MT5824 Topics in Groups

MQ

September 5, 2024

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

The goal of the course will be to introduce a variety of topics in more advanced group theory. We shall particularly be interested in topics that have some relation to the research of the group theorists in St Andrews.

The topics considered will be as follows:

Revision: Review of the basic concepts of subgroup, normal subgroup, quotient group and homomorphism. (Some new results will be proved which will used later in the course.)

Group Actions: We will explain how a group can induced permutations of a set and deduce structural properties about subgroups and homomorphisms.

Sylow's Theorem: We review Sylow's Theorem from the group action viewpoint and illustrate some applications.

Composition series: We consider how a group can be decomposed into essentially uniquely determined simple groups. This illustrates one example of a "series" for a group.

Building groups: We discuss how groups may be constructed and in particular some ways in which the above decomposition may be reversed. We shall review the direct product construction but also generalise it.

Soluble groups: We meet a particular class of groups that has a fairly restricted structure. We shall prove Hall's Theorem (a generalisation of Sylow's Theorem for soluble groups).

Nilpotent groups: We finish by discussing an even more restricted class of groups, of which the typical example is the p-group.

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 quotient groups G_i/G_{i+1} $(0 \leqslant i \leqslant n-1)$ yields information about G.

Recommended Texts: The following textbooks are appropriate and possibly useful for consultation. Only the first two are cheap enough to consider buying!

- John S. Rose, *A Course on Group Theory* (Dover Publications, New York, 1994), £6.50, QA171.R7.
- B. A. F. Wehrfritz, *Finite Groups: A Second Course on Group Theory* (World Scientific, Singapore, 1999), £18, not in library.
- Derek J. S. Robinson, *A Course in the Theory of Groups (Second Edition)*, Graduate Texts in Mathematics **80** (Springer–Verlag, New York, 1996), £52.50, QA171.R73.
- Joseph J. Rotman, *The theory of groups: an introduction* (Allyn & Bacon, 1965). QA171.R7.
- M. I. Kargapolov & Ju. I. Merzljakov, *Fundamentals of the Theory of Groups*, Graduate Texts in Mathematics **62** (Springer–Verlag, New York, 1979). QA171.K28M4

Section 1

Revision and Re-Activation

In this first section I shall principally recall definitions and results from earlier lecture courses. Often I will omit the proof of results that have been previously met during the lectures (though these notes will contain them). I shall also establish the notation to be used throughout the course. In a number of places I will be deviating slightly from that met in some of the earlier courses, but I hope that I am being more consistent with typical usage in the mathematical community when I do so.

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*:

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

(ii) there is an *identity element* 1 in G:

$$x1 = 1x = x \qquad \text{for all } x \in G;$$

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

$$xx^{-1} = x^{-1}x = 1.$$

Comments:

(i) I have made no reference to 'closure' explicity 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 creates a third element *in the group*, and so we have closure automatically.

(ii) Associativity ensures that we can safely omit brackets from a product $x_1x_2\dots x_n$ of n elements $x_1, x_2, \dots, x_n$ 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 $n \in \mathbb{Z}$. Standard power laws hold although we 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, 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 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 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] We have $1 \in H_i$ for all i, so $\bigcap_{i\in I} H_i \neq \varnothing$. 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.

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 $S \subseteq \langle X \rangle$.

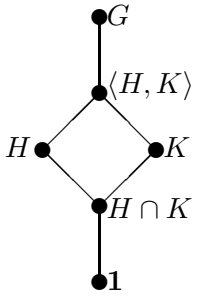
On the other hand, S is non-empty (for example, it contains the empty product (where $n = 0$) which by convention is taken to be the identity element 1), it contains all elements of X (the case $n = 1$ and $\varepsilon_1 = 1$), is clearly closed under products and

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

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. $\square$

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 line to denote inclusion. For example, the following illustrates the phenomena just discussed:



(For subgroups H and K of G, we have $H \cap K$ as the largest subgroup contained in H and K, and $\langle H, K \rangle$ as the smallest subgroup containing H and K.)

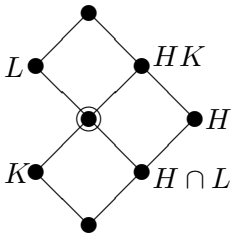
Before discussing more familiar concepts from previous courses, we prove a result that is extremely useful when manipulating subgroups.

Lemma 1.7 (Dedekind's Modular Law) *Let G be a group and H, K and L be subgroups of G with $K \leqslant L$. Then*

$$HK \cap L = (H \cap L)K.$$

(Here we define $HK = \{\, hk \mid h \in H,\, k \in K \,\}$. A similar formula defines the set product $(H \cap L)K$.)

As an *aide memoire*, the following diagram can be used to remember the formula:



The circled node represents both $HK \cap L$ and $(H \cap L)K$. (The diagram is slightly misleading in the context of the previous discussion: HK (and the other products appearing) need not be a subgroup, but the diagram is at least useful to remember the result.)

PROOF: $H \cap L \leqslant H$, so immediately we have $(H \cap L)K \subseteq HK$. Also $H \cap L$ and K are contained in L, so $(H \cap L)K \subseteq L$ (since L is closed under products). Thus

$$(H \cap L)K \subseteq HK \cap L.$$

Now let $x \in HK \cap L$. Then $x = hk$ where $h \in H$ and $k \in K$. Now $h = xk^{-1} \in L$ since $x \in L$ and $k \in K \leqslant L$. Thus $h \in H \cap L$ and so $x = hk \in (H \cap L)K$. □

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 1.8 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 subset

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

of G.

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' and always mean 'right coset'.

Theorem 1.9 *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 1.10 (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. □

At this point we insert two results about the index of subgroups. The first is frequently used while the second will be needed (much) later in the course.

Lemma 1.11 *Let H and K be subgroups of a group G with $K \leqslant H \leqslant G$. Then*

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

I shall omit the proof (both in the lectures and these notes). In full generality, it appears on Problem Sheet I, while for finite groups it is easily deduced from Lagrange's Theorem.

Lemma 1.12 *Let G be a group and H and K be subgroups of G. Then*

$$|G : H \cap K| \leqslant |G : H| \cdot |G : K|.$$

Furthermore, if $|G : H|$ and $|G : K|$ are coprime integers, then

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

PROOF: Define a map from the set of cosets of $H \cap K$ to the Cartesian product of the sets of cosets of H and of K by

$$\phi\colon (H \cap K)x \mapsto (Hx, Kx).$$

Now

$$\begin{aligned}(H \cap K)x = (H \cap K)y \quad &\text{if and only if} \quad xy^{-1} \in H \cap K \\ &\text{if and only if} \quad xy^{-1} \in H \text{ and } xy^{-1} \in K \\ &\text{if and only if} \quad Hx = Hy \text{ and } Kx = Ky.\end{aligned}$$

So ϕ is well-defined and injective. Therefore

$$|G : H \cap K| \leqslant |G : H| \cdot |G : K|. \tag{1.1}$$

Now suppose that $|G : H|$ and $|G : K|$ are coprime integers. First note that Equation (1.1) tells us that $|G : H \cap K|$ is an integer. We need to establish the reverse inequality. Now $H \cap K \leqslant H \leqslant G$, so

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

by Lemma 1.11. It follows that $|G : H \cap K|$ is divisible by $|G : H|$. It is similarly divisible by $|G : K|$. As these integers are coprime, we deduce

$$|G : H| \cdot |G : K| \text{ divides } |G : H \cap K|.$$

This establishes the required reverse inequality and completes the proof when taken together with Equation (1.1). □

Orders of elements and Cyclic groups

Definition 1.13 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 x has finite order n and $k \in \mathbb{Z}$, write $k = nq + r$ where $0 \leqslant r < n$. Then

$$x^k = x^{nq+r} = (x^n)^q x^r = x^r \tag{1.2}$$

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

Proposition 1.14 (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 $1, x, x^2, \ldots, x^{n-1}$.* □

Corollary 1.15 *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 (1.2) 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 1.16 A group G is called *cyclic* (with *generator* x) if $G = \langle x \rangle$.

Using ideas as just described, it is reasonably easy to establish the following (and also a corresponding result for infinite cyclic groups):

Theorem 1.17 *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.*

The proof of this theorem is omitted. It, and more, can be found on Problem Sheet I.

Normal subgroups and quotient groups

Definition 1.18 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 $N \trianglelefteq G$ 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 in greater detail in Section 2.

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

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

Theorem 1.19 *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 $N \trianglelefteq G$, we have $b^{(x')^{-1}} \in N$. 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 1.20 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 moment. I shall just mention some results (one part of which I shall prove, the rest appear on Problem Sheet I) which will be needed later.

Lemma 1.21 *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 holds even when HK is not a subgroup.

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

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

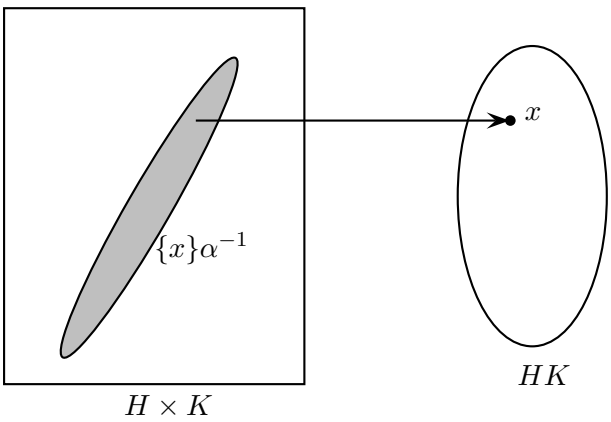
Then α is surjective. Fix a point $x \in HK$, say $x = h_0k_0$ for some fixed $h_0 \in H$ and $k_0 \in K$. Then for $(h, k) \in H \times K$,

$$\begin{aligned} (h,k)\alpha = x \quad & \text{if and only if} \quad hk = h_0k_0 \\ & \text{if and only if} \quad h_0^{-1}h = k_0k^{-1} \in H \cap K \\ & \text{if and only if} \quad h = h_0a,\ k = a^{-1}k_0 \quad \text{where } a \in H \cap K. \end{aligned}$$

Thus for each $x \in HK$, we see

$$\{\, (h,k) \in H \times K \mid (h,k)\alpha = x \,\} = \{\, (h_0a, a^{-1}k_0) \mid a \in H \cap K \,\}.$$

Hence we may partition $H \times K$ into $|HK|$ subsets, each corresponding to one point in HK and each of size $|H \cap K|$.



This proves

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

that is,

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

□

Homomorphisms

Definition 1.22 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 respects the multiplications present.

Note that I am writing my maps on the right, as is conventional in much of algebra. This has two 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. The second is that it will make certain proofs more notationally convenient.

Related to homomorphisms we have the following definition.

Definition 1.23 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 1.24 *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 1.25 *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 1.26 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.

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 1.27 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 1.28 (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 $\ker\phi \trianglelefteqslant G$, so we can form $G/\ker\phi$. The isomorphism is the map

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

□

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

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

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 1.24.) □

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 1.29 (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*

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

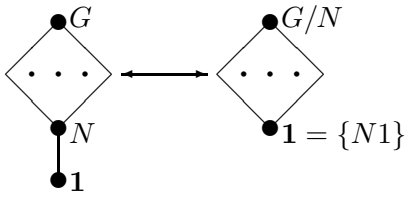
(ii) *Under the above correspondence, normal subgroups of G which contain N correspond to normal subgroups of G/N.*

Note we are saying that every subgroup of G/N has the form H/N where $N \leqslant H \leqslant G$. Specifically, if J is a subgroup of G/N, it corresponds to $H = \{\, x \in G \mid Nx \in J \,\}$ (the set of elements which are mapped into J by the natural map $G \to G/N$) and then $J = H/N$ for this H. Also part (ii) says:

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

(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 have $x = ny \in H_2$. 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 deduce $J = H/N = H\Phi$. 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 paragraph 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 1.30 (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

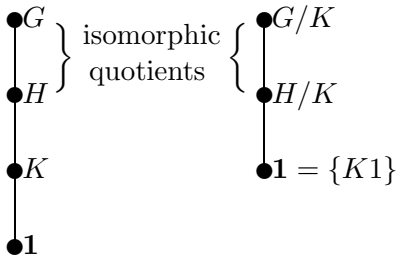
$$H/(H \cap N) \cong NH/N.$$

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

Theorem 1.31 (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 we have the following:



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, $H/K \trianglelefteqslant G/K$ and

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

□

This completes our rapid review of previous group theory, at least for now. Certain results will be reviewed later when we need them, while various examples will appear on problem sheets and during the course.

Section 2

Group Actions

The purpose of this section is to explain what it means for a group to 'act' on a set. There are two principal reasons for doing so.

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

(ii) This gives 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.

Let G be a group and Ω be a set. A group action of G on 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.

Definition 2.1 A *group action* is a map

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

(where Ω is a set and G is a group) 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.

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 produces the effect of the identity map when it is applied.

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

Example 2.2 (i) Let $\Omega = \{1, 2, \ldots, n\}$. 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 by composing them as maps.

Then S_n acts on Ω by

$$(i, \sigma) \mapsto i\sigma$$

(the effect of applying the permutation σ to the number $i \in \Omega$). The two conditions hold immediately: the first follows since multiplication in S_n is composition and the second holds since the identity element in S_n is the identity permutation (the map which fixes all points of Ω).

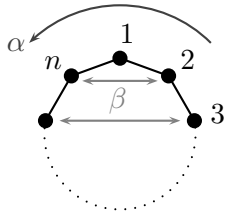
(ii) Recall that the *dihedral group* of order $2n$ is the subgroup of S_n generated by the following two permutations:

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

I shall denote this group by D_{2n}. (This is a slight modification from the notation used in MT4003, but at least consistent with my preferred textbooks.) Recall this has the following properties:

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

Now consider a regular n-gon with vertices labellled from 1 to n.



Applying α to the vertices induces an anti-clockwise rotation of the regular n-gon. Applying β produces a reflection in the axis through vertex 1. Hence both α and β induce transformations of the regular n-gon and consequently any produce of them does so also.

Conclusion: D_{2n} acts on the vertices of a regular n-gon.

(iii) Let V be a vector space of dimension n over a field F. Fix a basis $\{e_1, e_2, \ldots, e_n\}$ for V. Any linear transformation $T\colon V \to V$ can be represented 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).

Recall that 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.

These give us examples of group actions arising in combinatorial, geometrical and linear arenas. We shall also find lots of examples occurring of groups acting on something related to their own structure. We shall first develop the theory of group actions so that we can use the group theoretical examples to prove things about groups.

Orbits

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

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

Thus, the orbit containing ω consists of all the points of Ω we can arrive at by applying element of the group G to ω.

The basic properties of orbits are as follows.

Proposition 2.4 *Let G be a group, let 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 to our result that says a group is the disjoint union of the cosets of a subgroup. The difference here is that it is not necessarily the case that all the orbits have the same size.

It remains to prove Proposition 2.4.

PROOF OF PROPOSITION 2.4: (i) We have $\omega = \omega^1$, 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 if $g \in G$, we have

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

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

Similarly from $(\omega')^y = \omega^x$, we deduce

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

and hence $\omega^G \subseteq (\omega')^G$.

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

The following definition relates to this disjoint union of orbits.

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 $\omega' = \omega^x$. (For this is what it means for ω' to lie in the orbit containing ω.)

Stabilisers

Definition 2.7 Let the group G act on the set Ω. If $\omega \in \Omega$, then the *stabiliser* of ω in G is defined to be

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

Thus the stabiliser of ω is the set of all group elements which fix ω.

Lemma 2.8 *Let G act on Ω and $\omega \in \Omega$. The stabiliser G_ω of ω is a subgroup of G.*

PROOF: We easily check the conditions to be a subgroup. First $\omega^1 = \omega$, since we have an action, so $1 \in G_\omega$. 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 stabilisers help us is the following:

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

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

Thus the 'length' of an orbit equals the index of the corresponding stabiliser.

PROOF: We demonstrate the existence of a bijection from the set of cosets of the stabiliser 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 clearly 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. Thus

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

□

One thing to consider is the following observation: Suppose 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-Stabiliser Theorem,

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

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

Proposition 2.10 *Let G be a group, let 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 stabilisers G_ω and $G_{\omega'}$ are conjugate in G.*

PROOF: Since ω and ω' lie in the same orbit, there exists $x \in G$ such that $\omega' = \omega^x$. We shall show that

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

i.e.,

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

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

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

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 from the already established inclusion above we get

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

that is,

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

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 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 stabilisers 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 called the *conjugacy class* of g (in G).

The stabiliser 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 stabiliser of g consists of the set of elements of G which commute with g.

Definition 2.12 If G is a group and g is an element of G, the *centraliser* 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.

Proposition 2.13 *Let G be a group. Then*

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

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

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

(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 stabiliser is a subgroup.

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

(iv) Immediate from Proposition 2.10 (and specifically Equation 2.1). □

(This material also appeared in MT4003, but we are able to deduce it immediately from the technology of group actions. Thus group actions form a natural setting to discuss conjugation.)

We continue our discussion of conjugation to determine more properties.

Let G be a finite group. Then G is the disjoint union of its conjugacy classes:

$$G = \mathscr{C}_1 \cup \mathscr{C}_2 \cup \cdots \cup \mathscr{C}_k.$$

Hence

$$\begin{aligned} |G| &= |\mathscr{C}_1| + |\mathscr{C}_2| + \cdots + |\mathscr{C}_k| \\ &= \sum_{i=1}^{k} |G : \mathrm{C}_G(g_i)|, \end{aligned}$$

where g_i is a representative for the conjugacy class $\mathscr{C}_i$. Suppose that $|\mathscr{C}_i| = 1$ for $1 \leqslant i \leqslant \ell$ and $|\mathscr{C}_i| > 1$ for $i > \ell$. Then

$$|G| = \ell + \sum_{i=\ell+1}^{k} |G : \mathrm{C}_G(g_i)|.$$

Note

$$\begin{array}{lll} |\mathscr{C}_i| = 1 & \text{if and only if} & g_i^x = g_i \text{ for all } x \in G \\ & \text{if and only if} & g_i x = x g_i \text{ for all } x \in G. \end{array}$$

Definition 2.14 If G is a group, the *centre* of G is

$$\mathrm{Z}(G) = \{\, g \in G \mid gx = xg \text{ for all } x \in G \,\};$$

that is, the set of elements in G which commute with all elements of G.

The centre of G can easily be seen to be a subgroup of G. [PROOF [OMITTED IN LECTURES]: $1x = x = x1$ for all $x \in G$, so $1 \in \mathrm{Z}(G)$. If $g, h \in \mathrm{Z}(G)$, then $(gh)x = ghx = gxh = xgh = x(gh)$ for all $x \in G$, so

$gh \in \mathrm{Z}(G)$ and upon multiplying the equation $gx = xg$ on the left and on the right by g^{-1}, we obtain $xg^{-1} = g^{-1}(gx)g^{-1} = g^{-1}(xg)g^{-1} = g^{-1}x$ for all $x \in G$, so $g^{-1} \in \mathrm{Z}(G)$. Hence $\mathrm{Z}(G)$ is a subgroup of G.]

Our discussion above now establishes:

Theorem 2.15 (Class Equation) *Let G be a finite group. Then*

$$|G| = |\mathrm{Z}(G)| + \sum_{i=\ell+1}^{k} |G : \mathrm{C}_G(x_i)|$$

where $x_{\ell+1}, \ldots, x_k$ are representatives for the conjugacy classes of length greater than 1. □

Conjugation on subgroups

Example 2.16 (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 stabiliser is the so-called 'normaliser' of A:

Definition 2.17 If G is a group and A is a subset of G, the *normaliser* of A (in G) is

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

Since this is a stabiliser, it is always a subgroup of G (by Lemma 2.8). We shall be most interested in the case when we conjugate subgroups. To discuss this further we shall need to examine conjugation more carefully.

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 2.18 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.

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. Furthermore, the Orbit-Stabiliser Theorem (Theorem 2.9) tells us that the number of conjugates of H equals the index of its normaliser (this being the stabiliser for this action).

We record all this in the following observation.

Proposition 2.19 *Let G be a group.*

(i) *If $x \in G$, the conjugation map $\tau_x \colon g \mapsto g^x$ is an automorphism of G.*

(ii) *If H is a subgroup of G and $x \in G$, the conjugate H^x is a subgroup of G.*

(iii) *If H is a subgroup of G, the normaliser $\mathrm{N}_G(H)$ of H in G is a subgroup of G.*

(iv) *If H is a subgroup of G, the number of conjugates of H in G equals the index $|G : \mathrm{N}_G(H)|$ of the normaliser in G.* □

We call the automorphism $\tau_x \colon g \mapsto g^x$ an *inner automorphism* of G.

Permutation representations

The Orbit-Stabiliser Theorem tells us about the link between a group action and the indices of particular subgroups. We shall now 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 2.20 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, while all permutations possess inverses since they are bijective. We recover our friend the symmetric group S_n by considering the special case when $\Omega = \{1, 2, \ldots, n\}$.

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 $\rho_x\rho_{x^{-1}} = \rho_{x^{-1}}\rho_x = 1$, so ρ_x is a bijection and therefore

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

So to each element of G we associate a permutation of Ω. (Note that it is *not* an isomorphism: Ω is merely a set and does not necessarily have any group structure.) We therefore have 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 2.21 *Let G be a group, let Ω be a set and let G act on Ω. For each $x \in G$, the map*

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

is a permutation of Ω. The map

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

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

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

i.e., the elements of G which fix *all* points in Ω.

Example 2.22 (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).

Theorem 2.21 provides us with a homomorphism $\rho : G \to \mathrm{Sym}(G)$. What is the kernel of ρ?

$$\begin{array}{lll} x \in \ker\rho & \text{if and only if} & \rho_x = 1 \\ & \text{if and only if} & g\rho_x = g \quad \text{for all } g \in G \\ & \text{if and only if} & gx = g \quad \text{for all } g \in G \\ & \text{if and only if} & x = 1. \end{array}$$

Hence $\ker\rho = \mathbf{1}$ and so ρ is one-one. It follows that G is isomorphic to $\mathrm{im}\,\rho$ and we have proved Cayley's Theorem.

Theorem 2.23 (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. Verification of the details appears on Tutorial Sheet II.

Example 2.24 (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 define an action of G on Ω as follows:

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

This can be checked to be a well-defined action of G on Ω which is transitive (i.e., there is exactly one orbit). The stabiliser of the coset Hg is the conjugate H^g of the original subgroup H. Since we have an action, we associate a permutation representation $\rho\colon G \to \mathrm{Sym}(\Omega)$. The basic properties of ρ are summarised as follows:

Theorem 2.25 *Let H be a subgroup of G, let $\Omega = \{ Hx \mid x \in G \}$, and let G act on Ω by right multiplication. Let $\rho\colon G \to \mathrm{Sym}(\Omega)$ be the associated permutation representation.*

(i) *If $H < G$, then $G\rho$ is a non-trivial subgroup of* $\mathrm{Sym}(\Omega)$*;*

(ii) $\ker \rho = \bigcap_{x \in G} H^x$*;*

(iii) *the kernel* $\ker \rho$ *is the largest normal subgroup of G contained in H.*

Definition 2.26 We call this intersection $\bigcap_{x \in G} H^x$ (occurring as the kernel here) the *core* of H in G and denote it by $\mathrm{Core}_G(H)$.

p-Groups

We finish our section on group actions by establishing some tools concerning actions of p-groups. We then apply them to deduce results about the structure of such groups.

Definition 2.27 Let p be a prime number. A finite group G is called a *p-group* if its order is a power of p:

$$|G| = p^n \qquad \text{for some } n \geqslant 0.$$

An important tool relating to p-groups is the following:

Lemma 2.28 *Let G be a finite p-group and let G act on the finite set Ω. Define*

$$\mathrm{Fix}_G(\Omega) = \{\, \omega \in \Omega \mid \omega^x = \omega \text{ for all } x \in G \,\},$$

the set of fixed-points in the action. Then

$$|\mathrm{Fix}_G(\Omega)| \equiv |\Omega| \pmod{p}.$$

(Recall that to say two numbers are congruent modulo p means that their difference is divisible by p. Thus we are saying that

$$|\mathrm{Fix}_G(\Omega)| + kp = |\Omega|$$

for some integer $k \geqslant 0$.)

Proof: Express Ω as a disjoint union of orbits:

$$\Omega = \Omega_1 \cup \Omega_2 \cup \cdots \cup \Omega_k.$$

Suppose (without loss of generality) that $|\Omega_i| = 1$ for $i = 1, 2, \ldots, \ell$ and $|\Omega_i| > 1$ for $i = \ell + 1, \ldots, k$. So

$$\mathrm{Fix}_G(\Omega) = \Omega_1 \cup \Omega_2 \cup \cdots \cup \Omega_\ell \qquad \text{and} \qquad |\mathrm{Fix}_G(\Omega)| = \ell.$$

By the Orbit-Stabiliser Theorem (Theorem 2.9),

$$|\Omega_i| = |G : G_{\omega_i}| = |G|/|G_{\omega_i}|$$

for all i, where $\omega_i \in \Omega_i$. Now $|G|$ is a power of the prime p and hence each $|\Omega_i|$ is also a power of p. Therefore

$$p \text{ divides } |\Omega_i| \qquad \text{for } i = \ell + 1, \ldots, k.$$

Hence

$$\begin{aligned} |\Omega| &= |\Omega_1| + |\Omega_2| + \cdots + |\Omega_k| \\ &= |\mathrm{Fix}_G(\Omega)| + \sum_{i=\ell+1}^{k} |\Omega_i| \\ &\equiv |\mathrm{Fix}_G(\Omega)| \pmod{p}. \end{aligned}$$

□

As an application we shall prove:

Proposition 2.29 *Let G be a finite p-group. If N is a non-trivial normal subgroup of G, then*

$$N \cap \mathrm{Z}(G) \neq \mathbf{1}.$$

In particular, since G is a normal subgroup of itself, we obtain:

Corollary 2.30 *The centre of a non-trivial finite p-group is itself non-trivial.* □

Proof of Proposition 2.29: Since $N \trianglelefteq G$, we have $g^x = x^{-1}gx \in N$ for all $g \in N$ and $x \in G$. Consequently we may define an action of G on N by

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

(The conditions for an action follow from by the same argument as in Example 2.11. What is special here is that normality ensures that when we apply an element of G to an element of N we end up back inside N.) Now G is a p-group, so by Lemma 2.28:

$$|\mathrm{Fix}_G(N)| \equiv |N| \equiv 0 \pmod{p}$$

(since $|N| = p^r$ for some $r \geqslant 1$). Note

$$\begin{aligned} \mathrm{Fix}_G(N) &= \{\, g \in N \mid x^{-1}gx = g \text{ for all } x \in G \,\} \\ &= \{\, g \in N \mid gx = xg \text{ for all } x \in G \,\} \\ &= \{\, g \in N \mid g \in \mathrm{Z}(G) \,\} \\ &= N \cap \mathrm{Z}(G). \end{aligned}$$

Thus

$$|N \cap \mathrm{Z}(G)| \equiv 0 \pmod{p},$$

so

$$N \cap \mathrm{Z}(G) \neq \mathbf{1}.$$

□

We shall meet several further applications of Lemma 2.28 in the next section.

Section 3

Cauchy's Theorem and Sylow's Theorem

Sylow's Theorem was proved in the previous course (MT4003). Later in this section, I shall prove it (with the exception of existence of Sylow subgroups, which will be relegated to a problem sheet). This will be done again since it illustrates a major application of group actions. We begin with a related, but weaker, result.

Theorem 3.1 (Cauchy's Theorem) *Let G be a finite group, let p be a prime number and suppose that p divides $|G|$. Then G possesses an element of order p.*

One standard method of proof for this theorem is to proceed by induction on $|G|$. The following is a slick proof relying on group actions.

PROOF: Let

$$\Omega = \{\, (x_1, x_2, \ldots, x_p) \mid x_i \in G \text{ for all } i \text{ and } x_1 x_2 \ldots x_p = 1 \,\}.$$

Note that if x_1, x_2, $\ldots$, x_{p-1} are arbitrary elements of G, then there is a unique choice of x_p such that $(x_1, x_2, \ldots, x_p) \in \Omega$, namely

$$x_p = (x_1 x_2 \ldots x_{p-1})^{-1}.$$

Hence

$$|\Omega| = |G|^{p-1}.$$

Let H be a cyclic group of order p, say $H = \langle \pi \rangle$ where π is the p-cycle $(1\,2\,\ldots\,p)$. Let H act on Ω by cyclically permuting the entries:

$$(x_1, x_2, \ldots, x_p)^{\pi} = (x_2, x_3, \ldots, x_p, x_1).$$

Note that if $(x_1, x_2, \ldots, x_p) \in \Omega$, then

$$\begin{aligned} x_2 x_3 \ldots x_p x_1 &= x_1^{-1} \cdot x_1 x_2 \ldots x_p \cdot x_1 \\ &= x_1^{-1} \cdot 1 \cdot x_1 = 1. \end{aligned}$$

Hence $(x_2, x_3, \ldots, x_p, x_1) \in \Omega$. Thus we have defined a map

$$\begin{aligned} \Omega \times H &\to \Omega \\ \big((x_1, x_2, \ldots, x_p), \pi^i\big) &\mapsto (x_{i+1}, \ldots, x_p, x_1, \ldots, x_i) \end{aligned}$$

and this is an action of H on Ω. Since H is a p-group, Lemma 2.28 gives

$$\begin{aligned} |\mathrm{Fix}_H(\Omega)| &\equiv |\Omega| \pmod{p} \\ &= |G|^{p-1} \\ &\equiv 0 \pmod{p}. \end{aligned} \tag{3.1}$$

Now note that $(x_1, x_2, \ldots, x_p) \in \mathrm{Fix}_H(\Omega)$ means that

$$(x_1, x_2, \ldots, x_p) = (x_1, x_2, \ldots, x_p)^\pi = (x_2, x_3, \ldots, x_p, x_1)$$

so

$$x_1 = x_2 = \cdots = x_p.$$

Hence

$$\begin{aligned} \mathrm{Fix}_H(\Omega) &= \{\, (x, x, \ldots, x) \mid (x, x, \ldots, x) \in \Omega \,\} \\ &= \{\, (x, x, \ldots, x) \mid x \in G,\ x^p = 1 \,\}. \end{aligned}$$

Certainly $(1, 1, \ldots, 1) \in \mathrm{Fix}_H(\Omega)$, so Equation (3.1) implies that

$$|\mathrm{Fix}_H(\Omega)| \geqslant p.$$

In particular, there exists $x \in G$ with $x \neq 1$ such that

$$x^p = 1.$$

Hence $o(x) = p$. □

Corollary 3.2 *A finite group is a p-group if and only if every element has order equal to a power of p.*

PROOF: If G is a p-group, then a corollary of Lagrange's Theorem (Corollary 1.15) shows that every element has order dividing $|G|$, so every element has order equal to a power of p.

Conversely if G is not a p-group, then there exists a prime $q \neq p$ which divides $|G|$. Cauchy's Theorem provides an element in G of order q and this is not a power of p. □

We now turn to consider Sylow's Theorem.

Definition 3.3 Let p be a prime number and G be a finite group. Write $|G| = p^n m$ where p does not divide m. A *Sylow p-subgroup* of G is a subgroup of order p^n.

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

Theorem 3.4 (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 (mod p) *and divides m;*

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

Before proving the last three parts of this theorem, comments should be made as to what the theorem actually achieves for us. Part (i) guarantees existence of a subgroup within a finite group. This is useful since the best result we had previously was a theorem that could only be used for non-existence (Lagrange's Theorem). Once we have a subgroup, then we can act on the cosets and the entire machinery of the previous section can be exploited. Part (ii) tells us that these subgroups occur in a very restricted manner. Once we have a single Sylow p-subgroup P, then obviously every conjugate of P will also be a Sylow p-subgroup (since they all have the same order). This second part of the theorem guarantees that *all* the Sylow p-subgroups of the group arise in this way and so once we have one Sylow p-subgroup, we have all others in an expected manner. Part (iii) provides useful numeric restrictions upon how many Sylow subgroups occur. Finally, part (iv) tells us something stronger than Lagrange's Theorem does about the p-subgroups of G. Lagrange's Theorem tells us that Sylow p-subgroups are the largest p-subgroups of G in terms of *subgroup order*. The final part of the theorem tells us they are also *maximal* in terms of *containment*. Specifically, if we were to draw a diagram of the subgroups of G as suggested in Chapter 1, then the p-subgroups of G all occur as the collections of the nodes below a Sylow p-subgroup in the diagram.

PROOF: (i) Omitted: see Problem Sheet III.

For the remaining three parts we shall make use of various facts already established. The first two concern the product set HK from Lemma 1.21:

- If $H \leqslant G$ and $K \trianglelefteq G$, then $HK \leqslant G$;
- $|HK| = |H| \cdot |K| / |H \cap K|$.

Next, we shall be acting by conjugation so need to recall the normaliser (which is the stabiliser for conjugation on subgroups) and a particular property:

- $\mathrm{N}_G(H) = \{\, x \in G \mid H^x = H \,\}$;
- $H \trianglelefteq \mathrm{N}_G(H)$.

Finally the conjugation action will feature a p-group doing the acting, so we need to make use of Lemma 2.28:

- If H is a p-group acting on Ω, then $|\mathrm{Fix}_H(\Omega)| \equiv |\Omega| \pmod{p}$.

(ii)–(iv): Let P be a Sylow p-subgroup of G (which exists since we are assuming part (i) to have been already proved). Let Σ be the set of all conjugates of P:

$$\Sigma = \{\, P^g \mid g \in G \,\}.$$

Conjugation by an element induces an automorphism of G. Hence Σ consists of *some* of the Sylow p-subgroups. We must show that $|\Sigma| \equiv 1 \pmod{p}$, that Σ consists of *all* the Sylow p-subgroups of G and that every p-subgroup of G is contained in some member of Σ.

First let P act by conjugation on Σ:

$$\begin{aligned} \Sigma \times P &\to \Sigma \\ (Q, x) &\mapsto Q^x = x^{-1} Q x. \end{aligned}$$

Since P is a p-group, we may apply Lemma 2.28:

$$|\Sigma| \equiv |\mathrm{Fix}_P(\Sigma)| \pmod{p}.$$

Certainly P is fixed in this action: $P^g = P$ for all $g \in P$. Suppose that $Q \in \mathrm{Fix}_P(\Sigma)$. This means that

$$Q^g = Q \qquad \text{for all } g \in P;$$

that is, $P \leqslant \mathrm{N}_G(Q)$. On the other hand, $Q \trianglelefteq \mathrm{N}_G(Q)$, so we may apply Lemma 1.21(ii) to see that PQ is a subgroup of $\mathrm{N}_G(Q)$, and hence a subgroup of G. Part (iv) of the lemma tells us that

$$|PQ| = \frac{|P| \cdot |Q|}{|P \cap Q|},$$

so PQ is a p-subgroup of G. On the other hand, $P \leqslant PQ$ and $Q \leqslant PQ$, so as both P and Q are Sylow p-subgroups of G (that is, p-subgroups of G of largest possible order), we must have

$$Q = PQ = P.$$

Hence

$$\mathrm{Fix}_P(\Sigma) = \{P\},$$

so

$$|\Sigma| \equiv |\mathrm{Fix}_P(\Sigma)| = 1 \pmod{p}.$$

Now let H be any p-subgroup of G. Let H act on our set Σ by conjugation:

$$\begin{aligned} \Sigma \times H &\to \Sigma \\ (Q, g) &\mapsto Q^g. \end{aligned}$$

By Lemma 2.28,

$$|\mathrm{Fix}_H(\Sigma)| \equiv |\Sigma| \equiv 1 \pmod{p}.$$

Hence there exists at least one member of Σ, say Q, fixed by H:

$$Q^g = Q \qquad \text{for all } g \in H.$$

Therefore $H \leqslant \mathrm{N}_G(Q)$. Since $Q \trianglelefteq \mathrm{N}_G(Q)$, we see that HQ is a subgroup of $\mathrm{N}_G(Q)$, and hence of G, of order

$$|HQ| = \frac{|H| \cdot |Q|}{|H \cap Q|}.$$

Thus HQ is a p-subgroup of G containing the Sylow p-subgroup Q. This forces $HQ = Q$, so

$$H \leqslant HQ = Q.$$

Thus, every p-subgroup of G is contained in a conjugate of our original Sylow p-subgroup P and these certainly are among the Sylow p-subgroups of G. Consequently part (iv) of the Sylow's Theorem is now established.

Part (ii) now follows quickly from what we have established. If R is *any* Sylow p-subgroup of G, taking $H = R$ in the above argument shows that $R \leqslant Q$ for some $Q \in \Sigma$. But R and Q are both Sylow p-subgroups of G, so have the same order, so $R = Q \in \Sigma$. In conclusion, Σ consists of all the Sylow p-subgroups of G, and therefore they are all conjugate, and the number of Sylow p-subgroups is congruent to 1 (mod p).

To complete the proof of part (iii), recall that the number of conjugates of a subgroup equals the index of its normaliser:

$$|\Sigma| = |G : \mathrm{N}_G(P)|.$$

Now $P \leqslant \mathrm{N}_G(P) \leqslant G$, so

$$m = |G : P| = |G : \mathrm{N}_G(P)| \cdot |\mathrm{N}_G(P) : P|.$$

Hence $|\Sigma| = |G : \mathrm{N}_G(P)|$ divides m. □

Sylow's Theorem turns out to be a very powerful tool in elucidating the structure of a finite group. It is useful in finding subgroups and even normal subgroups. In many ways it was the first result which enabled the search for finite simple groups to begin.

Definition 3.5 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. When G is simple this process yields nothing new: one of these groups is trivial and the other is just a copy of G. Of course putting the information back together again afterwards is far from straightforward. Later in the course we shall see that in some sense there is a unique factorisation of groups into a number of simple factors. We shall meet *some* ways of putting groups back together, but this is very much an imprecise part of the theory. The few examples we shall give will go very little way in showing how to put groups together.

Example 3.6 Let G be a group of order 40. Then G is not simple: indeed, G has a normal Sylow 5-subgroup.

PROOF: $|G| = 40 = 2^3 \cdot 5$. By Sylow's Theorem, G possesses at least one Sylow 5-subgroup F, and the number of Sylow 5-subgroups is n_5, where

$$n_5 \equiv 1 \pmod 5 \qquad \text{and} \qquad n_5 \mid 8.$$

This forces $n_5 = 1$, so F is the unique Sylow 5-subgroup of G. Hence

$$F^g = F \qquad \text{for all } g \in G,$$

so $F \trianglelefteq G$. □

Example 3.7 Let G be a group of order 56. Then G is not simple: indeed, either G has a normal Sylow 2-subgroup or it has a normal Sylow 7-subgroup.

PROOF: $|G| = 56 = 2^3 \cdot 7$. Let n_7 be the number of Sylow 7-subgroups of G. Then

$$n_7 \equiv 1 \pmod 7 \qquad \text{and} \qquad n_7 \mid 8.$$

Hence $n_7 = 1$ or 8. If $n_7 = 1$, then the unique Sylow 7-subgroup of G is normal in G.

Suppose $n_7 = 8$. Consider two distinct Sylow 7-subgroups S_1 and S_2 of G. Then $|S_1| = |S_2| = 7$. The intersection $S_1 \cap S_2$ is a proper subgroup of S_1, so $|S_1 \cap S_2|$ divides 7, by Lagrange's Theorem. Hence $S_1 \cap S_2 = \mathbf{1}$. It follows that each Sylow 7-subgroup of G contains 6 non-identity elements (all of order 7) and these are contained in no other Sylow 7-subgroup. Hence the Sylow 7-subgroups account for

$$8 \times 6 = 48 \text{ elements of order } 7.$$

So G only contains 8 elements which do not have order 7. There can therefore be only one Sylow 2-subgroup (of order 8 consisting of these remaining 8 elements) and this is normal in G. □

Example 3.8 Let G be a group of order 36. Then G is not simple.

PROOF: 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:

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

(see Example 2.24). A group action determines a permutation representation and consequently we obtain a homomorphism $\rho\colon G \to S_4$. Since $|G| = 36 \geqslant |S_4| = 24$, we certainly have $\ker \rho \neq \mathbf{1}$. On the other hand, Theorem 2.25(i) 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 3.9 *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 2.25 tells us that the kernel of ρ is contained in T, while it must be a proper subgroup of T as $T \not\trianglelefteq G$. 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 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. □

These examples illustrate how we may apply Sylow's Theorem to show that certain groups are not simple. The next section discusses the importance of simple groups within an appropriate notion of factorisation of groups.

Section 4

The Jordan–Hölder Theorem

We start with a general definition.

Definition 4.1 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

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

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*. Note that we do not require each subgroup in the series to be normal in the whole group, only that it is normal in the previous subgroup in the chain. A *normal series* is a series where G_i is a normal subgroup of G for all i. Note also that the length n is also the number of factors occurring.

Obviously the above definition is rather generic. We shall be interested in three different types of series in this course and for all three we shall require special properties of the factors. The first case is where the factors are all required to be simple groups.

Definition 4.2 A *composition series* for a group G is a finite chain of subgroups

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

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.

The quotient groups

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

are called the *composition factors* of G.

Example 4.3 Let $G = S_4$, the symmetric group of degree 4. We have the following chain of subgroups:

$$S_4 > A_4 > V_4 > \langle (1\ 2)(3\ 4) \rangle > \mathbf{1}. \tag{4.1}$$

We know $A_4 \trianglelefteq S_4$ and $V_4 \trianglelefteq A_4$. Since V_4 is an abelian group, $\langle (1\ 2)(3\ 4) \rangle \trianglelefteq V_4$. Certainly $\mathbf{1} \trianglelefteq \langle (1\ 2)(3\ 4) \rangle$. Hence (4.1) is a series of subgroups each normal in the previous. We can calculate calculate the orders of each subgroup and hence calculate the order of the quotient groups:

$$\begin{aligned} |S_4/A_4| &= 2 \\ |A_4/V_4| &= 3 \\ |V_4/\langle (1\ 2)(3\ 4) \rangle| &= 2 \\ |\langle (1\ 2)(3\ 4) \rangle| &= 2. \end{aligned}$$

Thus the quotients are all of prime order. We now make use of the following fact:

Proposition 4.4 *Let p be a prime number. A group G of order p is cyclic and is simple.*

PROOF: Let H be a subgroup of G. Then $|H|$ divides $|G|$, by Lagrange's Theorem, so as $|G| = p$ is prime, we deduce $|H| = 1$ or $|H| = p = |G|$. Hence $H = \mathbf{1}$ or G. Thus the only *subgroups* G has are $\mathbf{1}$ and G, so certainly this applies to its *normal* subgroups. Thus G is simple.

Now let x be a non-identity element in G. Then $\langle x \rangle \neq \mathbf{1}$, so we have $\langle x \rangle = G$; i.e., G is cyclic. □

The conclusion is that the factors for the series (4.1) are simple groups (and cyclic), so we have a composition series for S_4. The composition factors are

$$C_2, C_3, C_2, C_2.$$

Example 4.5 The infinite cyclic group G has no composition series.

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

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

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 positive integer k (see Tutorial Sheet I). Hence G_{n-1} is an infinite cyclic group, so is not simple. This contradicts our series being a composition series. □

To understand the behaviour of composition series, consider the situation where we have subgroups

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

with $M \trianglelefteqslant N$. (The idea here is that M and N will be successive terms in a series which we are testing to see whether or not it is a composition series.) The Correspondence Theorem tells us that subgroups of N/M correspond to subgroups of N which contain M. Furthermore under this correspondence, normal subgroups of N/M correspond to normal subgroups of N which contain M. We conclude that

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

Proposition 4.6 *Every finite group possesses a composition series.*

PROOF: Let G be a finite group. We have at least one series of subgroups, namely

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

where each term is normal in the previous. Let

$$G = G_0 > G_1 > \cdots > G_n = \mathbf{1} \tag{4.2}$$

be the *longest* possible series of subgroups of G (so $G_{i+1} \trianglelefteqslant G_i$ for all i). This certainly exists since G has only finitely many subgroups, so only finitely many series. We claim that (4.2) is a composition series.

Suppose that it is not. Then one of the factors, say G_j/G_{j+1}, is not simple. This quotient then possesses a non-trivial proper normal subgroup and this corresponds to a subgroup N of G with

$$G_{j+1} < N \lhd G_j.$$

Then

$$G = G_0 > G_1 > \cdots > G_j > N > G_{j+1} > \cdots > G_n = \mathbf{1}$$

is a series in G (note $N \trianglelefteqslant G_j$, while certainly $G_{j+1} \trianglelefteqslant N$ since $G_{j+1} \trianglelefteqslant G_j$) and it is longer than (4.2). This contradicts our assumption that (4.2) is the longest such series. Hence (4.2) is indeed a composition series for G. □

On the other hand, we have an example of an infinite group (namely the infinite cyclic group) which does not possess a composition series. There are infinite groups that possess composition series, but infinite simple groups (which necessarily occur as some of the composition factors) are much less well understood than finite simple groups.

The important thing about composition series is that the composition factors occurring are essentially unique. This is the content of the following important theorem.

Theorem 4.7 (Jordan–Hölder Theorem) *Let G be a group and let*

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

and

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

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

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

and

$$\{H_0/H_1, H_1/H_2, \ldots, H_{m-1}/H_m\}$$

such that corresponding factors are isomorphic.

What this theorem tells us is that once we have determined one composition series for a (say, finite) group, then we have uniquely determined composition factors which can be thought of the ways of breaking our original group down into simple groups. Thus this is analogous to a 'prime factorisation' for groups.

To finish this section we shall present a few examples. However, to recognise when we have a composition series, we shall need to be able to recognise simple groups. We have already observed (Proposition 4.4) that cyclic groups of order p (p primes) are simple. It is not hard to show that these are all the abelian simple groups. The following theorem was (hopefully) established in the previous course.

Theorem 4.8 *Let $n \geqslant 5$. The alternating group A_n of degree n is simple.*

It is worth pointing out that at this point in time much much more is actually known. A mammoth effort by a large collection of mathematicians from the 1950s to the 1980s succeeded in classifying the finite simple groups. The complete proof runs to tens of thousands of pages of extremely complicated mathematics, and some doubt whether this actually 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 he or she is doing so.

Theorem 4.9 (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 families of groups of Lie type;*

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

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

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

that is, we successively construct the group $\mathrm{GL}_{n+1}(q)$ of invertible $(n+1)\times(n+1)$ matrices with entries from a field F containing 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 so-called *special linear group*; then factor out the centre (which happens to consist of all scalar matrices)

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

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 remaining twenty-six sporadic groups are as listed in the following table:

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 below

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

Unsurprisingly, we omit the proof of Theorem 4.9.

We finish the section by giving a few examples of composition series and composition factors.

Example 4.10 Let G be a finite abelian group of order n. Write

$$n = p_1^{r_1} p_2^{r_2} \dots p_s^{r_s}$$

where p_1, p_2, ..., p_s 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

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

are abelian simple groups. They are therefore cyclic of prime order. Now

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

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

$$\underbrace{C_{p_1}, C_{p_1}, \ldots, C_{p_1}}_{r_1 \text{ times}}, \underbrace{C_{p_2}, C_{p_2}, \ldots, C_{p_2}}_{r_2 \text{ times}}, \ldots, \underbrace{C_{p_s}, C_{p_s}, \ldots, C_{p_s}}_{r_s \text{ times}}.$$

Although the Jordan–Hölder Theorem tells us that the composition factors are essentially uniquely determined, the composition series need not be unique. For example, if $G = \langle x \rangle$ is cyclic of order 30, then we have several different composition series; e.g.,

$$G = \langle x \rangle > \langle x^2 \rangle > \langle x^6 \rangle > \mathbf{1}$$

where the composition factors are C_2, C_3 and C_5, and

$$G = \langle x \rangle > \langle x^3 \rangle > \langle x^{15} \rangle > \mathbf{1}$$

where the composition factors are C_3, C_5 and C_2; etc.

Later in the course we shall characterise the finite groups whose composition factors are cyclic as being the soluble groups.

Our final example has a unique composition series:

Example 4.11 Let $n \geqslant 5$ and consider the symmetric group S_n of degree n. We have the following series:

$$S_n > A_n > \mathbf{1} \tag{4.3}$$

which has factors C_2 and A_n. Both of these are simple groups, so (4.3) is a composition series for S_n. Furthermore it can be shown that S_n has precisely three normal subgroups (namely those occurring in the above series) and hence (4.3) is the only composition series for S_n.

To produce any more examples of composition series would probably require us to have more examples of groups. The Jordan–Hölder Theorem does also raise the question of how we put the composition factors back together. We have a unique decomposition but how complicated is the reverse process? The answers turns out to be rather difficult, but in the next section we shall meet some ways of creating new groups and this will give some ways of putting the composition factors back together.

Section 5

Building Groups

The purpose of this section is to describe two ways in which groups can be built using smaller groups. They are very much not the only ways that the decomposition process used to produce composition series can be reversed, but they are the easiest two to describe and handle. The first is the direct product, which was mentioned in the MT4003 course.

Direct products

Definition 5.1 Let G_1, G_2, ..., G_n be a collection of groups (all of whose binary operations are written multiplicatively). The (*external*) *direct product* is

$$G_1 \times G_2 \times \cdots \times G_n = \{\, (x_1, x_2, \ldots, x_n) \mid x_i \in G_i \text{ for all } i \,\}$$

with componentwise multiplication

$$(x_1, x_2, \ldots, x_n)(y_1, y_2, \ldots, y_n) = (x_1 y_1, x_2 y_2, \ldots, x_n y_n).$$

It is easy to check that $G = G_1 \times G_2 \times \cdots \times G_n$ is a group. We shall denote the identity element in each group G_i by 1. The identity element of G is then

$$(1, 1, \ldots, 1)$$

(the sequence containing the identity element of the group G_i in the ith position), while

$$(x_1, x_2, \ldots, x_n)^{-1} = (x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1}).$$

Write

$$\bar{G}_i = \{\, (1, \ldots, 1, x, 1, \ldots, 1) \mid x \in G_i \,\}$$

(where x occurs in the ith component). Then $\bar{G}_i$ is a subgroup of G; indeed the map

$$x \mapsto (1, \ldots, 1, x, 1, \ldots, 1)$$

is an isomorphism between G_i and $\bar{G}_i$. Furthermore

$$(y_1, \ldots, y_n)^{-1}(1, \ldots, 1, x, 1, \ldots, 1)(y_1, \ldots, y_n) = (1, \ldots, 1, y_i^{-1}xy_i, 1, \ldots, 1),$$

so $\bar{G}_i \trianglelefteq G$ (for $i = 1, 2, \ldots, n$).

Note that

$$(x_1, x_2, \ldots, x_n) = (x_1, 1, \ldots, 1)(1, x_2, 1, \ldots, 1) \ldots (1, \ldots, 1, x_n),$$

so

$$G = \bar{G}_1\bar{G}_2 \ldots \bar{G}_n.$$

Also

$$\bar{G}_1 \ldots \bar{G}_{i-1}\bar{G}_{i+1} \ldots \bar{G}_n = \{\, (x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) \mid x_j \in G_j \text{ for } j \neq i \,\},$$

so

$$\bar{G}_i \cap \bar{G}_1 \ldots \bar{G}_{i-1}\bar{G}_{i+1} \ldots \bar{G}_n = \mathbf{1}.$$

We give the following name to the situation we have just described:

Definition 5.2 Let G be a group and let $H_1, H_2, \ldots, H_n$ be subgroups of G. We say that G is the (*internal*) *direct product* of the subgroups H_i if

(i) H_i is a normal subgroup of G for all i;

(ii) $G = H_1H_2 \ldots H_n$;

(iii) $H_i \cap H_1H_2 \ldots H_{i-1}H_{i+1} \ldots H_n = \mathbf{1}$ for all i.

Theorem 5.3 (i) *The external direct product $G_1 \times G_2 \times \cdots \times G_n$ is the internal direct product of the subgroups $\bar{G}_1, \bar{G}_2, \ldots, \bar{G}_n$ defined above.*

(ii) *Let G be the internal direct product of the subgroups $H_1, H_2, \ldots, H_n$. Then*

$$G \cong H_1 \times H_2 \times \cdots \times H_n.$$

In view of this theorem it is usual not to distinguish between internal and external direct products. We often even go so far as to write '$=$' in part (ii) instead of '$\cong$'.

It should be noted that the condition for internal direct product is considerably stronger than '$H_i \cap H_j = \mathbf{1}$ for $i \neq j$'. This latter condition is not sufficient to ensure we have a direct product.

PROOF: We have already noted that (i) holds.

(ii) Define ϕ: $H_1 \times H_2 \times \cdots \times H_n \to G$ by

$$(x_1, x_2, \ldots, x_n) \mapsto x_1 x_2 \ldots x_n.$$

This is surjective since $G = H_1 H_2 \ldots H_n$. To show that ϕ is a homomorphism, we shall first show that elements from distinct H_i commute. Let $x \in H_i$ and $y \in H_j$ where $i \neq j$. Consider the element

$$x^{-1} y^{-1} x y.$$

(This is the *commutator* which we shall discuss in greater detail later in the course.) Note that

$$x^{-1}(y^{-1}xy) \in H_i \qquad \text{as } H_i \trianglelefteq G$$

and

$$(x^{-1}y^{-1}x)y \in H_j \qquad \text{as } H_j \trianglelefteq G.$$

Thus $x^{-1}y^{-1}xy \in H_i \cap H_j = \mathbf{1}$, so $x^{-1}y^{-1}xy = 1$ and therefore $xy = yx$.

Now if $(x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) \in H_1 \times H_2 \times \cdots \times H_n$, then

$$\begin{aligned}(x_1, \ldots, x_n)\phi \cdot (y_1, \ldots, y_n)\phi &= x_1 x_2 \ldots x_n y_1 y_2 \ldots y_n \\ &= x_1 y_1 \cdot x_2 \ldots x_n y_2 \ldots y_n \\ &= x_1 y_1 \cdot x_2 y_2 \cdot \ldots \cdot x_n y_n \\ &= (x_1 y_1, x_2 y_2, \ldots, x_n y_n)\phi \\ &= \big[(x_1, \ldots, x_n)(y_1, \ldots, y_n)\big]\phi.\end{aligned}$$

Hence ϕ is a homomorphism.

Finally if $(x_1, x_2, \ldots, x_n) \in \ker \phi$, then

$$x_1 x_2 \ldots x_n = 1,$$

so

$$\begin{aligned}x_i &= x_{i-1}^{-1} \ldots x_2^{-1} x_1^{-1} x_n^{-1} \ldots x_{i+1}^{-1} \\ &= x_1^{-1} \ldots x_{i-1}^{-1} x_{i+1}^{-1} \ldots x_n^{-1},\end{aligned}$$

so

$$x_i \in H_i \cap H_1 H_2 \ldots H_{i-1} H_{i+1} \ldots H_n = \mathbf{1}.$$

Therefore $x_i = 1$ for all i and we deduce that $\ker \phi = \mathbf{1}$.

This shows that ϕ is an isomorphism, so

$$G \cong H_1 \times H_2 \times \cdots \times H_n.$$

□

How direct products help us: Suppose we have a group G and we manage to find a system H_1, H_2, ..., H_n of (normal) subgroups such that G is the internal direct product. The theorem then tells us that

$$G \cong H_1 \times H_2 \times \cdots \times H_n$$

(an external direct product). The group multiplication in the latter is essentially straightforward: once we know how to multiply in each H_i (which should be easier since they are supposed to be smaller than G) then the multiplication in G is easily understood.

Semidirect products

We now wish to consider the situation where a group G can be expressed as $G = HN$ with $H \cap N = \mathbf{1}$ and only $N \trianglelefteq G$. (The direct product situation is when $H \trianglelefteq G$ also holds.) An element in G is expressible as $g = hn$ where $h \in H$ and $n \in N$. If we attempt to multiply two elements of G, then we calculate

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

Here $h_1 h_2 \in H$, $h_2^{-1} n_2 h_2 \in N$ (as $N \trianglelefteq G$) and so $(h_2^{-1} n_1 h_2) n_2 \in N$. 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 follow the same strategy as for direct products. We shall define an external semidirect product, establish certain properties and then define an internal semidirect product which will be isomorphic to an external one.

We shall need the following object as part of the construction. Recall (from Definition 2.18) that an automorphism of a group G is a map $G \to G$ which is an isomorphism.

Definition 5.4 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 is left as an exercise to check that $\operatorname{Aut} G$ is a group. (It is very similar to the proof that a symmetric group forms a group. Indeed $\operatorname{Aut} G$ is a subgroup of the symmetric group $\operatorname{Sym}(G)$.)

Definition 5.5 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 $H \ltimes_\phi N$ and is the set

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

with multiplication given by

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

If $h \in H$, then $h\phi$ is an automorphism of N and we shall write $n^{h\phi}$ 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 in a way that we shall use later.) This means that the multiplication in $H \ltimes_\phi N$ at least has meaning.

(As an aside, the above semidirect product might also be denoted by $N \rtimes_\phi H$, but this usually involves other additional notational adjustments so we avoid it.)

Proposition 5.6 *The semidirect product $H \ltimes_\phi N$ is a group.*

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

$$\begin{aligned}
[(h_1, n_1)(h_2, n_2)]\,(h_3, n_3) &= (h_1 h_2, n_1^{h_2\phi} n_2)(h_3, n_3) \\
&= (h_1 h_2 h_3, (n_1^{h_2\phi} n_2)^{h_3\phi} n_3) \\
&= (h_1 h_2 h_3, n_1^{(h_2\phi)(h_3\phi)} n_2^{h_3\phi} n_3),
\end{aligned}$$

while

$$\begin{aligned}
(h_1, n_1)\,[(h_2, n_2)(h_3, n_3)] &= (h_1, n_1)(h_2 h_3, n_2^{h_3\phi} n_3) \\
&= (h_1 h_2 h_3, n_1^{(h_2 h_3)\phi} n_2^{h_3\phi} n_3) \\
&= (h_1 h_2 h_3, n_1^{(h_2\phi)(h_3\phi)} n_2^{h_3\phi} n_3).
\end{aligned}$$

Comparing these products we deduce that the binary operation on the semidirect product is associative.

Identity:

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

(as the automorphism $h\phi$ must map 1 to 1) and

$$(h, n)(1, 1) = (h1, n^{1\phi} 1) = (h, n^{\mathrm{id}}) = (h, n)$$

(as the automorphism 1ϕ must be the identity so map n to n). Hence $(1, 1)$ is the identity element in $H \ltimes_\phi N$.

Inverses:

$$(h,n)\left(h^{-1},(n^{(h^{-1})\phi})^{-1}\right)=(hh^{-1},(n^{(h^{-1})\phi})(n^{(h^{-1})\phi})^{-1})=(1,1)$$

and

$$\begin{aligned}\left(h^{-1},(n^{(h^{-1})\phi})^{-1}\right)(h,n)&=\left(h^{-1}h,[(n^{(h^{-1})\phi})^{-1}]^{h\phi}n\right)\\&=\left(1,(n^{(h^{-1})\phi.h\phi})^{-1}n\right)&(1)\\&=\left(1,(n^{(h^{-1}h)\phi})^{-1}n\right)&(2)\\&=\left(1,(n^{1\phi})^{-1}n\right)\\&=(1,n^{-1}n)&(3)\\&=(1,1)\end{aligned}$$

(as (1) $h\phi$ is an homomorphism so maps inverses to inverses, (2) ϕ is a homomorphism, and (3) 1ϕ is the identity map so maps n to n). Thus $(h^{-1},(n^{(h^{-1})\phi})^{-1})$ is the inverse of (h,n) in $H\ltimes_\phi N$.

This completes the proof that $H\ltimes_\phi N$ is a group. □

Now define

$$\bar{H}=\{\,(h,1)\mid h\in H\,\}\qquad\text{and}\qquad\bar{N}=\{\,(1,n)\mid n\in N\,\}.$$

Define $\alpha\colon H\to\bar{H}$ by $h\mapsto(h,1)$ and $\beta\colon N\to\bar{N}$ by $n\mapsto(1,n)$. Clearly α and β are bijections. Now

$$(h_1\alpha)(h_2\alpha)=(h_1,1)(h_2,1)=(h_1h_2,1^{h_2\phi}1)=(h_1h_2,1)=(h_1h_2)\alpha$$

and

$$(n_1\beta)(n_2\beta)=(1,n_1)(1,n_2)=(1,n_1^{1\phi}n_2)=(1,n_1n_2)=(n_1n_2)\beta.$$

Hence α and β are isomorphisms. It follows that $\bar{H}$ and $\bar{N}$ are subgroups of $G=H\ltimes_\phi N$ which are isomorphic to H and N respectively.

Clearly $\bar{H}\cap\bar{N}=\mathbf{1}$. Also

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

so $G=\bar{H}\bar{N}$. So far these observations have some similarity to the direct product. The difference appears, however, when we consider conjugation:

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

so

$$(h,1)^{-1}(1,n)(h,1) = (1,n^{h\phi}). \tag{5.1}$$

We conclude that an element of $\bar{H}$ conjugates an element of $\bar{N}$ back into $\bar{N}$ and it does so by applying the corresponding automorphism of N to the component from N. So we then have $\bar{H} \leqslant \mathrm{N}_G(\bar{N})$, while $\bar{N} \leqslant \mathrm{N}_G(\bar{N})$ is always true. Hence $G = \bar{H}\bar{N} \leqslant \mathrm{N}_G(\bar{N})$ and we have

$$\bar{N} \trianglelefteqslant G.$$

We summarise these observations as follows:

Theorem 5.7 *Let H and N be groups, let $\phi\colon H \to \operatorname{Aut} N$ be a homomorphism and $G = H \ltimes_\phi N$, the semidirect product of N by H via ϕ. Then*

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

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

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

The Second Isomorphism Theorem then tells us that

$$G/\bar{N} = \bar{H}\bar{N}/\bar{N} \cong \bar{H}/(\bar{H} \cap \bar{N}) = \bar{H} \cong H.$$

So our semidirect product has a normal subgroup isomorphic to N and quotient group isomorphic to H.

We are now in a position to define what is meant by the internal version of the semidirect product.

Definition 5.8 Let G be a group. We say that G is the (*internal*) *semidirect product* of a subgroup N by another subgroup H if

(i) $N \trianglelefteqslant G$,

(ii) $G = HN$, and

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

In the situation when these conditions hold, we say that H is a *complement* to N. We shall also sometimes write $G = H \ltimes N$.

We now seek to show that an internal semidirect product 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 homomorphism $\phi\colon H \to \operatorname{Aut} N$ is.

Let G be an internal semidirect product of N by H. We shall define a map $\theta\colon H \times N \to G$ by

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

(At this point, we do not assume any group theoretical structure on the *set product* $H \times N$. It will eventually become a semidirect product.)

Now $G = HN$, so every element of G can be written in the form hn where $h \in H$ and $n \in N$. Therefore θ is surjective.

Suppose $hn = h'n'$ where $h, h' \in H$ and $n, n' \in N$. 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 we have 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 our semidirect product.

Now θ is a bijection

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

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

$$\begin{aligned} ((h_1, n_1)(h_2, n_2))\,\theta &= (h_1h_2, n_1^{h_2\phi}n_2)\theta \\ &= (h_1h_2, n_1^{h_2}n_2)\theta \\ &= h_1h_2n_1^{h_2}n_2 \\ &= h_1h_2 \cdot h_2^{-1}n_2h_2 \cdot n_2 \\ &= h_1n_1h_2n_2 \\ &= (h_1, n_1)\theta \cdot (h_2, n_2)\theta. \end{aligned}$$

Hence θ is a homomorphism and consequently is an isomorphism.

Theorem 5.9 *Let G be the internal semidirect product of N by H. Then $G \cong H \ltimes_\phi N$ 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 $h \in H$. □

As a consequence there is really no difference between external semidirect products and internal semidirect products. We shall therefore simply refer to the 'semidirect product.' Note that in both versions the homomorphism ϕ is simply telling us how the subgroup H acts by conjugation on the normal subgroup N.

For notational simplicity, we shall principally use internal semidirect products: there are simply fewer brackets kicking around and we can often suppress explicit reference to the homomorphism ϕ. Thus if we have a group G with subgroups H and N such that $N \trianglelefteqslant G$, $G = HN$ and $H \cap N = \mathbf{1}$, then we know that G is a semidirect product. We know its multiplication is then determined by the multiplication in the two smaller groups H and N together with an understanding of the way in which H acts by conjugation on N (i.e., we have the map ϕ determined). Provided we have this information available, we then 'understand' the structure of $H \ltimes N$.

In the examples which follow, we shall in the end be specifying the multiplication in our groups. We shall do this by means of a *presentation*. These were introduced briefly in MT4003. We shall use them in a very simple form. Informally a presentation has the form

$$G = \langle\, x_1, x_2, \ldots, x_d \mid r_1 = s_1, \ldots, r_k = s_k \,\rangle$$

and this indicates that G is the group generated by the elements x_1, x_2, $\ldots$, x_d subject to the requirement that the expressions (known as *relations*)

$$r_1 = s_1, \ldots, r_k = s_k$$

hold (i.e., the element in G given by the product r_1 equals the product s_1). For example,

$$C_n = \langle\, x \mid x^n = 1 \,\rangle,$$

while

$$D_{2n} = \langle\, x, y \mid x^n = y^2 = 1,\ y^{-1}xy = x^{-1} \,\rangle.$$

We shall be interested in presentations for semidirect products: we shall be giving information that specify the multiplications in the two subgroups N and H, while the conjugation of elements of H on those of N will also be specified (and it should be clear from the presentation that N is then forced to be a normal subgroup).

Example 5.10 Let G be a group of order 20. Let n_5 denote the number of Sylow 5-subgroups of G. Sylow's Theorem tells us that

$$n_5 \equiv 1 \pmod 5 \qquad \text{and} \qquad n_5 \mid 4.$$

Therefore $n_5 = 1$, so G has a unique Sylow 5-subgroup, say F. Then $F \trianglelefteq G$ 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 1.21 tells us that

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

Hence $G = TF$, $F \trianglelefteq G$ and $T \cap F = \mathbf{1}$. Thus $G = T \ltimes F$, the semidirect product of F by T.

We know that $|F| = 5$, so $F \cong C_5$; say $F = \langle x \rangle$ where $o(x) = 5$. We need to understand what possibilities there are for a homomorphism $\phi\colon T \to \operatorname{Aut} F$.

Consider any automorphism α of F. Then $\alpha\colon F \to F$ is a homomorphism so is determined by its effect on the generator x (if we know what $x\alpha$ is, then $(x^i)\alpha = (x\alpha)^i$ is determined for each i). Note that as α must be surjective, it must map x to another generator of F. Thus $x\alpha = x$, x^2, x^3 or x^4. (Note $x^5 = 1$, while these four elements all have order 5, so generate F and hence determine surjective homomorphisms $F \to F$; i.e., automorphisms of F.) Thus

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

Indeed $\operatorname{Aut} F \cong C_4$, since $\beta\colon x \mapsto x^2$ is a generator:

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

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

We now understand the structure of $\operatorname{Aut} F$. What about T? Since $|T| = 4$, there are two possibilities:

$$T \cong C_4 \qquad \text{or} \qquad T \cong C_2 \times C_2 \cong V_4.$$

Case 1: $T \cong C_4$.

If $\phi\colon T \to \operatorname{Aut} F$, then consider the image of ϕ is a subgroup of the cyclic group $\operatorname{Aut} F = \langle \beta \rangle$. Hence either $T\phi = \mathbf{1}$, $\langle \beta^2 \rangle$ or $\langle \beta \rangle$. We can choose our generator y for T such that y is mapped to our chosen generator for $T\phi$. Hence either $y\phi = 1$, or $y\phi = \beta^2$, or $y\phi = \beta$ (in the last case, ϕ is an isomorphism, in the first two, the kernel is non-trivial). Thus we have one of the following three possibilities:

$$y\phi = \mathrm{id}\colon x \mapsto x, \qquad y\phi = \beta^2\colon x \mapsto x^4, \qquad y\phi = \beta\colon x \mapsto x^2.$$

(We have saved ourselves some work by choosing y *after* we have determined what $T\phi$ is. The possibility that a generator z of T is mapped to $\beta^3 = \beta^{-1}$ is not considered, for in that case we choose $y = z^{-1}$.)

Therefore there are at most three essentially different possibilities in Case 1:

$$\begin{aligned} G &= \langle\, x, y \mid x^5 = y^4 = 1,\ y^{-1}xy = x \,\rangle \\ &= \langle\, x, y \mid x^5 = y^4 = 1,\ xy = yx \,\rangle \\ &= C_5 \times C_4 \cong C_{20} \end{aligned} \tag{5.2}$$

$$G = \langle\, x, y \mid x^5 = y^4 = 1,\ y^{-1}xy = x^4 \,\rangle \tag{5.3}$$

$$G = \langle\, x, y \mid x^5 = y^4 = 1,\ y^{-1}xy = x^2 \,\rangle. \tag{5.4}$$

Note that (5.3) and (5.4) are non-abelian groups, while (5.2) is abelian. All three groups have a unique Sylow 5-subgroup F. In (5.3), we calculate

$$y^{-2}xy^2 = y^{-1}(y^{-1}xy)y = y^{-1}x^4y = (y^{-1}xy)^4 = (x^4)^4 = x^{16} = x,$$

so y^2 commutes with x. We deduce that

$$\mathrm{C}_G(F) = \{\, g \in G \mid gh = hg \text{ for all } h \in F \,\}$$

is a group of order 10 (it contains x and y^2) for the group (5.3). A similar calculation in (5.4) shows that $\mathrm{C}_G(F) = F$ for this group. Hence there two non-abelian groups are not isomorphic.

We therefore do have three distinct groups: these groups definitely do exist since we can construct them using the semidirect product construction.

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

If $T\phi = \mathbf{1}$ (i.e., $\ker \phi = T$), choose any pair of generators y and z for T. We deduce

$$\begin{aligned} G &= \langle\, x, y, z \mid x^5 = y^2 = z^2 = 1,\ xy = yx,\ xz = zx,\ yz = zy \,\rangle \\ &= C_5 \times C_2 \times C_2 \cong C_2 \times C_{10}. \end{aligned}$$

If $T\phi \neq 1$, then $T\phi$ is a subgroup of $\operatorname{Aut} F = \langle \beta \rangle$, so must be cyclic. In addition, all elements in T have order dividing 2, so the same must be true of its image. Therefore $T\phi = \langle \beta^2 \rangle$. Pick $y \in T$ such that $y\phi = \beta^2$. Note $|T\phi| = 2$, so by the First Isomorphism Theorem, $|\ker \phi| = 2$. Choose $z \in T$ such that z generates this kernel. Then $T = \langle y, z \rangle$ and

$$G = \langle\, x, y, z \mid x^5 = y^2 = z^2 = 1,\ yz = zy,\ xz = zx,\ y^{-1}xy = x^4 \,\rangle.$$

Consider $x' = xz$. As x and z commute and $o(x)$ and $o(z)$ are coprime, we have $o(x') = o(x)o(z) = 10$. Also $(x')^2 = x^2z^2 = x^2$, which generates F, while $(x')^5 = x^5z^5 = z$. Hence $G = \langle x', y \rangle$ and

$$y^{-1}x'y = y^{-1}xzy = y^{-1}xyz = x^4z = (xz)^9 = (x')^{-1}.$$

Hence

$$\begin{aligned} G &= \langle\, x', y \mid (x')^{10} = y^2 = 1,\ y^{-1}x'y = (x')^{-1} \,\rangle \\ &\cong D_{20}. \end{aligned}$$

Conclusion: There are essentially five different groups of order 20.

Our final example has a more complicated aspect in that ideas from linear algebra become useful.

Example 5.11 Let G be a group of order $147 = 3 \cdot 7^2$ with non-cyclic Sylow 7-subgroups. The number of Sylow 7-subgroups 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 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 P is 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* $m(X)$ 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, $m(X)$ is a product of linear factors, so T is diagonalisable. Hence we may choose a new 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 $\lambda = 2$ and $\mu = 4$. Returning to a multiplicative notation we therefore have a group given by

$$\langle\, x, y, z \mid x^7 = y^7 = z^3 = 1,\ xy = yx,\ z^{-1}xz = x^2,\ z^{-1}yz = y^4 \,\rangle.$$

There are many more examples occurring here.

Section 6

Soluble Groups

We have already met the concept of a composition series for a group. In the next section 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 need the following concept.

Definition 6.1 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

$$xy = yx[x, y]. \tag{6.1}$$

The latter tells us that the commutator essentially measures by how much x and y fail to commute.

Lemma 6.2 *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 (6.1) and view it as telling us how to exchange group elements at the expense of introducing commutators. (This 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 I believe more can be learnt and understood via the collection process.

Definition 6.3 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 6.2 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

$$[x_1,y_1]\,[x_2,y_2]\ldots[x_n,y_n]$$

where $x_i, y_i \in G$ for each i.

Iterating this construction yields the derived series:

Definition 6.4 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. We then have a chain of subgroups

$$G = G^{(0)} \geqslant G^{(1)} \geqslant G^{(2)} \geqslant \cdots .$$

We shall see later that this is indeed a series in the sense of Definition 4.1 (in that each term is normal in the previous). Indeed far more is true as we shall see.

Definition 6.5 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.

Since when forming the derived series, we take the derived subgroup of the previous term at each stage, once we have a repetition then the series becomes constant. Thus if G is a soluble group of derived length d, its derived series has the form

$$G = G^{(0)} > G^{(1)} > G^{(2)} > \cdots > G^{(d)} = \mathbf{1}.$$

We seek to understand the properties a soluble group really has and to produce equivalent formulations so that examples can be more easily described. Accordingly, we being by establishing basic properties of the derived subgroup and the derived series.

Lemma 6.6 (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 a commutator of elements of G so belongs to the derived subgroup of G:

$$[x, y] \in G' \qquad \text{for all } x, y \in H.$$

Therefore

$$\langle\, [x, y] \mid x, y \in H \,\rangle \leqslant G',$$

so $H' \leqslant G'$.

(ii) 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 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

$$[a, b] \in G'\phi \qquad \text{for all } a, b \in K.$$

This forces $K' \leqslant G'\phi$. Using (ii) gives $K' = G'\phi$, as required. □

Lemma 6.7 *Subgroups and homomorphic images of soluble groups are themselves soluble.*

PROOF: Let G be a soluble group and H be a subgroup of G.

Claim: $H^{(i)} \leqslant G^{(i)}$ for all i.

We prove the claim by induction on i. The case $i = 0$ is the inclusion $H \leqslant G$ which holds by assumption.

Now suppose $H^{(i)} \leqslant G^{(i)}$. Apply Lemma 6.6(i) to give

$$(H^{(i)})' \leqslant (G^{(i)})';$$

that is,

$$H^{(i+1)} \leqslant G^{(i+1)}.$$

This completes the induction.

Now since G is soluble, $G^{(d)} = \mathbf{1}$ for some d. Therefore, as $H^{(d)} \leqslant G^{(d)}$, we have $H^{(d)} = \mathbf{1}$ and so we deduce that H is soluble.

Now let K be a homomorphic image of G. Thus there exists a surjective homomorphism $\phi\colon G \to K$.

Claim: $K^{(i)} = G^{(i)}\phi$ for all i.

We prove the claim by induction on i. The case $i = 0$ is the equation $K = G\phi$ which holds by assumption.

Now suppose $K^{(i)} = G^{(i)}\phi$. Thus ϕ induces a surjective homomorphism $G^{(i)} \to K^{(i)}$ and Lemma 6.6(iii) gives

$$(K^{(i)})' = (G^{(i)})'\phi;$$

that is,

$$K^{(i+1)} = G^{(i+1)}\phi.$$

This completes the induction.

Now as G is soluble we have $G^{(d)} = \mathbf{1}$ and thus

$$K^{(d)} = G^{(d)}\phi = \mathbf{1}\phi = \mathbf{1}.$$

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 6.8 *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 the second claim in Lemma 6.7, we have

$$G^{(d)}\pi = (G/N)^{(d)} = \mathbf{1}.$$

Hence

$$G^{(d)} \leqslant \ker \pi = N.$$

Therefore, by the first claim in Lemma 6.7,

$$(G^{(d)})^{(e)} \leqslant N^{(e)} = \mathbf{1};$$

that is,

$$G^{(d+e)} = \mathbf{1}.$$

Thus G is soluble. □

We have observed that if $\phi\colon G \to K$ is a surjective homomorphism then $G'\phi = K'$. In particular, if ϕ is an automorphism of G (that is, an isomorphism $G \to G$), then $G'\phi = G'$. We give the following special name to subgroups satisfying this property.

Definition 6.9 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. But then we have $H\phi^{-1} \leqslant H$ 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 for being a characteristic subgroup is less consistently developed than for, say, being a normal subgroup. I shall write

$$H \operatorname{char} G$$

to indicate that H is a characteristic subgroup of G.

Our observation above then is that

$$G' \operatorname{char} G$$

for all groups G and we shall soon see that all terms in the derived series are also characteristic.

Lemma 6.10 *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 the Correspondence Theorem does not work well with characteristic subgroups.)
- If $H \leqslant L \leqslant G$ and $H \operatorname{char} G$, then it does not necessarily follow that $H \operatorname{char} L$.

Proof of Lemma 6.10: (i) If $x \in G$, then $\tau_x\colon g \mapsto g^x$ is an 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 is an automorphism of H. Since $K \operatorname{char} H$, we deduce that $K^x = K\tau_x = K$. Thus $K \trianglelefteqslant G$. □

We have seen that $G' \operatorname{char} G$ holds. Recall the definition of the derived series:

$$G^{(0)} = G, \qquad G^{(i+1)} = (G^{(i)})' \quad \text{for } i \geqslant 0.$$

Therefore

$$G^{(i)} \operatorname{char} G^{(i-1)} \operatorname{char} G^{(i-2)} \operatorname{char} \cdots \operatorname{char} G^{(1)} \operatorname{char} G^{(0)} = G.$$

Applying Lemma 6.10(ii) we see that each $G^{(i)}$ is a characteristic subgroup (and hence a normal subgroup) of G for each i.

Proposition 6.11 *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. □

In particular, if G is a soluble group of derived length d then we have

$$G = G^{(0)} > G^{(1)} > \cdots > G^{(d)} = \mathbf{1}$$

and this is a normal series (each term is normal in G). In particular, we can consider the factors

$$G^{(0)}/G^{(1)},\ G^{(1)}/G^{(2)}, \ldots, G^{(d-1)}/G^{(d)};$$

i.e., the quotient groups $G^{(i)}/(G^{(i)})'$ for $i = 0, 1, \ldots, d-1$.

We now seek to elucidate information about these factors.

Lemma 6.12 *Let G be a group and N be a normal subgroup of G. Then 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. We often call G/G' the *abelianisation* of G.

Proof: 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 obtain $G' \leqslant N$.

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. □

In particular, the factors occurring in the derived series are all abelian. So if G is a soluble group, it has the derived series as a normal series with all factors abelian. The following result strengthens this and puts it into context.

Theorem 6.13 *Let G be a group. The following conditions are equivalent:*

(i) *G is soluble;*

(ii) *G has a chain of subgroups*

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

such that G_i is a normal subgroup of G and G_{i-1}/G_i is abelian for $i = 1, 2, \ldots, n$;

(iii) *G has a chain of subgroups*

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

such that G_i is a normal subgroup of G_{i-1} and G_{i-1}/G_i is abelian for $i = 1, 2, \ldots, n$.

We describe Condition (ii) as saying that G has a normal series with abelian factors, while (iii) says that G has a series (or subnormal series) with abelian factors.

PROOF: (i) $\Rightarrow$ (ii): The derived series is such a chain of subgroups.
(ii) $\Rightarrow$ (iii): Immediate: If $G_i \trianglelefteq G$ for $G_i \leqslant G_{i-1} \leqslant G$, then $G_i \trianglelefteq G_{i-1}$.
(iii) $\Rightarrow$ (i): Suppose

$$G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \ldots \geqslant G_n = \mathbf{1}$$

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 $G^{(i)} \leqslant G_i$. Now $G_{i+1} \trianglelefteq G_i$ and G_i/G_{i+1} is abelian. Hence $(G_i)' \leqslant G_{i+1}$ by Lemma 6.12. Further, by Lemma 6.6(i), $(G^{(i)})' \leqslant (G_i)'$. Hence

$$G^{(i+1)} = (G^{(i)})' \leqslant (G_i)' \leqslant G_{i+1}.$$

Hence by induction $G^{(n)} \leqslant G_n = \mathbf{1}$, so $G^{(n)} = \mathbf{1}$ and G is soluble. □

We now have a characterisation that a group is soluble if and only if it has a series with abelian factors. We shall obtain a further such equivalence by linking solubility to composition series. First, however, we note the following:

Example 6.14 An abelian group G is soluble. Indeed in an abelian group G

$$[x, y] = x^{-1}y^{-1}xy = 1 \qquad \text{for all } x \text{ and } y,$$

so $G' = \mathbf{1}$. (Of course, the condition $G' = \mathbf{1}$ is equivalent to G being abelian.)

In particular, the infinite cyclic group is soluble, though we know (Example 4.5) that this group does not have a composition series. Accordingly we cannot hope for composition series to give us complete information about soluble groups.

It turns out that as long as we avoid the infinite soluble groups, composition series do tell us whether or not our group is soluble.

Theorem 6.15 *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 part (ii) describes the groups with abelian composition factors.

PROOF: (ii) $\Rightarrow$ (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. Then $G_i \trianglelefteqslant G_{i-1}$ and G_{i-1}/G_i is abelian for each i. Thus this is a chain of subgroups as in part (iii) of Theorem 6.13 and therefore G is soluble by that result. Further

$$|G| = |G_0/G_1| \cdot |G_1/G_2| \cdot \ldots \cdot |G_{n-1}/G_n|,$$

a product of finitely many primes, so G is finite.

(i) $\Rightarrow$ (ii): Let G be a finite soluble group. Then by Theorem 6.13, G possesses a chain of subgroups

$$G = G_0 > G_1 > G_2 > \cdots > G_n = \mathbf{1} \tag{6.2}$$

such that $G_i \trianglelefteqslant G_{i-1}$ and G_{i-1}/G_i is abelian for all i. Note that G can only have at most finitely many such series. Thus we may assume that (6.2) is the longest series for G with abelian factors. Such a series must then be a composition series: for if some G_{i-1}/G_i is not simple, then there exists $N \trianglelefteqslant G_{i-1}$ with $G_i < N < G_{i-1}$. We then obtain a series

$$G = G_0 > \cdots > G_{i-1} > N > G_i > \cdots > G_n = \mathbf{1}$$

which is longer than (6.2) and the new factors occurring here satisfy

$$N/G_i \trianglelefteqslant G_{i-1}/G_i \qquad \text{and} \qquad G_{i-1}/N \cong \frac{G_{i-1}/G_i}{N/G_i}$$

(by the Third Isomorphism Theorem). Since G_{i-1}/G_i is abelian, we see that N/G_i and G_{i-1}/N are abelian. This contradicts the assumption that (6.2) is the longest series with abelian factors.

We now deduce that (6.2) is indeed a composition series and hence the composition factors of G are abelian. 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). □

So far this section has been rather devoid of examples. We have observed that all abelian groups are soluble, but this is not particularly far reaching. On the other hand, our two characterisation theorems, Theorems 6.13 and 6.15 do far better for helping us recognise (finite) soluble groups. These theorems tell us that a soluble group is one that is built from abelian groups.

Example 6.16 The symmetric group S_4 of degree 4 is soluble. Indeed in Example 4.3 we observed that

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

is a composition series for S_4 and the composition factors are C_2, C_3, C_2 and C_2. Hence S_4 is soluble by Theorem 6.15.

Example 6.17 The dihedral group D_{2n} of order $2n$ is soluble. Indeed D_{2n} contains an element α of order n, so $\langle \alpha \rangle$ has index 2 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 6.13.

Example 6.18 The symmetric group S_n of degree n is insoluble if $n \geqslant 5$. Indeed we know that A_n is non-abelian simple group, so is insoluble by Theorem 6.15. As a subgroup of a soluble group is always soluble, it must be the case that S_n is insoluble also.

Careful analysis of the examples in Section 3 shows that the groups we considered that were not simple in 3.6–3.9 are also soluble groups.

Finite soluble groups

For the rest of this section we shall work only with finite groups. Our goal is to study finite soluble groups in much greater detail and in particular prove Hall's Theorem concerning finite soluble groups. We shall prove these by induction on the group order. The method will involve working with quotients and so we begin by studying normal subgroups which are as small as possible.

Minimal normal subgroups

For the moment we shall work with arbitrary finite groups without assuming that they are also soluble. Solubility will return in due course.

Definition 6.19 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 which 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 $N = M$.

Note that, apart from the trivial group, all finite groups have minimal normal subgroups. To see this, we start with the group G itself. If this isn't a minimal normal subgroup, then there is a proper subgroup below it which is normal. If this isn't minimal, then there is a proper subgroup below it which is normal in G. Repeating this process must eventually stop (since G is finite) and yield a minimal normal subgroup.

We shall prove the following description of minimal normal subgroups.

Theorem 6.20 *A minimal normal subgroup of a finite group G is a direct product of isomorphic simple groups.*

In the case of a minimal normal subgroup of a finite soluble group, these simple groups will be cyclic of prime order. We shall work towards the proof of this theorem next. First we make the following definition.

Definition 6.21 A non-trivial group G is called *characteristically simple* if the only characteristic subgroups it has are $\mathbf{1}$ and G.

(Recall, from Definition 6.9, that a characteristic subgroup of G is a subgroup which is closed under applying all automorphisms of G.)

Lemma 6.22 *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 6.10(iii). Thus minimality of M forces $K = \mathbf{1}$ or $K = M$. Hence M is indeed characteristically simple. □

Theorem 6.20 then follows immediately from the following result. (The advantage of proving Theorem 6.23 over a direct attempt on Theorem 6.20 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 6.23 *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

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

(Recall what we mean by the direct product here: it is an internal direct product, so we need $S_i \cap S_1 \dots S_{i-1} S_{i+1} \dots S_k = \mathbf{1}$ for each i, as well as $N = S_1 S_2 \dots S_k$. We already assume $S_i \trianglelefteqslant G$, so the requirement $S_i \trianglelefteqslant N$ comes for free.)

Note that $S \in \mathscr{D}$, 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. Then as G is characteristically simple, N cannot be a characteristic subgroup of G. Hence there exists an automorphism ϕ of G such that

$$N\phi \not\leqslant N.$$

Let $N = S_1 \times S_2 \times \cdots \times S_k$ where each S_i is a minimal normal subgroup of G isomorphic to S. Therefore there exists i such that

$$S_i\phi \not\leqslant N.$$

Now ϕ is an automorphism of G, so $S_i\phi$ is a minimal normal subgroup of G. Now $N \cap S_i\phi \trianglelefteqslant G$ and $N \cap S_i\phi$ is properly contained in $S_i\phi$ (as $S_i\phi \not\leqslant N$). Therefore, by minimality, $N \cap S_i\phi = \mathbf{1}$. 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

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

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

Therefore

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

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 $J \trianglelefteqslant S_1$, then

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

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

We have now established Theorems 6.20 and 6.23 in a general setting. We are, however, only interested in soluble groups in the current section and Theorem 6.15 tells us that the only simple groups which can be occurring in this world 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 6.24 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 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

$$G \cong \underbrace{C_p \times C_p \times \cdots \times C_p}_{d \text{ times}}$$

for some d.

Putting together Theorem 6.15 and Theorem 6.20 gives:

Theorem 6.25 *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. We now move on to describe the type of subgroup this theorem concerns.

Hall subgroups

Definition 6.26 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 a Hall $\{p\}$-subgroup is precisely the same thing as a Sylow p-subgroup.

Example 6.27 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: thus, 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. If H were one of these, then we could let A_5 act on the cosets of H and obtain a homomorphism $\rho\colon A_5 \to S_r$ (where $r = 3$ or 4). Here $\ker\rho \neq \mathbf{1}$ and $\ker\rho \neq A_5$ (as $\ker\rho \leqslant H$), which would contradict the fact that A_5 is simple.

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 6.28 (P. Hall, 1928) *Let G be a finite soluble group and let π be a set of prime numbers. Then*

(i) *G has a Hall π-subgroup;*

(ii) *any two Hall π-subgroups of G are conjugate;*

(iii) *any π-subgroup of G is contained in a Hall π-subgroup.*

A subgroup of G is called a *π-subgroup* if its order is a product involving only the primes in π. There is a clear analogy between this theorem of Hall and Sylow's Theorem (Theorem 3.4).

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.

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. This first appeared in the context of nilpotent groups, and we shall use it in that context in the next section, but it is also needed for the hardest part of the proof of Hall's Theorem.

Lemma 6.29 (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 $N \trianglelefteqslant G$, 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

$$G = \mathrm{N}_G(P)N.$$

□

PROOF OF THEOREM 6.28: Our strategy is to prove part (i) and deduce part (iii) by showing that a π-subgroup is contained in a conjugate of the Hall π-subgroup found already. We shall then deduce part (ii) at the end. The argument is by induction on the group order dividing into several cases. Since the same cases arise in the proof of both (i) and (iii), we shall actually step through doing both parts together. (A proof of (i) can be extracted by just deleting the second half of each case.)

Thus we shall prove the following:

- G has a Hall π-subgroup H;
- if L is a π-subgroup of G then L is contained in some conjugate of H.

We prove these statements by induction on the order of G. Both are trivial if $|G| = 1$. Assume then that $|G| > 1$ and that these statements hold for soluble groups of order smaller than G. Write $|G| = mn$ where m is a product involving primes in π and n is a product involving primes not in π. (A Hall π-subgroup of G is then a subgroup of order m.) We can assume that $m > 1$ since otherwise the statements are trivially true.

Let M be a minimal normal subgroup of G. By Theorem 6.25, M is elementary abelian. We consider two cases according to the prime dividing the order of M.

Case 1: M 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, the above statements hold for G/M. The Correspondence Theorem tells us that a Hall π-subgroup of G/M has the form H/M where H is a subgroup 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.

Now let L be any π-subgroup of G. The image LM/M ($\cong L/(L \cap M)$) of L in the quotient group is a π-subgroup of G/M. Hence, by induction, some conjugate of H/M contains LM/M, say

$$LM/M \leqslant (H/M)^{Mx} = H^x/M$$

where $x \in G$. Thus

$$L \leqslant LM \leqslant H^x.$$

This completes Case 1.

Case 2: No minimal normal subgroup of G is an elementary abelian p-group with $p \in \pi$. In particular, our minimal normal subgroup M of G satisfies $|M| = q^\beta$ where $q \notin \pi$.

Then

$$|G/M| = mn/q^\beta = mn_1$$

where $n = n_1 q^\beta$. We now further subdivide according to n_1.

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.

Now let L be a π-subgroup of G. Now the image LM/M of L in the quotient group is a π-subgroup of G/M. Hence, by induction, LM/M is contained in some conjugate of K/M; say

$$LM/M \leqslant (K/M)^{Mx} = K^x/M$$

where $x \in G$. Hence $L \leqslant LM \leqslant K^x$, so $L^{x^{-1}} \leqslant K$. Then $L^{x^{-1}}$ is a π-subgroup of K and by induction (again) we deduce $L^{x^{-1}} \leqslant H^y$ for some $y \in K$. Hence

$$L \leqslant H^{yx}$$

and we have completed Subcase 2A.

Subcase 2B: $n_1 = 1$, so $|G| = mq^\beta$.

Note also that the general assumption of Case 2 still applies: G has no minimal normal subgroup which is elementary abelian-p for $p \in \pi$.

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 $N \trianglelefteq G$ and

$$|N| = p^\alpha q^\beta.$$

Let P be a Sylow p-subgroup of N. Let us now apply the Frattini Argument (Lemma 6.29):

$$G = \mathrm{N}_G(P)N.$$

But $N = PM$, so

$$G = \mathrm{N}_G(P)PM = \mathrm{N}_G(P)M$$

(as $P \leqslant \mathrm{N}_G(P)$).

Now consider $J = \mathrm{N}_G(P) \cap M$. Since M is abelian, $J \trianglelefteq M$. Also since $M \trianglelefteq G$, $J = \mathrm{N}_G(P) \cap M \trianglelefteq \mathrm{N}_G(P)$. Hence

$$J \trianglelefteq \mathrm{N}_G(P)M = G.$$

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 is then 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

$$mq^\beta = |G| = |\mathrm{N}_G(P)M| = |\mathrm{N}_G(P)| \cdot |M|,$$

so $|\mathrm{N}_G(P)| = m$. Hence $H = \mathrm{N}_G(P)$ is our Hall π-subgroup. (We have now completed the existence part of the whole theorem!)

Now consider some π-subgroup L of G. We have $G = HM$ above, so

$$\begin{aligned} LM &= LM \cap G \\ &= LM \cap HM \\ &= (LM \cap H)M \end{aligned}$$

by Dedekind's Modular Law (Lemma 1.7). Now $LM \cap H$ is a π-group (as a

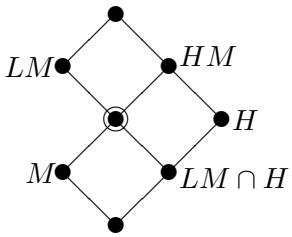


Figure 6.1: Subcase 2B: $LM \cap HM = (LM \cap H)M$

subgroup of H) and

$$\begin{aligned} |LM : LM \cap H| &= \frac{|(LM \cap H)M|}{|LM \cap H|} \\ &= \frac{|M|}{|LM \cap H \cap M|} = |M| \end{aligned}$$

(since $H \cap M = \mathbf{1}$ as they have coprime order). Hence $LM \cap H$ is a Hall π-subgroup of LM.

If $LM < G$, we can apply induction to the group LM to see that some conjugate of the Hall π-subgroup $LM \cap H$ contains the π-subgroup L:

$$L \leqslant (LM \cap H)^x \leqslant H^x$$

for some $x \in G$ (indeed we could pick $x \in LM$). We would then be done.

So suppose $LM = G$. Then as $L \cap M = \mathbf{1}$ (they have coprime order) we see

$$|G| = |LM| = |L| \cdot |M|,$$

so $|L| = mq^\beta/q^\beta = m$. Also, since $M \leqslant N$, we have $G = LN$ (we already know that $G = LM$). Thus

$$|G| = |LN| = \frac{|L| \cdot |N|}{|L \cap N|},$$

so

$$|L \cap N| = \frac{|L| \cdot |N|}{|G|} = \frac{m \cdot p^\alpha q^\beta}{mq^\beta} = p^\alpha.$$

Thus $L \cap N$ is a Sylow p-subgroup of N. By Sylow's Theorem, it is conjugate to the Sylow p-subgroup P which we already know about, say

$$L \cap N = P^x \qquad \text{where } x \in G$$

(indeed we can pick $x \in N$). Now $L \cap N \trianglelefteq L$, so

$$L \leqslant \mathrm{N}_G(L \cap N) = \mathrm{N}_G(P^x) = \mathrm{N}_G(P)^x = H^x.$$

Thus L is contained in some conjugate of our Hall π-subgroup H.

This completes the proof of the both statements. We have now shown that if G is a finite soluble group, then G has a Hall π-subgroup H (i.e., part (i) of Theorem 6.28 holds), and every π-subgroup of G is contained in a conjugate of H (and thus part (iii) of Theorem 6.28 holds).

Now let K be any Hall π-subgroup of G. By the second statement, $K \leqslant H^x$ for some $x \in G$. But these subgroups have the same order, so we deduce $K = H^x$ and so part (ii) of Theorem 6.28 holds.

This completes the proof of Hall's Theorem. □

Sylow systems and Sylow bases

We shall now examine some consequences of Hall's Theorem. Specifically we shall see how the Sylow subgroups of a soluble group can be arranged to have special properties. We begin with the following definition.

Definition 6.30 If p is a prime number, we write p' for the set of all primes not equal to p. A Hall p'-subgroup of a finite group G is called a *p-complement*.

Note that $2'$ then denotes the set of all odd primes.

The reason for the above nomenclature is as follows. Let G be a finite group and write $|G| = p^n m$ where p does not divide m. Then a Hall p'-subgroup H has order m, while a Sylow p-subgroup P has order p^n. As they have coprime orders, we see $H \cap P = \mathbf{1}$ and therefore

$$|HP| = |H| \cdot |P| = |G|,$$

so

$$G = HP, \quad H \cap P = \mathbf{1}.$$

This is the situation we referred to as H and P being complements (see Definition 5.8, although neither subgroup is necessarily normal here).

Now let G be a finite soluble group and write

$$|G| = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$$

where $p_1, p_2, \dots, p_k$ are the distinct prime factors of $|G|$. By Hall's Theorem, G has a Hall p'-subgroup for each prime. Let Q_1, Q_2, …, Q_k be Hall p_i'-subgroups for $i = 1, 2, \dots, k$, respectively. Thus they are characterised by

$$|Q_i| = |G|/p_i^{n_i} \qquad \text{and} \qquad |G : Q_i| = p_i^{n_i}.$$

Claim: $Q_1 \cap Q_2 \cap \cdots \cap Q_t$ is a Hall $\{p_{t+1}, \ldots, p_k\}$-subgroup of G.

We are intersecting subgroups whose indices are coprime. We recall the principal fact from Lemma 1.12 which we need: if $|G : H|$ and $|G : K|$ are coprime integers, then

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

Proof of Claim: This is certainly true when $t = 1$. Suppose then, as an inductive hypothesis, that the intersection $H = Q_1 \cap Q_2 \cap \cdots \cap Q_t$ is a Hall $\{p_{t+1}, \ldots, p_k\}$-subgroup of G. Then

$$|H| = p_{t+1}^{n_{t+1}} \ldots p_k^{n_k} \qquad \text{and} \qquad |G : H| = p_1^{n_1} \ldots p_t^{n_t}.$$

Now apply Lemma 1.12: H and Q_{t+1} have coprime indices, so

$$|G : H \cap Q_{t+1}| = |G : H| \cdot |G : Q_{t+1}| = p_1^{n_1} \ldots p_t^{n_t} p_{t+1}^{n_{t+1}}.$$

Hence $|H \cap Q_{t+1}| = p_{t+2}^{n_{t+2}} \ldots p_k^{n_k}$, so $H \cap Q_{t+1} = Q_1 \cap \cdots \cap Q_{t+1}$ is a Hall $\{p_{t+2}, \ldots, p_k\}$-subgroup of G. Thus the claim holds by induction. □

In particular, $P_k = Q_1 \cap Q_2 \cap \ldots Q_{k-1}$ is a Hall $\{p_k\}$-subgroup of G; that is, a Sylow p_k-subgroup of G.

Generalising in the obvious way, we deduce that

$$P_r = \bigcap_{i \neq r} Q_i$$

is a Sylow p_r-subgroup of G (for $r = 1, 2, \ldots, k$).

Now consider the two Sylow subgroups P_{k-1} and P_k. Firstly $P_{k-1} \cap P_k = \mathbf{1}$ (since they have coprime orders), so

$$|P_{k-1}P_k| = |P_{k-1}| \cdot |P_k| = p_{k-1}^{n_{k-1}} p_k^{n_k} = |P_k P_{k-1}|.$$

Further, by construction, both P_{k-1} and P_k are contained in the intersection $Q_1 \cap Q_2 \cap \cdots \cap Q_{k-2}$ and by our claim this intersection is a Hall $\{p_{k-1}, p_k\}$-subgroup of G; that is,

$$|Q_1 \cap Q_2 \cap \cdots \cap Q_{k-2}| = p_{k-1}^{n_{k-1}} p_k^{n_k}.$$

Now since it is a subgroup, this Hall subgroup is closed under products, so we deduce that

$$P_{k-1}P_k,\ P_k P_{k-1} \subseteq Q_1 \cap Q_2 \cap \cdots \cap Q_{k-2}.$$

Finally the subsets occurring in the previous inclusion all have the same size, so we deduce

$$P_{k-1}P_k = Q_1 \cap Q_2 \cap \cdots \cap Q_{k-2} = P_k P_{k-1}.$$

Generalising in the obvious way, we deduce that for all $r \neq s$:

$$P_r P_s = P_s P_r.$$

Definition 6.31 Let G be a finite group and let p_1, p_2, ..., p_k be the distinct prime factors of $|G|$.

(i) A *Sylow system* for G is a collection Q_1, Q_2, ..., Q_k such that Q_i is a Hall p_i'-subgroup of G (for $i = 1, 2, \ldots, k$).

(ii) A *Sylow basis* for G is a collection P_1, P_2, ..., P_k such that P_i is a Sylow p_i-subgroups of G (for $i = 1, 2, \ldots, k$) and such that

$$P_iP_j = P_jP_i \qquad \text{for all } i \text{ and } j.$$

We have shown:

Theorem 6.32 *A finite soluble group possesses a Sylow system and a Sylow basis.* □

Recall that the product HK of two subgroups is a subgroup if and only if $HK = KH$. Consequently, if we start with a Sylow basis P_1, P_2, ..., P_k for a finite soluble group G, then we can form

$$P_{i_1}P_{i_2}\ldots P_{i_s}$$

for any subset $\{i_1, i_2, \ldots, i_s\} \subseteq \{1, 2, \ldots, k\}$. The fact that the Sylow subgroups in our Sylow basis permute ensures that this is a subgroup and it is easy to see that its order is $p_{i_1}^{n_{i_1}} p_{i_2}^{n_{i_2}} \ldots p_{i_s}^{n_{i_s}}$. Thus we have formed a Hall subgroup for the appropriate collection of primes. Hence a Sylow basis is a nice collection of Sylow subgroups from which we may easily construct Hall subgroups.

Philip Hall proved far more than these results. The final two theorems of this section will not be proved (though the first appears, in guided form, on the problem sheet).

Theorem 6.33 (P. Hall) *Let G be a finite soluble group. Then any two Sylow bases for G are conjugate (that is, if P_1, P_2, ..., P_k and R_1, R_2, ..., R_k are two Sylow bases for G, where P_i and R_i are Sylow subgroups for the same prime, then there exists $x \in G$ such that $R_i = P_i^x$ for all i).*

This is much stronger than Sylow's Theorem. The latter tells us that each R_i is a conjugate of P_i. What the above theorem tells us is that when the Sylow subgroups come from a Sylow basis then we can actually choose the same element x to conjugate all the Sylow subgroups simultaneously.

Finally we have the following major converse to Hall's Theorem.

Theorem 6.34 (P. Hall) *Let G be a finite group which possesses a Hall p'-subgroup for every prime p. Then G is soluble.*

Putting Theorems 6.28 and 6.34 together, we see that a group is soluble if and only if it has Hall π-subgroups for all collections π of primes. (In particular, our observation that A_5 was missing some Hall subgroups is no longer surprising.)

Section 7

Nilpotent Groups

Recall the commutator is given by

$$[x, y] = x^{-1}y^{-1}xy.$$

Definition 7.1 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 the formula $G^{(i+1)} = [G^{(i)}, G^{(i)}]$ for all i. We now make a new definition which is similar but slightly less symmetrical in appearance.

Definition 7.2 The *lower central series* $(\gamma_i(G))$ (for $i \geqslant 1$) is the chain 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 7.3 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 $\gamma_2(G) = G'$.

We need the basic properties of the lower central series, so that we can study nilpotent groups.

Lemma 7.4 (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*

$$G = \gamma_1(G) \geqslant \gamma_2(G) \geqslant \gamma_3(G) \geqslant \cdots .$$

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 $\gamma_i(G)\phi = \gamma_i(K)$. 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 $\gamma_{i+1}(K) = [\gamma_i(K), K] \leqslant \gamma_{i+1}(G)\phi$.

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 a surjective homomorphism, so from (ii) we have

$$\gamma_i(G)\phi = \gamma_i(G).$$

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

$$\gamma_{i+1}(G) = [\gamma_i(G), G] \leqslant \gamma_i(G) \qquad \text{for all } i.$$

□

We deduce two consequences immediately:

Lemma 7.5 *Subgroups and homomorphic images of nilpotent groups are themselves nilpotent.*

PROOF: Let $\gamma_{c+1}(G) = \mathbf{1}$ and $H \leqslant G$. Then by Lemma 7.4(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 7.4(ii) gives $\gamma_{c+1}(K) = \gamma_{c+1}(G)\phi = \mathbf{1}\phi = \mathbf{1}$, so K is nilpotent. □

Note, however, that

$$N \trianglelefteqslant G,\ G/N \text{ and } N \text{ nilpotent} \quad \not\Rightarrow \quad G \text{ nilpotent.}$$

In this way, nilpotent groups are different to soluble groups.

Example 7.6 Finite p-groups are nilpotent.

(In fact, we shall see later that finite p-groups are the archetypal nilpotent group.)

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 Corollary 2.30: $\mathrm{Z}(G) \neq \mathbf{1}$. 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

$$\gamma_{c+1}(G/\mathrm{Z}(G)) = \mathbf{1}.$$

Let $\pi\colon G \to G/\mathrm{Z}(G)$ be the natural homomorphism. Then by Lemma 7.4(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 example illustrates that the centre has a significant role in the study of nilpotent groups. We make two further definitions:

Definition 7.7 The *upper central series* $(\mathrm{Z}_i(G))$ (for $i \geqslant 0$) is the chain of subgroups of the group G defined by

$$\mathrm{Z}_0(G) = \mathbf{1}$$

and

$$\mathrm{Z}_{i+1}(G)/\mathrm{Z}_i(G) = \mathrm{Z}(G/\mathrm{Z}_i(G)) \qquad \text{for } i \geqslant 0.$$

Here suppose we know that $\mathrm{Z}_i(G) \trianglelefteq G$. Then $\mathrm{Z}(G/\mathrm{Z}_i(G))$ is a normal subgroup of $G/\mathrm{Z}_i(G)$, so corresponds to a normal subgroup $\mathrm{Z}_{i+1}(G)$ of G containing $\mathrm{Z}_i(G)$ under the Correspondence Theorem. In this way we define a chain of subgroups

$$\mathbf{1} = \mathrm{Z}_0(G) \leqslant \mathrm{Z}_1(G) \leqslant \mathrm{Z}_2(G) \leqslant \cdots,$$

each of which is normal in G. Here $\mathrm{Z}_1(G) = \mathrm{Z}(G)$.

Definition 7.8 A *central series* for a group G is a chain of subgroups

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

such that G_i is a normal subgroup of G and $G_{i-1}/G_i \leqslant \mathrm{Z}(G/G_i)$ for all i.

Lemma 7.9 *Let*

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

be a central series for G. Then

$$\gamma_{i+1}(G) \leqslant G_i \qquad \textit{and} \qquad \mathrm{Z}_i(G) \geqslant G_{n-i}$$

for all i.

Proof: First observe $\gamma_1(G) = G = G_0$. Suppose that $\gamma_i(G) \leqslant G_{i-1}$ for some i. Now if $x \in \gamma_i(G)$ and $y \in G$, then

$$G_i x \in G_{i-1}/G_i \leqslant \mathrm{Z}(G/G_i),$$

so $G_i x$ commutes with $G_i y$. Therefore

$$G_i[x, y] = (G_i x)^{-1}(G_i y)^{-1}(G_i x)(G_i y) = G_i,$$

so $[x, y] \in G_i$. Hence

$$\gamma_{i+1}(G) = [\gamma_i(G), G] \leqslant G_i.$$

Thus, by induction, the first inclusion holds.

Also $\mathrm{Z}_0(G) = \mathbf{1} = G_n$. Suppose $\mathrm{Z}_i(G) \geqslant G_{n-i}$. Now since (G_i) is a central series for G we have

$$G_{n-i-1}/G_{n-i} \leqslant \mathrm{Z}(G/G_{n-i}).$$

Thus if $x \in G_{n-i-1}$ and $y \in G$, then

$$G_{n-i}x \text{ and } G_{n-i}y \text{ commute;} \quad \text{i.e., } [x, y] \in G_{n-i}.$$

Hence $[x, y] \in \mathrm{Z}_i(G)$, so $\mathrm{Z}_i(G)x$ and $\mathrm{Z}_i(G)y$ commute. Since y is an arbitrary element of G, we deduce that

$$\mathrm{Z}_i(G)x \in \mathrm{Z}(G/\mathrm{Z}_i(G)) = \mathrm{Z}_{i+1}(G)/\mathrm{Z}_i(G)$$

and this holds for all $x \in G_{n-i-1}$. Thus $G_{n-i-1} \leqslant \mathrm{Z}_{i+1}(G)$ and the second inclusion holds by induction. □

We have now established the link between a general central series and the behaviour of the lower and the upper central series.

Theorem 7.10 *The following conditions are equivalent for a group G:*

(i) $\gamma_{c+1}(G) = \mathbf{1}$ *for some c;*

(ii) $\mathrm{Z}_c(G) = G$ *for some c;*

(iii) *G has a central series.*

Thus these are equivalent conditions for a group to be nilpotent.

Proof: If G has a central series (G_i) of length n, then Lemma 7.9 gives

$$\gamma_{n+1}(G) \leqslant G_n = \mathbf{1} \qquad \text{and} \qquad \mathrm{Z}_n(G) \geqslant G_0 = G.$$

Hence (iii) implies both (i) and (ii).

If $\mathrm{Z}_c(G) = G$, then

$$G = \mathrm{Z}_c(G) \geqslant \mathrm{Z}_{c-1}(G) \geqslant \cdots \geqslant \mathrm{Z}_1(G) \geqslant \mathrm{Z}_0(G) = \mathbf{1}$$

is a central series for G (as $\mathrm{Z}_{i+1}(G)/\mathrm{Z}_i(G) = \mathrm{Z}(G/\mathrm{Z}_i(G))$). Thus (ii) implies (iii).

If $\gamma_{c+1}(G) = \mathbf{1}$, then

$$G = \gamma_1(G) \geqslant \gamma_2(G) \geqslant \cdots \geqslant \gamma_{c+1}(G) = \mathbf{1}$$

is a central series for G. (For if $x \in \gamma_{i-1}(G)$ and $y \in G$, then $[x, y] \in \gamma_i(G)$, so $\gamma_i(G)x$ and $\gamma_i(G)y$ commute for all such x and y; thus $\gamma_{i-1}(G)/\gamma_i(G) \leqslant \mathrm{Z}(G/\gamma_i(G))$.) Hence (i) implies (iii). □

Further examination of the link between this proof and Lemma 7.9 shows

$$\gamma_{c+1}(G) = \mathbf{1} \qquad \text{if and only if} \qquad \mathrm{Z}_c(G) = G.$$

Thus for a nilpotent group, the lower central series and the upper central series have the same length.

My next goal is to develop further equivalent conditions for finite groups to be nilpotent. Some of these observations work in greater generality.

Proposition 7.11 *Let G be a nilpotent group. Then every proper subgroup of G is properly contained in its normaliser:*

$$H < \mathrm{N}_G(H) \qquad \text{whenever } H < G.$$

PROOF: Let

$$G = \gamma_1(G) \geqslant \gamma_2(G) \geqslant \cdots \geqslant \gamma_{c+1}(G) = \mathbf{1}$$

be the lower central series. Then $\gamma_{c+1}(G) \leqslant H$ but $\gamma_1(G) \not\leqslant H$. Choose i as small as possible so that $\gamma_i(G) \leqslant H$. Then $\gamma_{i-1}(G) \not\leqslant H$. Now

$$[\gamma_{i-1}(G), H] \leqslant [\gamma_{i-1}(G), G] = \gamma_i(G) \leqslant H,$$

so

$$x^{-1}hxh^{-1} = [x, h^{-1}] \in H \qquad \text{for } x \in \gamma_{i-1}(G) \text{ and } h \in H.$$

Therefore

$$x^{-1}hx \in H \qquad \text{for } x \in \gamma_{i-1}(G) \text{ and } h \in H.$$

We deduce that $H^x = H$ for all $x \in \gamma_{i-1}(G)$, so that $\gamma_{i-1}(G) \leqslant \mathrm{N}_G(H)$. Therefore, since $\gamma_{i-1}(G) \not\leqslant H$, we deduce $\mathrm{N}_G(H) > H$. □

Let us now analyse how nilpotency affects the Sylow subgroups of a finite group. This links into the previous proposition via the following lemma.

Lemma 7.12 *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 $P \leqslant H$, 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 7.13 *Let G be a finite group. The following conditions on G are equivalent:*

(i) *G is nilpotent;*

(ii) *every Sylow subgroup of G is normal;*

(iii) *G is a direct product of p-groups (for various primes p).*

PROOF: (i) $\Rightarrow$ (ii): Let G be nilpotent and P be a Sylow p-subgroup of G (for some prime p). Let $H = \mathrm{N}_G(P)$. By Lemma 7.12, $\mathrm{N}_G(H) = H$. Hence, by Proposition 7.11, we must have $H = G$. That is, $\mathrm{N}_G(P) = G$ and so $P \trianglelefteqslant G$.

(ii) $\Rightarrow$ (iii): Let $p_1, p_2, \ldots, p_k$ be the distinct prime factors of $|G|$, say

$$|G| = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k},$$

and assume that G has a normal Sylow p_i-subgroup P_i for $i = 1, 2, \ldots, k$.

Claim: $P_1 P_2 \ldots P_j \cong P_1 \times P_2 \times \cdots \times P_j$ for all j.

Certainly this claim holds for $j = 1$. Assume it holds for a value j and consider $N = P_1 P_2 \ldots P_j \trianglelefteqslant G$ and $P_{j+1} \trianglelefteqslant G$. We have

$$\begin{aligned} |N| &= |P_1 \times P_2 \times \cdots \times P_j| \\ &= |P_1| \cdot |P_2| \cdot \ldots \cdot |P_j| \\ &= p_1^{n_1} p_2^{n_2} \ldots p_j^{n_j}, \end{aligned}$$

which is coprime to $|P_{j+1}|$. Hence $N \cap P_{j+1} = \mathbf{1}$ and therefore NP_{j+1} satisfies the conditions to be an (internal) direct product. Thus

$$NP_{j+1} \cong N \times P_{j+1} \cong P_1 \times P_2 \times \cdots \times P_j \times P_{j+1},$$

and by induction the claim holds.

In particular, note

$$|P_1 P_2 \ldots P_k| = |P_1 \times P_2 \times \cdots \times P_k| = |P_1| \cdot |P_2| \cdot \ldots \cdot |P_k| = |G|,$$

so

$$G = P_1 P_2 \ldots P_k \cong P_1 \times P_2 \times \cdots \times P_k.$$

(iii) $\Rightarrow$ (i): Suppose $G = P_1 \times P_2 \times \cdots \times P_k$, a direct product of non-trivial p-groups. Then

$$\mathrm{Z}(G) = \mathrm{Z}(P_1) \times \mathrm{Z}(P_2) \times \cdots \times \mathrm{Z}(P_k) \neq \mathbf{1}$$

(by Corollary 2.30). Then

$$G/\mathrm{Z}(G) = P_1/\mathrm{Z}(P_1) \times P_2/\mathrm{Z}(P_2) \times \cdots \times P_k/\mathrm{Z}(P_k)$$

is a direct product of p-groups of smaller order. By induction, $G/\mathrm{Z}(G)$ is nilpotent, say $\gamma_c(G/\mathrm{Z}(G)) = \mathbf{1}$. Now apply Lemma 7.4(ii) to the natural map $\pi\colon G \to G/\mathrm{Z}(G)$ to see that $\gamma_c(G)\pi = \gamma_c(G/\mathrm{Z}(G)) = \mathbf{1}$. Thus $\gamma_c(G) \leqslant \ker\pi = \mathrm{Z}(G)$ and hence

$$\gamma_{c+1}(G) = [\gamma_c(G), G] \leqslant [\mathrm{Z}(G), G] = \mathbf{1}.$$

Therefore G is nilpotent. □

This now tells us that the study of finite nilpotent groups reduces to understanding p-groups. There is plenty more that could be said here, but not much time in the course. Instead, I shall finish by introducing the concept of the Frattini subgroup which is of significance both in the study of general groups and in the study of finite nilpotent (and p-) groups.

Definition 7.14 A *maximal subgroup* (or *maximal proper subgroup*) of a group G is a subgroup $M < G$ such that there is no subgroup H with $M < H < G$.

Thus a maximal proper subgroup is a proper subgroup which is largest amongst the proper subgroups.

If G is a nilpotent group, then Proposition 7.11 tells us that

$$M < \mathrm{N}_G(M) \leqslant G,$$

for any maximal subgroup M of G. The maximality of M forces $\mathrm{N}_G(M) = G$; that is, $M \trianglelefteqslant G$. Thus:

Lemma 7.15 *Let G be a nilpotent group. Then every maximal subgroup of G is normal in G.* □

Definition 7.16 The *Frattini subgroup* $\Phi(G)$ of a group G is the intersection of all its maximal subgroups:

$$\Phi(G) = \bigcap_{\substack{M \text{ maximal} \\ \text{in } G}} M.$$

(If G is an (infinite) group and G has no maximal subgroup, then $\Phi(G) = G$.)

If we apply an automorphism to a maximal subgroup, we map it to another maximal subgroup. Hence the automorphism group permutes the maximal subgroups of G and we deduce:

Lemma 7.17 *If G is a group, then the Frattini subgroup $\Phi(G)$ is a characteristic subgroup of G.* □

Our most comprehensive theorem characterising nilpotent finite groups is then as follows:

Theorem 7.18 *Let G be a finite group. The following conditions are equivalent:*

(i) *G is nilpotent;*

(ii) *$H < \mathrm{N}_G(H)$ for all $H < G$;*

(iii) *every maximal proper subgroup of G is normal;*

(iv) *$\Phi(G) \geqslant G'$;*

(v) *every Sylow subgroup of G is normal;*

(vi) *G is a direct product of p-groups.*

PROOF: We have already proved that (i) $\Rightarrow$ (ii) (Proposition 7.11), (ii) $\Rightarrow$ (iii) (see the proof of Lemma 7.15) and (v) $\Rightarrow$ (vi) $\Rightarrow$ (i).

(iii) $\Rightarrow$ (iv): Let M be a maximal subgroup of G. By assumption, $M \trianglelefteqslant G$. Since M is maximal, the Correspondence Theorem tells us that G/M has no non-trivial proper subgroups. It follows first that G/M is cyclic and so is abelian. Lemma 6.12 gives

$$G' \leqslant M.$$

Hence

$$G' \leqslant \bigcap_{M \text{ max } G} M = \Phi(G).$$

(iv) $\Rightarrow$ (v): Let P be a Sylow p-subgroup of G and let $N = P\,\Phi(G)$ (which is a subgroup of G, since $\Phi(G) \trianglelefteqslant G$ by Lemma 7.17). Let $x \in N$ and $g \in G$. Then

$$x^{-1}x^g = [x, g] \in G' \leqslant \Phi(G) \leqslant N.$$

Hence $x^g \in N$ for all $x \in N$ and $g \in G$, so $N \trianglelefteqslant G$. Now P is a Sylow p-subgroup of N (since it is the largest possible p-subgroup of G, so is certainly largest amongst p-subgroups of N). Apply the Frattini Argument (Lemma 6.29):

$$\begin{aligned} G &= \mathrm{N}_G(P)\,N \\ &= \mathrm{N}_G(P)\,P\,\Phi(G) \\ &= \mathrm{N}_G(P)\,\Phi(G) \qquad (\text{as } P \leqslant \mathrm{N}_G(P)). \end{aligned}$$

From this we deduce that $G = \mathrm{N}_G(P)$: for suppose $\mathrm{N}_G(P) \neq G$. Then $\mathrm{N}_G(P) \leqslant M < G$ for some maximal subgroup M of G. By definition, $\Phi(G) \leqslant M$, so

$$\mathrm{N}_G(P)\,\Phi(G) \leqslant M < G,$$

a contradiction. Hence $\mathrm{N}_G(P) = G$ and so $P \trianglelefteqslant G$.

This completes all remaining stages in the proof. □

We shall complete the section by studying the Frattini subgroup of a finite group.

Theorem 7.19 *Let G be a finite group. Then the Frattini subgroup $\Phi(G)$ is nilpotent.*

Proof: Let P be a Sylow p-subgroup of $\Phi(G)$. The Frattini Argument (Lemma 6.29) gives

$$G = \mathrm{N}_G(P)\,\Phi(G).$$

If $\mathrm{N}_G(P) \neq G$, then there is a maximal proper subgroup M of G with $\mathrm{N}_G(P) \leqslant M < G$. By definition, $\Phi(G) \leqslant M$. Hence

$$\mathrm{N}_G(P)\,\Phi(G) \leqslant M < G,$$

contrary to above. Therefore $\mathrm{N}_G(P) = G$. Hence $P \trianglelefteqslant G$, and so in particular $P \trianglelefteqslant \Phi(G)$. Therefore $\Phi(G)$ is nilpotent by Theorem 7.13. □

We have used one property of the Frattini subgroup twice now, so it is worth drawing attention to it.

Definition 7.20 A subset S of a group G is a *set of non-generators* if it can always be removed from a set of generators for G without affecting the property of generating G.

Thus S is a set of non-generators if

$$G = \langle X, S\rangle \qquad \text{implies} \qquad G = \langle X\rangle$$

for all subsets $X \subseteq G$.

Lemma 7.21 *The Frattini subgroup $\Phi(G)$ is a set of non-generators for a finite group G.*

Proof: Let $G = \langle X, \Phi(G)\rangle$. If $\langle X\rangle \neq G$, then there exists a maximal subgroup M of G such that $\langle X\rangle \leqslant M < G$. By definition of the Frattini subgroup, $\Phi(G) \leqslant M$. Hence $X \cup \Phi(G) \subseteq M$, so $\langle X, \Phi(G)\rangle \leqslant M < G$ which contradicts the assumption. Therefore $G = \langle X\rangle$ and so we deduce $\Phi(G)$ is a set of non-generators for G. □

Finally we prove:

Theorem 7.22 *Let G be a finite group. Then G is nilpotent if and only if $G/\Phi(G)$ is nilpotent.*

PROOF: By Lemma 7.5, a homomorphic image of a nilpotent group is nilpotent. Consequently if G is nilpotent, then necessarily $G/\Phi(G)$ is nilpotent.

Conversely suppose $G/\Phi(G)$ is nilpotent. Let P be a Sylow p-subgroup of G. Then $P\Phi(G)/\Phi(G)$ is a Sylow p-subgroup of $G/\Phi(G)$. Hence

$$P\Phi(G)/\Phi(G) \trianglelefteqslant G/\Phi(G),$$

as $G/\Phi(G)$ is nilpotent. Therefore

$$P\,\Phi(G) \trianglelefteqslant G$$

by the Correspondence Theorem. Now P is a Sylow p-subgroup of $P\,\Phi(G)$ (as even G has no larger p-subgroups), so we apply the Frattini Argument (Lemma 6.29) to give

$$G = \mathrm{N}_G(P) \cdot P\,\Phi(G).$$

Therefore

$$G = \mathrm{N}_G(P)\,\Phi(G)$$

(as $P \leqslant \mathrm{N}_G(P)$). Now as $\Phi(G)$ is a set of non-generators for G (see Lemma 7.21), we deduce

$$G = \mathrm{N}_G(P).$$

Thus $P \trianglelefteqslant G$. Hence G is nilpotent by Theorem 7.13. □