MT5864
Advanced Group Theory

Martyn Quick

Version 1.0c, 17th August 2023

University of St Andrews

Contents

Introduction

The purpose of this course is to take the study of groups further beyond the contents of the previous course. Accordingly, we note:

Prerequisite: MT4003

Syllabus

The goal of the course will be to introduce a variety of topics in more advanced group theory. The topics considered will be as follows:

Revision: Review of the basic concepts of subgroup, normal subgroup, quotient group and homomorphism, and statement of Sylow's Theorem. (At least one new, but small, result will be proved that will be used repeatedly in the module.)

Group Actions: We will explain how a group can induce permutations of a set and how, as a consequence, to deduce structural properties about subgroups and homomorphisms.

Decomposition of groups into series: We shall discuss how a group can be broken down into various factors that arise from particular series. One specific example will be the composition series where a (finite) group is broken into essentially uniquely determined simple groups. This illustrates one example of a "series" for a group. We shall prove the Jordan–Hölder Theorem that shows these simple factors are indeed unique.

Semidirect products: We discuss how groups may be constructed and in particular some ways in which the above decomposition may be reversed. We present the semidirect product (which can be viewed as a generalization of the direct product encountered before) and show how this can be used to classify some finite groups of particular orders.

Soluble groups: We shall discuss in more detail a particular class of groups that was briefly introduced in *MT4003*. They have a fairly restricted structure and are defined via something called the derived series. They can be viewed as being constructed from abelian groups (though in a relatively general way) and it is this that makes them more tractible for study. We shall establish the existence of Hall subgroups in a finite soluble group (and these are generalizations of the Sylow subgroups met previously).

Nilpotent groups: We shall give a brief introduction to an even more restricted subclass of the soluble groups defined using what are called central series. In some senses, nilpotent groups are closer in behaviour to abelian groups though all finite groups of prime-power order are nilpotent (and p-groups can be viewed as the canonical examples).

Structure of permutation groups: Cayley's Theorem tells us that every group can be embedded as a subgroup of a symmetric group. We shall consider in more detail how structural information about subgroups of symmetric groups can be determined from information about the associated natural action.

Themes: There will be two main themes which we shall attempt to exploit during the course.

(i) *Group Actions:* essentially this boils down to a group inducing certain permutations of a set and using this to obtain information about the original group.

(ii) *Series:* If a group G has a collection of subgroups

$$G = G_0 > G_1 > G_2 > \cdots > G_n = \mathbf{1}$$

where G_{i+1} is a normal subgroup of G_i for all i, then information about the various quotient groups G_i/G_{i+1} $(0 \leqslant i \leqslant n-1)$ yields information about G.

Reading List

Electronically Available Resources

- Antonio Machi, *Groups: An introduction to ideas and methods of the theory of groups*, Springer 2012.
- Steven Roman, *Fundamentals of Group Theory: An advanced approach*, Birkäuser 2012.
- Derek J. S. Robinson, *A Course in the Theory of Groups (Second Edition)*, Graduate Texts in Mathematics **80**, Springer–Verlag, New York, 1996.
- Derek J. S. Robinson, *Abstract Algebra: An introduction with applications, 2nd edition*, De Gruyter, 2015.
- Harvey E. Rose, *A Course on Finite Groups*, Springer 2009.
- Joseph J. Rotman, *An Introduction to the Theory of Groups*, Graduate Texts in Mathematics **148**, Springer–Verlag, New York, 1995. [Earlier edition, Allyn & Bacon, 1965]
- Peter J. Cameron, *Permutation Groups*, Cambridge University Press 1999.
- John D. Dixon & Brian Mortimer, *Permutation Groups*, Graduate Texts in Mathematics **163**, Springer–Verlag, New York, 1996.

Physical Textbooks

The following are useful for consultation, but not essential. The first two used to be relatively cheap, but are possibly now out-of-print.

- John S. Rose, *A Course on Group Theory*, Dover Publications, New York, 1994.

- B. A. F. Wehrfritz, *Finite Groups: A Second Course on Group Theory*, World Scientific, Singapore, 1999.
- M. I. Kargapolov & Ju. I. Merzljakov, *Fundamentals of the Theory of Groups*, Graduate Texts in Mathematics **62**, Springer–Verlag, New York, 1979.

Chapter 1

Review/Revision

In this first section we shall principally recall definitions and results from earlier lecture courses. During the lectures, proofs of results that have been previously met will often be omitted (though these notes will contain many of them). We shall also specify the notation to be used throughout the course. We shall not introduce examples of groups in this chapter, but instead both use problem sheets and recall specific groups in various examples in later chapters.

Definition 1.1 A *group* G is a set with a binary operation (usually written multiplicatively)

$$\begin{aligned} G \times G &\to G \\ (x, y) &\mapsto xy \end{aligned}$$

such that

(i) the binary operation is *associative*: $x(yz) = (xy)z$ for all $x, y, z \in G$;

(ii) there is an *identity element* 1 in G: $x1 = 1x = x$ for all $x \in G$;

(iii) each element x in G possesses an *inverse* x^{-1}: $xx^{-1} = x^{-1}x = 1$.

Comments:

(i) This definition makes no explicit reference to 'closure' as an axiom. The reason for this is that this condition is actually built into the definition of a binary operation. A binary operation takes two elements of our group and produces an element *in the group*, and so we automatically obtain closure.

(ii) Associativity ensures that we can safely omit brackets from a product $x_1x_2 \dots x_n$ of n elements x_1, x_2, …, x_n of a group. Thus, for example, the following products are all equal:

$$x_1(x_2(x_3x_4)), \qquad (x_1(x_2x_3))x_4, \qquad ((x_1x_2)x_3)x_4, \qquad \text{etc.}$$

(iii) We can define powers x^n where $x \in G$ and $n \in \mathbb{Z}$. The standard power laws hold in group where the binary operation is multiplicatively written:

$$x^{m+n} = x^m x^n \qquad \text{and} \qquad x^{mn} = (x^m)^n$$

for $x \in G$ and $m, n \in \mathbb{Z}$. We do need to remember that in general group elements do not commute (so, for example, we cannot easily expand $(xy)^n$) although we can expand the following inverse:

$$(xy)^{-1} = y^{-1}x^{-1}.$$

PROOF: (OMITTED IN LECTURES)

$$(y^{-1}x^{-1})(xy) = y^{-1}x^{-1}xy = y^{-1}1y = y^{-1}y = 1,$$

so multiplying on the right by the inverse of xy yields $y^{-1}x^{-1} = (xy)^{-1}$. □

For completeness, let us record the term used for groups where all the elements present do commute:

Definition 1.2 A group G is called *abelian* if all its elements *commute*; that is, if

$$xy = yx \qquad \text{for all } x, y \in G.$$

Subgroups

Although one is initially tempted to attack groups by examining their elements in detail, this turns out not to be terribly fruitful. Even an only moderately sized group is unyielding to consideration of its multiplication table. Instead one needs to find some sort of "structure" to study and this is provided by subgroups and homomorphisms (and, particularly related to the latter, quotient groups).

A subgroup of a group is a subset which is itself a group under the multiplication inherited from the larger group. Thus:

Definition 1.3 A subset H of a group G is a *subgroup* of G if

(i) H is non-empty,

(ii) $xy \in H$ and $x^{-1} \in H$ for all $x, y \in H$.

We write $H \leqslant G$ to indicate that H is a subgroup of G. If G is a group, the set containing the identity element (which I shall denote by $\mathbf{1}$) and the whole group G are always subgroups. We shall usually be interested in finding other subgroups of a group.

We mention in passing that the above conditions for a subset to be a subgroup are not the only ones that can be used, but they are sufficient for our needs (and easily memorable).

The identity element of G lies in every subgroup, so it is easy to see that the conditions of Definition 1.3 are inherited by intersections. Therefore:

Lemma 1.4 *If $\{ H_i \mid i \in I \}$ is a collection of subgroups of a group G, then $\bigcap_{i \in I} H_i$ is also a subgroup of G.*

PROOF: (OMITTED IN LECTURES) Since $1 \in H_i$ for all i, it follows that $\bigcap_{i \in I} H_i \neq \varnothing$. Now let $x, y \in \bigcap_{i \in I} H_i$. Then for each i, $x, y \in H_i$, so $xy \in H_i$ and $x^{-1} \in H_i$ since $H_i \leqslant G$. We deduce that $xy \in \bigcap_{i \in I} H_i$ and $x^{-1} \in \bigcap_{i \in I} H_i$. Thus the intersection is a subgroup. □

In general, the union of a family of subgroups of a group is not itself a subgroup. This is not a disaster, however, as the following construction provides a way around this.

Definition 1.5 Let G be a group and X be a subset of G. The *subgroup of G generated by X* is denoted by $\langle X \rangle$ and is defined to be the intersection of all subgroups of G which contain X:

$$\langle X \rangle = \bigcap \{\, H \mid X \subseteq H \leqslant G \,\}$$

Lemma 1.4 ensures that $\langle X \rangle$ is a subgroup of G. It is the smallest subgroup of G containing X (in the sense that it is contained in all other such subgroups; that is, if H is any subgroup of G containing X then $\langle X \rangle \leqslant H$).

Lemma 1.6 *Let G be a group and X be a subset of G. Then*

$$\langle X \rangle = \{\, x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n} \mid n \geqslant 0,\ \ x_i \in X,\ \ \varepsilon_i = \pm 1 \text{ for all } i \,\}.$$

Thus $\langle X \rangle$ consists of all products of elements of X and their inverses.

Proof: (Omitted in lectures) Let S denote the set on the right-hand side. Since $\langle X \rangle$ is a subgroup (by Lemma 1.4) and by definition it contains X, we deduce that $\langle X \rangle$ must contain all products of elements of X and their inverses. Thus $S \subseteq \langle X \rangle$.

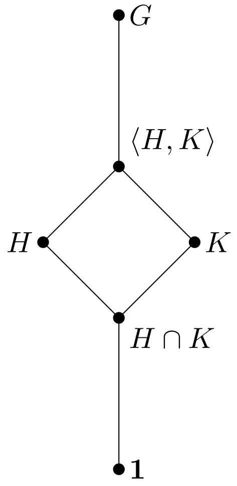
On the other hand, S is non-empty (for example, it contains the empty product (where $n = 0$) which by convention is taken to be the identity element 1), it contains all elements of X (the case $n = 1$ and $\varepsilon_1 = 1$), is clearly closed under products and

$$(x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n})^{-1} = x_n^{-\varepsilon_n} x_{n-1}^{-\varepsilon_{n-1}} \dots x_1^{-\varepsilon_1} \in S.$$

Hence S is a subgroup of G. The fact that $\langle X \rangle$ is the smallest subgroup containing X now gives $\langle X \rangle \leqslant S$ and we deduce the equality claimed in the lemma. □

Now if H and K are subgroups of G, we have $\langle H, K \rangle$ available as the smallest subgroup of G that contains both H and K. We usually use this instead of the union.

We will wish to manipulate the subgroups of a group and understand how they relate to each other. Useful in such a situation are diagrams where we represent subgroups by nodes and use an upward (sometimes sloping) line to denote inclusion. For example, the following illustrates the phenomena just discussed:



For subgroups H and K of G, the intersection $H \cap K$ is the largest subgroup contained in H and K, and $\langle H, K \rangle$ is the smallest subgroup containing H and K.

Cosets

Subgroups enforce a rigid structure on a group: specifically a group is the disjoint union of the cosets of any particular subgroup. Accordingly we need the following definition.

Definition 1.7 Let G be a group, H be a subgroup of G and x be an element of G. The (*right*) *coset* of H with *representative* x is the following subset of G:

$$Hx = \{\, hx \mid h \in H \,\}$$

We can equally well define what is meant by a left coset, but we shall work almost exclusively with right cosets. For the latter reason we shall simply use the term 'coset' to always mean 'right coset'.

Theorem 1.8 *Let G be a group and H be a subgroup of G.*

(i) *If $x, y \in G$, then $Hx = Hy$ if and only if $xy^{-1} \in H$.*

(ii) *Any two cosets of H are either equal or are disjoint: if $x, y \in G$, then either $Hx = Hy$ or $Hx \cap Hy = \varnothing$.*

(iii) *G is the disjoint union of the cosets of H.*

(iv) *If $x \in G$, the map $h \mapsto hx$ is a bijection from H to the coset Hx.*

Proof: (Omitted in lectures) (i) Suppose $Hx = Hy$. Then $x = 1x \in Hx = Hy$, so $x = hy$ for some $h \in H$. Thus $xy^{-1} = h \in H$.

Conversely if $xy^{-1} \in H$, then $hx = h(xy^{-1})y \in Hy$ for all $h \in H$, so $Hx \subseteq Hy$. Also $hy = hyx^{-1}x = h(xy^{-1})^{-1}x \in Hx$ for all $h \in H$, so $Hy \subseteq Hx$. Thus $Hx = Hy$ under this assumption.

(ii) Suppose that $Hx \cap Hy \neq \varnothing$. Then there exists $z \in Hx \cap Hy$, say $z = hx = ky$ for some $h, k \in H$. Then $xy^{-1} = h^{-1}k \in H$ and we deduce $Hx = Hy$ by (i).

(iii) If $x \in G$, then $x = 1x \in Hx$. Hence the union of all the (right) cosets of H is the whole of G. Part (ii) ensures this is a disjoint union.

(iv) By definition of the coset Hx, the map $h \mapsto hx$ is a surjective map from H to Hx. Suppose $hx = kx$ for some $h, k \in H$. Then multiplying on the right by x^{-1} yields $h = k$. Thus this map is also injective, so it is a bijection, as claimed. □

Write $|G : H|$ for the number of cosets of H in G and call this the *index* of H in G. The previous result tells us that our group G is the disjoint union of $|G : H|$ cosets of H and each of these contain $|H|$ elements. Hence:

Theorem 1.9 (Lagrange's Theorem) *Let G be a group and H be a subgroup of G. Then*

$$|G| = |G : H| \cdot |H|.$$

In particular, if H is a subgroup of a finite group G, then the order of H divides the order of G. □

The following fact about indices of subgroups is frequently used:

Lemma 1.10 *Let H and K be subgroups of a group G with $K \leqslant H \leqslant G$. Then*

$$|G : K| = |G : H| \cdot |H : K|.$$

For finite groups, this is easily deduced from Lagrange's Theorem:

$$|G:K| = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = |G:H| \cdot |H:K|.$$

The full proof for an arbitrary, possibly infinite, group is omitted. It appears on Problem Sheet I.

Orders of elements and cyclic groups

Definition 1.11 If G is a group and x is an element of G, we define the *order* of x to be the smallest positive integer n such that $x^n = 1$ (if such exists) and otherwise say that x has *infinite order*. We write $o(x)$ for the order of the element x.

If $x^i = x^j$ for $i < j$, then $x^{j-i} = 1$ and x has finite order and $o(x) \leqslant j - i$. In particular, the powers of x are always distinct if x has infinite order. If the element x has finite order n and $k \in \mathbb{Z}$, write $k = nq + r$ where $0 \leqslant r < n$. Then

$$x^k = x^{nq+r} = (x^n)^q x^r = x^r \tag{1.1}$$

(since $x^n = 1$). Furthermore 1, x, x^2, ..., x^{n-1} are distinct (by the first line of the previous paragraph). Hence:

Proposition 1.12 (i) *If $x \in G$ has infinite order, then the powers x^i (for $i \in \mathbb{Z}$) are distinct.*

(ii) *If $x \in G$ has order n, then x has precisely n distinct powers, namely 1, x, x^2, ..., x^{n-1}.* □

Corollary 1.13 *Let G be a group and $x \in G$. Then*

$$o(x) = |\langle x \rangle|.$$

If G is a finite group, then $o(x)$ divides $|G|$. □

Equation (1.1) yields a further observation, namely:

$$x^k = 1 \qquad \text{if and only if} \qquad o(x) \mid k.$$

In the case that a single element generates the whole group, we give a special name:

Definition 1.14 A group G is called *cyclic* (with *generator* x) if $G = \langle x \rangle$.

The following fact about the subgroups of finite cyclic groups was established in *MT4003*. The proof basically depends upon the ideas just described. The details are omitted here and found instead, together with the analogous result for the infinite cyclic groups, on Problem Sheet I.

Theorem 1.15 *Let G be a finite cyclic group of order n. Then G has precisely one subgroup of order d for every divisor d of n.*

Normal subgroups and quotient groups

Definition 1.16 A subgroup N of a group G is called a *normal subgroup* of G if $g^{-1}xg \in N$ for all $x \in N$ and all $g \in G$. We write $N \trianglelefteqslant G$ to indicate that N is a normal subgroup of G.

The element $g^{-1}xg$ is called the *conjugate* of x by g and is often denoted by x^g. We shall discuss this operation a little towards the end of this chapter, but in much greater detail in Chapter 2.

If $N \trianglelefteqslant G$, then we write G/N for the set of cosets of N in G:

$$G/N = \{\, Nx \mid x \in G \,\}.$$

Theorem 1.17 *Let G be a group and N be a normal subgroup of G. Then*

$$G/N = \{\, Nx \mid x \in G \,\},$$

the set of cosets of N in G, is a group when we define the multiplication by

$$Nx \cdot Ny = Nxy$$

for $x, y \in G$.

Proof: (Omitted in lectures) The part of this proof requiring the most work is to show that this product is actually well-defined. Suppose that $Nx = Nx'$ and $Ny = Ny'$ for some elements $x, x', y, y' \in G$. Then $x = ax'$ and $y = by'$ for some $a, b \in N$. Then

$$xy = (ax')(by') = ax'b(x')^{-1}x'y' = ab^{(x')^{-1}}x'y'.$$

Since $N \trianglelefteqslant G$, it follows that $b^{(x')^{-1}} \in N$. Hence $(xy)(x'y')^{-1} = ab^{(x')^{-1}} \in N$ and we deduce $Nxy = Nx'y'$. This shows that the above multiplication of cosets is indeed well-defined.

It remains to show that the set of cosets forms a group under this multiplication. If $x, y, z \in G$, then

$$(Nx \cdot Ny) \cdot Nz = Nxy \cdot Nz = N(xy)z = Nx(yz) = Nx \cdot Nyz = Nx \cdot (Ny \cdot Nz).$$

Thus the multiplication is associative. We calculate

$$Nx \cdot N1 = Nx1 = Nx = N1x = N1 \cdot Nx$$

for all cosets Nx, so $N1$ is the identity element in G/N, while

$$Nx \cdot Nx^{-1} = Nxx^{-1} = N1 = Nx^{-1}x = Nx^{-1} \cdot Nx,$$

so Nx^{-1} is the inverse of Nx in G/N.

Thus G/N is a group. □

Definition 1.18 If G is a group and N is a normal subgroup of G, we call G/N (with the above multiplication) the *quotient group* of G by N.

We shall discuss quotient groups later in this section. They are best discussed, however, in the context of homomorphisms, so we shall move onto these in a short while. We just mention some results (one part of which is proved here, the rest appear on Problem Sheet I) which will be needed later.

Lemma 1.19 *Let G be a group and let H and K be subgroups of G. Define $HK = \{\, hk \mid h \in H,\ k \in K \,\}$. Then*

(i) *HK is a subgroup of G if and only if $HK = KH$;*

(ii) *if K is a normal subgroup of G then HK is a subgroup of G (and consequently $HK = KH$);*

(iii) *if H and K are normal subgroups of G, then $H \cap K$ and HK are normal subgroups of G;*

(iv) *$|HK| \cdot |H \cap K| = |H| \cdot |K|$.*

When H and K are finite, then we can rearrange the last formula to give

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

This formula holds even when HK is not a subgroup.

Proof: (iv) Define a map $\alpha \colon H \times K \to HK$ by

$$(h, k) \mapsto hk.$$

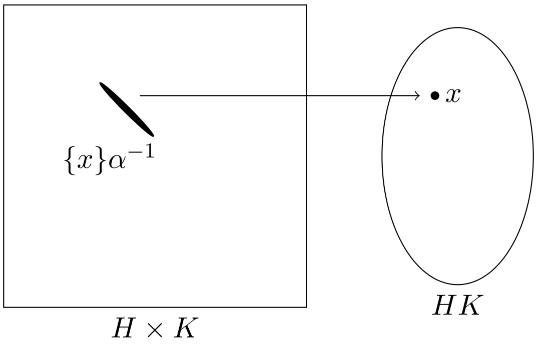
Then α is surjective. Fix a point $x \in HK$, say $x = h_0 k_0$ for some fixed $h_0 \in H$ and $k_0 \in K$. Then for $(h, k) \in H \times K$,

$$\begin{aligned} (h,k)\alpha = x \qquad & \text{if and only if} \qquad hk = h_0 k_0 \\ & \text{if and only if} \qquad h_0^{-1} h = k_0 k^{-1} \in H \cap K \\ & \text{if and only if} \qquad h = h_0 a,\ k = a^{-1} k_0 \quad \text{where } a \in H \cap K. \end{aligned}$$

Thus for each $x \in HK$, we see that the set of elements mapped by α to x is

$$\{x\}\alpha^{-1} = \{\, (h,k) \in H \times K \mid (h,k)\alpha = x \,\} = \{\, (h_0 a, a^{-1} k_0) \mid a \in H \cap K \,\}.$$

This set is in one-one correspondence with the set $H \cap K$ via the bijection $a \mapsto (h_0 a, a^{-1} k_0)$. Hence we may partition $H \times K$ into $|HK|$ subsets, each corresponding to one point in HK and of size $|H \cap K|$.



This proves

$$|H \times K| = |HK| \cdot |H \cap K|;$$

that is,

$$|H| \cdot |K| = |HK| \cdot |H \cap K|. \qquad \square$$

Homomorphisms

Definition 1.20 Let G and H be groups. A *homomorphism* from G to H is a map $\phi\colon G \to H$ such that

$$(xy)\phi = (x\phi)(y\phi) \qquad \text{for all } x, y \in G.$$

Thus a homomorphism between two groups is a map which, in the sense of the above formula, "preserves" their multiplications. Note that I am writing my maps on the right, as is conventional in much of algebra. This has several advantages: the first is that when we compose a number of maps we can read from left to right, rather than from right to left. It will also be consistent with the notation that we use for group actions in Chapter 2 and it will make certain proofs more notationally convenient.

The following definition presents important subsets (actually subgroups) that are related to homomorphisms.

Definition 1.21 Let $\phi\colon G \to H$ be a homomorphism between two groups. Then the *kernel* of ϕ is

$$\ker\phi = \{\, x \in G \mid x\phi = 1 \,\},$$

while the *image* of ϕ is

$$\operatorname{im}\phi = G\phi = \{\, x\phi \mid x \in G \,\}.$$

Note that $\ker\phi \subseteq G$ while $\operatorname{im}\phi \subseteq H$ here.

Lemma 1.22 *Let $\phi\colon G \to H$ be a homomorphism between two groups G and H. Then*

(i) $1\phi = 1$*;*

(ii) $(x^{-1})\phi = (x\phi)^{-1}$ *for all $x \in G$;*

(iii) *the kernel of ϕ is a normal subgroup of G;*

(iv) *the image of ϕ is a subgroup of H.*

Proof: (Omitted in lectures) (i) $1\phi = (1 \cdot 1)\phi = (1\phi)(1\phi)$ and multiplying by the inverse of 1ϕ yields $1 = 1\phi$.

(ii) $(x\phi)(x^{-1}\phi) = (xx^{-1})\phi = 1\phi = 1$ and multiplying on the left by the inverse of $x\phi$ yields $(x^{-1})\phi = (x\phi)^{-1}$.

(iii) By (i), $1 \in \ker\phi$. If $x, y \in \ker\phi$, then $(xy)\phi = (x\phi)(y\phi) = 1 \cdot 1 = 1$ and $(x^{-1})\phi = (x\phi)^{-1} = 1^{-1} = 1$, so we deduce $xy \in \ker\phi$ and $x^{-1} \in \ker\phi$. Therefore $\ker\phi$ is a subgroup of G. Now if $x \in \ker\phi$ and $g \in G$, then $(g^{-1}xg)\phi = (g^{-1}\phi)(x\phi)(g\phi) = (g\phi)^{-1}1(g\phi) = 1$, so $g^{-1}xg \in \ker\phi$. Hence $\ker\phi$ is a normal subgroup of G.

(iv) Let $g, h \in \operatorname{im}\phi$. Then $g = x\phi$ and $h = y\phi$ for some $x, y \in G$. Then $gh = (x\phi)(y\phi) = (xy)\phi \in \operatorname{im}\phi$ and $g^{-1} = (x\phi)^{-1} = (x^{-1})\phi \in \operatorname{im}\phi$. Thus $\operatorname{im}\phi$ is a subgroup of G. □

The kernel is also useful for determining when a homomorphism is injective.

Lemma 1.23 *Let $\phi\colon G \to H$ be a homomorphism between two groups G and H. Then ϕ is injective if and only if* $\ker\phi = \mathbf{1}$.

PROOF: Suppose ϕ is injective. If $x \in \ker\phi$, then $x\phi = 1 = 1\phi$, so $x = 1$ by injectivity. Hence $\ker\phi = \mathbf{1}$.

Conversely suppose that $\ker\phi = \mathbf{1}$. If $x\phi = y\phi$, then $(xy^{-1})\phi = (x\phi)(y\phi)^{-1} = 1$, so $xy^{-1} \in \ker\phi$. Hence $xy^{-1} = 1$ and, upon multiplying on the right by y, we deduce $x = y$. Hence ϕ is injective. □

Example 1.24 Let G be a group and N be a normal subgroup of G. Define a map $\pi\colon G \to G/N$ by

$$\pi\colon x \mapsto Nx.$$

The definition of the multiplication in the quotient group G/N ensures that π is a homomorphism. It is called the *natural map* (or *canonical homomorphism*). We see

$$\ker\pi = \{\, x \in G \mid Nx = N1 \,\};$$

that is,

$$\ker\pi = N,$$

and clearly $\operatorname{im}\pi = G/N$; that is, π is surjective.

Thus it is not just that every kernel is a normal subgroup, but also that every normal subgroup is the kernel of some homomorphism. Indeed, one can interpret this example together with the First Isomorphism Theorem (below) as saying that normal subgroups and homomorphisms are in some sense in correspondence.

Isomorphism Theorems

We shall finish this section by discussing the four important theorems that relate quotient groups and homomorphisms. We shall need the concept of isomorphism, so we recall that first.

Definition 1.25 An *isomorphism* between two groups G and H is a homomorphism $\phi\colon G \to H$ which is a bijection. We write $G \cong H$ to indicate that there is an isomorphism between G and H, and we say that G and H are *isomorphic.*

What this means is that if G and H are isomorphic groups, then the elements of the two groups are in one-one correspondence in such a way that the group multiplications produce precisely corresponding elements. Thus essentially the groups are identical: we may have given the groups different names and labelled the elements differently, but we are looking at identical objects in terms of their structure.

Theorem 1.26 (First Isomorphism Theorem) *Let G and H be groups and $\phi\colon G \to H$ be a homomorphism. Then $\ker\phi$ is a normal subgroup of G, $\operatorname{im}\phi$ is a subgroup of H and*

$$G/\ker\phi \cong \operatorname{im}\phi.$$

PROOF: (SKETCH) We already know that $\ker\phi \trianglelefteq G$, so we can form $G/\ker\phi$. The isomorphism is the map

$$(\ker\phi)x \mapsto x\phi \qquad (\text{for } x \in G). \qquad \square$$

Proof: (Omitted details) Let $K = \ker \phi$ and define $\theta \colon G/K \to \operatorname{im} \phi$ by $Kx \mapsto x\phi$ for $x \in G$. We note

$$\begin{array}{lll} Kx = Ky & \text{if and only if} & xy^{-1} \in K \\ & \text{if and only if} & (xy^{-1})\phi = 1 \\ & \text{if and only if} & (x\phi)(y\phi)^{-1} = 1 \\ & \text{if and only if} & x\phi = y\phi. \end{array}$$

This shows that θ is well-defined and also that it is injective. By definition of the image, θ is surjective. Finally

$$\big((Kx)(Ky)\big)\theta = (Kxy)\theta = (xy)\phi = (x\phi)(y\phi) = (Kx)\theta \cdot (Ky)\theta$$

for all $x, y \in G$, so θ is a homomorphism. Hence θ is the required isomorphism. (All other parts of the theorem are found in Lemma 1.22.) □

Rather than move straight on to the Second and Third Isomorphism Theorems, I shall deal with the Correspondence Theorem next so that I can use it when talking about the other Isomorphism Theorems. The Correspondence Theorem essentially tells us how to handle quotient groups, at least in terms of their subgroups, which is to some extent the principal way of handling them anyway.

Theorem 1.27 (Correspondence Theorem) *Let G be a group and let N be a normal subgroup of G.*

(i) *There is a one-one inclusion-preserving correspondence between subgroups of G containing N and subgroups of G/N given by*

$$H \mapsto H/N \qquad \text{whenever } N \leqslant H \leqslant G.$$

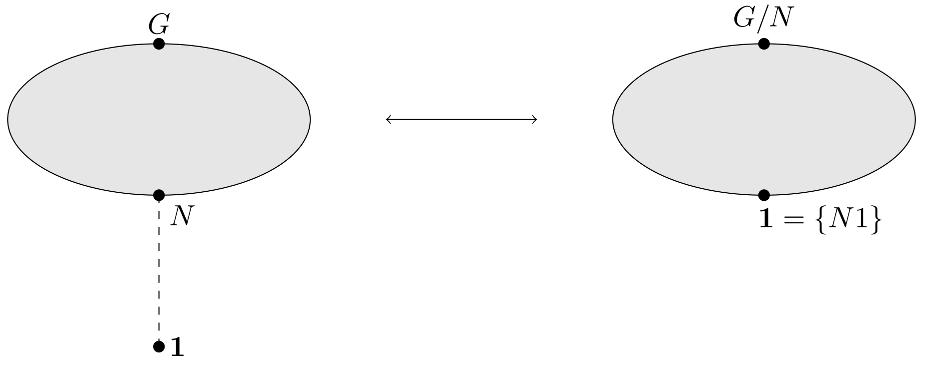
(ii) *Under the above correspondence, normal subgroups of G which contain N correspond to normal subgroups of G/N.*

The primary content of Part (i) of the Correspondence Theorem is that every subgroup of G/N can be uniquely expressed in the form H/N for some subgroup H of G that contains N. We shall frequently use the existence of this expression when trying to work with subgroups of the quotient group. Moreover, Part (ii) then tells us that this subgroup H/N is normal in G/N precisely when the corresponding subgroup H is normal in G; that is,

$$H \trianglelefteqslant G \qquad \text{if and only if} \qquad H/N \trianglelefteqslant G/N$$

for $N \leqslant H \leqslant G$.

If we view it that the ‘structure’ of a group is somehow the shape of the diagram of subgroups (with those ‘special’ subgroups which are normal indicated), then the Correspondence Theorem tells us how the structures of a group and a quotient are related. The diagram of subgroups of the quotient group G/N is simply that part of the diagram of subgroups sandwiched between G and N.



PROOF: (OMITTED IN LECTURES) Let $\mathscr{S}$ denote the set of subgroups of G that contain N (that is, $\mathscr{S} = \{\, H \mid N \leqslant H \leqslant G \,\}$) and let $\mathscr{T}$ denote the set of subgroups of G/N. Let $\pi \colon G \to G/N$ denote the natural map $x \mapsto Nx$.

First note that if $H \in \mathscr{S}$, then N is certainly also a normal subgroup of H and we can form the quotient group H/N. This consists of some of the elements of G/N and forms a group, so is a subgroup of G/N. Thus we do indeed have a map $\Phi \colon \mathscr{S} \to \mathscr{T}$ given by $H \mapsto H/N$. Also note that if $H_1, H_2 \in \mathscr{S}$ with $H_1 \leqslant H_2$, then we immediately obtain $H_1/N \leqslant H_2/N$, so Φ preserves inclusions.

Suppose $H_1, H_2 \in \mathscr{S}$ and that $H_1/N = H_2/N$. Let $x \in H_1$. Then $Nx \in H_1/N = H_2/N$, so $Nx = Ny$ for some $y \in H_2$. Then $xy^{-1} \in N$, say $xy^{-1} = n$ for some $n \in N$. Since $N \leqslant H_2$, we then deduce $x = ny \in H_2$. This shows $H_1 \leqslant H_2$ and a symmetrical argument shows $H_2 \leqslant H_1$. Hence if $H_1\Phi = H_2\Phi$ then necessarily $H_1 = H_2$, so Φ is injective.

Finally let $J \in \mathscr{T}$. Let H be the inverse image of J under the natural map π; that is,

$$H = \{\, x \in G \mid x\pi \in J \,\} = \{\, x \in G \mid Nx \in J \,\}.$$

If $x \in N$, then $Nx = N1 \in J$, since $N1$ is the identity element in the quotient group. Therefore $N \leqslant H$. If $x, y \in H$, then $Nx, Ny \in J$ and so $Nxy = (Nx)(Ny) \in J$ and $Nx^{-1} = (Nx)^{-1} \in J$. Hence $xy, x^{-1} \in H$, so we deduce that H is a subgroup which contains N. Thus $H \in \mathscr{S}$. We now consider the image of this subgroup H under the map Φ. If $x \in H$, then $Nx \in J$, so $H/N \leqslant J$. On the other hand, an arbitrary element of J has the form Nx for some element x in G and, by definition, this element x belongs to H. Hence every element of J has the form Nx for some $x \in H$ and we conclude $J = H/N = H\Phi$. Thus Φ is surjective.

This completes the proof of Part (i).

(ii) We retain the notation of Part (i). Suppose $H \in \mathscr{S}$ and that $H \trianglelefteqslant G$. Consider a coset Nx in H/N (with $x \in H$) and an arbitrary coset Ng in G/N. Now $g^{-1}xg \in H$ since $H \trianglelefteqslant G$, so $(Ng)^{-1}(Nx)(Ng) = Ng^{-1}xg \in H/N$. Thus $H/N \trianglelefteqslant G/N$.

Conversely suppose $J \trianglelefteqslant G/N$. Let $H = \{\, x \in G \mid Nx \in J \,\}$, so that $J = H/N$ (as in the last part of the proof of (i)). Let $x \in H$ and $g \in G$. Then $Nx \in J$, so $Ng^{-1}xg = (Ng)^{-1}(Nx)(Ng) \in J$ by normality of J. Thus $g^{-1}xg \in H$, by definition of H, and we deduce that $H \trianglelefteqslant G$.

Hence normality is preserved by the bijection Φ. □

Theorem 1.28 (Second Isomorphism Theorem) *Let G be a group, let H be a subgroup of G and let N be a normal subgroup of G. Then $H \cap N$ is a normal subgroup of H, NH is a subgroup of G, and*

$$H/(H \cap N) \cong NH/N.$$

Proof: The natural map $\pi\colon x \mapsto Nx$ is a homomorphism $G \to G/N$. Let ϕ be the restriction to H; i.e., $\phi\colon H \to G/N$ given by $x \mapsto Nx$ for all $x \in H$. Then ϕ is once again a homomorphism,

$$\ker\phi = H \cap \ker\pi = H \cap N$$

and

$$\operatorname{im}\phi = \{\, Nx \mid x \in H \,\} = \{\, Nnx \mid x \in H,\ n \in N \,\} = NH/N.$$

By the First Isomorphism Theorem, $H \cap N \trianglelefteqslant H$, $NH/N \leqslant G/N$ and

$$H/(H \cap N) \cong NH/N.$$

Finally NH is a subgroup of G by the Correspondence Theorem. □

Note: Since we shall need it later, we record that the isomorphism $H/(H \cap N) \to NH/N$ is given by

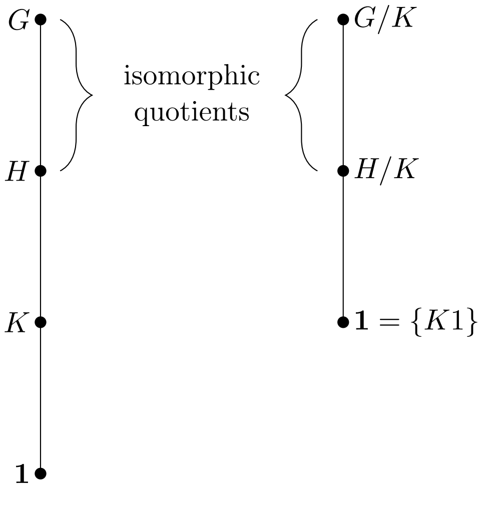
$$(H \cap N)x \mapsto Nx$$

(as this is the isomorphism that the proof of the First Isomorphism Theorem gives us).

Theorem 1.29 (Third Isomorphism Theorem) *Let G be a group and let H and K be normal subgroups of G such that $K \leqslant H \leqslant G$. Then H/K is a normal subgroup of G/K and*

$$\frac{G/K}{H/K} \cong G/H.$$

This theorem then tells us about the behaviour of normal subgroups of quotient groups and their associated quotients. Specifically, via the Correspondence Theorem we know that a normal subgroup of the quotient group G/K has the form H/K where $K \leqslant H \trianglelefteqslant G$. Now we would like to know what the quotient group by this normal subgroup is, and the Third Isomorphism Theorem tells us that it is the same as the quotient in the original group. In terms of our diagrams of subgroups, the following occurs:



Proof: Define $\theta\colon G/K \to G/H$ by $Kx \mapsto Hx$ for $x \in G$. This is a well-defined map [if $Kx = Ky$, then $xy^{-1} \in K \leqslant H$, so $Hx = Hy$] which is easily seen to be a homomorphism $[\big((Kx)(Ky)\big)\theta = (Kxy)\theta = Hxy = (Hx)(Hy) = (Kx)\theta \cdot (Ky)\theta$ for all $x, y \in G]$ and clearly $\operatorname{im}\theta = G/H$. The kernel is

$$\ker\theta = \{\, Kx \mid x \in H \,\} = H/K.$$

Hence, by the First Isomorphism Theorem, $H/K \trianglelefteq G/K$ and

$$\frac{G/K}{H/K} \cong G/H. \qquad \square$$

Sylow's Theorem

The final topic that we cover in this review section is the most important result from *MT4003*, indeed probably the most important theorem that there is concerning finite groups.

Definition 1.30 Let p be a prime number and G be a finite group.

(i) We say G is a *p-group* if its order is a power of p.

(ii) If G is any finite group, a *p-subgroup* of G is a subgroup whose order is a power of p.

(iii) Suppose that $|G| = p^n m$ where p does not divide m. A *Sylow p-subgroup* of G is a subgroup of order p^n.

Thus Lagrange's Theorem tells us that a Sylow p-subgroup of G is a p-subgroup of the largest possible order. Note that if $|G| = p^n m$ where $p \nmid m$ and P is a Sylow p-subgroup of G, then $|G : P| = m$ and this is coprime to p.

Theorem 1.31 (Sylow's Theorem) *Let p be a prime number, G be a finite group and write $|G| = p^n m$ where p does not divide m. Then*

(i) *G has a Sylow p-subgroup;*

(ii) *any two Sylow p-subgroups are conjugate in G;*

(iii) *the number of Sylow p-subgroups of G is congruent to $1 \pmod p$ and divides m;*

(iv) *any p-subgroup of G is contained in a Sylow p-subgroup.*

Before discussing initially the significance of this theorem, we will present some information about conjugation since this arises in part (ii) of the theorem.

Let G be a group and fix an element $x \in G$. Write τ_x for the map which is conjugation by x:

$$\begin{aligned} \tau_x \colon G &\to G \\ g &\mapsto g^x = x^{-1}gx. \end{aligned}$$

Observations:

(i)

$$(gh)\tau_x = x^{-1}ghx = x^{-1}gx \cdot x^{-1}hx = (g\tau_x)(h\tau_x)$$

for all $g, h \in G$; that is, τ_x is a homomorphism.

(ii)

$$g\tau_x\tau_{x^{-1}} = x(x^{-1}gx)x^{-1} = g$$

so that $\tau_x\tau_{x^{-1}} = \mathrm{id}_G$, and similarly $\tau_{x^{-1}}\tau_x = \mathrm{id}_G$. Hence τ_x is an invertible map (it has $\tau_{x^{-1}}$ as its inverse).

Invertible homomorphisms are, of course, called isomorphisms, but in the special case where the homomorphism is from a group back to itself, we give it a special name.

Definition 1.32 Let G be a group. An *automorphism* of G is a map $G \to G$ which is an isomorphism.

We have shown that τ_x (conjugation by x) is an automorphism of our group. We use the term *inner automorphism* to refer to the specific automorphisms that arise in this form; that is, the inner automorphisms of G are all the maps $G \to G$ of the form $\tau_x \colon g \mapsto g^x$ for $x \in G$.

Now if H is a subgroup of G, its image under this automorphism must still be a subgroup. Hence the conjugate

$$H^x = \{\, x^{-1}hx \mid h \in H \,\}$$

is also a subgroup of G. The inner automorphism τ_x restricts to an isomorphism $H \to H^x$ and hence this conjugate is isomorphic to the original subgroup H. In particular, the conjugates of H all have the same order as the original subgroup H.

Let us now return to Sylow's Theorem. What this significant theorem tells us is:

(i) Certain types of subgroups always exist in a finite group. In general, the converse of Lagrange's Theorem is false: there exist finite groups G with a divisor m of $|G|$ where there is no subgroup of order m. The first part of Sylow's Theorem essentially tells us that for divisors of $|G|$ that are prime-powers, the converse does hold. This means that we can actually find subgroups to work with, as opposed to using Lagrange's Theorem which mostly functions as a tool to say certain subgroups do not exist.

(ii) If P is a Sylow p-subgroup, then certainly every conjugate P^x (for $x \in G$) is also a Sylow p-subgroup as it has the same order. The theorem tells us that all the Sylow p-subgroups arise in this way and so, in particular, they all look essentially the same (that is, they are isomorphic).

(iii) We have strong numeric information about the Sylow subgroups and we shall exploit this at many points during the course.

(iv) The final part of the theorem tells us something stronger than Lagrange's Theorem about the p-subgroups of a group G. The earlier theorem tells us that Sylow p-subgroups are the largest p-subgroups of G in terms of their order. Part (iv) of Sylow's Theorem says they are also *maximal* in terms of *containment.* To be specific, if we were to draw a diagram of the subgroups of G as suggested earlier, then the p-subgroups of G all occur as the collections of the nodes below the Sylow p-subgroups in the diagram.

This completes our brief review of group theory covered in previous modules, at least for now. Some examples of groups will need to be recalled at various points in the notes and also on the problem sheets. A few additional results will be reviewed later. In particular, results about conjugation, centralizers, etc., will appear in the context of group actions in the next chapter since that is a natural common framework to discuss these concepts.

Chapter 2

Group Actions

The purpose of this chapter is to explain what it means for a group to 'act' on a set. There are a number of reasons why this concept is significant:

(i) Group actions are the main way that group theory applies to other branches of mathematics as well as to computer science and the physical sciences.

(ii) The important branch of group theory called *geometric group theory* is primarily concerned with the study of groups acting upon geometric structures.

(iii) Group actions give us a useful set of terminology and technology for referring to the behaviour of a group. For example, if we can say that a finite group G acts on its set of Sylow p-subgroups, then all the methods and results of this section can be applied to deduce information about the original group G. This will be the main reason we shall need this technology in this course.

An action of a group G on a set Ω will be a map $\mu\colon \Omega \times G \to \Omega$ satisfying certain properties. In order to make the properties more intuitive we shall denote the image of a pair (ω, x) under μ by ω^x. The idea here is to view ω^x as the result of applying the element $x \in G$ to the point $\omega \in \Omega$.

Definition 2.1 Let G be a group and Ω be a set. A *group action* of G on Ω is a map

$$\begin{aligned} \mu\colon \Omega \times G &\to \Omega \\ (\omega, x) &\mapsto \omega^x \end{aligned}$$

such that

(i) $(\omega^x)^y = \omega^{xy}$ for all $\omega \in \Omega$ and $x, y \in G$,

(ii) $\omega^1 = \omega$ for all $\omega \in \Omega$.

We then say that G *acts* on Ω.

As we indicated when discussing the choice of notation, we shall think of an action as a method of applying the element x of the group G to points in the set Ω. Thus the first condition states that applying two elements x and y in sequence has the same effect as applying the product xy, while the second condition is the requirement that the identity element of the group produces the effect of the identity map when it is applied.

We shall spend some time developing the theory of group actions. First we present a few examples which illustrate the concept and will allow us to recall some standard groups at the same time.

Example 2.2 (i) Let $\Omega = \{1, 2, \dots, n\}$. Recall that the *symmetric group of degree n* is denoted by S_n and consists of all bijections $\sigma \colon \Omega \to \Omega$. Such a bijection is called a *permutation* of Ω and we multiply permutations in the group S_n by composing them as maps.

As a consequence of the definition, the symmetric group S_n acts on the set Ω by

$$(\omega, \sigma) \mapsto \omega^{\sigma}$$

where the right-hand side denotes the effect of applying the permutation σ to the point $\omega \in \Omega$. The fact that this is an action follows immediately:

$$(\omega^{\sigma})^{\tau} = \omega^{\sigma\tau} \qquad \text{for } \sigma, \tau \in S_n \text{ and } \omega \in \Omega,$$

since the composite $\sigma\tau$ is defined to mean first apply σ and then apply τ, while

$$\omega^1 = \omega \qquad \text{for } \omega \in \Omega,$$

since the identity permutation 1 fixes all points of Ω.

The concept of a group action can be thought of as a generalization of his example and we shall link them further when we introduce permutation representaions later in the chapter.

(ii) If a group G acts on a set Ω and H is a subgroup of G, then H acts on the same set Ω by restricting the action $\Omega \times G \to \Omega$ to the subset $\Omega \times H$. The two conditions we required are inherited immediately. In particular, if H is a subgroup of the symmetric group S_n then H also acts on $\Omega = \{1, 2, \dots, n\}$.

One specific example is the *dihedral group* of order $2n$ which is the subgroup of S_n generated by the following two permutations:

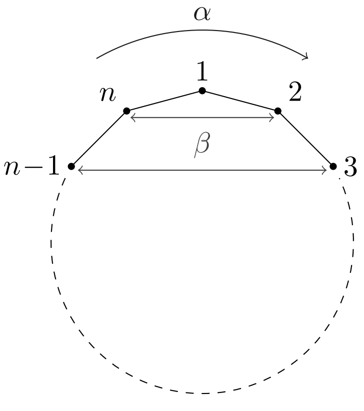
$$\begin{aligned} \alpha &= (1\ 2\ 3\ \dots\ n) \\ \beta &= \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & n & n{-}1 & \dots & 2 \end{pmatrix} \\ &= (2\ \ n)(3\ \ n{-}1)\cdots. \end{aligned}$$

We shall denote this group by D_{2n}. (The choice of notation for the dihedral group is not consistent in the literature. Some authors use D_n while others use D_{2n}. This choice to use of D_{2n} in these notes agrees with the lecturer's preferred textbooks.)

Recall these permutations have the following properties:

$$o(\alpha) = n, \qquad o(\beta) = 2, \qquad \beta\alpha = \alpha^{-1}\beta.$$

Now consider a regular polygon with n edges and vertices labelled from 1 to n:



If g is an element of D_{2n}, one determines an isometry of the above regular polygon as follows: If g moves i to j, then the associated isometry moves vertex i to vertex j. With this convention, α induces a clockwise rotation of the polygon through an angle of $2\pi/n$ while applying β produces a reflection in the axis passing through vertex 1. Since both of α and β preserve the edges between the vertices, it follows that every product of these elements also is an isometry of the polygon. We have consequently associated each element of $\Omega = \{1, 2, \dots, n\}$ to a vertex of the polygon and observed that the permutation that each element of D_{2n} produces on Ω corresponds to an isometry of the polygon.

Conclusion: The dihedral group D_{2n} acts on the vertices of a regular polygon with n sides.

(iii) Many groups arise as a collection of invertible functions defined on some set Ω. Such groups are also subgroups of the symmetric group on the set Ω and so act on the given set Ω. One specific example is the following.

Let V be a vector space of dimension n over a field F. Fix a basis $\{e_1, e_2, \dots, e_n\}$ for V. A linear transformation $T \colon V \to V$ can be represented, with respect to this basis, by an $n \times n$ matrix with entries from F and the transformation is invertible when the corresponding matrix is non-singular (i.e., has non-zero determinant). The *general linear group of degree n over F* is

$$\mathrm{GL}_n(F) = \{\, A \mid A \text{ is an } n \times n \text{ matrix over } F \text{ with } \det A \neq 0 \,\}.$$

Then $\mathrm{GL}_n(F)$ acts on V: a matrix A in $\mathrm{GL}_n(F)$ moves the vector v (from V) according to the linear transformation determined by A. It follows from the definition of matrix multiplication that

$$(vA)B = v(AB) \qquad \text{for all } v \in V \text{ and } A, B \in \mathrm{GL}_n(F)$$

and

$$vI = v \qquad \text{for all } v \in V.$$

These examples above illustrate how group actions arise in a variety of natural settings. We shall also find lots of examples occurring where a groups acts on something related to its own structure. Before we move on to these types of examples, we shall first develop the theory of group actions.

Orbits

Definition 2.3 Let G be a group, Ω be a set and let G act on Ω. If $\omega \in \Omega$, the *orbit* containing ω is defined to be the set

$$\omega^G = \{\, \omega^x \mid x \in G \,\}.$$

Thus, the orbit containing ω consists of all the points of Ω that can be reached by applying elements of the group G to ω. The basic properties of orbits are as follows.

Proposition 2.4 *Let G be a group, Ω be a set and let G act on Ω. Let $\omega, \omega' \in \Omega$. Then*

(i) $\omega \in \omega^G$;

(ii) *either* $\omega^G = (\omega')^G$ *or* $\omega^G \cap (\omega')^G = \varnothing$.

Thus part (ii) asserts that any two orbits are either disjoint or are equal. The proposition then yields:

Corollary 2.5 *Let the group G act on the set Ω. Then Ω is the disjoint union of its orbits.* □

There are some similarities here to the observation that says a group is the disjoint union of the cosets of a subgroup. Indeed, the fact that a group is the disjoint union of the cosets of a subgroup can be deduced using group actions (see Problem Sheet II). One difference here is that, in general, it is not necessarily the case that all the orbits have the same size.

PROOF OF PROPOSITION 2.4: (i) By definition $\omega = \omega^1$, so $\omega \in \omega^G$.

(ii) Suppose $\alpha \in \omega^G \cap (\omega')^G$. Hence there exist $x, y \in G$ such that $\alpha = \omega^x = (\omega')^y$. Apply y^{-1}:

$$\omega^{xy^{-1}} = (\omega^x)^{y^{-1}} = ((\omega')^y)^{y^{-1}} = (\omega')^{yy^{-1}} = (\omega')^1 = \omega'.$$

Now, for $g \in G$,

$$(\omega')^g = (\omega^{xy^{-1}})^g = \omega^{xy^{-1}g} \in \omega^G$$

and we deduce $(\omega')^G \subseteq \omega^G$.

Similarly from $(\omega')^y = \omega^x$, we deduce $(\omega')^{yx^{-1}} = \omega$ and hence

$$\omega^g = (\omega')^{yx^{-1}g} \qquad \text{for all } g \in G.$$

This shows $\omega^G \subseteq (\omega')^G$.

Hence if $\omega^G \cap (\omega')^G \neq \varnothing$, then $\omega^G = (\omega')^G$. □

Definition 2.6 We say that a group G acts *transitively* on a set Ω if it has precisely one orbit for its action.

Thus G acts transitively on Ω if for all $\omega, \omega' \in \Omega$ there exists $x \in G$ such that $\omega' = \omega^x$.

Examples:

(i) The symmetric group S_n acts transitively on $\Omega = \{1, 2, \dots, n\}$: if $i, j \in \Omega$ are distinct then $(i\ j)$ moves i to j and so these points lie in the same orbit.

(ii) The dihedral group D_{2n} also acts on $\Omega = \{1, 2, \dots, n\}$: if $i < j$, then the rotation α^{j-i} moves the vertex i to the vertex j and so the corresponding points like in the same orbit.

(iii) The general linear group $\mathrm{GL}_n(F)$ has two orbits on V: every linear map fixes the zero vector $\mathbf{0}$ and so $\{\mathbf{0}\}$ is an orbit. If v and w are non-zero vectors, then each can be extended to a basis and hence we can specify an invertible linear map that moves v to w. Hence $V \setminus \{\mathbf{0}\}$ is an orbit for $\mathrm{GL}_n(F)$.

Stabilizers

Definition 2.7 Let G be a group that acts on the set Ω. If $\omega \in \Omega$, then the *stabilizer* of ω in G is defined to be the following subset of G:

$$G_\omega = \{\, x \in G \mid \omega^x = \omega \,\}$$

Thus the stabilizer of ω is the set of all elements from G that fix ω.

Example: Let $G = S_n$, the symmetric group of degree n in its natural action on the set $\Omega = \{1, 2, \dots, n\}$ as in Example 2.2(i). If $\omega \in \Omega$, then an element of G_ω fixes the point ω and can permute the remaining $n-1$ points of Ω in any way that one chooses. Hence the stabilizer G_ω is a copy of the symmetric group S_{n-1} of degree $n-1$ (and when $\omega = n$, it is the natural copy of S_{n-1} inside S_n).

Lemma 2.8 *Let G be a group that acts on Ω and $\omega \in \Omega$. The stabilizer G_ω of ω is a subgroup of G.*

Proof: We check the conditions to be a subgroup. First $\omega^1 = \omega$, since we have an action, so $1 \in G_\omega$. In particular, the stabilizer G_ω is non-empty. Suppose $x, y \in G_\omega$. Then

$$\omega^{xy} = (\omega^x)^y = \omega^y = \omega$$

so $xy \in G_\omega$, while

$$\omega^{x^{-1}} = (\omega^x)^{x^{-1}} = \omega^{xx^{-1}} = \omega^1 = \omega$$

so $x^{-1} \in G_\omega$. Hence G_ω is a subgroup of G. □

The crucial reason why stabilizers help us is the following theorem:

Theorem 2.9 (Orbit-Stabilizer Theorem) *Let G be a group, Ω be a set and let G act on Ω. If $\omega \in \Omega$, then*

$$|\omega^G| = |G : G_\omega|.$$

Thus the 'length' (or size) of an orbit equals the index of the corresponding stabilizer.

Proof: We demonstrate the existence of a bijection from the set of cosets of the stabilizer G_ω to the orbit of ω. Define

$$\phi \colon G_\omega x \mapsto \omega^x.$$

We first check that this is well-defined. Suppose $G_\omega x = G_\omega y$ for some x and y. Then $xy^{-1} \in G_\omega$, so

$$\omega^{xy^{-1}} = \omega.$$

Apply y:

$$\omega^{xy^{-1}y} = \omega^y.$$

Therefore

$$\omega^x = \omega^y.$$

Hence ϕ is well-defined.

Suppose $x, y \in G$ and that $(G_\omega x)\phi = (G_\omega y)\phi$; that is,

$$\omega^x = \omega^y.$$

Therefore, upon applying y^{-1},

$$\omega^{xy^{-1}} = \omega^{yy^{-1}} = \omega^1 = \omega,$$

so $xy^{-1} \in G_\omega$ and we deduce $G_\omega x = G_\omega y$. Thus ϕ is injective.

Finally by definition the image of ϕ is the orbit of ω.

Hence $\phi \colon G_\omega x \mapsto \omega^x$ does define a bijection from the set of cosets of G_ω to the orbit of ω and we conclude

$$|\omega^G| = |G : G_\omega|.$$

□

We can make further observations about stabilizers. Indeed, suppose that a group G acts on the set Ω and that ω and ω' are two points that lie in the same orbit. We know that orbits are either disjoint or equal, so

$$\omega^G = (\omega')^G.$$

Hence, by the Orbit-Stabilizer Theorem,

$$|G : G_\omega| = |G : G_{\omega'}|.$$

In particular, if G is a finite group, we can now deduce already that $|G_\omega| = |G_{\omega'}|$. In fact, we can observe not only that this is true in general but far much more holds as the following result shows.

Proposition 2.10 *Let G be a group, Ω be a set and let G act on Ω. If two points ω and ω' lie in the same orbit of G on Ω, then the stabilizers G_ω and $G_{\omega'}$ are conjugate in G. Indeed, if $\omega' = \omega^x$ for $x \in G$, then*

$$G_{\omega'} = (G_\omega)^x = x^{-1} G_\omega x. \tag{2.1}$$

Proof: Since ω and ω' lie in the same orbit, there does indeed exist some $x \in G$ such that $\omega' = \omega^x$. To verify that the two stabilizers are conjugate in G, we shall establish Equation (2.1).

Let $g \in G_\omega$, so that $x^{-1}gx \in (G_\omega)^x$. Then

$$\begin{aligned}
(\omega')^{x^{-1}gx} &= (\omega^x)^{x^{-1}gx} \\
&= \omega^{xx^{-1}gx} \\
&= \omega^{gx} \\
&= \omega^x && \text{(as } g \in G_\omega) \\
&= \omega'.
\end{aligned}$$

Hence $x^{-1}gx \in G_{\omega'}$; that is, $(G_\omega)^x \subseteq G_{\omega'}$.

For the reverse inclusion, note first that from $\omega' = \omega^x$, we deduce $(\omega')^{x^{-1}} = \omega^{xx^{-1}} = \omega$, so applying the inclusion that we have already established above yields

$$(G_{\omega'})^{x^{-1}} \subseteq G_\omega;$$

that is,

$$x G_{\omega'} x^{-1} \subseteq G_\omega.$$

Multiply on the left by x^{-1} and on the right by x:

$$G_{\omega'} \subseteq x^{-1} G_\omega x = (G_\omega)^x.$$

Thus $G_{\omega'} = (G_\omega)^x$, as required. □

We shall continue to further develop the theory of group actions later, but we shall first consider a couple of examples which illustrate how we can apply this theory to the study of groups.

Conjugation

Example 2.11 (Conjugation Action) Let G be a group and attempt to define an action of G on itself by

$$\begin{aligned} G \times G &\to G \\ (g, x) &\mapsto x^{-1}gx = g^x, \end{aligned}$$

the *conjugate* of g by x. We need to check the conditions to be a group action:

(i) $(g^x)^y = y^{-1}(x^{-1}gx)y = y^{-1}x^{-1}gxy = (xy)^{-1}g(xy) = g^{xy}$ for all $g, x, y \in G$;

(ii) $g^1 = 1^{-1}g1 = 1g1 = g$ for all $g \in G$.

Thus we have a genuine action of G on itself. We should therefore consider the orbits and stabilizers for this action.

If $g \in G$, the orbit of G containing g (for this conjugation action) is

$$g^G = \{\, g^x \mid x \in G \,\} = \{\, x^{-1}gx \mid x \in G \,\},$$

the set of all conjugates of g. This is the *conjugacy class* of g in G.

The stabilizer of g under this action is

$$\begin{aligned} G_g &= \{\, x \in G \mid g^x = g \,\} \\ &= \{\, x \in G \mid x^{-1}gx = g \,\} \\ &= \{\, x \in G \mid gx = xg \,\}; \end{aligned}$$

i.e., with this particular action, the stabilizer of g consists of the set of elements of G which commute with g. We use the following term to refer to this specific example of a stabilizer for this particular action.

Definition 2.12 If G is a group and g is an element of G, the *centralizer* of g (in G) is

$$\mathrm{C}_G(g) = \{\, x \in G \mid gx = xg \,\}.$$

We may now apply the standard facts about group actions to make deductions about conjugation in a group. The result that we now give probably appeared in the module *MT4003*, but with a proof that was directly focused upon conjugation. By placing conjugation in the context of group actions, we can deduce what we want immediately from the theory just developed.

Proposition 2.13 *Let G be a group. Then*

(i) *G is the disjoint union of its conjugacy classes;*

(ii) *the centralizer of an element g is a subgroup of G;*

(iii) *the number of conjugates of an element g equals the index of its centralizer;*

(iv) *if $g, x \in G$ then*

$$\mathrm{C}_G(g^x) = \mathrm{C}_G(g)^x.$$

Proof: (i) Immediate from Corollary 2.5: a set is the disjoint union of the orbits in a group action.

(ii) Immediate from Lemma 2.8: a stabilizer is a subgroup.

(iii) Immediate from the Orbit-Stabilizer Theorem (Theorem 2.9: the length of an orbit equals the index of the corresponding stabilizer.

(iv) The fact that the centralizer of a conjugate of g is a conjugate of the centralizer of g is immediate from Proposition 2.10 (and specifically Equation 2.1). □

Conjugation on subgroups

Example 2.14 (Conjugation action on subsets and subgroups)
Let G be a group and let $\mathscr{P}(G)$ denote the set of all subsets of G (the *power set* of G). We define an action of G on $\mathscr{P}(G)$ by

$$\begin{aligned} \mathscr{P}(G) \times G &\to \mathscr{P}(G) \\ (A, x) &\mapsto A^x = x^{-1}Ax = \{\, x^{-1}ax \mid a \in A \,\}. \end{aligned}$$

A similar argument to Example 2.11 checks that this is indeed an action (this basically only relies on associativity of the group multiplication and the formula for the inverse of a product of two elements). The orbit containing the subset A is the set of all conjugates of A and the stabilizer is the so-called 'normalizer' of A:

Definition 2.15 If G is a group and A is a subset of G, the *normalizer* of A in G is

$$\mathrm{N}_G(A) = \{\, x \in G \mid A^x = A \,\}.$$

Since this is a stabilizer, it is always a subgroup of G (by Lemma 2.8). We shall be most interested in the case when we conjugate subgroups and here we make use of what we know about conjugation from Chapter 1. We know that the conjugation map $\tau_x \colon g \mapsto g^x = x^{-1}gx$ is an automorphism of the group G. (We called such an *inner automorphism* of the group.) As a consequence, it maps subgroups to subgroups and hence the conjugate H^x of a subgroup H is another subgroup. This tells us that the orbit of H under the conjugation action consists of subgroups of G that all are isomorphic to the original subgroup H.

We summarize information about conjugation of subgroups in the following observation.

Proposition 2.16 *Let G be a group and H be a subgroup of G.*

(i) *The normalizer $\mathrm{N}_G(H)$ of H in G is a subgroup of G.*

(ii) *The conjugates of H are subgroups of G that are isomorphic to H.*

(iii) *The number of conjugates of H in G is equal to the index $|G : \mathrm{N}_G(H)|$ of the normalizer in G.* □

In particular, if we consider conjugation of Sylow subgroups of a finite group G, some of what Sylow's Theorem tells us is that, for a given prime p, the Sylow p-subgroups form a single orbit under the conjugation action of G on its subgroups.

On the topic of Sylow's Theorem, we mention that the theorem can be proved in the language of group actions. Indeed, much of the proof that I used to present of parts (ii)–(iv) of Theorem 1.31 when I taught *MT4003* was essentially that but with the language of group actions stripped out. Even when phrased in terms of group actions, the proof is still quite long and so not worth doing again when there is plenty more group theory to be studied. Questions that guide you through the proof of Sylow's Theorem based on group actions appear on Problem Sheet II.

Permutation representations

We have already seen that with a group action certain subgroups, the stabilizers, are of particular significance. In particular, the Orbit-Stabilizer Theorem says there is a strong link between the orbits in the action and the indices of these subgroups. We now bring another part of group theory into the context of group actions. We shall construct a homomorphism associated to the group action. The image of the homomorphism lies within a symmetric group, so we recall the definition of the latter group.

Definition 2.17 Let Ω be any set. A *permutation* of Ω is a bijection $\sigma\colon \Omega \to \Omega$. The set of all permutations of Ω is called the *symmetric group on* Ω and is denoted by $\mathrm{Sym}(\Omega)$. It forms a group under composition of maps:

$$\omega\sigma\tau = (\omega\sigma)\tau$$

for $\omega \in \Omega$ and $\sigma, \tau \in \mathrm{Sym}(\Omega)$.

Associativity is immediately checked. The identity element in $\mathrm{Sym}(\Omega)$ is the identity map, which we shall denote by 1 (provided this will not cause confusion) in what follows. All permutations possess inverses since they are bijective and so we conclude that $\mathrm{Sym}(\Omega)$ is indeed a group. We recover our friend the symmetric group S_n by simply considering the special case when $\Omega = \{1, 2, \dots, n\}$.

Now let G be a group, Ω be a set and let G act on Ω. If $x \in G$, then we induce a map from Ω to itself by

$$\begin{aligned} \rho_x \colon \Omega &\to \Omega \\ \omega &\mapsto \omega^x. \end{aligned}$$

Now

$$\omega\rho_x\rho_{x^{-1}} = (\omega^x)^{x^{-1}} = \omega^{xx^{-1}} = \omega^1 = \omega$$

and

$$\omega\rho_{x^{-1}}\rho_x = (\omega^{x^{-1}})^x = \omega^{x^{-1}x} = \omega^1 = \omega.$$

Hence $\rho_x\rho_{x^{-1}} = \rho_{x^{-1}}\rho_x = 1$ (the identity map $\Omega \to \Omega$), so ρ_x is a bijection and therefore

$$\rho_x \in \mathrm{Sym}(\Omega) \qquad \text{for all } x \in G.$$

Consequently, to each element of G we associate a permutation of Ω. (Note that it is in general just a bijective function: Ω is merely a set and does not necessarily have any group structure.) We therefore determine a map

$$\begin{aligned} \rho \colon G &\to \mathrm{Sym}(\Omega) \\ x &\mapsto \rho_x. \end{aligned}$$

Now

$$\omega\rho_x\rho_y = (\omega^x)^y = \omega^{xy} = \omega\rho_{xy}$$

for all $\omega \in \Omega$ and $x, y \in G$, so

$$\rho_x \rho_y = \rho_{xy} \qquad \text{for all } x, y \in G.$$

Thus

$$(x\rho)(y\rho) = (xy)\rho \qquad \text{for all } x, y \in G;$$

i.e., ρ is a homomorphism. We record this as follows.

Theorem 2.18 *Let G be a group, Ω be a set and let G act on Ω. For each $x \in G$, the map*

$$\rho_x \colon \omega \mapsto \omega^x \qquad \text{(for } \omega \in \Omega\text{)}$$

is a permutation of Ω. The map

$$\begin{aligned} \rho \colon G &\to \mathrm{Sym}(\Omega) \\ x &\mapsto \rho_x \end{aligned}$$

is a homomorphism. □

We refer to the homomorphism ρ as a *permutation representation* of G. The kernel of ρ is often called the *kernel of the action*. This kernel consists of the elements x of G such that

$$\omega^x = \omega \qquad \text{for all } \omega \in \Omega;$$

i.e., the elements of G which fix *all* points in Ω. Consequently, $x \in \ker\rho$ if and only if x belongs to every stabilizer G_ω (for all $\omega \in \Omega$). Consequently:

Lemma 2.19 *Let G be a group, Ω be a set and let G act on Ω. If $\rho \colon G \to \mathrm{Sym}(\Omega)$ is the permutation representation associated to this action, then*

$$\ker\rho = \bigcap_{\omega\in\Omega} G_\omega$$

(the intersection of all stabilizers). □

Using the permutation representation associated to the following example of a group action will enable us to establish a theorem that was also covered in *MT4003*.

Example 2.20 (Right Regular Action) Let G be a group and attempt to define an action of G on itself by

$$\begin{aligned} G \times G &\to G \\ (g, x) &\mapsto gx. \end{aligned}$$

We check the conditions of a group action:

(i) $(gx)y = g(xy)$ for all $g, x, y \in G$ (by associativity),

(ii) $g1 = g$ for all $g \in G$.

So we do indeed have a group action: this is called the *right regular action* of G (on itself by right multiplication).

Observe that $x \in G$ fixes a point $g \in G$ in this action when $gx = g$; that is, if and only if $x = 1$ (by multiplying by the inverse of g). Hence all stabilizers are trivial:

$$G_g = \mathbf{1} \qquad \text{for all } g \in G.$$

Theorem 2.18 provides us with a homomorphism $\rho \colon G \to \mathrm{Sym}(G)$ and Lemma 2.19 now tells us that the kernel is trivial:

$$\ker \rho = \bigcap_{g \in G} G_g = \mathbf{1}.$$

Hence ρ is one-one and it follows that G is isomorphic to $\operatorname{im} \rho$ and we have proved Cayley's Theorem. (This result was also originally established in *MT4003*, but we have deduced it immediately from the technology we have developed concerning group actions.)

Theorem 2.21 (Cayley's Theorem) *Every group is isomorphic to a subgroup of a symmetric group.* □

Our final general example is extremely important: it will occur throughout the course. We shall observe that if we can find a subgroup H of a group G then we can define an action on the cosets of H and hence produce the associated permutation representation.

Example 2.22 (Action on Cosets) Let G be a group and H be a subgroup of G. Let $\Omega = \{\, Hg \mid g \in G \,\}$, the set of cosets of H in G. We shall define an action of G on Ω as follows:

$$\begin{gathered} \Omega \times G \to \Omega \\ (Hg, x) \mapsto Hgx. \end{gathered}$$

The first thing to do is check that this is well-defined, that is, the image of a coset Hg when we apply an element x of G does not depend upon the choice of representative g for the coset. Let $g, h, x \in G$ and suppose that $Hg = Hh$. Then $gh^{-1} \in H$. Now

$$(gx)(hx)^{-1} = gxx^{-1}h^{-1} = gh^{-1} \in H$$

and therefore $Hgx = Hhx$. Hence the action is well-defined. We shall write $Hg \cdot x$ to denote this action in what follows.

It is now straightforward to check that this is a group action:

$$(Hg \cdot x) \cdot y = Hgx \cdot y = Hgxy = Hg \cdot xy$$

and

$$Hg \cdot 1 = Hg1 = Hg$$

for all $g, x, y \in G$.

We shall now establish the main properties of this action on cosets:

Theorem 2.23 *Let H be a subgroup of a group G, let $\Omega = \{\, Hg \mid g \in G \,\}$ be the set of cosets of H, and let G act on Ω by right multiplication. Let $\rho \colon G \to \mathrm{Sym}(\Omega)$ be the permutation representation associated to the action. Then*

(i) *the action of G on Ω is transitive;*

(ii) *if H is a proper subgroup of G (that is, if $H \neq G$), then $G\rho$ is a non-trivial subgroup of* $\mathrm{Sym}(\Omega)$*;*

(iii) *the kernel of ρ is the intersection of the conjugates of H:*

$$\ker \rho = \bigcap_{g \in G} H^g;$$

(iv) *the kernel of ρ is the largest normal subgroup of G contained in H.*

Definition 2.24 We call this intersection $\bigcap_{g\in G} H^g$ (occurring as the kernel here) the *core* of H in G and shall denote it by $\mathrm{Core}_G(H)$.

Proof: (i) Consider two cosets Hg and Hh in Ω. Take $x = g^{-1}h$. Then

$$Hg \cdot x = Hgx = Hgg^{-1}h = Hh.$$

This shows that Hg and Hh lie in the same orbit. Hence G acts transitively on Ω.

(ii) Suppose $H \neq G$. Then Ω contains more than one coset: $|\Omega| > 1$. Since G acts transitively, it must induce at least one non-trivial permutation on Ω and so $G\rho \neq \mathbf{1}$.

(iii) We shall first compute the stabilizer of each coset Hg:

$$\begin{aligned} G_{Hg} &= \{\, x \in G \mid Hg \cdot x = Hg \,\} \\ &= \{\, x \in G \mid Hgx = Hg \,\} \\ &= \{\, x \in G \mid gxg^{-1} \in H \,\} \\ &= \{\, x \in G \mid x \in g^{-1}Hg \,\} = H^g. \end{aligned}$$

The kernel of ρ is then determined by Lemma 2.19:

$$\ker \rho = \bigcap_{g\in G} G_{Hg} = \bigcap_{g\in G} H^g.$$

(iv) Certainly $\ker \rho$ is a normal subgroup of G (since kernels are always normal subgroups). By the previous part,

$$\ker \rho = \bigcap_{g\in G} H^g \leqslant H^1 = H.$$

On the other hand, if K is any normal subgroup of G that is contained in H then $K = K^g \leqslant H^g$ for all $g \in G$. Hence

$$K \leqslant \bigcap_{g\in G} H^g = \ker \rho.$$

□

Applications

To illustrate the significance of the action on the cosets, we shall give some examples of how this can be used to establish information about finite simple groups. We start by recalling the term that was introduced in *MT4003*:

Definition 2.25 A non-trivial group G is *simple* if the only normal subgroups it has are $\mathbf{1}$ and G.

The idea here is that if G is *not* simple then it has a non-trivial proper normal subgroup N and we can break it down into two smaller groups N and G/N which are hopefully easier to handle than G. On the other hand, when G is simple this process yields nothing new: one of these groups is trivial and the other is just a copy of G. As a consequence, simple groups are the minimal building blocks (analogous, in some sense, to primes in number theory) from which all other (finite) groups are built. One of the things we shall discuss in the next chapter is how we can describe the factorization of a (finite) group into simple factors and to what extent this factorization is unique. Chapter 4 will give some descriptions of how the simple factors might be put back together, but we shall only start to describe what is a somewhat complicated topic.

To start we shall give one example of the use of the methods of *MT4003* (i.e., the following does not use group actions):

Example 2.26 *Show that there is no simple group of order* 858*.*

Solution: Let G be a group of order $858 = 2 \cdot 3 \cdot 11 \cdot 13$. Let n_{11} and n_{13} denote the number of Sylow 11- and Sylow 13-subgroups of G, respectively. By Sylow's Theorem,

$$\begin{aligned} n_{11} &\equiv 1 \pmod{11} \qquad \text{and} \qquad n_{11} \mid 78 \\ n_{13} &\equiv 1 \pmod{13} \qquad \text{and} \qquad n_{13} \mid 66. \end{aligned}$$

If $n_{11} = 1$, then the unique Sylow 11-subgroup of G would be normal in G and hence G would not be simple. Similarly if $n_{13} = 1$.

Suppose that $n_{11} = 78$. Consider two distinct Sylow 11-subgroups E_1 and E_2 of G. Then $|E_1| = |E_2| = 11$. The intersection $E_1 \cap E_2$ is a proper subgroup of E_1, so $|E_1 \cap E_2|$ divides 11, by Lagrange's Theorem. Hence $E_1 \cap E_2 = \mathbf{1}$. It follows that each Sylow 11-subgroup of G contains 10 non-identity elements (all of order 11) and these are contained in no other Sylow 11-subgroup of G. Hence the Sylow 11-subgroups account for

$$78 \times 10 = 780 \text{ elements of order } 11.$$

By exactly the same argument, if $n_{13} = 66$ then the Sylow 13-subgroups contain $66 \times 12 = 792$ elements of order 13.

Since $780 + 792 > |G|$, it must be the case that either $n_{11} = 1$ or $n_{13} = 1$. So G either has a normal subgroup of order 13 or a normal subgroup of order 11. Hence G is not simple. □

Let us now see how the use of group actions can help with this sort of problem.

Example 2.27 *Show that there is no simple group of order* 36*.*

Solution: Let H be a Sylow 3-subgroup of G. Then $|G : H| = 4$. Let G act on the set of right cosets of H by right multiplication,

$$(Hx, g) \mapsto Hxg,$$

and let $\rho\colon G \to S_4$ be the associated permutation representation. Since $|G| = 36 \geqslant |S_4| = 24$, it is certainly the case that $\ker\rho \neq \mathbf{1}$. On the other hand, Theorem 2.23(ii) tells us that $\ker\rho \neq G$ (because $G\rho \neq \mathbf{1}$). It follows that $\ker\rho$ is a non-trivial proper normal subgroup of G and hence G is not simple. □

Proposition 2.28 *Let p and q be distinct primes and let G be a finite group of order p^2q. Then one of the following holds:*

(i) *$p > q$ and G has a normal Sylow p-subgroup;*

(ii) *$q > p$ and G has a normal Sylow q-subgroup;*

(iii) *$p = 2$, $q = 3$, $G \cong A_4$ and G has a normal Sylow 2-subgroup.*

Proof: (i) Suppose $p > q$. Let n_p denote the number of Sylow p-subgroups of G. Then

$$n_p \equiv 1 \pmod p \qquad \text{and} \qquad n_p \mid q.$$

The latter forces $n_p = 1$ or q. But $1 < q < p + 1$, so $q \not\equiv 1 \pmod p$. Hence $n_p = 1$, so G has a unique Sylow p-subgroup which must be normal.

(ii) and (iii): Suppose $q > p$. Let n_q be the number of Sylow q-subgroups of G. If $n_q = 1$ then the unique Sylow q-subgroup of G would be normal in G (and Case (ii) would hold). So suppose that $n_q \neq 1$ (and we shall endeavour to show Case (iii) holds). Now

$$n_q \equiv 1 \pmod q \qquad \text{and} \qquad n_q \mid p^2.$$

So $n_q = p$ or p^2. But $1 < p < q + 1$, so $p \not\equiv 1 \pmod q$. Hence $n_q = p^2$, so

$$p^2 \equiv 1 \pmod q;$$

that is,

$$q \text{ divides } p^2 - 1 = (p + 1)(p - 1).$$

But q is prime, so either q divides $p - 1$ or it divides $p + 1$. However, $1 \leqslant p - 1 < q$, so the only one of these possibilities is that q divides $p + 1$. However $p < q$, so $p + 1 \leqslant q$ so we are forced into the situation where $p + 1 = q$. Hence

$$p = 2, \qquad q = 3$$

and

$$|G| = 2^2 \cdot 3 = 12.$$

Let T be a Sylow 3-subgroup of G $(q = 3)$ and let G act on the set of right cosets of T by right multiplication. This gives rise to the permutation representation

$$\rho\colon G \to S_4$$

(as $|G : T| = 4$, so we are acting on four points). Theorem 2.23 tells us that the kernel of ρ is contained in T, while it must be a proper subgroup of T as $T \ntrianglelefteq G$. Since $|T| = 3$, this forces $\ker \rho = \mathbf{1}$, so ρ is injective. Hence

$$G \cong \operatorname{im} \rho.$$

Now $\operatorname{im} \rho$ is a subgroup of S_4 of order 12 and therefore index 2. We deduce that $\operatorname{im} \rho = A_4$ and so $G \cong A_4$.

Finally

$$V_4 = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

is a subgroup of A_4 that is isomorphic to the Klein 4-group (hence our choice of notation V_4 for it). This is a Sylow 2-subgroup of A_4 and $V_4 \trianglelefteq S_4$ (and hence $V_4 \trianglelefteq A_4$). Therefore G has a normal Sylow 2-subgroup in this case. □

It is worth pointing out that at this point in time much is actually now known about finite simple groups. A mammoth effort by a large collection of mathematicians from the 1950s to the 1980s succeeded in establishing a full classification. The complete proof runs to tens of thousands of pages of extremely complicated mathematics and there has been doubt as to what extent this is truly complete. More work is still currently being done so as to check, clarify and simplify the proof. Nevertheless it is generally accepted that this Classification is correct, though typically when relying upon it a mathematician would normally state that they are doing so.

Theorem 2.29 (Classification of Finite Simple Groups) *Let G be a finite simple group. Then G is one of the following:*

(i) *a cyclic group of prime order;*

(ii) *an alternating group A_n where $n \geqslant 5$;*

(iii) *one of sixteen (infinite) families of groups of Lie type;*

(iv) *one of twenty-six sporadic simple groups.*

The fact that cyclic groups of prime order are simple is already known: it follows immediately from Lagrange's Theorem. The proof that the alternating groups of degree at least 5 are simple is more lengthy, but was one of the highlights of *MT4003*.

The groups of Lie type are essentially 'matrix-like' groups which preserve geometric structures on vector spaces over finite fields. For example, the first (and most easily described) family is the collection of groups $\mathrm{A}_n(q)$ where n is a positive integer and q is a prime-power (and where we require $q \geqslant 4$ if $n = 1$). The definition of this family is

$$\mathrm{A}_n(q) = \mathrm{PSL}_{n+1}(q) = \frac{\mathrm{SL}_{n+1}(q)}{\mathrm{Z}(\mathrm{SL}_{n+1}(q))}.$$

That is, we successively construct the group $\mathrm{GL}_{n+1}(q)$ of invertible $(n+1)\times(n+1)$ matrices with entries from the field $\mathbb{F}_q$ of q elements; then take those of determinant 1

$$\mathrm{SL}_{n+1}(q) = \{\, A \in \mathrm{GL}_{n+1}(q) \mid \det A = 1 \,\}$$

(the *special linear group*); then factor out the centre (which happens to consist of all scalar matrices in $\mathrm{SL}_{n+1}(q)$)

$$\mathrm{Z}(\mathrm{SL}_{n+1}(q)) = \{\, \lambda I \mid \lambda^{n+1} = 1 \text{ in } \mathbb{F}_q \,\},$$

Mathieu	M_{11}	7 920
Mathieu	M_{12}	95 040
Janko	J_1	175 560
Mathieu	M_{22}	443 520
Janko	J_2	604 800
Mathieu	M_{23}	10 200 960
Higman–Sims	HS	44 352 000
Janko	J_3	50 232 960
Mathieu	M_{24}	244 823 040
McLaughlin	McL	898 128 000
Held	He	4 030 387 200
Rudvalis	Ru	145 926 144 000
Suzuki	Suz	448 345 497 600
O'Nan	O'N	460 815 505 920
Conway	Co_3	495 766 656 000
Conway	Co_2	42 305 421 312 000
Fischer	Fi_{22}	64 561 751 654 400
Harada–Norton	HN	273 030 912 000 000
Lyons	Ly	51 765 179 004 000 000
Thompson	Th	90 745 943 887 872 000
Fischer	Fi_{23}	4 089 470 473 293 004 800
Conway	Co_1	4 157 776 806 543 360 000
Janko	J_4	86 775 571 046 077 562 880
Fischer	Fi_{24}'	1 255 205 709 190 661 721 292 800
Baby Monster	B	4 154 781 481 226 426 191 177 580 544 000 000
Monster	M	see text

Table 2.1: The sporadic simple groups

to form

$$\mathrm{PSL}_{n+1}(q) = \mathrm{SL}_{n+1}(q)/\mathrm{Z}(\mathrm{SL}_{n+1}(q))$$

and we have constructed a simple group (provided either $n \geqslant 2$, or $n = 1$ and $q \geqslant 4$).

The twenty-six sporadic groups are as listed in Table 2.1. The order of the Monster is too large to appear in the table, it is

$$|\mathrm{M}| = 808\,017\,424\,794\,512\,875\,886\,459\,904\,961\,710\,757\,005\,754\,368\,000\,000\,000$$

It will not surprise anyone that the proof of Theorem 2.29 is not included in these notes!

Chapter 3

Composition Series, Chief Series and the Jordan–Hölder Theorem

We begin this chapter with the following general definition.

Definition 3.1 Let G be a group. A *series* for G is a finite chain of subgroups

$$G = G_0 > G_1 > G_2 > \cdots > G_n = \mathbf{1}$$

such that G_{i+1} is a normal subgroup of G_i for $i = 0, 1, \ldots, n-1$. The collection of quotient groups

$$G_0/G_1, \quad G_1/G_2, \quad \ldots, \quad G_{n-1}/G_n$$

are called the *factors* of the series and we call the number n the *length* of the series.

Some authors refer to this as a *subnormal series* (coming from the fact that a subgroup that is normal in a normal subgroup of . . . of a normal subgroup is often called *subnormal*). In particular, we do not require each subgroup in the series to be normal in the whole group G, only that it is normal in the previous subgroup in the chain. However, the following term is used for a stronger situation:

Definition 3.2 Let G be a group. A *normal series* for G is a series

$$G = G_0 > G_1 > G_2 > \cdots > G_n = \mathbf{1}$$

such that G_i is a normal subgroup of G for every $i = 0, 1, \ldots, n$.

Observe that in each case the length n is the number of factors that occur in the series.

The first definition is rather general and does not give much information on its own. Indeed, one example of a (normal) series of a non-trivial group G is simply of length 1, namely

$$G > \mathbf{1},$$

with factor isomorphic to G. To actually obtain useful and interesting information about the group, we need stronger conditions on the nature of the series we are considering. There will be several examples of series occurring in this course and this chapter will consider two specific types of series. The first case is the following where the factors are all required to be simple groups.

Composition series

Definition 3.3 A *composition series* for a group G is a finite chain of subgroups

$$G = G_0 > G_1 > G_2 > \cdots > G_n = \mathbf{1}$$

such that, for $i = 0, 1, \ldots, n-1$, G_{i+1} is a normal subgroup of G_i and the quotient group G_i/G_{i+1} is simple. In this case, the factors

$$G_0/G_1, \quad G_1/G_2, \quad \ldots, \quad G_{n-1}/G_n$$

are called the *composition factors* of G.

The idea here is that if G possesses a composition series, then the composition factors are a collection of simple groups that arise as some sort of factorization of G. One of the main goals of this chapter is to establish the following theorem that says that these factors are uniquely determined.

Theorem 3.4 (Jordan–Hölder Theorem) *Let G be a group and let*

$$G = G_0 > G_1 > G_2 > \cdots > G_m = \mathbf{1}$$

and

$$G = H_0 > H_1 > H_2 > \cdots > H_n = \mathbf{1}$$

be composition series for G. Then $m = n$ and there is a one-one correspondence between the two collections of composition factors

$$G_0/G_1, \quad G_1/G_2, \quad \ldots, \quad G_{m-1}/G_m$$

and

$$H_0/H_1, \quad H_1/H_2, \quad \ldots, \quad H_{n-1}/H_n$$

such that the corresponding factors are isomorphic.

We shall delay the proof of the theorem until later in the chapter. At this stage, it is illustrative to consider some examples and to examine what the condition for a factor in a series to be simple actually means.

Example 3.5 (i) The trivial group $\mathbf{1}$ has composition series of length 0:

$$G_0 = \mathbf{1}$$

and so has no composition factors. This example is included just to point out what a series of length zero looks like!

(ii) Let $G = S_4$, the symmetric group of degree 4. Then we can construct the following chain of subgroups:

$$S_4 > A_4 > V_4 > \langle (1\ 2)(3\ 4) \rangle > \mathbf{1}. \tag{3.1}$$

We know that $A_4 \trianglelefteq S_4$ with quotient $S_4/A_4 \cong C_2$ and that $V_4 \trianglelefteq A_4$ with quotient $A_4/V_4 \cong C_3$. Since V_4 is abelian, each of its subgroups is normal. Finally

$$V_4/\langle (1\ 2)(3\ 4) \rangle \cong C_2 \qquad \text{and} \qquad \langle (1\ 2)(3\ 4) \rangle \cong C_2.$$

This shows that the chain (3.1) is a composition series for S_4 and that the composition factors of S_4 (which are unique up to isomorphism by the Jordan–Hölder Theorem) are

$$C_2,\ C_3,\ C_2,\ C_2$$

(all of which are indeed simple groups as they are cyclic of prime order).

(iii) Let $n \geqslant 5$ and consider the symmetric group S_n of degree n. Then

$$S_n > A_n > \mathbf{1} \tag{3.2}$$

is a composition series for S_n with composition factors isomorphic to C_2 and A_n. (Here we use the fact that the alternating group A_n is simple for $n \geqslant 5$.) Furthermore, it can be shown that S_n has precisely three normal subgroups (namely those appearing in (3.2)) and hence this is the only composition series for S_n.

(iv) The following is a straightforward example of a group with more than one (actually it has precisely two) composition series. Let $G = A_5 \times C_2$, the *direct product* of the alternating group A_5 of degree 5 and the cyclic group of order 2. It follows from the definition of the multiplication in a direct product that the projection maps

$$\begin{aligned} \pi_1 \colon G &\to A_5 & \qquad \pi_2 \colon G &\to C_2 \\ (x,y) &\mapsto x & (x,y) &\mapsto y \end{aligned}$$

are surjective homomorphisms.

Hence $M = \ker \pi_1 = \mathbf{1} \times C_2 \cong C_2$ and $N = \ker \pi_2 = A_5 \times \mathbf{1} \cong A_5$ are normal subgroups of G with simple quotients

$$G/M \cong A_5 \qquad \text{and} \qquad G/N \cong C_2.$$

Thus we obtain composition series

$$G = A_5 \times C_2 > \mathbf{1} \times C_2 > \mathbf{1} \qquad \text{and} \qquad G = A_5 \times C_2 > A_5 \times \mathbf{1} > \mathbf{1}$$

for G. The composition factors of the first are isomorphic to A_5 and C_2 (in that order), while those of the second are C_2 and A_5.

The third example above illustrates that, although the Jordan–Hölder Theorem says that the composition factors are uniquely determined, it does not mean that the composition series are unique, nor that the composition factors have to occur within the composition series in the same order. It is also easy to construct similar examples using abelian groups (for context, see also Example 3.9 below where we describe what the composition factors of a finite abelian group are).

Example 3.6 The infinite cyclic group has no composition series.

Proof: Let $G = \langle x \rangle$, where $o(x) = \infty$, and suppose that

$$G = G_0 > G_1 > G_2 > \cdots > G_n = \mathbf{1}$$

is a composition series for G. Then G_{n-1} is a non-trivial subgroup of G, so $G_{n-1} = \langle x^k \rangle$ for some $k > 0$ and this is an infinite cyclic group, so is not simple. This contradicts the assumption that the above is a composition series for G. □

To understand the behaviour of composition series, consider some subgroups of a group G

$$G \geqslant M > N \geqslant \mathbf{1}$$

where N is a normal subgroup of M. (The context here is that we might be considering a particular series $G = G_0 > G_1 > \cdots > G_n = \mathbf{1}$ and that $M = G_i$ and $N = G_{i+1}$ for some i. We seek to investigate what property ensures that G_i/G_{i+1} is simple so that we understand when the series is a composition series.) The Correspondence Theorem tells us that subgroups of M/N correspond to subgroups of M which contain N. Furthermore under this correspondence, normal subgroups of M/N correspond to normal subgroups of M which contain N. We conclude that

> *M/N is simple if and only if the only normal subgroups of M containing N are M and N themselves.*

Accordingly, we can now describe what it means for a series of subgroups to be a composition series:

Proposition 3.7 *Let G be a group and*

$$G = G_0 > G_1 > G_2 > \cdots > G_n = \mathbf{1} \tag{3.3}$$

be a series of subgroups of G (i.e., $G_{i+1} \trianglelefteq G_i$ for each i). Then this is a composition series for G if and only if it is maximal, *in the sense that one cannot create a longer series by inserting an additional subgroup.*

Proof: We can insert such a subgroup H into (3.3) to form another series when

$$G = G_0 > G_1 > \cdots > G_i > H > G_{i+1} > \cdots > G_n = \mathbf{1}$$

with $H \trianglelefteq G_i$. (The additional requirement that $G_{i+1} \trianglelefteq H$ follows immediately because $G_{i+1} \trianglelefteq G_i$ by assumption.) Thus (3.3) is maximal when, for every i, there is no normal subgroup H of G_i with $G_i > H > G_{i+1}$; that is, by the Correspondence Theorem when G_i/G_{i+1} is simple. This establishes the claim. □

We shall use the term *refine* to refer to this process of inserting additional terms into a series.

Corollary 3.8 *Let G be a finite group. Then every series for G can be refined to a composition series. In particular, every finite group has a composition series.*

Proof: Start with any series for the finite group G. If it is not a composition series, then we can insert an additional subgroup by Proposition 3.7. We repeat this process until we reach a composition series. The process cannot continue forever, since G is finite so only has finitely many subgroups. To see every finite group G has a composition series, start with the series $G > \mathbf{1}$ and refine to a composition series. □

Example 3.9 Let G be a finite abelian group of order n and write

$$n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$$

where p_1, p_2, …, p_k are the distinct prime factors of n. If

$$G = G_0 > G_1 > G_2 > \cdots > G_m = \mathbf{1}$$

is a composition series, then the composition factors

$$G_0/G_1, \quad G_1/G_2, \quad \dots, \quad G_{m-1}/G_m$$

are *abelian* simple groups and so are cyclic of prime order. Now

$$|G| = |G_0/G_1| \cdot |G_1/G_2| \cdot \dots \cdot |G_{m-1}/G_m|$$

must be the prime factorization of $|G| = n$ and hence the composition factors of G are

$$\underbrace{C_{p_1}, C_{p_1}, \dots, C_{p_1}}_{r_1 \text{ times}}, \; \underbrace{C_{p_2}, C_{p_2}, \dots, C_{p_2}}_{r_2 \text{ times}}, \; \dots, \; \underbrace{C_{p_k}, C_{p_k}, \dots, C_{p_k}}_{r_k \text{ times}}.$$

Chief series

It still remains to establish the Jordan–Hölder Theorem, but before we do that we shall introduce another type of series. Recall that a *normal series* is a series for a group G where every term is a normal subgroup of G.

Definition 3.10 A *chief series* for a group G is a normal series

$$G = G_0 > G_1 > G_2 > \cdots > G_n = \mathbf{1}$$

which is maximal; that is, one cannot create a longer normal series by inserting an additional normal subgroup of G. The quotient groups

$$G_0/G_1, \quad G_1/G_2, \quad \dots, \quad G_{n-1}/G_n$$

are called the *chief factors* of G.

According to Proposition 3.7, a composition series for a group is one that is maximal amongst all composition series, so chief series are the corresponding analogue for *normal* series of a group. The same argument as used for Corollary 3.8 (i.e., inserting normal subgroups of G until we cannot insert any more) establishes:

Proposition 3.11 *Let G be a finite group. Then every normal series for G can be refined to a chief series. In particular, every finite group has a chief series.* □

Example 3.12 (i) If G is any simple group, then

$$G > \mathbf{1}$$

is its only chief series and it has a single chief factor, namely G.

(ii) Let $n \geqslant 5$. Then the composition series

$$S_n > A_n > \mathbf{1}$$

for the symmetric group S_n of degree n is also a chief series (as each term happens to be normal in S_n) and the chief factors of S_n coincide with the composition series.

(iii) Let $G = S_4$, the symmetric group of degree 4. Consider the following chain of normal subgroups of G:

$$S_4 > A_4 > V_4 > \mathbf{1} \tag{3.4}$$

We know that each is a normal subgroup of S_4. Since V_4 consists of the identity together with the conjugacy class of all the permutations of the form $(a\ b)(c\ d)$, there is no normal subgroup N that can be inserted between $\mathbf{1}$ and V_4. The quotients $S_4/A_4 \cong C_2$ and $A_4/V_4 \cong C_3$ are simple. Hence (3.4) is a chief series for S_4 and its chief factors are:

$$C_2, \ C_3, \ C_2 \times C_2.$$

If it happens that every term in some composition series for G happens to be a normal subgroup of G (as in Example 3.12(ii)) then this will also be a chief series. In this case, maximality amongst all series implies maximal amongst normal series. However, in general, a chief series does not need to be a composition series. If

$$G = G_0 > G_1 > G_2 > \cdots > G_n = \mathbf{1}$$

is a chief series, then it might be possible to insert some subgroup H with $G_{i+1} < H < G_i$ and $H \trianglelefteqslant G_i$ (for some i) to create a longer series. We just cannot do so using a subgroup H that also satisfies $H \trianglelefteqslant G$.

In the description of chief series, we have referred to *the* chief factors of a group. Accordingly, we would like to know that they are uniquely determined by the group under consideration. The relevant theorem is:

Theorem 3.13 (Jordan–Hölder Theorem for Chief Series) *Let G be a group and let*

$$G = G_0 > G_1 > G_2 > \cdots > G_m = \mathbf{1}$$

and

$$G = H_0 > H_1 > H_2 > \cdots > H_n = \mathbf{1}$$

be chief series for G. Then $m = n$ and there is a one-one correspondence between the two collections of chief factors

$$G_0/G_1, \quad G_1/G_2, \quad \dots, \quad G_{m-1}/G_m$$

and

$$H_0/H_1, \quad H_1/H_2, \quad \dots, \quad H_{n-1}/H_n$$

such that the corresponding factors are isomorphic.

Comparing this to the Jordan–Hölder Theorem for composition series (Theorem 3.4), one can see that the two theorems are basically identical. They both say that for *maximal* series of a particular type (i.e., series or normal series, respectively), the factors occurring are essentially unique. In view of this, in these lecture notes we shall give a single proof that covers both cases simultaneously.

The Jordan–Hölder Theorem

The goal now is to present a unified argument that establishes the two versions of the Jordan–Hölder Theorem. Accordingly, fix a group G and a collection $\mathcal{S} = \mathcal{S}(G)$ of subgroups of G with the following properties:

($\mathcal{S}1$) the trivial group $\mathbf{1}$ and the whole group G are in $\mathcal{S}$;

($\mathcal{S}2$) if $H, K \in \mathcal{S}$, then $H \cap K \in \mathcal{S}$;

($\mathcal{S}3$) if $H, K, L \in \mathcal{S}$ with $H \leqslant L$ and $K \trianglelefteqslant L$, then $HK \in \mathcal{S}$.

One observes that if $\mathcal{S}$ is the collection of all subgroups of G or is the collection of all normal subgroups of G, then it satisfies these three properties.

If $M \in \mathcal{S}$, then define

$$\mathcal{S}(M) = \{\, H \leqslant M \mid H \in \mathcal{S} \,\};$$

that is, the set of subgroups of M that belong to the collection $\mathcal{S}$. Observe that the collection $\mathcal{S}(M)$ satisfies the same three conditions ($\mathcal{S}1$)–($\mathcal{S}3$) when expressed to relate to subgroups of M (that is, $\mathbf{1}, M \in \mathcal{S}(M)$ and this collection of subgroups of M satisfies ($\mathcal{S}2$) and ($\mathcal{S}3$).) This will enable us to argue by induction in our proof.

Consider two series for G whose terms belong to the collection $\mathcal{S}$:

$$G = G_0 > G_1 > G_2 > \cdots > G_m = \mathbf{1}$$

and

$$G = H_0 > H_1 > H_2 > \cdots > H_n = \mathbf{1}$$

(so we assume $G_i, H_j \in \mathcal{S}$, $G_{i+1} \trianglelefteq G_i$ and $H_{j+1} \trianglelefteq H_j$ for all i and j). We shall say that these series are *isomorphic* if $m = n$ and there is an *isomorphism* between their factors; that is, a bijection between the factors

$$G_0/G_1,\ G_1/G_2,\ \ldots,\ G_{m-1}/G_m \qquad \text{and} \qquad H_0/H_1,\ H_1/H_2,\ \ldots,\ H_{n-1}/H_n$$

that maps each factor G_i/G_{i+1} to an isomorphic factor H_j/H_{j+1}.

We shall now prove the following theorem:

Theorem 3.14 (General Version of Jordan–Hölder Theorem) *Let G be a group with a collection of subgroups $\mathcal{S} = \mathcal{S}(G)$ satisfying Conditions (S1)–(S3) and let*

$$G = G_0 > G_1 > G_2 > \cdots > G_m = \mathbf{1} \tag{3.5}$$

and

$$H = H_0 > H_1 > H_2 > \cdots > H_n = \mathbf{1} \tag{3.6}$$

be series for G consisting of subgroups from $\mathcal{S}$ that are maximal (in the sense that one cannot create a longer series by inserting an additional subgroup from $\mathcal{S}$). Then these two maximal series of subgroups from $\mathcal{S}$ are isomorphic.

The Jordan–Hölder Theorem (Theorem 3.4) and the version for chief series (Theorem 3.13) then follow as special cases when $\mathcal{S}$ is the set of all subgroups of G and when $\mathcal{S}$ is the set of all normal subgroups of G, respectively.

PROOF: Assume without loss of generality that $m \leqslant n$. We shall proceed by induction on m. If $m = 0$, then $G = \mathbf{1}$ and hence necessarily $n = 0$ also. In this case there are no factors and the claimed isomorphism exists vacuously.

Suppose then that $m > 0$ and that the Jordan–Hölder Theorem holds for all groups with suitable collections $\mathcal{S}$ of subgroups and maximal series of $\mathcal{S}$-subgroups of length $< m$. To complete the induction step, we split into two cases.

Case 1: $G_1 = H_1$.

In this case, $G_0/G_1 = G/G_1 = H_0/H_1$. Furthermore,

$$G_1 > G_2 > \cdots > G_m = \mathbf{1}$$

and

$$G_1 = H_1 > H_2 > \cdots > H_n = \mathbf{1}$$

are maximal series for G_1 consisting of subgroups in $\mathcal{S}(G_1)$ of lengths $m-1$ and $n-1$, respectively. Hence, by induction, $m - 1 = n - 1$ (that is, $m = n$) and there is an isomorphism between the factors

$$G_1/G_2,\ \ldots,\ G_{m-1}/G_m \qquad \text{and} \qquad H_1/H_2,\ \ldots,\ H_{n-1}/H_n.$$

Since $G_0/G_1 = H_0/H_1$, this extends to the required isomorphism between the factors of the two series (3.5) and (3.6) for G.

Case 2: $G_1 \neq H_1$.

Conditions ($\mathcal{S}2$) and ($\mathcal{S}3$) ensure that $D = G_1 \cap H_1$ and G_1H_1 are subgroups in $\mathcal{S}$. Note that $G_1 \leqslant G_1H_1 \trianglelefteq G_0 = G$ and $H_1 \leqslant G_1H_1 \trianglelefteq H_0 = G$. Since the series (3.5) and (3.6) are maximal, we cannot insert G_1H_1 as a new term into them. Hence either $G_1H_1 = G$ or $G_1 = G_1H_1 = H_1$. We have assumed the latter does not occur and so $G_1H_1 = G$.

By the Second Isomorphism Theorem,

$$\frac{H_0}{H_1} = \frac{G}{H_1} = \frac{G_1H_1}{H_1} \cong \frac{G_1}{G_1 \cap H_1} = \frac{G_1}{D},$$

with isomorphism $\theta \colon G_1/D \to G/H_1$ given by $Dx \mapsto H_1x$ for $x \in G_1$. Similarly $G_0/G_1 = G/G_1 \cong H_1/D$. Now as D is a normal subgroup of G belonging to $\mathcal{S}$, it has a maximal series with terms in $\mathcal{S}$:

$$D = D_2 > D_3 > \cdots > D_k = \mathbf{1}$$

(For finite groups, this is established by the same argument as used for Corollary 3.8 and Proposition 3.11: just keep refining the series $D > \mathbf{1}$ by inserting terms from $\mathcal{S}$ until we cannot insert any more. When G is infinite, we are using a theorem, which appears on Problem Sheet III, that says if G has a maximal series with terms from $\mathcal{S}$ then so does any normal subgroup in $\mathcal{S}$.) We now have four series for G with terms from $\mathcal{S}$:

$$\begin{aligned}
G &= G_0 > G_1 > G_2 > \cdots > G_m = \mathbf{1} && (3.5)\\
G &= G_0 > G_1 > D = D_2 > \cdots > D_k = \mathbf{1} && (3.7)\\
G &= H_0 > H_1 > D = D_2 > \cdots > D_k = \mathbf{1} && (3.8)\\
G &= H_0 > H_1 > H_2 > \cdots > H_n = \mathbf{1} && (3.6)
\end{aligned}$$

By assumption, (3.5) and (3.6) are maximal series with terms from $\mathcal{S}$. In fact the same is true for (3.7) and (3.8). We just need to ensure that one cannot insert a term from $\mathcal{S}$ between G_1 and D nor between H_1 and D.

Suppose $D \leqslant M \trianglelefteq G_1$ with $M \in \mathcal{S}$. Since $H_1 \trianglelefteq G$, use of Condition ($\mathcal{S}3$) shows that $MH_1 \in \mathcal{S}$ and this satisfies $H_1 \leqslant MH_1 \leqslant G$. Moreover the isomorphism $\theta \colon G_1/D \to G/H_1$, given by $Dx \mapsto H_1x$ for $x \in G_1$, maps the normal subgroup M/D to MH_1/H_1, so $MH_1 \trianglelefteq G$. Since the series (3.6) is maximal, we cannot insert MH_1 as a new term and therefore $MH_1 = H_1$ or G. If $MH_1 = H_1$, then M/D is mapped by θ to the trivial subgroup of G/H_1 and hence $M = D$. If $MH_1 = G$, then M/D is mapped to the whole quotient group G/H_1 and hence $M = G_1$. Therefore the series (3.7), and similarly the series (3.8), is maximal.

Now Case 1 applies to the series (3.5) and (3.7). We deduce that $m = k$ and there is an isomorphism between their factors. We have already observed that $G_0/G_1 \cong H_1/D$ and $H_0/H_1 \cong G_1/D$ and hence there is an isomorphism between the series (3.7) and (3.8) that simply interchanges the first pair of factors. Finally Case 1 applies to the series (3.8) and (3.6) (as we know the former has length $k = m$) and hence $m = k = n$ and there is an isomorphism between the factors of these series. In conclusion, $m = n$ and, upon composing the isomorphisms, we obtain the required isomorphism between the factors of (3.5) and (3.6).

This completes the induction step and establishes the Jordan–Hölder Theorem (in its general form, and therefore also the specific versions stated earlier). □

Characteristic subgroups

We know that composition factors of a group are simple groups. One might ask what can be said about the chief factors. In the remainder of the chapter, we aim to describe these chief factors. To do so, we first introduce the following concept.

Definition 3.15 A subgroup H of a group G is said to be a *characteristic subgroup* of G if $x\phi \in H$ for all $x \in H$ and all automorphisms ϕ of G.

The definition requires that $H\phi \leqslant H$ for all automorphisms ϕ of G. It then follows that $H\phi^{-1} \leqslant H$ for any automorphism ϕ and applying ϕ then yields $H \leqslant H\phi$. Thus H is a characteristic subgroup if and only if $H\phi = H$ for all automorphisms ϕ of G.

The notation used for a characteristic subgroup is less consistent in the literature than for, say, being a normal subgroup. In these notes, we shall write

$$H \operatorname{char} G$$

to indicate that H is a characteristic subgroup of G.

Lemma 3.16 *Let G be a group.*

(i) *If $H \operatorname{char} G$, then $H \trianglelefteqslant G$.*

(ii) *If $K \operatorname{char} H$ and $H \operatorname{char} G$, then $K \operatorname{char} G$.*

(iii) *If $K \operatorname{char} H$ and $H \trianglelefteqslant G$, then $K \trianglelefteqslant G$.*

Thus there is considerable difference between characteristic subgroups and normal subgroups. For example, note that in general

- $K \trianglelefteqslant H \trianglelefteqslant G$ does not imply $K \trianglelefteqslant G$.
- If $\phi\colon G \to K$ is a homomorphism and $H \operatorname{char} G$, then it does not follow necessarily that $H\phi \operatorname{char} G\phi$. (Consequently there is no version of the Correspondence Theorem that will work well with characteristic subgroups.)
- If $H \leqslant L \leqslant G$ and $H \operatorname{char} G$, then it does not necessarily follow that $H \operatorname{char} L$.

Problem Sheet III contains a question that addresses the existence of examples illustrating the above three points.

Proof of Lemma 3.16: (i) If $x \in G$, then $\tau_x\colon g \mapsto g^x$ is an (inner) automorphism of G. Hence if $H \operatorname{char} G$, then

$$H^x = H\tau_x = H \qquad \text{for all } x \in G,$$

so $H \trianglelefteqslant G$.

(ii) Let ϕ be an automorphism of G. Then $H\phi = H$ (as $H \operatorname{char} G$). Hence the restriction $\phi|_H$ of ϕ to H is an automorphism of H and we deduce

$$x\phi \in K \qquad \text{for all } x \in K$$

(since this is the effect that the restriction $\phi|_H$ has when applied to elements of K). Thus $K \operatorname{char} G$.

(iii) Let $x \in G$. Then $H^x = H$ (as $H \trianglelefteqslant G$) and therefore $\tau_x\colon g \mapsto g^x$ (for $g \in H$) is a bijective homomorphism $H \to H$; that is, τ_x induces an automorphism of H. Since $K \operatorname{char} H$, we deduce that $K^x = K\tau_x = K$. Thus $K \trianglelefteqslant G$. □

Minimal normal subgroups

Definition 3.17 Let G be a finite group. A *minimal normal subgroup* of G is a non-trivial normal subgroup of G which has no non-trivial proper subgroup that is also normal in G.

Thus M is a minimal normal subgroup of G if

(i) $\mathbf{1} < M \trianglelefteqslant G$;

(ii) if $\mathbf{1} \leqslant N \leqslant M$ and $N \trianglelefteqslant G$, then either $N = \mathbf{1}$ or $N = M$.

Lemma 3.18 *Let G be a non-trivial finite group and*

$$G = G_0 > G_1 > G_2 > \cdots > G_n = \mathbf{1}$$

be a chief series for G. Then each chief factor G_i/G_{i+1} is a minimal normal subgroup of G/G_{i+1}.

In particular, the last term G_{n-1} of the chief series is a minimal normal subgroup of G.

Proof: Since a chief series is a maximal normal series, there is no normal subgroup N of G satisfying $G_{i+1} < N < G_i$. Hence, by the Correspondence Theorem, there is no normal subgroup N/G_{i+1} of G/G_{i+1} satisfying $\mathbf{1} < N/G_{i+1} < G_i/G_{i+1}$. □

We shall prove the following description of minimal normal subgroups, which therefore also describes all chief factors of a finite group.

Theorem 3.19 *A minimal normal subgroup of a finite group G is a direct product of isomorphic simple groups.*

We shall work towards the proof of this theorem in the remainder of the chapter. First we make the following definition.

Definition 3.20 A non-trivial group G is called *characteristically simple* if the only characteristic subgroups it has are $\mathbf{1}$ and G.

Lemma 3.21 *A minimal normal subgroup of a group is characteristically simple.*

Proof: Let M be a minimal normal subgroup of the group G. Let K be a characteristic subgroup of M. Then

$$K \operatorname{char} M \trianglelefteqslant G,$$

so $K \trianglelefteqslant G$ by Lemma 3.16(iii). Thus minimality of M forces $K = \mathbf{1}$ or $K = M$. Hence M is indeed characteristically simple. □

Theorem 3.19 then follows immediately from the following result. (The advantage of proving Theorem 3.22 over a direct attempt on Theorem 3.19 is that we can concentrate only on the characteristically simple group rather than having to juggle both the minimal normal subgroup and its embedding in the larger group.)

Theorem 3.22 *A characteristically simple finite group is a direct product of isomorphic simple groups.*

Proof: Let G be a finite group which is characteristically simple. Let S be a minimal normal subgroup of G. (So $S \neq \mathbf{1}$. It is possible that $S = G$.) Consider the following set

$$\mathscr{D} = \{\, N \trianglelefteq G \mid N = S_1 \times S_2 \times \cdots \times S_k \text{ where each } S_i \text{ is a minimal normal subgroup of } G \text{ isomorphic to } S \,\}.$$

(Recall what is needed to be a direct product here: We need $N = S_1 S_2 \dots S_k$ and $S_i \cap S_1 \dots S_{i-1} S_{i+1} \dots S_k = \mathbf{1}$ for each i. The condition that each S_i is normal in N comes for free, since we required $S_i \trianglelefteq G$ in the definition of the set $\mathscr{D}$.)

Note that our original subgroup S is a member of $\mathscr{D}$, so $\mathscr{D}$ certainly contains non-trivial members. Choose $N \in \mathscr{D}$ of largest possible order.

Claim: $N = G$.

Suppose our maximal member N of $\mathscr{D}$ is not equal to G. Since it belongs to our set $\mathscr{D}$,

$$N = S_1 \times S_2 \times \cdots \times S_k$$

where each S_i is a minimal normal subgroup of G isomorphic to S. As G is characteristically simple, N cannot be a characteristic subgroup of G. Hence there exists an automorphism ϕ of G such that

$$N\phi \nleqslant N.$$

Therefore there exists i such that

$$S_i\phi \nleqslant N.$$

Now ϕ is an automorphism of G, so $S_i\phi$ is a minimal normal subgroup of G. Observe that $N \cap S_i\phi \trianglelefteq G$ and $N \cap S_i\phi$ is properly contained in $S_i\phi$ (as $S_i\phi \nleqslant N$). Therefore, by minimality of $S_i\phi$, we deduce $N \cap S_i\phi = \mathbf{1}$. It follows that

$$N \cdot S_i\phi = N \times S_i\phi = S_1 \times S_2 \times \cdots \times S_k \times S_i\phi$$

and

$$N \cdot S_i\phi \trianglelefteq G.$$

This shows that $N \cdot S_i\phi \in \mathscr{D}$. This contradicts N being a maximal member of $\mathscr{D}$.

This establishes the claim, so

$$G = N = S_1 \times S_2 \times \cdots \times S_k,$$

where each S_i is a minimal normal subgroup of G isomorphic to our original minimal normal subgroup S.

It remains to check that S is simple. If $J \trianglelefteq S_1$, then

$$J \trianglelefteq S_1 \times S_2 \times \cdots \times S_k = G.$$

Therefore, as S_1 is a minimal normal subgroup of G, we must have $J = \mathbf{1}$ or $J = S_1$. Hence S_1 (and accordingly S) is simple.

We have consequently shown that, indeed, G is a direct product of isomorphic simple groups. □

Chapter 4

Semidirect Products

The primary purpose of this chapter is to discuss ways in which grups can be built from smaller groups. In some sense, we are considering how to reverse the decomposition that composition series (or, indeed, chief series) and the Jordan–Hölder Theorem give us. One question you might ask is:

> If a finite group G has composition factors S_1, S_2, ..., S_k, what are the possibilities for G?

This turns out to be an extremely difficult question to answer in general, but the content of this chapter will provide one of the more straightforward ways to build a group with a given normal subgroup N and a given quotient Q.

This construction arises naturally in the context of attempting to classify groups given specific information. We shall first illustrate the sort of question one might consider and answer it using the direct product construction. First recall that if a group G has normal subgroups M and N such that $G = MN$ and $M \cap N = \mathbf{1}$, then

$$G \cong M \times N = \{\, (x, y) \mid x \in M,\ y \in N \,\}.$$

The multiplication in the direct product $M \times N$ is componentwise:

$$(x_1, y_1)(x_2, y_2) = (x_1x_2, y_1y_2)$$

for $x_1, x_2 \in M$ and $y_1, y_2 \in N$. Accordingly if we find such normal subgroups M and N and we fully understand their structure, then this implies that we have fully determined the possibility for G. (A verification of the above isomorphism, as revision of direct products, appeared on Problem Sheet I.)

Example 4.1 *Classify the finite groups of order* 45*.*

Solution: Let G be a group of order $45 = 3^2 \cdot 5$. The number of Sylow 3-subgroups is congruent to 1 (mod 3) and divides 5. Therefore G has a unique Sylow 3-subgroup T. The number of Sylow 5-subgroups is congruent to 1 (mod 5) and divides 9 and we conclude that G also has a unique Sylow 5-subgroup F. Since the conjugate of a Sylow p-subgroup is again a Sylow p-subgroup, it follows that $T \trianglelefteq G$ and $F \trianglelefteq G$. By Lagrange's Theorem, $T \cap F = \mathbf{1}$ (as these subgroups have coprime order) and hence

$$|G| = \frac{|T| \cdot |F|}{|T \cap F|} = 3^2 \cdot 5 = 45.$$

We deduce that $G = TF$. This shows that G satisfies the criteria to be a direct product:

$$G \cong T \times F.$$

Now T is a group of order 9 and we know (from *MT4003*) that a group of order p^2 (for p prime) is abelian and is isomorphic to either C_{p^2} or $C_p \times C_p$. Hence $T \cong C_9$ or $C_3 \times C_3$. Equally, F is a group of order 5 (which is prime), so $F \cong C_5$. We conclude that there are (up to isomorphism) two possibilities for G:

$$G \cong C_9 \times C_5 \qquad \text{or} \qquad G \cong C_3 \times C_3 \times C_5$$

The Classification of Finite Abelian Groups (again from *MT4003*) tells us that these groups are not isomorphic. Hence there are precisely two groups (up to isomorphism) of order 45. □

This method of using direct products works very well when the number theory happens to fall nicely and one can find the required normal subgroups. However, consider the case of trying to classify groups of order $20 = 2^2 \cdot 5$. Application of Sylow's Theorem shows that there is a unique Sylow 5-subgroup, but all can conclude about the Sylow 2-subgroups is that the number of them is either 1 or 5. We would have one normal subgroup (the Sylow 5-subgroup) but not necessarily the two normal subgroups required for the direct product. We now introduce a new construction to cover this situation.

Semidirect products

Suppose that a group G can be expressed as $G = NH$ with $H \cap N = \mathbf{1}$ and only $N \trianglelefteq G$. (The direct product case is when $H \trianglelefteq G$ also holds.) An element in G is expressible as $g = nh$ where $h \in H$ and $n \in N$. If we attempt to multiply two elements of G, then we calculate

$$(n_1h_1)(n_2h_2) = n_1(h_1n_2h_1^{-1}) \cdot h_1h_2$$

Here $h_1h_2 \in H$, $h_1n_2h_1^{-1} \in N$ (as $N \trianglelefteq G$) and so $n_1(h_1n_2h_1^{-1}) \in N$. This formula shows us that to be able to work effectively in G, we need to be able to (i) multiply in H, (ii) multiply in N, and (iii) conjugate elements of N by elements of H. The semidirect product construction is designed to encode these three pieces of information.

We shall need the following object as part of the construction. Recall (from Definition 1.32) that an automorphism of a group G is a bijective homomorphism $G \to G$.

Definition 4.2 Let G be a group. The *automorphism group* of G is denoted by $\operatorname{Aut} G$ and consists of all automorphisms of G:

$$\operatorname{Aut} G = \{\, \phi \colon G \to G \mid \phi \text{ is an automorphism} \,\}.$$

The product of two automorphisms ϕ and ψ is the composite $\phi\psi$.

It was verified on Problem Sheet II that $\operatorname{Aut} G$ is a group. The verification is very similar to the proof that a symmetric group forms a group. Indeed one can observe $\operatorname{Aut} G$ is a subgroup of the symmetric group $\operatorname{Sym}(G)$.

Definition 4.3 Let H and N be groups and let $\phi \colon H \to \operatorname{Aut} N$ be a homomorphism. The (*external*) *semidirect product* of N by H via ϕ is denoted by $N \rtimes_\phi H$ and is the set

$$N \rtimes_\phi H = \{\, (n,h) \mid n \in N,\ h \in H \,\}$$

with multiplication given by

$$(n_1,h_1)(n_2,h_2) = (n_1 n_2^{(h_1\phi)^{-1}}, h_1h_2).$$

If $h \in H$, then $h\phi$ is an automorphism of N and we are writing $n^{h\phi}$ for the image of an element $n \in N$ under the automorphism $h\phi$. (The reason for using exponential notation is twofold: firstly to make the notation easier to distinguish and secondly to be suggestive of conjugation in a way that we shall use later.) This means that the above multiplication in $N \rtimes_\phi H$ at least has meaning.

Aside: If $G = NH$ where $N \trianglelefteq G$ and $H \leqslant G$, then also $G = HN$ (see Lemma 1.19). As a consequence, it should not be surprising to learn that we can also define an external semidirect product as $H \ltimes_\phi N$ with respect to some homomorphism $\phi \colon H \to \operatorname{Aut} N$ with elements denoted by pair (h,n) where $h \in H$ and $n \in N$. This can indeed be done and the result is a group isomorphic to the one given in Definition 4.3. In some ways the formulae involved are slightly more pleasant with this alternative construction, but the majority of the literature on group theory seems to use the $N \rtimes H$ version with the normal subgroup N on the left. Accordingly these lecture notes follow the standard convention of writing $N \rtimes_\phi H$ for the semidirect product.

Proposition 4.4 *The semidirect product $N \rtimes_\phi H$ is a group.*

Proof: We need to check the axioms of a group. First associativity (which is straightforward, but messy):

$$\begin{aligned}\big((n_1,h_1)(n_2,h_2)\big)(n_3,h_3) &= \big(n_1 n_2^{(h_1\phi)^{-1}}, h_1h_2\big)(n_3,h_3) \\ &= \big(n_1 n_2^{(h_1\phi)^{-1}} n_3^{((h_1h_2)\phi)^{-1}}, h_1h_2h_3\big) \\ &= \big(n_1 n_2^{(h_1\phi)^{-1}} n_3^{(h_2\phi)^{-1}(h_1\phi)^{-1}}, h_1h_2h_3\big),\end{aligned}$$

using the fact that ϕ is a homomorphism, so that $\big((h_1h_2)\phi\big)^{-1} = \big((h_1\phi)(h_2\phi)\big)^{-1} = (h_2\phi)^{-1}(h_1\phi)^{-1}$. On the other hand

$$\begin{aligned}(n_1,h_1)\big((n_2,h_2)(n_3,h_3)\big) &= (n_1,h_1)\big(n_2 n_3^{(h_2\phi)^{-1}}, h_2h_3\big) \\ &= \big(n_1 (n_2 n_3^{(h_2\phi)^{-1}})^{(h_1\phi)^{-1}}, h_1h_2h_3\big) \\ &= \big(n_1 n_2^{(h_1\phi)^{-1}} n_3^{(h_2\phi)^{-1}(h_1\phi)^{-1}}, h_1h_2h_3\big)\end{aligned}$$

using the fact that the inverse of $h_1\phi$ is an automorphism, in particular a homomorphism, and so maps products to products. Comparing these formulae we deduce that the binary operation on the semidirect product is associative.

Identity:

$$(1,1)(n,h) = (1n^{(1\phi)^{-1}}, 1h) = (n^{\mathrm{id}}, h) = (n,h)$$

(since the automorphism 1ϕ must be the identity) and

$$(n,h)(1,1) = (n1^{(h\phi)^{-1}}, h1) = (n1,h) = (n,h)$$

Hence $(1,1)$ is the identity element in $N \rtimes_{\phi} H$.

Inverses:

$$\begin{aligned}
(n,h)\big((n^{h\phi})^{-1}, h^{-1}\big) &= \big(n((n^{h\phi})^{-1})^{(h\phi)^{-1}}, hh^{-1}\big) \\
&= \big(n(n^{(h\phi)(h\phi)^{-1}})^{-1}, 1\big) && (*) \\
&= (n(n^{\mathrm{id}})^{-1}, 1) \\
&= (nn^{-1}, 1) \\
&= (1,1),
\end{aligned}$$

since $(*)$ $(h\phi)^{-1}$ is a homomorphism so maps inverses to inverses, and

$$\begin{aligned}
\big((n^{h\phi})^{-1}, h^{-1}\big)(n,h) &= \big((n^{h\phi})^{-1} n^{((h^{-1})\phi)^{-1}}, h^{-1}h\big) \\
&= \big((n^{h\phi})^{-1} n^{h\phi}, 1\big) && (\dagger) \\
&= (1,1)
\end{aligned}$$

since $(\dagger)$ ϕ is a homomorphism so maps inverses to inverses. Thus $\big((n^{h\phi})^{-1}, h^{-1}\big)$ is the inverse of (n,h) in $N \rtimes_{\phi} H$.

This completes the proof that $N \rtimes_{\phi} H$ is a group. □

We have now successful constructed a group G from two groups N and H and the specified homomorphism $\phi\colon H \to \operatorname{Aut} N$. The following summarizes the properties of this group, though we leave the proofs to Problem Sheet IV since they are mostly an exercise in computation (and therefore a good way to practice working with this group).

Theorem 4.5 *Let H and N be groups, $\phi\colon H \to \operatorname{Aut} N$ be a homomorphism and $G = N \rtimes_{\phi} H$ be the semidirect product of N by H via ϕ. Then*

(i) *$\bar{N} = \{\, (n,1) \mid n \in N \,\}$ is a normal subgroup of G that is isomorphic to N;*

(ii) *$\bar{H} = \{\, (1,h) \mid h \in H \,\}$ is a subgroup of G that is isomorphic to H;*

(iii) *$\bar{H} \cap \bar{N} = \mathbf{1}$ and $G = \bar{N}\bar{H}$;*

(iv) *the quotient group $G/\bar{N}$ is isomorphic to H;*

(v) *conjugation of an element of $\bar{N}$ by an element of $\bar{H}$ is determined by the homomorphism ϕ:*

$$(1,h)^{-1}(n,1)(1,h) = (n^{h\phi}, 1) \qquad \text{for all } n \in N \text{ and } h \in H.$$

In the case of a direct product, sometimes one refers to the *external* direct product by which one means the group defined as ordered pairs

$$G = G_1 \times G_2 = \{\, (x,y) \mid x \in G_1,\ y \in G_2 \,\}$$

with componentwise multiplication and the *internal* direct product by which ones means a group G with two normal subgroups G_1 and G_2 satisfying $G = G_1G_2$ and $G_1 \cap G_2 = \mathbf{1}$. What we has observed previously (see, for example, Problem Sheet I for one direction) is that an internal direct product is isomorphic to the corresponding external direct product and that the external direct product has normal subgroups that satisfy the properties of an internal direct product. As a consequence, we tend to move fluidly between the two viewpoints and rarely distinguish between them. (These groups are isomorphic; i.e., essentially the same.)

In the case of semidirect products, a similar viewpoint is taken. We have just described an external version, namely the construction appearing in Definition 4.3, and we have just recorded its basic structural properties in Theorem 4.5. We shall take some of these properties as being the *internal* description for a group to be a semidirect product and show that indeed a group satisfying these properties is isomorphic to a group built using the semidirect product construction.

We shall therefore assume that G is a group with two subgroups H and N such that

(i) N is a normal subgroup of G,

(ii) $G = NH$, and

(iii) $H \cap N = \mathbf{1}$.

When these conditions hold, we shall sometimes say that H is a *complement* to N and write $G = N \rtimes H$. Our goal is to show that it is isomorphic to some external semidirect product of N by H. There are various stages to proceed through, but the most significant is to work out what the required homomorphism $\phi\colon H \to \operatorname{Aut} N$ should be.

We shall define a map $\theta\colon N \times H \to G$ by

$$(n, h) \mapsto nh.$$

(At this point, we do not assume any group theoretical structure on the *set* $N \times H$. It will eventually become a semidirect product.) Now $G = NH$, so every element of G can be written in the form nh where $n \in N$ and $h \in H$. Therefore θ is surjective. Suppose $nh = n'h'$ where $n, n' \in H$ and $h, h' \in N$. Then

$$h(h')^{-1} = n^{-1}n' \in H \cap N = \mathbf{1}.$$

This forces $h = h'$ and $n = n'$. Therefore this expression for an element of G as a product is unique and we deduce that θ is injective.

We now know that θ is a bijection, but we seek to endow the domain of θ with the structure of an (external) semidirect product and consequently need to specify a homomorphism $\phi\colon H \to \operatorname{Aut} N$ to use when constructing this group. Let $h \in H$. Then $N^h = N$ in the group G since $N \trianglelefteq G$. Hence conjugation by h determines a map

$$\begin{aligned} \phi_h\colon N &\to N \\ n &\mapsto n^h. \end{aligned}$$

Its inverse is $\phi_{h^{-1}}\colon n \mapsto n^{h^{-1}}$, so ϕ_h is a bijection. Also

$$(mn)\phi_h = h^{-1}(mn)h = h^{-1}mh \cdot h^{-1}nh = (m\phi_h)(n\phi_h).$$

Hence $\phi_h \in \operatorname{Aut} N$. Finally

$$n\phi_{hk} = (hk)^{-1}n(hk) = k^{-1}(h^{-1}nh)k = n\phi_h\phi_k$$

for $n \in N$, so

$$\phi_{hk} = \phi_h\phi_k \qquad \text{for all } h, k \in H.$$

We deduce that $\phi\colon h \mapsto \phi_h$ is a homomorphism $H \to \operatorname{Aut} N$. We use this map ϕ to construct the semidirect product $N \rtimes_\phi H$.

In view of what we have already shown, we can now view the bijection θ as a map

$$\begin{aligned} \theta\colon N \rtimes_\phi H &\to G \\ (n,h) &\mapsto nh. \end{aligned}$$

Let $(n_1,h_1),(n_2,h_2) \in N \rtimes_\phi H$. Then

$$\begin{aligned} \big((n_1,h_1)(n_2,h_2)\big)\theta &= (n_1 n_2^{(h_1\phi)^{-1}}, h_1h_2)\theta \\ &= (n_1 n_2^{h_1^{-1}}, h_1h_2)\theta \\ &= n_1 n_2^{h_1^{-1}} h_1 h_2 \\ &= n_1 \cdot h_1 n_2 h_1^{-1} \cdot h_1 h_2 \\ &= n_1 h_1 n_2 h_2 \\ &= (n_1,h_1)\theta \cdot (n_2,h_2)\theta. \end{aligned}$$

Hence θ is a homomorphism and consequently is an isomorphism. We have established the following theorem:

Theorem 4.6 *Let G be a group with a normal subgroup N and a subgroup H such that $G = NH$ and $H \cap N = \mathbf{1}$. Then G is isomorphic to the semidirect product $N \rtimes_\phi H$ where $\phi\colon H \to \operatorname{Aut} N$ is the homomorphism given by*

$$h\phi\colon n \mapsto n^h$$

for $n \in N$ and $h \in H$. □

In view of this theorem, we tend to view groups that satisfy the hypotheses as being "the same" (since that is what isomorphic means) as a semidirect product as constructed by Definition 4.3. We use the term *semidirect product* to refer to both situations and we try to move between both viewpoints quite smoothly.

Indeed, for notational simplicity, we frequently drop the brackets in the semidirect product construction. To be precise, let N and H be groups and $\phi\colon H \to \operatorname{Aut} N$ be a homomorphism from H to the automorphism group of N. We shall write $G = N \rtimes_\phi H$ (and sometimes simply $N \rtimes H$ if ϕ is sometimes understood) to be the set of products

$$G = \{\, nh \mid n \in N,\ h \in H \,\}$$

with multiplication given by

$$n_1h_1 \cdot n_2h_2 = n_1 n_2^{(h_1\phi)^{-1}} h_1 h_2.$$

We identify N with the set of elements of the form $n1$ for $n \in N$ and H with the set of elements of the form $1h$ for $h \in H$. Then, according to Theorem 4.5, the conjugation in G of an element of N by an element of H is determined by the homomorphism ϕ:

$$h^{-1}nh = n^{h\phi} \qquad \text{for } h \in H \text{ and } n \in N.$$

It is for this reason that we sometimes omit reference to the homomorphism ϕ: a semidirect product is determined by the two groups N and H from which it is built together with a description of the result of conjugating an element of N by an element of H.

Warnings:

(i) Note, however, that to construct a semidirect product $G = N \rtimes H$ you cannot simply specify $h^{-1}nh$ for each $h \in H$ and $n \in N$. If there isn't some homomorphism $\phi\colon H \to \operatorname{Aut} N$ involved (as we have described above) then the result will not be a group.

(ii) If G is a group which is not simple, it does not necessarily decompose as a semidirect product. We might be able to find a non-trivial proper normal subgroup N of G, but there is no guarantee that there will be a complement H to N in G. For example, if N is *any* non-trivial proper normal subgroup of the quaternion group Q_8, there does not exist a subgroup H of Q_8 with $N \cap H = \mathbf{1}$ and $NH = Q_8$. Consequently Q_8 cannot be decomposed in a proper way as a semidirect product.

Applications of semidirect products

We shall now give a few examples of semidirect products. In the first example below, we shall classify the groups of order 20. The method will be to show that if $|G| = 20$ then $G \cong N \rtimes_\phi H$ for some N, H and ϕ using Theorem 4.6. We shall describe all the options for the three ingredients N, H and ϕ in the semidirect product construction and hence will have determined all the groups of order 20.

Example 4.7 *Determine how many groups of order* 20 *there are (up to isomorphism).*

Solution: Let G be a group of order $20 = 2^2 \cdot 5$. By Sylow's Theorem, the number of Sylow 5-subgroups is congruent to 1 (mod 5) and divides 4. Hence G has a unique Sylow 5-subgroup F. Then we know $F \trianglelefteq G$ and $|F| = 5$.

Let T be a Sylow 2-subgroup of G, so $|T| = 4$. Then $T \cap F = \mathbf{1}$ by Lagrange's Theorem, while Lemma 1.19 tells us that

$$|FT| = \frac{|F| \cdot |T|}{|F \cap T|} = \frac{5 \cdot 4}{1} = 20.$$

Hence $G = FT$, $F \trianglelefteq G$ and $T \cap F = \mathbf{1}$. Thus, by Theorem 4.6, $G \cong F \rtimes_\phi T$, the semidirect product of F by T with respect to a suitable homomorphism $\phi\colon T \to \operatorname{Aut} F$. In order to describe all possible such groups G, we need to determine the possibilities for F, T and the homomorphism ϕ.

We know that $|F| = 5$, so $F \cong C_5$. Fix a generator x for F, so $o(x) = 5$. Since $|T| = 4$, there are two possibilities for T: either $T \cong C_4$ or $C_2 \times C_2$. In order to determine the possibilities for ϕ, we first need to be able to describe the automorphism group of F.

An automorphism α of F of is determined by its effect on the generator x, since if we know what $x\alpha$ is then $(x^i)\alpha = (x\alpha)^i$ is determined by α. Furthermore, since the powers of x are mapped to powers of $x\alpha$, in order that α be surjective, necessarily $x\alpha$ must be a generator of F. Thus $x\alpha = x$, x^2, x^3 or x^4. (Note that all the non-identity elements of F have order 5 and therefore generate F.) Finally, if g is a generator of F, then $x^i \mapsto g^i$ does define an automorphism of F. Thus all four choices do indeed give automorphisms of F and so

$$|\operatorname{Aut} F| = 4.$$

In fact, we can determine which group of order 4 this automorphism group is. Consider the automorphism β given by $x \mapsto x^2$ and compute its powers:

$$\begin{aligned} x\beta^2 &= (x\beta)\beta = (x^2)\beta = (x\beta)^2 = (x^2)^2 = x^4 \\ x\beta^3 &= (x\beta^2)\beta = (x^4)\beta = (x\beta)^4 = (x^2)^4 = x^8 = x^3 \\ x\beta^4 &= (x\beta^3)\beta = (x^3)\beta = (x\beta)^3 = (x^2)^3 = x^6 = x. \end{aligned}$$

So $\beta^4 = \mathrm{id}_F$ and $o(\beta) = 4$. Thus $\operatorname{Aut} F = \langle \beta \rangle$ is cyclic of order 4.

We are now able to describe all the groups of order 20. We shall consider each possibility for T in turn and determine what the options are for the homomorphism $\phi\colon T \to \operatorname{Aut} F$.

Case 1: $T \cong C_4$.

If $\phi\colon T \to \operatorname{Aut} F$ is a homomorphism, then the image of ϕ must be a subgroup of $\operatorname{Aut} F = \langle \beta \rangle$ that could occur as an image of the cyclic group T. Since $|T| = |\operatorname{Aut} F| = 4$, there are three possibilities: $T\phi = \mathbf{1}$, $\langle \beta^2 \rangle$ or $\langle \beta \rangle$ (these three being the unique subgroups of $\operatorname{Aut} F$ of order 1, 2 and 4, respectively).

(i) If $T\phi = \mathbf{1}$, then every element of T commutes with all elements of F (since if $g\phi$ is the automorphism that $g \in T$ induces when it acts by conjugation on F). Therefore in this case, G is a direct product:

$$G \cong F \times T = C_5 \times C_4 \cong C_{20}$$

(using the standard fact, from *MT4003*, that $C_m \times C_n \cong C_{mn}$ when $\gcd(m, n) = 1$).

(ii) If $T\phi = \langle \beta^2 \rangle$, then $|\ker \phi| = 2$; that is $\ker \phi$ is the unique subgroup of order 2 in $T \cong C_4$. If y is a generator for T, then $y \notin \ker \phi$ (as y has order 4) and therefore $y\phi = \beta^2$. Hence in this case

$$G \cong F \rtimes_\phi T$$

where a generator y of T induces the automorphism $\beta^2\colon x \mapsto x^4$ when it acts by conjugation: $y^{-1}xy = x^4$.

(iii) If $T\phi = \langle \beta \rangle$, then ϕ is actually an isomorphism from T to $\operatorname{Aut} F$ (both are cyclic of order 4). Hence one of the generators of T will be mapped to our chosen generator β of $\operatorname{Aut} F$: there exists a generator y for T satisfying $y\phi = \beta$. Hence in this case

$$G \cong F \rtimes_\phi T$$

where some generator y of T induces the automorphism β when it acts by conjugation: $y^{-1}xy = x^2$.

All thee groups can definitely be constructed: the homomorphisms ϕ described all exist (as they correspond to the three normal subgroups C_4, C_2 and $\mathbf{1}$, respectively, of the cyclic group $T = C_4$). Hence these semidirect products can indeed be constructed and we have shown that every group G of order 20 with $T \cong C_4$ can be written in one of these forms. Moreover, each of the three possibilities describes a unique group. For example, suppose that $G = F \rtimes_\phi T$ where $F = \langle x \rangle$, $T = \langle y \rangle$ and $y^{-1}xy = x^4$ as in construction (ii). Then every element of G can be unique expressed in the form $g = x^i y^j$ where $0 \leqslant i \leqslant 4$ and $0 \leqslant j \leqslant 3$ (since $G = FT$) and multiplication is completely determined by the facts that $o(x) = 5$, $o(y) = 4$ and $y^{-1}xy = x^4$: A product $x^i y^j \cdot x^k y^\ell$ can be rearranged to one of the required form by repeated use of the conjugation formula.

We must still check that the three groups are not isomorphic to each other (i.e., that we have not by accident constructed the same group twice). First note that the group in (i) is abelian, but the other two semidirect products constructed are non-abelian (as the two elements x and y used do not commute). Let $G = F \rtimes_{\phi} T$ be the group occurring in construction (iii), so $\phi \colon T \to \operatorname{Aut} F$ is an isomorphism, $F = \langle x \rangle$, $T = \langle y \rangle$ and $y\phi = \beta$. Suppose that $g \in \mathrm{Z}(G)$. Since $G = FT$, we can write $g = x^i y^j$ where $0 \leqslant i \leqslant 4$ and $0 \leqslant j \leqslant 3$. Then

$$x = x^g = x^{x^i y^j} = x^{y^j} = x\beta^j.$$

Since an automorphism of F is determined by its effect on x, we deduce $\beta^j = \mathrm{id}_F$ and so $j = 0$. If $i \neq 0$, then some power of $g = x^i$ equals x and we would deduce $x \in \mathrm{Z}(G)$. However, this is not true since $x^y = x^2 \neq x$. This shows that $g = 1$ and we have shown that the group constructed in (iii) has trivial centre.

In the case of the group $G = F \rtimes_{\phi} T$ constructed in (ii), the homomorphism $\phi \colon T \to \operatorname{Aut} F$ has kernel of order 2. We chose y to be a generator for $T \cong C_4$ and so $y^2 \in \ker \phi$. This means that y^2 commutes with x and all its powers. On the other hand, clearly y^2 commutes with all powers of y. Therefore y^2 commutes with all elements of $G = FT$ and so y^2 is a non-identity element of $\mathrm{Z}(G)$ in this case.

We conclude that the two non-abelian groups of order 20 constructed above are not isomorphic to each other as they have different centres. Therefore there are precisely *three* distinct groups of order 20 with cyclic Sylow 2-subgroups.

Case 2: $T \cong C_2 \times C_2$.

If $\phi \colon T \to \operatorname{Aut} F$ in this case, then the image of ϕ must be cyclic as it is a subgroup of $\operatorname{Aut} F = \langle \beta \rangle$ but also every element in $T\phi$ has order dividing 2 (as this is true for all elements of T). Therefore there are just two possibilities: $T\phi = \mathbf{1}$ or $\langle \beta^2 \rangle$.

(i) If $T\phi = \mathbf{1}$, then every element of T commutes with every element of F and so we obtain a direct product:

$$\begin{aligned} G \cong F \times T &= C_5 \times C_2 \times C_2 \\ &\cong C_2 \times C_{10}. \end{aligned}$$

(ii) If $T = \langle \beta^2 \rangle$, then $|\ker \phi| = 2$. Choose an element y that generates $\ker \phi$ and $z \in T \backslash \ker \phi$. Then $y\phi = 1$ and $z\phi = \beta^2$. Note that these two elements y and z generate T and so from these two images we can construct the image of every element of T under ϕ. Thus we have completely determined the semidirect product:

$$G \cong F \rtimes_{\phi} T$$

where two generators y and z for T are such that y commutes with all elements in F and $z^{-1}xz = x\beta^2 = x^4$.

As in Case 1, both these constructions define unique groups. (In fact, the group in construction (ii) is isomorphic to the dihedral group D_{20} of order 20, as is observed on Problem Sheet IV.) In addition, this second group is non-abelian and so is not isomorphic to $C_2 \times C_{10}$. Finally, none of them are isomorphic to any of the three groups in Case 1 since they have different Sylow 2-subgroups.

Conclusion: There are, up to isomorphism, precisely *five* groups of order 20. □

The following example has a more complicated aspect in that ideas from linear algebra become useful.

Example 4.8 In this example, we shall construct a non-abelian group G of order $147 = 3 \cdot 7^2$ with non-cyclic Sylow 7-subgroup. The number of Sylow 7-subgroups in a group of order 147 divides 3 and is congruent to 1 (mod 7). Hence there is a unique Sylow 7-subgroup P. By assumption, $P \cong C_7 \times C_7$.

Now (temporarily) write the group operation in the abelian group P additively, so $P = \mathbb{F}_7 \oplus \mathbb{F}_7$, where $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$ is the field containing 7 elements. Thus we can view P as a vector space of dimension 2 over the field $\mathbb{F}_7$. A homomorphism $P \to P$ then corresponds to a linear transformation, so automorphisms correspond to invertible linear transformations:

$$\operatorname{Aut} P \cong \mathrm{GL}_2(\mathbb{F}_7) = \{\, A \mid A \text{ is a } 2 \times 2 \text{ matrix over } \mathbb{F}_7 \text{ with } \det A \neq 0 \,\}.$$

If z is a generator for the Sylow 3-subgroup of G, then z induces an automorphism of P via conjugation; that is, z induces an invertible linear transformation T of P such that $T^3 = I$. Hence the *minimal polynomial* $m_T(X)$ of T divides

$$X^3 - 1 = (X-1)(X-2)(X-4) \qquad (\text{over } \mathbb{F}_7)$$

and must be of degree at most 2. In particular, $m_T(X)$ is a product of linear factors, so T is diagonalisable. Hence we may choose a basis $\{x, y\}$ for P such that the matrix of T with respect to this basis is

$$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix},$$

where $\lambda, \mu \in \{1, 2, 4\}$. For example, one such group occurs when we select $\lambda = 2$ and $\mu = 4$. Returning to multiplicative notation, with this choice of λ and μ, we will have constructed a semidirect product $(C_7 \times C_7) \rtimes C_3$ with generators x and y for the Sylow 7-subgroup and a generator z for the Sylow 3-subgroup that acts by conjugation in the following way:

$$z^{-1}xz = x^2 \qquad \text{and} \qquad z^{-1}yz = y^4.$$

Wreath products

We finish this chapter by giving another example of the use of the semidirect product construction.

Let G and H be any groups and suppose that G acts on the set $\Omega = \{1, 2, \dots, n\}$. (In fact, we can use any finite set Ω — and with some minor adjustment even an infinite set — but we choose to use this specific set to make the notation more convenient.) Take B to be the direct product of n copies H_i of the group H:

$$B = H_1 \times H_2 \times \cdots \times H_n$$

Elements of B are written as $b = (h_1, h_2, \dots, h_n)$, a sequence of elements of H indexed by Ω; that is,

$$B = \{\, (h_1, h_2, \dots, h_n) \mid h_1, h_2, \dots, h_n \in H \,\}.$$

Now define an action of G on B by permuting the entries of these elements:

$$(h_1, h_2, \dots, h_n)^g = (h_{1g^{-1}}, h_{2g^{-1}}, \dots, h_{ng^{-1}}) \tag{4.1}$$

This formula indicates that applying g move the contents of entry i of the element $b \in B$ into the entry ig in b^g. We verified on Problem Sheet II that this is an action of G.

Recall that the subgroup H_i is identified with the following set of elements of B:

$$H_i = \{ (1, \dots, 1, h, 1, \dots, 1) \mid h \in H \}$$

(where the h is in the ith position). If $g \in G$ has the effect of moving i to j (that is, $ig = j$) and $b = (1, \dots, 1, h, 1, \dots, 1) \in H_i$, then the jth entry of b^g is the entry in position $jg^{-1} = i$ of b. Hence, for this g and b, we compute

$$b^g = (1, \dots, 1, h, 1, \dots, 1) \qquad \text{with } h \text{ in the } j\text{th position.}$$

This shows that

$$H_i^g = H_j = H_{ig}$$

and, in conclusion, we deduce that G permutes the factors of B in the same way as it permutes the elements of Ω.

Write $\phi\colon G \to \mathrm{Sym}(B)$ for the associated permutation representation and let $\phi_g = g\phi$ for $g \in G$; that is,

$$\phi_g\colon (h_1, h_2, \dots, h_n) \mapsto (h_{1g^{-1}}, h_{2g^{-1}}, \dots, h_{ng^{-1}}).$$

In fact, ϕ_g is an automorphism of B because

$$\begin{aligned}\big((h_1, h_2, \dots, h_n)(k_1, k_2, \dots, k_n)\big)^{\phi_g} &= (h_1k_1, h_2k_2, \dots, h_nk_n)^g \\ &= (h_{1g^{-1}}k_{1g^{-1}}, h_{2g^{-1}}k_{2g^{-1}}, \dots, h_{ng^{-1}}k_{ng^{-1}}) \\ &= (h_{1g^{-1}}, h_{2g^{-1}}, \dots, h_{ng^{-1}})(k_{1g^{-1}}, k_{2g^{-1}}, \dots, k_{ng^{-1}}) \\ &= (h_1, h_2, \dots, h_n)^{\phi_g} \cdot (k_1, k_2, \dots, k_n)^{\phi_g}.\end{aligned}$$

This shows that ϕ_g is a homomorphism, while we already know that it is a permutation and consequently bijective. Hence $\phi\colon G \to \operatorname{Aut} B$. We may therefore construct the semidirect product

$$W = B \rtimes_\phi G$$

with respect to this action.

Definition 4.9 Let G and H be groups and let G act on the set $\Omega = \{1, 2, \dots, n\}$. The semidirect product W constructed above is called the *wreath product* of H by G with respect to the action of G on Ω. We shall use the notation $W = H \operatorname{wr}_\Omega G$ to denote this group. The normal subgroup B is usually called the *base group* of the wreath product.

In summary, a wreath product is a special type of semidirect product that is built with normal subgroup B that is a direct product of copies of one of our starting ingredients H and the complement G to B acts to permute the direct factors of B in the same way that it permutes the elements of the set Ω. (The formula (4.1) specifies explicitly how one computes the conjugation of an element of B by an element of H. It is this that we have to depend upon when computing in the wreath product.) We shall use wreath products in our discussion of subgroups of symmetric groups in Chapter 7.

Let us now consider an example of the wreath product construction:

Example 4.10 Let $G = S_2 \cong C_2$ acting on the set $\Omega = \{1, 2\}$ in the natural way. Take $H = \langle a \rangle \cong C_2$. We then construct the wreath product $W = C_2 \operatorname{wr}_\Omega S_2 = C_2 \operatorname{wr}_\Omega C_2$ with respect to this action. The base group of W is

$$B = C_2 \times C_2 = \{(1, 1), (a, 1), (1, a), (a, a)\} \cong V_4.$$

To simplify notation, and in line with what we have done earlier, we shall write elements of W as products $b\sigma$ where $b \in B$ and $\sigma \in S_2$.

Observe that $W = B \rtimes S_2$ is a group of order 8. It is non-abelian because

$$(a, 1)^{(1\ 2)} = (1, a) \neq (a, 1).$$

Hence W is isomorphic to one of the two non-abelian groups of order 8. Observe that W contains many elements of order 2, for example, $(a, 1)$, $(1, a)$, (a, a) and $(1\ 2)$. Hence $W \cong D_8$, the dihedral group of order 8.

As an example of computing within this wreath product, observe that

$$\begin{aligned} \big((a, 1)\,(1\ 2)\big)^2 &= (a, 1)\,(1\ 2)\,(a, 1)\,(1\ 2) \\ &= (a, 1)\,(1, a) \\ &= (a, a). \end{aligned}$$

We conclude that the element $g = (a, 1)\,(1\ 2)$ satisfies $g^4 = 1$ but $g^2 \neq 1$. Hence this g is one of the two elements of order 4 in the wreath product W.

Chapter 5

Soluble Groups

We have already met the concept of a composition series for a group. In this chapter we shall consider groups whose composition factors are all abelian. We can think of this as the class of groups we can build using only abelian groups. To give a general description of these groups we use the following concept.

Definition 5.1 Let G be a group and $x, y \in G$. The *commutator* of x and y is the element

$$[x, y] = x^{-1}y^{-1}xy.$$

Note that the following equations hold immediately:

$$[x, y] = x^{-1}x^{y}$$
$$[x, y] = (y^{-1})^{x}y$$

and

$$xy = yx\,[x, y]. \tag{5.1}$$

The latter tells us that the commutator can be viewed as a measure of by how much x and y fail to commute.

Lemma 5.2 *Let G and H be groups, let $\phi\colon G \to H$ be a homomorphism and let $x, y, z \in G$. Then*

(i) $[x, y]^{-1} = [y, x]$;

(ii) $[x, y]\phi = [x\phi, y\phi]$;

(iii) $[x, yz] = [x, z]\,[x, y]^{z}$;

(iv) $[xy, z] = [x, z]^{y}\,[y, z]$.

Proof: (i) $[x, y]^{-1} = (x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}yx = [y, x]$.

(ii) $[x, y]\phi = (x^{-1}y^{-1}xy)\phi = (x\phi)^{-1}(y\phi)^{-1}(x\phi)(y\phi) = [x\phi, y\phi]$.

(iii) For this and part (iv), we shall rely on Equation (5.1) which we view as telling us how to exchange group elements at the expense of introducing commutators. (This process is known as ‘collection’.) So

$$xyz = yzx\,[x, yz]$$

but if we collect one term at a time we obtain

$$\begin{aligned} xyz &= yx\,[x,y]\,z \\ &= yxz\,[x,y]^z \\ &= yzx\,[x,z]\,[x,y]^z. \end{aligned}$$

Hence

$$yzx\,[x,yz] = yzx\,[x,z]\,[x,y]^z,$$

so

$$[x,yz] = [x,z]\,[x,y]^z.$$

(iv)

$$xyz = zxy\,[xy,z]$$

and

$$\begin{aligned} xyz &= xzy\,[y,z] \\ &= zx\,[x,z]\,y\,[y,z] \\ &= zxy\,[x,z]^y\,[y,z]. \end{aligned}$$

Comparing we deduce

$$[xy,z] = [x,z]^y\,[y,z].$$ □

Both parts (iii) and (iv) can be proved by a more simple-minded expansion of the terms on both sides, but more insight can be obtained with use of the collection process.

Definition 5.3 Let G be a group. The *derived subgroup* (or *commutator subgroup*) G' of G is the subgroup generated by all commutators of elements from G:

$$G' = \langle\, [x,y] \mid x,y \in G\,\rangle.$$

Part (i) of Lemma 5.2 tells us that the inverse of a commutator is again a commutator, but we have no information about products of commutators. Consequently, a typical element of G' has the form

$$[x_1,y_1]\,[x_2,y_2]\dots[x_n,y_n]$$

where $x_i, y_i \in G$ for each i. In general, a product of commutators need not itself be a commutator. There do exist examples of groups where a product of two commutators is not itself a commutator, but they are not so easy to construct and the smallest finite example has order 96. Nevertheless do note that the elements of the derived subgroup are *not* necessarily themselves commutators.

Observe that if $x,y \in G$ are two elements that commute, then $[x,y] = x^{-1}y^{-1}xy = x^{-1}y^{-1}yx = 1$. On the other hand, it follows immediately from Equation (5.1) that if $[x,y] = 1$, then x and y commute. In particular:

Lemma 5.4 *Let G be a group. Then $G' = \mathbf{1}$ if and only if G is an abelian group.* □

We can strengthen this observation in the following key properties that characterize the derived subgroup. This lemma was established in *MT4003*.

Lemma 5.5 *Let G be a group and N be a normal subgroup of G. Then:*

(i) *the derived subgroup G' is a characteristic subgroup of G and hence normal in G;*

(ii) *G/N is abelian if and only if $G' \leqslant N$.*

In particular, G/G' is an abelian group and it is the largest quotient group of G which is abelian. The quotient G/G' is often called the *abelianization* of G.

Proof: (i) By Lemma 5.2(ii), if $x, y \in G$ and ϕ is an automorphism of G, then $[x, y]\phi = [x\phi, y\phi] \in G'$. Since ϕ is a homomorphism, it follows that any product of commutators in G is mapped into G' for ϕ. Thus $G'\phi \leqslant G'$ for all automorphisms ϕ of G and so G' is a characteristic subgroup of G. Therefore $G' \trianglelefteq G$ by Lemma 3.16(i).

(ii) Suppose G/N is abelian. Then

$$Nx \cdot Ny = Ny \cdot Nx \qquad \text{for all } x, y \in G,$$

so

$$N[x, y] = (Nx)^{-1}(Ny)^{-1}(Nx)(Ny) = N1 \qquad \text{for all } x, y \in G.$$

Thus $[x, y] \in N$ for all $x, y \in G$ and we deduce $G' \leqslant N$.

Conversely if $G' \leqslant N$, then $[x, y] \in N$ for all $x, y \in G$ and reversing the above steps shows that G/N is abelian. □

Iterating the construction of the derived subgroup yields the derived series:

Definition 5.6 The *derived series* ($G^{(i)}$) (for $i \geqslant 0$) is the chain of subgroups of the group G defined by

$$G^{(0)} = G$$

and

$$G^{(i+1)} = (G^{(i)})' \qquad \text{for } i \geqslant 0.$$

So $G^{(1)} = G'$, $G^{(2)} = (G')' = G''$, etc. This produces a chain of subgroups

$$G = G^{(0)} \geqslant G^{(1)} \geqslant G^{(2)} \geqslant \cdots .$$

We shall see later that, when G is soluble, this is indeed a series in the sense of Definition 3.1 (in that each term is normal in the previous). In fact, it is a normal series (each term is normal in G) and more: each term is a characteristic subgroup of G.

Definition 5.7 A group G is called *soluble* (*solvable* in the U.S.) if $G^{(d)} = \mathbf{1}$ for some d. The least such d is called the *derived length* of G.

When forming the derived series, we take the derived subgroup at each stage of the previous term. Consequently, once we obtain a repetition then the series is constant from that point. Thus if G is a soluble group of derived length d, its derived series has the form

$$G = G^{(0)} > G^{(1)} > G^{(2)} > \cdots > G^{(d)} = \mathbf{1}$$

with strict inclusions: $G^{(i)}$ is a proper subgroup of $G^{(i-1)}$ for $i = 1, 2, \dots, d$.

Example 5.8 We shall compute the derived series of some familiar groups. The process involves *some* direct computation of commutators combined with the use of Lemma 5.5 that characterizes the derived subgroup.

(i) Let $G = S_4$, the symmetric group of degree 4. Observe

$$[(1\ 2), (1\ 3)] = (1\ 2)\,(1\ 3)\,(1\ 2)\,(1\ 3) = (1\ 3\ 2)$$

and similarly every 3-cycle is a commutator. Since the 3-cycles generate the alternating group, we deduce that $A_4 \leqslant G'$. On the other hand, $S_4/A_4 \cong C_2$, which is abelian, so $G' \leqslant A_4$ by Lemma 5.5. Therefore

$$G' = A_4.$$

We now repeat this process:

$$[(1\ 2\ 3), (1\ 2\ 4)] = (1\ 3\ 2)\,(1\ 4\ 2)\,(1\ 2\ 3)\,(1\ 2\ 4) = (1\ 2)\,(3\ 4)$$

and similarly every product of two disjoint transpositions is a commutator. Hence $V_4 \leqslant G'' = A_4'$. On the other hand, $A_4/V_4 \cong C_3$, which is abelian, so $A_4' \leqslant V_4$ by Lemma 5.5. Therefore

$$G'' = A_4' = V_4.$$

Finally V_4 is an abelian group, so $G''' = V_4' = \mathbf{1}$. Thus the symmetric group S_4 is soluble of derived length 3.

(ii) Let $n \geqslant 5$ and let $G = A_n$, the alternating group of degree n. Then G is a non-abelian simple group. Therefore $G' \neq \mathbf{1}$ but, since G' is a normal subgroup of G, this forces $G' = G$. Hence $G' = A_n$. If we repeat the process, then we will always produce the same subgroup and hence $G^{(i)} = G = A_n$ for all $i \geqslant 0$. We conclude that the alternating group A_n, for $n \geqslant 5$, is not soluble.

To move beyond such computations and to fully understand the properties of a soluble group, we shall produce some equivalent formulations. This will enable us to describe examples of soluble groups more easily. We begin by establishing basic properties of the derived subgroup and the derived series.

Lemma 5.9 (i) *If H is a subgroup of G, then $H' \leqslant G'$.*

(ii) *If $\phi\colon G \to K$ is a homomorphism, then $G'\phi \leqslant K'$.*

(iii) *If $\phi\colon G \to K$ is a surjective homomorphism, then $G'\phi = K'$.*

Proof: (i) If $x, y \in H$, then $[x, y]$ is in particular a commutator of elements from G so belongs to the derived subgroup of G:

$$[x, y] \in G' \qquad \text{for all } x, y \in H.$$

Therefore

$$\langle\, [x, y] \mid x, y \in H \,\rangle \leqslant G',$$

that is, $H' \leqslant G'$.

(ii) This is similar to Lemma 5.5(i). If $x, y \in G$, then $[x, y]\phi = [x\phi, y\phi] \in K'$. Since K' is closed under products, it follows that any product of commutators in G is mapped into K' by the homomorphism ϕ. Thus $G'\phi \leqslant K'$.

(iii) Let $a, b \in K$. Since ϕ is surjective, there exists $x, y \in G$ such that $a = x\phi$ and $b = y\phi$. Thus

$$[a, b] = [x\phi, y\phi] = [x, y]\phi \in G'\phi.$$

Thus

$$[a,b] \in G'\phi \qquad \text{for all } a,b \in K.$$

The image of a subgroup under the homomorphism ϕ is itself a subgroup of the codomain, so we see that $G'\phi$ is a subgroup of K that contains all commutators $[a,b]$ for $a,b \in K$. The definition of the derived subgroup now forces $K' \leqslant G'\phi$. Using (ii) gives $K' = G'\phi$, as required. □

Corollary 5.10 (i) *If H is a subgroup of G, then $H^{(i)} \leqslant G^{(i)}$ for all i.*

(ii) *If $\phi \colon G \to K$ is a surjective homomorphism, then $G^{(i)}\phi = K^{(i)}$ for all i.*

PROOF: We prove both parts by induction on i using the previous lemma as the tool to establish the induction step.

(i) When $i = 0$, the claimed inclusion is $H \leqslant G$ which holds by assumption. Suppose then that $H^{(i)} \leqslant G^{(i)}$ for some $i \geqslant 0$. Apply Lemma 5.9(i) to give

$$(H^{(i)})' \leqslant (G^{(i)})';$$

that is,

$$H^{(i+1)} \leqslant G^{(i+1)}.$$

This completes the induction.

(ii) The assumption that ϕ is a surjective homomorphism tells us that $G\phi = K$. This is the claimed formula when $i = 0$. Now suppose that $G^{(i)}\phi = K^{(i)}$ for some $i \geqslant 0$. Hence, upon restricting the $G^{(i)}$, ϕ induces a surjective homomorphism $G^{(i)} \to K^{(i)}$. Apply Lemma 5.9(iii) to this homomorphism to give

$$(G^{(i)})'\phi = (K^{(i)})';$$

that is,

$$G^{(i+1)}\phi = K^{(i+1)}.$$

This completes the induction. □

We can now deduce the following observation about soluble groups:

Theorem 5.11 *Subgroups and homomorphic images of soluble groups are themselves soluble.*

PROOF: Let G be a soluble group and H be a subgroup of G. The assumption tells us that $G^{(d)} = \mathbf{1}$ for some d. Therefore, using Corollary 5.10(i), since $H^{(d)} \leqslant G^{(d)}$, we obtain $H^{(d)} = \mathbf{1}$ and so we deduce that H is soluble.

Now let K be a homomorphic image of G; that is, there exists a surjective homomorphism $\phi \colon G \to K$. We have assumed $G^{(d)} = \mathbf{1}$ for some d and thus, by Corollary 5.10(ii),

$$K^{(d)} = G^{(d)}\phi = \mathbf{1}\phi = \mathbf{1}.$$

Hence K is soluble. □

It follows that quotient groups (which are the same as homomorphic images) of soluble groups are themselves soluble. There is a rather strong converse to the above lemma as well.

Proposition 5.12 *Let G be a group and N be a normal subgroup of G such that both G/N and N are soluble. Then G is soluble.*

PROOF: Let $\pi \colon G \to G/N$ be the natural map. By assumption $(G/N)^{(d)} = \mathbf{1}$ and $N^{(e)} = \mathbf{1}$ for some d and e. Now, by Corollary 5.10(ii),

$$G^{(d)}\pi = (G/N)^{(d)} = \mathbf{1}.$$

Hence

$$G^{(d)} \leqslant \ker \pi = N.$$

Therefore, by Corollary 5.10(i),

$$(G^{(d)})^{(e)} \leqslant N^{(e)} = \mathbf{1};$$

that is,

$$G^{(d+e)} = \mathbf{1}.$$

Thus G is soluble. □

We have already observed that the derived subgroup G' is a characteristics subgroup of G; that is,

$$G' \operatorname{char} G.$$

Since the terms of the derived series are defined recursively using the derived subgroup (that is, $G^{(i+1)} = (G^{(i)})'$ for all $i \geqslant 0$), it follows that each term of the derived series is characteristic in the previous one:

$$G^{(i)} \operatorname{char} G^{(i-1)} \operatorname{char} G^{(i-2)} \operatorname{char} \cdots \operatorname{char} G^{(1)} \operatorname{char} G^{(0)} = G$$

for all $i \geqslant 0$. Now apply Lemma 3.16(ii) to conclude that each term $G^{(i)}$ of the derived series is a characteristic subgroup (and hence a normal subgroup) of G.

Proposition 5.13 *The derived series*

$$G = G^{(0)} \geqslant G^{(1)} \geqslant G^{(2)} \geqslant \cdots$$

is a chain of subgroups each of which is a characteristic subgroup of G and hence each of which is a normal subgroup of G. □

Consequently, if G is a soluble group of derived length d then its derived series has the form

$$G = G^{(0)} > G^{(1)} > \cdots > G^{(d)} = \mathbf{1}$$

and this is a *normal series* (that is, each term is normal in G). Moreover, each factor has the form

$$G^{(i)}/G^{(i+1)} = G^{(i)}/(G^{(i)})'$$

and this is an abelian group by Lemma 5.5. Thus if G is soluble then it has a normal series with abelian factors. This property fully describes what it means for a group to be soluble:

Theorem 5.14 *Let G be a group. The following conditions are equivalent:*

(i) *G is soluble;*

(ii) *G has a series with abelian factors.*

PROOF: (i) ⇒ (ii): The derived series is such a series (indeed, it is a *normal* series with abelian factors).

(ii) ⇒ (i): Suppose that

$$G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \ldots \geqslant G_n = \mathbf{1}$$

is a series where G_{i-1}/G_i is abelian for all i.

Claim: $G^{(i)} \leqslant G_i$ for all i.

We prove the claim by induction on i. Since $G^{(0)} = G = G_0$, the claim holds for $i = 0$.

Suppose $G^{(i)} \leqslant G_i$ for some $i \geqslant 0$. Now $G_{i+1} \trianglelefteq G_i$ and G_i/G_{i+1} is abelian. Hence $(G_i)' \leqslant G_{i+1}$ by Lemma 5.5. Further, by Lemma 5.9(i), $(G^{(i)})' \leqslant (G_i)'$ and consequently

$$G^{(i+1)} = (G^{(i)})' \leqslant (G_i)' \leqslant G_{i+1}.$$

Therefore, by induction, $G^{(n)} \leqslant G_n = \mathbf{1}$, so $G^{(n)} = \mathbf{1}$ and G is soluble. □

The above theorem provides a general characterization of soluble groups. We shall also describe a characterization of soluble groups in terms of composition series (as introduced in Definition 3.3). Note, however, that the infinite cyclic group is abelian, so soluble, but it does not have a composition series (see Example 3.6). Consequently, we cannot hope for composition series to give us complete information about soluble groups. However, as long as we avoid *infinite* soluble groups, the composition factors do determine whether or not a group is soluble.

Theorem 5.15 *Let G be a group. Then the following conditions are equivalent:*

(i) *G is a finite soluble group;*

(ii) *G has a composition series with all composition factors cyclic of prime order.*

Recall that the abelian simple groups are precisely the cyclic groups of (various) prime orders. Thus condition (ii) describes the groups with abelian composition factors.

PROOF: (ii) ⇒ (i): Let

$$G = G_0 > G_1 > G_2 > \cdots > G_n = \mathbf{1}$$

be a composition series for G and suppose that all the factors are cyclic. This is, in particular, a series for G with abelian factors and so G is soluble by Theorem 5.14. Furthermore,

$$|G| = |G_0/G_1| \cdot |G_1/G_2| \cdot \ldots \cdot |G_{n-1}/G_n|,$$

a product of finitely many primes, so G is finite.

(i) ⇒ (ii): Let G be a finite soluble group. Then by Theorem 5.14, G possesses a series

$$G = G_0 > G_1 > G_2 > \cdots > G_n = \mathbf{1} \tag{5.2}$$

with abelian factors. Now use Corollary 3.8 to refine this to a composition series for G (that is, repeatedly insert additional terms into the series until we cannot insert any more). Observe that if $G_{i+1} < N < G_i$, then N/G_{i+1} is a subgroup of G_i/G_{i+1} and so is abelian, while by the Third Isomorphism Theorem

$$G_i/N \cong \frac{G_i/G_{i+1}}{N/G_{i+1}},$$

which is a quotient of an abelian group and so is abelian. Hence the refinement process preserves the property that the factors are abelian. The result is a composition series for G with abelian factors. Since the only abelian simple groups are cyclic of prime order, we deduce that all the composition factors of G are cyclic of prime order (for various primes). □

This characterization of a finite soluble group in terms of its composition factors gives further insight into our collection of examples given in Example 5.8. For example, we observed that S_4 is soluble but we also know (from Example 3.5(ii)) that its composition factors are C_2 (three times) and C_3. Equally, if G is a non-abelian simple group (for example, $G = A_n$ for $n \geqslant 5$) than G is its only composition factor and so G is not soluble.

The following examples, and non-examples, of soluble groups can also be deduced using the theory that we have developed.

Example 5.16 (i) We have already observed that the symmetric group S_4 of degree 4 is soluble. We know, from Theorem 5.11, that a subgroup of a soluble group is soluble. Hence, for example, the alternating group A_4 of degree 4 and the dihedral group D_8 of order 8 are also soluble.

(ii) Since A_n is not soluble for $n \geqslant 5$, it follows that the symmetric group S_n, for $n \geqslant 5$, is not soluble. (Indeed, the composition factors of S_n are C_2 and A_n.)

(iii) Let $n \geqslant 3$. We shall show that the dihedral group D_{2n} of order $2n$ is soluble. First D_{2n} contains an element α of order n, so $\langle \alpha \rangle$ has index 2 and so is normal. Thus

$$D_{2n} > \langle \alpha \rangle > \mathbf{1}$$

is a series for D_{2n} with both factors cyclic. Hence D_{2n} is soluble by Theorem 5.14.

Careful analysis of the examples at the end of Chapter 2 shows that the groups we considered that were not simple in 2.26–2.28 are also soluble groups.

Hall's Theorem

For the rest of this chapter we shall work only with *finite* soluble groups. Our goal is to prove Hall's Theorem concerning the existence of Hall subgroups in a finite soluble groups. We shall prove this by induction on the group order and one key step will be to take the quotient by a minimal normal subgroup.

Recall from Definition 3.17 that a minimal normal subgroup of a finite group G is a non-trivial normal subgroup M such that if $1 \leqslant N \leqslant M$ with $N \trianglelefteq G$ then either $N = \mathbf{1}$ or $N = M$. Theorem 3.19 tells us that a minimal normal subgroup of a finite group is a direct product of isomorphic simple groups. However, if G is a finite *soluble* group then non-abelian simple groups cannot occur by Theorem 5.15. The only possible simple groups that can occur are cyclic groups of prime order. Thus in a finite soluble group, a minimal normal subgroup is a direct product of cyclic groups of order p (for some prime p). We give a special name to these groups:

Definition 5.17 Suppose that p is a prime number. An *elementary abelian p-group* G is an abelian group such that

$$x^p = 1 \qquad \text{for all } x \in G.$$

Recall from the Fundamental Theorem of Finite Abelian Groups (see *MT4003*) that a finite abelian group is a direct product of cyclic groups. It follows that a finite group is an elementary abelian p-group if and only if

$$G \cong \underbrace{C_p \times C_p \times \dots \times C_p}_{d \text{ times}}$$

for some d. We have therefore observed that combining Theorem 5.15 with Theorem 3.19 gives:

Theorem 5.18 *A minimal normal subgroup of a finite soluble group is an elementary abelian p-group for some prime number p.* □

This result will be used in the induction step of our proof of Hall's Theorem. Before stating that theorem, we describe the type of subgroup with which this theorem is concerned.

Hall subgroups

Definition 5.19 Let π be a set of prime numbers and let G be a finite group. A *Hall π-subgroup* of G is a subgroup H of G such that $|H|$ is a product involving only the primes in π and $|G : H|$ is a product involving only primes not in π.

If p is a prime number, then this definition means that a Hall $\{p\}$-subgroup (that is, when $\pi = \{p\}$ contains just one prime) is precisely the same thing as a Sylow p-subgroup.

Example 5.20 Consider the alternating group A_5 of degree 5. Here

$$|A_5| = 60 = 2^2 \cdot 3 \cdot 5,$$

so a Hall $\{2, 3\}$-subgroup of A_5 has order 12. We already know of a subgroup with this order: namely, A_4 is a Hall $\{2, 3\}$-subgroup of A_5.

A Hall $\{2, 5\}$-subgroup of A_5 would have order 20 and index 3, while a Hall $\{3, 5\}$-subgroup of A_5 would have order 15 and index 4. Suppose that one of these subgroups exists, say H with $|A_5 : H| = r = 3$ or 4. Let A_5 act on the cosets of H to determine a non-trivial homomorphism $\rho \colon A_5 \to S_r$. However A_5 is simple, so necessarily ρ is then injective, but this is impossible as $|A_5| > |S_r|$.

Hence A_5 does not have any Hall π-subgroups for $\pi = \{2, 5\}$ or $\pi = \{3, 5\}$.

So in insoluble groups, some Hall π-subgroups might exist, while others might not (in fact, it is a theorem that some definitely do not!). This is in stark contrast to soluble groups where we shall observe that Hall π-subgroups always do exist:

Theorem 5.21 (P. Hall, 1928) *Let G be a finite soluble group and let π be a set of prime numbers. Then G has a Hall π-subgroup.*

Hall subgroups and this theorem are named after Philip Hall (1904–1982), a British mathematician who did groundbreaking research into the theory of finite and infinite groups in the early and mid-parts of the twentieth century. In fact, he established more properties of Hall subgroups that are analogous to the behaviour of Sylow subgroups. He also showed that, in a finite soluble group G,

(i) any two Hall π-subgroups of G are conjugate, and

(ii) any π-subgroup (that is, a subgroup whose order is a product involving only primes in π) of G is contained in a Hall π-subgroup.

The proofs of these two facts will not be established in this module, but similar methods are used to what we do when proving Theorem 5.21.

A number of tools are needed in the course of this theorem. The one remaining fact that has not already been established is the following result. It first appeared in the study of nilpotent groups (which are discussed in the next chapter). We shall use this lemma in the most complicated step in the proof of Hall's Theorem.

Lemma 5.22 (Frattini Argument) *Let G be a finite group, N be a normal subgroup of G and P be a Sylow p-subgroup of N. Then*

$$G = \mathrm{N}_G(P)\, N.$$

The name of the lemma suggests (correctly) that it is the method of proof that is actually most important here. The idea can be adapted to many situations and turns out to be very useful.

Proof: Let $x \in G$. Since $N \trianglelefteq G$, we have

$$P^x \leqslant N^x = N,$$

so P^x is a Sylow p-subgroup of N. Sylow's Theorem then tells us that P^x and P are conjugate in N:

$$P^x = P^n \qquad \text{for some } n \in N.$$

Therefore

$$P^{xn^{-1}} = P,$$

so $y = xn^{-1} \in \mathrm{N}_G(P)$. Hence $x = yn \in \mathrm{N}_G(P)\, N$. The reverse inclusion is obvious, so

$$G = \mathrm{N}_G(P)\, N. \qquad \square$$

Proof of Theorem 5.21: Let G be a finite soluble group and write $|G| = mn$ where m is a product involving primes in π and n is a product involving primes not in π. We shall show, by induction on the order of G, that G has a subgroup of order m. If $m = 1$, then the trivial subgroup is the subgroup of order m and, in particular, this establishes the base case. We can therefore assume that $m > 1$ and that the result holds for all soluble groups of order less than $|G|$.

Since we are now considering a non-trivial soluble group G, it has a minimal normal subgroup and, by Theorem 5.18, this is elementary abelian. We consider two cases according to the prime dividing the order of a minimal normal subgroup.

Case 1: G possesses a minimal normal subgroup M that is an elementary abelian p-group where $p \in \pi$. Write $|M| = p^\alpha$.

Then

$$|G/M| = mn/p^\alpha = m_1 n,$$

where $m = m_1 p^\alpha$. By induction, G/M has a Hall π-subgroup; that is, a subgroup of order m_1. The Correspondence Theorem tells us this has the form H/M for some subgroup H of G containing M. Then

$$|H/M| = m_1$$

so

$$|H| = m_1 |M| = m_1 p^\alpha = m.$$

Hence H is a Hall π-subgroup of G.

Case 2: No minimal normal subgroup of G is an elementary abelian p-group with $p \in \pi$.

Let M be a minimal normal subgroup of G, so M is an elementary abelian q-group for some prime $q \notin \pi$. Write $|M| = q^\beta$ so

$$|G/M| = mn/q^\beta = mn_1$$

where $n = n_1 q^\beta$. We now further subdivide according to whether or not $n_1 = 1$. (The case when $n_1 = 1$ is the most complicated.)

Subcase 2A: $n_1 \neq 1$.

By induction, G/M has a Hall π-subgroup, which has the form K/M where K is a subgroup of G containing M and

$$|K/M| = m.$$

Then

$$|K| = m|M| = mq^\beta = mn/n_1 < mn.$$

We shall further apply induction to K. This has smaller order than G and hence possesses a Hall π-subgroup. Let H be a Hall π-subgroup of K. Then $|H| = m$, so H is also a Hall π-subgroup of G.

Subcase 2B: $n_1 = 1$, so $|G| = mq^\beta$.

Note also that the general assumption of Case 2 still applies: G has a minimal normal subgroup M with $|M| = q^\beta$ and it has no minimal normal subgroup whose order is a power of a prime in π. The previous steps essentially just depended on careful application of induction. In this case, we need to do far more group theory and we shall establish that our Hall π-subgroup arises in a specific manner.

Now $|G/M| = m > 1$. Let N/M be a minimal normal subgroup of G/M. Then N/M is an elementary abelian p-group for some $p \in \pi$ (since m is a product involving only primes in π), say $|N/M| = p^\alpha$. Then $N \trianglelefteqslant G$, by the Correspondence Theorem, and

$$|N| = p^\alpha q^\beta.$$

Let P be a Sylow p-subgroup of N. Let us now apply the Frattini Argument (Lemma 5.22):

$$G = \mathrm{N}_G(P)\, N.$$

But we know $|P| = p^\alpha$ and $|M| = q^\beta$, so $N = PM$. Hence

$$G = \mathrm{N}_G(P)\, PM = \mathrm{N}_G(P)\, M$$

(as $P \leqslant \mathrm{N}_G(P)$).

Now consider $J = \mathrm{N}_G(P) \cap M$. Since M is abelian, $J \trianglelefteqslant M$. Also since $M \trianglelefteqslant G$, $J = \mathrm{N}_G(P) \cap M \trianglelefteqslant \mathrm{N}_G(P)$. Hence

$$J \trianglelefteqslant \mathrm{N}_G(P)\, M = G.$$

But M is a minimal normal subgroup of G, so $J = \mathbf{1}$ or $J = M$.

If $J = \mathrm{N}_G(P) \cap M = M$, then $M \leqslant \mathrm{N}_G(P)$, so $G = \mathrm{N}_G(P)$. Hence P is a normal p-subgroup of G and some subgroup of P is a minimal normal subgroup of G and this must be an elementary abelian p-group with $p \in \pi$. This is contrary to the general assumption made for Case 2.

Thus $J = \mathbf{1}$, so $\mathrm{N}_G(P) \cap M = \mathbf{1}$. Now

$$mq^\beta = |G| = |\mathrm{N}_G(P)\, M| = |\mathrm{N}_G(P)| \cdot |M|,$$

by Lemma 1.19(iv). Therefore $|\mathrm{N}_G(P)| = m$. Hence $H = \mathrm{N}_G(P)$ is a Hall π-subgroup, which is what we were trying to find.

This completes the induction and establishes the existence of Hall subgroups in a finite soluble group. □

Chapter 6

Nilpotent Groups

In Chapter 5, we defined a collection of subgroups of a group called the derived series using the concept of the commutator

$$[x, y] = x^{-1}y^{-1}xy.$$

In this chapter, we shall define another collection of subgroups and hence define a class of groups called the nilpotent groups. Recall that if $x, y \in G$, then $[x, y] = 1$ if and only if x and y commute.

Definition 6.1 Let A and B be subgroups of a group G. Define the *commutator subgroup* $[A, B]$ by

$$[A, B] = \langle\, [a, b] \mid a \in A,\ b \in B\,\rangle,$$

the subgroup generated by all commutators $[a, b]$ with $a \in A$ and $b \in B$.

In this notation, the derived series is then given recursively by setting $G^{(0)} = G$ and $G^{(i+1)} = [G^{(i)}, G^{(i)}]$ for all integers $i \geqslant 0$. We now make a new definition which is similar but slightly less symmetrical in its form.

Definition 6.2 The *lower central series* $\big(\gamma_i(G)\big)$ (for integers $i \geqslant 1$) is the collection of subgroups of the group G defined by $\gamma_1(G) = G$ and

$$\gamma_{i+1}(G) = [\gamma_i(G), G] \qquad \text{for } i \geqslant 1.$$

Definition 6.3 A group G is called *nilpotent* if $\gamma_{c+1}(G) = \mathbf{1}$ for some c. The least such c is called the *nilpotency class* of G.

It is easy to see that $G^{(i)} \leqslant \gamma_{i+1}(G)$ for all i (by induction on i). Thus if G is nilpotent, then it is soluble. Note also that $\gamma_2(G) = G'$. Consequently, we observe:

Lemma 6.4 *Let G be a group. Then $\gamma_2(G) = \mathbf{1}$ if and only if G is abelian. In particular, the nilpotent groups of class $\leqslant 1$ are precisely the abelian groups.* □

In order that we can study nilpotent groups, we shall need some basic properties of the lower central series. The first two parts are proved by a very similar argument to that used for the derived series in Lemma 5.9 and Corollary 5.10.

Lemma 6.5 (i) *If H is a subgroup of G, then $\gamma_i(H) \leqslant \gamma_i(G)$ for all i.*

(ii) *If $\phi\colon G \to K$ is a surjective homomorphism, then $\gamma_i(G)\phi = \gamma_i(K)$ for all i.*

(iii) *$\gamma_i(G)$ is a characteristic subgroup of G for all i.*

(iv) *The lower central series of G is a chain of subgroups*

$$G = \gamma_1(G) \geqslant \gamma_2(G) \geqslant \gamma_3(G) \geqslant \cdots .$$

In particular, if G is a nilpotent group, then the lower central series

$$G = \gamma_1(G) > \gamma_2(G) > \cdots > \gamma_{c+1}(G) = \mathbf{1}$$

is a normal series for G.

Proof: (i) Proceed by induction on i. Note that $\gamma_1(H) = H \leqslant G = \gamma_1(G)$. If we assume that $\gamma_i(H) \leqslant \gamma_i(G)$, then this together with $H \leqslant G$ gives $[\gamma_i(H), H] \leqslant [\gamma_i(G), G]$, so $\gamma_{i+1}(H) \leqslant \gamma_{i+1}(G)$.

(ii) Again proceed by induction on i. Note that $\gamma_1(G)\phi = G\phi = K = \gamma_1(K)$. Suppose that $\gamma_i(G)\phi = \gamma_i(K)$ for some i. If $x \in \gamma_i(G)$ and $y \in G$, then

$$[x, y]\phi = [x\phi, y\phi] \in [\gamma_i(G)\phi, G\phi] = [\gamma_i(K), K] = \gamma_{i+1}(K),$$

so $\gamma_{i+1}(G)\phi = [\gamma_i(G), G]\phi \leqslant \gamma_{i+1}(K)$.

On the other hand, if $a \in \gamma_i(K)$ and $b \in K$, then $a = x\phi$ and $b = y\phi$ for some $x \in \gamma_i(G)$ and $y \in G$. So

$$[a, b] = [x\phi, y\phi] = [x, y]\phi \in [\gamma_i(G), G]\phi = \gamma_{i+1}(G)\phi.$$

Thus $\gamma_{i+1}(K) = [\gamma_i(K), K] \leqslant \gamma_{i+1}(G)\phi$.

Putting the two inclusions together, We deduce that $\gamma_{i+1}(G)\phi = \gamma_{i+1}(K)$ to complete the inductive step.

(iii) If ϕ is an automorphism of G, then $\phi\colon G \to G$ is, in particular, a surjective homomorphism, so from (ii) we conclude that

$$\gamma_i(G)\phi = \gamma_i(G).$$

Thus $\gamma_i(G) \operatorname{char} G$.

(iv) From (iii), $\gamma_i(G) \trianglelefteq G$. Hence if $x \in \gamma_i(G)$ and $y \in G$, then

$$[x, y] = x^{-1}x^y \in \gamma_i(G).$$

Hence

$$\gamma_{i+1}(G) = [\gamma_i(G), G] \leqslant \gamma_i(G) \qquad \text{for all } i. \qquad \square$$

We deduce two consequences immediately:

Lemma 6.6 *Subgroups and homomorphic images of nilpotent groups are themselves nilpotent.*

Proof: Suppose that $\gamma_{c+1}(G) = \mathbf{1}$ and $H \leqslant G$. Then by Lemma 6.5(i), $\gamma_{c+1}(H) \leqslant \gamma_{c+1}(G) = \mathbf{1}$, so $\gamma_{c+1}(H) = \mathbf{1}$ and H is nilpotent.

If K is a homomorphic image of G, say $\phi\colon G \to K$ is a surjective homomorphism, then Lemma 6.5(ii) tells us that $\gamma_{c+1}(K) = \gamma_{c+1}(G)\phi = \mathbf{1}\phi = \mathbf{1}$, so K is nilpotent. □

In contrast to soluble groups, if N is a normal subgroup of a group G such that G/N and N are both nilpotent, one cannot deduce that G is nilpotent.

Example 6.7 First observe that if G is a nilpotent group of class c then its lower central series has the form

$$G = \gamma_1(G) > \gamma_2(G) > \cdots > \gamma_c(G) > \gamma_{c+1}(G) = \mathbf{1}$$

and by definition $[\gamma_c(G), G] = \gamma_{c+1}(G) = \mathbf{1}$. Hence every element of the last non-trivial term $\gamma_c(G)$ of the lower central series commutes with every element of G; that is $\gamma_c(G) \leqslant \mathrm{Z}(G)$. Thus if G is a non-trivial nilpotent group, then its centre is non-trivial.

We know that $\mathrm{Z}(S_3) = \mathbf{1}$ (as can be shown by a direct computation), so S_3 is *not* nilpotent. However A_3 and $S_3/A_3 \cong C_2$ are both abelian and hence nilpotent.

This last observation tells us that being nilpotent has something to do with non-trivial centre. This idea will enable us to show that every finite p-group is nilpotent. We shall start with the following observation, which was proved in *MT4003* and which we have used regularly on the problem sheets already. However, for completeness we shall give a proof based on group actions.

Lemma 6.8 *Let G be a non-trivial finite p-group. Then the centre $\mathrm{Z}(G)$ of G is non-trivial.*

PROOF: Let G be a finite group of order $|G| = p^n$ for some prime p and some integer $n \geqslant 1$. Let G act on itself by conjugation. It is then the disjoint union of the orbits, which are the conjugacy classes of G:

$$G = \mathscr{C}_1 \cup \mathscr{C}_2 \cup \cdots \cup \mathscr{C}_k$$

The size of each conjugacy class equals the index of the centralizer of an element within it:

$$|\mathscr{C}_i| = |G : \mathrm{C}_G(x_i)|$$

where $x_i \in \mathscr{C}_i$. Hence $|\mathscr{C}_i| = 1$ if and only if $\mathscr{C}_i = \{x_i\} \subseteq \mathrm{Z}(G)$. If $x_i \notin \mathrm{Z}(G)$, then $|G : \mathrm{C}_G(x_i)|$ is a non-trivial power of p. Consequently,

$$p^n = |\mathscr{C}_1| + |\mathscr{C}_2| + \cdots + |\mathscr{C}_k| \equiv |\mathrm{Z}(G)| \pmod{p}.$$

Hence $|\mathrm{Z}(G)| \neq 1$ and so $\mathrm{Z}(G) \neq \mathbf{1}$. □

Proposition 6.9 *A finite p-group is nilpotent.*

PROOF: Let G be a finite p-group, say $|G| = p^n$. We proceed by induction on $|G|$. If $|G| = 1$, then immediately G is nilpotent (as $\gamma_1(G) = G = \mathbf{1}$).

Now suppose $|G| > 1$. Apply Lemma 6.8: $\mathrm{Z}(G) \neq \mathbf{1}$. Consider the quotient group $G/\mathrm{Z}(G)$. This is a p-group of order smaller than G, so by induction it is nilpotent, say

$$\gamma_{c+1}(G/\mathrm{Z}(G)) = \mathbf{1}$$

for some c. Let $\pi \colon G \to G/\mathrm{Z}(G)$ be the natural homomorphism. Then by Lemma 6.5(ii),

$$\gamma_{c+1}(G)\pi = \gamma_{c+1}(G/\mathrm{Z}(G)) = \mathbf{1},$$

so $\gamma_{c+1}(G) \leqslant \ker \pi = \mathrm{Z}(G)$. Thus

$$\gamma_{c+2}(G) = [\gamma_{c+1}(G), G] \leqslant [\mathrm{Z}(G), G] = \mathbf{1},$$

so G is nilpotent. □

The goal in the remainder of this chapter is to demonstrate that essentially all finite groups are built as direct products of p-groups. Consequently, the examples from Proposition 6.9 are in some sense archetypal.

Proposition 6.10 *Let G be a nilpotent group. Then every proper subgroup of G is properly contained in its normalizer:*

$$H < \mathrm{N}_G(H) \qquad \textit{whenever } H < G.$$

PROOF: Let

$$G = \gamma_1(G) \geqslant \gamma_2(G) \geqslant \cdots \geqslant \gamma_{c+1}(G) = \mathbf{1}$$

be the lower central series of G and let H be a proper subgroup of G. Then $\gamma_{c+1}(G) \leqslant H$ but $\gamma_1(G) \nleqslant H$. Choose i as small as possible so that $\gamma_i(G) \leqslant H$. Then $\gamma_{i-1}(G) \nleqslant H$. Now

$$[\gamma_{i-1}(G), H] \leqslant [\gamma_{i-1}(G), G] = \gamma_i(G) \leqslant H,$$

so

$$x^{-1}hxh^{-1} = [x, h^{-1}] \in H \qquad \text{for all } x \in \gamma_{i-1}(G) \text{ and } h \in H.$$

Therefore

$$H^x = \{\, x^{-1}hx \mid h \in H \,\} \leqslant H \qquad \text{for all } x \in \gamma_{i-1}(G).$$

Note that also that $H^{x^{-1}} \leqslant H$ for all $x \in \gamma_{i-1}(G)$, so $H^x = H$ for all $x \in \gamma_{i-1}(G)$. Hence $\gamma_{i-1}(G) \leqslant \mathrm{N}_G(H)$. Therefore, since $\gamma_{i-1}(G) \nleqslant H$, we deduce $\mathrm{N}_G(H) > H$. □

The final lemma we need to analyze the behaviour of nilpotent finite groups is the following observation about Sylow subgroups:

Lemma 6.11 *Let G be a finite group and let P be a Sylow p-subgroup of G for some prime p. Then*

$$\mathrm{N}_G(\mathrm{N}_G(P)) = \mathrm{N}_G(P).$$

PROOF: Let $H = \mathrm{N}_G(P)$. Then $P \trianglelefteq H$, so P is the unique Sylow p-subgroup of H. (Note that as it is a Sylow p-subgroup of G and since $P \leqslant H$, it is also a Sylow p-subgroup of H, as it must have the largest possible order for a p-subgroup of H.) Let $g \in \mathrm{N}_G(H)$. Then

$$P^g \leqslant H^g = H,$$

so P^g is also a Sylow p-subgroup of H and we deduce $P^g = P$; that is, $g \in \mathrm{N}_G(P) = H$. Thus $\mathrm{N}_G(H) \leqslant H$, so we deduce

$$\mathrm{N}_G(H) = H,$$

as required. □

We can now characterise finite nilpotent groups as being built from p-groups in the most simple way.

Theorem 6.12 *Let G be a finite group. Then G is nilpotent if and only if it is the direct product of its Sylow subgroups.*

PROOF: First suppose that G is a nilpotent finite group. Let P be a Sylow p-subgroup of G (for some prime p) and $H = \mathrm{N}_G(P)$. By Lemma 6.11, $\mathrm{N}_G(H) = H$. Hence, by Proposition 6.10, it must be the case that $H = G$; that is, $\mathrm{N}_G(P) = G$ and so $P \trianglelefteqslant G$.

Now if P_1, P_2, ..., P_k are all the Sylow subgroups of G (one for each prime divisor of $|G|$), then we have just observed that each P_i is a normal subgroup of G. Then, with repeated use of Lemma 1.19,

$$P_1 \dots P_{i-1} P_{i+1} \dots P_k$$

is a normal subgroup of G of order $|P_1| \dots |P_{i-1}||P_{i+1}| \dots |P_k|$. This order is not divisible by the prime corresponding to P_i and hence, by Lagrange's Theorem,

$$P_1 \dots P_{i-1} P_{i+1} \dots P_k \cap P_i = \mathbf{1}$$

for each i. Also $G = P_1 P_2 \dots P_k$ (again by the formula from Lemma 1.19) and we have verified the condition to be a direct product:

$$G = P_1 \times P_2 \times \dots \times P_k.$$

Conversely, if $G = P_1 \times P_2 \times \dots \times P_k$ is the direct product of its Sylow subgroups, then a straightforward calculation shows

$$\gamma_i(G) = \gamma_i(P_1) \times \gamma_i(P_2) \times \dots \times \gamma_i(P_k)$$

for each $i \geqslant 1$. Since each P_i is nilpotent by Proposition 6.9, there exists some c such that $\gamma_{c+1}(P_i) = \mathbf{1}$ for each i. Therefore $\gamma_{c+1}(G) = \mathbf{1}$ and G is nilpotent. □

Chapter 7

The Structure of Permutation Groups

In this chapter, we return to the general theme of understanding the action of a group on a set. We begin with the following pair of definitions.

Definition 7.1 (i) Let G be a group and let G act on a set Ω. We say this action is *faithful* if the kernel of the associated permutation representation is trivial.

(ii) If Ω is a set, a *permutation group* on Ω is any subgroup of the symmetric group $\mathrm{Sym}(\Omega)$.

If $\rho \colon G \to \mathrm{Sym}(\Omega)$ is the permutation representation determined by the action of the group G on some set Ω, then the image of ρ certainly is a permutation group on Ω. Moreover,

$$G/\ker\rho \cong \operatorname{im}\rho \leqslant \mathrm{Sym}(\Omega).$$

Consequently, if G acts faithfully on Ω, then $\ker\rho = \mathbf{1}$, so

$$G \cong \operatorname{im}\rho \leqslant \mathrm{Sym}(\Omega).$$

This establishes the first part of the following observations about the above concepts:

Lemma 7.2 (i) *If a group G acts faithfully on a set Ω, then G is isomorphic to a permutation group on Ω.*

(ii) *If G is a permutation group on Ω, then G acts faithfully on Ω (in a natural way).*

Accordingly, this result is saying that the two parts of Definition 7.1 are talking about the same thing. The word "natural" in part (ii) of the lemma just means that we are talking about the obvious action. Indeed:

Proof: (ii) Let $G \leqslant \mathrm{Sym}(\Omega)$. Each element of G is a permutation of Ω, so we can define

$$\begin{aligned} \Omega \times G &\to \Omega \\ (\omega, x) &\mapsto \omega^x \end{aligned}$$

(applying the permutation x to the point ω). Since multiplication in G is composition of maps, this is a group action (see Example 2.2(i) for the case $G = S_n$). Let $\rho \colon G \to \mathrm{Sym}(\Omega)$ be the associated permutation representation, say $\rho \colon x \mapsto \rho_x$, where ρ_x is the permutation

$$\rho_x \colon \omega \mapsto \omega^x \qquad \text{for all } \omega \in \Omega.$$

Consequently, ρ_x is simply the permutation x in $\mathrm{Sym}(\Omega)$ for each $x \in G$. Hence ρ is simply the identity map from G to itself and certainly $\ker \rho = \mathbf{1}$. □

In this chapter, we shall be concerned with the question of what we can say about permutation groups. The simplistic first answer to that question is that we cannot say very much at all: Cayley's Theorem tells us that every group occurs as a subgroup of some symmetric group. Consequently, the collection of all permutation groups is essentially the same as the collection of all groups.

We can, however, make progress if we try to use information about the nature of the action of a permutation group G upon the given set Ω then we can describe structural information about G. We shall phrase much of our discussion about the nature of the actions of a group G on a set Ω, but sometimes we shall assume the action is faithful in order that we can say something about the structure of the group. In some sense, in this chapter we shall investigate the way in which such a group G is embedded in the symmetric group $\mathrm{Sym}(\Omega)$ rather than just stopping at the point where Cayley's Theorem tells us there is an embedding.

Intransitive groups

The following small example illustrates the ideas within this section. Our goal is essentially to understand how the orbits of a permutation group on Ω relate to how it is embedded within the symmetric group $\mathrm{Sym}(\Omega)$.

Example 7.3 Consider $G = \langle (1\ 2)(3\ 4) \rangle \leqslant S_4$ in its natural action on $\Omega = \{1, 2, 3, 4\}$. There are two orbits for G, namely $\Omega_1 = \{1, 2\}$ and $\Omega_2 = \{3, 4\}$. Let $\rho_1 \colon G \to \mathrm{Sym}(\Omega_1)$ and $\rho_2 \colon G \to \mathrm{Sym}(\Omega_2)$ be the permutation representations associated to the induced actions of G on the orbits Ω_1 and Ω_2. By definition, $\big((1\ 2)(3\ 4)\big)\rho_1$ is the permutation on Ω_1 induced by the generator of G. This permutation moves 1 to 2 and 2 to 1, so

$$\big((1\ 2)(3\ 4)\big)\rho_1 = (1\ 2)$$

and similarly $\big((1\ 2)(3\ 4)\big)\rho_2 = (3\ 4)$. We define $G_1 = G\rho_1$ and $G_2 = G\rho_2$, so by our calculation above

$$G_1 = \langle (1\ 2) \rangle \qquad \text{and} \qquad G_2 = \langle (3\ 4) \rangle.$$

Observe that

$$\langle G_1, G_2 \rangle = \langle (1\ 2), (3\ 4) \rangle \cong G_1 \times G_2$$

and that $G = \langle (1\ 2)(3\ 4) \rangle \leqslant \langle G_1, G_2 \rangle$.

We shall observe that the behaviour of an arbitrary intransitive permutation group is very similar to that of the group in Example 7.3.

Let G be a permutation group on Ω; that is, some subgroup of $\mathrm{Sym}(\Omega)$. There is therefore an associated action of G on Ω obtained by applying elements of G to the points in Ω. We shall maintain the standard notation of Chapter 2 for group actions, so we write ω^x for the effect of applying $x \in G$ to ω.

Under the action of G on Ω, we can express Ω as a disjoint union of orbits:

$$\Omega = \Omega_1 \cup \Omega_2 \cup \cdots \cup \Omega_m.$$

Recall that G is *transitive* if there is just one orbit; that is, when $m = 1$. We shall start with the following lemma, which appears as Question 2 on Problem Sheet II:

Lemma 7.4 *Let G be a group that acts on a set Ω and let Γ be an orbit of G on Ω. Then there is an induced action of G on Γ and this action is transitive.*

PROOF: (OMITTED IN LECTURES) Suppose that $\Gamma = \omega^G$ is the orbit of the point ω under the action of G. Define

$$\begin{aligned} \Gamma \times G &\to \Gamma \\ (\gamma, x) &\mapsto \gamma^x; \end{aligned}$$

that is, we apply x to γ under the action of G on Ω. Note that if $\gamma = \omega^g \in \Gamma$, then $\gamma^x = \omega^{gx} \in \Gamma$ also. Hence we genuinely do have a map $\Gamma \times G \to \Gamma$. The fact that this is an action of G on Γ is inherited immediately: $(\gamma^x)^y = \gamma^{xy}$ and $\gamma^1 = \gamma$ for all $\gamma \in \Gamma$ and $x, y \in G$, because these equations hold for all points in Ω.

If $\gamma, \gamma' \in \Gamma$, say $\gamma = \omega^g$ and $\gamma' = \omega^h$, then $\gamma^{g^{-1}h} = \omega^{gg^{-1}h} = \omega^h = \gamma'$. Hence the action of G on the orbit Γ is transitive. □

Consider one of the orbits Ω_i. The lemma tells us that there is an induced transitive action of G on Ω_i. Let $\rho_i \colon G \to \mathrm{Sym}(\Omega_i)$ be the associated permutation representation and $G_i = G\rho_i$ be the image of G in the symmetric group $\mathrm{Sym}(\Omega_i)$. We have thus associated to our permutation group G a number

$$G_1,\ G_2,\ \dots,\ G_m$$

of transitive permutation groups $G_i \leqslant \mathrm{Sym}(\Omega_i)$.

Furthermore, if $h \in \mathrm{Sym}(\Omega_i)$, we can view it as a permutation of Ω by assuming that h fixes all points in $\Omega \setminus \Omega_i$. Thus we extend the definition of h by setting $\omega^h = \omega$ for all $\omega \in \Omega \setminus \Omega_i$. Consequently, we have built various permutation groups

$$G_i \leqslant \mathrm{Sym}(\Omega_i) \leqslant \mathrm{Sym}(\Omega).$$

If $h \in \mathrm{Sym}(\Omega_i)$, then h is a product of cycles that move only points in Ω_i. Since distinct orbits are disjoint, if $h_i \in \mathrm{Sym}(\Omega_i)$ and $h_j \in \mathrm{Sym}(\Omega_j)$ with $i \neq j$, then

$$h_i h_j = h_j h_i \tag{7.1}$$

since disjoint cycles commute.

We can now describe how *intransitive* permutations groups are embedded within the symmetric group:

Theorem 7.5 *Let G be a permutation group on Ω, let $\Omega_1, \Omega_2, \dots, \Omega_m$ be the orbits of G on Ω, and let G_i be the group of permutations induced by G on Ω_i. Then*

(i) *G_i is a transitive permutation group on Ω_i;*

(ii) *$\langle G_1, G_2, \dots, G_m \rangle \cong G_1 \times G_2 \times \dots \times G_m$;*

(iii) *$G \leqslant \langle G_1, G_2, \dots, G_m \rangle$;*

(iv) *for all i, the restriction to G of the projection π_i onto the ith direct factor is surjective (that is, $G\pi_i = G_i$).*

Recall that the projection $\pi_i \colon G_1 \times G_2 \times \dots \times G_m \to G_i$ is given by $(x_1, x_2, \dots, x_m) \mapsto x_i$. A subgroup H of a direct product $G_1 \times G_2 \times \dots \times G_m$ is called a *subdirect product* if $H\pi_i = G_i$ for $i = 1, 2, \dots, m$. Condition (iv) is therefore saying that G is not simply some arbitrary subgroup of the direct product $G_1 \times G_2 \times \dots \times G_m$, but is actually a subdirect product and so can be viewed as rather large.

Proof: We have already shown that G_i is a transitive subgroup of Ω_i. We turn to the other parts of the statement:

(ii) Define $\theta \colon G_1 \times G_2 \times \cdots \times G_m \to \mathrm{Sym}(\Omega)$ by

$$(h_1, h_2, \ldots, h_m) \mapsto h_1 h_2 \ldots h_m.$$

It follows from Equation (7.1) that θ is a homomorphism:

$$\begin{aligned}\big((h_1, h_2, \ldots, h_m)(k_1, k_2, \ldots, k_m)\big)\theta &= (h_1k_1, h_2k_2, \ldots, h_mk_m)\theta \\ &= h_1k_1h_2k_2 \ldots h_mk_m \\ &= h_1h_2 \ldots h_mk_1k_2 \ldots k_m \\ &= (h_1, h_2, \ldots, h_m)\theta \cdot (k_1, k_2, \ldots, k_m)\theta\end{aligned}$$

The image $\operatorname{im}\theta = G_1G_2 \ldots G_m$ is therefore a subgroup of $\mathrm{Sym}(\Omega)$ and it must consequently coincide with $\langle G_1, G_2, \ldots, G_m \rangle$.

If $(h_1, h_2, \ldots, h_m) \in G_1 \times G_2 \times \cdots \times G_m$, then $h = h_1h_2 \ldots h_m$ has the same effect on a point in Ω_i as does h_i (since all the other h_j fix all points in Ω_i). Hence if $h_1h_2 \ldots h_m = 1$ (the identity permutation) then $h_1 = h_2 = \cdots = h_m = 1$. This shows that $\ker\theta = \mathbf{1}$ and we conclude that θ is an isomorphism from the direct product $G_1 \times G_2 \times \cdots \times G_m$ to $\langle G_1, G_2, \ldots, G_m \rangle = G_1G_2 \ldots G_m$. Thus

$$\operatorname{im}\theta = \langle G_1, G_2, \ldots, G_m \rangle \cong G_1 \times G_2 \times \cdots \times G_m.$$

(iii) If $g \in G$, let $g_i = g\rho_i \in G_i$ be the permutation of Ω_i induced by g. If $\omega \in \Omega_i$, then

$$\omega^{g_1g_2\cdots g_m} = \omega^{g_i} = \omega^g,$$

since g_1, …, g_{i-1}, g_{i+1}, …, g_m fix all points of Ω_i. Hence

$$\omega^{g_1g_2\cdots g_m} = \omega^g \qquad \text{for all } \omega \in \Omega.$$

Therefore $g = g_1g_2 \ldots g_m$ (since these permutations have the same effect on points in Ω). Hence every element $g \in G$ lies in $\operatorname{im}\theta = \langle G_1, G_2, \ldots, G_m \rangle$; that is,

$$G \leqslant \langle G_1, G_2, \ldots, G_m \rangle.$$

(iv) Fix $i = 1$, 2, …, m and let $h \in G_i$. Then $h = g\rho_i$ for some $g \in G$. Let us write this g as $g = g_1g_2 \ldots g_m$ as in part (iii) where $g_j = g\rho_j$ for each j. In particular, $g_i = h$. This is the unique expression of g as a product of elements from each G_j as provided by the direct product and the projection map π_i maps g to g_i; that is, $g\pi_i = g_i = h$. Hence the restriction of π_i to G is surjective, as claimed. This shows G is a subdirect product of the subgroups G_1, G_2, …, G_n. □

In conclusion, if G is an intransitive permutation group, then it embeds in the direct product of a number of transitive permutation groups of smaller degree. In some sense, this reduces the study of arbitrary permutation groups to the study of transitive groups and an understanding of direct products.

Transitive groups

In view of what we have just achieved, namely showing how the study of an intransitive permutation group can be reduced to studying a number of transitive groups, we shall work with transitive permutation groups for the remainder of this chapter. We shall start with a refinement of the Orbit-Stabilizer Theorem that characterizes the action of a transitive group.

The following terminology is used in the refinement that we present. It is useful when discussing group actions and permutation groups.

Definition 7.6 (i) Let G be a group that has actions on two sets Ω and Ω'. We say that these actions are *equivalent* if there is a bijection $\phi\colon \Omega \to \Omega'$ such that

$$(\omega^x)\phi = (\omega\phi)^x \qquad \text{for all } \omega \in \Omega \text{ and } x \in G.$$

(ii) Let G be a permutation group on a set Ω and H be a permutation group on a set Ω'. We say that G and H are *permutation isomorphic* if there is a bijection $\phi\colon \Omega \to \Omega'$ and an isomorphism $\theta\colon G \to H$ such that

$$(\omega^x)\phi = (\omega\phi)^{x\theta} \qquad \text{for all } \omega \in \Omega \text{ and } x \in G.$$

We can interpret both parts of the definition as saying the actions are essentially the same. The two concepts are closely linked with each other. Indeed, if the actions of G on two sets Ω and Ω' are equivalent, then the two permutations groups obtained via the associated permutations representations turn out to be permutation isomorphic. (See Problem Sheet VII for more details.)

Theorem 7.7 (Orbit-Stabilizer Theorem, Improved) *Let G be a group that acts transitively on a set Ω and let $\omega \in \Omega$. Let Ω' be the set of cosets of the stabilizer G_ω and let G act on Ω' by right multiplication. Then these actions of G are equivalent.*

PROOF: In our original proof of the Orbit-Stabilizer Theorem (Theorem 2.9) we showed that

$$\begin{aligned} \phi\colon \Omega' &\to \Omega \\ G_\omega g &\mapsto \omega^g \end{aligned}$$

is a well-defined bijection. In fact, it is an equivalence between the actions of G on Ω' and Ω as the following calculation shows: If $g, x \in G$, then

$$(G_\omega g x)\phi = \omega^{gx} = (\omega^g)^x = \big((G_\omega g)\phi\big)^x.$$

Hence the actions of G on Ω' and Ω are equivalent. □

This theorem then tells us that any transitive action of a group G is essentially the same as its action on the cosets of some subgroup. Conversely, we also observed in Theorem 2.23 that the action of a group G on the cosets of a subgroup H is always transitive.

A special case of transitive action will be significant later in the chapter. We introduce the relevant terminology here.

Definition 7.8 Let G be a group that acts on the set Ω. We say that this action is *regular* (and that G acts *regularly* on Ω) if G is transitive on Ω and the stabilizer G_ω is trivial for all $\omega \in \Omega$.

Recall that if G acts transitively on Ω then the stabilizers are all conjugate in G (see Proposition 2.10). Hence to show that a transitive is regular, it suffices to show that one stabilizer is trivial. Recall from Example 2.20 that the right regular action of a group is an example of a transitive action that is regular (hence the name of that action). In fact, the following shows that this is essentially the only regular action.

Lemma 7.9 *Suppose that G acts regularly on the set Ω. Then the action of G on Ω is equivalent to the right regular action of G on itself. In particular, if $\omega \in \Omega$, every element of Ω is uniquely expressible as ω^x for $x \in G$ and $|\Omega| = |G|$.*

Proof: This follows immediately from Theorem 7.7. If $\omega \in \Omega$, the stabilizer $G_\omega = \mathbf{1}$ and hence the theorem says the bijection $\phi \colon G \to \Omega$ given by $g \mapsto \omega^g$ has the required property to establish the actions are equivalent. In particular, $|\Omega| = |G|$. □

Before discussing transitive groups in more detail, we shall establish the following fact that will also be used later in the chapter.

Lemma 7.10 *Let G be a group that acts transitively on a set Ω, H be a subgroup of G and $\omega \in \Omega$. Then the induced action of H on Ω is transitive if and only if $G = G_\omega H$.*

Proof: Suppose H is transitive on Ω. Let $g \in G$. Then $\omega^g \in \Omega$ is, by assumption, in the same orbit as ω under the action of H, so $\omega^g = \omega^h$ for some $h \in H$. Then $\omega^{gh^{-1}} = \omega$, so gh^{-1} belongs to the stabilizer G_ω. Hence $g = (gh^{-1})h \in G_\omega H$. Therefore $G = G_\omega H$.

Conversely, suppose that $G = G_\omega H$. Since G acts transitively on Ω, we calculate

$$\Omega = \omega^G = \omega^{G_\omega H} = \omega^H$$

(since every element of G_ω fixes ω). Hence H acts transitively on Ω. □

Blocks

We shall use the following concept to analyze the action of a transitive group.

Definition 7.11 Let G be a group that acts transitively on a set Ω. A *block* for G is a non-empty set Δ of Ω such that, for every $x \in G$, either $\Delta^x = \Delta$ or $\Delta^x \cap \Delta = \varnothing$.

Recall that G acts transitively on Ω, so there is only one orbit. What blocks enable us to do is further break down the action since we obtain a partition of the set Ω that interacts well with the action. We first establish the existence of the partition:

Lemma 7.12 *Let G be a group that acts transitively on a set Ω. If Δ is a block, then $\Sigma = \{\, \Delta^x \mid x \in G \,\}$ is a partition of Ω.*

Proof: Fix some $\delta \in \Delta$. If $\omega \in \Omega$, then as G acts transitively, there exists $x \in G$ such that $\omega = \delta^x$. Therefore $\omega \in \Delta^x$. Hence Ω is the union of the sets in Ω.

Suppose $\Delta^x \cap \Delta^y \neq \varnothing$. Apply y^{-1} to deduce $\Delta^{xy^{-1}} \cap \Delta \neq \varnothing$. Since Δ is a block, this shows that $\Delta^{xy^{-1}} = \Delta$. Applying y then shows that $\Delta^x = \Delta^y$. We conclude that the members of Σ are either disjoint or equal and it follows that Ω is indeed the disjoint union of the members of Σ. □

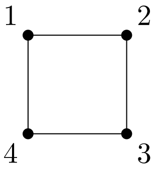
Definition 7.13 Let G be a group that acts transitively on Ω. If Δ is a block for G, we call the set $\Sigma = \{\, \Delta^x \mid x \in G \,\}$ a *system of blocks.*

We have observed that every block gives rise to a system of blocks. In practice, it is often easier to find the system of blocks Σ for a group G (that is, the partition of Ω preserved by G), observe that G permutes the members of this system and hence deduce that each member of Σ is a block.

We now present some trivial examples of blocks and other examples that illustrate how they arise.

Example 7.14 (i) Let G be any group acting transitively on any set Ω. Observe that Ω is a block since $\Omega^x = \Omega$ for all $x \in G$. If $\omega \in \Omega$, then $\Delta = \{\omega\}$ is a block since if x fixes ω, then $\Delta^x = \Delta$ and if $\omega^x \neq \omega$, then $\Delta^x \cap \Delta = \varnothing$. The whole set Ω and the singletons $\{\omega\}$ are called *trivial blocks.*

(ii) Let $G = D_8$, the dihedral group of order 8, viewed as a subgroup of S_4 via the following (standard) labelling of the square:



Take $\Delta = \{1, 3\}$. If $x \in D_8$, then x moves the points in Δ to opposite vertices of the square; that is, $\Delta^x = \{1, 3\}$ or $\{2, 4\}$. Thus Δ is a block for this action.

Observe that $\Gamma = \{1, 2\}$ is *not* a block, because upon applying a rotation clockwise through an angle of $\pi/2$ we calculate $\Gamma^{(1\ 2\ 3\ 4)} = \{2, 3\}$ which meets Γ in a single point.

(iii) Let Ω_1 and Ω_2 be sets with $|\Omega_1|, |\Omega_2| > 1$. Let $\Omega = \Omega_1 \times \Omega_2$ and take $G = \mathrm{Sym}(\Omega_1) \times \mathrm{Sym}(\Omega_2)$. We define an action of G on Ω by

$$(\alpha, \beta)^{(x,y)} = (\alpha^x, \beta^y)$$

for $\alpha \in \Omega_1$, $\beta \in \Omega_2$, $x \in \mathrm{Sym}(\Omega_1)$, $y \in \mathrm{Sym}(\Omega_2)$. It is straightforward to verify this is an action.)

[(Omitted in lectures) The verification is as follows:

$$\begin{aligned}\big((\alpha, \beta)^{(x_1,y_1)}\big)^{(x_2,y_2)} &= (\alpha^{x_1}, \beta^{y_1})^{(x_2,y_2)} \\ &= \big((\alpha^{x_1})^{x_2}, (\beta^{y_1})^{y_2}\big) \\ &= (\alpha^{x_1 x_2}, \beta^{y_1 y_2}) \\ &= (\alpha, \beta)^{(x_1 x_2, y_1 y_2)} \\ &= (\alpha, \beta)^{(x_1,y_1)(x_2,y_2)}\end{aligned}$$

and

$$(\alpha, \beta)^{(1,1)} = (\alpha^1, \beta^1) = (\alpha, \beta).]$$

This action is transitive since if $\alpha_1, \alpha_2 \in \Omega_1$ and $\beta_1, \beta_2 \in \Omega_2$, there exist $x \in \mathrm{Sym}(\Omega_1)$ and $y \in \mathrm{Sym}(\Omega_2)$ with $\alpha_1^x = \alpha_2$ and $\beta_1^y = \beta_2$ and then $(\alpha_1, \beta_1)^{(x,y)} = (\alpha_2, \beta_2)$.

Fix $\alpha \in \Omega_1$ and define

$$\Delta = \{\alpha\} \times \Omega_2 = \{\, (\alpha, \omega) \mid \omega \in \Omega_2 \,\}.$$

If $(x, y) \in G$, then $\Delta^{(x,y)} = \{\alpha^x\} \times \Omega_2$. Hence $\Delta^{(x,y)} = \Delta$ when x fixes α and $\Delta^{(x,y)} \cap \Delta = \varnothing$ when $\alpha^x \neq \alpha$. This shows that Δ is a block for the direct product G acting on the set $\Omega = \Omega_1 \times \Omega_2$. Our assumption that $|\Omega_1|, |\Omega_2| > 1$ ensures that this Δ is a non-trivial block.

Similarly sets of the form $\Gamma = \Omega_1 \times \{\beta\}$, for $\beta \in \Omega_2$, are non-trivial blocks for this action of G on Ω.

NOTE: This action of $G = \mathrm{Sym}(\Omega_1) \times \mathrm{Sym}(\Omega_2)$ on $\Omega = \Omega_1 \times \Omega_2$ is transitive. It should not be confused with the *intransitive* action of G on $\Omega_1 \cup \Omega_2$ considered earlier, see Theorem 7.5.

Lemma 7.15 *Let G be a group that acts transitively on a set Ω. If N is a normal subgroup of G and $\omega \in \Omega$, then the orbit $\Delta = \omega^N$ of ω under the action of N is a block for G.*

PROOF: If $x \in G$, then $Nx = xN$ since $N \trianglelefteqslant G$. Hence

$$\Delta^x = \omega^{Nx} = \omega^{xN} = (\omega^x)^N,$$

the orbit of ω^x under the action of N. Since orbits of N are either disjoint or equal, we conclude either $\Delta^x \cap \Delta = \varnothing$ or $\Delta^x = \Delta$. Hence Δ is a block for G. □

Blocks arise in the classification and description of transitive groups in the following definition.

Definition 7.16 Let G be a group that acts transitively on the set Ω. We say that G acts *imprimitively* on Ω if there is some non-trivial block Δ for G. If, on the other hand, the only blocks for G are the trivial ones (as in Example 7.14(i)), then we say that G acts *primitively* on Ω.

Lemma 7.17 *Let G be a group that acts transitively on a set Ω.*

(i) *If H is a subgroup of G that contains the stabilizer G_ω of some point $\omega \in \Omega$, then ω^H is a block for G.*

(ii) *If Δ is a block for G that contains some point ω, then $\Delta = \omega^H$ for some subgroup H of G with $G_\omega \leqslant H$.*

PROOF: (i) Suppose $G_\omega \leqslant H \leqslant G$. Take $\Delta = \omega^H = \{\, \omega^h \mid h \in H \,\}$. Suppose $\Delta^x \cap \Delta \neq \varnothing$ for some $x \in G$. Then there exists $\delta \in \Delta$, say $\delta = \omega^h$ where $h \in H$, such that $\delta^x \in \Delta$. Then $\omega^{hx} = \omega^k$ for some $k \in H$, so $hxk^{-1} \in G_\omega \leqslant H$. Since $h, k \in H$, we deduce $x \in H$. Therefore

$$\Delta^x = \{\, \omega^{hx} \mid h \in H \,\} = \omega^H = \Delta$$

because $Hx = H$. It follows that Δ is a block for G.

(ii) Let Δ be a block for G that contains ω. Define $H = \{\, x \in G \mid \omega^x \in \Delta \,\}$. Then $1 \in H$ because $\omega^1 = \omega \in \Delta$. Let $x, y \in H$. Then $\omega^x \in \Delta \cap \Delta^x$ and we deduce $\Delta^x = \Delta$. Similarly $\Delta^y = \Delta$. Hence $\Delta^{xy} = (\Delta^x)^y = \Delta^y = \Delta$ and $\Delta^{x^{-1}} = \Delta^{xx^{-1}} = \Delta$. From this, we deduce $\omega^{xy}, \omega^{x^{-1}} \in \Delta$ and hence $xy, x^{-1} \in H$. This shows that H is a subgroup of G. Furthermore H contains the stabilizer G_ω as $\omega^x = \omega \in \Delta$ for all $x \in G_\omega$.

Now by definition $\omega^x \in \Delta$ for all $x \in H$. If $\delta \in \Delta$, then $\delta = \omega^x$ for some $x \in G$ (as G acts transitively) and this x belongs to H by definition. We conclude that $\Delta = \omega^H$ for the subgroup H just constructed. □

This lemma enables us to establish the following theorem.

Theorem 7.18 *Let G be a group that acts transitively on Ω and let $\omega \in \Omega$. Then there is a one-one inclusion-preserving correspondence between the set of subgroups of G that contain the stabilizer G_ω and the set of blocks for G that contain ω. This correspondence is given by*

$$H \mapsto \omega^H \qquad \text{for } H \geqslant G_\omega.$$

PROOF: By Lemma 7.17(i), the map $\phi\colon H \mapsto \omega^H$ is a function from the set of subgroups of G containing G_ω to the set of blocks containing ω. Part (ii) of the lemma tells us that ϕ is surjective.

Suppose that H and K are subgroups of G containing G_ω. If $H \leqslant K$, then by definition $\omega^H \subseteq \omega^K$. Conversely suppose that $H\phi \subseteq K\phi$; that is, $\omega^H \subseteq \omega^K$. If $h \in H$, then $\omega^h \in \omega^H = \omega^K$, so $\omega^h = \omega^k$ for some $k \in K$. Then $\omega^{hk^{-1}} = \omega$, so $hk^{-1} \in G_\omega \leqslant K$. We deduce $h = (hk^{-1})k \in K$. This shows $H \leqslant K$. Hence

$$H \leqslant K \qquad \text{if and only if} \qquad \omega^H \subseteq \omega^K;$$

that is, ϕ preserves inclusions.

In particular, if $H\phi = K\phi$ the above (applied to the inclusions $H\phi \subseteq K\phi$ and $K\phi \subseteq H\phi$) shows that $H = K$. We conclude that ϕ is injective, which completes the proof of the theorem. □

We are now able to characterize primitivity in terms of the stabilizers of points. It will depend upon the following term (which also appeared earlier on Problem Sheet VI in the context of nilpotent groups):

Definition 7.19 A *maximal subgroup* of a group G is a proper subgroup $M < G$ such that there is no subgroup H with $M < H < G$.

Corollary 7.20 *Let G be a group that acts transitively on a set Ω with $|\Omega| > 1$. Then G acts primitively on Ω if and only if every stabilizer G_ω (for $\omega \in \Omega$) is maximal in G.*

To place this corollary in context, recall that Theorem 7.7 tells us that a transitive action is equivalent to the action on the cosets of a subgroup (namely the stabilizer G_ω of any point ω). We are now observing furthermore that it is primitive when this subgroup is maximal.

PROOF: Since G acts transitively, $|G : G_\omega| = |\Omega| > 1$, so G_ω is a proper subgroup of G.

Suppose first that G is imprimitive in its action on Ω. Then there is some non-trivial block Δ for G. Let $\omega \in \Delta$. Then $\{\omega\} \subset \Delta \subset \Omega$ are blocks containing ω, so by Theorem 7.18, Δ corresponds to a subgroup H with $G_\omega < H < G$. In particular, the stabilizer G_ω is not maximal in G. (Since the stabilizers are conjugate — see Proposition 2.10 — they are consequently *all* not maximal.)

Conversely, suppose some stabilizer G_ω is not maximal in G. Then there is a subgroup H of G with $G_\omega < H < G$. Applying Theorem 7.18, we conclude $\Delta = \omega^H$ is a block for G with $\{\omega\} \subset \omega^H \subset \Omega$. Hence Δ is a non-trivial block and so G acts imprimitively on Ω.

By taking the contrapositive, we have established the characterization of primitive groups. □

The reason for the presence of the assumption that Ω contains more than one point is to avoid a trivial case. If $\Omega = \{\omega\}$, then all elements of the group G fix ω (as there is only one point!), so the stabilizers G_ω all equal G. The action is primitive here (as there are no non-empty subsets of Ω except for a singleton), but the stabilizer G_ω is not maximal because it is not a *proper* subgroup.

Imprimitive groups

Our next goal is to describe the structure of transitive groups that are imprimitive. This should be viewed as analogous to our descriptions of intransitive groups in Theorem 7.5. This description will be expressed in terms of wreath products, as introduced in Chapter 4, and so we start by looking at these groups.

Let H be a permutation group on a set Δ and K be a permutation group on a set $\Sigma = \{1, 2, \dots, n\}$; that is, $H \leqslant \mathrm{Sym}(\Delta)$ and $K \leqslant \mathrm{Sym}(\Sigma)$. Let

$$\Omega = \Delta \times \Sigma = \{\, (\delta, i) \mid \delta \in \Delta,\ 1 \leqslant i \leqslant n \,\}.$$

Then we can express Ω as the union

$$\Omega = \bigcup_{i=1}^{n} (\Delta \times \{i\})$$

of n disjoint sets that are in one-one correspondence with Δ. Let $W = H \operatorname{wr}_\Sigma K$ be the wreath product of H by K with respect to the action of K on Σ. Thus W is the semidirect product

$$W = B \rtimes K$$

where the base group $B = \{\, (h_1, h_2, \dots, h_n) \mid h_i \in H \,\}$ is a direct product of n copies of H and where the action of K on B is given by permuting the entries:

$$(h_1, h_2, \dots, h_n)^k = (h_{1k^{-1}}, h_{2k^{-1}}, \dots, h_{nk^{-1}})$$

for $(h_1, h_2, \dots, h_n) \in B$ and $k \in K$.

We shall now construct an action of W on Ω. If $g = (h_1, h_2, \dots, h_n)k \in W$ where $h_1, h_2, \dots, h_n \in H$ and $k \in K$, define

$$(\delta, i)^g = (\delta^{h_i}, ik); \tag{7.2}$$

that is, apply the ith element h_i to $\delta \in \Delta$ and apply the permutation k to $i \in \Sigma$. (We are mixing notation by writing the action of H as exponentiation, but that of K as juxtaposition. It will keep later notation cleaner to do so!) If $g = (h_1, h_2, \dots, h_n)k$ and $g' = (h'_1, h'_2, \dots, h'_n)k'$ are elements of W, then

$$\begin{aligned} gg' &= (h_1, h_2, \dots, h_n)k(h'_1, h'_2, \dots, h'_n)k' \\ &= (h_1, h_2, \dots, h_n)(h'_1, h'_2, \dots, h'_n)^{k^{-1}} kk' \\ &= (h_1, h_2, \dots, h_n)(h'_{1k}, h'_{2k}, \dots, h'_{nk})kk' \\ &= (h_1 h'_{1k}, h_2 h'_{2k}, \dots, h_n h'_{nk})kk'. \end{aligned}$$

Then

$$\begin{aligned} \big((\delta, i)^g\big)^{g'} &= (\delta^{h_i}, ik)^{g'} \\ &= (\delta_{h_i h'_{ik}}, ikk') \\ &= (\delta, i)^{gg'}. \end{aligned}$$

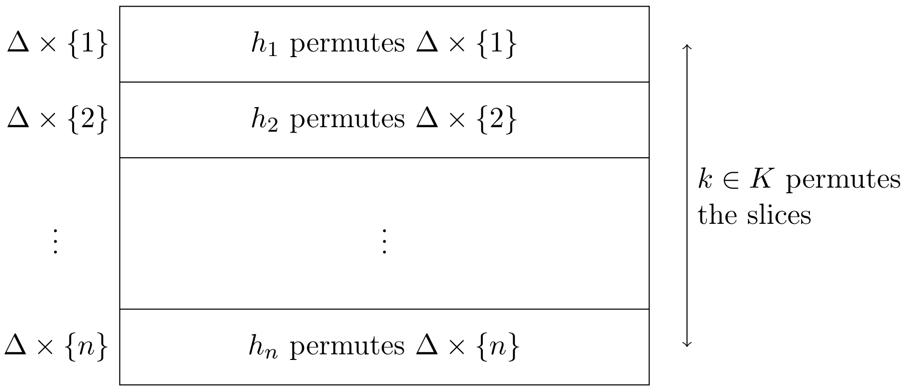

$\Delta \times \{1\}$
h_1 permutes $\Delta \times \{1\}$
$\Delta \times \{2\}$
h_2 permutes $\Delta \times \{2\}$
$\vdots$
$\vdots$
$\Delta \times \{n\}$
h_n permutes $\Delta \times \{n\}$
$k \in K$ permutes the slices

Figure 7.1: The imprimitive action of the wreath product W on $\Omega = \Delta \times \Sigma$

The identity element of W is $(1, 1, \ldots, 1)1$ and this fixes all elements of Ω. Hence W acts on the set Ω.

If $g = (h_1, h_2, \ldots, h_n)k$ is a non-identity element of W, then either there is some i such that $h_i \neq 1$, so h_i moves some point $\delta \in \Delta$, or $k \neq 1$, so k moves some point $i \in \Sigma$. Hence there exists $(\delta, i) \in \Omega$ such that $(\delta, i)^g = (\delta^{h_i}, ik) \neq (\delta, i)$. This show that the action of W on Ω is faithful.

If H acts transitively on Δ and K acts transitively on Σ, then this action of W on Ω is also transitive. If $(\delta, i), (\delta', j) \in \Omega$, take any $h_i \in H$ with $\delta^{h_i} = \delta'$ and $k \in K$ with $ik = j$. Then $g = (\ldots, h_i, \ldots)k$ moves (δ, i) to (δ', j), no matter what we choose for the other elements of H appearing within g. On the other hand, if $g = bk$ with $b \in B$ and $k \in K$, then the formula (7.2) for the action tells us that

$$(\Delta \times \{i\})^g = \Delta \times \{ik\}.$$

It follows that $\Delta \times \{i\}$ is a block for W. It is a non-trivial block provided $|\Delta|, |\Sigma| > 1$.

We record our observations:

Lemma 7.21 *Let H and K be transitive permutation groups on the sets Δ and $\Sigma = \{1, 2, \ldots, n\}$, respectively, where $|\Delta|, |\Sigma| > 1$. Then the wreath product $W = H \operatorname{wr}_\Sigma K$ acts transitively and faithfully, but imprimitively on the set $\Omega = \Delta \times \Sigma$ by the formula*

$$(\delta, i)^g = (\delta^{h_i}, ik)$$

for $\delta \in \Delta$, $i \in \Sigma$ and $g = (h_1, h_2, \ldots, h_n)k \in W$. □

We call this the *imprimitive action* of the wreath product W on $\Delta \times \Sigma$. To understand this action, one can think of the index from Σ as providing a way to slice the set Ω into copies of Δ. The entries of each element $b = (h_1, h_2, \ldots, h_n)$ of the base group act independently on each slice: b permutes the entries of $\Delta \times \{i\}$ in the same way as h_i acts on Δ. An element $g = (h_1, h_2, \ldots, h_n)k$ of the wreath product W first shuffles the points in each slice $\Delta \times \{i\}$ according to the element $h_i \in H$ and then k permutes the slices. See Figure 7.1 for an illustration of this action of the wreath product. Since the action is faithful, Lemma 7.2 tells us that we can identify W with a subgroup of $\operatorname{Sym}(\Delta \times \Sigma)$.

We complete our discussion of imprimitive permutation groups by observing that every imprimitive permutation group can be viewed as being contained within a wreath product. Thus wreath products are maximal amongst the *imprimitive* permutation groups.

Theorem 7.22 *Let G be a permutation group that acts transitively on a finite set Ω and let Δ be a block for G. Let $\Sigma = \{1, 2, \dots, n\}$ where n is the number of blocks in the system obtained from Δ. Then G is contained in a subgroup of $\mathrm{Sym}(\Omega)$ that is permutationally isomorphic to a wreath product $\mathrm{Sym}(\Delta) \mathbin{\mathrm{wr}_\Sigma} \mathrm{Sym}(\Sigma)$ in its imprimitive action on $\Delta \times \Sigma$.*

Proof: Let $\Sigma' = \{\, \Delta^x \mid x \in G \,\}$ be the system of blocks determined by Δ and write $\Sigma' = \{\Delta_1, \Delta_2, \dots, \Delta_n\}$. (We have used the finiteness of Ω at this point to ensure that Σ' contains only finitely many blocks.) If $\Delta_i = \Delta^y \in \Sigma'$, then $\Delta_i^x = \Delta^{yx} \in \Sigma'$ for all $x \in G$. Moreover, if $\gamma \in \Delta_i$ and $\delta \in \Delta_j$, then by transitivity there exists $x \in G$ such that $\gamma^x = \delta$. Therefore, as these are blocks, $\Delta_i^x = \Delta_j$. We conclude that G acts transitively on Σ'. Hence there is an associated permutation representation $\rho\colon G \to S_n$ satisfying

$$\Delta_i^x = \Delta_{i(x\rho)}$$

for each $i \in \Sigma = \{1, 2, \dots, n\}$ and $x \in G$.

Take $\Omega' = \Delta \times \Sigma$. There is a bijection $\phi\colon \Omega \to \Omega'$ that maps each Δ_i bijectively to $\Delta \times \{i\}$. This bijection ϕ determines an isomorphism $\theta\colon \mathrm{Sym}(\Omega) \to \mathrm{Sym}(\Omega')$ by

$$\theta\colon \sigma \mapsto \phi^{-1}\sigma\phi.$$

Let $W = \mathrm{Sym}(\Delta) \mathbin{\mathrm{wr}_\Sigma} \mathrm{Sym}(\Sigma)$ be the wreath product and view it is as subgroup of $\mathrm{Sym}(\Omega')$ via the imprimitive action as descibed in Lemma 7.21.

Claim: $G\theta \leqslant W$

Indeed, if $g \in G$ and $i \in \Sigma$, then

$$(\Delta \times \{i\})^{g\theta} = (\Delta \times \{i\})^{\phi^{-1}g\phi} = \Delta_i^{g\phi} = \Delta_{i(g\rho)}^{\phi} = \Delta \times \{i(g\rho)\}.$$

Note that, according to the imprimitive action of the wreath product, $g\rho \in \mathrm{Sym}(\Sigma)$ permutes the sets $\Delta \times \{i\}$ by moving the second factor. Hence

$$(\Delta \times \{i\})^{(g\theta)(g\rho)^{-1}} = \Delta \times \{i\}$$

for each $i \in \Sigma$. Hence $(g\theta)(g\rho)^{-1}$ has the effect of applying a permutation of each set $\Delta \times \{i\}$; that is, it is an element of the base group B of the wreath product W (as illustrated in Figure 7.1. This shows that $g\theta = b(g\rho) \in W$ for some $b \in B$.

Applying the inverse of the isomorphism θ we conclude $G \leqslant W\theta^{-1}$; that is, G is contained in a subgroup isomorphic to the wreath product W. Furthermore, this is a permutation isomorphism since if $\omega \in \Omega$ and $x \in W\theta^{-1}$, then

$$(\omega\phi)^{x\theta} = (\omega\phi)^{\phi^{-1}x\phi} = (\omega^x)\phi.$$

(Essentially the choice of isomorphism $\theta\colon \mathrm{Sym}(\Omega) \to \mathrm{Sym}(\Omega')$ was designed to induce a permutation isomorphism.) □

Primitive groups

We have now shown that an intransitive action of a permutation group essentially corresponds to a direct product decomposition and that a transitive but imprimitive action essentially corresponds to a decomposition as a wreath product. We shall finish the chapter, by examining the structure of a primitive permutation group. The ideas presented here are motivated by an important theorem called the O'Nan–Scott Theorem, but we will not be able to go as far as proving that quite difficult theorem. Nevertheless, we shall indicate some of the ideas that arise within it.

Example 7.23 *Let $n \geqslant 3$. Show that the alternating group A_n in its natural action on $\Omega = \{1, 2, \dots, n\}$ is primitive.*

Solution: Let Δ be a block for A_n in its action on Ω and assume that $|\Delta| \geqslant 2$. Let $\alpha, \beta \in \Delta$ be distinct points. Suppose that $\gamma \in \Omega \setminus \{\alpha, \beta\}$. Take $x = (\alpha\ \beta\ \gamma) \in A_n$. Then $\beta = \alpha^x \in \Delta^x$ and so $\Delta^x = \Delta$ (since Δ is a block). Hence $\gamma = \beta^x \in \Delta$ also. We conclude that $\Delta = \Omega$.

Hence there are no non-trivial blocks for A_n and hence this group acts primitively on Ω. □

Our second example will be relevant to the discussion of the structure of primitive groups at the end of the chapter. First recall that if V is a vector space of dimension n over a field F, then it is an additive group and the general linear group $\mathrm{GL}_n(F)$ has a natural action upon it. Accordingly, we can make the following definition:

Definition 7.24 Let V be a vector space of dimension n over some field F. The *affine general linear group* $\mathrm{AGL}_n(F)$ is the semidirect product $V \rtimes \mathrm{GL}_n(F)$ determined by the natural action of $\mathrm{GL}_n(F)$ on the vector space V.

Each linear map $h \in \mathrm{GL}_n(F)$ is, in particular, an automorphism of the additive group $(V, +)$. Hence we obtain an associated homomorphism $\mathrm{GL}_n(F) \to \mathrm{Aut}(V, +)$ and so can form the above semidirect product. We shall write elements of $\mathrm{AGL}_n(F)$ as ordered pairs (x, h) where $x \in V$ and $h \in \mathrm{GL}_n(F)$.

Example 7.25 (i) *Show that $\mathrm{AGL}_n(F)$ acts transitively on the vector space V by the formula*

$$v^{(x,h)} = (v + x)h$$

where $v, x \in V$ and vh denotes the image of v under application of the linear map h.

(ii) *Show that this action is primitive provided $n \geqslant 1$.*

Solution: Throughout this solution, we shall write $G = \mathrm{AGL}_n(F)$.

(i) Since $\mathrm{AGL}_n(F)$ is a semidirect product, the multiplication is given by

$$(x, h)(y, k) = (x + yh^{-1}, hk).$$

Hence, using the fact that h and k induce linear maps on V,

$$\begin{aligned} v^{(x,h)(y,k)} &= v^{(x+yh^{-1},hk)} \\ &= (v + x + yh^{-1})hk \\ &= vhk + xhk + yk \end{aligned}$$

and

$$\begin{aligned} (v^{(x,h)})^{(y,k)} &= \big((v + x)h + y\big)k \\ &= vhk + xhk + yk \end{aligned}$$

so that

$$(v^{(x,h)})^{(y,k)} = v^{(x,h)(y,k)}$$

for all $v \in V$ and $(x, h), (y, k) \in G$. The identity element of G is $(0, 1)$ and

$$v^{(0,1)} = (v + 0)1 = v \qquad \text{for all } v \in V.$$

(Here 0 is the zero vector in V and 1 is the identity map.) Hence we do indeed have an action of G on V. Finally if $v, w \in V$, then $g = (w - v, 1) \in G$ and

$$v^{(w-v,1)} = v + (w - v) = w.$$

Hence $G = \mathrm{AGL}_n(F)$ acts transitively on V.

(ii) Assume that $\dim V \geqslant 1$, so $V \neq \mathbf{0}$. We shall show that the stabilizer G_0 of the zero vector is maximal in $G = \mathrm{AGL}_n(F)$. First observe that $0^{(x,h)} = xh$ and so, since h is an invertible linear map, it follows that $0^{(x,h)} = 0$ if and only if $x = 0$. Hence

$$G_0 = \{\, (0, h) \mid h \in \mathrm{GL}_n(F) \,\};$$

that is, this stabilizer equals $\mathrm{GL}_n(F)$ under the standard identification of the complement with the corresponding subgroup of the semidirect product. Since $V \neq \mathbf{0}$, G_0 is a proper subgroup of G.

We now show that this stabilizer is a maximal subgroup of G. Suppose that K is a subgroup of G with $G_0 < K \leqslant G$. Hence there exists some $(x, h) \in K$ with $x \neq 0$. Since $\mathrm{GL}_n(F) = G_0 < K$, the subgroup K contains the element

$$(x, h)(0, h^{-1}) = (x + 0h^{-1}, hh^{-1}) = (x, 1).$$

If y is a non-zero vector in V, there exists some invertible linear map $k \in \mathrm{GL}_n(F)$ that moves x to y. Hence K also contains

$$(0, k^{-1})(x, 1) = (xk, k^{-1}) = (y, k^{-1})$$

and now if h' is any element of $\mathrm{GL}_n(F)$, K also contains

$$(y, k^{-1})(0, kh') = (y, h').$$

Since y is an arbitrary non-zero vector and $h' \in \mathrm{GL}_n(F)$ is arbitrary, we conclude $K = \mathrm{AGL}_n(F)$. (Note we already know that K contains all pairs with $y = 0$ since $G_0 < K$.)

This shows that the stabilizer G_0 is a maximal subgroup of G. Corollary 7.20 tells us that G acts primitively on the vector space V. □

We now move into the final phase of the chapter. We shall develop some theory concerning primitive actions and hence be able to say something about the structure of permutation groups that are primitive. We shall make use of the centralizer of a subgroup, which is defined as follows:

Definition 7.26 Let G be a group and H be a subgroup of G. The *centralizer* of H in G is

$$\mathrm{C}_G(H) = \{\, x \in G \mid xh = hx \text{ for all } h \in H \,\},$$

the set of all elements that commute with every element of H.

Note that $\mathrm{C}_G(H) = \bigcap_{h \in H} \mathrm{C}_G(h)$ expresses this centralizer as an intersection of centralizers of elements. We already know the latter are subgroups of G and hence $\mathrm{C}_G(H)$ is also a subgroup. It is quite easy (see Problem Sheet VII) to verify that if N is a normal subgroup of G, then $\mathrm{C}_G(N)$ is also a normal subgroup of G.

Lemma 7.27 *Let G be a permutation group on Ω and H be a subgroup of G that acts transitively on Ω. If $C = \mathrm{C}_G(H)$ is the centralizer of H in G, then $C_\omega = 1$ for all $\omega \in \Omega$.*

Proof: Fix $\omega \in \Omega$. Suppose that $x \in C_\omega$. Let $\alpha \in \Omega$ be arbitrary. Since H acts transitively, there exists some $h \in H$ such that $\alpha = \omega^h$. Note that $xh = hx$ (because $x \in \mathrm{C}_G(H)$) and so

$$\alpha^x = \omega^{hx} = \omega^{xh} = \omega^h = \alpha$$

using the fact that x fixes ω. Hence x fixes all points of Ω and therefore $x = 1$ (since C is faithful on Ω). This shows $C_\omega = \mathbf{1}$ for all $\omega \in \Omega$. □

Lemma 7.28 *Let G be a finite group and let M and N be distinct minimal normal subgroups of G. Then $[M, N] = \mathbf{1}$.*

Proof: Note that $M \cap N$ is a normal subgroup of G contained in both M and N. If it were non-trivial, then $M = M \cap N = N$ by minimality of the two subgroups, contrary to the assumption that $M \neq N$. Hence $M \cap N = \mathbf{1}$. If $x \in M$ and $y \in N$, then

$$[x, y] = x^{-1}y^{-1}xy \in M \cap N$$

since $y^{-1}xy \in M$ and $x^{-1}y^{-1}x \in N$. Hence $[x, y] = 1$ for all $x \in M$ and $y \in N$; that is, $[M, N] = \mathbf{1}$. □

We can now give the main first step in the description of the structure of a finite primitive permutation group. It is expressed in terms of minimal normal subgroups. Recall from Theorem 3.19 that a minimal normal subgroup of a finite group is a direct product of isomorphic simple groups. It is therefore either an elementary abelian p-group for some prime p (that is, a direct product of cyclic groups of order p) or a direct product of isomorphic non-abelian finite simple groups. In the case of primitive permutation groups, there is actually considerable constraint in the possibility for minimal normal subgroups.

Theorem 7.29 *Let G be a non-trivial finite primitive permutation group on a set Ω. Then one of the following holds:*

(i) *G has a unique minimal normal subgroup N which is abelian, N acts regularly on Ω and $\mathrm{C}_G(N) = N$;*

(ii) *G has precisely two minimal normal subgroups M and N, these are both non-abelian, act regularly on Ω with $\mathrm{C}_G(M) = N$ and $\mathrm{C}_G(N) = M$;*

(iii) *G has a unique minimal normal subgroup N that is non-abelian and $\mathrm{C}_G(N) = \mathbf{1}$.*

Proof: We first make an observation about the action of a minimal normal subgroup N of G. The orbits of N on Ω are blocks for G by Lemma 7.15. Since G is primitive, either there is one orbit or they are all singletons. However, $N \neq \mathbf{1}$ and G acts faithfully, so the latter is not possible. Hence N acts transitively on Ω.

Now suppose that N is an abelian group. Let $C = \mathrm{C}_G(N)$, so that $N \leqslant C$. Certainly then C also acts transitively on Ω. Apply Lemma 7.27 to deduce that $C_\omega = \mathbf{1}$. It follows that $N_\omega = \mathbf{1}$. Hence N and C both act regularly on Ω. Therefore $|N| = |C| = |\Omega|$ by Lemma 7.9. We deduce that $C = \mathrm{C}_G(N) = N$. Now if M is any other minimal normal subgroup of G, then M commutes with N by Lemma 7.28. Hence $M \leqslant C = N$, which forces $M = N$, by minimality. This establishes that (i) holds when N is abelian.

For the remainder of the proof, we assume that the minimal normal subgroups of G are non-abelian. Suppose that M and N are two distinct minimal normal subgroups of G. We know these both act transitively on Ω. Let $C = \mathrm{C}_G(N)$. Then $M \leqslant C$ by Lemma 7.28 and so C acts transitively on Ω. Apply Lemma 7.27 to deduce that $C_\omega = \mathbf{1}$. Hence $M_\omega = \mathbf{1}$

and we deduce that both M and C act regularly on Ω. Therefore $|M| = |C| = |\Omega|$ by Lemma 7.9 and hence $M = C = \mathrm{C}_G(N)$. We can interchange the roles of M and N to conclude N is also regular on Ω and $N = \mathrm{C}_G(M)$. Also there cannot be a further minimal normal subgroup R for then the same argument shows $R = \mathrm{C}_G(N) = M$. This establishes that (ii) holds when G has more than one minimal normal subgroup.

Finally suppose that G has a unique minimal normal subgroup N and this is non-abelian. Let $C = \mathrm{C}_G(N) \trianglelefteqslant G$. Since N is a direct product of non-abelian simple groups, its centre is trivial, so $N \cap C = \mathbf{1}$. If it were the case that $C \neq \mathbf{1}$, then there would exist some minimal normal subgroup M contained in C, but this could not equal N as $N \nleqslant C$. Hence $C = \mathrm{C}_G(N) = \mathbf{1}$ in this final case and we have established that (iii) holds. □

To prove the theorem that classifies the finite primitive permutation groups, one analyzes the cases that arise in the above theorem. In Case (iii), the unique minimal normal subgroup N of the primitive group G may or may not be regular in its action of Ω. Accordingly the final classification is split into whether or not the minimal normal subgroup is regular. We shall not prove the O'Nan–Scott Theorem in this lecture course since it would take too long, but we will summarize the theorem by giving the names of the classes of primitive permutation groups that arise.

Theorem 7.30 (O'Nan–Scott Theorem) *Suppose that G is a non-trivial finite primitive permutation group on a set Ω and let N be a minimal normal subgroup of G. Then*

(i) *either N is regular on Ω and G is of one of the following types:*

- *affine type,*
- *regular non-abelian type;*

(ii) *or N is not regular on Ω and G is of one of the following types:*

- *diagonal type,*
- *product type,*
- *an almost simple group.*

We shall not describe all these "types" in detail here. Many have structures that are related to wreath products but more complicated. We shall define the last term:

Definition 7.31 A finite group G is called *almost simple* if it has a unique minimal normal subgroup N such that N is a non-abelian simple group.

When $n \geqslant 5$, the example of the symmetric group S_n acting in the natural way on the set $\Omega = \{1, 2, \dots, n\}$ is an example of a primitive group that is almost simple (with $N = A_n$). If G is almost simple with minimal normal subgroup N then, upon identifying N with its group of inner automorphisms, we can embed G in the automorphism group $N \leqslant G \leqslant \operatorname{Aut} N$ (see Problem Sheet VII). Studying these groups essentially reduces to having a detailed understanding of the Classification of Finite Simple Groups and, in particular, a good description of the maximal subgroups of almost simple groups. This has been a topic of considerable research over many years, particularly since the completion of the Classification of Finite Simple Groups.

What we shall do to finish the course is to describe the affine type groups. We return to Case (i) of Theorem 7.29. Let G be a finite primitive permutation group on Ω such that G has a unique minimal normal subgroup N that is abelian, that acts regularly on Ω and that $\mathrm{C}_G(N) = N$. Fix $\omega \in \Omega$ and let $H = G_\omega$. Then $G = HN$ by Lemma 7.10 and $H \cap N = N_\omega = \mathbf{1}$. Hence G has the structure of a semidirect product $G = N \rtimes_\phi H$ for some $\phi\colon H \to \operatorname{Aut} N$.

Since N is an abelian minimal normal subgroup of G, it is an elementary abelian p-group for some prime p by Theorem 3.19. We shall write the group operation in N additively so that

$$N \cong V = \underbrace{\mathbb{F}_p \oplus \mathbb{F}_p \oplus \cdots \oplus \ldots \mathbb{F}_p}_{d \text{ times}}.$$

This V has the structure of a d-dimensional vector space over the field $\mathbb{F}_p$ of p elements. To simplify notation, we shall identify N and V via this isomorphism. Homomorphisms of N are therefore linear maps and $\operatorname{Aut} N \cong \mathrm{GL}_d(\mathbb{F}_p)$. Hence we can assume $\phi\colon H \to \mathrm{GL}_d(\mathbb{F}_p)$. Since the map ϕ is induced by conjugation of elements of N by elements of H, $h \in \ker\phi$ if and only if h commutes with all elements of N; that is,

$$\ker\phi = \mathrm{C}_H(N) = H \cap \mathrm{C}_G(N) = H \cap N = \mathbf{1}.$$

Hence ϕ is injective and so, again to simplify notation, we shall identify H with its image in $\mathrm{GL}_d(\mathbb{F}_p)$. In conclusion, we have shown $G = N \rtimes_\phi H$ where N has the structure of a vector space of dimension d over $\mathbb{F}_p$ and H is a subgroup of $\mathrm{GL}_d(\mathbb{F}_p)$.

Now let us examine the action of G on Ω. We shall write the elements of G as ordered pairs (x,h) where $x \in N$ and $h \in H$. Lemma 7.9 tells us that every element of Ω is uniquely expressible in the form $\omega^{(v,1)}$ for $v \in N$. Since every element of H fixes ω, we see the action is given by

$$(\omega^{(v,1)})^{(x,h)} = \omega^{(0,h^{-1})(v,1)(x,h)} = \omega^{(0,h^{-1})(v+x,h)} = \omega^{((v+x)h,1)},$$

where we write vh for the image of the vector v under the linear map h (which is how elements of H act by conjugation on N). We conclude that there is a bijection $\psi\colon N \to \Omega$ given by $v\psi = \omega^{(v,1)}$ which has the property that

$$(v\psi)^{(x,h)} = (v^{(x,h)})\psi$$

where the action of $G = N \rtimes H$ on $N = V$ is given by

$$v^{(x,h)} = (v+x)h.$$

The latter is the formula for the action of the affine general linear group $\mathrm{AGL}_d(\mathbb{F}_p)$ considered in Example 7.25. Here $G = N \rtimes H$ has been identified with a subgroup of $\mathrm{AGL}_d(\mathbb{F}_p) = V \rtimes \mathrm{GL}_d(\mathbb{F}_p)$ via our identification of N with V and H with a subgroup of $\mathrm{GL}_d(\mathbb{F}_p)$. It follows that we have a permutation isomorphism between the action of this subgroup of $\mathrm{AGL}_d(\mathbb{F}_p)$ and the action of G on Ω.

We have now described the affine type primitive groups arising in the O'Nan–Scott Theorem:

Theorem 7.32 (Affine Type Primitive Groups) *Let G be a finite primitive permutation group on a set Ω and suppose that G has an abelian minimal normal subgroup N. Let $|N| = p^d$ where p is a prime number. Then there is a subgroup H of $\mathrm{GL}_d(\mathbb{F}_p)$ such that G is permutationally isomorphic to the subgroup $V \rtimes H$ of the affine general linear group $\mathrm{AGL}_d(\mathbb{F}_p)$ in its natural action on the vector space V of dimension d over $\mathbb{F}_p$.* □

There is one final thing to note about this theorem. Not all choices of H give rise to primitive actions, but if one assumes the additional condition that H acts *irreducibly* (that is, there is no non-zero proper subspace W of V that is invariant under the action of H) then this completely characterizes the finite primitive groups of affine type.

Versions

Significant updates to the notes will be listed below. Updates that are merely correcting typographic errors and similar will be indicated by appending a letter to the version number on the front page and will not be listed below.

Version 0.1: New version of lecture notes begun 22nd Aug 2022 in view of change of module title and syllabus.

Version 0.2: Preliminary release version comprising Chapters 1–4.

Version 0.3: Inserted a small example of a stabilizer into Chapter 2. Drafted Chapters 5 & 6. Fixed some typos in earlier chapters.

Version 1.0: First full version of all chapters. Small revisions to the start of Chapter 4.