GROUP THEORY, MATH 60036: Lecture Notes

Lecturer: Martin Liebeck

The course: we will focus almost exclusively on finite groups. There is a massive theory of infinite groups, but that has a very different flavour, and needs a course of its own. A summary of the chapters of the course:

1. Revision and basics
2. Composition series and the Jordan-Hölder theorem
3. Some families of simple groups
4. The Sylow theorems
5. Extensions and semidirect products
6. Solvable groups
7. Nilpotent groups
8. The Frattini subgroup
9. The transfer homomorphism

Books There are many good books and online notes covering the material in the course. Here are three books:

I.M. Isaacs, *Algebra*

J. Rotman, *Introduction to the theory of groups*

J. Rose, *A course in group theory*

And some online notes of P. Cameron:

https://webspace.maths.qmul.ac.uk/p.j.cameron/notes/gt.pdf

1 Revision and basics

Knowledge of the group theory covered in the Year 2 Groups and Rings course is assumed. In this section this will be summarised, and further basic material added.

A. Some examples of groups

Here are various groups that you should have seen before. One point of notation before starting: we shall usually write 1 (or 1_G) for the identity element of a group G. We shall also write just 1 for the identity subgroup $\{1\}$. The notation $H \leq G$ means that H is a subgroup of G (as opposed to $H \subseteq G$, which just means that H is a subset of G). Also $H < G$ means that H is a *proper* subgroup (i.e. $H \neq G$).

Cyclic groups For each $n \in \mathbb{N}$ there is a cyclic group

$$\begin{aligned} C_n &= \{z \in \mathbb{C} : z^n = 1\} \text{ (under complex multiplication)} \\ &= \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}, \text{ where } \omega = e^{2\pi i/n} \\ &= \langle \omega \rangle. \end{aligned}$$

There is also an infinite cyclic group $(\mathbb{Z}, +) = \langle 1 \rangle$.

Every cyclic group is isomorphic to C_n or $\mathbb{Z}$. For example, the additive group of integers modulo n, which we will denote by $\mathbb{Z}/n$, is isomorphic to C_n. (This is often also denoted by $\mathbb{Z}/n\mathbb{Z}$ or just $\mathbb{Z}_n$.)

Of course $\mathbb{Z}/n$ has multiplication as well as addition (it is a ring). For p prime, $\mathbb{Z}/p$ is a field, and we'll often write this field as $\mathbb{F}_p$.

Dihedral groups The dihedral group D_{2n} is defined to be the symmetry group of a regular n-sided polygon. It has $2n$ elements: n rotations $1, \rho, \rho^2, \ldots, \rho^{n-1}$, and n reflections (where ρ is the clockwise rotation by $2\pi/n$). If σ is one of the reflections, then all of the reflections can be written as $\sigma, \sigma\rho, \ldots, \sigma\rho^{n-1}$. This is just saying that if $H = \langle \rho \rangle$ is the rotation subgroup, then D_{2n} is the union of the two cosets H and σH. Thus

$$D_{2n} = \langle \rho, \sigma \rangle, \text{ with relations } \rho^n = \sigma^2 = 1, \ \sigma\rho = \rho^{-1}\sigma.$$

Using these relations we can work out any product of two elements of D_{2n}.

Quaternion group Q_8 This is an important group of order 8. It can be defined as the group generated by the two matrices

$$A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \ B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Up to isomorphism, the only non-abelian groups of order 8 are D_8 and Q_8. (Qn on Sheet 1.)

Symmetric and Alternating groups Let X be a set. The symmetric group on X, written $Sym(X)$, is defined to be the group of all permutations of X, the group multiplication being composition of functions. For $X = \{1, 2, \ldots, n\}$ we write S_n for $Sym(X)$. So S_n is the group of all permutations of $\{1, \ldots, n\}$. The alternating group A_n is the subgroup of S_n consisting of all even permutations. We have

$$|S_n| = n!, \ \ |A_n| = \frac{1}{2}|S_n|.$$

General linear and Special linear groups For F a field, the general linear group $GL_n(F)$ is defined to be the group of all invertible $n \times n$ matrices over F, under matrix multiplication. If F is a finite field, then $GL_n(F)$ is a finite group. The special linear group

$$SL_n(F) = \{g \in GL_n(F) : \det(g) = 1\}$$

is a normal subgroup of $GL_n(F)$ (as it is the kernel of the determinant homomorphism $g \mapsto \det(g)$).

B. Homomorphisms, normal subgroups, quotient groups

Let G be a group. A subgroup N of G is a *normal* subgroup, written $N \lhd G$, if $gNg^{-1} = N$ for all $g \in G$. (Equivalently, $gN = Ng$ for all g.) If $N \lhd G$, we can define the *quotient group* G/N: its elements are the cosets gN for $g \in G$, with multiplication defined by

$$(gN)(hN) = ghN \quad \text{for all } g, h \in G.$$

A map $\phi : G \mapsto H$ is a *homomorphism* if $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$. The *kernel* $\mathrm{Ker}(\phi) = \{g \in G : \phi(g) = 1\}$ is a normal subgroup of G, and the image $\mathrm{Im}(\phi)$ is a subgroup of H. Here are two basic results about all this:

Proposition 1.1 (First Isomorphism Theorem) *Let $\phi : G \mapsto H$ be a homomorphism with kernel K. Then the quotient group $G/K \cong \mathrm{Im}(\phi)$.*

Proposition 1.2 (Subgroup Theorem) *Let $N \lhd G$. Then every subgroup of G/N is of the form H/N, where $N \leq H \leq G$.*

A group G is *simple* if its only normal subgroups are 1 and G itself.

Examples (1) For p prime, C_p is obviously simple.

(2) Less obviously, for $n \geq 5$ the alternating group A_n is simple (will be proved in Section 3). Note that A_4 is *not* simple: it has a normal subgroup $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$.

An important normal subgroup of any group G is its *centre* $Z(G)$, defined by

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

C. Automorphisms

An *automorphism* of a group G is an isomorphism $\phi : G \mapsto G$. The set of all automorphisms of G is denoted by $\mathrm{Aut}(G)$, and is a group under composition.

For $g \in G$, the conjugation map ι_g sending $x \mapsto gxg^{-1}$ ($x \in G$) is an automorphism of G, called an *inner* automorphism. Define

$$\mathrm{Inn}(G) = \{\iota_g : g \in G\}.$$

The map $g \mapsto \iota_g$ from $G \mapsto \mathrm{Aut}(G)$ is a homomorphism. Its image is $\mathrm{Inn}(G)$ and its kernel is $Z(G)$. Hence by Prop. 1.1,

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

Note that $G/Z(G)$ cannot be an arbitrary group – for example, it cannot be a nontrivial cyclic group (problem on Sheet 1).

Definition A subgroup N of G is *characteristic* if $\alpha(N) = N$ for all $\alpha \in \mathrm{Aut}(G)$. Write this as $N \,\mathrm{char}\, G$.

Note that $N \,\mathrm{char}\, G \Rightarrow N \lhd G$, since taking $\alpha = \iota_g$, we have $N = \iota_g(N) = gNg^{-1}$ for all $g \in G$.

Some general examples of characteristic subgroups: $Z(G) \,\mathrm{char}\, G$ and $\mathrm{Inn}(G) \,\mathrm{char}\, \mathrm{Aut}(G)$ for any group G. A non-example: if $G = C_2 \times C_2$, then G has no characteristic subgroups apart from 1 and G itself.

We know that if M, N are subgroups of G such that $M \lhd N$ and $N \lhd G$, then M is not necessarily normal in G. But if M is characteristic in N, then it *is* normal in G:

Proposition 1.3 *Let M, N be subgroups of G, and suppose $M \,\mathrm{char}\, N$ and $N \lhd G$. Then $M \lhd G$.*

Proof Let $g \in G$. As $N \lhd G$, we have $\iota_g(N) = N$. Hence the restriction of ι_g to N is an autormorphism of N, and so $\iota_g(M) = M$ since $M \,\mathrm{char}\, N$. This means that $gMg^{-1} = M$, as required. $\square$

For example, if $N \triangleleft G$ then $Z(N) \triangleleft G$ (since $Z(N)$ char N).

D. Generators

Let G be a group and S a subset of G. The subgroup of G *generated by* S is defined to be the intersection of all subgroups containing S, and is written as $\langle S \rangle$. If S is a finite subset then $\langle S \rangle$ consists of all products of the form $x_1^{a_1} \cdots x_k^{a_k}$, where $x_1, \ldots, x_k \in S$ (not necessarily distinct) and each $a_i \in \mathbb{Z}$. If $G = \langle S \rangle$ for some finite subset S, we say that G is *finitely generated*.

For example, $D_{2n} = \langle \rho, \sigma \rangle$, $C_n = \langle \omega \rangle$ and $S_n = \langle (i\, j) : 1 \leq i < j \leq n \rangle$.

Commutators For $x, y \in G$ define $[x, y] = xyx^{-1}y^{-1}$. This is called the *commutator* of x and y. Notice that $[x, y] = 1$ iff $xy = yx$. The *commutator subgroup* of G is the subgroup generated by all commutators, and is denoted by G' (some authors also write $[G, G]$). In other words,

$$G' = \langle\, [x, y] : x, y \in G \,\rangle.$$

Proposition 1.4 (i) *The commutator subgroup G' is a characteristic subgroup of G (so in particular $G' \triangleleft G$), and G/G' is abelian.*

(ii) *Let $N \triangleleft G$. Then G/N is abelian iff $G' \leq N$.*

Note: each element of G' is a product of commutators, but might not itself be a commutator.

E. Direct products

If $G_1, \ldots, G_k$ are groups, their *direct product* $G_1 \times \cdots \times G_k$ is defined to be the group with

- elements $(g_1, \ldots, g_k)$ where each $g_i \in G_i$,
- multiplication $(g_1, \ldots, g_k)\,(h_1, \ldots, h_k) = (g_1 h_1, \ldots, g_k h_k)$.

Let $G = G_1 \times G_2$. Then G has subgroups $A_1 = G_1 \times 1 \cong G_1$ and $A_2 = 1 \times G_2 \cong G_2$ such that

- $A_1, A_2 \triangleleft G$,
- $A_1 \cap A_2 = 1$,
- $G = A_1 A_2$,

where we define $A_1 A_2 = \{a_1 a_2 : a_i \in A_i\}$. Conversely:

Proposition 1.5 *Suppose that G is a group, and A, B are subgroups with the following properties:*

- $A, B \triangleleft G$,
- $A \cap B = 1$,
- $G = AB$ *(i.e. $G = \{ab : a \in A, b \in B\}$).*

Then $G \cong A \times B$.

For example, let $G = D_{12} = \langle \rho, \sigma \rangle$. This has subgroups $A = \langle \rho^2, \sigma \rangle \cong D_6$ and $B = \langle \rho^3 \rangle \cong C_2$. Check that the conditions of Prop. 1.5 hold. Hence

$$D_{12} \cong D_6 \times C_2.$$

Abelian groups The main result classifies all finitely generated abelian groups. For a group G and an integer $m \geq 0$, write $G^m = G \times \cdots \times G$ (where there are m copies of G here, and if $m = 0$ we just set $G^m = 1$).

Theorem 1.6 *If G is a finitely generated abelian group, then there exists an integer $m \geq 0$ and prime powers $p_i^{a_i}$ for $i = 1, \ldots, k$, such that*

$$G \cong \mathbb{Z}^m \times C_{p_1^{a_1}} \times \cdots \times C_{p_k^{a_k}},$$

a direct product of cyclic groups. The integer m and the prime powers $p_i^{a_i}$ are uniquely determined by G.

F. Group actions

An *action* of a group G on a set Ω is a homomorphism $\rho : G \mapsto Sym(\Omega)$. For $g \in G, \omega \in \Omega$, we usually just write $g(\omega)$ instead of $(\rho(g))(\omega)$. We can define an equivalence relation $\sim$ on Ω by

$$\alpha \sim \beta \;\Leftrightarrow\; \beta = g(\alpha) \text{ for some } g \in G.$$

The equivalence classes are called the *orbits* of G on Ω. We denote the orbit containing α by α^G, so that

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

If there is only one orbit, we say that G is *transitive* on Ω.

For $\alpha \in \Omega$, the *stabilizer* of α is defined to be

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

This is a subgroup of G. Also, for $x \in G$ the stabilizer of $x(\alpha)$ is equal to $xG_\alpha x^{-1}$; in other words, $G_{x(\alpha)} = xG_\alpha x^{-1}$.

Proposition 1.7 (Orbit stabilizer theorem) *The size of the orbit α^G is equal to $|G : G_\alpha|$ (which is equal to $|G|/|G_\alpha|$).*

In particular, if G is transitive on Ω, then $|\Omega| = |G : G_\alpha|$ for any $\alpha \in \Omega$.

In the Year 2 course there were two very nice applications of the orbit stabilizer theorem:

Proposition 1.8 (Cauchy's theorem) *If G is a finite group and a prime p divides $|G|$, then G contains an element of order p.*

Recall that for a prime p, a finite group is a *p-group* if $|G| = p^a$ for some a.

Proposition 1.9 *If G is a nontrivial p-group, then $Z(G) \neq 1$.*

G. Conjugacy classes

Recall that for $g \in G$, we defined the inner automorphism ι_g of G to send $x \mapsto gxg^{-1}$ for all $x \in G$. Thus $\iota_g \in Sym(G)$, and the map $\rho : G \mapsto Sym(G)$ sending $g \mapsto \iota_g$ is an action of G on itself. The orbit containing x is

$$x^G = \{gxg^{-1} : g \in G\}.$$

This is called the *conjugacy class* of G containing x. The stabilizer of x is $\{g \in G : gxg^{-1} = x\}$, which is the same as $\{g \in G : gx = xg\}$, the set of elements of G that commute with x. We denote this subgroup by $C_G(x)$ (rather than G_x), and call it the *centralizer* of x. By the orbit stabilizer theorem, we have:

Proposition 1.10 *The size of the conjugacy class x^G is*

$$|x^G| = |G : C_G(x)|.$$

In particular, $|x^G| = 1 \Leftrightarrow C_G(x) = G \Leftrightarrow x \in Z(G)$.

From the last result we can deduce what is sometimes called the *class equation* for a finite group G: if $C_1, \ldots, C_k$ are the conjugacy classes of G of size greater than 1, then

$$|G| = |Z(G)| + \sum_{i=1}^{k} |C_i|. \tag{1.1}$$

Notice also that if $N \triangleleft G$, then N is a union of conjugacy classes of G including the class $\{1\}$, since

$$n \in N \Rightarrow gng^{-1} \in N \ \forall g \in G \Rightarrow n^G \subseteq N.$$

So in principle, if we know the conjugacy classes of a finite group G, we can compute all the normal subgroups by considering unions of conjugacy classes and checking whether they form a subgroup. In practice this is not a good method, but it works well for some small groups (and we shall use it later to prove that A_5 is simple – see Prop. 1.14).

H. Conjugacy classes of S_n, A_n, $GL_n(F)$

Recall that if $x \in S_n$, then x can be written as a product of disjoint cycles of lengths $k_1, \ldots, k_r$, where $\sum k_i = n$. Taking $k_1 \geq k_2 \geq \cdots \geq k_r$, we say that the *cycle-shape* of x is $(k_1, \ldots, k_r)$. For example, $x = (125)(37)(48) \in S_8$ has cycle-shape $(3, 2, 2, 1) = (3, 2^2, 1)$.

Proposition 1.11 *For $x \in S_n$, the conjugacy class x^{S_n} consists of all permutations with the same cycle-shape as x.*

Proof First consider a cycle $c = (a_1\, a_2 \cdots a_k) \in S_n$. For any $g \in S_n$, we have

$$gcg^{-1} = (g(a_1)\, g(a_2) \cdots g(a_k))$$

(to see this simply check that the LHS and RHS both have the same effect on every element of $\{1, \ldots, n\}$). Hence for $x = c_1 c_2 \cdots c_r$, a product of disjoint cycles of lengths $k_1, \ldots, k_r$, we have

$$gxg^{-1} = (gc_1g^{-1})\,(gc_2g^{-1}) \cdots (gc_rg^{-1}),$$

which is a product of disjoint cycles of the same lengths $k_1, \ldots, k_r$. Hence x^{S_n} is contained in the set of permutations of cycle-shape $(k_1, \ldots, k_r)$.

Conversely, if $y = c'_1 \cdots c'_r$ is of cycle-shape $(k_1, \ldots, k_r)$, then there exists $g \in S_n$ such that $gc_ig^{-1} = c'_i$ for all i, so $gxg^{-1} = y$ and $y \in x^{S_n}$. $\square$

By Prop. 1.10, the size of the class x^{S_n} is equal to $|S_n : C_{S_n}(x)|$. This can be worked out using the next result.

Proposition 1.12 *Let $x \in S_n$ have cycle-shape $(r_1^{a_1}, \ldots, r_k^{a_k})$, where $r_1, \ldots, r_k$ are distinct. Then $|C_{S_n}(x)| = \prod_1^k r_i^{a_i} a_i!$*

Proof This is a question on Sheet 1.

Example The conjugacy classes of S_5:

cycle-shape	(1^5)	$(2, 1^3)$	$(3, 1^2)$	$(4, 1)$	(5)	$(2^2, 1)$	$(3, 2)$
$\lvert x^{S_5}\rvert$	1	10	20	30	24	15	20

Classes in A_n Let $x \in A_n$. Obviously $x^{A_n} \subseteq x^{S_n}$. When are they equal?

Proposition 1.13 *Let $x \in A_n$.*

(i) *If $C_{S_n}(x) \leq A_n$, then $|x^{A_n}| = \frac{1}{2}|x^{S_n}|$ and x^{S_n} splits into two A_n-conjugacy classes.*

(ii) *If $C_{S_n}(x) \not\leq A_n$, then $x^{A_n} = x^{S_n}$.*

Proof (i) Suppose $C_{S_n}(x) \leq A_n$, so $C_{S_n}(x) = C_{A_n}(x)$. Then

$$|x^{A_n}| = |A_n : C_{A_n}(x)| = \frac{1}{2}|S_n : C_{S_n}(x)| = \frac{1}{2}|x^{S_n}|.$$

(ii) Suppose $C_{S_n}(x) \not\leq A_n$. Then $C_{A_n}(x)$ consists of the even permutations in $C_{S_n}(x)$, so $|C_{A_n}(x)| = \frac{1}{2}|C_{S_n}(x)|$. Hence

$$|x^{A_n}| = |A_n : C_{A_n}(x)| = |S_n : C_{S_n}(x)| = |x^{S_n}|. \quad \square$$

Example The conjugacy classes of A_5:

cycle-shape	(1^5)	$(3, 1^2)$	(5)	$(2^2, 1)$
splits?	no	no	yes	no
$\lvert x^{A_5}\rvert$	1	20	12, 12	15

Using this list of conjugacy classes sizes, we see that the only possible unions of classes of A_5 including $\{1\}$ that have order dividing 60 are 1 and A_5 itself. So this proves:

Proposition 1.14 *The group A_5 is simple.*

Classes in $GL_n(F)$ We know from Year 2 Linear Algebra that every $n \times n$ matrix over F is similar to a unique Rational Canonical Form (RCF). So the conjugacy classes of $GL_n(F)$ correspond bijectively to the RCFs of invertible $n \times n$ matrices over F.

Example Consider $G = GL_2(\mathbb{F}_3)$. The possible characteristic polys of its elements are the monic quadratics which do not have 0 as a root: these are

$$(x-1)^2,\ (x+1)^2,\ x^2-1,\ x^2+1,\ x^2+x-1,\ x^2-x-1.$$

For the first two polys in this list, there are 2 RCFS; and for the others there is 1 RCF. So $GL_2(\mathbb{F}_3)$ has 8 conjugacy classes.

I. Coset actions

Let G be a group with a subgroup H, and define $\Omega = \{xH : x \in G\}$, the set of left cosets of H in G. For $g \in G$, we can define a permutation $\pi_g \in Sym(\Omega)$ by

$$\pi_g : xH \mapsto gxH \quad \forall xH \in \Omega.$$

Proposition 1.15 (i) *The map $\pi : G \mapsto Sym(\Omega)$ sending $g \mapsto \pi_g$ is a transitive action of G on Ω.*

(ii) *Let $N = \mathrm{Ker}(\pi)$. Then*

$$N = \bigcap_{x \in G} xHx^{-1} \lhd G,$$

and G/N is isomorphic to a subgroup of $Sym(\Omega)$.

(iii) *Let $|\Omega| = n$. Then $|G/N|$ divides $n!$*

Proof (i) First, π is a homomorphism as $\pi_{g_1}\pi_{g_2}(xH) = \pi_{g_1}(g_2xH) = \pi_{g_1g_2}(xH)$. The action is transitive, since the orbit of the coset $H \in \Omega$ is $\{\pi_g(H) : g \in G\} = \{gH : g \in G\} = \Omega$.

(ii) We have

$$\begin{aligned}\mathrm{Ker}(\pi) &= \{g \in G : \pi_g = e \in Sym(\Omega)\}\\ &= \{g \in G : gxH = xH\ \forall x \in G\}\\ &= \{g \in G : x^{-1}gx \in H\ \forall x \in G\}\\ &= \textstyle\bigcap_{x \in G} xHx^{-1}.\end{aligned}$$

Also $G/N \cong \mathrm{Im}(\pi)$, a subgroup of $Sym(\Omega)$.

(iii) This follows by (ii) and Lagrange's theorem. □

Corollary 1.16 *Suppose G has a subgroup H of index n. Then G has a normal subgroup $N \leq H$ such that $|G/N|$ divides $n!$*

Example We show that every proper subgroup of A_5 has index at least 5. To prove this, let $G = A_5$ and suppose G has a proper subgroup H such that $|G : H| \leq 4$. Then by the corollary, G has a normal subgroup $N \leq H$ such that $|G/N|$ divides 4! As G is simple, N must be 1. But $|G| = 60$ does not divide 4!, contradiction.

Note that A_5 *does* have a subgroup of index 5, namely A_4.

As a special case of a coset action, consider the case where the subgroup $H = 1$. Then we can identify the set Ω of left cosets with G, and the permutation π_g sends $x \mapsto gx$ for all $x \in G$. This is called the *right regular action* of G on itself. The kernel is 1, so we see that G is isomorphic to a subgroup of $Sym(G)$. This is known as Cayley's theorem:

Proposition 1.17 (Cayley's theorem) *If $|G| = n$, then G is isomorphic to a subgroup of S_n.*

J. Conjugates of subgroups

Let G be a group with a subgroup H. For $g \in G$, we can check that gHg^{-1} is also a subgroup, and is isomorphic to H via the isomorphism $h \mapsto ghg^{-1}$. We write ${}^gH = gHg^{-1}$, and call this subgroup a *conjugate* of H. Let $\Omega = \{{}^gH : g \in G\}$, the set of all conjugates of H in G. Then G acts transitively by conjugation on Ω (i.e. the action of $x \in G$ sends ${}^gH \mapsto^{xg} H$). The stabilizer of H in this action is

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

a subgroup of G called the *normalizer* of H. Hence by the orbit stabilizer theorem:

Proposition 1.18 *The number of distinct conjugates of H in G is equal to $|G : N_G(H)|$.*

Notice that $H \triangleleft G$ iff $N_G(H) = G$.

Let us record one further piece of notation here. For a subset $X \subseteq G$, the *centralizer* in G of X is

$$C_G(X) = \{g \in G : gx = xg \ \ \forall x \in X\}.$$

This is a subgroup, as it is $\bigcap_{x \in X} C_G(x)$.

To conclude this chapter , here is a basic result about products of subgroups. If H and K are subsets of a group G, we define $HK = \{hk : h \in H, k \in K\}$.

Proposition 1.19 *Let H, K be subgroups of a finite group G.*

(i) *Then $|HK| = \frac{|H|\,|K|}{|H \cap K|}$.*

(ii) *If $H \leq N_G(K)$, then HK is a subgroup of G.*

Proof (i) Define a map $\phi : H \times K \mapsto HK$ by $\phi(h, k) = hk$ for $h \in H, k \in K$. For $x = h_1k_1$, check that the inverse image

$$\phi^{-1}(x) = \{(h_1y, y^{-1}k_1) : y \in H \cap K\}.$$

Hence $|\phi^{-1}(x)| = |H \cap K|$ for all $x \in HK$. It follows that $|H \times K| = |HK|\,|H \cap K|$.

(ii) Suppose $H \leq N_G(K)$. We check the subgroup properties for HK. Obviously $1 \in HK$. For closure, let $h_1k_1, h_2k_2 \in HK$: then

$$(h_1k_1)(h_2k_2) = h_1h_2\,(h_2^{-1}k_1h_2)\,k_2 \in HK.$$

For inverses, note that $(hk)^{-1} = k^{-1}h^{-1} = h^{-1}\,(hk^{-1}h^{-1}) \in HK$. $\square$

2 Composition series and the Jordan Hölder theorem

The main result of this chapter, the Jordan Hölder theorem, shows that every finite group is "built" out of a unique collection of simple groups. We begin with a definition.

Definition Let G be a group and let $N \lhd G$. We say that N is a *maximal normal* subgroup if $N \neq G$ and also

$$N \leq M \lhd G \Rightarrow M = N \text{ or } G.$$

In other words, N is a proper normal subgroup of G that is contained in no larger proper normal subgroup.

Lemma 2.1 *If N is a maximal normal subgroup of G, then G/N is a simple group.*

Proof Suppose $K \lhd G/N$. By Prop. 1.2, we have $K = M/N$, where $N \leq M \lhd G$. Hence $M = N$ or G, and so $K = 1$ or G/N. Hence G/N is simple. □

Now let G be finite. Choose a maximal normal subgroup $G_1 \lhd G$, then a maximal normal $G_2 \lhd G_1$ (note G_2 is normal in G_1, but not necessarily normal in G), and continue. So we get a series

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_r = 1. \tag{2.1}$$

By Prop. 2.1, each quotient group G_i/G_{i-1} is simple.

Definition We call such a series (2.1) a *composition series* for G. The simple groups G_i/G_{i-1} for $i = 0, 1, \ldots, r$ are called the *composition factors* of the series.

Example Let $G = C_{12}$. There are three composition series:

$$\begin{array}{ll} C_{12} \rhd C_4 \rhd C_2 \rhd 1, & \text{comp. factors } C_3, C_2, C_2 \\ C_{12} \rhd C_6 \rhd C_2 \rhd 1, & \text{comp. factors } C_2, C_3, C_2 \\ C_{12} \rhd C_6 \rhd C_3 \rhd 1, & \text{comp. factors } C_2, C_2, C_3 \end{array}$$

We see that each composition series has the same collection of composition factors, occuring in different orders.

Theorem 2.2 (Jordan-Hölder theorem) *Any two composition series for a finite group G give the same collection of composition factors (possibly in a different order).*

For the proof we need the following result. Recall that for subsets A, B of a group G, we define $AB = \{ab : a \in A, b \in B\}$. Usually this is not a subgroup (even if A and B are) – but in Prop. 1.19(ii) we gave a condition under which it is a subgroup.

Proposition 2.3 *Let G be a group, let H be a subgroup of G, and let $N \lhd G$. Then the following hold:*

(i) *$H \cap N \lhd H$,*

(ii) *HN is a subgroup of G,*

(iii) *$HN/N \cong H/H \cap N$.*

Part (iii) is known as the **Second Isomorphism Theorem**.

Proof Part (i) is clear, and part (ii) follows from Prop. 1.19(ii).

Now consider part (iii). Define $\phi : H \mapsto HN/N$ by $\phi(h) = hN$ for all $h \in H$. Then ϕ is a homomorphism, and

$$h \in \mathrm{Ker}(\phi) \Leftrightarrow (h \in H) \cap (hN = N) \Leftrightarrow h \in H \cap N,$$

so $\mathrm{Ker}(\phi) = H \cap N$. Also ϕ is surjective, since any coset in HN/N has the form $hnN = hN = \phi(h)$, where $h \in H, n \in N$. Hence by the First Iso Theorem (1.1),

$$H/\mathrm{Ker}(\phi) = H/H \cap N \cong \mathrm{Im}(\phi) = HN/N. \quad \square$$

Proof of Jordan-Hölder theorem 2.2

The proof is by induction on $|G|$. The base case $|G| = 1$ is trivial. Consider two composition series for G:

$$G \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_r = 1. \tag{2.2}$$

$$G \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_s = 1. \tag{2.3}$$

Case 1: $G_1 = H_1$. In this case, the two series after this term are both composition series for G_1. Hence by induction, they have the same length and composition factors. Adding the composition factor G/G_1 gives the result for G.

Case 2: $G_1 \neq H_1$. In this case, let $K = G_1 \cap H_1 \lhd G$. Choose a composition series for K:

$$K \rhd K_3 \rhd \cdots \rhd K_t = 1.$$

Claim We have $G_1/K \cong G/H_1$ and $H_1/K \cong G/G_1$.

Assuming the Claim (we'll prove it later), we can deduce the theorem as follows. We now have two composition series for G_1:

$$G_1 \rhd G_2 \rhd G_3 \rhd \cdots \rhd G_r = 1,$$
$$G_1 \rhd K \rhd K_3 \rhd \cdots \rhd K_t = 1.$$

By induction, these series have the same length and composition factors. Hence the list of composition factors for the series (2.2) is

$$G/G_1,\ G_1/K,\ K/K_3, \ldots, K_{t-1}. \tag{2.4}$$

Similarly, we have two composition series for H_1:

$$H_1 \rhd H_2 \rhd H_3 \rhd \cdots \rhd H_s = 1,$$
$$H_1 \rhd K \rhd K_3 \rhd \cdots \rhd K_t = 1.$$

By induction these series have the same composition factors, so the list of composition factors for the series (2.3) is

$$G/H_1,\ H_1/K,\ K/K_3, \ldots, K_{t-1}. \tag{2.5}$$

By the Claim, the lists (2.4) and (2.5) are the same (with the first two terms interchanged). So the series (2.2) and (2.3) have the same composition factors, completing the proof of the theorem.

It remains to prove the Claim. We have $G_1 \lhd G$ and $H_1 \lhd G$. So G_1H_1 is a subgroup, and in fact $G_1H_1 \lhd G$ (since $g(g_1h_1)g^{-1} = (gg_1g^{-1})(gh_1g^{-1}) \in G_1H_1$ for $g_1 \in G_1, h_1 \in H_1$). Also $G_1 \neq H_1$ (this is the assumption for Case 2), so $G_1 < G_1H_1 \lhd G$, and so $G_1H_1 = G$ as G_1 is maximal normal in G. Hence using the Second Iso theorem 2.3(iii),

$$G/H_1 = G_1H_1/H_1 \cong G_1/G_1 \cap H_1 = G_1/K.$$

Similarly $G/G_1 \cong H_1/K$, and the Claim is proved. $\square$

By the Jordan-Hölder theorem, every finite group is "built" from a unique list of simple composition factors. But there can be many different groups with the same list of composition factors:

Examples (1) The groups with comp factors C_2, C_3: these are C_6 and D_6.

(2) The groups with comp factors C_p, C_p (p prime): these have order p^2, so are abelian (Sheet 1 qn) – C_{p^2}, $C_p \times C_p$.

(3) Comp factors A_5, C_2: examples are S_5 and $A_5 \times C_2$. Are there others? Yes – see later!

(4) Comp factors $C_p, \ldots, C_p$ (p primes, k factors): all groups of order p^k. There are many different such groups (up to iso of course) – eg. $\sim 56,000$ groups of order 2^8.

(5) Comp factors $C_{p_1}, \ldots C_{p_k}$ (p_i primes, not necessarily distinct): all *solvable* groups of order $p_1 \cdots p_k$. See Chapter 6 for some theory of these.

The Jordan-Hölder theorem poses two basic problems in finite group theory:

(1) What are the finite simple groups?

(2) Give a list of simple groups, what are the groups with these comp factors?

Problem (1) was one of the main focusses of group theory for the 20th century; we'll discuss further in Chapter 3.

Problem (2) is usually referred to as the *Extension Problem*: given groups N, H, what are the groups G such that $N \lhd G$ and $G/N \cong H$? Such a group G is called an *extension* of N by H. We'll discuss the theory of extensions in Chapter 5.

3 Some finite simple groups

In this chapter we'll produce two families of non-abelian finite simple groups, and then briefly discuss the classification of finite simple groups. (The abelian finite simple grops are just C_p, p prime – Sheet 1 qn).

A. Alternating groups

This is our first family of simple groups.

Theorem 3.1 *For $n \geq 5$, the alternating group A_n is simple.*

For the proof we need

Proposition 3.2 *Let $n \geq 4$. Then every element of A_n can be expressed as a product of 3-cycles.*

Proof Let $x \in A_n$. Then x is a product of and even number of 2-cycles, say $x = t_1 t_2 \cdots t_{2k}$. Consider $t_1 t_2$, assuming $t_1 \neq t_2$. If these 2-cycles are not disjoint, then $t_1 t_2$ is a 3-cycle; and if they are disjoint, say $t_1 t_2 = (12)(34)$ (after relabelling), then $t_1 t_2 = (123)(234)$. Hence each of the products $t_1 t_2, t_3 t_4, \ldots, t_{2k-1} t_{2k}$ is a product of 3-cycles. □

Proof of Theorem 3.1 The proof is by induction on n. We know that A_5 is simple by Prop. 1.14, starting the induction.

Now assume $n \geq 6$, and let $G = A_n$. Let $N \neq 1$ be a normal subgroup of G. For any $i \in \{1, \ldots, n\}$, the stabilizer $G_i \cong A_{n-1}$, which by induction is simple. Since $N \cap G_i \triangleleft G_i$, it follows that $N \cap G_i = 1$ or G_i.

Suppose $N \cap G_i = G_i$ for some i. Then $G_i \leq N$, so N contains a 3-cycle t. As $N \triangleleft G$, the conjugacy class $t^G \subseteq N$. By Prop. 1.13, t^G consists of all the 3-cycles, and hence $\langle t^G \rangle = A_n$ by Prop. 3.2. Hence $N = G$ in this case.

Assume now that $N \cap G_i = 1$ for all i. We now emply a cunning trick using commutators. Let $1 \neq n \in N$. We can find a 3-cycle t that does not commute with n: relabelling points, we can take $n = (1\,2) \cdots$ or $(1\,2\,3\ldots) \cdots$, and then let $t = (1\,2\,4)$. Consider the commutator

$$x = [t, n] = tnt^{-1}n^{-1} \neq 1$$

(it is not 1 as $tn \neq nt$). On the one hand, $x = (tnt^{-1})n^{-1}$ is in N, since $N \triangleleft G$. On the other hand,

$$x = t\,(nt^{-1}n^{-1}) = (1\,2\,4)\,(2\,j\,k).$$

So $x \in N$ and x moves at most 5 points, which means that $x \in G_i$ for some i, a contradiction. This completes the proof. □

B. Matrix groups

Our next family of simple groups will consist of matrix groups over finite fields. Recall that $GL_n(F)$ is the group of invertible $n \times n$ matrices over a field F. For each prime power $q = p^a$, there is a finite field of order q, which we denote by $\mathbb{F}_q$, and we usually write $GL_n(q)$ for the group $GL_n(\mathbb{F}_q)$. First we compute the order of these groups.

Proposition 3.3 *We have*

$$|GL_n(q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1}) = q^{\frac{1}{2}n(n-1)}\prod_{i=1}^{n}(q^i-1).$$

Proof We need to compute the number of invertible $n \times n$ matrices over $\mathbb{F}_q$. Let $V = \mathbb{F}_q^n$, an n-dimensional vector space over $\mathbb{F}_q$, and note that the number of vectors $|V| = q^n$. Recall that a matrix is invertible iff its rows are linearly independent vectors in $V = \mathbb{F}_q^n$. For such a matrix, denoting its rows by $r_1, \ldots, r_n$,

$$\begin{array}{ll}
\text{number of choices for row } r_1 & = |V \setminus 0| = q^n - 1, \\
\text{number of choices for row } r_2 & = |V \setminus \mathrm{Sp}(r_1)| = q^n - q, \\
\text{number of choices for row } r_3 & = |V \setminus \mathrm{Sp}(r_1, r_2)| = q^n - q^2, \\
\ldots & \ldots \\
\text{number of choices for row } r_n & = |V \setminus \mathrm{Sp}(r_1, \ldots, r_{n-1})| = q^n - q^{n-1}.
\end{array}$$

Hence $|GL_n(q)|$ is the product of these terms. □

Recall the *special linear group* $SL_n(F) = \{g \in GL_n(q) : \det(g) = 1\}$. As for GL, we write $SL_n(q)$ for the group $SL_n(\mathbb{F}_q)$.

Proposition 3.4 *$SL_n(q)$ is a normal subgroup of $GL_n(q)$, and has order $\frac{|GL_n(q)|}{q-1}$.*

Proof Denote by $\mathbb{F}_q^*$ the multiplicative group $\mathbb{F}_q \setminus 0$. The homomorphism $\det : GL_n(q) \mapsto \mathbb{F}_q^*$ has kernel $SL_n(q)$ and image $\mathbb{F}_q^*$ of order $q-1$. □

Now consider the centres of the groups $GL_n(F)$ and $SL_n(F)$. A question on Sheet 1 asks you to show that

$$Z_{GL} = Z(GL_n(F)) = \{\lambda I_n : \lambda \in F^*\},$$
$$Z_{SL} = Z(SL_n(F)) = \{\lambda I_n : \lambda^n = 1\}.$$

Definition The *projective general linear* group $PGL_n(F)$ and *projective special linear* group $PSL_n(F)$ are defined by

$$PGL_n(F) = GL_n(F)/Z_{GL}, \quad PSL_n(F) = SL_n(F)/Z_{SL}.$$

It is a basic fact that for $n \geq 2$, the finite projective special linear groups $PSL_n(q)$ are simple, with the exception of $PSL_2(2)$ and $PSL_2(3)$. We shall prove this just for the case $n = 2$. (The case $n \geq 3$ is no harder, but the proof is different to the $n = 2$ case and would take too much time.)

What is the order of $PSL_2(q)$? Well, by Props. 3.3 and 3.4, we have $|SL_2(q)| = q(q^2-1)$. The order of the centre $Z_{SL} = \{\lambda I_2 : \lambda^2 = 1\}$ is the number of solutions to the equation $\lambda^2 = 1$ in $\mathbb{F}_q$; this is 2 if q is odd (solutions $\lambda = \pm 1$), and 1 if q is even (since then $q = 2^a$ and the only solution is $\lambda = 1$ as $-1 = 1$ in $\mathbb{F}_q$). Hence $|Z_{SL}| = (2, q-1)$ (the gcd) and so

$$|PSL_2(q) = q(q^2-1)/(2, q-1). \tag{3.1}$$

For example, $|PSL_2(2)| = 6$, $|PSL_2(3)| = 12$, $|PSL_2(4)| = |PSL_2(5)| = 60$, $|PSL_2(7)| = 168$. In fact the following isomorphisms hold (qn on Sheet 2):

$$PSL_2(2) \cong S_3, \quad PSL_2(3) \cong A_4.$$

So these groups are not simple.

Theorem 3.5 *For $q > 3$, the group $PSL_2(q)$ is simple.*

The proof has some similarities with the proof of simplicity of A_n. We use commutators at several points, and also we use a special generating set: for A_n this was the 3-cycles, and for $SL_n(q)$ (and $PSL_n(q)$), it is the *elementary matrices*.

Recall that an elementary $n \times n$ matrix over a field F is a matrix of the form

$$E_{ij}(\lambda) = I_n + \lambda E_{ij},$$

where $\lambda \in F$ and E_{ij} is the matrix with 1 in the ij-entry and 0 elsewhere (and also $i \neq j$).

Proposition 3.6 *Let $A \in GL_n(F)$ with $\det(A) = \mu$. Then $A = U\,D(\mu)$, where U is a product of elementary matrices, and $D(\mu)$ is the diagonal matrix $\mathrm{diag}(1, \ldots, 1, \mu)$.*

Proof This is just row reduction from Year 1 linear algebra. Recall that if an $n \times n$ matrix A has rows $r_1, \ldots, r_n$, then $E_{ij}(\lambda)A$ has the same rows, except that r_i is replaced by $r_i + \lambda r_j$.

Let $A = (a_{ij})$. Adding some row to row 2, we can assume that $a_{21} \neq 0$. Then add $a_{21}^{-1}(1 - a_{11})r_2$ to r_1 to get $a_{11} = 1$. Now subtract multiples of r_1 from the other rows to get a matrix $U_1 A$ with first column $(1, 0, \ldots, 0)^T$, where U_1 is a product of elementary matrices. Repeat with columns $2, \ldots, n-1$ to get

$$U_{n-1}A = \begin{pmatrix} I_{n-1} & * \\ 0 & \mu \end{pmatrix},$$

where again U_{n-1} is a product of elementary matrices. Finally, clearing the last column gives $U_n A = D(\mu)$. Then $A = U_n^{-1} D(\mu)$. The result follows, since the inverse of an elementary matrix is also elementary. □

Corollary 3.7 *For any field F and any $n \geq 2$, the special linear group $SL_n(F)$ is generated by elementary matrices.*

Proof of Theorem 3.5

Let $G = SL_2(q)$ with $q > 3$. Let N be a subgroup of G such that $Z_{SL} < N \triangleleft G$. We'll show that $N = G$, which is enough to prove that $G/Z_{SL} = PSL_2(q)$ is simple.

Step 1 If $E_{12}(\lambda) \in N$ for some $0 \neq \lambda \in \mathbb{F}_q$, then $N = G$.

Proof Let $U_{12} = \{E_{12}(\beta) : \beta \in \mathbb{F}_q\} \cong (\mathbb{F}_q, +)$. For any $\alpha \in \mathbb{F}_q^*$, N contains

$$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{pmatrix} = E_{12}(\lambda\alpha^2),$$

and hence $U_{12} \cap N \supseteq \{E_{12}(\lambda\alpha^2) : \alpha \in \mathbb{F}_q^* \text{ or } \alpha = 0\}$. Since the squares in $\mathbb{F}_q^*$ form a subgroup of size $(q-1)/(2, q-1)$, the latter set has size greater than $\frac{1}{2}q$. Hence $U_{12} \leq N$.

Also N contains

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = E_{21}(\lambda),$$

and so we see similarly that $U_{21} \leq N$. Hence $N = SL_2(q) = G$ by Cor. 3.7.

Step 2 If N contains a matrix $A = \begin{pmatrix} \alpha & 0 \\ \beta & \alpha^{-1} \end{pmatrix}$ for some $\alpha \neq \pm 1$, then $N = G$.

Proof As $N \triangleleft G$, N contains the commutator

$$[E_{21}(1), A] = E_{21}(1 - \alpha^{-2}).$$

Hence $N = G$ by Step 1.

Now we complete the proof of the theorem. We can assume that N contains no element A as in Step 2. Let $n \in N \setminus Z_{SL}$. By our assumption, n is not triangularisable, so its minimal polynomial is irreducible, hence is $x^2 - \beta x + 1$ for some $\beta \in \mathbb{F}_q$ (the constant term is 1 since n has det 1). By the RCF theorem, there exists $y \in GL_2(q)$ such that

$$y^{-1}ny = \begin{pmatrix} 0 & -1 \\ 1 & \beta \end{pmatrix}.$$

Letting $\mu = \det(y)$, we have $y = gD(\mu)$ where $g \in SL_2(q) = G$, and hence

$$g^{-1}ng = D(\mu) \begin{pmatrix} 0 & -1 \\ 1 & \beta \end{pmatrix} D(\mu)^{-1} = \begin{pmatrix} 0 & -\mu \\ \mu^{-1} & \beta \end{pmatrix} = n' \in N.$$

Now consider the commutator

$$[\begin{pmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{pmatrix}, -n'] = \begin{pmatrix} \alpha^{-2} & 0 \\ \mu\beta(\alpha^2 - 1) & \alpha^2 \end{pmatrix} = n'' \in N.$$

This matrix is of the form A in Step 2, unless $\alpha^2 = \pm 1$, i.e. $\alpha^4 = 1$. As $q \geq 4$, we can choose $\alpha \in \mathbb{F}_q^*$ such that $\alpha^4 \neq 1$ unless $q = 5$. So the proof is complete, apart from this case.

Assume finally that $q = 5$. Let $\alpha = 2$, so that $\alpha^2 = -1$. Let $n'' \in N$ be the matrix above. Then $(n'')^2$ is a non-identity elementary matrix unless $\beta = 0$, in which case n is diagonalisable, contrary to assumption. This completes the proof. $\square$

The Classification

One of the main focusses in finite group theory in the 20th century was the attempt to classify all the finite simple groups. A real strategy for doing this did not emerge until the 1950s, and one of the first of many monumental theorems was the famous Odd Order Theorem of Feit and Thompson, published in 1963. This theorem, the proof of which occupied 255 pages of the Pacific Journal of Mathematics, states that every group of odd order is solvable – so any non-abelian finite simple group must necessarily have even order. This may not sound like a big deal, but it is. It means that any such simple group G must have an element t of order 2, and the classification strategy, originally proposed by Brauer, was to attempt to restrict the possibilities for the structure of the centralizer $C_G(t)$, and then to classify the simple groups G with such a centralizer. Hundreds of mathematicians worked on the project over a period of about 50 years, and eventually the classification theorem was finally proved. It is estimated that the papers and books containing the proof consisted of over 15.000 pages. This is surely the longest and most complicated proof of any single result in mathematical history. Since then, several authors have been revising and streamlining the original proof and it is being published in a series of twelve volumes, nine of which have now appeared.

Here is a somewhat rough statement of the classification theorem – necessarily rough, as we have defined very few of the examples of simple groups in the statement.

Classification theorem for finite simple groups The following is a list of all the finite simple groups:

(1) cyclic groups C_p (p prime)

(2) alternating groups A_n ($n \geq 5$)

(3) six families of "classical" matrix groups over finite fields $\mathbb{F}_q$: the first of these families is $PSL_n(q)$

(4) ten families of "exceptional groups of Lie type" over fields $\mathbb{F}_q$

(5) 26 "sporadic" groups.

The sporadic simple groups are those simple groups that do not lie in any of the infinite families in (1)–(4). The first of these were the five Mathieu groups, discovered in 1861. The next sporadic group was not discovered until 1965, by Janko, and subsequently a steady stream of new sporadic groups was found by various methods, until the last and biggest one, the Monster, was constructed in 1982. It is a truly monstrous group of order roughly 10^{54}, constructed as a group of 196884×196884 matrices.

In the course we will develop a few methods for studying simple groups, mainly concerning their possible orders. For example, we already know that a simple group cannot have prime power order p^a with $a \geq 2$ (since such a group has a nontrivial centre, by Prop. 1.9). Such methods will be illustrated in Chapter 4, and in the final Chapter 7 we will introduce some more sophisticated methods for studying simple groups.

4 Sylow's theorems

Lagrange's theorem says that if G is a group of order n, then the order of any subgroup of G divides n. However, the converse is not true: if m is a divisor of n, then G may or may not have a subgroup of order m. An example is $G = A_4$ of order 12, which has no subgroup of order 6 (question on Sheet 1).

In 1872, Sylow published some theorems, the first of which provides a converse to Lagrange for all prime powers that divide $n = |G|$.

Theorem 4.1 (Sylow I) *Let $|G| = p^a m$, where p is prime and $p \nmid m$. Then G has a subgroup of order p^a.*

Proof The proof goes by induction on $|G|$. The result holds trivially for $|G| = 1$, starting the induction. Recall the conjugacy class equation (1.1):

$$|G| = |Z(G)| + \sum_{i=1}^{k} |x_i^G|, \tag{4.1}$$

where $x_1^G, \ldots, x_k^G$ are the non-central conjugacy classes of G.

We consider the two possibilities: (1) $p \mid |Z(G)|$, and (2) $p \nmid |Z(G)|$.

Case (1) Suppose $p \mid |Z(G)|$. Then by Cauchy's theorem 1.8, there exists $z \in Z(G)$ of order p. (Note that this uses Cauchy's theorem only for the *abelian* group $Z(G)$ – Cauchy's theorem is actually much easier to prove for abelian groups than for general groups.) Then $\langle z \rangle \triangleleft G$, and by induction, the quotient group $G/\langle z \rangle$ has a subgroup $P/\langle z \rangle$ of order p^{a-1}. Then $|P| = p^a$, giving the result in this case.

Case (2) Suppose $p \nmid |Z(G)|$. Then by(4.1), there exists a conjugacy class x_i^G such that p does not divide $|x_i^G|$. By Prop. 1.10, $|x_i^G| = |G : C_G(x_i)|$, so this means that p^a divides $|C_G(x_i)|$. As x_i is non-central $|C_G(x_i)| < |G|$, and so by induction, $C_G(x_i)$ has a subgroup of order p^a. Hence the result holds in this case also. □

Definition Let $|G| = p^a m$, where p is prime and $p \nmid m$. A subgroup of G of order p^a is called a *Sylow p-subgroup* of G. We write $Syl_p(G)$ for the set of all Sylow p-subgroups of G.

Let $P \in Syl_p(G)$. For $g \in G$, the conjugate ${}^gP = gPg^{-1}$ is also a subgroup of order p^a, so ${}^gP \in Syl_p(G)$. Thus G acts by conjugation on $Syl_p(G)$. The stabilizer of P in this action is $\{g \in G : gPg^{-1} = P\} = N_G(P)$, the normalizer of P in G.

Define $n_p(G) = |Syl_p(G)|$, the number of Sylow p-subgroups of G.

Theorem 4.2 (Sylow II) *We have $n_p(G) \equiv 1$ mod p.*

Theorem 4.3 (Sylow III) *Let Q be a p-subgroup of G. Then there exists $P \in Syl_p(G)$ such that $Q \leq P$.*

Theorem 4.4 (Sylow IV) *$Syl_p(G)$ is a single conjugacy class of subgroups of G; that is, for any $P, Q \in Syl_p(G)$, there exists $g \in G$ such that $Q = {}^gP$.*

We shall prove these shortly. First we derive a corollary.

Corollary 4.5 *Let $P \in Syl_p(G)$. Then the following hold:*

(i) $n_p(G) = |G : N_G(P)|$,

(ii) $n_p(G)$ *divides* $|G|$,

(iii) $n_p(G) = 1$ *iff* $P \triangleleft G$.

Proof (i) Theorem 4.4 says that G acts transitively on $Syl_p(G)$. Since the stabilizer of P is $N_G(P)$, the orbit stabilizer theorem gives (i).

Parts (i) and (iii) follow from (i). $\square$

For the proof of the Sylow theorems II-IV we need the following result.

Lemma 4.6 *Let $P \in Syl_p(G)$, and let Q be a p-subgroup of G. If $Q \leq N_G(P)$, then $Q \leq P$.*

Proof Suppose $Q \leq N_G(P)$. Then by Prop. 1.19, PQ is a subgroup of G, and

$$|PQ| = \frac{|P|\,|Q|}{|P \cap Q|} = p^a\,|Q : P \cap Q|,$$

where $|P| = p^a$. Since $p^{a+1} \nmid |G|$, it follows that $Q = P \cap Q$, which means that $Q \leq P$. $\square$

Proof of Theorem 4.2

Let $P \in Syl_p(G)$. Consider the action of P on $Syl_p(G)$ by conjugation. In this action, $\{P\}$ is an orbit of size 1. If $\{Q\}$ is another orbit of size 1, then ${}^xQ = Q$ for all $x \in P$, which means that $P \leq N_G(Q)$. By Lemma 4.6, this implies that $P \leq Q$, and hence $P = Q$ (as they both have the same order).

We conclude that in the action of P on $Syl_p(G)$, there is exactly one orbit of size 1. By the orbit stabilizer theorem, the other orbits have size dividing $|P|$, hence divisible by p. Therefore $|Syl_p(G)| = n_p(G) \equiv 1 \bmod p$. $\square$

Proof of Theorem 4.3

Let Q be a p-subgroup of G. Consider the action of Q on $Syl_p(G)$ by conjugation. As $n_p(G) \equiv 1 \bmod p$ by Thm. 4.2, not every orbit of Q has size divisible by p, and so there is an orbit of size 1; call it $\{P\}$. Then $Q \leq N_G(P)$, and so $Q \leq P$ by Lemma 4.6. $\square$

Proof of Theorem 4.4

Let $P \in Syl_p(G)$, and let Ω be the orbit of G on $Syl_p(G)$ containing P; that is,

$$\Omega = \{\, {}^gP : g \in G\}.$$

Consider the action of P on Ω. As we saw in the proof of Thm. 4.2, P has exactly one orbit of size 1, and the others have size divisible by p, so $|\Omega| \equiv 1 \bmod p$.

Now let $Q \in Syl_p(G)$ and consider the action of Q on Ω. As $|\Omega| \equiv 1 \bmod p$, there is an orbit of size 1; call it $\{R\}$. Then $Q \leq N_G(R)$, and so $Q = R$ by Lemma 4.6. Hence $Q \in \Omega$. Since Q was arbitrary, this shows that $\Omega = Syl_p(G)$, completing the proof. $\square$

For convenience, here is a summary of the information provided by the Sylow theorems:

Summary Let G be a finite group and p a prime.

(1) $Syl_p(G) \neq \emptyset$.

(2) G acts transitively by conjugation on $Syl_p(G)$.

(3) If $n_p(G) = |Syl_p(G)|$, then $n_p(G) \equiv 1 \bmod p$.

(4) If $P \in Syl_p(G)$, then $n_p(G) = |G : N_G(P)|$ and this divides $|G|$.

(5) $n_p(G) = 1$ iff $P \lhd G$.

These facts can be used rather effectively to study groups via "Sylow arithmetic". We now give a few examples of this; more can be found in the exercises on Sheet 2.

Proposition 4.7 *Let $|G| = pq$, where p, q are primes and $p > q$. Then*

(i) *G has a normal Sylow p-subgroup.*

(ii) *If also $q \nmid p - 1$, then $G \cong C_{pq}$.*

Proof (i) By items (3) and (4) above, $n_p(G) = 1$ or q. As $p > q$, we have $q \not\equiv 1 \bmod p$, so $n_p(G) = 1$, which means that $P \lhd G$ by (5) (where $P \in Syl_p(G)$).

(ii) Suppose $q \nmid p - 1$. Then $p \not\equiv 1 \bmod q$, so $n_q(G) = 1$ and so $Q \lhd G$, where $Q \in Syl_q(G)$. We now have $P \lhd G$, $Q \lhd G$, $P \cap Q = 1$ and $G = PQ$. It follows by Prop. 1.5 that $G \cong P \times Q \cong C_p \times C_q \cong C_{pq}$. $\square$

Note that if $q \mid p - 1$, then there exists a non-abelian group of order pq. This is best constructed as a "semidirect product", which we shall do in the next chapter (see Prop. 5.4).

Proposition 4.8 *Let $|G| = p^2q$ with p, q primes. Then G has either a normal Sylow p-subgroup or a normal Sylow q-subgroup.*

Proof Suppose false, so that $n_p(G) > 1$ and $n_q(G) > 1$. Then we must have $n_p(G) = q \equiv 1 \bmod p$.

Also $n_q(G) = p$ or p^2. If $n_q(G) = p$, then $p \equiv 1 \bmod q$, and so $p > q$; but this is not possible as $q \equiv 1 \bmod p$.

Hence $n_q(G) = p^2$. Now we count elements of order q in G. There are p^2 Sylow q-subgroups, all of prime order q, and if $Q_1, Q_2 \in Syl_q(G)$ are distinct, then $Q_1 \cap Q_2 = 1$. Hence

$$|\bigcup\{Q \setminus 1 : Q \in Syl_q(G)\}| = p^2(q-1) = |G| - p^2.$$

Let $P \in Syl_p(G)$. Since $|P| = p^2$, this implies that P is the only Sylow p-subgroup. Hence $n_p(G) = 1$, a contradiction. $\square$

Proposition 4.9 *Let $|G| = p^3q$ with p, q prime. Then one of the following holds:*

(i) *G has either a normal Sylow p-subgroup or a normal Sylow q-subgroup.*

(ii) $|G| = 24$.

Proof This is a question on Sheet 2.

Notice that the exception in part (ii) really exists: S_4 is a group of order 24 with no normal Sylow 2-subgroup or Sylow 3-subgroup.

The orders of simple groups

Suppose we want to investigate which positive integers can be equal to the order of a finite non-abelian simple group. The Sylow theorems provide us with the following tool.

Proposition 4.10 *Let $|G| = p^a m$, where p is prime, $a \geq 1$, $m \geq 2$ and $p \nmid m$. Suppose G is simple, and let $n = n_p(G)$. Then*

(i) *n divides m.*

(ii) *$n \equiv 1$ mod p and $n > 1$.*

(iii) *$|G|$ divides $n!$*

Proof Parts (i) and (ii) are Sylow theorems (note that $n > 1$ as a Sylow p-subgroup is not normal in the simple group G).

Now consider (iii). By Sylow IV, G acts transitively on $\Omega = Syl_p(G)$, and $|\Omega| = n$. Hence there is a homomorphism $\phi : G \mapsto Sym(\Omega) \cong S_n$. Then $\mathrm{Ker}(\phi) \lhd G$, and $\mathrm{Ker}(\phi) \neq G$. As G is simple, $\mathrm{Ker}(\phi) = 1$. Hence $G \cong \mathrm{Im}(\phi) \leq S_n$, proving (iii). $\square$

Using this we can rule out many possible order of simple groups. Here is one example:

Proposition 4.11 *If G is a non-abelian simple group of order ≤ 100, then $|G| = 60$ and $G \cong A_5$.*

Proof This is a question in Sheet 2. Here is a sketch to get started. We can rule out prime powers by Prop. 1.9, and numbers of the form pq, p^2q or p^3q (apart from 24) by Props. 4.7, 4.8, 4.9. The remaining numbers ≤ 100 are: $24, 30, 36, 42, 48, 60, \ldots, 100$. These can be ruled out one by one (apart from 60 of course).

For example, suppose $|G| = 24 = 2^3 3$ and G is simple. Then $n_2(G)$ must be 3. But this implies that $|G|$ divides 3!, a contradiction.

We omit the rest of the proof. The trickiest part is to show that a simple group of order 60 must be isomorphic to A_5. This requires some nice applications of Sylow theorems. $\square$

5 Extensions and semidirect products

If N, H are groups, an *extension of N by H* is a group G with the following properties:

- G has a normal subgroup $N_0 \cong N$,
- the quotient group $G/N_0 \cong H$.

We represent this by a sequence

$$N \mapsto^{\phi} G \mapsto^{\psi} H,$$

where ϕ is injective, ψ is surjective, and $\mathrm{Ker}(\psi) = \mathrm{Im}(\phi)$. (In this setup, the normal subgroup $N_0 = \mathrm{Im}(\phi)$.)

Examples (1) C_4 and $C_2 \times C_2$ are both extensions of C_2 by C_2.

(2) S_4 is an extension of $V_4 \cong C_2 \times C_2$ by S_3. So is $S_3 \times C_2 \times C_2$.

(3) Let p be prime, and define the subgroup

$$G = \{\begin{pmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{pmatrix} : \alpha \in \mathbb{F}_p^*, \beta \in \mathbb{F}_p\} \leq SL_2(p).$$

Then G has subgroups

$$N = \{\begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} : \beta \in \mathbb{F}_p\} \cong \mathbb{F}_p^+, \quad H = \{\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} : \alpha \in \mathbb{F}_p^*\} \cong \mathbb{F}_p^*.$$

Check that $N \lhd G$, $G = NH$. $N \cap H = 1$ and $G/N = NH/N \cong H$. Hence G is an extension of $\mathbb{F}_p^+$ by $\mathbb{F}_p^*$.

The extension problem Given N, H, can we find (up to isomorphism) *all* extensions of N by H?

In general this is a very difficult question, but we shall solve it for extensions of a certain type – namely, *split* extensions. Here is the definition of these.

Definition Let G be a group with a normal subgroup $N_0 \cong N$ and let $G/N_0 = H$; so G is an extension of N by H. We say the extension is *split* if there exists a subgroup H_0 of G such that

$$G = N_0 H_0 \text{ and } N_0 \cap H_0 = 1.$$

Note that $H = G/N_0 = N_0H_0/N_0 \cong H_0$.

Examples (1) $C_2 \times C_2$ is a split extension of C_2 by C_2; and S_4 is a split extension of $C_2 \times C_2$ by S_3.

(2) C_4 is a non-split extension of C_2 by C_2; and $SL_2(3)$ is a non-split extension of C_2 by A_4 (Sheet 3).

(3) For any N, H, the direct product $N \times H$ is a split extension of N by H: take $N_0 = N \times 1$, $H_0 = 1 \times H$.

Aim Given N, H, to construct *all* split extensions of N by H.

The semidirect product

Suppose we have a split extension

$$G = NH,\ N \lhd G,\ N \cap H = 1. \tag{5.1}$$

For $h \in H$, define the map $\iota_h : N \mapsto N$ by $\iota_h(n) = hnh^{-1}$ for $n \in N$.

Proposition 5.1 *Let $G = NH$ be a split extension as in* (5.1).

(i) *Every $g \in G$ can be written as $g = nh$ for unique elements $n \in N, h \in H$.*

(ii) $\iota_h \in \mathrm{Aut}(N)$.

(iii) *The map $\iota : H \mapsto \mathrm{Aut}(N)$ sending $h \mapsto \iota_h$ is a homomorphism.*

(iv) *Multiplication in G is determined by the homomorphism ι, as follows:*

$$(n_1h_1)\,(n_2h_2) = (n_1\iota_{h_1}(n_2))\,(h_1h_2)$$

for $n_i \in N, h_i \in H$.

Proof (i) $n_1h_1 = n_2h_2 \Rightarrow n_2^{-1}n_1 = h_2h_1^{-1} \in N \cap H = 1 \Rightarrow n_1 = n_2, h_1 = h_2$.
(ii) ι_h is a bijection, and $\iota_h(n_1n_2) = hn_1n_2h^{-1} = (hn_1h^{-1})(hn_2h^{-1}) = \iota_h(n_1)\iota_h(n_2)$.
(iii) $\iota_{h_1h_2}(n) = h_1h_2nh_2^{-1}h_1^{-1} = \iota_{h_1}\iota_{h_2}(n)$.
(iv) We have

$$\begin{aligned}(n_1h_1)\,(n_2h_2) &= n_1\,(h_1n_2h_1^{-1})\,h_1h_2\\ &= (n_1\iota_{h_1}(n_2))\,(h_1h_2). \quad \square\end{aligned}$$

Summarising: given a split extension $G = NH$ as in (5.1), there is a homomorphism $\iota : H \mapsto \mathrm{Aut}(N)$ that determines the multiplication in G as in 5.1(iv).

Conversely, given groups N, H and a homomorphism $\iota : H \mapsto \mathrm{Aut}(N)$, we shall construct a split extension of N by H with multiplication as in 5.1(iv), called the *semidirect product* $N \rtimes_\iota H$, as follows.

Construction of $N \rtimes_\iota H$. The set of elements is $\{(n, h) : n \in N, h \in H\}$, with multiplication

$$(n_1, h_1)\,(n_2, h_2) = (n_1\iota_{h_1}(n_2), h_1h_2),$$

where $n_i \in N, h_i \in H$ and $i_{h_1} = \iota(h_1)$.

From the definition it is not completely obvious that this multiplication defines a group. We prove this and other basic properties in the next result.

Proposition 5.2 *Let $X = N \rtimes_\iota H$ as defined above.*

(i) *X is a group under this multiplication.*

(ii) *Let $N_0 = \{(n, 1_H) : n \in N\}$, $H_0 = \{(1_N, h) : h \in H\}$. Then N_0, H_0 are subgroups of X isomorphic to N, H; and $N_0 \lhd X$, $N_0 \cap H_0 = 1$ and $X = N_0H_0$.*

(iii) *If $G = NH$ is a split extension with multiplication as in* 5.1(iv)*, then $G \cong N \rtimes_\iota H$.*

Proof (i) *Associativity:* For $n_i \in N, h_i \in H$,

$$\begin{aligned}(\,(n_1,h_1)(n_2,h_2)\,)\,(n_3,h_3) &= (n_1\iota_{h_1}(n_2),h_1h_2)\,(n_3,h_3)\\ &= (n_1\iota_{h_1}(n_2)\iota_{h_1h_2}(n_3),h_1h_2h_3)\\ &= (n_1\iota_{h_1}(n_2\iota_{h_2}(n_3)),h_1h_2h_3)\\ &= (n_1,h_1)\,(n_2\iota_{h_2}(n_3),h_2h_3)\\ &= (n_1,h_1)\,(\,(n_2,h_2)(n_3,h_3)\,).\end{aligned}$$

Identity is $(1_N,1_H)$.
Inverse of (n,h) is $(\iota_{h^{-1}}(n^{-1}),h^{-1})$.

(ii) The maps $N \mapsto X$ and $H \mapsto X$ defined by $n \mapsto (n,1_H)$ and $h \mapsto (1_N,h)$ are injective homomorphisms, with images $N_0 \cong N$, $H_0 \cong H$. Clearly $N_0 \cap H_0 = 1$, and $X = N_0H_0$ (since $(n,h) = (n,1)(1,h)$). Finally, $N_0 \lhd X$ since

$$(1,h)\,(n,1)\,(1,h)^{-1} = (\iota_h(n),1).$$

(iii) Let $G = NH$, with multiplication as in 5.1(iv). Define $\phi : N \rtimes_\iota H \mapsto G$ by $\phi(n,h) = nh$ for $n \in N, h \in H$. Then ϕ is a bijection, and is also a homomorphism, as

$$\begin{aligned}\phi(\,(n_1,h_1)(n_2,h_2)\,) &= \phi(n_1\iota_{h_1}(n_2),h_1h_2)\\ &= n_1\iota_{h_1}(n_2)h_1h_2\\ &= (n_1h_1)(n_2h_2)\quad\square\end{aligned}$$

Summary To construct *all* split extensions of N by H:

- find all homomorphisms $\iota : H \mapsto \mathrm{Aut}(N)$
- the corresponding semidirect products $N \rtimes_\iota H$ are (up to isomorphism) all the split extensions.

Examples (1) If $\iota : H \mapsto \mathrm{Aut}(N)$ is the trivial homomorphism (sending $h \mapsto 1$ for all $h \in H$), then the multiplication in $N \rtimes_\iota H$ is $(n_1,h_1)\,(n_2,h_2) = (n_1n_2,h_1h_2)$, and so $N \rtimes_\iota H = N \times H$, the direct product.

(2) Let G be the split extension of $\mathbb{F}_p^+$ by $\mathbb{F}_p^*$ defined in (3) of the first set of examples above. Check that for $\alpha \in \mathbb{F}_p^*$, $\beta \in \mathbb{F}_p$,

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

Hence $G = \mathbb{F}_p^+ \rtimes_\iota \mathbb{F}_p^*$, where $\iota : \mathbb{F}_p^* \mapsto \mathrm{Aut}(\mathbb{F}_p^*)$ is defined by

$$\iota(\alpha) : \beta \mapsto \beta\alpha^2.$$

(3) What are the split extensions of $C_2 \times C_2$ by C_3? If G is such an extension, then $G \cong (C_2 \times C_2) \rtimes_\iota C_3$, where $\iota : C_3 \mapsto \mathrm{Aut}(C_2 \times C_2)$. By a question on Sheet 1, $\mathrm{Aut}(C_2 \times C_2) \cong GL_2(2) \cong S_3$. So there are three such homoms ι: writing $C_3 = \langle x \rangle$, they are

(a) ι_1, the trivial homom,

(b) $\iota_2 : x \mapsto (1\,2\,3)$,

(c) $\iota_3 : x \mapsto (1\,3\,2)$.

In case (a), $G \cong C_2 \times C_2 \times C_3$. But what about (b) and (c)? Since we know that $A_4 = V_4C_3$ is a split extension of $C_2 \times C_2$ by C_3, at least one of (b) and (c) give semidirect product isomorphic to A_4. Which one? Both?

Example (3) leads to the following basic question:

Question Let $\iota : H \mapsto \mathrm{Aut}(N)$ and $j : H \mapsto \mathrm{Aut}(N)$ be homoms. When are the semidirect products $N \rtimes_\iota H$ and $N \rtimes_j H$ isomorphic?

In general this is a difficult question. But the next proposition provides a useful sufficient condition.

Proposition 5.3 *Let N, H be finite groups, and let $\iota, j : H \mapsto \mathrm{Aut}(N)$ be homomorphisms. Suppose there exist $\alpha \in \mathrm{Aut}(N)$ and $\beta \in \mathrm{Aut}(H)$ such that*

$$j(\beta(h)) = \alpha\, \iota(h)\, \alpha^{-1} \quad \textit{for all } h \in H. \tag{5.2}$$

Then $N \rtimes_\iota H \cong N \rtimes_j H$.

Proof Define $\phi : N \rtimes_\iota H \mapsto N \rtimes_j H$ by

$$\phi(n, h) = (\alpha(n), \beta(h)) \quad \text{for } n \in N, h \in H.$$

Then ϕ is a bijection, so we need to show ϕ is a homomophism. Well,

$$\begin{aligned} \phi(n_1, h_1)\, \phi(n_2, h_2) &= (\alpha(n_1), \beta(h_1))\, (\alpha(n_2), \beta(h_2)) \\ &= (\alpha(n_1) j_{\beta(h_1)}(\alpha(n_2)),\ \beta(h_1)\beta(h_2)). \end{aligned} \tag{5.3}$$

and

$$\begin{aligned} \phi(\,(n_1, h_1)\,(n_2, h_2)\,) &= \phi(n_1 \iota_{h_1}(n_2),\ h_1 h_2) \\ &= (\alpha(n_1 \iota_{h_1}(n_2)),\ \beta(h_1 h_2)) \\ &= (\alpha(n_1)\alpha(\iota_{h_1}(n_2)),\ \beta(h_1 h_2)). \end{aligned} \tag{5.4}$$

The right hand sides of (5.3) and (5.4) are equal by the hypothesis (5.2) of the proposition. □

Example Let's return to Example (3) above. There we see that condition (5.2) holds for the homoms ι_2 and ι_3, taking $\beta \in \mathrm{Aut}(C_3)$ to send $x \mapsto x^2$ and $\alpha = 1$. Hence

$$(C_2 \times C_2) \rtimes_{\iota_1} C_3 \cong (C_2 \times C_2) \rtimes_{\iota_2} C_3 \cong A_4.$$

Remark Condition (5.2) is certainly not in general necessary for the isomorphism $N \rtimes_\iota H \cong N \rtimes_j H$. For example, let $G = T \times T$ for some group T. Then $G \cong T \rtimes_\iota T \cong T \rtimes_j T$, where $\iota : T \mapsto \mathrm{Aut}(T)$ is the trivial homom and $j : T \mapsto \mathrm{Aut}(T)$ is the homom sending $t \mapsto c_t$, where c_t is the automorphism of T conjugating all elements by t (see Sheet 3 qn). So ι has image 1, while j has image $\mathrm{Inn}(T)$, and provided T is non-abelian (so that $\mathrm{Inn}(T) \neq 1$), there are no auts α, β that satisfy condition (5.2).

Here is out next application of this result.

The groups of order pq

We return to the classification of groups G of order pq, where p, q are primes with $p > q$, started in Prop. 4.7. By that proposition, if $q \nmid q-1$ then $G \cong C_{pq}$. So assume that $q \mid p-1$. Also by 4.7, G has a normal Sylow p-subgroup $P = \langle x \rangle \cong C_p$. Let $Q \in Syl_q(G)$, a subgroup of order q. Then $G = PQ$.

So we have $G = PQ$ with $P \lhd G$ and $P \cap Q = 1$. By Prop. 5.2, G is isomorphic to a semidirect product $C_p \rtimes_\iota C_q$, where $\iota : C_q \mapsto \mathrm{Aut}(C_p)$ is a homomorphism.

One possibility for ι is the trivial homomorphism, in which case $G \cong C_p \times C_q \cong C_{pq}$.

Let us now look for nontrivial homomorphisms ι. We know (problem on sheet 1) that $\mathrm{Aut}(C_p) \cong \mathbb{F}_p^*$. By a well-known result in number theory, $\mathbb{F}_p^*$ is a cyclic group (of order $p-1$). Hence it has a unique subgroup $\langle a \rangle$ of order q. A corresponding automorphism $\alpha \in \mathrm{Aut}(C_p)$ sends $x \mapsto x^a$, where $a^q \equiv 1 \bmod p$. So there is a nontrivial homomorphism $\iota : C_q \mapsto \mathrm{Aut}(C_p)$ sending $y \mapsto \alpha$, where $C_q = \langle y \rangle$. All other such homoms send $y^i \mapsto \alpha$ for some $i \in \{1, \ldots, q-1\}$, and hence are of the form $\iota \circ \beta$, where $\beta \in \mathrm{Aut}(C_q)$ sends $y^i \mapsto y$. Hence by Prop. 5.3, all such semidirect products are isomorphic to the group

$$C_p \rtimes_\iota C_q = \langle x, y : x^p = y^q = 1,\ yxy^{-1} = x^a \rangle. \tag{5.5}$$

We have now proved

Proposition 5.4 *Let p, q be primes with $p > q$.*

(i) *If $q \nmid p-1$ then $G \cong C_{pq}$.*

(ii) *If $q \mid p-1$ then up to ismorphism there are two groups of order pq, namely C_{pq} and the group defined by the presentation* (5.5).

We have seen in some of the above examples that non-split extensions can exist. However, there are quite a few results showing that under various hypotheses, all extensions split. Here is an elementary example of such a result.

Proposition 5.5 *Suppose N, H are finite abelian groups of coprime orders. Then every extension of N by H splits.*

Proof The is a question on Sheet 3.

Note This is a special case of a much more general result, the *Schur-Zassenhaus theorem*, which says that if N, H are *any* finite groups of coprime orders, then every extension of N by H splits. We'll prove this for *solvable* groups in the next chapter (see Thm. 6.10), but the general case is much harder.

Example Let G be an extension of $C_2 \times C_2$ by C_3. By Prop. 5.5, the extension splits, so by a previous example, $G \cong C_2 \times C_2 \times C_3$ or A_4.

6 Solvable groups

As mentioned in Chapter 2, the finite solvable groups are those for which all composition factors are cyclic groups of prime order. However this is not a convenient definition to work with, and we adopt the following definition.

Definition A finite group G is *solvable* if it has a series of subgroups

$$1 = N_0 \leq N_1 \leq \cdots \leq N_s = G,$$

where $N_i \lhd G$ and N_i/N_{i-1} is abelian, for all i.

Examples (1) Abelian groups are solvable.

(2) We show that any finite p-group G is solvable. The key fact is that $Z(G) \neq 1$ (provided $G \neq 1$) by Prop. 1.9. Define the series $1 = N_0 \leq N_1 \leq \cdots$ by $N_1 = Z(G)$, $N_2/N_1 = Z(G/N_1)$, and inductively, $N_i/N_{i-1} = Z(G/N_{i-1})$. Then $N_{i-1} < N_i$ by 1.9, so the series terminates at G; and the quotients N_i/N_{i-1} are abelian. Hence G is solvable.

(3) Let G be the subgroup consisting of all upper triangular matrices in $GL_n(q)$. We show that G is solvable. Let N be the subgroup of G of matrices with all diagonal entries 1. Then $N \lhd G$ and $G/N \cong (\mathbb{F}_q^\times)^n$, which is abelian. Also N is a p-group (where $q = p^a$), so has a series of normal subgroups N_i as in (2) above. Each N_i is characteristic in N, hence normal in G. Hence G is solvable.

The derived series

For a finite group G, recall the *derived subgroup* $G' = \langle [x, y] : x, y \in G \rangle$. Then define $G'' = (G')'$, and inductively,

$$G^{(i)} = (G^{(i-1)})'.$$

(So $G^{(1)} = G', G^{(2)} = G''$.) The series

$$G \geq G^{(1)} \geq G^{(2)} \geq \cdots$$

is called the *derived series* of G. We shall show that G is solvable iff its derived series terminates at 1. First we need a preliminary result.

Proposition 6.1 *If $\phi : G \mapsto H$ is a surjective homomorphism, then $\phi(G^{(i)}) = H^{(i)}$ for all i. Also $G^{(i)}$ char G for all i.*

Proof For $x, y \in G$,

$$[\phi(x), \phi(y)] = \phi(x)\phi(y)\phi(x)^{-1}\phi(y)^{-1} = \phi([x, y]).$$

Hence ϕ maps the set of commutators in G to the set of commutators in H. This map is surjective (since ϕ is), and hence $\phi(G') = H'$. Now repeating, we see that $\phi(G^{(i)}) = H^{(i)}$. The last assertion of the prop follows, taking $H = G$. $\square$

Proposition 6.2 *G is solvable iff $G^{(r)} = 1$ for some r.*

Proof Suppose $G^{(r)} = 1$, and consider the series

$$1 = G^{(r)} \leq G^{(r-1)} \leq \cdots \leq G^{(1)} \leq G.$$

Each $G^{(i)} \lhd G$ and each quotient $G^{(i)}/G^{(i+1)} = G^{(i)}/(G^{(i)})'$ is abelian. Hence G is solvable.

Conversely, suppose G is solvable. So there is a series

$$1 = N_0 \leq N_1 \leq \cdots \leq N_s = G,$$

where $N_i \lhd G$ and N_i/N_{i-1} is abelian, for all i. Then $N_i' \leq N_{i-1}$, so $G' \leq N_{s-1}$, $G'' \leq N_{s-1}' \leq N_{s-2}$, and so on, finishing with $G^{(s)} \leq N_0 = 1$. $\square$

Definition For a solvable group G, the *derived length* $dl(G)$ is defined by $dl(G) = \min\{r : G^{(r)} = 1\}$.

Proposition 6.3 (i) *Subgroups and quotient groups of solvable groups are solvable.*

(ii) *If $N \lhd G$, and N, G/N are both solvable, then G is solvable.*

Proof (i) Let G be solvable. If $H \leq G$ then $H' \leq G'$ and in general, $H^{(i)} \leq G^{(i)}$. Hence $H^{(i)} = 1$ for some i, so H is solvable.

Now let $N \lhd G$. By Prop. 6.1 applied to the natural map $\phi : G \mapsto G/N$, we have $(G/N)^{(i)} = \phi(G^{(i)})$ for all i, so $(G/N)^{(i)} = 1$ for some i. Hence G/N is solvable.

(ii) Since G/N is solvable, there exists r such that $(G/N)^{(r)} = \phi(G^{(r)}) = N$ (where ϕ is as above). Hence $G^{(r)} \leq N$. As N is solvable, $N^{(s)} = 1$ for some s. Then $G^{(r+s)} = 1$, so G is solvable. $\square$

We can now justify the original definition of solvability (in terms of composition factors).

Proposition 6.4 *Let G be a finite group, and let $1 = G_0 \lhd G_1 \lhd \cdots \lhd G_r = G$ be a composition series for G. Then G is solvable iff all the composition factors G_i/G_{i-1} are cyclic of prime order.*

Proof Suppose G is solvable. Then each quotient G_i/G_{i-1} is solvable, by Prop. 6.3(i). It remains to show that any solvable simple group is of prime order: this is easy, because if H is solvable simple, then H' is a proper normal subgroup of H, hence $H' = 1$; then H is abelian simple, so H has prime order (eg. by Sheet 1, Q1).

Conversely, suppose all the composition factors G_i/G_{i-1} are cyclic of prime order. Then G/G_{r-1} is abelian, so $G' \leq G_{r-1}$; next, G_{r-1}/G_{r-2} abelian implies that $G'' \leq G_{r-2}$. Continuing, we end up with $G^{(r)} = 1$, and so G is solvable. $\square$

Theory of solvable groups

Definition Let A be a finite abelian group. We say A is *elementary abelian* if there is a prime p such that $x^p = 1$ for all $x \in A$.

Proposition 6.5 *If A is elementary abelian, then $A \cong C_p \times \cdots \times C_p = (C_p)^k$ for some prime p.*

Proof By the classification of finite abelian groups, $A \cong C_{p_1^{a_1}} \times \cdots \times C_{p_k^{a_k}}$, where each p_i is prime. The condition $x^p = 1$ for all x implies that $p_i^{a_i} = p$ for all i. $\square$

Definition Let $N \lhd G$. We say N is a *minimal normal subgroup* of G if $N \neq 1$ and N contains no smaller nontrivial normal subgroup of G.

For example, V_4 is a minimal normal subgroup of S_4; and A_4 is not (as it contains V_4).

Proposition 6.6 *Let G be a finite group, and let N be a minimal normal subgroup of G. Suppose that N is solvable. Then N is elementary abelian.*

Proof As N is solvable, $N' < N$. Also N' char N, so $N' \lhd G$. As N is minimal normal, this implies $N' = 1$, so N is abelian. Let p be a prime divisor of $|N|$, and $A = \{x \in N : x^p = 1\}$. Then A is a nontrivial subgroup of N (as N is abelian), and is characteristic in N, hence normal in G. Hence $A = N$, completing the proof. $\square$

Definition For a finite group G, a *chief series* is a series

$$1 = N_0 \leq N_1 \leq \cdots \leq N_r = G,$$

where each $N_i \lhd G$, and each N_{i+1}/N_i is minimal normal in G/N_i. The quotients N_{i+1}/N_i are the *chief factors*.

We remark that there is a Jordan-Hölder type theorem about the uniqueness of the list of chief factors of a finite group, but we won't prove it here.

Example S_4 has a unique chief series $1 < V_4 < A_4 < S_4$. The chief factors are $C_2 \times C_2$, C_3 and C_2.

From Prop. 6.6 we deduce:

Corollary 6.7 *All chief factors of a finite solvable group are elementary abelan p-groups, for various primes p.*

Hall's Theorem

This is a vast generalisation of Sylow I that holds just for solvable groups. It concerns so-called *π-subgroups*, where π is a set of primes. We say a positive integer n is a *π-number* if n is divisible only by primes in π, and is a *π'-number* if it is divisible by no primes in π.

For example, 12 is a $\{2,3\}$-number and a $\{2,3,7\}$-number, and also a $\{5,7\}'$-number.

Definition A subgroup $H \leq G$ is a π-subgroup if $|H|$ is a π-number.

Theorem 6.8 (Hall's Theorem) *Let π be any set of primes, and G a finite solvable group. Write $|G| = nm$, where n is a π-number and m a π'-number. Then G has a subgroup of order n.*

Such a subgroup H is called a *Hall π-subgroup* of G. Note that $|H| = n$ and $|G : H| = m$, so $\gcd(|H|, |G : H|) = 1$. Note also that if π just consists of a single prime p, then H is a Sylow p-subgroup.

Remark Thm. 6.8 is an analogue of Sylow I – there are also analogues of Sylow III and IV: all Hall π-subgroups of a solvable group are conjugate; and any π-subgroup is contained in a Hall π-subgroup. We won't prove these here.

Examples (1) If G is abelian, then G has a unique Hall π-subgroup for any π: this can be defined as $G_\pi = \{g \in G : o(g) \text{ a } \pi\text{-number}\}$.

(2) Let G be a group of upper triangular matrices in $SL_2(p)$, as in Example (2) on p.24. So $G \cong \mathbb{F}_p^+ \rtimes \mathbb{F}_p^\times$, a solvable group. Let π be a set of primes.

If $p \notin \pi$, then G has a Hall π-subgroup $H_\pi \leq \mathbb{F}_p^\times$; this is not normal in G, so is not unique.

If $p \in \pi$, then G has a Hall π-subgroup $\mathbb{F}_p \rtimes H_{\pi\setminus p}$; this is normal in G, and unique.

(3) If G is non-solvable, then G may contain Hall π-subgroups for some sets π, but not for others. For example, A_5 (of order $60 = 2^2.3.5$) has a Hall $\{2,3\}$-subgroup, namely A_4; but it does not have a Hall $\{2,5\}$- or $\{3,5\}$-subgroup (these would have index 3 or 4 respectively, so cannot exist by Cor. 1.16).

For the proof of Theorem 6.8, we need two preliminary results, both very important. The first is called the "Frattini Argument" – the argument of the proof is a very typical application of the Sylow theorems.

Proposition 6.9 (Frattini Argument) *Let $N \lhd G$ and let $P \in Syl_p(N)$. Then $G = N_G(P)\,N$.*

Proof Let $g \in G$. Then $g^{-1}Pg \leq g^{-1}Ng = N$, so $g^{-1}Pg \in Syl_p(N)$. By Sylow IV, there exists $n \in N$ such that $g^{-1}Pg = n^{-1}Pn$. Then $ng^{-1}Pgn^{-1} = P$, so $gn^{-1} = x \in N_G(P)$, and so $g = xn \in N_G(P)\,N$. As $g \in G$ was arbitrary, it follows that $G = N_G(P)\,N$. $\square$

The next result is a generalisation of Proposition 5.5 to solvable groups – it is the solvable group case of the *Schur-Zassenhaus theorem.*

Theorem 6.10 *Let N and H be finite solvable groups of coprime orders. Then every extension of N by H splits.*

Proof Let G be an extension of N by H. So $N \lhd G$, $G/N \cong H$, and $\gcd(|N|, ||G/N|) = 1$. Also G is solvable by Prop. 6.3. The proof goes by induction on $|G|$. The result is trivial if $|G| = 1$ and also if $N = G$, so assume that $N < G$.

Let M/N be a minimal normal subgroup of G/N. By Prop. 6.6, M/N is a p-group for some prime p. Let $P \in Syl_p(M)$. Then $M = PN$.

Let $X = N_G(P)$. By Prop. 6.9,

$$G = XM = XPN = XN,$$

the last equality since $P \leq N_G(P) = X$.

Suppose now that $X < G$. We apply induction to the group X. Note that X is solvable, $N \cap X \lhd X$ and $X/N \cap X \cong XN/N = G/N$, so $|N \cap X|$ and $|X/N \cap X|$ are coprime, and hence the induction hypothesis tells us that this extension X splits. In other words there is a subgroup $K \leq X$ such that $K(N \cap X) = X$ and $K \cap (N \cap X) = 1$. Then

$$G = XN = K\,(N \cap X)\,N = KN,\ K \cap N = K \cap X \cap N = 1.$$

Hence G splits as an extension of N by H.

Now suppose that $X = G$. Since $X = N_G(P)$ this means that $P \lhd G$. In this case we apply induction to G/P. Note that $M/P \lhd G/P$ and $\gcd(|M/P|, |G/M|)$ divides $\gcd(|N|, |G/N|) = 1$, so the induction hypothesis gives a subgroup K/P of G/P such that

$$(M/P)\,(K/P) = G/P,\ (M/P) \cap (K/P) = 1.$$

This implies that

$$G = MK = NPK = NK \ \text{ (as } P \leq K), \text{ and } M \cap K = P.$$

Finally, we show $N \cap K = 1$. As p divides $|G/N|$, it does not divide $|N|$, and hence the fact that $N \cap K \leq M \cap K = P$ implies that $N \cap K = 1$. We now have $G = NK$ and $N \cap K = 1$, so the extension G splits and the proof by induction is complete. $\square$

Proof of Theorem 6.8

Let G be a finite solvable group and π a set of primes. We prove by induction that G has a Hall π-subgroup. The result is trivial if $|G| = 1$, so assume $|G| > 1$.

Let M be a minimal normal subgroup of G. By induction applied to the solvable group G/M, this group has a Hall π-subgroup H/M. So

- H/M is a π-group,
- $|(G/M) : (H/M)| = |G : H|$ is a π'-number.

Also by Prop. 6.6, M is a p-group for some prime p.

If $p \in \pi$ then H is a π-group, and hence H is a Hall π-subgroup of G, as required.

Now assume $p \notin \pi$. Then $\gcd(|M|, |H/M|) = 1$. Hence by Thm. 6.10, H splits as an extension of M, so there is a subgroup $K \leq H$ such that

$$H = KM, \ K \cap M = 1.$$

Then $|K| = |H/M|$ is a π-number, and $|G : K| = |G : H|\,|H : K| = |G : H|\,|M|$ is a π'-number. Hence K is a Hall π-subgroup, and the proof is complete. $\square$

7 Nilpotent groups

This is a special class of solvable groups, defined as follows.

Definition A finite group G is *nilpotent* if there is a series of subgroups

$$1 = G_0 \leq G_1 \leq \cdots \leq G_r = G,$$

where for all i,

$$G_i \triangleleft G \text{ and } G_{i+1}/G_i \leq Z(G/G_i). \tag{7.1}$$

Such a series is called a *central series* for G.

Remarks (1) Abelian groups are nilpotent (with central series $1 \leq G$).

(2) Nilpotent groups are solvable, since the condition $G_{i+1}/G_i \leq Z(G/G_i)$ implies that G_{i+1}/G_i is abelian.

The next result provides a huge source of nilpotent groups.

Proposition 7.1 *Every finite p-group (p prime) is nilpotent.*

Proof We use the basic fact that every nontrivial p-group has a nontrivial centre (Prop. 1.9). Let P be a nontrivial p-group, and define a series of subgroups $1 = P_0 < P_1 < P_2 \cdots$ as follows: define $P_1 = Z(P)$; then define P_2 to be the subgroup containing P_1 such that $P_2/P_1 = Z(P/P_1)$, and inductively define P_{i+1} to be the subgroup such that

$$P_{i+1}/P_i = Z(P/P_i).$$

By Prop. 1.9, this is a strictly increasing series, so it must terminate at $P_r = P$. By definition, it is therefore a central series for P. $\square$

What we have just defined is known as the *upper central series* for P. Here is the definition of this series in general.

Upper central series Let G be a finite group, and define $Z_0(G) = 1$, $Z_1(G) = Z(G)$, and inductively define $Z_{i+1}(G)$ by

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G)).$$

Then the series $1 = Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots$ is called the *upper central series* of G. It *is* a central series, as each $Z_i(G)$ is characteristic in G, and the centrality property (7.1) holds by the definition of $Z_{i+1}(G)$. We will prove in Thm. 7.2 below that G is nilpotent iff this series terminates at G (ie. iff there exists n such that $Z_n(G) = G$).

Next we define another important central series for any finite group:

Lower central series Let G be a finite group. For $H, K \subseteq G$, define

$$[H, K] = \langle [h, k] : h \in H, k \in K \rangle.$$

Note that $[H, K] = [K, H]$ (since $[k, h] = [h, k]^{-1}$).

Now define $\gamma_0(G) = G$, $\gamma_1(G) = [G, G] = G'$, and inductively,

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

Then the series

$$G = \gamma_0(G) \geq \gamma_1(G) \geq \gamma_2(G) \geq \cdots$$

is called the *lower central series* of G. It *is* a central series, as each $\gamma_i(G)$ is characteristic in G, and the centrality property $\gamma_i(G)/\gamma_{i+1}(G) \leq Z(G/\gamma_{i+1}(G))$ holds, since for $x \in \gamma_i(G)$, $g \in G$, we have

$$[x\gamma_{i+1}(G),\, g\gamma_{i+1}(G)] = [x,g]\gamma_{i+1}(G) = \gamma_{i+1}(G).$$

We will prove that G is nilpotent iff this series terminates at 1 (ie. iff there exists n such that $\gamma_n(G) = 1$).

Example Let $G = D_8 = \langle \rho, \sigma \rangle$. Then $Z(G) = G' = \langle \rho^2 \rangle$, so both the lower and upper central series are $1 < \langle \rho^2 \rangle < G$.

Theorem 7.2 *Let G be a finite group and let n be a positive integer. The following are equivalent:*

(i) $Z_n(G) = G$

(i) $\gamma_n(G) = 1$.

Moreover, G is nilpotent iff both these conditions hold for some n.

For the proof we need the next proposition.

Proposition 7.3 *Let G be a finite group, and $X, Y \leq G$.*

(i) $Y \leq N_G(X)$ *iff* $[X,Y] \leq X$.

(ii) *Suppose $Y \lhd G$ and $Y \leq X$. Then*

$$X/Y \leq Z(G/Y) \Leftrightarrow [X,G] \leq Y.$$

Proof (i) Suppose $Y \leq N_G(X)$. Then for $x \in X, y \in Y$, we have $[x,y] = xyx^{-1}y^{-1} \in X$, so $[X,Y] \leq X$. Conversely, if $[x,y] \in X$ for all $x \in X, y \in Y$, then we see that $yx^{-1}y^{-1} \in X$, and hence $Y \leq N_G(X)$.

(ii) For $x \in X$ we have

$$\begin{aligned} xY \in Z(G/Y) &\Leftrightarrow [xY,\, gY] = Y \ \ \forall g \in G \\ &\Leftrightarrow [x,g]Y = Y \ \ \forall g \in G \\ &\Leftrightarrow [x,g] \in Y \ \ \forall g \in G. \end{aligned}$$

Part (ii) follows. $\square$

Proof of Theorem 7.2

If conclusion (i) or (ii) holds, then G is nilpotent. Hence in this proof we can assume that G is nilpotent, and aim to show that (i) and (ii) hold for exactly the same non-empty set of positive integers n.

Let

$$1 = N_0 \leq \cdots \leq N_k = G \tag{7.2}$$

be a central series for G. Then by Prop. 7.3(ii), for each i we have

$$[N_{i+1}, G] \leq N_i.$$

Now $\gamma_0(G) = G = N_k$, so $\gamma_1(G) = [G, G] \leq [N_k, G] \leq N_{k-1}$, and inductively,

$$\gamma_i(G) = [\gamma_{i-1}(G), G] \leq [N_{k-i+1}, G] \leq N_{k-i}.$$

As $N_0 = 1$, we conclude that

$$\gamma_k(G) = 1.$$

Hence (ii) holds for $n = k$. It follows also that (i) $\Rightarrow$ (ii): for if $Z_n(G) = G$, we take the central series (7.2) with $N_i = Z_i(G)$ and $k = n$, and then by the above reasoning, we have $\gamma_n(G) = 1$.

Thus we have shown that (ii) holds with $n = k$, and that (i) $\Rightarrow$ (ii).

Resuming the proof, let's return to the arbitrary central series (7.2). We now show by induction that for all i, we have

$$N_i \leq Z_i(G). \tag{7.3}$$

This is true for $i = 0$ as both groups are 1. For convenience, write $Z_i = Z_i(G)$. Let $i \geq 1$ and assume that $N_{i-1} \leq Z_{i-1}$. Then by Prop. 7.3(ii), we have

$$[N_i, G] \leq N_{i-1} \leq Z_{i-1}.$$

Moreover, $[N_i Z_{i-1}, G] \leq Z_{i-1}$, since for $n \in N_i, z \in Z_{i-1}$ we have $[nz, g] = [n, zg]\,[z, g] \in [N_i, G]\, Z_{i-1} \leq Z_{i-1}$. Hence by Prop. 7.3 again,

$$N_i Z_{i-1}/Z_{i-1} \leq Z(G/Z_{i-1}) = Z_i/Z_{i-1},$$

showing that $N_i \leq Z_i$. Hence (7.3) is proved by induction.

It follows from (7.3) that $Z_k(G) = N_k = G$, and hence (i) holds with $n = k$. Also, (ii) $\Rightarrow$ (i): for if $\gamma_n(G) = 1$, we take the central series (7.2) with $N_i = \gamma_{n-i}(G)$ and $k = n$, and then by the above reasoning, we have $Z_n(G) = G$. This completes the proof of the theorem. $\square$

Definition For a nilpotent group G, the smallest integer n such that $Z_n(G) = G$ (or equivalently $\gamma_n(G) = 1$) is called that *nilpotence class* (or just the *class*) of G.

Examples (1) Abelian groups have class 1.

(2) A non-abelian group G has class 2 iff $G' \leq Z(G)$. Examples of such groups are D_8, Q_8 and the group of upper unitriangular matrices in $GL_3(p)$ (of order p^3).

Corollary 7.4 *Subgroups and quotient groups of nilpotent groups are nilpotent.*

Proof Let G be nilpotent, so that $\gamma_n(G) = 1$ for some n. If $H \leq G$ then also $\gamma_n(H) = 1$, so H is nilpotent.

Now let $N \lhd G$, and $\phi : G \mapsto G/N$ the canonical homom. As in the proof of Prop. 6.1, we see that $\phi(\gamma_i(G)) = \gamma_i(\phi(G))$ for all i, and hence $\gamma_n(\phi(G)) = 1$. So G/N is nilpotent. $\square$

Notice that in contrast to Prop. 6.3(ii) for solvable groups, it is not the case that N, G/N both nilpotent implies that G is nilpotent. For example $S_3 = C_3 \rtimes C_2$ is not nilpotent.

The next result is the basic structure theorem for finite nilpotent groups.

Theorem 7.5 *For a finite group G, the following conditions are equivalent:*

(i) *G is nilpotent.*

(ii) *For any $H < G$, we have $H < N_G(H)$.*

(iii) *Every maximal subgroup of G is normal.*

(iv) *Every Sylow subgroup of G is normal.*

(v) *$G \cong P_1 \times \cdots \times P_k$, where each P_i is a p_i-group and $p_1, \ldots, p_k$ are distinct primes.*

Proof **((i) ⇒ (ii))** Assume (i), and let $1 = N_0 \leq \cdots \leq N_k = G$ be a central series. Let $H < G$, and choose r maximal such that $N_r \leq H$ (so $r \geq 0$ and $r < k$). Now $N_{r+1}/N_r \leq Z(G/N_r)$, so by Prop. 7.3(ii), we have $[N_{r+1}.H] \leq N_r \leq H$. This implies that $N_{r+1} \leq N_G(H)$ by Prop. 7.3(i). Hence $H < N_G(H)$.

((ii) ⇒ (iii)) Assume (ii). Let M be a maximal subgroup of G. Then by (ii), $M < N_G(M)$, so $N_G(M) = G$ as M is maximal. Hence (iii) holds.

((iii) ⇒ (iv)) Assume (iii). Let $P \in Syl_p(G)$. Suppose $P \not\lhd G$, so $N_G(P) < G$. Then there is a maximal subgroup M of G containing $N_G(P)$. By (iii), $M \lhd G$. As $P \in Syl_p(M)$, the Frattini argument (Prop. 6.9) gives $G = N_G(P)\, M = M$, a contradiction. Hence $P \lhd G$.

((iv) ⇒ (v)) Assume (iv). Let $P_1, \ldots, P_k$ be the Sylow subgroups of G, and $|P_i| = p_i^{a_i}$ with p_i prime. As each $P_i \lhd G$, for $i \neq j$ we have $[P_i, P_j] \leq P_i \cap P_j = 1$. Hence $P_1 P_2 \cdots P_k$ is a subgroup of G of order $\prod p_i^{a_i} = |G|$. Hence $G = P_1 P_2 \cdots P_k$ and each element $g \in G$ has a unique expression $g = x_1 \cdots x_k$ with $x_i \in P_i$ for all i. It now follows that the map

$$\phi : \; g \mapsto (x_1, \ldots, x_k)$$

is an isomorphism $G \mapsto P_1 \times \cdots \times P_k$.

((v) ⇒ (i)) Assume (v). Each P_i is nilpotent, so $\gamma_{n_i}(P_i) = 1$ for some n_i. If $n = \max(n_i)$, then $\gamma_n(P_1 \times \cdots \times P_k) = 1$. Hence G is nilpotent. □

Solvable radical and Fitting subgroup

These will be the largest solvable and nilpotent normal subgroups of a finite group. To prove their existence we need:

Proposition 7.6 *Let G be a finite group with normal subgroups M and N. (So MN is also a normal subgroup of G.)*

(i) *If M, N are both solvable, so is MN.*

(ii) *If M, N are both nilpotent, so is MN.*

Proof (i) We have $MN/N \cong M/M \cap N$ which is solvable by Prop. 6.3(i). Hence MN is solvable by Prop. 6.3(ii).

(ii) This is much more tricky. Suppose $M, N \lhd G$ are both nilpotent. We shall prove that every Sylow subgroup of MN is normal, hence MN is nilpotent by Thm. 7.5.

Let p be a prime and $S \in Syl_p(MN)$. As $M \lhd MN$, we have $S \cap M \in Syl_p(M)$. Since M is nilpotent, $S \cap M$ is therefore the unique Sylow p-subgroup of M. Hence $S \cap M$ char $M \lhd MN$, and so $S \cap M \lhd MN$. Similarly $S \cap N \lhd MN$. We now observe that

$$|MN|_p = \frac{|M|_p |N|_p}{|M \cap N|_p} \leq \frac{|S \cap M|\,|S \cap N|}{|S \cap M \cap N|} = |(S \cap M)(S \cap N)| \leq |S|.$$

As $|MN|_p = |S|$, all the inequalities are equalities, and so $S = (S \cap M)(S \cap N)$. Both factors are normal in MN, and hence $S \lhd MN$, as required. $\square$

Corollary 7.7 *Every finite group has a unique largest solvable normal subgroup $R(G)$, and a unique largest nilpotent normal subgroup $F(G)$.*

Proof Choose $R \lhd G$, maximal subject to being solvable. If S is another solvable normal subgroup of G, then by Prop. 7.6, RS is a solvable normal subgroup containing R. By the maximal choice of R, it follows that $RS = R$, so $S \leq R$. The proof for the nilpotent case is identical. $\square$

Note that if G is solvable, then any minimal normal subgroup is abelian (hence nilpotent) by Prop. 6.6. Hence $F(G) \neq 1$ for (nontrivial) solvable groups G.

Examples The Fitting subgroups $F(S_3) = A_3$ and $F(S_4) = V_4$. There are further examples on Sheet 4.

The next result is a fundamental property of the Fitting subgroup of a solvable group.

Proposition 7.8 *If G is solvable, then $C_G(F(G)) \leq F(G)$. (Hence $C_G(F(G)) = Z(F(G))$.)*

Proof This is Q7 on Sheet 4. $\square$

The point is that G acts by conjugation on $F = F(G)$, giving a homom. $\pi : G \mapsto \mathrm{Aut}(F)$. The kernel of this homom. is $C_G(F)$, which by the prop. is $Z(F)$. Hence $G/Z(F)$ is isomorphic to a subgroup of $\mathrm{Aut}(F)$. This is often a useful basic piece of structural information about a solvable group G.

For example, if we know that G is solvable and $F = F(G) \cong (C_p)^n$ (p prime), then $F = Z(F)$ and $\mathrm{Aut}(F) \cong GL_n(p)$. So G is an extension of $(C_p)^n$ by a (solvable) subgroup of $GL_n(p)$.

8 The Frattini subgroup

Definition Let G be a finite group. The intersection of all the maximal subgroups of G is called the *Frattini* subgrop of G, denoted by $\Phi(G)$.

For example, $\Phi(C_2 \times C_2) = 1$, $\Phi(D_8) = \langle \rho^2 \rangle = Z(D_8)$.

Proposition 8.1 *Let $x \in \Phi(G)$. Then for any subset $S \subseteq G$,*

$$G = \langle S, x \rangle \Rightarrow G = \langle S \rangle. \tag{8.1}$$

Conversely, if $x \in G$ has property (8.1) *for all $S \subseteq G$, then $x \in \Phi(G)$.*

Proof Let $x \in \Phi(G)$, and suppose $S \subseteq G$ with $G = \langle S, x \rangle$. If $G \neq \langle S \rangle$, then there is a maximal subgroup M of G such that $\langle S \rangle \leq M$. But $x \in \Phi(G) \leq M$, so $G = \langle S, x \rangle \leq M$, a contradiction. Hence $G = \langle S \rangle$.

Conversely, suppose $x \in G$ has property (8.1). If $x \notin \Phi(G)$, then there is a maximal subgroup M of G such that $x \notin M$. Then $\langle M, x \rangle = G$, but $\langle M \rangle = M \neq G$, contradicting (8.1) (with $S = M$). Hence $x \in \Phi(G)$. $\square$

In light of property (8.1), we say that $\Phi(G)$ consists of the *non-generators* of G.

Proposition 8.2 *$\Phi(G)$ is a characteristic (hence normal) nilpotent subgroup of G.*

Proof Any automorphism of G permutes the set of maximal subgroups, hence stabilizes their intersection $\Phi(G)$, so $\Phi(G)$ is characteristic in G.

Now let p be a prime and $P \in Syl_p(\Phi(G))$. By the Frattini argument 6.9, we have $G = N_G(P)\,\Phi(G)$, and hence $G = N_G(P)$ by the non-generation property 8.1. So $P \lhd G$, hence certainly $P \lhd \Phi(G)$. We have now shown that every Sylow subgroup of $\Phi(G)$ is normal, and so $\Phi(G)$ is nilpotent by Theorem 7.5. $\square$

Notice that Prop. 8.2 implies that $\Phi(G) \leq F(G)$, the Fitting subgroup of G.

One major use of the Frattini subgroup is in the study of p-groups. We start with an elementary fact.

Proposition 8.3 *If P is an elementary abelian p-group then $\Phi(P) = 1$.*

Proof We have $P \cong (\mathbb{F}_p)^n$ for some n, and $\mathrm{Aut}(P) \cong GL_n(p)$. As it is a characteristic subgroup, $\Phi(P)$ is a subspace of $\mathbb{F}_p^n$ that is invariant under $GL_n(p)$. Since the only such invariant proper subspace is the zero subspace, we have $\Phi(P) = 1$. $\square$

Here is the main result.

Theorem 8.4 (Burnside Basis Theorem) *Let P be a p-group with $|P| = p^n$ and $|\Phi(P)| = p^{n-d}$, where $d \geq 1$.*

(i) *Then $P/\Phi(P) \cong (C_p)^d$, elementary abelian of order p^d.*

(ii) *If $N \lhd P$ and P/N is elementary abelian, then $\Phi(P) \leq N$; so $\Phi(P)$ is the unique normal subgroup of P that is minimal subject to having elementary abelian quotient.*

(iii) *Regard $P/\Phi(P)$ as the vector space $\mathbb{F}_p^d$, and denote by $x \mapsto \bar{x}$ the canonical map $P \mapsto P/\Phi(P)$. Then for $x_1, \ldots, x_d \in P$,*

$$P = \langle x_1, \ldots, x_d \rangle \Leftrightarrow \bar{x}_1, \ldots, \bar{x}_d \text{ is a basis of } \mathbb{F}_p^d.$$

Proof (i) If M is maximal in P then $M \lhd P$ by Thm 7.5, and $|P/M| = p$ (exercise). So $P' \leq M$ and also $x^p \in M$ for all $x \in P$. Hence $P' \leq \Phi(P)$ and $P/\Phi(P)$ is an abelian group such that $\bar{x}^p = 1$ for all elements $\bar{x}$, ie. $P/\Phi(P)$ is elementary abelian.

(ii) Suppose $N \lhd P$ and P/N is elementary abelian. Then $\Phi(P/N) = 1$ by Prop 8.3. The maximal subgroups of P/N are of the form M/N, where M is maximal in P and contains N. So the intersection of all these is N (as $\Phi(P/N) = N$, the identity element of P/N). This implies that $\Phi(P) \leq N$, as required.

(iii) Suppose $P = \langle x_1, \ldots, x_d \rangle$. Then $\bar{x}_1, \ldots, \bar{x}_d$ span $\mathbb{F}_p^d$, and so they form a basis.

Conversely, suppose $\bar{x}_1, \ldots, \bar{x}_d$ is a basis of $\mathbb{F}_p^d$. Then $P = \langle x_1, \ldots, x_d, \Phi(P) \rangle$, and so $P = \langle x_1, \ldots, x_d \rangle$ by Prop 8.1. $\square$

Corollary 8.5 *With notation as in the previous theorem, we have $d(P) = d$, where $d(P)$ is the minimal number of generators for P.*

The theorem makes it fairly routine to compute the Frattini subgroup of a given p-group in many cases. Here are some examples.

Examples What is $\Phi(D_8)$? Well, we know $d(D_8) = 2$, so $D_8/\Phi(D_8) \cong C_2^2$, and so $\Phi(D_8)$ has order 2, hence is equal to $\langle \rho^2 \rangle$. Similarly $\Phi(D_{2^n}) = \langle \rho^{2^{n-2}} \rangle$. Also $\Phi(Q_8) = Z(Q_8)$, of order 2. There are many more examples on Sheet 4.

The general theory of p-groups is rather difficult, as there are so many of them (eg. there are 10494213 groups of order 2^9 and 49487365422 of order 2^{10}; it is unknown how many there are of order 2^{11} or higher powers). But groups of order p^n for n small can be classified using some of the theory we have covered. We shall discuss this for the orders p^3 and $2^4 = 16$.

Groups of order p^3

We know the groups of order 2^3, and also the abelian groups of order p^3 (namely C_{p^3}, $C_{p^2} \times C_p$, $C_p \times C_p \times C_p$). So we focus on non-abelian groups with p odd.

In the proof of the theorem to follow, we shall need the following technical fact.

Proposition 8.6 *Let G be a group such that $G' \leq Z(G)$. Then for any $x, y \in G$ and $n \geq 1$,*

$$x^n y^n = (xy)^n [x^{-1}, y^{-1}]^{n(n-1)/2}.$$

Proof The proof is by induction on n, using the equation

$$xy = yx\,[x^{-1}, y^{-1}]. \tag{8.2}$$

Note that $[x^{-1}, y^{-1}] \in Z(G)$ since $G' \leq Z(G)$ by hypothesis.

Assume the result for n, and consider

$$\begin{aligned} (xy)^{n+1}[x^{-1}, y^{-1}]^{(n+1)n/2} &= (xy)^n [x^{-1}, y^{-1}]^{n(n-1)/2} xy\,[x^{-1}, y^{-1}]^n \\ &= x^n y^n xy\,[x^{-1}, y^{-1}]^n \text{ (by induction hyptothesis)} \\ &= x^{n+1} y^{n+1} \text{ (using (8.2) } n \text{ times). } \square \end{aligned}$$

Theorem 8.7 *Let p be an odd prime. Up to isomorphism, there are exactly two non-abelian groups of order p^3. These are:*

(1) $P_1 = \langle a, b, c : a^p = b^p = c^p = 1,\ [a,b] = c,\ [a,c] = [b,c] = 1\rangle \cong (C_p \times C_p) \rtimes C_p$;

(2) $P_2 = \langle a, b : a^{p^2} = b^p = 1,\ [a,b] = a^p\rangle \cong C_{p^2} \rtimes C_p$.

Note that P_1 is isomorphic to the group of upper unitriangular matrices in $GL_3(p)$, via the map

$$a \mapsto \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},\ b \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},\ c \mapsto \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Also the P_i can be seen as the claimed semidirect products by noting that $P_i = NH$ with $N \lhd P_i$, $N \cap H = 1$, where N, H are as follows:

$$\begin{aligned} i = 1:&\ N = \langle a, c\rangle \cong C_p \times C_p,\ H = \langle b\rangle \cong C_p \\ i = 2:&\ N = \langle a\rangle \cong C_{p^2},\ H = \langle b\rangle \cong C_p. \end{aligned}$$

Proof of Theorem 8.7

Let $|P| = p^3$ with P non-abelian. By Thm 8.4, $P/\Phi(P) \cong (C_p)^d$ where d is 1,2 or 3. If $d = 1$ then P is cyclic; and if $d = 3$ then $P \cong (C_p)^3$. These are abelian, so we must have $d = 2$. Hence

$$P = \langle a, b\rangle,\ \ \Phi(P) = \langle c\rangle$$

for some elements a, b, c. Also $\Phi(P) = Z(P) = P'$.

Case 1 Assume $a^p = b^p = 1$. Since $[a,b] \neq 1$ (as P is non-abelian), we can take $c = [a,b]$. This gives all the relations for the group P_1, so $P \cong P_1$ in this case.

Case 2 Now assume that a has order p^2, so $a^{p^2} = 1$, $a^p \neq 1$. We have $a^p \in \Phi(P)$, so $\Phi(P) = \langle a^p\rangle$.

(2a) Assume $b^p = 1$. Then we can take $[a,b] = a^p$ and we have the relations for the group P_2, so $P \cong P_2$ in this case.

(2b) Now assume b has order p^2. Replacing a, b by suitable powers, we can take $a^p = c$, $b^p = c^{-1}$ (where $\Phi(P) = \langle c\rangle$). Now by Prop 8.6,

$$1 = a^p b^p = (ab)^p [a^{-1}, b^{-1}]^{p(p-1)/2}.$$

As p is odd, it divides $p(p-1)/2$, so $[a^{-1}, b^{-1}]^{p(p-1)/2} = 1$ and hence $(ab)^p = 1$. Now replacing b by ab, we have $P = \langle a, b\rangle$ and $b^p = 1$, so we are back in case (2a), and the proof is complete. $\square$

Groups of order 16

There are actually 15 groups of order 16, and it would take a lot of effort to completely classify them, so here we will just do a partial classification – but using all the theory we have developed so far.

First we need to define some new classes of p-groups, Most of these will be defined as semidirect products, using the next result.

Proposition 8.8 *Let p be a prime and $n \geq 3$, and let $G = C_{p^n} = \langle x \rangle$. Then G has automorphisms α_i $(i = 1, 2, 3)$ of order p defined as follows:*

(i) $\alpha_1(x) = x^{p^{n-1}+1}$

(ii) $p = 2 : \ \alpha_2(x) = x^{-1}$

(iii) $p = 2 : \ \alpha_3(x) = x^{2^{n-1}-1}$.

Proof These are clearly automorphisms of G, so we just need to check they have order p. For α_1, we have $\alpha_1^p(x) = x^{(p^{n-1}+1)^p}$, and

$$(1 + p^{n-1})^p = 1 + p^n + \binom{p}{2} p^{2n-2} + \cdots \equiv 1 \bmod p^n.$$

Hence $\alpha_1^p(x) = x$, so α_1 has order p. Similar calculations apply for α_2, α_3. $\square$

Here are our new classes of p-groups. The first three are defined as semidirect products via homomorphisms $\iota_r : C_p \mapsto \mathrm{Aut}(C_{p^{n-1}})$ for $r = 1, 2, 3$, where $C_p = \langle x \rangle$ and ι_r sends $x \mapsto \alpha_r$ with α_r as in the previous prop.

Definition Four classes of groups of order p^n $(n \geq 3)$:

(1) $\mathrm{Mod}_{p^n} = C_{p^{n-1}} \rtimes_{\iota_1} C_p = \langle x, y : x^{p^{n-1}} = y^p = 1, \ y^{-1}xy = x^{p^{n-2}+1} \rangle$

(2) Dihedral $D_{2^n} = C_{2^{n-1}} \rtimes_{\iota_2} C_2 = \langle x, y : x^{2^{n-1}} = y^2 = 1, \ y^{-1}xy = x^{-1} \rangle$

(3) Semidihedral $SD_{2^n} = C_{2^{n-1}} \rtimes_{\iota_3} C_2 = \langle x, y : x^{2^{n-1}} = y^2 = 1, \ y^{-1}xy = x^{2^{n-2}-1} \rangle$

(4) Generalised quaternion $Q_{2^n} = \langle x, y : x^{2^{n-1}} = y^4 = 1, \ x^{2^{n-2}} = y^2, \ y^{-1}xy = x^{-1} \rangle$.

Note that Q_{2^n} is a non-split extension of $C_{2^{n-1}}$ by C_2. Note also that for p odd, Mod_{p^3} is isomorphic to the group P_2 in Theorem 8.7.

In fact, these four classes are *all* the non-abelian p-groups that have a cyclic subgroup of index p, but this is quite difficult to prove.

Classifying groups of order 16

As I said, we shall achieve a partial classification. Let $|P| = 16$. Using Thm 8.4 we divide the analysis into cases as follows:

I: $P/\Phi(P) \cong C_2$

IIa: $P/\Phi(P) \cong C_2^2$, $\Phi(P) \cong C_4$

IIb: $P/\Phi(P) \cong C_2^2$, $\Phi(P) \cong C_2^2$

III: $P/\Phi(P) \cong C_2^3$

IV: $P/\Phi(P) \cong C_2^4$.

In Case I, P is cyclic, and in Case IV, we have $P \cong C_2^4$. The other cases require substantial effort. We shall just deal with Case IIa:

Theorem 8.9 *Let P be as in Case IIa. Then P is isomorphic to one of the groups*

$$C_8 \times C_2, \ D_{16}, \ SD_{16}, \ Q_{16}, \ \mathrm{Mod}_{16}.$$

Proof We'll just give a sketch and leave some of the details at the end to Q4, Sheet 4. We have $P/\Phi(P) \cong C_2^2$ and $\Phi(P) = \langle a \rangle \cong C_4$.

The main step is to prove that there is an element $x \in P$ such that $x^2 = a$ (so x has order 8). We prove this in the following steps. Define

$$K = \langle x^2 : x \in P \rangle.$$

Then K is characteristic, hence normal in P. Every non-identity element of the quotient P/K has order 2, so P/K is abelian (standard Year 1 argument), hence is elementary abelian. Therefore by Thm 8.4(ii), we have $\Phi(P) \leq K$. On the other hand $P/\Phi(P)$ is elementary abelian, so $x^2 \in \Phi(P)$ for all $x \in P$, and hence $K \leq \Phi(P)$. We conclude that

$$K = \Phi(P) = \langle a \rangle.$$

If a set of elements generates C_4, then one of the elements must generate C_4. Hence it follows that one of the generators x^2 of K generates $\Phi(P)$. Hence there exists $x \in P$ such that $x^2 = a$, as claimed.

Thus x has order 8, so $\langle x \rangle \lhd P$. Hence if we pick any $y \in P \setminus \langle x \rangle$, then we have

$$P = \langle x, y \rangle,\ y^{-1}xy = x^s,\ y^2 = x^{2r}$$

for some r, s. Clearly $s = 1, 3, 5$ or 7. We now leave it as an exercise on Sheet 4 to check that these possibilities for s lead to the groups in the conclusion, as follows:

$s = 1$: $P \cong C_8 \times C_2$

$s = 3$: $r = 0$ or 2, $P \cong SD_{16}$ in both cases

$s = 5$: $r = 0, 1, 2$ or 3, $P \cong \mathrm{Mod}_{16}$ in all cases

$s = 7$: $r = 0$ or 2, $P \cong D_{16}$ or Q_{16}. $\square$

9 The Transfer Homomorphism

The theory of transfer is a method for constructing homomorphisms from a finite group G to abelian groups. As such, it can be a powerful tool for telling whether the commutator subgroup G' is proper in G.

Here is the definition. Let G be a finite group, and H a subgroup with $|G:H| = n$. Choose right coset representatives $y_1, \ldots, y_n$, so $G = \bigcup_1^n Hy_i$. For $x \in G$, there is a permutation $\sigma_x \in S_n$ such that $Hy_i x = Hy_{\sigma_x(i)}$ for all i. So there are elements $h_i(x) \in H$ such that

$$y_i x = h_i(x) y_{\sigma_x(i)} \quad (1 \le i \le n). \tag{9.1}$$

Definition The *transfer* map $\tau : G \mapsto H/H'$ is defined by

$$\tau(x) = \prod_{i=1}^{n} h_i(x) H'.$$

Example Let $G = D_6 = \langle \rho, \sigma \rangle$ and $H = \langle \sigma \rangle$. Choose coset reps e, ρ, ρ^2. Then $h_i(\rho) = e$ and $h_i(\sigma) = \sigma$ for all i, so $\tau(\rho) = e$, $\tau(\sigma) = \sigma$.

Proposition 9.1 (i) *The transfer map τ is a homomorphism $G \mapsto H/H'$.*

(ii) *τ is independent of the choice of coset representatives $y_1, \ldots, y_n$.*

Proof (i) Let $x_1, x_2 \in G$. From (9.1),

$$y_i x_1 x_2 = h_i(x_1 x_2) y_{\sigma_{x_1 x_2}(i)}.$$

On the other hand,

$$\begin{aligned} (y_i x_1) x_2 &= (h_i(x_1) y_{\sigma_{x_1}(i)}) x_2 \\ &= h_i(x_1) h_{\sigma_{x_1}(i)}(x_2) y_{\sigma_{x_1 x_2}(i)}. \end{aligned}$$

As H/H' is abelian, it follows that

$$\tau(x_1 x_2) = \prod_i h_i(x_1) h_{\sigma_{x_1}(i)}(x_2) H' = \tau(x_1)\tau(x_2).$$

(ii) Let $y_1', \ldots, y_n'$ be another set of coset reps, ordered so that $Hy_i' = Hy_i$ for all i. There are elements $z_i \in H$ such that $y_i' = z_i h_i$. Then by (9.1),

$$\begin{aligned} &y_i' x = h_i'(x) y'_{\sigma_x(i)} = h_i'(x) z_{\sigma_x(i)} y_{\sigma_x(i)}, \text{ and} \\ &y_i' x = z_i y_i x = z_i h_i(x) y_{\sigma_x(i)}. \end{aligned}$$

It follows that $h_i'(x) = z_i h_i(x) z_{\sigma_x(i)}^{-1}$. So

$$\prod_i h_i'(x)\, H' = (\prod z_i \prod h_i(x) \prod z_{\sigma_x(i)}^{-1})\, H' = \prod_i h_i(x)\, H',$$

and part (ii) follows. □

How to compute $\tau(x)$

Let $\tau : G \mapsto H/H'$ be the transfer homomorphism defined above. Let $\Omega = \{Hg : g \in G\}$, the set of right cosets of H in G, and consider the action of $x \in G$ on Ω sending

$Hg \mapsto Hgx$. (This is a right-action as opposed to the left-action defined in Section I of Chapter 1 (p.8), but it fits in with our notation for the transfer map.) Let the disjoint cycles of this action of x be as follows:

$$(Hx_1, Hx_1x, \ldots, Hx_1x^{r_1-1}) \cdots (Hx_t, Hx_tx, \ldots, Hx_tx^{r_t-1}),$$

where $Hx_ix^{r_i} = Hx_i$ for each $i = 1, \ldots, t$ and $\sum_1^t r_i = |G : H|$. Take the elements x_ix^j for $1 \leq i \leq t$, $1 \leq j \leq r_i$, as the coset representatives for H in G. Then from the definition of τ, we have

$$\tau(x) = (1 \cdots 1 \cdot x_1x^{r_1}x_1^{-1}) \cdots (1 \cdots 1 \cdot x_tx^{r_t}x_t^{-1})\, H'.$$

Hence we have proved:

Proposition 9.2 *For $x \in G$, we have $\tau(x) = (\prod_{i=1}^t x_ix^{r_i}x_i^{-1})H'$, where*

- $\sum_1^t r_i = |G : H|$,
- $x_ix^{r_i}x_i^{-1} \in H$ *for each* i,
- *each r_i divides $o(x)$, the order of x.*

Corollary 9.3 *Let $|G/Z(G)| = m$, and let $\tau : G \mapsto Z(G)$ be the transfer. Then $\tau(x) = x^m$ for all $x \in G$.*

Proof By Prop 9.2, $\tau(x) = \prod_{i=1}^t x_ix^{r_i}x_i^{-1}$, where $x_ix^{r_i}x_i^{-1} \in Z(G)$, hence is equal to x^{r_i}. So $\tau(x) = \prod_1^t x^{r_i} = x^m$. $\square$

In our main applications of transfer, we shall consider the transfer homomorphism $\tau : G \mapsto P/P'$, where P is a Sylow subgroup of G. First, a definition:

Definition (1) For $H \leq G$ and $x, y \in H$, we write $x \sim^H y$ if x and y are H-conjugate (ie. there exists $h \in H$ such that $y = hxh^{-1}$). Note that $x \sim^H y \Rightarrow x \sim^G y$, but the converse is not necessarily true.

(2) We say that a subgroup H of G *has no fusion in* G if, for any $x, y \in H$,

$$x \sim^G y \Rightarrow x \sim^H y.$$

In general, the *fusion pattern* of H is the equivalence relation on H defined by $x \sim y$ iff $x \sim^G y$. A measure of this is provided by the *focal subgroup*, defined below.

Example Let $G = A_4$. The subgroup $P_3 = \langle (1\,2\,3) \rangle \in Syl_3(G)$ has no fusion in G. However the subgroup $P_2 = V_4 \in Syl_2(G)$ does have fusion in G, since for $x, y \in P_2 \setminus 1$ with $x \neq y$, we have $x \sim^G y$ but $x \not\sim^{P_2} y$.

Definition For $P \leq G$, the *focal subgroup* of P in G is

$$F_G(P) = \langle xy^{-1} : x, y \in P,\, x \sim^G y \rangle.$$

Proposition 9.4 *For $P \leq G$, the following hold.*

(i) *We have $P' \leq F_G(P) \leq P \cap G'$.*

(ii) *If P has no fusion in G, then $F_G(P) = P'$.*

Proof (i) For $x \in P$, $g \in G$ and $y = gxg^{-1}$,

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

Taking $g \in P$, we see that $P' \leq F_G(P)$. Also $F_G(P) \leq G'$, proving part (i).

(ii) If P has no fusion in G, then $F_G(P) = \langle xy^{-1} : x, y \in P,\ x \sim^P y \rangle = P'$. $\square$

Example (1) Let $G = A_4$, and let P_3, P_2 be the subgroups defined in the previous example. Then $F_G(P_3) = P_3' = 1$, while $F_G(P_2) = P_2$.

(2) Now let $G = A_5$, and $P_5 = \langle x \rangle \in Syl_5(G)$, where $x = (12345)$. Note that $x \sim^G x^{-1}$, so P_5 has fusion in G and $F_G(P_5)$ contains x^2. Hence $F_G(P_5) = P_5$.

Theorem 9.5 (Focal subgroup theorem) *Let $P \in Syl_p(G)$, and let $\tau : G \mapsto P/P'$ be the transfer homomorphism. Then*

$$F_G(P) = P \cap G' = P \cap \mathrm{Ker}(\tau).$$

Proof We know that $F_G(P) \leq P \cap G'$ by Prop 9.4, and also $G' \leq \mathrm{Ker}(\tau)$ since $G/\mathrm{Ker}(\tau) \cong \mathrm{Im}(\tau)$ is abelian. Hence

$$F_G(P) \leq P \cap G' \leq P \cap \mathrm{Ker}(\tau).$$

So the prove the theorem, it is enough to show that

$$P \cap \mathrm{Ker}(\tau) \leq F_G(P). \tag{9.2}$$

Let $x \in P \cap \mathrm{Ker}(\tau)$. By Prop 9.2,

$$\tau(x) = (\prod_{i=1}^{t} x_i x^{r_i} x_i^{-1})P',$$

where $\sum_1^t r_i = n = |G : P|$ and $x_i x^{r_i} x_i^{-1} \in P$ for each i. Noting that $x^{-r_i} x_i x^{r_i} x_i^{-1} \in F_G(P)$, it follows that

$$\begin{aligned} \tau(x) &= x^n (\textstyle\prod_{i=1}^{t} x^{-r_i} x_i x^{r_i} x_i^{-1}) P' \\ &= x^n f P', \text{ where } f \in F_G(P). \end{aligned}$$

As $x \in \mathrm{Ker}(\tau)$, we have $\tau(x) = P'$, and hence $x^n f \in P'$. By Prop 9.4, $P' \leq F_G(P)$, so $x^n \in F_G(P)$. Now $n = |G : P|$ is coprime to p, whereas $x \in P$ has order a power of p, so $\langle x^n \rangle = \langle x \rangle$. Hence $x \in F_G(P)$. Thus (9.2) is proved, and the proof of the theorem is complete. $\square$

Corollary 9.6 *Suppose $P \in Syl_p(G)$ has no fusion in G. Then $P \cap G' = P'$.*

Proof By Prop 9.4(ii), $F_G(P) = P'$. Hence $P' = P \cap G'$ by Thm 9.5. $\square$

Remark The corollary implies that if $P \in Syl_p(G)$ is nontrivial and has no fusion, then $G' < G$ (since $P' < P$); in particular, G is not simple (unless it is C_p). This is a nice "local-to-global" result – showing how *local* information (about fusion properties of a Sylow p-subgroup) can lead to *global* information (about the structure of the whole group G).

The next theorem is a famous local-to-global result, proved by Burnside in 1900.

Burnside's Transfer Theorem

Before stating the theorem, here is an elementary but basic fact about normalizers of subgroups.

Proposition 9.7 *Let $H \leq G$. Then there is a homomorphism $\pi : N_G(H) \mapsto \mathrm{Aut}(H)$ such that $\mathrm{Ker}(\pi) = C_G(H)$. (So $N_G(H)/C_G(H) \cong \mathrm{Im}(\pi) \leq \mathrm{Aut}(H)$.)*

Proof Let $N = N_G(H)$. For $n \in N$ we have $nHn^{-1} = H$, so we can define $\pi(n) : H \mapsto H$ by

$$\pi(n) : h \mapsto nhn^{-1} \quad \forall h \in H.$$

Then $\pi(n) \in \mathrm{Aut}(H)$, and $\pi : N \mapsto \mathrm{Aut}(H)$ is a homomorphism (check). Finally,

$$n \in \mathrm{Ker}(\pi) \Leftrightarrow \pi(n) = \mathrm{id} \Leftrightarrow nhn^{-1} = h \; \forall h \in H \Leftrightarrow n \in C_G(H).$$

So $\mathrm{Ker}(\pi) = C_G(H)$. $\square$

Example Let $G = A_5$ and $V_4 = \langle (12)(34), (13)(24) \rangle \leq G$. Then $N_G(V_4) = A_4$ and $C_G(V_4) = V_4$. So $N_G(V_4)/C_G(V_4) \cong C_3 \leq \mathrm{Aut}(V_4)$.

Theorem 9.8 (Burnside's Transfer Theorem) . *Let $P \in Syl_p(G)$, and suppose that $P \leq Z(N_G(P))$. Then $\exists N \lhd G$ such that $G = PN$ and $P \cap N = 1$.*

A normal subgroup N satisfying the conclusion of the theorem is called a *normal p-complement* in G. Note that $|G| = |P|\,|N|$, so N is a p'-subgroup.

What does the hypothesis $P \leq Z(N_G(P))$ in the theorem mean? Well, for a start, the centre of any group is abelian, so it means that the Sylow p-subgroup P is abelian. Another way to say this is that $P \leq C_G(P)$. Also, $P \leq Z(N_G(P))$ implies that $N_G(P)$ centralizes P, so that $N_G(P) \leq C_G(P)$. So the hypothesis $P \leq Z(N_G(P))$ can be rewritten as

$$P \leq C_G(P) = N_G(P).$$

Note that this means the homomorphism $\pi : N_G(P) \mapsto \mathrm{Aut}(P)$ of Prop 9.7 is trivial.

Examples (1) If $G = A_4$ and $P = P_3 = \langle (123) \rangle \in Syl_3(G)$, then $P = C_G(P) = N_G(P)$.

(2) In general, if $G = PN$, where P is an abelian p-group, N is a p'-group, and $N \lhd G$, then $P \in Syl_p(G)$ and $P \leq Z(N_G(P))$. (Qn on Sheet 5.)

For the proof of Burnside's theorem, we need the following result.

Proposition 9.9 *Let $P \in Syl_p(G)$. Then for any $x, y \in C_G(P)$,*

$$x \sim^G y \Rightarrow x \sim^{N_G(P)} y.$$

Proof Let $x, y \in C_G(P)$. Then $P \leq C_G(x) \cap C_G(y)$, so P is a Sylow p-subgroup of both $C_G(x)$ and $C_G(y)$. Assume that $x \sim^G y$. So $y = gxg^{-1} = {}^g x$ for some $g \in G$. Then

$$P \leq C_G(x) \Rightarrow {}^g P \leq C_G({}^g x) = C_G(y).$$

Hence P and ${}^g P$ are Sylow p-subgroups of $C_G(y)$. By Sylow IV (Thm 4.4), there exists $c \in C_G(y)$ such that $P = {}^{cg}P$. Then $cg \in N_G(P)$ and ${}^{cg}x = {}^c y = y$. Hence $x \sim^{N_G(P)} y$. $\square$

Proof of Burnside's theorem 8.4

Assume that $P \in Syl_p(G)$ and $P \leq Z(N_G(P))$, so that $P \leq C_G(P) = N_G(P)$.

Claim We have $F_G(P) = 1$.

To prove this, recall that $F_G(P) = \langle xy^{-1} : x, y \in P, x \sim^G y \rangle$. Let $x, y \in P$ with $x \sim^G y$. Then by Prop 9.9, we have $x \sim^{N_G(P)} y$. So $y = nxn^{-1}$ for some $n \in N_G(P)$. But $N_G(P) = C_G(P)$, so $n \in C_G(P)$, so $nxn^{-1} = x$. Hence $y = x$ and $xy^{-1} = 1$. This proves the Claim.

Let $\tau : G \mapsto P$ be the transfer homomorphism. By the Claim and Theorem 9.5,

$$P \cap \mathrm{Ker}(\tau) = F_G(P) = 1.$$

Let $N = \mathrm{Ker}(\tau)$. Then $P \cap N = 1$, so $|PN| = |P|\,|N|$, and so N is a p'-group. Also $G/N \cong \mathrm{Im}(\tau) \leq P$, so G/N is a p-group. It follows that $G = PN$ and $P \cap N = 1$. This completes the proof of the theorem. $\square$

Some applications

We give two applications of Burnside's transfer theorem. The first is an addition to the methods of "Sylow arithmetic" given in Chapter 4. We illustrate with an example:

Example If $|G| = 12100 = 2^2 3^2 5^2$, then G is not simple.

Proof Assume G is simple. Then $n_{11}(G) \equiv 1 \bmod 11$, divides $|G|$ and is not equal to 1, so $n_{11}(G) = 100$. Let $P \in Syl_{11}(G)$. Then

$$n_{11}(G) = |G : N_G(P)| = 100 = |G : P|.$$

Hence $P = N_G(P)$. Also $|P| = 11^2$, so P is abelian. Hence $P \leq C_G(P) = N_G(P)$. Then Burnside's theorem implies that G has a normal 11-complement, so G is not simple, a contradiction. $\square$

Our second application is the following result.

Proposition 9.10 *Suppose all Sylow subgroups of G (for all primes) are cyclic. Then G is solvable.*

Proof The proof goes by induction on $|G|$. The result is trivial for $|G| = 1$, so assume $|G| > 1$.

Let p be the smallest prime divisor of $|G|$, and let $P \in Syl_p(G)$. By Prop 9.7, $N_G(P)/C_G(P)$ is isomorphic to a subgroup of $\mathrm{Aut}(P)$. Also P is cyclic, hence abelian, so $P \leq C_G(P)$, and so $N_G(P)/C_G(P)$ is a p'-group.

Now P is cyclic, say $P \cong C_{p^a}$. By a question on Sheet 1, $\mathrm{Aut}(C_{p^a})$ has order $\phi(p^a) = p^{a-1}(p-1)$. This is divisible by no prime greater than p. Since $N_G(P)/C_G(P)$ is a p'-subgroup of $\mathrm{Aut}(P)$ and p is the smallest prime divisor of $|G|$, it follows that $N_G(P)/C_G(P) = 1$. Hence $P \leq C_G(P) = N_G(P)$.

By Burnside's theorem 8.4, there exists $N \lhd G$ such that $G = PN$ and $N \cap P = 1$. The Sylow subgroups of N are Sylow subgroups of G, hence are cyclic, and so by induction, N is solvable. As $G/N \cong P$ is also solvable, G is solvable by Prop 6.3(ii). $\square$

That's the end of the course. Hope you enjoyed it!