows are linearly independent; this holds if and only if the first row is non-zero and, for $k = 2, \ldots, n$, the $k$th row is not in the subspace spanned by the first $k-1$ rows. The number of possible rows is $q^n$, and the number lying in any $i$-dimensional subspace is $q^i$. So the number of choices of the first row of an invertible matrix is $q^n - 1$, while for $k = 2, \ldots, n$, the number of choices for the $k$th row is $q^n - q^{k-1}$. Multiplying these together gives the result.

Next we investigate normal subgroups of $\mathrm{GL}(n,q)$.

**Proposition 2.3.4** *The determinant map* $\det : \mathrm{GL}(n,F) \to F^\times$ *is a homomorphism.*

**Proof** This is the simple fact from linear algebra that $\det(AB) = \det(A)\det(B)$.

The kernel of the determinant map is the set of $n \times n$ matrices with determinant 1. This is denoted $\mathrm{SL}(n,F)$, the *special linear group* of dimension $n$ over $F$. Thus, $\mathrm{SL}(n,F) \lhd \mathrm{GL}(n,F)$, and

$$\mathrm{GL}(n,F)/\mathrm{SL}(n,F) \cong F^\times$$

(the last fact follows from the First Isomorphism Theorem, since it is easy to see that det is onto: for every element $u \in F$ there exists an $n \times n$ matrix $A$ with $\det(A) = u$.

In particular, we see that

$$|\,\mathrm{SL}(n,q)| = |GL(n,q)|/(q-1).$$

The *projective space* $\mathrm{PG}(n-1,F)$ is the set of 1-dimensional subspaces of $F^n$, the $n$-dimensional vector space over $F$. (Really it is a geometric object and has a lot of structure, but we only need to regard it as a set. Watch out for the confusing dimension shift!) We have

$$|\,\mathrm{PG}(n-1,F)| = \frac{q^n-1}{q-1}.$$

For there are $q^n-1$ non-zero vectors in $F^n$, each of which spans a 1-dimensional subspace; but each 1-dimensional subspace is spanned by any of its $q-1$ non-zero vectors.

There is an action of $\mathrm{GL}(n,F)$ on $\mathrm{PG}(n-1,F)$: the matrix $A$ maps the subspace $\langle v\rangle$ to the subspace $\langle vA\rangle$.

**Proposition 2.3.5** *The following conditions on a matrix $A\in\mathrm{GL}(n,F)$ are equivalent:*

*(a) $A\in Z(GL(n,F))$;*

*(b) A belongs to the kernel of the action of $\mathrm{GL}(n,F)$ on the projective space $\mathrm{PG}(n-1,F)$;*

*(c) A is a scalar matrix, that is, $A=\lambda I$ for some $\lambda\in F^\times$.*

**Proof** (a) ⇔ (c): Clearly scalar matrices commute with everything and so lie in the centre of the group. Suppose $A\in Z(\mathrm{GL}(n,q))$. If $E$ is the matrix with entries 1 on the diagonal and in position $(1,2)$ and zero elsewhere, then $EA$ is obtained from $A$ by adding the second row to the first, while $AE$ is obtained by adding the first column to the second. If these are equal, then the first and second diagonal elements of $A$ are equal, and the other entries in the first column and second row are zero. Repeating the argument for the $i$th row and $j$th column, we conclude that $A$ is a scalar matrix.

(b) ⇔ (c): Again it is clear that a scalar matrix fixes every 1-dimensional subspace. Let $A$ be a matrix which fixes all 1-dimensional subspaces. Let $e_1,\ldots,e_n$ be the standard basis vectors. Then we have $e_iA=\alpha_ie_i$ for $i=1,\ldots,n$, (for some $\alpha_1,\ldots,\alpha_n\in F^\times$), so $A$ is a diagonal matrix. Also,

$$\begin{aligned}(e_i+e_j)A &= \beta(e_i+e_j) \text{ for some } \beta\in F^\times,\\ e_iA+e_jA &= \alpha_ie_i+\alpha_je_j,\end{aligned}$$

so $\alpha_i=\beta=\alpha_j$. Thus $A$ is a scalar matrix.

Thus we see that $Z(\mathrm{GL}(n,F))$ is the group of scalar matrices, and is isomorphic to $F^\times$ (so is cyclic of order $q-1$ if $F=\mathbb{F}_q$).

We define the *projective general and special linear groups* by

$$\mathrm{PGL}(n,F)=\mathrm{GL}(n,F)/Z, \qquad \mathrm{PSL}(n,F)=\mathrm{SL}(n,F)/(Z\cap\mathrm{SL}(n,F)),$$

where $Z=Z(\mathrm{GL}(n,q))$. Thus, the projective groups are the images of the linear groups in the action on the projective space $\mathrm{PG}(n-1,F)$, so we can think of them as groups of permutations of this space.

We have $|\mathrm{PGL}(n,q)|=|\mathrm{GL}(n,q)|/(q-1)=|\mathrm{SL}(n,q)|$. What is the order of $\mathrm{PSL}(n,q)$?

The kernel of the action of $\mathrm{SL}(n,F)$ on the projective space consists of the scalar matrices $\lambda I$ with determinant 1, that is, for which $\lambda^n=1$. If $F=\mathbb{F}_q$, then the multiplicative group is cyclic of order $q-1$, and the number of solutions of $\lambda^n=1$ is $\gcd(n,q-1)$. So we have

$$|\mathrm{PSL}(n,q)|=|\mathrm{SL}(n,q)|/\gcd(n,q-1).$$

In particular, if $\gcd(n,q-1)=1$, then $\mathrm{PSL}(n,q)=\mathrm{PGL}(n,q)=\mathrm{SL}(n,q)$: for in this case, the first group is a subgroup of the second and a quotient of the third, but all three have the same order.

For $n=2$, we find that

$$|\mathrm{PSL}(2,q)|=\begin{cases}(q+1)q(q-1) & \text{if } q \text{ is a power of 2,}\\ (q+1)q(q-1)/2 & \text{if } q \text{ is odd.}\end{cases}$$

In this case, the number of points of $\mathrm{PG}(1,q)$ is $(q^2-1)/(q-1)=q+1$, and so $\mathrm{PGL}(2,q)$ and $\mathrm{PSL}(2,q)|$ are subgroups of the symmetric group $S_{q+1}$. We examine the first few cases.

$q=2$: $\mathrm{PSL}(2,2)=\mathrm{PGL}(2,2)$ is a subgroup of $S_3$ of order $3\cdot 2\cdot 1=6$; so it is isomorphic to $S_3$.

$q=3$: $\mathrm{PGL}(2,3)$ is a subgroup of $S_4$ of order $4\cdot 3\cdot 2=24$; so $\mathrm{PGL}(2,3)\cong S_4$. Also $\mathrm{PSL}(2,3)$ is a subgroup of index 2, so $\mathrm{PSL}(2,3)\cong A_4$.

$q=4$: $\mathrm{PGL}(2,4)=\mathrm{PSL}(2,4)$ is a subgroup of $S_5$ of order $5\cdot 4\cdot 3=60$; so $\mathrm{PSL}(2,4)\cong A_5$.

$q=5$: $\mathrm{PGL}(2,5)$ is a subgroup of $S_6$ of order $6\cdot 5\cdot 4=120$, and hence index 6; so it is the stabiliser of a synthematic total, and hence is isomorphic to $S_5$. Moreover, $\mathrm{PSL}(2,5)$ is a subgroup of index 2, so is isomorphic to $A_5$.

$q=7$: $\mathrm{PSL}(2,7)$ has order $8\cdot 7\cdot 6/2=168$. It turns out to be isomorphic to the group we met on Problem Sheet 1.

There is a simpler way to think of the action of $\mathrm{PSL}(2,F)$ on the projective line. The 1-dimensional subspaces of $F^2$ are of two types: those with a unique spanning vector with first coordinate 1, say $(1,x)$ for $x \in F$; and one spanned by $(0,1)$. We denote points of the first type by the corresponding field element $x$, and the point of the second type by $\infty$. Then the elements of $\mathrm{PGL}(2,F)$ are the *linear fractional* maps

$$x \mapsto \frac{ax+b}{cx+d}$$

for $a,b,c,d \in F$, $ad-bc \neq 0$, with the “natural” conventions for dealing with $\infty$: for $a \neq 0$ we have $a/0 = \infty$, $a\infty = \infty$, and $(b\infty)/(a\infty) = b/a$; also $\infty + c = \infty$ for any $c$. The group $\mathrm{PSL}(2,F)$ consists of those linear fractional maps with $ad-bc = 1$.

### 2.3.3 Simplicity of $\mathrm{PSL}(n,F)$

The main result is:

**Theorem 2.3.6** *For $n \geq 2$ and any field $F$, the group $\mathrm{PSL}(n,F)$ is simple, except in the two cases $n=2$, $F=\mathbb{F}_2$ or $n=2$, $F=\mathbb{F}_3$.*

We saw the two exceptional cases (which are isomorphic to $S_3$ and $A_4$) in the preceding section. The remainder of this section is devoted to the proof of simplicity in the other cases.

We have two preliminary jobs, concerning transitivity and generation.

**Proposition 2.3.7** *For $n \geq 2$, the group $\mathrm{PSL}(n,F)$ acts doubly transitively on the points of the projective space $\mathrm{PG}(n-1,F)$.*

**Proof** Let $\langle v_1 \rangle$ and $\langle v_2 \rangle$ be two distinct 1-dimensional subspaces of $F^n$. Then $v_1$ and $v_2$ are linearly independent, and so for any other pair $\langle w_1 \rangle$ and $\langle w_2 \rangle$, there is a linear map carrying $v_1$ to $w_1$ and $v_2$ to $w_2$. (Simply extend both $(v_1,v_2)$ and $(w_1,w_2)$ to bases, and take the unique linear map taking the first basis to the second.) If this map has determinant $c$, we can follow it by the map multiplying the first basis vector by $c^{-1}$ and fixing the rest to find one with determinant 1 which does the job.

A *transvection* is a linear map of a vector space $V$ of the form $v \mapsto v + f(v)a$, where $a \in V$, $f \in V^*$ (that is, $f$ is a linear map from $V$ to $F$), and $f(a) = 0$. We will call the corresponding map of the projective space a transvection also, though geometers sometimes use the term “elation”. A transvection of $F^2$ is also called a “shear”. We denote the above transvection by $T(a,f)$.

For $a \neq 0$, let $A(a)$ be the set of all transvections $T(a,f)$ with given $a$, as $f$ runs over all elements of $V^*$ satisfying $f(a) = 0$. Since $T(a,f_1)T(a,f_2) =$

$T(a, f_1 + f_2)$, we see that $A(a)$ is an abelian group isomorphic to $\mathrm{Ann}(a)$, the *annihilator* of $a$, a subspace of codimension 1 in $V^*$.

Any transvection belongs to $\mathrm{SL}(n,F)$. (Transvections have determinant 1 since they are represented by strictly upper triangular matrices with respect to a suitable basis. Indeed, if we let $a$ be the first vector in a basis, then a transvection is represented by the matrix

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ * & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ * & 0 & 0 & \dots & 1 \end{pmatrix}$$

whose first column represents the element $f \in V^*$.

The transvection group $A(a)$ acts faithfully on the projective space, since it is clearly disjoint from the group $Z$ of scalar matrices (the kernel of the action). It is obviously normal in the stabiliser of $a$, since it is easy to check that $g^{-1}A(a)g = A(ag)$ for any $g \in \mathrm{PSL}(n,F)$.

**Proposition 2.3.8** *For $n \geq 2$, the group* $\mathrm{PSL}(n,F)$ *is generated by transvections.*

**Proof** We use induction on $n$.

For $n = 2$, represent $\mathrm{PSL}(2,F)$ as the group of linear fractional transformations. The transvections with $a = \langle (0,1) \rangle$ are the maps of the form $x \mapsto x + a$ (fixing $\infty$); they form a group acting transitively on the points different from $\infty$. So the group $H$ generated by all transvections is 2-transitive. It suffices now to show that the stabiliser of two points in $H$ is the same as that in $\mathrm{PSL}(2,F)$.

Now the stabiliser of $\infty$ and 0 in $\mathrm{PSL}(2,F)$ is the group of maps of the form $x \mapsto ax/d$ with $ad = 1$, in other words, $x \mapsto a^2x$. We have to show that we can generate this map by transvections, which we show by the following calculation:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a-1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a-a^2 & 1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}.$$

Now suppose the result is true for $n-1$. Let $H$ be the subgroup of $\mathrm{PSL}(n,F)$ generated by transvections. First, we observe that $G$ is transitive on the projective space, since given two subspaces $\langle a \rangle$ and $\langle b \rangle$, we have transvections of $\langle a, b \rangle$ fixing a complement pointwise, and in the group they generate we can map one point to the other. So it suffices to show that the stabiliser of a point $\langle a \rangle$ is generated by transvections.

Now the stabiliser of $\langle a \rangle$ in $G$ contains all the transvections of $\mathrm{PSL}(n-1,F)$ acting on the quotient space $V/\langle a \rangle$. By induction, these generate $\mathrm{PSL}(n-1,F)$. So if we take an arbitrary element of $\mathrm{PSL}(n,F)$ fixing $\langle a \rangle$, we can multiply it by a suitable product of transvections so that on the quotient space it is diagonal with all but one diagonal entry equal to 1. That is, we can reduce to a matrix of the form

$$\begin{pmatrix} \lambda & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ x_1 & x_2 & \dots & x_{n-1} & \lambda^{-1} \end{pmatrix}.$$

By further multiplication by transvections we can reduce to the case where $x_1 = \ldots = x_{n-1} = 0$. Now apart from the identity in the middle, we have just the matrix

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$$

which is dealt with as in the case $n = 2$.

**Proof of the Theorem** First, we recall the statement of Iwasawa's Lemma:

**Theorem 2.3.9** *Let $G$ be a group with a faithful primitive action on $\Omega$. Suppose that there is an abelian normal subgroup $A$ of* Stab$(\alpha)$ *with the property that the conjugates of $A$ generate $G$. Then any non-trivial normal subgroup of $G$ contains $G'$. In particular, if $G = G'$, then $G$ is simple.*

We will take $G = \mathrm{PSL}(n,F)$ acting on $\Omega = \mathrm{PG}(n-1,F)$. (The action is doubly transitive and hence primitive.) We have seen that the transvection group $A(a)$ is abelian and normal in the stabiliser of $\langle a \rangle$, and that its conjugates generate $G$. So only one thing remains to be proved:

**Proposition 2.3.10** *For $n \geq 2$, the group* $\mathrm{PSL}(n,F)$ *is equal to its derived group except in the cases $n = 2$, $F = \mathbb{F}_2$, and $n = 2$, $F = \mathbb{F}_3$.*

**Proof** Since all transvection groups are conjugate, it suffices to find a transvection group in the derived group; that is, to express the elements of one transvection group as commutators.

Suppose first that $|F| > 3$. It suffices to do the case $n = 2$, since all the calculations below can be done in the upper left-hand corner of a matrix with the identity in the bottom right and zeros elsewhere. Since $|F| > 3$, there is an element $a \in F$ satisfying $a^2 \neq 0, 1$. Then $\mathrm{SL}(2,F)$ contains the matrix $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$, as we saw above; and

$$\begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1 & (a^2-1)x \\ 0 & 1 \end{pmatrix},$$

and $(a^2-1)x$ runs through $F$ as $x$ does.

Now suppose that $n \geq 3$, and that $|F| = 2$ or $|F| = 3$ (indeed this argument works for all $F$). Again we need only consider $3\times 3$ matrices. We have

$$\begin{pmatrix} 1 & -x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

The proof is complete.

# Exercises

**2.1** Consider the regular action of $G$ on itself by right multiplication. Show that there is a congruence $\equiv_H$ for each subgroup $H$ of $G$, whose classes are the right cosets of $H$, and that these are all the congruences.

**2.2** Show that the actions of $G$ on the coset spaces $\cos(H,G)$ and $\cos(K,G)$ are isomorphic if and only if the subgroups $H$ and $K$ are conjugate.

**2.3** Let $G$ be the symmetry group of the cube. Show that the action of $G$ on the set of vertices of the cube is transitive but imprimitive, and describe all the congruences. Repeat for the action of $G$ on the set of faces, and on the set of edges.

**2.4** An *automorphism* of a group $G$ is an isomorphism from $G$ to itself. An *inner automorphism* of $G$ is a conjugation map, one of the form $c_g : x \mapsto g^{-1}xg$.

(a) Show that the set of automorphisms, with the operation of conjugation, is a group $\mathrm{Aut}(G)$.

(b) Show that the set of inner automorphisms is a subgroup $\mathrm{Inn}(G)$ of $\mathrm{Aut}(G)$.

(c) Show that $\mathrm{Inn}(G) \cong G/Z(G)$, where $Z(G)$ is the centre of $G$.

(d) Show that $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$. (The quotient $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is defined to be the *outer automorphism group* $\mathrm{Out}(G)$ of $G$.)

**2.5** Let $G$ be a group. Then there is in a natural way an action of the automorphism group $\mathrm{Aut}(G)$ of $G$ on the set $G$. The identity is fixed by all automorphisms, so $\{1\}$ is an orbit of size 1 for this action.

(a) Suppose that $G\setminus\{1\}$ is an orbit for $\mathrm{Aut}(G)$. Show that all non-identity elements of $G$ have the same order, and deduce that the order of $G$ is a power of a prime $p$, and hence that $G$ is an elementary abelian $p$-group.

(b) Suppose that $\mathrm{Aut}(G)$ acts doubly transitively on $G \setminus \{1\}$. Show that either $|G| = 2^d$ for some $d$, or $|G| = 3$.

(c) Suppose that $\mathrm{Aut}(G)$ acts triply transitively on $G \setminus \{1\}$. Show that $|G| = 4$.

**2.6** Show that a permutation group which acts primitively on $\{1, \dots, n\}$ and contains a transposition is the symmetric group $S_n$.

**2.7** Show that a permutation group which acts primitively on $\{1, \dots, n\}$ and contains a 3-cycle is the symmetric group $S_n$ or the alternating group $A_n$.

**2.8** Let $n \geq 2$. Let $G$ be the symmetric group $S_n$ of permutations of $\{1, 2, \dots, n\}$. Let $\Omega$ be the set of 2-element subsets of $\{1, 2, \dots, n\}$. There is a "natural" action of $G$ on $\Omega$ given by $\{i, j\}g = \{ig, jg\}$. (You are not required to show that this is an action.) Prove the following assertions:

(a) If $n = 2$, the action is not faithful.

(b) If $n = 3$, the action is doubly transitive.

(c) If $n = 4$, the action is imprimitive.

(d) If $n \geq 5$, the action is primitive but not doubly transitive.

**2.9** Show that the outer automorphism of $S_6$ interchanges the conjugacy classes of types $[1,1,1,1,2]$ and $[2,2,2]$, those of types $[1,1,1,3]$ and $[3,3]$, and those of types $[1,2,3]$ and $[6]$, and fixes the other classes.

**2.10** Let $\mathrm{Aut}(G)$ denote the automorphism group of the group $G$.

(a) Let $V_4$ denote the Klein group. Prove that $\mathrm{Aut}(V_4) \cong S_3$.

(b) Prove that $\mathrm{Aut}(S_3) \cong S_3$.

(c) Find another group $G$ such that $\mathrm{Aut}(G) \cong G$.

(d) Let $G$ be the elementary abelian group of order 8. Prove that $|\mathrm{Aut}(G)| = 168$. Is there any connection with the question on Problem Sheet 1?

**2.11** Let $G$ be a finite group of order greater than 2. Prove that $G$ has a non-identity automorphism. (Hint: treat abelian and non-abelian groups separately.)

**Remark:** It is also true that, if $G$ is an infinite group, then $G$ has a non-identity automorphism; but the proof requires the Axiom of Choice. (Can you prove this?)

**2.12** (a) Construct addition and multiplication tables for a field with eight elements. [I hope you have met this before, and that this question is revision.]

(b) Prove that any two fields with eight elements are isomorphic. [*Hint:* you probably used an irreducible polynomial of degree 3 over $\mathbb{Z}_2$ in your construction: there are two such polynomials. If you use one polynomial in the construction, show that the field you construct also contains a root of the other polynomial.]

**2.13** Let $G$ be a subgroup of $G$. Let $N_G(H)$ be the *normaliser* of $H$ in $G$, the largest subgroup of $G$ in which $H$ is contained as a normal subgroup. Alternatively,

$$N_G(H) = \{g \in G : g^{-1}Hg = H\}.$$

(a) Prove that, in the action of $G$ on the coset space $\cos(H,G)$, a coset $Hg$ is fixed by $H$ if and only if $g \in N_G(H)$.

(b) Suppose that $|G| = p^n$, where $p$ is prime, and that $H < G$. Prove that $H < N_G(H)$. (Recall that $H < G$ means "$H$ is a subgroup of $G$ and $H \neq G$".)

**2.14** Show that

(a) $\mathrm{SL}(2,F)$ does not contain a subgroup isomorphic to $\mathrm{PSL}(2,F)$;

(b) if $F = \mathrm{GF}(q)$ with $q > 3$, then the only composition series for $\mathrm{SL}(2,q)$ is $\{I\} \lhd \{\pm I\} \lhd \mathrm{SL}(2,q)$;

(c) $\mathrm{SL}(2,q)$ is not isomorphic to $C_2 \times \mathrm{PSL}(2,q)$.

**2.15** Consider $G = \mathrm{PGL}(2,F)$ as the group of linear fractional transformations $x \mapsto (ax+b)/(cx+d)$ of $F \cup \{\infty\}$ with $ad - bc \neq 0$.

(a) Show that $G$ acts transitively.

(b) Show that the stabiliser of $\infty$ is the "affine group" of all transformations $x \mapsto ax+b$ with $a \neq 0$. Deduce that $G$ is doubly transitive.

(c) Show that the stabiliser of $\infty$ and $0$ is the multiplicative group of $F$. Deduce that $G$ is triply transitive and that the stabiliser of any three points is the identity.

**2.16** Show that there is no simple group whose order is the product of three distinct primes.

**2.17** Let $V$ consist of the $\binom{6}{2} = 15$ 2-element subsets of $\{1,2,3,4,5,6\}$, together with one extra symbol 0. Define an operation $\oplus$ on $V$ by the rules

- $v \oplus 0 = 0 \oplus v = v$ and $v \oplus v = 0$ for any $\in V$;
- $\{a,b\} \oplus \{a,c\} = \{b,c\}$ for all distinct $a,b,c \in \{1,\dots,6\}$;
- $\{a,b\} \oplus \{c,d\} = \{e,f\}$ if $\{a,\dots,f\} = \{1,\dots,6\}$.

Prove that $(V,\oplus)$ is an elementary abelian 2-group of order 16, that is, the additive group of a 4-dimensional vector space over $\mathbb{F}_2$. Deduce that $S_6$ is a subgroup of $\mathrm{GL}(4,2)$. What is its index?

**2.18** This (quite difficult) question outlines a proof that any simple group of order 168 is isomorphic to $\mathrm{PSL}(2,7)$. Let $G$ be a simple group of order 168.

(a) Show that $G$ has 8 Sylow 7-subgroups, and that the normaliser of one such subgroup, say $P$, has order 21.

(b) Hence show that $G$ acts doubly transitively on a set of 8 points, and the stabiliser of a point acts as the group

$$N = \{x \mapsto ax+b : a \in \{1,2,4\}, b \in \mathbb{Z}_7\}$$

of $\mathbb{Z}_7$. Deduce that the identity and the two maps $x \mapsto 2x$ and $x \mapsto 4x$ form a Sylow 3-subgroup $Q$ of $G$.

(c) Let the stabilised point be named $\infty$. Show that there is an element $t$ of order 2 in $G$ which interchanges $\infty$ and normalises $Q$.

(d) Show that $t$ is an even permutation, and deduce that it must interchange the two sets $\{1,2,4\}$ and $\{3,5,6\}$.

(e) By laborious computation (which you may omit), show that necessarily $t = (\infty,0)(1,6)(2,3)(4,5)$; in other words, $t$ is the map $x \mapsto -1/x$.

(f) Show that $N$ and $t$ generate $G$.

(g) Now every element of $G$ lies in $\mathrm{PSL}(2,7)$ (the group of linear fractional transformations of $\{\infty\} \cup \mathbb{Z}_7$. By comparing orders, $G = \mathrm{PSL}(2,7)$.

# Chapter 3

# Group extensions

## 3.1 Semidirect product

### 3.1.1 Definition and properties

Let $A$ be a normal subgroup of the group $G$. A *complement* for $A$ in $G$ is a subgroup $H$ of $G$ satisfying

- $HA = G$;
- $H \cap A = \{1\}$.

It follows that every element of $G$ has a *unique* expression in the form $ha$ for $h \in H$, $a \in A$. For, if $h_1a_1 = h_2a_2$, then

$$h_2^{-1}h_1 = a_2a_1^{-1} \in H \cap A = \{1\},$$

so $h_2^{-1}h_1 = a_2a_1^{-1} = 1$, whence $h_1 = h_2$ and $a_1 = a_2$.

We are going to give a general construction for a group with a given normal subgroup and a given complement. First some properties of complements.

**Proposition 3.1.1** *Let $H$ be a complement for the normal subgroup $A$ of $G$. Then*

*(a) $H \cong G/A$;*

*(b) if $G$ is finite then $|A| \cdot |H| = |G|$.*

**Proof** (a) We have

$$G/A = HA/A \cong H/H \cap A = H,$$

the first equality because $G = HA$, the isomorphism by the Third Isomorphism Theorem, and the second equality because $H \cap A = \{1\}$.

(b) Clear.

**Example** There are two groups of order 4, namely the cyclic group $C_4$ and the Klein group $V_4$. Each has a normal subgroup isomorphic to $C_2$; in the Klein group, this subgroup has a complement, but in the cyclic group it doesn't. (The complement would be isomorphic to $C_2$, but $C_4$ has only one subgroup isomorphic to $C_2$.)

If $A$ is a normal subgroup of $G$, then $G$ acts on $A$ by conjugation; the map $a \mapsto g^{-1}ag$ is an automorphism of $A$. Suppose that $A$ has a complement $H$. Then, restricting our attention to $A$, we have for each element of $H$ an automorphism of $A$, in other words, a map $\phi : H \to \mathrm{Aut}(A)$. Now this map is an automorphism: for

- $(g\phi)(h\phi)$ maps $a$ to $h^{-1}(g^{-1}ag)h$,
- $(gh)\phi$ maps $a$ to $(gh)^{-1}a(gh)$,

and these two expressions are equal. We conclude that, if the normal subgroup $A$ has a complement $H$, then there is a homomorphism $\phi : H \to \mathrm{Aut}(A)$.

Conversely, suppose that we are given a homomorphism $\phi : H \to \mathrm{Aut}(A)$. For each $h \in H$, we denote the image of $a \in A$ under $h\phi$ by $a^h$, to simplify the notation. Now we make the following construction:

- we take as set the Cartesian product $H \times A$ (the set of ordered pairs $(h,a)$ for $h \in H$ and $a \in A$);
- we define an operation on this set by the rule
$$(h_1,a_1) * (h_2,a_2) = (h_1h_2, a_1^{h_2}a_2).$$

We will see the reason for this slightly odd definition shortly.

Closure obviously holds; the element $(1_H, 1_A)$ is the identity; and the inverse of $(h,a)$ is $(h^{-1},(a^{-1})^{h^{-1}})$. (One way round, we have

$$(h,a) * (h^{-1},(a^{-1})^{h^{-1}}) = (hh^{-1}, a^{h^{-1}}(a^{-1})^{h^{-1}}) = (1_H, 1_N);$$

you should check the product the other way round for yourself.) What about the associative law? If $h_1,h_2,h_3 \in H$ and $a_1,a_2,a_3 \in N$, then

$$\begin{aligned}((h_1,a_1)*(h_2,a_2))*(h_3,a_3) &= (h_1h_2, a_1^{h_2}a_2)*(h_3,a_3) = (h_1h_2h_3,(a_1^{h_2}a_2)^{h_3}a_3),\\ (h_1,a_1)*((h_2,a_2)*(h_3,a_3)) &= (h_1,a_1)*(h_2h_3,a_2^{h_3}a_3) = (h_1h_2h_3,a_1^{h_2h_3}a_2^{h_3}a_3),\end{aligned}$$

and the two elements on the right are equal.

So we have constructed a group, called the *semi-direct product* of $A$ by $H$ using the homomorphism $\phi$, and denoted by $A \rtimes_\phi H$. If the map $\phi$ is clear, we sometimes simply write $A \rtimes H$. Note that the notation suggests two things: first, that $A$ is the normal subgroup; and second, that the semi-direct product is a generalisation of the direct product. We now verify this fact.

**Proposition 3.1.2** *Let $\phi : H \to \mathrm{Aut}(A)$ map every element of $H$ to the identity automorphism. Then $A \rtimes_\phi H \cong A \times H$.*

**Proof** The hypothesis means that $a^h = n$ for all $a \in A$, $h \in H$. So the rule for the group operation in $A \rtimes_\phi H$ simply reads

$$(h_1, a_1) * (h_2, a_2) = (h_1 h_2, a_1 a_2),$$

which is the group operation in the direct product.

**Theorem 3.1.3** *Let $G$ be a group with a normal subgroup $A$ and a complement $H$. Then $G \cong A \rtimes_\phi H$, where $\phi$ is the homomorphism from $H$ to $\mathrm{Aut}(A)$ given by conjugation.*

**Proof** As we saw, every element of $G$ has a unique expression in the form $ha$, for $h \in H$ and $a \in A$; and

$$(h_1 a_1)(h_2 a_2) = h_1 h_2 (h_2^{-1} a_1 h_2) a_2 = (h_1 h_2)(a_1^{h_2} a_2),$$

where $a_1^{h_2}$ here means the image of $a_1$ under conjugation by $h_2$. So, if $\phi$ maps each element $h \in H$ to conjugation of $A$ by $h$ (an automorphism of $A$), we see that the map $ha \mapsto (h, a)$ is an isomorphism from $G$ to $A \rtimes_\phi H$.

**Example:** Groups of order $pq$, where $p$ and $q$ are distinct primes. Let us suppose that $p > q$. Then there is only one Sylow $p$-subgroup $P$, which is therefore normal. Let $Q$ be a Sylow $q$-subgroup. Then $Q$ is clearly a complement for $P$; so $G$ is a semi-direct product $P \rtimes_\phi Q$, for some homomorphism $\phi : Q \to \mathrm{Aut}(P)$.

Now $\mathrm{Aut}(C_p) \cong C_{p-1}$ (see below). If $q$ does not divide $p-1$, then $|Q|$ and $|\mathrm{Aut}(P)|$ are coprime, so $\phi$ must be trivial, and the only possibility for $G$ is $C_p \times C_q$. However, if $q$ does divide $p-1$, then $\mathrm{Aut}(C_p)$ has a unique subgroup of order $q$, and $\phi$ can be an isomorphism from $C_q$ to this subgroup. We can choose a generator for $C_q$ to map to a specified element of order $q$ in $\mathrm{Aut}(C_p)$. So there is, up to isomorphism, a unique semi-direct product which is not a direct product.

In other words, the number of groups of order $pq$ (up to isomorphism) is 2 if $q$ divides $p-1$, and 1 otherwise.

Why is $\mathrm{Aut}(C_p) \cong C_{p-1}$? Certainly there cannot be more than $p-1$ automorphisms; for there are only $p-1$ possible images of a generator, and once one is chosen, the automorphism is determined. We can represent $C_p$ as the additive group of $\mathbb{Z}_p$, and then multiplication by any non-zero element of this ring is an automorphism of the additive group. So $\mathrm{Aut}(C_p)$ is isomorphic to the multiplicative group of $\mathbb{Z}_p$. The fact that this group is cyclic is a theorem of number theory (a generator for this cyclic group is called a *primitive root* mod $p$). We simply refer to Number Theory notes for this fact.

### 3.1.2 The holomorph of a group

Let $A$ be any group. Take $H = \mathrm{Aut}(A)$, and let $\phi$ be the identity map from $H$ to $\mathrm{Aut}(A)$ (mapping every element to itself). Then the semidirect product $A \rtimes_\phi \mathrm{Aut}(A)$ is called the *holomorph* of $A$.

**Example** Let $A$ be the Klein group. Its automorphism group is the symmetric group $S_3$. The holomorph $V_4 \rtimes S_3$ is the symmetric group $S_4$.

**Example** Let $p$ be a prime and $n$ a positive integer. Let $A$ be the elementary abelian group of order $p^n$ (the direct product of $n$ copies of $C_p$). Show that $\mathrm{Aut}(A) = \mathrm{GL}(n,p)$. The holomorph of $A$ is called the *affine group* of dimension $n$ over $\mathbb{Z}_p$, denoted by $\mathrm{AGL}(n,p)$. **Exercise:** Write down its order.

### 3.1.3 Wreath product

Here is another very important example of a semidirect product. Let $F$ and $H$ be groups, and suppose that we are also given an action of $H$ on the set $\{1,\dots,n\}$. Then there is an action of $H$ on the group $F^n$ (the direct product of $n$ copies of $F$) by "permuting the coordinates": that is,

$$(f_1, f_2, \dots, f_n)^h = (f_{1h}, f_{2h}, \dots, f_{nh})$$

for $f_1,\dots,f_n \in F$ and $h \in H$, where $ih$ is the image of $i$ under $h$ in its given action on $\{1,\dots,n\}$. In other words, we have a homomorphism $\phi$ from $H$ to $\mathrm{Aut}(F^n)$. The semi-direct product $F^n \rtimes_\phi H$ is known as the *wreath product* of $F$ by $H$, and is written $F \,\mathrm{Wr}\, H$ (or sometimes as $F \wr H$).

**Example** Let $F = H = C_2$, where $H$ acts on $\{1,2\}$ in the natural way. Then $F^2$ is isomorphic to the Klein group $\{1,a,b,ab\}$, where $a^2 = b^2 = 1$ and $ab = ba$. If $H = \{h\}$, then we have $a^h = b$ and $b^h = a$; the wreath product $F \,\mathrm{Wr}\, H$ is a group of order 8. Prove that it is isomorphic to the dihedral group $D_8$ (see also below).

There are two important properties of the wreath product, which I will not prove here. The first shows that it has a "universal" property for imprimitive permutation groups.

Let $G$ be a permutation group on $\Omega$, (This means that $G$ acts faithfully on $\Omega$, so that $G$ is a subgroup of the symmetric group on $\Omega$, and assume that $G$ acts imprimitively on $\Omega$. Recall that this means there is an equivalence relation on $\Omega$ which is non-trivial (not equality or the universal relation) and is preserved by $G$. In this situation, we can produce two smaller groups which give information about $G$:

- $H$ is the permutation group induced by $G$ on the set of congruence classes, that is, the image of the action of $G$ on the equivalence classes).
- Let $\Delta$ be a congruence class, and $F$ the permutation group induced on $\Delta$ by its setwise stabiliser in $G$.

**Theorem 3.1.4** *With the above notation, G is isomorphic to a subgroup of* $F\,\mathrm{Wr}\,H$.

**Example** The partition $\{\{1,2\},\{3,4\}\}$ of $\{1,2,3,4\}$ is preserved by a group of order 8, which is isomorphic to $D_8$. The two classes of the partition are permuted transitively by a group isomorphic to $C_2$; and the subgroup fixing $\{1,2\}$ setwise also acts on it as $C_2$. The theorem illustrates that $C_2\,\mathrm{Wr}\,C_2 \cong D_8$; we can write the elements down explicitly as permutations. With the earlier notation, $a=(1,2)$, $b=(3,4)$, and $H=(1,3)(2,4)$.

The other application concerns group extensions, a topic we return to in the next section of the notes. Let $F$ and $H$ be arbitrary groups. An *extension* of $F$ by $H$ refers to any group $G$ which has a normal subgroup isomorphic to $F$ such that the quotient is isomorphic to $H$. Note that the semi-direct product is an extension.

**Theorem 3.1.5** *Every extension of F by H is isomorphic to a subgroup of* $F\,\mathrm{Wr}\,H$.

**Example** There are two extensions of $C_2$ by $C_2$, namely $C_4$ and the Klein group $V_4$. We find them in the wreath product, using the earlier notation, as follows:

- $\langle ah\rangle = \langle(1,4,2,3)\rangle \cong C_4$ (note that $(ah)^2 = ahah = aa^h = ab$);
- $\langle ab,h\rangle = \langle(1,2)(3,4),(1,3)(2,4)\rangle \cong V_4$.

## 3.2 Extension theory

In this section we tackle the harder problem of describing all *extensions* of a group $A$ by a group $H$; that is, all groups $G$ which have a normal subgroup (isomorphic to) $A$ with quotient $G/A$ isomorphic to $H$. As suggested, we will call the normal subgroup $A$.

We will assume in this chapter that $A$ is abelian. Later we will discuss briefly why we make this assumption.

We begin as in the preceding section of the notes. The group $G$ acts on $A$ by conjugation: that is, we have a homomorphism $\phi : G \to \mathrm{Aut}(A)$. Since $A$ is abelian, its action on itself by conjugation is trivial; that is, $A \le \mathrm{Ker}(\phi)$. Now we have the following useful result, which can be regarded as a generalisation of the First Isomorphism Theorem:

**Proposition 3.2.1** *Let $\theta : G \to H$ be a group homomorphism, and suppose that $N$ is a normal subgroup of $G$ satisfying $N \leq \mathrm{Ker}(\theta)$. Then $\theta$ induces a homomorphism $\bar{\theta} : G/N \to H$.*

**Proof** Of course, we would like to define $(Ng)\bar{\theta} = g\theta$. We have to check that this is well-defined. So suppose that $Ng_1 = Ng_2$, so that $g_2(g_1)^{-1} \in N$. Then by assumption, $(g_2(g_1^{-1}))\theta = 1_H$, and so $g_1\theta = g_2\theta$, as required.

Now proving that $\bar{\theta}$ is a homomorphism is a routine check, which you should do for yourself.

In our case, $A \leq \mathrm{Ker}\,\phi$, so $\phi$ induces a homomorphism (which we will also call $\phi$, by abuse of notation) from $H \cong G/A$ to $\mathrm{Aut}(A)$.

Note that we are now in the same situation as the case where there is a complement: we have a homomorphism from $H$ to $\mathrm{Aut}(A)$. Now here are a few questions for you to think about:

- What goes wrong if $A$ is not abelian?
- Is it possible that the same extension gives rise to different homomorphisms (in the case where $A$ is abelian)? Is this possible in the case where $A$ has a complement in $G$?
- (much harder) Is there an extension of $A$ by $H$ in which we cannot define a homomorphism from $H$ to $\mathrm{Aut}(A)$ to describe the conjugation action? ($A$ has to be non-abelian and not complemented.)

Now we begin to describe the group $G$. First of all, since $G/A$ is isomorphic to $H$, we can label the cosets of $A$ in $G$ by elements of $H$ (their images under the homomorphism from $G/A$ to $H$). How do we describe the elements of $G$? For this, we need to choose a set of coset representatives. Let $r(h)$ be the representative of the coset corresponding to $H$. We can, and shall, assume that $r(1) = 1$ (use the identity as representative of the coset $A$). If there is a complement we could use its elements as coset representatives; but in general this is not possible. Note that we have

$$r(h)^{-1}ar(h) = a^h,$$

where $a^h$ is shorthand for the image of $A$ under the automorphism $h\phi$.

Now, for $h_1, h_2 \in H$, the element $r(h_1)r(h_2)$ lies in the coset labelled by $h_1h_2$, but it is not necessarily equal to $r(h_1h_2)$. So we define a "fudge factor" to give us the difference between these elements:

$$r(h_1)r(h_2) = r(h_1h_2)f(h_1,h_2)$$

where $f(h_1,h_2) \in A$. Thus $f$ is a function from $H \times H$ to $A$ (that is, it takes two arguments in $H$ and outputs an element of $A$).

Now we are ready to examine the group $G$. Each element of $G$ has a unique representation in the form $r(h)a$ where $h \in H$ and $a \in A$. Said otherwise, there is a bijection between $H \times A$ (as a set) and $G$. What happens when we multiply two elements?

$$\begin{aligned} r(h_1)a_1r(h_2)a_2 &= r(h_1)r(h_2)a_1^{h_2}a_2 \\ &= r(h_1h_2)f(h_1,h_2)a_1^{h_2}a_2. \end{aligned}$$

At this point we are going to change our notation and write the group operation in $A$ as addition. So the product of $r(h_1)a_1$ and $r(h_2)a_2$ has coset representative $r(h_1h_2)$ and differs from it by the element $a_1^{h_2} + a_2 + f(h_1,h_2)$ of $A$. We will simplify notation in another way too. Instead of writing an element of $G$ as $r(h)a$, we will write it as the corresponding element $(h,a)$ of $H \times A$.

Before going on, let us look at a special case. What does it mean if $f(h_1,h_2) = 0$ for all $h_1,h_2 \in H$? This means that the chosen coset representatives require no fudge factor at all: $r(h_1)r(h_2) = r(h_1,h_2)$. This just means that $r$ is a homomorphism from $H$ to $G$, and its image is a complement for $A$. This is the semi-direct product case. So the function $f$ should measure how far we are from a semi-direct product. So it does, but things are a little more complicated . . .

Here is another special case. In primary school you learned how to add two-digit numbers. What is $37+26$? You add 7 and 6, giving 13; you write down 3 and carry 1. Then you add 3 and 2 together with the carried 1 to get 6, so the answer is 63. If you did all your calculations mod 10 and didn't worry about carrying, the answer would be 53. Said another way, the sum of the elements $(3,7)$ and $(2,6)$ in $\mathbb{Z}_{10} \times \mathbb{Z}_{10}$ is $(5,3)$. But there is another extension of $\mathbb{Z}_{10}$ by $\mathbb{Z}_{10}$, namely $\mathbb{Z}_{100}$, which has a normal subgroup $A$ (consisting of the multiples of 10) isomorphic to $\mathbb{Z}_{10}$ with quotient group $\mathbb{Z}_{10}$. If we use $(a,x)$ to denote the element $10a+x$ (belonging to the coset of $A$ containing $x$), then $(3,7)+(2,6) = (6,3)$. The carried 1 is exactly what we described as a fudge factor before. So in this case

$$f(x,y) = \begin{cases} 0 & \text{if } x+y \leq 9, \\ 1 & \text{if } x+y \geq 10. \end{cases}$$

So you should think of the function $f$ as a generalisation of the rules for carrying in ordinary arithmetic, to any group extension with abelian normal subgroup and arbitrary quotient.

The function $f$ is not arbitrary, but must satisfy a couple of conditions. The fact that $r(1) = 0$ shows that $f(1,h) = f(h,1) = 0$ for all $h \in H$. (Remember that we are writing $A$ additively, so the identity is now 0.) Also, let's do the calculation for the associative law. To simplify matters I will just work it out for elements of the form $(h,0)$.

$$\begin{aligned}((h_1,0)(h_2,0))(h_3,0) &= (h_1h_2,f(h_1,h_2))(h_3,0)=(h_1h_2h_3,f(h_1,h_2)^{h_3}+f(h_1h_2,h_3)),\\ (h_1,0)((h_2,0)(h_3,0)) &= (h_1,0)(h_2h_3,f(h_2,h_3))=(h_1h_2h_3,f(h_1,h_2h_3)+f(h_2,h_3))\end{aligned}$$

So the function $f$ must satisfy

$$f(h_1,h_2)^{h_3}+f(h_1h_2,h_3)=f(h_1,h_2h_3)+f(h_2,h_3)$$

for all $h_1,h_2,h_3\in H$.

Accordingly, we make a definition. Let $A$ be an abelian group (written additively), and $H$ a group. Let a homomorphism $\phi : H \to \mathrm{Aut}(A)$ be given; write the image of $a$ under $h\phi$ as $a^h$. A *factor set* is a function $f : H\times H\to A$ satisfying

- $f(1,h)=f(h,1)=0$ for all $h\in H$;
- $(h_1,h_2)^{h_3}+f(h_1h_2,h_3)=f(h_1,h_2h_3)+f(h_2,h_3))$ for all $h_1,h_2,h_3\in H$.

**Theorem 3.2.2** *Given an abelian group $A$, a group $H$, a homomorphism $\phi : H \to$ $\mathrm{Aut}(A)$, and a factor set $f$, define an operation on $H\times A$ by the rule*

$$(h_1,a_1)*(h_2,a_2)=(h_1h_2,a_1^{h_2}+a_2+f(h_1,h_2)).$$

*Then $(H\times A,*)$ is a group; it is an extension of $A$ by $H$, where the action of $H$ on $A$ is given by $\phi$, and the "fudge factor" for a suitable choice of coset representatives by $f$.*

However, this is not the end of the story. Before we continue, let us make two simple observations.

**Proposition 3.2.3** *Given $A$, $H$ and $\phi$, the set of all factor sets is an abelian group, with operation given by*

$$(f+f')(h_1,h_2)=f(h_1,h_2)+f'(h_1,h_2).$$

We will denote this group by $\mathrm{FS}(A,H,\phi)$.

**Proposition 3.2.4** *If the chosen coset representatives form a complement for $A$ in $G$, then the corresponding factor set is identically zero.*

The reason why there is more to do lies in the choice of coset representatives. Suppose that the function $s$ defines another choice of coset representatives. The values $r(h)$ and $s(h)$ are in the same coset of $A$, so they differ by an element of $A$; say $s(h) = r(h)d(h)$, where $d$ is a function from $H$ to $A$. Since $r(1) = s(1) = 0$, we have $d(1) = 0$.

Let $f_r$ and $f_s$ be the factor sets corresponding to the coset representatives $r$ and $s$. Then

$$\begin{array}{rcl} r(h_1h_2)d(h_1h_2)f_s(h_1,h_2) & = & s(h_1h_2)f_s(h_1,h_2) \\ & = & s(h_1)s(h_2) \\ & = & r(h_1)d(h_1)r(h_2)d(h_2) \\ & = & r(h_1)r(h_2)d(h_1)^{h_2}d(h_2) \\ & = & r(h_1h_2)f_r(h_1,h_2)d(h_1)^{h_2}d(h_2). \end{array}$$

Reverting to additive notation, we see that

$$f_s(h_1,h_2) - f_r(h_1,h_2) = d(h_1)^{h_2} + d(h_2) - d(h_1h_2).$$

Now let $d$ be any *function* from $H$ to $A$ satisfying $d(1) = 0$, and define a function $\delta d : H \times H \to A$ by

$$\delta d(h_1,h_2) = d(h_1)^{h_2} + d(h_2) - d(h_1h_2).$$

Then some calculation shows that $\delta d$ is a factor set. The special factor sets of this form are called *inner factor sets*.

Now at last we can summarise our conclusions.

**Theorem 3.2.5** *Let the abelian group $A$, the group $H$, and the map $\phi : H \to \mathrm{Aut}(A)$ be given.*

*(a) The factor sets form an abelian group* $\mathrm{FS}(H,A,\phi)$*, and the inner factor sets form a subgroup* $\mathrm{IFS}(H,A,\phi)$ *of* $\mathrm{FS}(H,A,\phi)$.

*(b) Two factor sets arise from different choices of coset representatives in the same extension if and only if their difference is an inner factor set.*

We define the *extension group* $\mathrm{Ext}(H,A,\phi)$ to be the quotient $\mathrm{FS}(H,A,\phi)/IFS(H,A,\phi)$. Now the elements of $\mathrm{Ext}(H,A,\phi)$ "describe" extensions of $A$ by $H$ with action $\phi$. In particular,

- the zero element of $\mathrm{Ext}(H,A,\phi)$ describes the semidirect product $A \rtimes_\phi H$;
- if $\mathrm{Ext}(H,A,\phi) = \{0\}$, then the only extension of $A$ by $H$ with action $\phi$ is the semi-direct product $A \rtimes_\phi H$.

We say that an extension of $A$ by $H$ *splits* if it is a semi-direct product; the last conclusion can be expressed in the form "if $\mathrm{Ext}(H,A,\phi) = \{0\}$ then any extension of $A$ by $H$ with action $\phi$ splits".

There is one important case where this holds.

**Theorem 3.2.6 (Schur's Theorem)** *Suppose that $A$ is an abelian group and $H$ a group satisfying* $\gcd(|A|,|H|) = 1$*, Then any extension of $A$ by $H$ splits.*

**Proof** Let $m = |A|$ and $n = |H|$. Now if $f$ is any factor set, then $mf(h_1,h_2) = 0$ for any $h_1,h_2 \in H$; in other words, $mf = 0$ in $\mathrm{FS}(H,A,\phi)$, and so $m\overline{f} = 0$ in $\mathrm{Ext}(H,A,\phi)$, where $\overline{f}$ is the image of $f$ in FS / IFS.

We now show that $nf$ is an inner factor set. Define a function $d : H \to A$ by

$$d(h) = \sum_{h_1 \in H} f(h_1,h).$$

Consider the equation

$$f(h_1,h_2)^{h_3} + f(h_1h_2,h_3) = f(h_1,h_2h_3) + f(h_2,h_3)).$$

Sum this equation over $h_1 \in H$; we obtain

$$d(h_2)^{h_3} + d(h_3) = d(h_2h_3) + nf(h_2,h_3),$$

where we obtain $d(h_3)$ in the second term because $h_1h_2$ runs through $H$ as $h_1$ does. Thus,

$$nf(h_2,h_3) = d(h_2)^{h_3} + d(h_3) - d(h_2h_3),$$

which asserts that $nf$ is an inner derivation.

Now this says that $n\overline{f} = 0$ in $\mathrm{Ext}(H,A,\phi)$.

Our hypothesis says that $\gcd(m,n) = 1$. By Euclid's algorithm, there exist integers $a$ and $b$ such that $am + bn = 1$. Now, calculating in $\mathrm{Ext}(H,A,\phi)$,

$$\overline{f} = (am+bn)\overline{f} = a(m\overline{f}) + b(n\overline{f}) = 0.$$

Since $f$ was arbitrary, we have $\mathrm{Ext}(H,A,\phi) = \{0\}$.

In fact, a more general result is true. Zassenhaus improved Schur's theorem by showing that it is not necessary to assume that $A$ is abelian, as long as one of $A$ and $H$ is soluble. Now if the orders of $A$ and $H$ are coprime, then at least one of them is odd; and Feit and Thompson showed that any group of odd order is soluble. So we can say that if $\gcd(|A|,|H|) = 1$, then any extension of $A$ by $H$ splits, with no extra conditions on $A$ or $H$. This is known as the *Schur–Zassenhaus Theorem.*

Let us calculate $\mathrm{Ext}(C_2, C_2, \phi)$, where $\phi$ is the trivial homomorphism. Let $f$ be a factor set. Let $H = \{1, h\}$ and $A = \{0, a\}$. We have $f(1,1) = f(1,h) = f(h,1) = 0$, so there are two possible factor sets: we can have $f(h,h) = 0$ or $f(1,1) = a$.

What about inner factor sets? The function $d$ satisfies $d(1) = 0$; so we have

$$\delta d(h,h) = d(h) + d(h) - d(0) = 0,$$

So there is only one possible inner factor set.

Thus, $\mathrm{Ext}(C_2, C_2) = FS(C_2, C_2)/IFS(C_2, C_2) \cong C_2$, and there are just two extensions of $C_2$ by $C_2$. Of course we have known this all along; the only extensions are $C_4$ and $C_2 \times C_2$. Nevertheless, calculating factor sets and inner factor sets can easily be done by computer, so it is quite practical to decide what the possible extensions are.

There is one further problem, which we will not address (and causes a lot of difficulty in the theory). Non-isomorphic extensions correspond to different elements of the Ext group; but sadly, the converse is not true. Different elements of Ext may yield isomorphic groups. For example, $\mathrm{Ext}(C_p, C_p) = C_p$, but there are only two non-isomorphic extensions ($C_{p^2}$ and $C_p \times C_p$), not $p$ of them.

# Exercises

**3.1** Show that the holomorph of $A$ acts on $A$ in such a way that $A$ acts by right multiplication and $\mathrm{Aut}(A)$ acts in the obious way (its elements are automorphisms of $A$, which are after all permutations!). Note that all automorphisms fix the identity element of $A$; in fact, $\mathrm{Aut}(A)$ is the stabiliser of the identity in this action of the holomorph.

**3.2** Let $G$ be a transitive permutation group with a regular normal subgroup $A$. Show that $G$ is isomorphic to a subgroup of the holomorph of $A$.

**3.3** Let $A$, $B$ and $C$ be finite abelian groups. Show that the following are equivalent:

(a) $A$ has a subgroup isomorphic to $B$ with quotient isomorphic to $C$;

(b) $A$ has a subgroup isomorphic to $C$ with quotient isomorphic to $B$.

Show that this equivalence is false for

- infinite abelian groups;
- non-abelian groups.

**3.4** Let $G$ be the group $S_3 \times S_3$. Let $A$ denote the first direct factor. Find two complements to $A$ in $G$, one of which is normal and the other is not. Hence show that this group can be expressed as $S_3 \rtimes_\phi S_3$ with two different homomorphisms $\phi$ from $S_3$ to $\mathrm{Aut}(S_3)$. (Note that $\mathrm{Aut}(S_3)$ is isomorphic to $S_3$.)

**3.5** A group $G$ is called *complete* if it has the properties $Z(G) = \{1\}$ and $\mathrm{Out}(G) = \{1\}$. If $G$ is complete, then

$$\mathrm{Aut}(G) = \mathrm{Inn}(G) \cong G/Z(G) = G,$$

in other words, a complete group is isomorphic to its automorphism group. Prove that, if $G$ is complete, then the holomorph of $G$ is isomorphic to $G \times G$.

**3.6** Find a group $G$ which is not complete but satisfies $\mathrm{Aut}(G) \cong G$.

**3.7** Recall that the *affine group* $\mathrm{AGL}(n, p)$ is the semidirect product of $(C_p)^n$ by its automorphism group $\mathrm{GL}(n, p)$. We regard $(C_p)^n$ as the additive group of the $n$-dimensional vector space over the field $\mathbb{F}_p$.

(a) Show that the affine group $\mathrm{AGL}(n,2)$ is a triply transitive permutation group of degree $2^n$. [Hint: The stabiliser of the zero vector is $\mathrm{GL}(n,2)$; show that this group is doubly transitive on non-zero vectors.]

(b) Show that $\mathrm{AGL}(2,2)$ is isomorphic to the symmetric group $S_4$.

(c) Show that the affine group $\mathrm{AGL}(3,2)$ is contained in the alternating group $A_8$ as a subgroup of index 15.

(d) Show that $A_8$ acts doubly transitively on the 15 elements of $\cos(\mathrm{AGL}(3,2), A_8)$.

**Remark:** In fact, $A_8$ is isomorphic to $\mathrm{GL}(4,2)$, and this action on 15 points is isomorphic to the action on the non-zero vectors of the 4-dimensional vector space.

**3.8** Let $A = H = C_{10}$, where the elements of both $A$ and $H$ are represented as $\{0, 1, 2, \ldots, 9\}$. Let $\phi : H \to \mathrm{Aut}(A)$ be the trivial homomorphism mapping everything to the identity. Let $f : A \times A \to H$ be the usual “carry digit” from elementary arithmetic, that is,

$$f(h_1, h_2) = \begin{cases} 0 & \text{if } h_1 + h_2 \leq 9, \\ 1 & \text{if } h_1 + h_2 \geq 10. \end{cases}$$

(In this formula, addition is usual addition of integers, not addition in $C_{10}$.)

(a) Show that $f$ is a factor set.

(b) Show that $f$ is not an inner factor set.

(c) Show that the extension of $A$ by $H$ constructed using the action $\phi$ and the factor set $f$ is isomorphic to $C_{100}$.

# Chapter 4

# Soluble and nilpotent groups

## 4.1 Soluble groups

There are several ways to recognise when a finite group is soluble. Recall that the *derived group* or *commutator subgroup* $G'$ of $G$ is the subgroup generated by all *commutators* $[g,h] = g^{-1}h^{-1}gh$ for $g,h \in G$. It is a normal subgroup of $G$ with the properties that $G/G'$ is abelian, and if $N$ is any normal subgroup of $G$ such that $G/N$ is abelian, then $G' \leq N$. Inductively we define $G^{(r)}$ for $r \in \mathbb{N}$ by $G^{(0)} = G$ and $G^{(r+1)} = (G^{(r)})'$ for $r \geq 0$.

Note that, if $G^{(i)} = G^{(i+1)}$, then $G^{(i)} = G^{(j)}$ for all $j > i$.

**Theorem 4.1.1** *For the finite group G, the following properties are equivalent:*

*(a) There is a chain of subgroups*

$$G = G_0 \geq G_1 \geq G_2 \geq \cdots \geq G_{r-1} \geq G_r = \{1\}$$

*such that $G_i \lhd G_{i-1}$ and $G_{i-1}/G_i$ is cyclic of prime order for $i = 1,2,\ldots,r$ (in other words, all the composition factors of G are cyclic of prime order);*

*(b) There is a chain of subgroups*

$$G = H_0 \geq H_1 \geq H_2 \geq \cdots \geq H_{s-1} \geq H_s = \{1\}$$

*such that $H_i \lhd G$ and $H_{i-1}/H_i$ is abelian for $i = 1,2,\ldots,s$;*

*(c) there exists r such that $G^{(r)} = \{1\}$.*

**Proof** (c) implies (b): If $G^{(r)} = \{1\}$, then the subgroups $H_i = G^{(i)}$ satisfy the conditions of (b).

(b) implies (a): Suppose that we have a chain of subgroups as in (b). Now if $A$ is a finite abelian group, then $A$ has a composition series with cyclic composition factors of prime order. (The proof is by induction. Working from the bottom up, let $H_s = \{1\}$ and $H_{s-1}$ the subgroup generated by an element of prime order; using the inductive property, choose a composition series for $A/H_{s-1}$, and use the Correspondence Theorem to lift them to a composition series of $A$ containing $H_{s-1}$.)

Now choose a composition series in each abelian quotient, and lift each to a part of a composition series between $G_{i-1}$ and $G_i$.

(a) implies (c): We use the fact that, if $G/N$ is abelian, then $G' \leq N$. If a composition series with prime cyclic factor groups exists as in (a), then by an easy induction, the $i$th term $G^{(i)}$ in the derived series is contained in $G_i$; so $G^{(r)} = \{1\}$.

The *derived length* or *soluble length* of the soluble group $G$ is the minimum $r$ such that $G^{(r)} = \{1\}$. Note that a non-trivial finite group is abelian if and only if it is soluble with derived length 1.

**Theorem 4.1.2** *(a) Subgroups, quotient groups, and direct products of soluble groups are soluble.*

*(b) If $G$ has a normal subgroup $N$ such that $N$ and $G/N$ are soluble, then $G$ is soluble.*

**Proof** (a) If $H \leq G$ then all commutators of elements of $H$ belong to $G'$, and so $H' \leq G'$. By induction, $H^{(i)} \leq G^{(i)}$ for all $i$. So, if $G^{(r)} = \{1\}$, then $H^{(r)} = \{1\}$.

If $N \leq G$, then $[Ng, Nh] = N[g,h]$, so $(G/N)' = G'N/N$. By induction, $(G/N)^{(i)} = G^{(i)}N/N$ for all $i$. So, if $G^{(r)} = \{1\}$, then $(G/N)^{(r)} = \{1\}$.

In $G \times H$, we have $[(g_1,h_1),(g_2,h_2)] = ([g_1,g_2],[h_1,h_2])$ for all $g_1,g_2 \in G$ and $h_1,h_2 \in H$. So $(G \times H)' = G' \times H'$. By induction, $(G \times H)^{(i)} = G^{(i)} \times H^{(i)}$ for all $i$. So, if $G^{(r)} = \{1\}$ and $H^{(s)} = \{1\}$, then $(G \times H)^{(t)} = \{1\}$, where $t = \max\{r,s\}$.

Suppose that $N^{(r)} = \{1\}$ and $(G/N)^{(s)} = \{1\}$. Arguing as in (a), we see that $G^{(s)} \leq N$, and so $G^{(r+s)} = \{1\}$.

**Remark** The arguments in the proof show that the derived length of a subgroup or quotient of $G$ are not greater than the derived length of $G$, while the derived length of a direct product is the maximum of the derived length of the factors.

## 4.2 Nilpotent groups

Recall that the *centre* of $G$ is the subgroup $Z(G) = \{g \in G : gx = xg \text{ for all } x \in G\}$. It is an abelian normal subgroup of $G$. Now we define a series of subgroups of $G$

called the *upper central series* of $G$ as follows: $Z_0(G) = \{1\}$, $Z_{i+1}(G)$ is the normal subgroup of $G$ corresponding to the centre of $G/Z_i(G)$ by the Correspondence Theorem. (Briefly we say $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$.)

Note that, if $Z_i(G) = Z_{i+1}(G)$ (that is, if the centre of $G/Z_i(G)$ is trivial), then $Z_i(G) = Z_j(G)$ for all $j > i$.

The group $G$ is said to be *nilpotent* if $Z_r(G) = G$ for some $r$; the smallest such $r$ is called the *nilpotency class* of $G$. Again, a non-trivial finite group is abelian if and only if it is nilpotent with nilpotency class 1.

**Theorem 4.2.1** *The following conditions for a finite group $G$ are equivalent:*

*(a)* $Z_r(G) = G$ *for some* $r$*;*

*(b) there is a chain of subgroups*

$$G = H_0 \geq H_1 \geq H_2 \geq \cdots \geq H_{s-1} \geq H_s = \{1\}$$

*such that* $H_i \lhd G$ *and* $H_{i-1}/H_i \leq Z(G/H_i)$ *for* $i = 1, 2, \ldots, s$*;*

*(c) all Sylow subgroups of $G$ are normal;*

*(d) $G$ is the direct product of its Sylow subgroups.*

Thus nilpotency of a finite group can be defined by any of the equivalent conditions of the Theorem. (As for solubility, the conditions are no longer equivalent for infinite groups.) Note that

(a) a nilpotent group is soluble (for the centre of a group is abelian, so the quotients of the groups in the chain (b) are abelian);

(b) a group of prime power order is nilpotent;

(c) the smallest non-abelian group, $S_3$, is soluble but not nilpotent.

**Proof** (a) implies (b): If $Z_r(G) = G$, then the subgroups $H_i = Z_{r-i}(G)$ satisfy the conditions of (b).

(b) implies (c): We defer this for a moment.

(c) implies (d): This is proved by a straightforward induction on the number of primes dividing $|G|$.

(d) implies (a): Recall that, if $P$ is a non-trivial group of prime-power order, then $Z(P) \neq \{1\}$. Thus, by induction, a group of prime-power order satisfies (a). Moreover, it is easy to see that

$$Z(P_1 \times \cdots \times P_m) = Z(P_1) \times \cdots \times Z(P_m);$$

so a direct product of groups satisfying (a) also satisfies (a).

The remaining implication is a little more difficult; it follows from a couple of lemmas which we now prove.

**Lemma 4.2.2** *Let $P$ be a Sylow $p$-subgroup of the group $G$, and $H$ a subgroup of $G$ which contains the normaliser $N_G(P)$ of $P$. Then $N_G(H) = H$.*

**Proof** Take $g \in N_G(H)$, so that $g^{-1}Hg = H$. Then $g^{-1}Pg \leq H$, so $g^{-1}Pg$ is a Sylow $p$-subgroup of $H$. By Sylow's theorem, all the Sylow $p$-subgroups of $H$ are conjugate, so there exists $h \in H$ satisfying $h^{-1}(g^{-1}Pg)h = P$. Then $gh \in N_G(P) \leq H$, so $gh \in H$. Since $h \in H$, it follows that $g \in H$. So $N_G(H) = H$, as claimed.

**Remark** This argument is known as the *Frattini argument*.

**Lemma 4.2.3** *Suppose that $G$ satisfies (b) of the Theorem. If $H$ is a proper subgroup of $G$, then $H < N_G(H)$.*

**Proof** Let $i$ be maximal such that $G_i \leq H$. Then $i \neq 0$, since $H < G$. Now $G_{i-1} \not\leq H$, so there is a coset $G_i g$ in $G_{i-1}/G_i$ which is not in $H/G_i$ but commutes with all cosets of $G_i$, and hence normalises $H/G_i$. Thus, $N_{G/G_i}(H/G_i) > H/G_i$. Judicious use of the Correspondence Theorem shows that $N_G(H) > H$.

Now we can show that (b) implies (c) in the theorem. Suppose that $G$ satisfies (b), and let $P$ be a Sylow $p$-subgroup of $G$, for some prime $p$. Let $H = N_G(P)$. Then $N_G(H) = H$. But if $H < G$, then $N_G(H) > H$; so we must have $H = G$ as required.

**Remark** The condition

If $H < G$, then $H < N_G(H)$

is equivalent to the four conditions of the theorem, and so provides another equivalent to nilpotency of a finite group. [Can you prove this?]

## 4.3 Supersoluble groups

A finite group $G$ is *supersoluble* if there is a chain

$$G = G_0 > G_1 > G_2 > \cdots > G_{r-1} > G_r = \{1\}$$

of subgroups such that $G_i \triangleright G$ and $G_{i-1}/G_i$ is cyclic of prime order for $i = 1, 2, \ldots, r$.

Look back at the first theorem of this chapter. In a soluble group $G$, we may assume *either* that all the subgroups in the chain are normal in $G$ (with the quotients being abelian), *or* that all the quotients are cyclic of prime order (with each subgroup being normal in the one before). The example $G = A_4$ shows that we cannot ask both things in general. The only candidate for $G_1$ is $V_4$, which is not cyclic; its cyclic subgroups of order 2 are not normal in $G$. In other words, $A_4$ is not supersoluble. However, $S_3$ is supersoluble.

Supersoluble groups form a class between nilpotent and soluble. (Any nilpotent group is supersoluble, because a subgroup contained in the centre of a group $G$ is normal.) They are not as important as either nilpotent or soluble groups. Here is a surprising fact about them.

**Theorem 4.3.1** *If $G$ is supersoluble, then $G'$ is nilpotent.*

**Proof** This depends on the fact that the automorphism group of a cyclic group of prime order is abelian. (In fact, $\mathrm{Aut}(C_p) = C_{p-1}$.) Hence, a homomorphism from $G$ to $\mathrm{Aut}(C_p)$ has the property that its kernel contains $G'$.

Let

$$G = G_0 > G_1 > G_2 > \cdots > G_{r-1} > G_r = \{1\}$$

be a series of subgroups such that $G_i \lhd G$ and $G_{i-1}/G_i$ is cyclic of prime order for $i = 1, 2, \ldots, r$. Now consider the series

$$G' = H_0 \geq H_1 \geq H_2 \geq \cdots \geq H_{r-1} \geq H_r = \{1\},$$

where $H_i = G_i \cap G'$. Then $H_i \lhd G'$, and

$$H_{i-1}/H_i = (G_{i-1} \cap G')/(G_i \cap (G_{i-1} \cap G')) \cong (G_{i-1} \cap G')G_i/G_i \leq G_{i-1}/G_i,$$

so $H_{i-1}/H_i$ is either trivial or cyclic of prime order. By dropping terms from the series, we can assume it is always cyclic of prime order.

Now $G$ acts by conjugation on $H_{i-1}/H_i$. By our earlier remark, $G'$ acts trivially on this quotient, which means that $H_{i-1}/H_i \leq Z(G'/H_i)$. Since this is true for all $i$, we see that $G'$ is nilpotent.

# Exercises

**4.1** What is the smallest group which is supersoluble but not nilpotent? What is the smallest group that is soluble but not supersoluble?

**4.2** Calculate the sequence of derived subgroups of the group $S_4$ and of the group $\mathrm{GL}(2,3)$.

**4.3** Closure properties.

(a) Prove that subgroups, quotients, and direct products of nilpotent groups are nilpotent.

(b) Prove that subgroups, quotients, and direct products of soluble groups are soluble.

(c) Prove that an extension of a soluble group by a soluble group (that is, a group with a soluble normal subgroup having soluble factor group) is soluble. Does this hold with “nilpotent” replacing “soluble”?

(d) Do the above properties hold for supersoluble groups?

**4.4** Let $n$ be a positive integer greater than 2, and let $G = D_{2n}$ be the dihedral group of order $2n$.

(a) Prove that $G$ is not abelian.

(b) Prove that $G$ is soluble and calculate the series of derived subgroups of $G$.

(c) Prove that $G$ is nilpotent if and only if $n$ is a power of 2.

(d) Is $G$ supersoluble?

**4.5** Show that any group of order smaller than 60 is soluble.

**4.6** The *lower central series* of a group $G$ is the series of subgroups defined by the rule that $\gamma^1(G) = G$ and $\gamma^{i+1}(G) = [\gamma^i(G), G]$, where $[H,K]$ denotes the subgroup generated by all commutators $[h,k] = h^{-1}k^{-1}hk$ for $h \in H$ and $k \in K$.

(a) Prove that each term in the lower central series is a normal subgroup of $G$.

(b) Prove that $\gamma^i(G)/\gamma^{i+1}(G) \leq Z(G/\gamma^{i+1}(G))$.

(c) Prove that $G$ is nilpotent if and only if $\gamma^i(G) = 1$ for some $i$, and in this case the length of the lower central series is equal to the nilpotency class of $G$.

(d) What, if any, is the relationship between the terms in the upper and lower central series?

# Chapter 5

# Solutions to some of the exercises

**1.5** (a) By the Subgroup Test, we have to show that $H \cap K$ is non-empty (which it is, as it contains the identity), and that if $x, y \in H \cap K$, then $xy^{-1} \in H \cap K$. This holds because $x, y \in H$, so $xy^{-1} \in H$ (as $H$ is a subgroup), and similarly $xy^{-1} \in K$.

(b) We claim that, if $x \in HK$, then $x$ can be written as $hk$ (with $h \in H$ and $k \in K$) in exactly $|H \cap K|$ ways. Given one such expression $x = hk$, we have $x = (hg^{-1})(gk)$ for all $g \in H \cap K$, giving $|H \cap K|$ expressions, Conversely, if $x = h'k'$ is any such expression, then $hk = h'k'$, so $(h')^{-1}h = k'k_{-1} = g$, say, so $h' = hg^{-1}$ and $k' = gk$. So we have found all such expressions.

Hence $|HK| = |H| \cdot |K| / |H \cap K|$, since by counting the pairs $(h, k)$ we overcount by a factor of $|H \cap K|$.

(c) Clearly $HK$ is non-empty. If $h_1k_1, h_2k_2 \in HK$, then

$$\begin{array}{rcll} (h_1k_1)(h_2k_2)^{-1} & = & h_1kh_2^{-1} & \text{where } k = k_1k_2^{-1} \\ & = & h_1h_3k & \text{where } h_3 = kh_2^{-1}k^{-1} \in kHk^{-1} = K \\ & \in & HK, & \end{array}$$

so $HK$ is a subgroup.

(d) Let $G = S_3$, and let $H$ and $K$ be the subgroups of order 2 generated by $(1,2)$ and $(1,3)$ respectively. Then $|HK| = 4$, and so $HK$ cannot be a subgroup of a group of order 6, by Lagrange's Theorem.

**1.15** We have

$$\begin{array}{rcl} (q_1 + q_2)\theta & = & \mathrm{e}^{2\pi \mathrm{i}(q_1+q_2)} \\ & = & \mathrm{e}^{2\pi \mathrm{i} q_1} \cdot \mathrm{e}^{2\pi \mathrm{i} q_2} \\ & = & q_1\theta \cdot q_2\theta, \end{array}$$

so $\theta$ is a homomorphism.

Since every root of unity has the form $\mathrm{e}^{2\pi \mathrm{i}q}$ for some rational number $q$, $\theta$ is onto. Its kernel is

$$\{q \in \mathbb{Q} : \mathrm{e}^{2\pi \mathrm{i}q} = 1\} = \mathbb{Z}.$$

So $\mathbb{Q}/\mathbb{Z} \cong A$, by the First Isomorphism Theorem.

Every element of $A$ has finite order (the order of $\mathrm{e}^{2\pi \mathrm{i}q}$ is the denominator of $q$), while every non-zero element of the infinite cyclic group has infinite order. So they are not isomorphic.

**1.17** (a) Split the $n$ points up into $a_1$ sets of size $p^i$ for $i = 0, \dots, r$, and let $G$ be the group fixing each of these sets. It is easily seen that $G$ is the direct product of symmetric groups of the appropriate sizes.

Some slightly tedious number theory (which we will need later) shows that the power of $p$ dividing $n!$ is the same as the power of $p$ dividing $|G|$.

(b) The power of $p$ dividing $p^i!$ is as claimed: if we write out the factorial as a product, there are $p^{i-1}$ terms which are multiples of $p$, of which $p^{i-2}$ are multiples of $p^2$, and so on.

Given a set of size $p^i$, choose partitions $\pi_1, \pi_2, \dots, \pi_{i-1}$ where $pi_j$ has $p^j$ parts of size $p^{i-j}$, and each partition refines the one before. Now consider permutations which fix all these partitions, and permute the parts of $\pi_{j+1}$ in each part of $\pi_j$ cyclically. This has the required order.

(c) Take the direct product of Sylow $p$-subgroups of $S_{p^i}$ for each $i$ to get a Sylow $p$-subgroup of $G$. By our remark in the first part, this is also a Sylow $p$-subgroup of $S_n$.

(d) Given any finite group $H$ of order $n$, by Cayley's Theorem we can embed $H$ into the symmetric group $S_n$, which has a Sylow $p$-subgroup. By Sylow's Lemma, $H$ has a Sylow $p$-subgroup.

**1.19** (a) We are looking for Sylow $p$-subgroups for $p = 5, 3, 2$; they should have orders $5, 3, 8$ respectively. It is enough to give an example of each.

$p = 5$: the cyclic group generated by a 5-cycle;

$p = 3$: the cyclic group generated by a 3-cycle;

$p = 2$: the dihedral group of symmetries of a square, fixing the remaining point.

There are 24 elements of order 5, hence $24/4 = 6$ Sylow 5-subgroups; 20 elements of ordedr 3, hence $20/2 = 10$ Sylow 3-subgroups. To count the Sylow 2-subgroups we note that, by the conjugacy part of Sylow's theorem, they are all symmetry groups of squares, so we have to count the number of ways of labelling a square and an isolated point. There are 5 choices for the isolated point, and 3 ways of labelling the square; so 15 Sylow 2-subgroups.

(b) The conjugacy classes in $S_5$ have sizes 1 (the identity), 10 (the transpositions), 15 (products of two transpositions), 20 (the 3-cycles), 20 (the products of a 2-cycle and a 3-cycle), 30 (the 4-cycles), and 24 (the 5-cycles). How can we choose some of these, including the identity, to have size dividing 120? There are trivial solutions corresponding to the identity and the whole group; what others are there? A little thought shows that the numerical solutions are $1+24+15$ or $1+24+15+20$. A subgroup containing elements which are the product of a 2-cycle and a 3-cycle would also contain their squares, which are 3-cycles; so the 20 must be the class of 3-cycles. Now it is easy to see that we can write a 3-cycle as the product of two double transpositions; so if we include 15 we must also include 20. So the only possibility is to use all the even permutations, obtaining $A_5$.

Thus the only normal subgroups are $\{1\}, A_5$ and $S_5$.

**1.20** (a) The number of Sylow 5-subgroups of a group of order 40 is congruent to 1 (mod 5) and divides 8, so is 1; thus a Sylow 5-subgroup is normal.

(b) The number of Sylow 7-subgroups of a group of order 84 is congruent to 1 (mod 7) and divides 12, so is 1; thus a Sylow 7-subgroup is normal.

**1.21** (a) Let $G = C_n$, with generator $a$, and let $H$ be a subgroup of $G$. Let $k$ be the smallest positive integer for which $a^k \in H$. (There certainly are some positive integers with this property, e.g. $k = n$.) Now we claim that, if $a^m \in H$, then $k$ divides $m$. For if not, then let $m = kq + r$, with $0 < r < k$; then $a^r = a^m \cdot (a^k)^{-q} \in H$, contradicting the definition of $k$. So $a^k$ generates $H$, which is thus cyclic.

(b) Let $G$ be the dihedral group of order $2n$, the group of symmetries of a regular $n$-gon. Then $G$ contains a cyclic group $C$ of order $n$ consisting of rotations; all the elements outside $C$ are reflections. Let $H$ be any subgroup of $G$. If $H \leq C$, then $H$ is cyclic, by (a); so suppose not. Then $H \cap C$ is a cyclic group of order $m$, say, and $|H| = 2m$. An element of $H$ outside $C$ is a reflection (so has order 2) and conjugates a generator of $H \cap C$ to its inverse (since it conjugates every element of $C$ to its inverse). Thus $H$ is a dihedral group.

(c) Further to (b), we see that $G$ contains a unique cyclic subgroup of order $m$ consisting of rotations, for every $m$ dividing $n$. Also, if $K$ is such a subgroup, and $t$ any reflection, then $\langle K, t \rangle$ is a dihedral group. If $|K| = m$, then the dihedral group $\langle K, t \rangle$ contains $m$ reflections. Since there are $n$ involutions, there must be $n/m$ dihedral subgroups of order $2m$.

If $n$ is odd, then all these dihedral groups are conjugate, so they are not normal (unless $m = n$, in which case we have the whole group). If $n$ is even, the reflections fall into two conjugacy classes. Now if $n/m$ is even, then the dihedral group of order $2m$ contains reflections from only one class, so there are two conjugacy classes of dihedral groups, while if $n/m$ is odd, then all the dihedral groups contain reflections from both classes and so all is conjugate.

So the normal subgroups are: all the cyclic rotation groups $C_m$; and the dihedral groups $D_{2m}$ for $m = 1$ and (if $n$ is even) $m = 2$.

(d) In $D_{12}$, we see that there are three normal subgroups of index 2, namely $C_6$ and two $D_6$s. Moreover, $C_6$ has two composition series $C_6 \rhd C_2 \rhd \{1\}$ and $C_6 \rhd C_3 \rhd \{1\}$, while $D_6$ has only one, namely $D_6 \rhd C_3 \rhd \{1\}$. So there are four composition series for $D_{12}$.

**1.23** The normal subgroups of $S_4$ are $A_4$, $V_4$ (the Klein group) and $\{1\}$. So any composition series must begin $S_4 \rhd A_4$. Now the normal subgroups of $A_4$ are $V_4$ and $\{1\}$, so the series must continue $A_4 \rhd V_4$. Finally, $V_4$ has three cyclic subgroups of order 2, all normal, so there are three ways to continue the series as $V_4 \rhd C_2 \rhd \{1\}$.

**1.24** (a) Let $G$ be an elementary abelian $p$-group. If its order were divisible by a prime $q \neq p$, then by Cauchy's Theorem it would contain an element of order $q$, which it does not. So $|G|$ is a power of $p$.

(b) There are two ways to argue. First, use the structure theorem for finite abelian groups to express $G$ as a direct product of cyclic groups. Since all non-identity elements have order $p$, these cyclic groups must all be $C_p$.

The second method avoids using this theorem. Write the abelian group $G$ additively, and define $ng = g + g + \cdots + g$ ($n$ times) for $0 \leq n \leq p-1$. Since $pg = 0$, it is easy to show that this scalar multiplication makes $G$ into a vector space over the field $\mathrm{GF}(p)$ of integers mod $p$. Choose a basis for this vector space. Translating back to group theory language, the elements of this basis are generators of cyclic groups whose direct product is $G$.

**2.8** (a) If $n = 2$, then $\Omega$ contains only the single element $\{1,2\}$, and obviously every element of $S_2$ fixes it; so the action is not faithful. (If $g = (1,2)$, then $\{1,2\}g = \{1g, 2g\} = \{2,1\} = \{1,2\}$.)

(b) If $n = 3$, the map

$$\{1,2\} \mapsto 3, \qquad \{2,3\} \mapsto 1, \qquad \{1,3\} \mapsto 2$$

is an isomorphism from the action on $\Omega$ to the usual action on $\{1,2,3\}$, which is obviously doubly transitive.

(c) If $n = 4$, then the relation $\{i,j\} \sim \{k,l\}$ if the sets $\{i,j\}$ and $\{k,l\}$ are equal or disjoint, is a congruence: it is obviously invariant under $S_4$, and the fact that it is an equivalence relation is most easily seen by observing that the three equivalence classes form a partition of $\Omega$. So $S_4$ is imprimitive.

(d) Assume that $n \geq 5$. To show that the action of $S_n$ on $\Omega$ is primitive, suppose that $\equiv$ is a congruence, which is not the relation of equality, so two unequal pairs are congruent. There are two cases:

- Two pairs with an element in common, say $\{a,b\}$ and $\{a,c\}$, are congruent. Since $S_n$ acts transitively on configurations like this, it follows that every two pairs with an element in common are congruent. Then for example, $\{1,2\}$ is congruent to $\{1,3\}$ and to $\{2,4\}$; so two disjoint pairs are also congruent. Now reason as in the next case.
- Two disjoint pairs are congruent, say $\{a,b\}$ and $\{c,d\}$. Again $S_n$ is transitive on such configurations, so every two disjoint pairs are congruent. Now $\{1,2\}$ is congruent to $\{3,4\}$ and to $\{3,5\}$ [here we use the fact that $n \geq 5$], so two pairs with an element in common are congruent. Now reason as in the preceding case.

The conclusion is that any two pairs are congruent, so the congruence is the universal relation. Thus the group is primitive.

To show it is not doubly transitive, observe that a permutation cannot map two intersecting pairs like $\{1,2\}$ and $\{1,3\}$ to two disjoint pairs like $\{1,2\}$ and $\{3,4\}$.

**2.10** (a) Any automorphism of a group $G$ must permute the elements of $G$ and fix the identity, so must permute the non-identity elements. If $G = V_4$, there are three non-identity elements, so $\mathrm{Aut}(G) \leq S_3$. Why is it equal to $S_3$? One way to see this is to observe that, if $V_4 = \{1,a,b,c\}$, then we can specify the multiplication as follows:

- $1x = x1 = x$ and $x^2 = 1$ for all $x \in G$;
- the product of any two distinct non-identity elements is the third.

Stated in this way, it is clear that any permutation of the non-identity elements is an automorphism of the group.

(b) Let $G = S_3$. Since $Z(G) = \{1\}$, we have

$$G \cong \mathrm{Inn}(G) \leq \mathrm{Aut}(G),$$

and we are done if we can show that $G$ has at most six automorphisms. But $G$ has two elements of order 3 and three of order 2; any choice of an element $a$ of order 3 and $b$ of order 2 generates the group, so an automorphism is uniquely determined by what it does to $a$ and $b$. And $a$ must go to an element of order 3, and $b$ to an element of order 2, so there are at most $2 \cdot 3 = 6$ choices.

(c) For $n > 2$ and $n \neq 6$, the symmetric group has trivial centre and no outer automorphisms; so

$$\mathrm{Aut}(S_n) \cong \mathrm{Inn}(S_n) \cong S_n/Z(S_n) \cong S_n.$$

Many other examples are possible, for example dihedral groups of order greater than 4.

(d) Suppose that $G$ is elementary abelian of order 8. Then $G$ is isomorphic to the additive group of a 3-dimensional vector space over the field $\mathbb{Z}_2$ with two elements. Any map taking a basis to a basis extends uniquely to an automorphism. So the order of the automorphism group is equal to the number of bases. Now there are

- 7 choices for the first basis vector $u$ (any non-zero vector);
- 6 choices for the second basis vector $v$ (any vector which is not a multiple of $u$, thus 0 and $u$ are excluded);
- 4 choices for the third basis vector (any vector which is not a linear combination of $u$ and $v$, thus 0, $u$, $v$ and $u+v$ are excluded).

Now it is a simple exercise to label the Fano plane with the seven non-zero vectors of the 3-dimensional vector space in such a way that three points form a line if and only if the corresponding vectors sum to 0. So any automorphism of the group will be an automorphism of the Fano plane. Since the two automorphism groups have the same order 168, they are equal.

**2.11** If $G$ is non-abelian, suppose that $gh \neq hg$. Then conjugation by $g$ (the map $x \mapsto g^{-1}xg$) is an (inner) automorphism of $G$, and is not the identity, since it doesn't fix $h$.

If $G$ is abelian, then the map $\mapsto x^{-1}$ is an automorphism, since $(xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1}$. If some element of $G$ is not equal to its inverse, then this automorphism is non-trivial. [Note that the map $x \mapsto x^{-1}$ is an automorphism of $G$ if and only if $G$ is abelian.]

Finally, if every element of $G$ is equal to its inverse, then $G$ is an elementary abelian 2-group, and so is isomorphic to the additive group of a $k$-dimensional vector space over $\mathbb{Z}_2$ (where $|G| = 2^k$). Since $|G| > 2$ we have $k > 1$. Now choose a basis for $G$; the map which switches the first two basis vectors and fixes the rest is a non-trivial automorphism.

All of this works exactly the same for infinite groups except for the innocent-looking phrase “choose a basis”. The proof that every (infinite-dimensional) vector space has a basis requires the Axiom of Choice.

**2.12** (a) We construct $\mathbb{F}_8$ by adjoining to $\mathbb{F}_2 = \mathbb{Z}_2$ the root of an irreducible cubic polynomial $f(x)$.

> The reason for this is that, if $f$ is irreducible, then the ideal $\langle f \rangle$ of the polynomial ring $\mathbb{F}_2[x]$ generated by $f$ is maximal, and hence the quotient ring $\mathbb{F}_2[x]/\langle f \rangle$ is a field (see Algebraic Structures II notes). Now the Division algorithm shows that, if $p$ is any polynomial over $\mathbb{F}_2$, then we can write $p(x) = f(x)q(x) + r(x)$, where $\deg(r) < \deg(f) = 3$, so $r$ belongs to the coset $\langle f \rangle + p$. Thus every coset contains a representative of degree less than 3. It is easy to see that this coset representative is unique. The number of polynomials of degree less than 3 is $2^3 = 8$ (since $ax^2 + bx + c$ has three coefficients each of which can be any element of $\mathbb{F}_2$). So there are 8 cosets of $\langle f \rangle$ in $\mathbb{F}_2[x]$, and the quotient is a field with 8 elements.
>
> We note in passing that, if we use the symbols $0, 1, \alpha$ to denote the cosets $\langle f \rangle$, $\langle f \rangle + 1$ and $\langle f \rangle + x$ respectively, then $f(\alpha) = \langle f \rangle + f(x) = \langle f \rangle = 0$. Thus $\alpha$ is a root of $f$.

There are eight polynomials of degree 3 over $\mathbb{F}_2$. If $f$ is an irreducible polynomial of degree 3, then $f(0) = 1$ (since if $f(0) = 0$ then $x$ is a factor of $f(x)$), and $f(1) = 1$ (since if $f(1) = 0$ then $x + 1$ is a factor of $f(x)$). This leaves just the two irreducible polynomials $f(x) = x^3 + x + 1$ and $g(x) = x^3 + x^2 + 1$.

Now take the polynomial $f$. The eight elements of our field are $a\alpha^2 + b\alpha + c$, where $a, b, c \in \mathbb{F}_2$ and $\alpha^3 + \alpha + 1 = 0$. Addition is straightforward: to add two expressions of this form, we simply add the coefficients of $\alpha^2$, the coefficients of $\alpha$, and the constant terms. For example, $(\alpha^2 + 1) + (\alpha^2 + \alpha) = \alpha + 1$.

Multiplication can be done by multiplying in the usual way and using the fact that $\alpha^3 = \alpha + 1$ to reduce the degree of the product. A more user-friendly way to multiply is to use “logarithms”. We construct a table of powers of $\alpha$:

| | | | | | |
|---|---|---|---|---|---|
| $\alpha^0$ | | | | | $1$ |
| $\alpha^1$ | | | $\alpha$ | | |
| $\alpha^2$ | $\alpha^2$ | | | | |
| $\alpha^3$ | | | $\alpha$ | $+$ | $1$ |
| $\alpha^4$ | $\alpha^2$ | $+$ | $\alpha$ | | |
| $\alpha^5$ | $\alpha^2$ | $+$ | $\alpha$ | $+$ | $1$ |
| $\alpha^6$ | $\alpha^2$ | | | $+$ | $1$ |

and $\alpha^7 = 1 = \alpha^0$. So the multiplicative group is cyclic of order 7, in agreement with what we know.

Now to multiply two elements, use the table to express them as powers of $\alpha$, add the exponents mod 7, and use the table in reverse to express the result in the standard form. For example,

$$(\alpha^2+1)(\alpha^2+\alpha)=\alpha^6\cdot\alpha^4=\alpha^{10}=\alpha^3=\alpha+1.$$

(b) Let $\beta=\alpha^3$. (Why this choice? Trial and error – see below.) Then

$$\beta^3+\beta^2+1=\alpha^9+\alpha^6+1=\alpha^2+(\alpha^2+1)+1=0,$$

so $\beta$ is a root of the other irreducible polynomial $g$. So the field we construct already contains a root of $g$, and thus is the field obtained by adjoining such a root to $\mathbb{F}_2$. So the two irreducible polynomials give the same field.

If you try $\gamma=\alpha^2$, you will find that $f(\gamma)=0$, so $\gamma$ is a root of the same irreducible polynomial as is $\alpha$. In fact, this agrees with our observation that the *Frobenius map* $u\mapsto u^2$ is an automorphism of $\mathbb{F}_8$. Similarly, $\alpha^4$, the result of applying the Frobenius map twice, will also satisfy $f$. The other two elements $\alpha^6=(\alpha^3)^2$ and $\alpha^5=(\alpha^3)^4$ are roots of $g$.

**2.13** (a) The following are equivalent (for $g\in G$):

- $Hg$ is fixed by $H$,
- $(Hg)h=Hg$ for all $h\in H$,
- $Hghg^{-1}=H$ for all $h\in H$,
- $ghg^{-1}\in H$ for all $h\in H$,
- $gHg^{-1}=H$,
- $g^{-1}Hg=H$.

(b) Let $H=p^k$. Then the coset space $\cos(H,G)$ has size $p^{n-k}$, a multiple of $p$ (since $H<G$). Now consider the action restricted to $H$, and split $\cos(H,G)$ into orbits. By the Orbit-Stabiliser Theorem, the size of each orbit is a power of $p$; and at least one orbit (namely $\{H\}$) has size $1=p^0$. So there must be at least $p$ orbits of size 1; that is, at least $p$ cosets of $H$ lie in $N_G(H)$, by (a). So $N_G(H)>H$.

**2.14** (a) $\mathrm{PSL}(2,F)$ contains an involution; indeed, it is easy to see that it contains more than one involution. (For example, thinking of it as the group of linear fractional transformations, $z\mapsto -a^2/z$ is an involution for any non-zero $a\in F$, so if $|F|>3$ there is more than one such element. The case $|F|=3$ can be handled directly.) So it cannot be a subgroup of a group with only one involution. [An *involution* is an element of order 2.]

(b) Since the composition factors are $C_2$ and $\mathrm{PSL}(2,q)$, and there is no subgroup (normal or otherwise) isomorphic to $\mathrm{PSL}(2,q)$, the composition series must be $G \rhd H \rhd \{1\}$, where $H \cong C_2$. By the first part of the question, there is only one such subgroup $H$, namely $\{\pm I\}$.

(c) Immediate from (a) (or (b)).

**2.15** (a) We can map 0 to $b$ by the map $x \mapsto x+b$ (that is, $x \mapsto (1x+b)/(0x+1)$), and 0 to $\infty$ by $x \mapsto 1/x$. So the orbit containing 0 is the whole of $F \cup \{\infty\}$.

(b) The map $x \mapsto (ax+b)/(cx+d)$ maps $\infty$ to $a/c$. If this is to be $\infty$, we must have $c = 0$, so that $x \mapsto (ax+b)/d = (a/d)x + (b/d)$. Nothing is affected if we take $d = 1$, giving the form stated.

This group is transitive on $F$ (we saw this implicitly in (a)), so the result follows from:

**Fact** *Suppose that $G$ is transitive on $\Omega$, and the stabiliser of a point $\omega \in \Omega$ is transitive on $\Omega \setminus \{\omega\}$. Then $G$ is doubly transitive on $\Omega$.*

**Proof** Suppose that we want to map $(\alpha,\beta)$ to $(\gamma,\delta)$, where $\alpha \neq \beta$ and $\gamma \neq \delta$. Choose $g \in G$ mapping $\alpha$ to $\omega$, and $g' \in G$ mapping $\gamma$ to $\omega$. Then $\beta g$ and $\delta g'$ are both different from $\Omega$; so choose $h \in \mathrm{Stab}(\omega)$ mapping $\beta g$ to $\delta g'$. Then check that $gh(g')^{-1}$ is the element we are looking for.

(c) If $x \mapsto ax+b$ fixes 0, then $b = 0$, so the stabiliser of $\infty$ and 0 is the group $x \mapsto ax$ for $a \in F^{\times}$. Clearly it is transitive on $F \setminus \{0\}$: we can map 1 to $a$ by multiplying by $a$.

Now a result similar to the Fact above shows that, if $G$ is doubly transitive and the stabiliser of two points is transitive on the remaining points then $G$ is triply transitive.

Since $G$ is triply transitive, all three-point stabilisers are conjugate; and the stabiliser of $\infty$, 0 and 1 is the identity. (The map $x \mapsto ax$ maps 1 to 1 if and only if $a = 1$.)

**2.16** Suppose that $G$ is a simple group of order $pqr$, where $p > q > r$. The number of Sylow $p$-subgroups is congruent to 1 mod $p$ and divides $qr$; it cannot be 1 (since $G$ is simple), $q$ or $r$ (since it is at least $p+1$), so must be $qr$.

Now the Sylow $p$-subgroups between them contain the identity and $qr(p-1)$ elements of order $p$ (since any two intersect only in the identity).

Similarly, the number of Sylow $q$-subgroups is congruent to 1 mod $q$ and divides $pr$, so must be either $p$ or $pr$, giving us at least $p(q-1)$ elements of order $q$.

Similarly, there are at least $q(r-1)$ elements of order $r$. So

$$1+qr(p-1)+p(q-1)+q(r-1)\leq pqr,$$

which is obviously false.

**2.17** The proof that $G$ is a group is all straightforward except for the associative law, which requires a lot of case-by-case analysis. Then the proof that it is an elementary abelian 2-group is straightforward.

For the associative law, the cases where one or more of the three terms is 0 are all trivial. The case where the first and second, or second and third, are equal are also trivial. The case where the first and last elements are equal holds since $x+(y+x)=(x+y)+x$ by commutativity. I reckon that the following cases need to be considered:

- $\{a,b\}$, $\{a,c\}$, $\{a,d\}$;
- $\{a,b\}$, $\{a,c\}$, $\{b,c\}$;
- $\{a,b\}$, $\{a,c\}$, $\{b,d\}$;
- $\{a,b\}$, $\{a,c\}$, $\{c,d\}$;
- $\{a,b\}$, $\{a,c\}$, $\{d,e\}$;
- $\{a,b\}$, $\{c,d\}$, $\{a,e\}$;
- $\{a,b\}$, $\{c,d\}$, $\{c,e\}$;
- $\{a,b\}$, $\{c,d\}$, $\{e,f\}$.

Here is a different argument avoiding cases.

Step 1: The set of all subsets of $\{1,\ldots,n\}$, with the operation of symmetric difference, is an elementary abelian 2-group. (Mapping each subset $A$ to the $n$-tuple of 0s and 1s having 1s in the positions of $A$ and 0s elsewhere is a bijection to $(\mathbb{Z}_2)^n$, and it is easy to see that it is a group isomorphism.)

Step 2: The set of subsets of even cardinality is a subgroup $W$, and the set $\{\emptyset,\{1,\ldots,n\}\}$ is a subgroup $U$.

Step 3: If $n$ is even, then $U\leq W$, and so $W/U$ is an elementary abelian 2-group of order $2^{n-2}$.

Step 4: If $n=6$, then every coset of $U$ apart from $U$ itself has the form $\{\{a,b\},\{c,d,e,f\}\}$. Choose $\{a,b\}$ as the coset representative, and check that the group operation takes exactly the form given in the question (where 0 denotes the coset $U$).

An elementary abelian 2-group is the additive group of a vector space over $\mathbb{F}_2$, where scalar multiplication is given by $0v = 0$ and $1v = v$. Any group automorphism is a vector space automorphism. So the automorphism group of $(V, \oplus)$ is $\mathrm{GL}(4,2)$. But clearly $S_6$, acting by permuting the elements of the sets (so that $0g = 0$ and $\{a,b\}g = \{ag,bg\}$) is a group of automorphisms.

The index is $(2^4-1)(2^4-2)(2^4-2^2)(2^4-2^3)/6! = 28$.

**Remark** In fact, $\mathrm{GL}(4,2)$ is isomorphic to the alternating group $A_8$. The embedding of $S_6$ into $A_8$ is given by the following map:

$$g \in S_6 \mapsto \begin{cases} g & \text{if } g \text{ is an even permutation;} \\ g(7,8) & \text{if } g \text{ is an odd permutation.} \end{cases}$$

If you are interested in classical groups, I will mention that $S_6$ is isomorphic to the symplectic group $\mathrm{Sp}(4,2)$, which naturally occurs as a subgroup of $\mathrm{GL}(4,2)$.

**2.18** (a) Immediate from Sylow's Theorem.

(b) $G$ acts on the set of eight Sylow 7-subgroups; the stabiliser of one such subgroup $P$ is its normaliser $N(P)$. Now $P$ is cyclic of order 7; we can take it to be generated by the map $x \mapsto x+1$ of $\mathbb{Z}_7$. The normaliser of this subgroup in $S_7$ can be shown to be the group of maps $x \mapsto ax+b$ where $a,b \in \mathbb{Z}_7$ and $a \neq 0$, of order 42. A subgroup of order 21 must contain $P$, and must consist of maps $x \mapsto ax+b$ where $a$ runs through a subgroup of order 3 of the multiplicative group of $\mathbb{Z}_7$, necessarily $\{1,2,4\}$.

$G$ is doubly transitive by the fact proved in Question 1.

The maps $x \mapsto ax$ for $a = 1,2,4$ form a subgroup of order 3, necessarily a Sylow 3-subgroup $Q$.

(c,d) By double transitivity there is an element $t$ interchanging $\infty$ and 0; it must normalise $Q$, since $Q$ is the two-point stabiliser, and must consist of four 2-cycles (the only alternative is 3, and then it would be an odd permutation). If it were to fix the two orbits of $Q$ it would fix a point in each and have only three 2-cycles.

(e) There are not too many possibilities for $t$; laborious calculation show that, in all cases except that given, we can obtain a non-identity permutation fixing three points from the ones we are given.

(f) The group $H$ generated by $N$ and $t$ is transitive, and contains $N$, the stabiliser of $\infty$; so it must be equal to $G$. (Both $G$ and $H$ contain $N$ as a subgroup of index 8, so they are equal.)

(g) As noted, we have shown that $G \leq \mathrm{PSL}(2,7)$. Both groups have order 168, so they are equal.

**3.3** This can be done by hard work using the Fundamental Theorem of Finite Abelian Groups. Here is a trick which makes it easier.

Let $A$ be a finite abelian group of order $n$. Let $A^*$ be the set of all homomorphisms from $A$ to the multiplicative group of $n$th roots of unity in the complex numbers. Then the operation of multiplication (that is, $a(\phi\psi) = (a\phi)(a\psi)$) makes $A^*$ a group. By using the FTFAG, we can see that $A^*$ is a group isomorphic to $A$.

Now if $B \leq A$, let $B^\dagger$ be the set of elements of $A^*$ which are the identity on $B$. Then $B^\dagger$ is the kernel of a homomorphism from $A^*$ to $B^*$, whose image is $B^*$; so $A^*/B^\dagger \cong B$. Thus $A$ has a subgroup $C$ with $A/C \cong B$; and $C \cong A/B$, by considering $(A^*)^*$, which is isomorphic to $A$.

The infinite cyclic group $\mathbb{Z}$ has the property that all its subgroups are infinite cyclic groups (the groups $n\mathbb{Z}$ for positive integers $n$) and all its quotients are finite cyclic groups $\mathbb{Z}/n\mathbb{Z}$. Clearly it doesn't have this property the other way round.

The quaternion group of order 8 has four non-trivial subgroups (all normal), once $C_2$ and three $C_4$s. but $Q_8/C_2 \cong V_4$, which is not in the list of subgroups.

**3.4** We have $G = S_3 \times S_3$, and $A = S_3 \times \{1\} = \{(g,1) : g \in S_3\}$.

One complement is $H_1 = \{1\} \times S_3 = \{(1,g) : g \in S_3\}$. It is clear that this is a complement. Moreover, $H_1$ commutes with $A$, so the action $\phi_1$ of $H_1$ on $A$ is trivial; the semidirect product $A \rtimes_\phi H_1$ is just the direct product $A \times H_1$.

Another complement is the *diagonal* subgroup

$$H_2 = \{(g,g) : g \in S_3\}.$$

(We have $(g,h) \in A \cap H_2 \Rightarrow h = 1$ and $g = h$, so $A \cap H_2 = \{1\}$; and similarly $AH_2 = G$.) The action $\phi_2$ of $H_2$ on $A$ is the usual conjugation action of $S_3$ on itself, since

$$(g,g)^{-1}(x,1)(g,g) = (g^{-1}xg,1).$$

**Remark:** Since $\mathrm{Aut}(S_3)$ is isomorphic to $S_3$, the semidirect product in the second case is the holomorph of $S_3$. So this holomorph is isomorphic to $S_3 \times S_3$.

**3.5** Suppose that $G$ is complete. Then $\mathrm{Out}(G) = \{1\}$, so

$$\mathrm{Aut}(G) = \mathrm{Inn}(G) \cong G/Z(G) \cong G,$$

the last isomorphism holding because also $Z(G) = \{1\}$.

As in the preceding question, let $A$ be the first direct factor in $G \times G$, let $H_1$ be the second direct factor, and let $H_2$ be the diagonal subgroup $\{(g,g) : g \in G\}$. Then each of $H_1$ and $H_2$ is a complement to $A$, so $G \times G \cong A \rtimes H_1 \cong A \rtimes H_2$; each of $A$, $H_1$ and $H_2$ is isomorphic to $G$, but the homomorphism $\phi_1 : H_1 \to \mathrm{Aut}(A)$ is trivial (since the two direct factors commute) while the homomorphism $\phi_2 : H_2 \to \mathrm{Aut}(A)$ is the identity map.

**3.6** An example of such a group is the dihedral group $D_8$. It is generated by two elements $g$ and $h$ satisfying $g^4 = 1$, $h^2 = 1$, $h^{-1}gh = g^{-1}$. It can be checked that the eight maps which send $g \mapsto g^a$ and $h \mapsto hg^b$ (for $a = \pm 1$, $b = 0,1,2,3$) each extend to automorphisms of $G$; and these are the only possibilities, since $g$ must map to an element of order 4, and $h$ to an element of order 2 which is not a power of $g$. Moreover, if $s : g \mapsto g, h \mapsto hg$ and $t : g \mapsto g^{-1}, h \mapsto h$, then it can be checked that $s^4 = 1$, $t^2 = 1$, and $t^{-1}st = s^{-1}$. So $s$ and $t$ generate a dihedral group of order 8.

But $D_8$ is not complete since $|Z(D_8)| = 2$.

**3.7** (a) $\mathrm{AGL}(n,2)$ is generated by the translations of $V = \mathbb{F}_2^n$ and the invertible linear maps. The translation group acts transitively, so it suffices to show that the stabiliser of the zero vector (which is $\mathrm{GL}(n,2)$) is doubly transitive.

Now, over $\mathbb{F}_2$, any two non-zero vectors are linearly independent (the only possible linear combination would be $v_1 + v_2 = 0$, implying that $v_1 = v_2$), so can be extended to a basis; and we can carry any basis to any other by an element of the general linear group. So $\mathrm{GL}(n,2)$ is doubly transitive, as required.

(b) $\mathrm{AGL}(2,2)$ has order $4|\mathrm{GL}(2,2)| = 4 \cdot 6 = 24$, and acts on the four vectors of $\mathbb{F}_2^2$, so is a subgroup of $S_4$. So $\mathrm{AGL}(2,2) \cong S_4$.

(c) $\mathrm{AGL}(3,2)$ acts on the eight points of $\mathbb{F}_2^3$, so is a subgroup of $S_8$. We need to show it is contained in $A_8$, that is, consists of even permutations. The translations are products of four 2-cycles, so are even permutations. For the elements of $\mathrm{GL}(3,2)$, either do this directly, or use the fact that if it were not so then $A_8 \cap \mathrm{GL}(3,2)$ would be a subgroup of index 2 in $\mathrm{GL}(3,2)$, hence normal, contradicting the simplicity of this group.

Now the index is $\frac{1}{2} 8!/(8 \cdot 168) = 15$.

(d) The action of $A_8$ on the fifteen cosets of $\mathrm{AGL}(3,2)$ is transitive. So we have to show that $\mathrm{AGL}(3,2)$ is transitive on the other 14 cosets.

This group contains a Sylow 7-subgroup, which has order 7 and is generated by a product of two 7-cycles. (The only alternative would be that the generator is a single 7-cycle; then the Sylow 7-subgroup would lie in eight conjugates of $\mathrm{AGL}(3,2)$, which is not possible.) So if the conclusion is false, then $\mathrm{AGL}(3,2)$ itself would have two orbits of size 7. Pick one of these orbits and count the ordered pairs $(\alpha, \beta)$ where $\beta$ lies in the specified orbit of the stabiliser of $\alpha$; there are 105 such pairs. Since 105 is odd, these pairs cannot be interchanged by an element of $A_8$. But an element of order 2 in $A_8$ must interchange some pair of points, a contradiction.

An alternative argument would be that, if $\mathrm{AGL}(3,2)$ acts on 7 points, the translation group must act trivially; and it cannot act trivially on the whole set since $A_8$ is simple. Thus not all orbits can have size 7 (or 1).

# Index