Group Theory Notes

Francesco N. Chotuck

Abstract

This is the Imperial College London postgraduate module MATH70036 Group Theory, instructed by Professor Martin Liebeck.

Contents

1 Basics

Note 1.1. In this section, we review fundamental concepts of group theory (without proofs). Any new concepts will be discussed in greater detail and accompanied by proofs.

Remark 1.2. The following will be notation that will be used throughout the course.

- For a group G the identity element will be denoted by 1 or 1_G.
- The trivial group is 1.
- A subgroup H of G is denoted by $H \leq G$.
- A subset $H \subseteq G$.

Definition 1.3. Let a and b be two integers. We say that b **divides** a if there exists an integer q such that $a = qb$. If b divides a, we write $b \mid a$.

Theorem 1.4

Some basic properties of divisibility, let $a, b, c \in \mathbb{Z}$:

1. If $a \mid b$ and $b \mid c$, then $a \mid c$.
2. If $a \mid b$ and $a \mid c$ then $a \mid (bx + cy)$ for all $x, y \in \mathbb{Z}$.
3. If $a \mid 1$ then $a = \pm 1$.
4. If $a \mid b$ and $b \mid a$ then $a = \pm b$.
5. Suppose $c \neq 0$ then, $a \mid b$ if and only if $ac \mid bc$.

1.1 Recollections and useful facts

Theorem 1.5

If G is a group with $|G| \leq 5$, then G is Abelian.

Theorem 1.6

Let G be a group. Suppose $g \in G$:

1. if g has infinite order, then $g^n = 1 \iff n = 0$;
2. if g has infinite order, then $g^m = g^n \iff m = n$;
3. if g has finite order d, then $g^n = 1 \iff d \mid n$;
4. if g has finite order d, then $g^m = g^n \iff m \equiv n \pmod{d}$.

Proposition 1.7 (Subgroup test [2, Theorem 2.2.])
A subset S of a group G is a subgroup if and only if $1 \in S$ and $s, t \in S$ imply $st^{-1} \in S$.

Theorem 1.8 ([2, Theorem 2.5.])**.** The intersection of any family of subgroups of a group G is again a subgroup of G.

1.1.1 Lagrange's theorem

Definition 1.9. If S is a subgroup of G and if $g \in G$ then a **right coset** of S in G is the subset of G

$$Sg = \{sg : s \in S\}$$

(a **left coset** is $gS = \{gs : s \in S\}$). One calls g a **representative** of the coset.

Lemma 1.10 ([2, Lemma 2.8.])**.** If $S \leq G$, then $Sa = Sb$ if and only if $ab^{-1} \in S$ ($aS = bS$ if and only if $b^{-1}a \in S$).

Theorem 1.11 ([2, Theorem 2.9.])
If $S \leq G$, then any two right (or any two left) cosets of S in G are either identical or disjoint.

Remark 1.12. From this theorem it follows that cosets partition the group.

Definition 1.13. If $S \leq G$, then the **index** of S in G, denoted by $|G : S|$ is the number of right (or left) cosets of S in G.

Proposition 1.14 ([2, Exercise 2.10.])**.** If G is a finite group and $K \leq H \leq G$, then

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

Theorem 1.15 (Lagrange [2, Theorem 2.11.])
If G is a finite group and $S \leq G$, then $|S|$ divides $|G|$ and

$$|G : S| = \frac{|G|}{|S|}.$$

Corollary 1.16 ([2, Corollary 2.12.])**.** If G is a finite group and $g \in G$, then the order of g divides $|G|$.

Corollary 1.17 ([2, Corollary 2.13])**.** If p is a prime and $|G| = p$, then G is a cyclic group.

Corollary 1.18 (Fermat [2, Corollary 2.14.])
If p is a prime and $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$.

Corollary 1.19. Suppose that $|G| = n$ and $g \in G$, then $g^n = 1$.

Corollary 1.20. If $|G|$ is prime, then G has a no proper subgroup.

1.2 Permutation/Symmetric groups

Definition 1.21. If X is a non-empty set, a **permutation** of X is a bijection $\alpha : X \to X$.

Definition 1.22. The **permutation/symmetric group** of X, denoted by $\mathrm{Sym}(X)$, is defined to be the group of all permutation of X. The group multiplication being the composition of functions.

Remark 1.23. For $X = \{1, 2, \ldots, n\}$ we write S_n for $\mathrm{Sym}(X)$.

Theorem 1.24 ([2, Exercise 1.28.])
If $\alpha = (1\ 2\ \ldots\ r-1\ r)$, then $\alpha^{-1} = (r\ r-1\ \ldots\ 2\ 1)$.

Proposition 1.25. The group S_n has order $n!$.

Proposition 1.26. Suppose that $a_1, \ldots, a_n \in \{1, 2, \ldots, n\}$ are distinct and let $\alpha = (a_1\ \ldots\ a_n)$ then α has order n.

Definition 1.27. A 2-cycle is called a **transposition**.

Theorem 1.28 ([2, Exercise 1.5.])
If $1 \leq r \leq n$, then there are

$$\frac{1}{r}[n(n-1)\cdots(n-r+1)]$$

r-cycles in S_n.

Theorem 1.29 ([2, Theorem 1.1.])**.** Every permutation $\alpha \in S_n$ is either a cycle or a product of disjoint cycles.

Theorem 1.30 ([2, Theorem 1.3.])**.** Every permutation $\alpha \in S_n$ is a product of transpositions.

Proof. By the theorem above it suffices to factor cycles, and

$$(1\ 2\ \ldots\ r) = (1\ r)(1\ r-1)\cdots(1\ 2).$$

□

Definition 1.31. A permutation $\alpha \in S_n$ is **even** if it is a product of an even number of transpositions; otherwise, α is odd.

Lemma 1.32 ([2, Lemma 1.4.])**.** If $k, l \geq 0$, then

$$(a\ b)(a\ c_1\ \ldots\ c_k\ b\ d_1\ \ldots,\ d_l) = (a\ c_1\ \ldots\ c_k)(b\ d_1\ \ldots,\ d_l)$$

and

$$(a\ b)(a\ c_1\ \ldots\ c_k)(b\ d_1\ \ldots,\ d_l) = (a\ c_1\ \ldots\ c_k\ b\ d_1\ \ldots,\ d_l)$$

Proposition 1.33 ([2, Exercise 1.19.])
An r-cycle is an even permutation if and only if r is odd.

Proposition 1.34 ([2, Exercise 2.9.])
The group S_n is generated by:

- $(1\ 2), (1\ 3), \ldots, (1\ n)$;
- $(1\ 2), (2\ 3), \ldots, (i\ i+1), \ldots, (n-1\ n)$;
- $(1\ 2)$ and $(1\ 2\ \ldots\ n)$.

Proposition 1.35. The set of all even permutations, denoted by A_n, is a subgroup of S_n with order $\frac{n!}{2}$.

Definition 1.36. The group A_n is called the **alternating group** on n letters.

Proposition 1.37 ([2, Exercise 2.7.])
If $n > 2$, then A_n is generated by all the 3-cycles.

Remark 1.38. We can write $(ij)(jk) = (ijk)$ and $(ij)(kl) = (ijk)(jkl)$.

1.3 Cyclic groups

Theorem 1.39. For each $n \in \mathbb{N}$ there exists a cyclic group C_n.

Proof. Take $C_n = \{z \in \mathbb{C} : z^n = 1\}$. □

Theorem 1.40. There exists an infinite cyclic group.

Proof. This group is $(\mathbb{Z}, +)$. □

Theorem 1.41
Every cyclic group is isomorphic to C_n or $\mathbb{Z}$.

Example 1.42. The additive group of integers modulo n, which we denote by $\mathbb{Z}_n$ (or $\mathbb{Z}/n$, $\mathbb{Z}/n\mathbb{Z}$) is isomorphic to C_n.

Lemma 1.43 ([2, Lemma 2.15.])
If G is a cyclic group of order n, then there exists a unique subgroup of order d for every divisor d of n.

Example 1.44. Let $G = C_{12} = \{0, 1, \ldots, 11\}$, a cyclic group of order 12 generated by $g = 1$. For each divisor of 12, there is a unique subgroup:

- $C_1 = \{0\}$,
- $C_2 = \{0, 6\}$,
- $C_3 = \{0, 4, 8\}$,
- $C_4 = \{0, 3, 6, 9\}$,
- $C_6 = \{0, 2, 4, 6, 8, 10\}$,
- $C_{12} = G$

Theorem 1.45 ([2, Theorem 2.17.])
A group G of order n is cyclic if and only if, for each divisor d of n, there is at most one cyclic subgroup of G having order d.

Theorem 1.46 ([2, Theorem 2.19.])
Let p be a prime. A group of order p^n is cyclic if and only if it is an Abelian group having a unique subgroup of order p.

Proposition 1.47 ([2, Exercise 2.18.])**.** Every subgroup of a cyclic group is cyclic.

Definition 1.48. The **Euler ϕ-function** is defined as follows:

$$\phi(n) = \begin{cases} 1 & \text{if } n = 1 \\ |\{k : 1 \leq k \leq n \text{ and } \gcd(k, n) = 1\}| & \text{if } n > 1. \end{cases}$$

Note 1.49. This function counts how many numbers are coprime to n.

Proposition 1.50 ([2, Exercise 2.22.])**.** We have the following:

1. if p is prime, then $\phi(p^k) = p^k - p^{k-1}$;
2. if the distinct prime divisors of n are $p_1, \ldots, p_i$ then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_i}\right).$$

Proposition 1.51 ([2, Exercise 2.20.])
If $G = \langle g \rangle$ is cyclic of order n, then a^k is also a generator of G if and only if $\gcd(k, n) = 1$. Furthermore, the number of generators of G is $\phi(n)$.

1.4 Dihedral group

Definition 1.52. The **dihedral group** D_{2n} is defined to be the symmetry group of a regular n-sided polygon. It has $2n$ elements:

- n rotations $1, \rho, \ldots, \rho^{n-1}$ (where ρ is the clockwise rotation by $\frac{2\pi}{n}$);
- n reflections, σ.

Proposition 1.53

If σ is one of the reflections then all the reflections can be written as $\sigma, \sigma\rho, \ldots, \sigma\rho^{n-1}$.

Corollary 1.54. If $H = \langle \rho \rangle$ then $D_{2n} = H \cup \sigma H$.

Theorem 1.55

We can write

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

Remark 1.56. To remember the last relation, think of 'pop-o' for $\rho\sigma\rho = \sigma$.

Exam Questions 1.57 (Q1(c) Exam 2016)

For a positive integer n, define $\tau(n)$ to be the number of positive integer divisors of n. Define $\sigma(n)$ to be the sum of the positive integer divisors of n. Show that the number of distinct subgroups of D_{2n} is $\tau(n) + \sigma(n)$.

Solution. Let d be a divisor of n. Then N has a unique subgroup K_d of order d. Let H be a subgroup of D_{2n} whose intersection with N is K_d. Then either $H = K_d$, or else $H = K_d \cup K_d x$ for some reflection x. Furthermore, if x is any reflection, then $K_d \cup K_d x$ is a subgroup of D_{2n}. Any such subgroup contains d reflections, and there are n/d reflections in D_{2n}, hence there are n/d subgroups of this form. It follows that the number of subgroups of D_{2n} is

$$\sum_{d|n} 1 + n/d = \sum_{d|n} 1 + d = \tau(n) + \sigma(n)$$

as required.

1.5 Quaternion group

Definition 1.58. The **quaternion group**, Q_8, is a group of order 8 which is generated by the two matrices

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

Theorem 1.59

A presentation of it would be

$$Q_8 = \langle A, B \mid A^4 = 1, A^2 = B^2, BA = A^{-1}B \rangle.$$

1.6 Homomorphism

Theorem 1.60 ([2, Exercise 2.44.])

A homomorphism $\phi : G \to H$ is an injection if and only if $\ker \phi = 1$.

Definition 1.61. If S and T are non-empty subsets of a group G, then

$$ST = \{st : s \in S \text{ and } t \in T\}.$$

Theorem 1.62 (Product formula [2, Theorem 2.20.])**.** If S and T are subgroups of a finite group G, then

$$|ST|\,|S \cap T| = |S|\,|T|.$$

Remark 1.63. The subset ST need not be a subgroup.

1.6.1 Normal subgroups

Definition 1.64. A subgroup $K \leq G$ is a **normal subgroup**, denoted by $K \triangleleft G$, if $gKg^{-1} = K$ for every $g \in G$.

Proposition 1.65. The kernel of a homomorphism $\phi : G \to H$ is a normal subgroup of G.

Definition 1.66. For $x, y \in G$, we say they are **conjugate** if $y = gxg^{-1}$ for some $g \in G$.

Example 1.67. If $\mathbb{F}$ is a field, then the matrices $A, B \in \mathrm{GL}_n(\mathbb{F})$ are conjugate if and only if they are similar.

Proposition 1.68

Some results.

1. If $S \leq G$ and $|G : S| = 2$ then $S \triangleleft G$ [2, Exercise 2.30.].
2. If $H \leq G$, then $H \triangleleft G$ if and only if, for all $x, y \in G$, $xy \in H$ if and only if $yx \in H$ [2, Exercise 2.32.].
3. If $K \leq H \leq G$ and $K \triangleleft G$, then $K \triangleleft H$ [2, Exercise 2.33.].
4. The intersection of any family of normal subgroups of a group G is itself a normal subgroup of G [2, Exercise 2.37.].

Example 1.69
Key example of normal subgroups.

- $\mathrm{SL}_n(\mathbb{F}) \triangleleft \mathrm{GL}_n(\mathbb{F})$ for every $n \geq 1$ and every field $\mathbb{F}$ [2, Exercise 2.35.].
- $A_n \triangleleft S_n$ for every n [2, Exercise 2.36.].
- $V_4 \triangleleft S_4$ [2, Exercise 2.45.].

Definition 1.70. Let G be a group, the **centre** of G is

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

Proposition 1.71
Let G be a group, then $Z(G) \triangleleft G$.

Corollary 1.72
Some properties.

- If $n \geq 3$ then $Z(S_n) = 1$ [2, Exercise 3.1.].
- If G is not Abelian, then $G/Z(G)$ is not cyclic [2, Exercise 3.3.].

  Note 1.73. The contrapositive is more useful.

- $Z(G_1 \times \cdots \times G_k) = Z(G_1) \times \cdots \times Z(G_k)$ [2, Exercise 3.5.].
- The centre of D_n is given by

$$Z(D_n) = \begin{cases} 1 & \text{if } n \text{ odd} \\ \left\{1, \rho^{\frac{n}{2}}\right\} & \text{if } n \text{ even} \end{cases}$$

Definition 1.74. A group $G \neq 1$ is **simple** if its normal subgroups are 1 and G itself.

Example 1.75
Example of simple groups.

- For p prime, C_p is simple.
- A_n for $n \geq 5$ is simple. A_4 is not simple as V_4 is a normal subgroup.

Exam Questions 1.76 (Q1 Problem Sheet 1)

Let G be an Abelian simple group. Show that $G \cong C_p$ for some prime p.

Solution. Let G be an Abelian simple group. Since G is Abelian, every subgroup is normal, so the cyclic subgroup $\langle x \rangle$ generated by x is normal in G, i.e., $\langle x \rangle \triangleleft G$. Since G is simple and $\langle x \rangle \neq \{1\}$, it must be that $\langle x \rangle = G$. So G is cyclic. Now, consider two cases:

- **Case 1:** G is infinite. Then G is an infinite cyclic group, i.e., $G \cong (\mathbb{Z}, +)$. But $\mathbb{Z}$ has many nontrivial proper subgroups, such as $2\mathbb{Z} = \langle 2 \rangle$, which is normal (in fact, all subgroups of $\mathbb{Z}$ are normal since it is Abelian). This contradicts the assumption that G is simple. Hence, G cannot be infinite.
- **Case 2:** G is finite. Then G is a finite cyclic group, say of order n, i.e., $G \cong C_n$. We claim that n must be a prime number.

Suppose for contradiction that n is not prime, say $n = ab$ for some integers $1 < a, b < n$. Then the subgroup $\langle x^a \rangle$ has order b, and since G is cyclic (and hence Abelian), this subgroup is normal in G. But $\langle x^a \rangle$ is a proper, nontrivial normal subgroup of G, contradicting the simplicity of G.

Therefore, n must be prime, say $n = p$. Thus, $G \cong C_p$, as required.

1.6.2 Quotient groups

Theorem 1.77 ([2, Theorem 2.21.])**.** If $N \triangleleft G$, then the cosets of N in G form a group, denoted by G/N, of order $|G : N|$. The multiplication is defined by

$$(gN)(hN) = ghN$$

for all $g, h \in G$.

Corollary 1.78 ([2, Corollary 2.22.])**.** If $N \triangleleft G$, then the natural map (i.e. the map $\eta : G \to G/N$ defined by $\eta(g) = Ng$) is a surjective homomorphism with kernel N.

Proposition 1.79 (Subgroup theorem)

Let $N \triangleleft G$, then every subgroup of G/N is of the form H/N, where $N \leq H \leq G$.

1.6.3 Commutator subgroup

Definition 1.80. If $a, b \in G$, the **commutator** of a and b, is

$$[a, b] = aba^{-1}b^{-1}.$$

The **commutator subgroup** of G, denoted by G' is the subgroup of G generated by all the commutators i.e. $G' = \langle [x, y] : x, y \in G \rangle$.

Exam Questions 1.81 (Q1(b) Exam 2021)

Let N and K be normal subgroup in a group G. Is the commutator subgroup $[N, K]$ equal to $N \cap K$? Provide a proof or give a counterexample.

Solution. Let $n \in N$ and $k \in K$. Then, $x := [n, k]$ is contained in N since

$$x = n^{-1}(k^{-1}nk)$$

and in K since

$$x = (n^{-1}k^{-1}n)k.$$

Although the commutator subgroup $[N, K]$ might be smaller than $N \cap K$, for instance, if the whole G is Abelian, then $[N, K] = 1$, while $N \cap K$ could be larger.

Proposition 1.82

Let G' be the commutator subgroup of G, then G/G' is Abelian.

Proof. Let $aG', bG' \in G/G'$ be arbitrary cosets. Consider their product:

$$aG' \cdot bG' = abG'$$

We wish to show:

$$abG' = baG' \iff ab(ba)^{-1} \in G'$$

Compute:

$$ab(ba)^{-1} = aba^{-1}b^{-1} = [a, b]^{-1}$$

Since $[a, b] \in G'$, and G' is a subgroup (hence closed under inverses), we have:

$$[a, b]^{-1} \in G' \Rightarrow abG' = baG'$$

Therefore, G/G' is abelian. □

Proposition 1.83. Let $\phi : G \to A$ be a homomorphism where A is an Abelian group then, $G' \leq \ker(A)$.

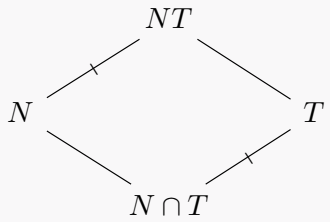
1.6.4 The isomorphism theorems

Theorem 1.84

We state the three isomorphism theorems in order.

1. Let $\phi : G \to H$ be a homomorphism. Then $\ker \phi$ is a normal subgroup of G and $G/\ker \phi \cong \mathrm{Im}(\phi)$ [2, Theorem 2.24.].
2. Let N and T be subgroups of G with normal N. Then $N \cap T \triangleleft T$ and
$$T/(N \cap T) \cong NT/N,$$
[2, Theorem 2.26.].
3. Let $K \leq H \leq G$, where both $K, H \triangleleft G$. Then $H/K \triangleleft G/K$ and
$$(G/K)/(H/K) \cong G/H,$$
[2, Theorem 2.27.]

Remark 1.85. The following diagram is mnemonic for the second isomorphism theorem:



1.7 Automorphisms

Definition 1.86. An **automorphism** of a group G is an isomorphism $\phi : G \to G$. The set of all automorphisms of G is denoted by $\mathrm{Aut}(G)$.

Proposition 1.87. The set $\mathrm{Aut}(G)$ is a group under composition.

Definition 1.88. For $g \in G$, the conjugation map $\iota_g : x \mapsto gxg^{-1}$ for $x \in G$ is an automorphism of G, called an **inner** automorphism. The set of all inner automorphisms is $\mathrm{Inn}(G) = \{\iota_g : g \in G\}$.

Proposition 1.89. $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$.

Proof. By definition. □

Proposition 1.90. We have that $G/Z(G) \cong \mathrm{Inn}(G)$.

Proof. The map $g \mapsto \iota_g$ from $G \to \mathrm{Aut}(G)$ is a homomorphism. Its image is $\mathrm{Inn}(G)$ and its kernel is $Z(G)$ hence by the first isomorphism we have the desired result. □

Exam Questions 1.91 (Q3 Problem Sheet 1)

The questions.

(a) Prove that $\mathrm{Aut}(C_n)$ is an Abelian group of order $\phi(n)$ (where ϕ is the Euler ϕ-function).

(b) Let p be prime. Show that $\mathrm{Aut}(C_p) \cong (\mathbb{F}_p^\times, \times)$, the multiplicative group of the field $\mathbb{F}_p$.

(c) Let p be prime. Show that $\mathrm{Aut}((C_p)^n) \cong \mathrm{GL}_n(\mathbb{F}_p)$ (Hint: $C_p^n \cong (\mathbb{F}_p^+)^n$.)

(d) Show that $\mathrm{Aut}(S_3) \cong S_3$ (Hint: first consider $\mathrm{Inn}(S_3)$.)

Solution. We prove each part in turn.

(a) Let $C_n = \langle x \rangle$. If $\alpha \in \mathrm{Aut}(C_n)$, then $\alpha(x) = x^a$, which has order n hence, $\gcd(a, n) = 1$. We have that $\alpha(x^i) = x^{ai}$ for all i thus,

$$|\mathrm{Aut}(C_n)| \leq \phi(n).$$

Finally, we note that for any a coprime to n, the map $x^i \mapsto x^{ai}$ for all i, is an automorphism of C_n. So, $|\mathrm{Aut}(C_n)| = \phi(n)$. It is clear that these maps commute under composition so $\mathrm{Aut}(C_n)$ is Abelian.

(b) This follows from part (a) by comparing the orders of the two groups and also that they are both cyclic hence, Abelian.

(c) Identify $(C_p)^n$ with $(\mathbb{F}_p^n, +)$. Let $V = \mathbb{F}_p^n$ be a vector space, then any automorphism of $(\mathbb{F}_p^n, +)$ preserves the addition and scalar multiplication of vectors. This is because for any $i \in \mathbb{F}_p^*$ and $v \in V$ we have that

$$\alpha(iv) = \alpha(\underbrace{v + \cdots + v}_{i \text{ times}}) = i\alpha(v).$$

Hence, $\alpha : V \to V$ is an invertible linear map i.e. $\alpha \in \mathrm{GL}_n(\mathbb{F}_p)$.

(d) We know $Z(S_3) = 1$, so $\mathrm{Inn}(S_3) \cong \frac{S_3}{Z(S_3)} \cong S_3$ thus, $|\mathrm{Aut}(S_3)| \geq 6$. Let $\alpha \in \mathrm{Aut}(S_3)$. For $t \in S_3$ of order 2, $\alpha(t)$ has also order 2 so, α permutes the elements of order 2, which are $\{(12), (13), (23)\} = T$. So we have a homomorphism $\mathrm{Aut}(S_3) \to \mathrm{Sym}(T)$. This map has trivial kernel because if α fixes all the elements of T then, it fixes all the elements of S_3. Hence, $\mathrm{Aut}(S_3) \leq \mathrm{Sym}(T) = 6$. We conclude that $\mathrm{Aut}(S_3) = \mathrm{Inn}(S_3) \cong S_3$.

1.8 Characteristic

Definition 1.92. A subgroup N of G is **characteristic** if $\alpha(N) = N$ for all $\alpha \in \mathrm{Aut}(G)$. We write this as N char G.

Example 1.93. Some examples:

- C_2 char C_4.

- C_2 is not a characteristic subgroup of $C_2 \times C_2$.
- $\mathrm{Inn}(G)$ char $\mathrm{Aut}(G)$.

Example 1.94

Let G be a group, then $Z(G)$ is a characteristic subgroup of G. To show this pick an element $x \in Z(G)$, then by definition $xg = gx$ for all $g \in G$. Hence, $\alpha(x)\alpha(g) = \alpha(g)\alpha(x)$ for all $g \in G$ which implies $\alpha(x) \in Z(G)$.

Proposition 1.95

Let M and N be subgroups of the group G.

- Suppose N char G then $N \triangleleft G$.
- Suppose M char N where $N \triangleleft G$ then $M \triangleleft G$.

Proof. We prove each statement in turn.

1. Let $g \in G$. The assumption means that $\iota_g(N) = N$ for all $g \in G$ i.e. $gNg^{-1} = N$ for all $g \in G$ which is the definition of $N \triangleleft G$.
2. Consider the ι_g in the previous proof. The restriction of ι_g to N is an automorphism of N, and so $\iota_g(M) = M$ since M char N. This means that $gMg^{-1} = M$ as required.

□

Proposition 1.96

We have the following.

1. G' char G (so $G' \triangleleft G$) and G/G' is Abelian.
2. Let $N \triangleleft G$, then G/N is Abelian if and only if $G' \leq N$.

Proof. We prove each statement in turn.

1. For $\alpha \in \mathrm{Aut}(G)$ we have that $\alpha([x, y]) = [\alpha(x), \alpha(y)]$ so, $\alpha(G') = G'$. Moreover, by construction, G/G' has trivial commutator, so it is Abelian.
2. If G/N is Abelian, then for all $g, h \in G$, we have
$$ghN = hgN \Rightarrow ghg^{-1}h^{-1} \in N$$
so $[g, h] \in N \Rightarrow G' \leq N$.
Conversely, if $G' \leq N$, then in G/N we have
$$[gN, hN] = [g, h]N = N,$$
so all commutators vanish and G/N is Abelian.

□

1.9 Generators

Definition 1.97. 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 finite subset then $\langle S \rangle$ consists of all products of the form $x_1^{a_1} \cdots a_k^{a_k}$, where $x_1, \ldots, x_k \in S$ (not necessarily distinct) and each $a_i \in \mathbb{Z}$.

Definition 1.98. If $G = \langle S \rangle$ for some finite subset S, we say that G is **finitely generated**.

Example 1.99. We can write

- $C_n = \langle \omega \rangle$ where ω is a root of unity.
- $D_{2n} = \langle \rho, \sigma \rangle$.
- $S_n = \langle \{(ij) : i < j\} \rangle = \langle (12 \cdots n), (12) \rangle$

1.10 Direct products

Definition 1.100. If $G_1, \ldots, G_k$ are groups, their **direct products** $G_1 \times \cdots \times G_k$ is defined to be the group with

- elements $(g_1, \ldots, g_k)$ where each $g_i \in G_i$,
- the multiplication is defined component wise i.e. $(g_1, \ldots, g_k)(h_1, \ldots, h_k) = (g_1 h_1, \ldots, g_k h_k)$.

Proposition 1.101. The group $G_1 \times G_2$ 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 $A_1 A_2 = \{a_1 a_2 : a_i \in A_i\}$.

Proposition 1.102. 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 $G \cong A \times B$.

Example 1.103

The group $D_{12} = \langle \rho, \sigma \rangle$ has subgroups $\langle \rho^2, \sigma \rangle \cong D_6$ and $\langle \rho^3 \rangle \cong C_2$. The conditions of the proposition above hold hence

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

Proposition 1.104

Let G be a group and let $N \trianglelefteq G$ be a normal subgroup of index 2. Then for any subgroup $H \leq G$ such that $H \not\subseteq N$, we have

$$G = NH.$$

Proof. Since $[G : N] = 2$, there are exactly two cosets: N and gN for any $g \in G \setminus N$. Since $H \not\subseteq N$, there exists $h \in H \setminus N$, so $h \in gN$. Therefore, every element $g \in G$ is either in N or in hN, and hence $G = N \cup hN \subseteq NH$. As $NH \subseteq G$, we conclude $G = NH$. □

Proposition 1.105

Let $H, K \trianglelefteq G$ be normal subgroups of a group G such that $H \cap K = \{1\}$. Then:

$$HK \cong H \times K.$$

Proof. Define a map:

$$\varphi : H \times K \to HK, \quad \varphi(h, k) = hk.$$

- Since $H, K \trianglelefteq G$, for all $h_2 \in H, k_1 \in K$, $k_1 h_2 k_1^{-1} \in H$, so:

  $$\varphi(h_1, k_1) \cdot \varphi(h_2, k_2) = h_1 k_1 h_2 k_2 = h_1 (k_1 h_2 k_1^{-1})(k_1 k_2) \in HK.$$

  So φ is a homomorphism.

- If $\varphi(h, k) = 1$, then $hk = 1 \Rightarrow h = k^{-1} \in H \cap K = \{1\} \Rightarrow h = k = 1$. So φ is injective.

- Every element of HK is of the form hk, so φ is surjective.

□

Proposition 1.106. Some results of direct products.

1. $H \times K$ is Abelian if and only if H and K are Abelian [2, Exercise 2.61.].
2. If $\gcd(m, n) = 1$ then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ [2, Exercise 2.62.].
3. If $A \triangleleft H$ and $B \triangleleft K$ then $A \times B \triangleleft H \times K$ and

   $$(H \times K)/(A \times K) \cong (H/A) \times (K/B).$$

   [2, Theorem 2.30.].
4. If $G = H \times K$, then $G/(H \times 1) \cong K$ [2, Corollary 2.31.].

Theorem 1.107

For a group G and an integer $m \geq 0$, write $G^m = G \times \cdots \times G$ m times, if $m = 0$ set $G^m = 1$. If G is 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

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

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

Note 1.108. The $\mathbb{Z}^m$ is used when the group G is of infinite order.

Example 1.109

To count how many finitely generated Abelian groups of order n there are, we consider the prime factorisation. For example: consider a group of order $24 = 2^3 \cdot 3^1$. The number of Abelian groups of this order, up to isomorphism is given by

$$(\text{number of Abelian groups of order } 2^3) \cdot (\text{number of Abelian groups of order } 3^1)$$

which is the same as (unordered)

$$(\text{number of integer partitions of } 3) \cdot (\text{number of integer partitions of } 1)$$

List all abelian groups of order $2^3 = 8$, corresponding to partitions of the exponent 3:

$$C_8, \quad C_4 \times C_2, \quad C_2 \times C_2 \times C_2$$

The only abelian group of order 3 is C_3. Combine each 2-part with the 3-part using that $C_m \times C_n \cong C_{mn}$ when $\gcd(m, n) = 1$:

- $C_8 \times C_3 \cong C_{24}$
- $(C_4 \times C_2) \times C_3 \cong C_2 \times C_{12}$
- $(C_2 \times C_2 \times C_2) \times C_3 \cong C_2 \times C_2 \times C_6$

There are three Abelian groups of order 24 up to isomorphism:

- C_{24},
- $C_2 \times C_{12}$,
- $C_2 \times C_2 \times C_6$.

1.11 Group actions

Definition 1.110. An **action** of a group G on a set Ω is homomorphism $\rho : G \to \mathrm{Sym}(\Omega)$. For $g \in G$ and $\omega \in \Omega$ we write $g(\omega)$ instead of $[\rho(g)](\omega)$.

Definition 1.111. We can define an equivalence relation $\sim$ on Ω by

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

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

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

Definition 1.112. If there is only one orbit we say that G is **transitive** on Ω.

Definition 1.113. For $\alpha \in \Omega$ the **stabiliser** of α is defined to be

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

Corollary 1.114. The stabiliser is a subgroup of G.

Example 1.115
Consider the group S_n, the stabiliser $G_\alpha \cong S_{n-1}$ for any $\alpha \in S_n$.

Corollary 1.116. For $x \in G$ and $\alpha \in \Omega$ the stabiliser of $x(\alpha)$ is equal to $xG_\alpha x^{-1}$ i.e. $G_{x(\alpha)} = xG_\alpha x^{-1}$.

Proposition 1.117 (Orbit-stabiliser theorem)
The size of the orbit

$$\left|\alpha^G\right| = |G : G_\alpha| = \frac{|G|}{|G_\alpha|}.$$

In particular, if G is transitive on Ω then

$$\Omega = |G : G_\alpha|$$

for any $\alpha \in \Omega$.

Note 1.118. If $H \leq G$, recall that $|G : H|$ is the **index** of H in G is the number of cosets in G with respect to H.

Proposition 1.119 (Cauchy's theorem)
If G is a finite group and a prime p divides $|G|$, then G contains an element of order p.

Note 1.120. Recall that for a prime p, a finite group is a p-group if $|G| = p^a$ for some a.

Corollary 1.121. If G is a non-trivial group of order p then $Z(G) \neq 1$.

1.12 Conjugacy classes

Theorem 1.122. The map

$$\rho : G \to \mathrm{Sym}(G)$$
$$g \mapsto \iota_g$$

where $\iota_g(x) = gxg^{-1}$ is an action.

Definition 1.123. For this action the orbit containing x is

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

is called the **conjugacy class** of G containing x.

Definition 1.124. If $x \in G$, then the **centraliser** of x is

$$C_G(x) = \{ g \in G : gx = xg \},$$

i.e. the set of all $g \in G$ which commute with x.

Corollary 1.125. $C_G(x)$ is a subgroup of G.

Proposition 1.126

For this action, the size of the conjugacy class is

$$\left| x^G \right| = |G : C_G(x)|.$$

In particular,

- this number is a divisor of $|G|$, when G is finite,
- $\left| x^G \right| = 1 \iff C_G(x) = G \iff x \in Z(G)$.

Exam Questions 1.127 (Q1(a) Exam 2009)

Let $g \in G \setminus \{1\}$ and $\mathcal{C}$ be the conjugacy class of $g \in G$. Show that either $|\mathcal{C}| \leq \frac{|G|}{3}$ or else $|\mathcal{C}| = \frac{|G|}{2}$.

Solution. The conjugacy class is an orbit of G in its conjugation action. By the orbit-stabiliser theorem we have that $|\mathcal{C}| = \frac{|G|}{|C_G(g)|}$. We have that $|C_G(g)| \geq 2$ since it must contain $\{1, g\}$. We have two cases:

- if $|C_G(g)| \geq 3$ then $|\mathcal{C}| \leq \frac{|G|}{3}$;
- otherwise $|C_G(g)| = 2$ and thus $|\mathcal{C}| = \frac{|G|}{2}$.

Corollary 1.128

If $c_1, \ldots, c_k$ are the conjugacy classes of G such that each $c_i > 1$ then the **class equation** is defined as

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

Exam Questions 1.129 (Q1 Exam 2009)

Let G be a group of size p^n where p is a prime and $n \geq 1$. Prove that the centre $Z(G)$ of G is different from 1.

Solution. Assume the conditions of the problem. Let $\mathcal{C}_1, \ldots, \mathcal{C}_k$ be the conjugacy classes of G. By the class equation we know

$$|G| = |Z(G)| + \sum_{i=1}^{k} |\mathcal{C}_i| .$$

Each $\mathcal{C}_i = \{{}^a g_i : a \in G\}$ is an orbit of G in its conjugation action. By the orbit-stabiliser theorem we have that

$$|\mathcal{C}_i| = \frac{|G|}{|C_G(g_i)|}.$$

It is clear that $|\mathcal{C}_i| \mid |G|$ and $|\mathcal{C}_i| > 1$ since $C_G(g_i) \neq G$ as $g_i \notin Z(G)$. It follows that $p \mid |\mathcal{C}_i|$ for all $i \in \{1, \ldots, k\}$, $p \mid G$ thus by the class equation $p \mid Z(G)$. Since $1 \in Z(G)$ and $p \mid Z(G)$ we must have that $|Z(G)| > 1$.

Corollary 1.130

If $N \triangleleft G$, then N is a union of conjugacy classes of G including the class $\{1\}$.

Note 1.131. 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.

Proof. For $n \in N$ we have that $gng^{-1} \in N$ for all $g \in G$ hence, $n^G \subseteq N$. □

Proposition 1.132

Useful results.

- If $\alpha \in S_n$ is an n-cycle, then $C_{S_n}(\alpha) = \langle \alpha \rangle$ [2, Exercise 3.2.]
- For every $a, x \in G$ we have that $C_G(axa^{-1}) = aC_G(x)a^{-1}$ [2, Exercise 3.6.].
- If $H \leq G$ and $h \in H$, then $C_H(h) = C_G(h) \cap H$ [2, Exercise 3.6.].

1.12.1 Conjugacy classes of D_n

Theorem 1.133

The conjugacy classes of D_n:

- If n is odd, then the conjugacy classes of D_n are

$$\{1\}, \left\{\rho^i, \rho^{-i} : 1 \leq i \leq \frac{1}{2}(n-1)\right\} \text{ and } \left\{\sigma\rho^i : 0 \leq i \leq n-1\right\}$$

- If n is even, then the conjugacy classes of D_n are

$$\{1\}, \left\{\rho^{n/2}\right\}, \left\{\rho^i, \rho^{-i} : 1 \leq i \leq \frac{n}{2}-1\right\}, \left\{\sigma\rho^{2i} : 0 \leq i \leq \frac{n}{2}-1\right\}, \text{ and } \left\{\sigma\rho^{2i+1} : 0 \leq i \leq \frac{n}{2}-1\right\}.$$

1.12.2 Conjugacy classes of S_n

Proposition 1.134

Let $\sigma \in S_n$ be given, there's a superfast way to compute conjugations of a cycle $(\iota_1, \cdots, \iota_n) \in S_n$ by σ. Namely:

$$\sigma(\iota_1, \cdots, \iota_n)\sigma^{-1} = (\sigma(\iota_1), \cdots, \sigma(\iota_n))$$

Definition 1.135. Any $x \in S_n$ can be written as the product of disjoint cycles of length $k_1, \ldots, k_r$ such that $\sum_i k_i = n$. Taking $k_1 \geq k_2 \geq \cdots k_r$, we say that the **cycle-shape** of x is $(k_1, \ldots, k_r)$.

Example 1.136

For $x = (125)(37)(48) \in S_8$ it has cycle shape $(3, 2, 2, 1) = (3, 2^2, 1)$. We include a 1 in the cycle shape to indicate the presence of (6) which is omitted from x.

Theorem 1.137

Permutations $\alpha, \beta \in S_n$ are conjugate if and only if they have the same cycle shape.

Note 1.138. Equivalently, 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

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

Hence, for $x = c_1 c_2 \cdots c_r$, a product of disjoint cycles of length $k_1, \ldots, k_r$ 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 $k_1, \dots, k_r$. Hence, x^{S_n} is contained in the set of permutations of cycle-shape $(k_1, \dots, k_r)$.

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

Proposition 1.139

Let $x \in S_n$ have cycle-shape $(r_1^{a_1}, \dots, r_k^{a_k})$ where each r_i are distinct. Then

$$|C_{S_n}(x)| = \prod_{i=1}^{k} r_i^{a_i} \cdot a_i!$$

Note 1.140. This result is useful as we know that the size of the conjugacy class

$$x^{S_n} = |S_n : C_{S_n}(x)|.$$

Example 1.141

The size of conjugacy classes of S_5:

cycle-shape	(1^5)	$(2, 1^3)$	$(3, 1^2)$	$(4, 1)$	(5)	$(2^2, 1)$	$(3, 2)$
$\lvert C_{S_n}(x)\rvert$	$5!$	$2 \cdot 3! = 12$	$3 \cdot 2! = 6$	4	5	$2^2 \cdot 2! = 8$	$3 \cdot 2 = 6$
$\lvert x^{S_5}\rvert$	1	10	20	30	24	15	20

Corollary 1.142 ([2, Corollary 3.6.])**.** A subgroup $H \leq S_n$ is a normal subgroup if and only if, whenever $\alpha \in H$, then every β having the same cycle-shape as α also lies in H.

1.12.3 Conjugacy classes of A_n

Proposition 1.143

Let $x \in A_n$. We have that $x^{A_n} \subseteq x^{S_n}$.

1. If $C_{S_n}(x) \leq A_n$ then $\left|x^{A_n}\right| = \frac{1}{2}\left|x^{S_n}\right|$ and x^{S_n} **splits** into two A_n-conjugacy classes.
2. If $C_{S_n}(x) \not\leq A_n$ then $x^{A_n} = x^{S_n}$.

Proof. We prove each statement in turn.

1. Suppose $C_{S_n}(x) \leq A_n$ so, $C_{S_n}(x) = C_{A_n}(x)$ then
$$\left|x^{A_n}\right| = |A_n : C_{A_n}(x)| = \frac{1}{2}|S_n : C_{S_n}(x)| = \frac{1}{2}\left|x^{S_n}\right|.$$
2. 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,
$$\left|x^{A_n}\right| = |A_n : C_{A_n}(x)| = |S_n : C_{S_n}(x)| = \left|x^{S_n}\right|.$$

□

Proposition 1.144. The group A_5 is simple.

Proof. 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

Note 1.145. A conjugacy class in S_n splits in A_n if the cycle type is made of disjoint, odd-length cycles of different sizes.

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. □

Exam Questions 1.146 (Q8 Problem Sheet 1)
Prove that A_4 has no subgroup of order 6.

Solution. For the sake of contradiction, suppose it does. Then $|A_4 : H| = \frac{\left(\frac{4!}{2}\right)}{6} = 2$ hence, $H \triangleleft A_4$ and H has an element of order 2 say t. Then H contains the conjugacy class $t^{A_4} = \{(12)(34), (13)(24), (14)(23)\}$. But this means $H \geq V_4$ a subgroup of order 4 which does not divide 6.

1.12.4 Conjugacy classes of $\mathbf{GL}_n(\mathbb{F})$

Note 1.147. We need to recall some facts first.

Definition 1.148. Let $f(x) \in F[X]$ be a monic polynomial of the form

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x^1 + a_0,$$

the **companion matrix** of $f(x)$ is the $n \times n$ matrix:

$$C(f) = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

Proposition 1.149. We have the following:

- If $A, B \in M_n(\mathbb{F})$ then $A \oplus B = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$.
- If $f, g \in F[X]$ are coprime then $C(f) \oplus C(g) = C(fg)$.

Theorem 1.150 (Rational canonical form theorem)**.** Let V be a finite-dimensional vector space over a field $\mathbb{F}$, and let $T : V \to V$ be a linear map. Let the minimal polynomial

$$m_T(x) = \prod_{i=1}^{t} f_i(x)^{k_i},$$

where each $f_i \in F[X]$ are distinct. Then there exists a basis $\mathcal{B}$ of V such that

$$[T]_{\mathcal{B}} = \bigoplus_{i=1}^{t} C(f_i(x)^{k_i}).$$

Definition 1.151. We call the matrix $[T]_{\mathcal{B}}$ as described above, **rational canonical form** (RCF).

Proposition 1.152

The conjugacy classes of $\mathrm{GL}_n(\mathbb{F})$ correspond bijectively to the Rational canonical form of invertible $n \times n$ matrices over $\mathbb{F}$.

Note 1.153. RCF's are a similar construction to Jordan normal forms but are valid over any field $\mathbb{F}$. JNF are only valid over $\mathbb{C}$.

Example 1.154. Let $G = \mathrm{GL}_3(\mathbb{F}_2)$, where the field $\mathbb{F}_2 = \{0, 1\}$. Let us compute the number of conjugacy classes.

We need the minimal polynomial of the matrices in G, so it suffices to consider the irreducible polynomials in $\mathbb{F}_2[X]$ of degree ≤ 3, which are

$$x,\ x+1,\ x^2+x+1,\ x^3+x+1,\ x^3+x^2+1.$$

The possible characteristic polynomials of elements of G are products of these irreducible that have total degree 3, but with no factor x (as matrices in G are invertible). There are four such polynomials, listed in column 1 of Table 1 below. The possible minimal polynomials divide these, and have the same irreducible factors; there are six possible minimal polynomials, listed in column 2 of the table. For each possible minimal polynomial, there is only one RCF matrix, as listed in column 3 of the table. We conclude that $\mathrm{GL}(3, \mathbb{F}_2)$ has 6 conjugacy classes, and representatives of each of these classes are given by the matrices in column 3.

char. poly.	**possible min. polys.**	**RCF**
$(x+1)^3$	$(x+1)$, $(x+1)^2$, $(x+1)^3$	I, $\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}$, $\begin{pmatrix}0&1&1\\1&0&1\\0&1&1\end{pmatrix}$
$(x+1)(x^2+x+1)$	$(x+1)(x^2+x+1)$	$\begin{pmatrix}1&0&0\\0&0&1\\0&1&1\end{pmatrix}$
x^3+x+1	x^3+x+1	$\begin{pmatrix}0&0&1\\1&0&1\\0&1&0\end{pmatrix}$
x^3+x^2+1	x^3+x^2+1	$\begin{pmatrix}0&0&1\\0&1&0\\1&0&1\end{pmatrix}$

Table 1: Conjugacy classes of $GL(3,\mathbb{F}_2)$

Note 1.155. Because we are in $\mathbb{F}_2$ we have that $-1 \equiv 1 \pmod 2$.

Example 1.156 (Conjugacy classes in GL)
Two examples.

- Consider $\mathrm{GL}_2(\mathbb{F}_3)$. To find how many RCF's there are it suffices to consider the characteristic polynomials. First notice that 0 cannot be a root of these polynomials as then the matrix would not be in G. The polynomials 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 polynomials there are 2 RCF's and the other only 1. So there are 8 conjugacy classes.

- For $\mathrm{GL}_3(\mathbb{F}_2)$, the possible characteristic polynomials are

$$(x+1)^3, (x+1)(x^2+x+1), x^3+x+1, x^3+x^2+1.$$

  The first polynomial has 3 RCF's, so there are only 6 conjugacy classes.

To get these polynomials, we need to consider the irreducible polynomials over the field and the mix-and-match the possible eigenvalues to get more polynomials.

1.13 Coset action

Proposition 1.157

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

$$\pi_g : xH \mapsto gxH \quad \text{for all } xH \in \Omega.$$

1. The map $\pi : G \to \mathrm{Sym}(\Omega)$ sending $g \mapsto \pi_g$ is a transitive action of G on Ω.
2. We have that
$$\ker(\pi) = \bigcap_{x \in G} xHx^{-1} \lhd G$$
which is the largest normal subgroup of G contained in H. Furthermore, $G/\ker(\pi)$ is isomorphic to a subgroup of $\mathrm{Sym}(\Omega)$.
3. If $|\Omega| = n = |G : H|$ then $|G/\ker(\pi)|$ divides $n!$.

Proof. We prove each statement in turn.

1. 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
$$\{\pi_g(H) : g \in G\} = \{gH : g \in G\} = \Omega.$$
2. We have
$$\begin{aligned}\ker(\pi) &= \{g \in G : \pi_g = e \in \mathrm{Sym}(\Omega)\} \\ &= \{g \in G : gxH = xH \,\forall x \in G\} \\ &= \{g \in G : x^{-1}gx \in H \,\forall x \in G\} \\ &= \bigcap_{x \in G} xHx^{-1}.\end{aligned}$$
By the first isomorphism theorem, $G/\ker(\pi) \cong \mathrm{Im}(\pi)$, a subgroup of $\mathrm{Sym}(\Omega)$.
3. This follows by (2) and Lagrange's theorem.

□

Corollary 1.158

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 1.159

A few examples.

- 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 $\mathrm{Sym}(G)$.

Exam Questions 1.160 (Q1(b) Exam 2010)

Let $n \geq 5$ and $2 < k < n$. Stating carefully any results from the course that you use, prove that S_n has no subgroup of index k.

Solution. We will use the theorem that A_n is simple when $n \geq 5$. Suppose that S_n has a subgroup H of index $2 < k < n$. By the proposition above we know that H contains a normal subgroup N of S_n of index at most $k!$. Now $N \cap A_n$ is a normal subgroup of A_n by the second isomorphism theorem. There are two cases:

- $N \cap A_n = A_n$, but then $A_n \leq N$ and so $2 \geq |S_n : N| \geq |S_n : H| = k > 2$ which is a contradiction.
- $N \cap A_n = 1$. In this case, by the second isomorphism theorem we have that $|NA_n| = |N|\,|A_n| \leq n!$ and so $|N| \leq \frac{n!}{|A_n|} = 2$. However, $n! = |G : N|\,|N| \leq k! \cdot 2 \leq (n-1)! \cdot 2$ giving that $n \leq 2$ which is a contradiction again.

So S_n cannot have a subgroup of index k between 2 and $n - 1$.

Proposition 1.161 (Cayley's theorem)

If $|G| = n$ then G is isomorphic to a subgroup of S_n.

1.14 Conjugates of subgroups

Definition 1.162. Let $H \leq G$. For $g \in G$, the **conjugate** of H by G is the set

$$^gH = gHg^{-1} = \left\{ghg^{-1} : h \in H\right\}.$$

Proposition 1.163. The set ^gH is a subgroup and is isomorphic to H by the map $h \mapsto ghg^{-1}$.

Proposition 1.164
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 ${}^gH \mapsto^{xg} H$).

Definition 1.165. The stabiliser of H using the action from above is

$$\begin{aligned} N_G(H) &= \{g \in G : {}^gH = H\} \\ &= \{g \in G : gHg^{-1} = H\}, \end{aligned}$$

a subgroup of G called the **normaliser** of H.

Proposition 1.166
Let $H \leq G$.

1. The number of distinct conjugates of H in G is equal to $|G : N_G(H)|$.
2. $N_G(H) = G$ if and only if $H \triangleleft G$.

Example 1.167. Let $G = S_4$ and $H = C_3 = \langle(123)\rangle$. Since $H \triangleleft S_3 < S_4$ we have that $N_G(H) = S_3$ and the number of conjugates of H in G is $|S_4 : S_3| = 4$.

Proof. Use orbit-stabiliser theorem. □

Definition 1.168. For a subset $X \subseteq G$, the **centraliser** in G of X is

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

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

Proposition 1.169
Let $H \leq G$. Then,

1. $C_G(H) \triangleleft N_G(H)$, and
2. $N_G(H)/C_G(H) \lesssim \mathrm{Aut}(H)$ ($\lesssim$ means isomorphic to a subgroup).

Proof. For $n \in N_G(H) = N$ i.e. ${}^nH = H$, define $\iota_n = H \to H$ to be $h \mapsto nhn^{-1}$ for $h \in H$. Then $\iota_n \in \mathrm{Aut}(H)$, and the map $\iota : N \to \mathrm{Aut}(H)$ with $n \mapsto \iota_n$ is a homomorphism. Also, $n \in \ker(\iota) \iff \iota_n = \mathrm{id} \iff nhn^{-1} = h$ for all $h \in H \iff n \in C_G(H)$. So $\ker(\iota) = C_G(H) \triangleleft N$ by the first isomorphism theorem we have $N_G(H)/C_G(H) \cong \mathrm{Im}(\iota) \leq \mathrm{Aut}(H)$. □

Example 1.170

A few examples.

- Let $G = S_4$ and $H = \langle(123)\rangle$ then $N_G(H) = S_3$ and also $C_G(H) = H$. So, $N_G(H)/C_G(H) = S_3/A_3 \cong C_2 \cong \mathrm{Aut}(H)$.
- If we instead let $H = V_4 \triangleleft G$, here $N_G(H) = G$ and $C_G(H) = H$, so we have $N_G(H)/C_G(H) = S_4/V_4 \cong S_3 \leq \mathrm{Aut}(V_4)$. Now, since $V_4 \cong C_2 \times C_2$ and $\mathrm{Aut}(C_2 \times C_2) \cong \mathrm{GL}_2(\mathbb{F}_2) \cong S_3$.

Proposition 1.171. If H and K are subsets of a group G, we define $HK = \{hk : h \in H, k \in K\}$.

Proposition 1.172

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

1. Then $|HK| = \frac{|H||K|}{|H \cap K|}$.
2. If $H \leq N_G(K)$, then HK is a subgroup of G.

Proof. We prove each statement in turn.

1. Define a map $\phi : H \times K \to HK$ 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 $|H \times K| = |HK||H \cap K|$.
2. 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 $(hk)^{-1} = k^{-1}h^{-1} = h^{-1}(hk)^{-1}h \in HK$.

□

1.15 Groups of small order

Proposition 1.173

Up to isomorphism groups of order ≤ 8 are:

Order	G
2, 3, 5, 7	C_2, C_3, C_5, C_7
4	$C_4, C_2 \times C_2$
6	C_6, D_6
8	$C_8, C_4 \times C_2, C_2 \times C_2 \times C_2, D_8, Q_8$

Table 2: Groups of Various Orders

2 Jordan-Hölder theorem

Note 2.1. The main result of this section shows that every finite group is "built" out of a unique collection of simple groups.

2.1 Composition series

Definition 2.2. Let G be a group and let $N \triangleleft G$. We say that N is a **maximal normal** subgroup if $N \neq G$ and

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

Note 2.3. That is, N is a proper subgroup of G that is contained in no larger normal subgroup.

Lemma 2.4. If N is a maximal normal subgroup of G, then G/N is a simple group.

Proof. Suppose $K \triangleleft G/N$. By a proposition, $K = M/N$ where $N \leq M \triangleleft G$. Since N is maximal normal in G, $M = N$ or G. Thus, $K = 1$ or G/N, so G/N is simple. □

Definition 2.5. Let G be a finite group and choose a maximal normal subgroup $G_1 \triangleleft G$, then a maximal normal $G_2 \triangleleft G_1$ (G_2 is not necessarily normal in G) and continue. So, we get a series

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_r = 1.$$

Such series is a **composition series** for G. The simple group G_i/G_{i+1} for $i \in \{0, 1, \ldots, r\}$ are called the **composition factors** of the series.

Remark 2.6. Note that G_2 is normal in G_1, but not necessarily normal in G. By the lemma above we are guaranteed that each quotient G_i/G_{i+1} is simple.

Example 2.7

Let $G = C_{12}$. This is an Abelian group so, any subgroup is immediately normal. From a previous proposition the subgroups are the ones of order $d \mid n$, namely C_6, C_4, C_3, C_2. There are three composition series:

$$\begin{aligned} &C_{12} \triangleright C_4 \triangleright C_2 \triangleright 1, \quad \text{comp. factors } C_3, C_2, C_2 \\ &C_{12} \triangleright C_6 \triangleright C_2 \triangleright 1, \quad \text{comp. factors } C_2, C_3, C_2 \\ &C_{12} \triangleright C_6 \triangleright C_3 \triangleright 1, \quad \text{comp. factors } C_2, C_2, C_3 \end{aligned}$$

We see that each of the series has the same composition factors but in different orders.

2.2 The theorem

Proposition 2.8
Let G be a group, let $H \leq G$, and let $N \triangleleft G$. Then the following hold:

1. $H \cap N \triangleleft H$,
2. $HN \leq G$,
3. The second isomorphism theorem: $HN/N \cong H/(H \cap N)$.

Proof. We prove each statement in turn.

(i) Clear.

(ii) Follows from a proposition.

(iii) Define a map $\phi : H \to HN/N$ by $\phi(h) = hN$. Then:

- ϕ is a homomorphism.
- $\ker(\phi) = \{h \in H : hN = N\} = H \cap N$.
- ϕ is surjective: every coset in HN/N has the form $hnN = hN = \phi(h)$ for some $h \in H$, $n \in N$.

By the First Isomorphism Theorem:

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

$\square$

Theorem 2.9 (Jordan-Hölder theorem)
Any two composition series for a finite group G give the same collection of composition factors (possibly in a different order).

Proof. We proceed by induction on $|G|$. The base case $|G| = 1$ is trivial. Let

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

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

be two composition series of G.

- **Case 1:** $G_1 = H_1$.
  Then both remaining series are composition series for G_1, so by induction they have the same length and composition factors. Adding G/G_1 gives the result for G.
- **Case 2:** $G_1 \neq H_1$.
  Let $K = G_1 \cap H_1 \triangleleft G$. Take a composition series for K:

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

  Claim:

  $$G_1/K \cong G/H_1, \quad H_1/K \cong G/G_1.$$

Assuming the claim, we can form two composition series for G_1 and H_1:

For G_1:

$$G_1 \triangleright G_2 \triangleright \cdots \triangleright G_r = 1, \quad G_1 \triangleright K \triangleright K_3 \triangleright \cdots \triangleright K_t = 1.$$

By induction, both have same factors, so (2.2) has:

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

For H_1:

$$H_1 \triangleright H_2 \triangleright \cdots \triangleright H_s = 1, \quad H_1 \triangleright K \triangleright K_3 \triangleright \cdots \triangleright K_t = 1.$$

So (2.3) has:

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

By the claim, (2.4) and (2.5) list the same factors (just swap first two terms), so the theorem holds.

We provce the claim. Since $G_1, H_1 \triangleleft G$, then $G_1H_1 \leq G$ and is normal. Also, since $G_1 \neq H_1$ and both are maximal normal, $G_1H_1 = G$.

Apply Second Isomorphism Theorem:

$$G/H_1 = G_1H_1/H_1 \cong G_1/(G_1 \cap H_1) = G_1/K,$$

$$G/G_1 \cong H_1/K.$$

So the claim holds. □

Example 2.10

Some 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 C_{p^2}, $C_p \times C_p$.
3. Comp factors A_5, C_2: examples are S_5 and $A_5 \times C_2$.
4. Comp factors $C_p, \ldots, C_p$ (p primes, k factors): all groups of order p^k.
5. Comp factors $C_{p_1}, \ldots, C_{p_k}$ (p_i primes, not necessarily distinct): all *solvable* groups of order $p_1 \cdots p_k$.

Exam Questions 2.11 (Q2 Exam 2009)

Suppose that the group G has just two composition factors S_1 and S_2.

(a) Let $X \neq Y$ be two simple normal subgroups of G, both different from $\{1\}$. Show that $X \cap Y = \{1\}$, G/X is simple and that $G = XY$.

(b) Assume that G has at least two different composition series. Show that G is isomorphic to $S_1 \times S_2$.

(c) Show that if S_1 and S_2 are non-abelian then $S_1 \times S_2$ has precisely two composition series.

(d) Is part (c) true if S_1 and S_2 are allowed to be Abelian?

Solution. We provide the solution for each part.

(a) Since $X \neq Y$ without loss of generality we have that $Y \not\subseteq X$ hence, $X \cap Y \neq Y$. Now ${}^g(X \cap Y) = {}^gX \cap {}^gY = X \cap Y$ for any $g \in G$, since X and Y are both normal. So, $X \cap Y \triangleleft G$ and in particular $X \cap Y \triangleleft Y$ (by a proposition above). But Y is simple so $X \cap Y = 1$.

For the sake of contradiction suppose G/X is not simple, then G will have a normal series $1 \triangleleft X \triangleleft M \triangleleft G$ with some $M \neq X, G$ and so G will have more than 3 composition factors, which contradicts the Jordan-Hölder theorem. Hence, G/X must be simple.

We have that ${}^gXY = {}^gX{}^gY = XY$ for any $g \in G$ since $X, Y \triangleleft G$, so $XY \triangleleft G$. By the second isomorphism theorem we have that $\frac{XY}{X} \triangleleft G/X$. Since $Y \not\subseteq X$ we have $XY \neq X$, and as G/X is simple we must have $XY = G$.

(b) Suppose G has composition series

$$1 \triangleleft X \triangleleft G \quad \text{and} \quad 1 \triangleleft Y \triangleleft G$$

with $X \neq Y$. Then $XY = G$ and $X \cap Y = 1$ by part (a). By a proposition in the course we have that $G \cong X \times Y$ where X, Y are the composition factors of G. By the Jordan-Hölder theorem these are S_1 and S_2.

(c) Let $G = S_1 \times S_2$, two possible composition series for G are

$$1 \triangleleft S_1 \times 1 \triangleleft G \quad \text{and} \quad 1 \triangleleft 1 \times S_2 \triangleleft G.$$

Suppose there is another, say $1 \triangleleft X \triangleleft G$, the subgroups $X, S_1 = S_1 \times 1$ and $S_2 = 1 \times S_2$ are distinct normal simple subgroups of G. By the argument in part (a) we have $X \cap S_1 = X \cap S_2 = 1$. We know $[A, B] \leq A \cap B$ if $A, B \triangleleft G$. Hence, $[X, S_1] = [X, S_2] = 1$ but then X commutes with $G = S_1 S_2$ so X is Abelian. This cannot be the case as G has no Abelian composition factors (only S_1 and S_2).

(d) The statement would be FALSE. For example consider when $S_1 = S_2 = C_2$, the group $G = C_2 \times C_2$ has three subgroups of size 2, hence 3 different composition series.

3 Some finite simple groups

3.1 Alternating groups

Lemma 3.1. Let $n \geq 4$. Then every element of A_n can be expressed as a product of 3-cycles.

> **Note 3.2.** Recall that 3-cycles (in fact any odd-cycle) are made up of even transpositions.

Proof. Let $x \in A_n$, then x is a product of an 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. Whereas 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. □

Corollary 3.3
If $N \triangleleft A_n$ and N contains a 3-cycle then $N = A_n$.

Proof. Let $t \in N$ then t is a 3-cycle as $N \triangleleft A_n$. The conjugacy class of t, $t^{A_n} \subseteq N$ is the set of all 3-cycles as conjugate elements must have the same cycle-shape. Then all 3-cycles are in t^{A_n} hence $N = A_n$. □

Theorem 3.4
For $n \geq 5$, the alternating group A_n is simple.

Proof. We proceed by induction on n. The base case A_5 is simple by a proposition. Assume $n \geq 6$, and let $G = A_n$. Suppose $N \triangleleft G$, with $N \neq 1$. For each $i \in \{1, \ldots, n\}$, the point stabiliser $G_i \cong A_{n-1}$, which is simple by induction. Since $N \cap G_i \triangleleft G_i$, it follows that

$$N \cap G_i = 1 \quad \text{or} \quad N \cap G_i = G_i.$$

- **Case 1:** $N \cap G_i = G_i$ for some i. Then $G_i \leq N$, so N contains a 3-cycle t. As $N \triangleleft G$, the entire conjugacy class $t^G \subseteq N$. By a proposition t^G consists of all 3-cycles, and by another proposition, $\langle t^G \rangle = A_n$. Hence $N = G$.
- **Case 2:** $N \cap G_i = 1$ for all i. Let $1 \neq n \in N$. There exists a 3-cycle $t \in A_n$ such that $tn \neq nt$. Without loss of generality, let $n = (12)\cdots$, and $t = (1\ 2\ 4)$. Consider the commutator:
$$x = [t, n] = tnt^{-1}n^{-1} \neq 1.$$
Note that:
  - $x = (tnt^{-1})n^{-1} \in N$, since $N \triangleleft G$,
  - $x = t(nt^{-1}n^{-1}) = (1\ 2\ 4)(2\ j\ k)$ for some j, k.

  Thus, $x \in N$ and moves at most 5 points, so $x \in G_i$ for some i. But then $x \in N \cap G_i = 1$, a contradiction. Therefore, no such nontrivial N exists, and A_n is simple.

□

3.2 Matrix groups

Remark 3.5. For each prime power $q = p^a$, there is a finite field of order q, which we denote by $\mathbb{F}_q$. We will now write $\mathrm{GL}_n(q)$ for the group $\mathrm{GL}_n(\mathbb{F}_q)$.

Proposition 3.6

We have

$$\begin{aligned}|\mathrm{GL}_n(q)| &= (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})\\ &= \prod_{i=0}^{n-1}(q^n-q^i)\\ &= q^{\frac{1}{2}n(n-1)}\prod_{i=1}^{n}(q^i-1).\end{aligned}$$

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 if and only if its rows are linearly independent vectors in $V=\mathbb{F}_q^n$. For such a matrix, denoting its rows by $r_1,\dots,r_n$,

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

□

Proposition 3.7

$\mathrm{SL}_n(q)\triangleleft \mathrm{GL}_n(q)$ and

$$\mathrm{SL}_n(q) = \frac{|\mathrm{GL}_n(q)|}{q-1}.$$

Proof. Denote $\mathbb{F}_q^*$ the multiplicative group $\mathbb{F}_q\setminus\{0\}$. The homomorphism $\det:\mathrm{GL}_n(q)\to\mathbb{F}_q^*$ has kernel $\mathrm{SL}_n(q)$ and image $\mathbb{F}_q^*$ of order $q-1$. □

Proposition 3.8

The centres of these groups are given by

$$\begin{aligned}Z_{\mathrm{GL}} &= Z(\mathrm{GL}_n(\mathbb{F})) = \{\lambda I_n : \lambda\in\mathbb{F}^*\},\\ Z_{\mathrm{SL}} &= Z(\mathrm{SL}_n(\mathbb{F})) = \{\lambda I_n : \lambda^n = 1\}.\end{aligned}$$

Definition 3.9. The **projective linear group** $\mathrm{PGL}_n(\mathbb{F})$ and **projective special linear group** $\mathrm{PSL}_n(\mathbb{F})$ are defined by

$$\mathrm{PGL}_n(\mathbb{F}) = \mathrm{GL}_n(\mathbb{F})/Z_{\mathrm{GL}} \quad\text{and}\quad \mathrm{PSL}_n(\mathbb{F}) = \mathrm{SL}_n(\mathbb{F})/Z_{\mathrm{SL}}.$$

Lemma 3.10. For $\mathbb{F}_q$ we have that

$$|Z_{\mathrm{GL}}| = q - 1 \quad \text{and} \quad |Z_{\mathrm{SL}}| = \gcd(n, q-1).$$

Proposition 3.11

We have that

$$|\mathrm{PSL}_n(q)| = \frac{1}{\gcd(n, q-1)(q-1)} q^{\frac{1}{2}n(n-1)} \prod_{i=1}^{n} (q^i - 1).$$

In particular,

$$|\mathrm{PSL}_2(q)| = \frac{q(q^2-1)}{\gcd(2, q-1)}.$$

Example 3.12

We have the following:

- $|\mathrm{PSL}_2(2)| = 6$.
- $|\mathrm{PSL}_2(3)| = 12$.
- $|\mathrm{PSL}_2(4)| = |\mathrm{PSL}_2(5)| = 60$.
- $|\mathrm{PSL}_2(7)| = 168$.
- $|\mathrm{PSL}_2(8)| = 504$.

For the next theorem, the proof resembles that of the simplicity of A_n. Commutators play an essential role, and we also use a special generating set. For A_n, this was the 3-cycles; for $SL_n(q)$ (and hence $PSL_n(q)$), it is the **elementary matrices**.

Definition 3.13. Recall: an **elementary matrix** $E_{ij}(\lambda)$ over a field F, for $i \neq j$, is defined by:

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

where $\lambda \in F$, and E_{ij} is the matrix with 1 in the ij-entry and 0 elsewhere.

Proposition 3.14. Let $A \in GL_n(F)$ with $\det(A) = \mu$. Then $A = UD(\mu)$, where U is a product of elementary matrices and $D(\mu) = \mathrm{diag}(1, \ldots, 1, \mu)$.

Proof. This follows from Gaussian elimination. Suppose A has rows $r_1, \ldots, r_n$. Each operation of the form $E_{ij}(\lambda)$ adds λr_j to r_i, preserving row structure.

Let $A = (a_{ij})$. Start with column 1:

- Use a row operation to ensure $a_{21} \neq 0$,
- Then add $a_{21}^{-1}(1 - a_{11})r_2$ to r_1 to set $a_{11} = 1$,
- Subtract suitable multiples of r_1 from other rows to zero the first column.

This gives a matrix U_1A with first column $(1, 0, \ldots, 0)^T$, where U_1 is a product of elementary matrices. Repeat this process for columns 2 through $n-1$ to obtain:

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

where again U_{n-1} is a product of elementary matrices. Clear the last column to obtain $U_nA = D(\mu)$, so $A = U_n^{-1}D(\mu)$. As the inverse of a product of elementary matrices is again a product of elementary matrices, the result follows. □

Corollary 3.15

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

Exam Questions 3.16 (Mastery Question 2023)

Prove teh above corollary (4 marks).

Solution. *Proof.* Let $A \in SL_n(F)$. Recall that if $r_1, \ldots, r_n$ are the rows of A, 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_1A with first column $(1, 0, \ldots, 0)^\top$, 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. Since $\det(A) = 1$, we have $\mu = 1$. Finally, clearing the last column gives $U_nA = I_n$. Then $A = U_n^{-1}$. Since the inverse of an elementary matrix is also elementary, this shows that A is a product of elementary matrices. Hence $SL_n(F)$ is generated by the elementary matrices. □

3.2.1 Simplicity of PSL$(2, q)$

Proposition 3.17

For $q > 3$, the group $\mathrm{PSL}_2(q)$ is simple.

Remark 3.18. We have that $\mathrm{PSL}_2(2) \cong S_3$ and $\mathrm{PSL}_2(3) \cong A_4$.

Two proofs of the theorem

We will give two proofs. The first is based on a famous lemma of Iwasawa and the second is a direct proof.

First proof 1 - Iwasawa

This approach uses a permutation action of $PSL_2(q)$ that is *2-transitive*.

Definition 3.19. Let G be a group acting on a set Ω. The action is **2-transitive** if for any two ordered pairs $(\alpha_1, \beta_1), (\alpha_2, \beta_2)$ of distinct elements of Ω (i.e., $\alpha_i \neq \beta_i$), there exists $g \in G$ such that

$$g(\alpha_1) = \alpha_2 \quad \text{and} \quad g(\beta_1) = \beta_2.$$

Note 3.20. In other words, not only can the group send any point to any other (which is what transitivity means), but it can do so while also simultaneously sending a second point to a second specified target — provided the points are all distinct.

Example 3.21

Some examples.

- The symmetric group S_n acts 2-transitively on $\{1, 2, \ldots, n\}$ because you can permute any pair of distinct elements to any other pair.
- The alternating group A_n also acts 2-transitively on $\{1, \ldots, n\}$ when $n \geq 4$, but not for $n \leq 3$. This is because A_n, being the even permutations, lacks enough flexibility in small degrees to match arbitrary pairs.
- Visualising this: if you imagine labelling chairs with numbers and reassigning students, a 2-transitive group means you can always swap any two students into any two seats, while maintaining the group's structure.

Now let $H = SL_2(F)$ where F is a field, and let $V = F^2$ be the 2-dimensional vector space over F. Define

$$\Omega = \{\langle v \rangle : v \in V \setminus \{0\}\},$$

the set of 1-dimensional subspaces of V.
Define an action of H on Ω: for $g \in H$, $g \cdot \langle v \rangle = \langle g(v) \rangle$.

Lemma 3.22

This action of $H = SL_2(F)$ is 2-transitive, and its kernel is $Z = \{\pm I\}$.

Proof. Let $(\langle v_1 \rangle, \langle v_2 \rangle)$ and $(\langle w_1 \rangle, \langle w_2 \rangle)$ be two ordered pairs of distinct 1-spaces. Since both pairs span V, there exists $g \in GL_2(F)$ with

$$g(v_1) = w_1, \quad g(v_2) = w_2.$$

Let $\lambda = \det(g)$, and define $h = \lambda^{-1} g$, so that $h \in SL_2(F) = H$, and h sends $v_1 \mapsto w_1$, $v_2 \mapsto w_2$. Thus, the action is 2-transitive.

Now consider the kernel of the action. Let $k \in \ker(H \to \mathrm{Sym}(\Omega))$, i.e., $k \cdot \langle v \rangle = \langle v \rangle$ for all v. Then k fixes all 1-dimensional subspaces. For the standard basis $\{e_1, e_2\}$, we must have

$$k(e_1) = \alpha e_1, \quad k(e_2) = \beta e_2, \quad k(e_1 + e_2) = \gamma(e_1 + e_2),$$

for some scalars α, β, γ. But then $\alpha = \beta = \gamma$, so $k = \alpha I$, and $\det(k) = \alpha^2 = 1 \Rightarrow \alpha = \pm 1$.
Hence $\ker = \{\pm I\}$. □

Remark 3.23. Since $PSL_2(q) = SL_2(F)/\{\pm I\}$, we obtain the following.

Corollary 3.24
Let $G = PSL_2(F)$, and $\Omega = \{\langle v\rangle : v \in V \setminus \{0\}\}$. Then $G \leq \mathrm{Sym}(\Omega)$ acts 2-transitively.

Theorem 3.25 (Iwasawa's Lemma)
Let $G \leq \mathrm{Sym}(\Omega)$ be a finite 2-transitive permutation group. Assume the following conditions on G:

1. For every $\alpha \in \Omega$, there exists $U \triangleleft G_\alpha$ such that:
   - U is abelian,
   - $\langle gUg^{-1} : g \in G\rangle = G$ (i.e., the normal closure of U in G is all of G).
2. $G = G'$, i.e., G is equal to its own commutator subgroup (it is **perfect**).

Then G is simple.

Proof. Suppose $1 \neq N \triangleleft G$. We aim to show that $N = G$.

- **Claim 1:** N is transitive on Ω. *Proof.* Pick any $n \in N \setminus \{1\}$, and $\alpha, \beta \in \Omega$ such that $n(\alpha) = \beta \neq \alpha$. By 2-transitivity of G, for any $\gamma \in \Omega \setminus \{\alpha\}$, there exists $g \in G$ such that
$$g(\alpha) = \alpha, \quad g(\beta) = \gamma.$$
Then $gng^{-1} \in N$, and $gng^{-1}(\alpha) = g(\beta) = \gamma$, so $\alpha^N = \Omega$.
- **Claim 2:** For any $\alpha \in \Omega$, $NG_\alpha = G$. *Proof.* Let $g \in G$, and let $\beta = g(\alpha)$. By Claim 1, there exists $n \in N$ such that $n(\alpha) = \beta$. Then $n^{-1}g \in G_\alpha \Rightarrow g \in NG_\alpha$.
- **Claim 3:** Let $U \triangleleft G_\alpha$ be as in (i). Then $NU \triangleleft G$. *Proof.* Since $N \triangleleft G$ and $U \triangleleft G_\alpha$, we have:
$$NU \triangleleft NG_\alpha = G \quad \text{(by Claim 2)}.$$
- **Claim 4:** $NU = G$. *Proof.* From Claim 3, $NU \triangleleft G$, and by assumption (i), the normal closure of U in G is the whole of G, i.e., $G = \langle gUg^{-1}\rangle \subseteq NU$. Thus $NU = G$.

We now finish the proof. By Claim 4 and the Second Isomorphism Theorem,
$$G/N = NU/N \cong U/(U \cap N).$$
Since U is abelian, the quotient is abelian. So G/N is abelian. But $G = G'$ by assumption (2), so G/N must also be perfect. The only group that is both abelian and perfect is the trivial group. Hence $G/N = 1 \Rightarrow N = G$.

We conclude that any nontrivial normal subgroup $N \triangleleft G$ must be all of G. Therefore, G is simple. □

We now prove the main theorem.

Proof. Let $G = PSL_2(q)$ with $q > 3$, and consider the 2-transitive action of G on Ω, as in Corollary 3.9. Recall that $G = SL_2(q)/Z$, where $Z = \{\pm I\}$, and elements of G are represented as gZ for $g \in SL_2(q)$.

Let $V = \mathbb{F}_q^2$, and fix the standard basis e_1, e_2. Define $\alpha = \langle e_1 \rangle \in \Omega$. Then the stabiliser of α in G, denoted G_α, consists of elements in G that fix the line spanned by e_1.

Every such matrix in $SL_2(q)$ must send $e_1 \mapsto ae_1$, so:

$$G_\alpha = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} : a \in \mathbb{F}_q^*, b \in \mathbb{F}_q \right\} \Big/ Z.$$

Define the subgroup

$$U = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} Z : b \in \mathbb{F}_q \right\} \cong (\mathbb{F}_q, +).$$

Then $U \triangleleft G_\alpha$, and U is abelian, satisfying part (1) of Iwasawa's lemma.

To verify the second part of condition (1), consider $n = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in SL_2(q)$. Then:

$$nUn^{-1} = \left\{ \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} Z : b \in \mathbb{F}_q \right\}.$$

By a previous corollary, elementary matrices generate $SL_2(q)$, and since U and nUn^{-1} generate these elementary matrices, we have:

$$\langle U, nUn^{-1} \rangle = G.$$

Thus condition (1) of Iwasawa's lemma is satisfied.

To verify condition (2), we must show $G = G'$, i.e., that G is perfect. We show that the commutator subgroup G' contains a generating set of G. Let $a \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$, and consider:

$$\left[\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & ba^2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b(a^2-1) \\ 0 & 1 \end{pmatrix}.$$

Since $q > 3$, there exists $a \in \mathbb{F}_q \setminus \{0, \pm 1\}$ so that $a^2 \neq 1$, implying that G' contains elements of the form

$$\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix},$$

i.e., $G' \supseteq U$. But we also have $G' \supseteq nUn^{-1}$, and thus G' contains a generating set for G. Hence:

$$G' = G.$$

Both conditions (1) and (2) of Iwasawa's lemma are satisfied. Therefore, $G = PSL_2(q)$ is simple. □ □

Second proof - direct approach

Let $G = SL_2(q)$ with $q > 3$, and let N be a normal subgroup of G such that

$$Z_{SL} < N \triangleleft G,$$

where $Z_{SL} = \{\pm I\}$ is the centre. We aim to show $N = G$, which implies that $G/Z_{SL} = PSL_2(q)$ is simple.

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

  Proof. Let
  $$U_{12} = \{E_{12}(\beta) : \beta \in \mathbb{F}_q\} \cong (\mathbb{F}_q, +).$$
  Observe that for any $\alpha \in \mathbb{F}_q^*$, we compute:
  $$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{pmatrix} = E_{12}(\lambda\alpha^2).$$
  Hence, conjugation allows us to generate
  $$\{E_{12}(\lambda\alpha^2) : \alpha \in \mathbb{F}_q^*\}.$$
  Since the squares in $\mathbb{F}_q^*$ form a subgroup of index 2, this set has size at least $\frac{q-1}{2}$, which is greater than $\frac{q}{2}$. So $U_{12} \leq N$.

  Similarly, using
  $$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} E_{12}(\lambda) \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = E_{21}(\lambda),$$
  we get $U_{21} \leq N$. Since $SL_2(q)$ is generated by U_{12} and U_{21} (Corollary 3.7), it follows that $N = SL_2(q) = G$.

- **Step 2:** If N contains a matrix of the form
  $$A = \begin{pmatrix} \alpha & 0 \\ \beta & \alpha^{-1} \end{pmatrix} \quad \text{for } \alpha \notin \{\pm 1\},$$
  then $N = G$.

  Proof. Since $N \triangleleft G$, it also contains the commutator:
  $$[E_{21}(1), A] = E_{21}(1 - \alpha^2).$$
  As $\alpha \notin \{\pm 1\}$, we get $E_{21}(\lambda) \in N$ for some $\lambda \neq 0$, and hence by Step 1, $N = G$.

- **Final Step:** Assume N contains no element as in Step 2. Let $n \in N \setminus Z_{SL}$. Since $n \notin Z_{SL}$, n is not diagonalisable, so its minimal polynomial is irreducible:
  $$x^2 - \beta x + 1 \quad \text{for some } \beta \in \mathbb{F}_q.$$
  By the Rational Canonical Form theorem, there exists $y \in GL_2(q)$ such that:
  $$y^{-1}ny = \begin{pmatrix} 0 & -1 \\ 1 & \beta \end{pmatrix}.$$

Let $\mu = \det(y)$, so $y = gD(\mu)$ with $g \in SL_2(q)$, and:

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

Now compute the commutator:

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

This is of the form 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 $\alpha^4 \neq 1$ (this is always possible if $q > 5$). So $n'' \in N$ is of the form in Step 2, and hence $N = G$.

Exceptional Case: If $q = 5$, then take $\alpha = 2$, so $\alpha^2 = -1$. Then

$$n'' = (\text{a non-identity unipotent matrix}) \in N,$$

i.e., n'' is of the form $E_{12}(\lambda)$ with $\lambda \neq 0$. Hence Step 1 applies, and the proof is complete.

In all cases, $N = SL_2(q)$, so $PSL_2(q) = G/Z_{SL}$ is simple.

4 The Sylow theorems

4.1 p-groups

> **Note 4.1.** The order of a group G has consequences for its structure. A rough rule of thumb is that the more complicated the prime factorisation of $|G|$, the more complicated the group.

Definition 4.2. If p is a prime, then a p-group is a group in which every element has order of a power of p.

Lemma 4.3 ([2, Lemma 4.1.])**.** If G is a finite Abelian group whose order is divisible by a prime p, then G contains an element of order p.

Theorem 4.4 ([2, Theorem 4.2.])
If G is a finite group whose order is divisible by p, then G contains an element of order p.

> **Note 4.5.** In this theorem, we have removed the hypothesis that G is Abelian from the lemma preceding it.

Corollary 4.6

A few corollaries.

- A finite group G is a p-group if and only if $|G|$ is a power of p [2, Corollary 4.3.].
- If $G \neq 1$ is a finite p-group, then its centre $Z(G) \neq 1$ [2, Theorem 4.4.].
- If p is a prime, then every group G of order p^2 is Abelian [2, Corollary 4.5.].
- Let G be a finite p-group. if $H < G$, then $H < N_G(H)$ [2, Theorem 4.6.].

4.2 The theorems

Note 4.7. 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. For example A_4 is of order 12 but has no subgroups of order 6.

Definition 4.8. Let $|G| = p^a m$, where p is a prime and $p \nmid m$. A subgroup of G of order p^a is called a **Sylow p-subgroup** of G. We write $\mathrm{Syl}_p(G)$ for the set of all Sylow p-subgroups of G. We define

$$n_p(G) = \left|\mathrm{Syl}_p(G)\right|,$$

the number of Sylow p-subgroups of G.

Proposition 4.9

Some facts about Sylow p-subgroups.

- Let $P \in \mathrm{Syl}_p(G)$, for $g \in G$, the conjugate ${}^gP = gPg^{-1}$ is also a subgroup of order p^a hence, ${}^gP \in \mathrm{Syl}_p(G)$.
- G acts by conjugation on $\mathrm{Syl}_p(G)$.
- The stabiliser of P in the conjugation action is

  $$N_G(P) = \left\{g \in P : gPg^{-1} = P\right\},$$

  the normaliser of P in G.

Lemma 4.10. Let $P \in \mathrm{Syl}_p(G)$, and let Q be a p-subgroup of G. If $Q \leq N_G(P)$, then $Q \leq P$.

Note 4.11. This lemma is used in the proof of the Sylow theorems II-IV.

Proof. Suppose $Q \leq N_G(P)$, then by a proposition previously stated we know that $PQ \leq G$, 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 $Q = P \cap Q$, hence $Q \leq P$. □

Theorem 4.12

The Sylow theorems.

- **Sylow I.** Let $|G| = p^a m$ where p is prime and $p \nmid m$. Then G has a subgroup of order p^a, i.e. it has a Sylow p-subgroup of order p^a.
- **Sylow II.** We have $n_p(G) \equiv 1 \pmod{p}$.
- **Sylow III.** Let Q be a p-subgroup of G (i.e. $|Q| = p^b$). Then there exists $P \in \mathrm{Syl}_p(G)$ such that $Q \leq P$.
- **Sylow IV.** G acts transitively by conjugation on $\mathrm{Syl}_p(G)$. That is, for any $P, Q \in \mathrm{Syl}_p(G)$, there exists a $g \in G$ such that $Q = gPg^{-1} =^g P$.

Note 4.13. We can interpret Sylow IV as: for a given prime, p the Sylow p-subgroups are conjugate to each other.

Proof. We prove each theorem in turn.

1. We proceed by induction on $|G|$. The base case $|G| = 1$ is trivial.

   Recall the **conjugacy class equation**:

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

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

   We consider two cases based on whether $p \mid |Z(G)|$ or not.

   - **Case 1:** $p \mid |Z(G)|$. By Cauchy's Theorem (for abelian groups), since $Z(G)$ is abelian and $p \mid |Z(G)|$, there exists an element $z \in Z(G)$ of order p. Then $\langle z \rangle \triangleleft G$, as $z \in Z(G)$. By the induction hypothesis, the quotient group $G/\langle z \rangle$ has a subgroup $P/\langle z \rangle$ of order p^{a-1}. Thus, $|P| = p^a$, giving the result in this case.
   - **Case 2:** $p \nmid |Z(G)|$. By the class equation, there must exist some non-central conjugacy class x_i^G such that $p \nmid |x_i^G|$. By a previous proposition, we have:

     $$|x_i^G| = [G : C_G(x_i)],$$

     so $p^a \mid |G| \Rightarrow p^a \mid |C_G(x_i)|$.

   Since x_i is non-central, $C_G(x_i) < G$. By induction, $C_G(x_i)$ has a subgroup of order p^a, completing the proof.

2. Let $P \in \mathrm{Syl}_p(G)$, and consider the action of P on $\mathrm{Syl}_p(G)$ by conjugation:

   $$x \cdot Q = xQx^{-1} \quad \text{for } x \in P.$$

   Then $\{P\}$ is a fixed point (i.e., an orbit of size 1).

Suppose there is another orbit $\{Q\}$ of size 1. Then $xQx^{-1} = Q$ for all $x \in P$, which implies $P \leq N_G(Q)$. By Lemma 4.6, $P, Q \in \mathrm{Syl}_p(G)$ and $P \leq Q \Rightarrow P = Q$, since they are both of the same order.

Hence, there is exactly one orbit of size 1 in this action. All other orbits have size divisible by $|P|$, hence divisible by p. Therefore, the total number of Sylow p-subgroups satisfies:

$$|\mathrm{Syl}_p(G)| = n_p(G) \equiv 1 \mod p. \qquad \square$$

3. Let Q be a p-subgroup of G, and consider the action of Q on $\mathrm{Syl}_p(G)$ by conjugation. By Sylow II, $n_p(G) \equiv 1 \mod p$, so not all orbits of this action can have size divisible by p. There exists an orbit of size 1, say $\{P\}$, where $P \in \mathrm{Syl}_p(G)$. Then $Q \leq N_G(P)$, and hence $Q \leq P$ by the lemma above.

4. Let $P \in \mathrm{Syl}_p(G)$, and define the orbit of P under the action of G by conjugation as:
$$\Omega = \{{}^gP : g \in G\}.$$
This is the orbit of G acting on $\mathrm{Syl}_p(G)$, so $\Omega \subseteq \mathrm{Syl}_p(G)$.

   By Sylow II, P has an orbit of size 1 under its own conjugation action, and all other orbits have size divisible by p. Hence, $|\Omega| \equiv 1 \mod p$.

   Now let $Q \in \mathrm{Syl}_p(G)$, and consider the action of Q on Ω by conjugation. Again, by Sylow II, there is an orbit of size 1, say $\{R\} \subseteq \Omega$, such that $Q \leq N_G(R)$. By the lemma above, $Q = R$. Therefore, $Q \in \Omega$, and since $Q \in \mathrm{Syl}_p(G)$ was arbitrary, it follows that
$$\Omega = \mathrm{Syl}_p(G),$$
   so the action of G on $\mathrm{Syl}_p(G)$ by conjugation is transitive.

$\square$

Corollary 4.14

Let $P \in \mathrm{Syl}_p(G)$, then the following hold:

1. $n_p(G) = |G : N_G(P)|$,
2. $n_p(G) \mid |G|$,
3. $n_p(G) = 1 \iff P \triangleleft G$.

Proof. We prove each statement in turn.

1. By Sylow IV, the group G acts transitively on the set of Sylow p-subgroups $\mathrm{Syl}_p(G)$. The stabiliser of a Sylow subgroup P under this action is its normaliser $N_G(P)$. By the orbit-stabiliser theorem,
$$|\mathrm{Orb}(P)| = [G : N_G(P)] = n_p(G),$$
   which proves 1.

2. Since $n_p(G) = |G : N_G(P)|$, and $|N_G(P)| \mid |G|$, it follows that $n_p(G) \mid |G|$.
3. We have $n_p(G) = 1 \iff [G : N_G(P)] = 1 \iff N_G(P) = G \iff P \triangleleft G$.

□

4.3 Sylow arithmetic

Example 4.15 (Summary)

Let G be a finite group and p a prime. We summarise the previous section:

1. $\mathrm{Syl}_p(G) \neq \varnothing$.
2. G acts transitively by conjugation on $\mathrm{Syl}_p(G)$.
3. If $n_p(G) = \left|\mathrm{Syl}_p(G)\right|$, then $n_p(G) \equiv 1 \pmod{p}$.
4. If $P \in \mathrm{Syl}_p(G)$, then $n_p(G) = |G : N_G(P)|$ and this divides $|G|$.
5. $n_p(G) = 1 \iff P \triangleleft G$.

Note 4.16. These facts can be used to study group via "Sylow arithmetic".

Proposition 4.17

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

1. G has a normal Sylow p-subgroup.
2. If also $q \nmid p - 1$, then $G \cong C_{pq}$.

Proof. We prove each statement in turn.

1. By Sylow's Theorem, the number of Sylow p-subgroups satisfies $n_p(G) = 1$ or q. Since $p > q$, we have $q \nmid p - 1$, hence $q \not\equiv 1 \pmod{p}$. So $n_p(G) = 1$, and thus the Sylow p-subgroup $P \in \mathrm{Syl}_p(G)$ is normal in G: $P \triangleleft G$.
2. Suppose now that $q \nmid p - 1$. Then $p \not\equiv 1 \pmod{q}$, and hence the number of Sylow q-subgroups is $n_q(G) = 1$, so $Q \in \mathrm{Syl}_q(G)$ is also normal in G: $Q \triangleleft G$.

   We now have:

   $$P \triangleleft G, \quad Q \triangleleft G, \quad P \cap Q = \{1\}, \quad |PQ| = |P||Q| = pq = |G|.$$

   Hence $G = PQ$, and by Proposition 1.5, we conclude:

   $$G \cong P \times Q \cong C_p \times C_q \cong C_{pq}.$$

   (Since p, q are distinct primes, the cyclic groups of order p and q are coprime, so the product is cyclic of order pq.)

□

Example 4.18. Suppose we have a group G, such that $|G| = 15$. Then $G \cong C_{15}$.

Proposition 4.19
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 not, i.e., assume $n_p(G) > 1$ and $n_q(G) > 1$. Then by Sylow's Theorem, we must have $n_p(G) \equiv 1 \mod p$, and since $n_p(G) \mid q$, it follows that $n_p(G) = q$. Thus $q \equiv 1 \mod p$.

Now $n_q(G) = p$ or p^2. If $n_q(G) = p$, then $p \equiv 1 \mod q$, so $p > q$. But then $q \equiv 1 \mod p$ and $p > q$ cannot both hold — contradiction. Thus $n_q(G) = p^2$.

Now consider the number of elements of order q. Each Sylow q-subgroup has $q - 1$ such elements, and distinct Sylow q-subgroups intersect trivially. So:

$$\left| \bigcup_{Q \in \mathrm{Syl}_q(G)} (Q \setminus \{1\}) \right| = p^2(q-1) = |G| - p^2.$$

Hence the remaining p^2 elements must lie in the Sylow p-subgroups. Let $P \in \mathrm{Syl}_p(G)$. Since $|P| = p^2$, this forces P to be the only such subgroup: $n_p(G) = 1$ — contradiction. Therefore, at least one Sylow subgroup must be normal. □

Proposition 4.20
Let $|G| = p^3q$, with p, q prime. Then ONE of the following holds:

1. G has either a normal Sylow p-subgroup OR a normal Sylow q-subgroup.
2. $|G| = 24 = 2^3 \cdot 3$.

Example 4.21
S_4 is a group of order 24 with no normal Sylow 2-subgroup or Sylow 3-subgroup.

4.4 The orders of simple groups

Note 4.22. 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.

Example 4.23 (Trick)
We have the following divisibility condition. Given a group G, such that $|G| = p^a m$ then,

$$n_p(G) \mid \frac{|G|}{p^a}.$$

Proposition 4.24
Let $|G| = p^a m$, where p is prime, $a \geq 1, m \geq 2$ and $p \nmid m$. Suppose G is simple then,

1. $n_p(G) \mid m$ (this does not rely on the simplicity assumption),
2. $n_p(G) \equiv 1 \pmod{p}$ and $n_p(G) > 1$,
3. $|G| \mid n_p(G)!$.

Proof. Parts (1) and (2) follow from Sylow's Theorem. Since G is simple, a Sylow p-subgroup cannot be normal, so $n > 1$. For (3), let $\Omega = \mathrm{Syl}_p(G)$, so $|\Omega| = n$. Then G acts transitively on Ω by conjugation (Sylow IV), giving a homomorphism:

$$\varphi : G \to \mathrm{Sym}(\Omega) \cong S_n.$$

As G is simple, either $\ker(\varphi) = 1$ or $\ker(\varphi) = G$. But the action is nontrivial, so $\ker(\varphi) = 1$, and $G \hookrightarrow S_n$, so:

$$|G| \mid |S_n| = n!.$$

□

Proposition 4.25. If G is a non-Abelian simple group such that $|G| \leq 100$, then $|G| = 60$ and $G \cong A_5$.

Sketch of proof. This is guided by previous results and exercises. We rule out:

- Prime power orders.
- Orders of the form pq, p^2q, p^3q.

What remains for $|G| \leq 100$ are:

$$24, 30, 36, 42, 48, 60, \ldots, 100.$$

All can be eliminated using Sylow theorems, except 60. For example: suppose $|G| = 24 = 2^3 \cdot 3$, and G is simple. Then $n_2(G) = 3$ (by Prop. 4.10), so $|G| \mid 3! = 6$, a contradiction. The hard part is to show that the only simple group of order 60 is A_5. This requires careful application of Sylow theorems □

Example 4.26 (Practice test 1 Q2)

For which of the following numbers n does there exist a simple group of order n:

1. $n = 27$.
   Since 27 is prime this group is cyclic (i.e. $\mathbb{Z}/27\mathbb{Z}$). Every subgroup of a cyclic group is normal hence, this group cannot be simple.

2. $n = 36$.
   Let $|G| = 2^2 3^2$. To determine if a simple group of this order exists we study its Sylow subgroups and see if we reach a contradiction in one of the propositions. We assume G is simple. Then $n_3(G) \equiv 1 \pmod 3$ and $n_3(G) \mid 4$ hence, $n_3(G) = 4$. By one of the propositions in this section we must have that $|G| \mid n_3(G)! = 4!$, which is clearly a contradiction. We conclude that no such simple group exists.

3. $n = 360$.
   We notice that $360 = \frac{1}{2} \cdot 720 = \frac{1}{2}6!$. There exists a group of order $\frac{1}{2}6!$ which is simple, namely A_6.

4. $n = 280$.
   We proceed with a similar approach as before. Let $|G| = 2^3 \cdot 5 \cdot 7 = 280$ and assume that G is a simple group. Applying Sylow's theorems, we find:

   - $n_5(G) \equiv 1 \mod 5$,
   - $n_5(G) > 1$ (since G is assumed to be simple),
   - $n_5(G) \mid \frac{|G|}{5} = 56$.

   From these conditions, we conclude that $n_5(G) = 56$. By a similar argument, we find $n_7(G) = 8$.

   Now, consider two distinct Sylow 5-subgroups, P_1 and P_2, of order 5. Since $P_1 \cap P_2 = 1$, all non-identity elements in each P_i must have order 5 (by Lagrange's theorem). Thus, if $N_5(G)$ denotes the total number of elements of order 5 in G (since elements in the same conjugacy class have the same order), we have:

   $$N_5(G) = 56 \cdot 4 = 224,$$

   since there are 56 Sylow 5-subgroups, each contributing 4 elements of order 5.

   Similarly, for the Sylow 7-subgroups, we find that $N_7(G) = 8 \cdot 6 = 48$ elements of order 7.

   This leaves:

   $$280 - 224 - 48 = 8$$

   elements unaccounted for, which must belong to the Sylow 2-subgroup(s). Since there are exactly 8 elements remaining, they must all form a single Sylow 2-subgroup of order 8. Consequently, there is only one Sylow 2-subgroup, meaning it is normal in G.

   This contradicts the assumption that G is simple, as a simple group cannot have non-trivial normal subgroups. Therefore, we conclude that no simple group of order 280 exists.

5 Extensions and semidirect products

Note 5.1. A group G having normal subgroups K can be "factored" into K and G/K. The study of extensions involves the inverse question: given $K \triangleleft G$ and G/K, to what extent can one recapture G?

Definition 5.2. If N and H are groups, then an **extension** of N by H is a group G such that

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

We represent this by a sequence

$$1 \to N \xrightarrow{\phi} G \xrightarrow{\psi} H \to 1$$

where ϕ is injective, ψ is surjective and $\ker(\psi) = \mathrm{Im}(\phi)$ i.e. it is a short exact sequence (in this setup the normal subgroup $N_0 = \mathrm{Im}(\phi)$).

Note 5.3. Therefore, we can say that G is an extension of N by H if we can find a short exact sequence as above.

Example 5.4

An example of a short exact sequence is

$$1 \to N \to G \to G/N \to 1.$$

Example 5.5. Some examples.

- C_4 and $C_2 \times C_2 \cong V_4$ are both extensions of C_2 by C_2.
- S_4 is an extension of $V_4 \cong C_2 \times C_2$ by S_3, since $V_4 \triangleleft S_4$ and $S_4/V_4 \cong S_3$.
- A_4 is an extension of V_4 by C_3 [2, Exercise 7.2.].
- If p is a prime, every non-Abelian group of order p^3 is an extension of C_p by $C_p \times C_p$ [2, Exercise 7.3.].

Example 5.6

Let p be a prime, and define the subgroup

$$G = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{pmatrix} : \alpha \in \mathbb{F}_p^*, \beta \in \mathbb{F}_p \right\} \leq \mathrm{SL}_2(p).$$

Then G has subgroups

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

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

5.1 The extension problem

Note 5.7. Given N and H can we find (up to isomorphism) all extensions of N by H? In general this is a very difficult question, but we prove it for extensions of a certain type.

Definition 5.8. Let G be a group with normal subgroup $N_0 \cong N$ and let $G/N_0 \cong H$; so G is an extension of N by H. We say that the extension is **split** if there exists a subgroup H_0 of G such that

$$G = N_0H_0 \quad \text{and} \quad N_0 \cap H_0 = 1.$$

Note that,

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

Note 5.9. In the language of short exact sequences, for a an extension to split we need to find a map $s : H \to G$ such that $\psi \circ s = \mathrm{id}_H$.

Example 5.10

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

5.2 Semidirect product

Suppose we have a split extension

$$G = NH \text{ such that } N \triangleleft G \text{ and } N \cap H = 1.$$

For $h \in H$, define the map

$$\iota_h : N \hookrightarrow N$$
$$\iota_h(n) = hnh^{-1}$$

for $n \in N$.

Proposition 5.11. Let $G = NH$ be a split extension as above.

1. Every $g \in G$ can be written as $g = nh$ for unique elements $n \in N$ and $h \in H$.
2. $\iota_h \in \mathrm{Aut}(N)$.
3. The map $\iota : H \to \mathrm{Aut}(N)$ sending $h \mapsto \iota_h$ is a homomorphism.
4. Multiplication in G is determined by the homomorphism ι, as follows:

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

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

Proof. We prove each statement in turn.

- Suppose $n_1h_1 = n_2h_2$. Then $n_2^{-1}n_1 = h_2h_1^{-1} \in N \cap H = \{1\}$, so $n_1 = n_2$, $h_1 = h_2$. Hence the representation is unique.
- ι_h is an automorphism, since for $n \in N$, we have:

$$\iota_h(n_1n_2) = hn_1n_2h^{-1} = (hn_1h^{-1})(hn_2h^{-1}) = \iota_h(n_1)\iota_h(n_2).$$

- For $h_1, h_2 \in H$,

$$\iota_{h_1h_2}(n) = h_1h_2nh_2^{-1}h_1^{-1} = \iota_{h_1}(\iota_{h_2}(n)) = (\iota_{h_1} \circ \iota_{h_2})(n).$$

  So ι is a homomorphism.
- Compute:

$$(n_1h_1)(n_2h_2) = n_1(h_1n_2h_1^{-1})h_1h_2 = (n_1 \cdot \iota_{h_1}(n_2))(h_1h_2).$$

□

5.2.1 The construction of $N \rtimes_\iota H$

Note 5.12. Given a split extension $G = NH$ there is a homomorphism $\iota : H \to \mathrm{Aut}(N)$ that determines the multiplication in G. In this section, we consider the converse. Given group N, H and a homomorphism $\iota : H \to \mathrm{Aut}(N)$, we will construct a split extension of N by H with the same multiplication outlined in the previous section.

Definition 5.13. The set of elements of the set $N \rtimes_\iota H$ is

$$\{(n, h) : n \in N, h \in H\}$$

with multiplication

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

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

Proposition 5.14. Let $X = N \rtimes_\iota H$ as defined above.

1. X is a group under the multiplication defined above.
2. Let

$$N_0 = \{(n, 1_H) : n \in N\} \text{ and } H_0 = \{(1_N, h) : h \in H\}.$$

   Then N_0 and H_0 are subgroups of X isomorphic to N, H respectively. Furthermore,
   - $N_0 \triangleleft X$,
   - $N_0 \cap H_0 = 1$, and
   - $X = N_0H_0$.
3. If $G = NH$ is a split extension with multiplication as in the previous section, then $G \cong N \rtimes_\iota H$.

Proof. We prove each statement in turn.

1. *Associativity:* For $n_i \in N, h_i \in H$, we compute:

   $$((n_1,h_1)(n_2,h_2))(n_3,h_3) = (n_1\iota_{h_1}(n_2), h_1h_2)(n_3,h_3) = (n_1\iota_{h_1}(n_2)\cdot\iota_{h_1h_2}(n_3), h_1h_2h_3),$$

   while:

   $$(n_1,h_1)((n_2,h_2)(n_3,h_3)) = (n_1\cdot\iota_{h_1}(n_2\cdot\iota_{h_2}(n_3)), h_1h_2h_3),$$

   and these are equal because ι_{h_1} is a homomorphism.

   Identity: $(1_N, 1_H)$.

   Inverses: For (n,h), the inverse is $(\iota_{h^{-1}}(n^{-1}), h^{-1})$.

2. The maps

   $$N \hookrightarrow X, \quad n \mapsto (n, 1_H), \qquad H \hookrightarrow X, \quad h \mapsto (1_N, h)$$

   are injective homomorphisms. Their images are N_0, H_0, which intersect trivially and generate X. We compute:

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

   so $N_0 \triangleleft X$.

3. Let $G = NH$ with multiplication as above. Define:

   $$\phi : N \rtimes_\iota H \to G, \quad \phi(n,h) = nh.$$

   Then ϕ is a bijection and a homomorphism:

   $$\phi((n_1,h_1)(n_2,h_2)) = \phi(n_1\cdot\iota_{h_1}(n_2), h_1h_2) = n_1\iota_{h_1}(n_2)h_1h_2 = n_1h_1n_2h_2 = \phi(n_1,h_1)\phi(n_2,h_2).$$

   Hence $G \cong N \rtimes_\iota H$. □

□

Example 5.15 (Summary)
To construct all split extensions of N by H:

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

Example 5.16. Suppose N and H are any group, and $\iota : H \to \mathrm{Aut}(N)$ is the trivial homomorphism (i.e. $\iota(h) = \mathrm{id}_N$ for all $h \in H$), then the multiplication in $N \rtimes_\iota H$ is

$$\begin{aligned}(n_1,h_1)(n_2,h_2) &= (n_1\iota_{h_1}(n_2), h_1h_2)\\ &= (n_1n_2, h_1h_2).\end{aligned}$$

Hence, $N \rtimes_{\mathrm{id}} H = N \times H$, the direct product.

Example 5.17. Let $G = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{pmatrix} : \alpha \in \mathbb{F}_p^*, \beta \in \mathbb{F}_p \right\} \leq \mathrm{SL}_2(p)$ i.e. the split extension of $\mathbb{F}_p^+$ by $\mathbb{F}_p^*$ from a previous example. We note that that for $\alpha \in \mathbb{F}_p^*$ and $\beta \in \mathbb{F}_p$ we have

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

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

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

Proposition 5.18

Let N, H be finite groups, and let $\iota, j : H \to \mathrm{Aut}(N)$ be homomorphisms. Suppose there exists $\alpha \in \mathrm{Aut}(N)$ and $\beta \in \mathrm{Aut}(H)$ such that the following diagram commutes

$$\begin{array}{ccc} H & \xrightarrow{\iota} & \mathrm{Aut}(N) \\ {\scriptstyle\beta}\downarrow & & \downarrow \\ H & \xrightarrow[j]{} & \mathrm{Aut}(N) \end{array}$$

(the map from $\mathrm{Aut}(N) \to \mathrm{Aut}(N)$ is conjugation by α) i.e. $j(\beta(h)) = \alpha\iota(h)\alpha^{-1}$ for all $h \in H$. Then $N \rtimes_\iota H \cong N \rtimes_j H$.

Note 5.19. This proposition is to determine when semidirect products are isomorphic.

Remark 5.20. The converse of the proposition does not hold, namely given that $N \rtimes_\iota H \cong N \rtimes_j H$ there does not exist automorphism α and β that satisfy the conditions in the proposition. For example, let $G = T \times T$ for some group T. Then $G \cong T \rtimes_\iota T \cong T \rtimes_j T$, where $\iota : T \to \mathrm{Aut}(T)$ is the trivial homomorphism and $j : T \to \mathrm{Aut}(T)$ is the homomorphism 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 automorphisms α, β that satisfy the condition of the proposition.

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

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

This is a bijection since α and β are automorphisms.

We check ϕ is a homomorphism. Let $(n_1, h_1), (n_2, h_2) \in N \rtimes_\iota H$. Then:

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

On the other hand:

$$\begin{aligned} \phi((n_1, h_1)(n_2, h_2)) &= \phi(n_1 \cdot \iota_{h_1}(n_2), h_1h_2) \\ &= (\alpha(n_1 \cdot \iota_{h_1}(n_2)), \beta(h_1h_2)) \\ &= (\alpha(n_1) \cdot \alpha(\iota_{h_1}(n_2)), \beta(h_1)\beta(h_2)). \end{aligned} \tag{5.4}$$

By the hypothesis (5.2), we have

$$j_{\beta(h_1)}(\alpha(n_2)) = \alpha(\iota_{h_1}(n_2)).$$

Thus, the right-hand sides of (5.3) and (5.4) are equal, so ϕ is a homomorphism. Hence ϕ is an isomorphism. □

Example 5.21

Find (up to isomorphism) all the split extension of $C_2 \times C_2 \cong V_4$ by C_3.

Solution. To do so we need to find all homomorphisms

$$\iota : C_3 \to \mathrm{Aut}(C_2 \times C_2).$$

From a problem sheet we know that $\mathrm{Aut}(C_2 \times C_2) \cong \mathrm{GL}_2(\mathbb{F}_2) \cong S_3$, so there are three such homomorphisms. Writing $C_3 = \langle x \rangle$ they are

1. ι_1, the trivial homomorphism
2. $\iota_2 : x \mapsto (123)$
3. $\iota_3 : x \mapsto (132)$

In the first case $G \cong C_2 \times C_2 \times C_3$. For the remaining cases we know that $A_4 = V_4 C_3$ is a split extension of $C_2 \times C_2$ by C_3 so $A_4 \cong (C_2 \times C_2) \rtimes_j C_3$ for some $j \in \iota_2, \iota_3$. The question is which one. We notice that the proposition above holds,

$$\begin{array}{ccc} \langle x \rangle & \xrightarrow{\iota_2} & S_3 \qquad (x \mapsto (123)) \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle\mathrm{id}} \\ \langle x \rangle & \xrightarrow[\iota_3]{} & S_3 \qquad (x \mapsto (132)) \end{array}$$

So the two remaining cases are isomorphic.

5.3 The groups of order pq

Proposition 5.22. We have that $\mathrm{Aut}(C_p) \cong \mathbb{F}_p^*$.

Proposition 5.23

Let p and q be primes such that $p > q$.

1. If $q \nmid p - 1$ then $G \cong C_{pq}$.
2. If $q \mid p - 1$ then $G \cong C_p \rtimes_\iota C_q$ where,

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

Proof. We classify groups G of order pq, where $p > q$ are primes.

By a previous proposition, if $q \nmid p-1$, then $G \cong C_{pq}$, proving part (1).

Assume now that $q \mid p-1$. Then by Sylow's Theorems, G has a normal Sylow p-subgroup $P \cong C_p$, and a Sylow q-subgroup $Q \cong C_q$. Since $P \triangleleft G$ and $Q \in \mathrm{Syl}_q(G)$, we can write $G = PQ$, with $P \cap Q = \{1\}$, so by a previous proposition, $G \cong C_p \rtimes_\iota C_q$ for some homomorphism

$$\iota : C_q \to \mathrm{Aut}(C_p).$$

If ι is trivial, then the semidirect product is the direct product:

$$C_p \rtimes_\iota C_q \cong C_p \times C_q \cong C_{pq}.$$

Now we examine nontrivial homomorphisms. Since

$$\mathrm{Aut}(C_p) \cong \mathbb{F}_p^\times,$$

and $\mathbb{F}_p^\times$ is cyclic of order $p-1$, it has a unique subgroup of order q, say $\langle a \rangle$. So we define an automorphism $\alpha \in \mathrm{Aut}(C_p)$ sending $x \mapsto x^a$, and hence define

$$\iota : C_q \to \mathrm{Aut}(C_p), \quad y \mapsto \alpha.$$

Any other homomorphism is of the form $\iota \circ \beta$, where $\beta \in \mathrm{Aut}(C_q)$, sending $y \mapsto y^i$. So by a previous proposition, all such semidirect products are isomorphic to the group with presentation:

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

where $a^q \equiv 1 \mod p$, and $a \not\equiv 1 \mod p$ (to be nontrivial). This gives a second group of order pq not isomorphic to C_{pq}, completing the proof. □

Proposition 5.24. Suppose N and H are finite Abelian groups of coprime orders. Then every extension of N by H splits.

Proof. On exercise sheet 3. □

Example 5.25. Let G be an extension of $V_4 \cong C_2 \times C_2$ by C_3 by the above proposition the extension splits, so by a previous example $G = C_2 \times C_2 \times C_3$ or A_4.

6 Soluble groups

Definition 6.1. A finite group G is **soluble** if it has a series of subgroups

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

where $N_i \triangleleft G$ and N_{i+1}/N_i is Abelian for all i.

Note 6.2. In American English we say 'solvable'.

Example 6.3

Some examples.

1. Abelian groups are soluble.
2. S_3 is soluble since $1 \triangleleft A_3 \cong C_3 \triangleleft S_3$.
3. However, for $n \geq 5$ the groups A_n and S_n are not soluble, since A_n is simple and S_n contains A_n.
4. D_n is soluble for all n since $1 \triangleleft \langle \rho \rangle \triangleleft D_n$.
5. Any finite p-group G is soluble [2, Theorem 5.19.]. We can construct a series with $N_0 = 1, N_1 = Z(G) \neq 1$ since the centre of p-groups is non-trivial. Then we choose N_i such that $N_2/N_1 = Z\left(G/N_1\right), N_3/N_2 = Z\left(G/N_2\right)$ and so on.
6. Let $G \leq \mathrm{GL}_n(q)$ be the subgroup of all upper triangular matrices. We have that is soluble.

   Proof. We can define the homomorphism $\phi : G \to (\mathbb{F}_q^*)^n$ such that $A \mapsto (\lambda_1, \ldots, \lambda_n)$ where λ_i are the diagonal entries. The kernel N is the subgroup of G of matrices with all diagonal entries 1. Then $N \triangleleft G$ and $G/N \cong (\mathbb{F}_q^*)^n$, which is Abelian. Since N is a p-group (where $q = p^a$) it has a series of normal subgroups N_i as defined in the previous example. Each N_i is characteristic in N hence, normal in G, which implies G is solvable. □
7. $\mathrm{GL}_2(2)$ is soluble since it is isomorphic to S_3.
8. For most values of n and q GL is not soluble as it contains SL.

Theorem 6.4 ([2, Corollary 5.18.])**.** If H and K are soluble groups, then $H \times K$ is soluble.

6.1 The derived series

Definition 6.5. For a finite group G, the **derived subgroup** is $G' = \langle [x, y] : x, y \in G \rangle$. Then define $G'' = (G')'$, and recursively,

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

Definition 6.6. The series

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

is called the **derived series** (or **commutator series**) of G.

Proposition 6.7. If $\phi : G \twoheadrightarrow H$ is a surjective homomorphism, then $\phi\left(G^{(i)}\right) = H^{(i)}$ for all i. Furthermore, $G^{(i)}$ char G for all i.

Proof. For $x, y \in G$

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

Hence, ϕ maps the set of commutators in G to the set of commutators in H. This map is surjective since ϕ is, thus $\phi(G') = H'$. Repeating this argument we arrive at the desired result. If we take $H = G$ we obtain the last assertion of the proposition. □

Proposition 6.8
A group G is solvable if and only if $G^{(r)} = 1$ for some r.

Proof. We prove each direction in turn.

- Proof of ($\Rightarrow$).
  Suppose $G^{(r)} = 1$, and consider the series
  $$1 = G^{(r)} \leq G^{(r-1)} \leq \cdots \leq G^{(1)} \leq G.$$
  We have that each $G^{(i)} \triangleleft G$, and each quotient $G^{(i)}/G^{(i+1)} = G^{(i)}/(G^{(i)})'$ is Abelian. Hence, G is soluble.
- Proof of ($\Leftarrow$).
  Suppose G is soluble, then there exists a series
  $$1 = N_0 \leq N_1 \leq \cdots \leq N_s = G$$
  such that $N_i \triangleleft G$ and N_{i+1}/N_i 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 $G^{(s)} \leq N_0 = 1$.

□

Definition 6.9. For a soluble group G, the **derived length** is defined by $dl(G) = \min\{r : G^{(r)} = 1\}$.

Example 6.10
Example.

1. Abelian group have derived length 1.
2. The commutator series of D_8 is
   $$1 \leq \langle \rho^2 \rangle \leq D_8$$
   which has derived length 2.

Proposition 6.11. We have the following.

1. Subgroups and quotient groups of soluble groups are soluble.
2. Suppose $N \triangleleft G$ and G/N are soluble, then G is soluble.

Proof. We prove each statement in turn.

1. Let G be soluble. If $H \leq G$, then $H' \leq G'$ and in general $H^{(i)} \leq G^{(i)}$. Since, G is soluble we have that $G^{(i)} = 1$ for some i hence, $H^{(i)} = 1$ for some i, which implies H is soluble.

   Let $N \triangleleft G$ and consider the natural surjective map $\phi : G \twoheadrightarrow G/N$. By a proposition from above, we have $\phi(G^{(i)}) = (G/N)^{(i)}$ for all i therefore, $(G/N)^{(i)} = 1$ for some i, hence G/N is soluble.

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

□

Proposition 6.12

Let G be a finite group, and let

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

be a composition series for G i.e. each $G_i \triangleleft G_{i+1}$ and each G_{i+1}/G_i is simple. Then G is soluble if and only if all the composition factors G_{i+1}/G_i are cyclic of prime order.

Proof. We prove each direction in turn.

- Proof of ($\Rightarrow$).
  Suppose G is solvable. Then by a previous proposition,each quotient G_i/G_{i-1} is solvable. We now show that any solvable simple group is cyclic of prime order. Let H be a solvable simple group. Then $H' \triangleleft H$ and $H' \neq H$, since H is not perfect (solvable). But H is simple, so $H' = 1$, hence H is abelian. Now H is also simple and abelian, so $H \cong C_p$ for some prime p. Hence each G_i/G_{i-1} is cyclic of prime order.

- Proof of ($\Leftarrow$).
  Conversely, suppose all the composition factors G_i/G_{i-1} are cyclic of prime order. Then G/G_{r-1} is abelian of prime order, so $G' \leq G_{r-1}$. Next, since G_{r-1}/G_{r-2} is abelian, we have $G'' \leq G_{r-2}$, and so on. Iterating this process gives $G^{(r)} = 1$, the trivial group, so G is solvable.

□

6.2 Theory of soluble groups

Definition 6.13. 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 6.14

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 theorem of finite Abelian groups it follows that $A \cong C_{p_1^{a_1}} \times \cdots \times C_{p_k^{a_k}}$, where each p_i is prime. The condition $x^p = 1$ for all x implies that $p_i^{a_i} = p$ for all i. □

Definition 6.15. Let $N \triangleleft G$. We say N is a **minimal normal subgroup** of G if $N \neq 1$ and $M \triangleleft G$ such that $M < N$ implies $M = 1$. That is, N contains no smaller non-trivial normal subgroups of G.

Example 6.16. V_4 is a minimal normal subgroup of S_4; and A_4 is not as it contains V_4.

Proposition 6.17

Let G be a finite group, and let N be a minimal normal subgroup of G. Suppose that N is soluble, then N is elementary Abelian.

Proof. Since N is solvable, its derived subgroup $N' < N$. Moreover, N' is characteristic in N, hence normal in G because $N \triangleleft G$. But N is a minimal normal subgroup of G, so $N' = 1$. Thus N is abelian.

Let p be a prime dividing $|N|$, and define

$$A = \{x \in N : x^p = 1\}.$$

Then A is a nontrivial subgroup of N (as N is abelian), and is characteristic in N. Hence $A \triangleleft G$. By minimal normality of N, we must have $A = N$. So every element of N has order dividing p, and N is abelian. Hence N is an elementary abelian p-group. □

Corollary 6.18. Minimal normal subgroups of soluble groups are elementary Abelian.

Definition 6.19. 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 $N_i \triangleleft G$, 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**.

Remark 6.20. We remark that there is a 'Jordan-Hölder theorem' about the uniqueness of the list of chief factors of a finite group, but this will not be proved.

Example 6.21. 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.

Corollary 6.22

All chief factors of a finite soluble group are elementary Abelian p-groups, for various primes p.

6.3 Hall's theorem

Note 6.23. The main results of this section are generalisation of the Sylow theorems that hold for (and, in fact characterise) finite soluble groups.

Definition 6.24. If π is a set of primes, then a **π-number** is an integer n all of whose prime factors lie in π. The complement of π is denoted by π', and so a **π'-number** is an integer n none of whose prime factors lie in π.

Example 6.25. For example, 12 is a $\{2,3\}$-number and a $\{2,3,7\}$ number, and also a $\{5,7\}'$-number.

Definition 6.26. A subgroup $H \leq G$ is a **π-subgroup** if $|H|$ is a π-number (so the order of its elements is a π-number).

Proposition 6.27 (Frattini argument)
Let $N \triangleleft G$ and let $P \in \mathrm{Syl}_p(N)$. Then $G = N_G(P)N$.

Proof. Let $g \in G$. Then $g^{-1}Pg \leq g^{-1}Ng = N$, so $g^{-1}Pg \in \mathrm{Syl}_p(N)$. 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 $G = N_G(P)N$. □

Exam Questions 6.28 (Q3 Exam 2021)
The questions.

(e) Give an application of the Frattini argument.

(f) Deduce the simplicity of A_7 from that of A_6.

Solution. We prove each part.

(e) It is used to show the normaliser of the normaliser of a Sylow subgroup is just the normaliser.

(f) Let N be a non-trivial normal subgroup of A_7. Then, $N \cap A_6$ is a normal subgroup of A_6, so either $N \cap A_6 = A_6$ or $N \cap A_6 = 1$. Since the action of A_7 on the 7-set is primitive, the action of N is transitive. If $N \cap A_6 = A_6$, then $N = A_7$ by the order reason. If $N \cap A_6 = 1$, then $|N| = 7$, $N \cong C_7$, which is impossible since by the Frattini argument $N_{A_7}(C_7)$ has order 21, which is less than the order of A_7.

Theorem 6.29
Let N and H be finite soluble groups of coprime orders. Then every extension of N by H splits.

Proof. Let G be a group such that $N \triangleleft G$, $G/N \cong H$, and $|N|$ and $|G/N|$ are coprime. Also G is solvable by a previous proposition.

We proceed by induction on $|G|$. The result is clear if $|G| = 1$, or if $N = G$, so assume $N < G$.

Let M/N be a minimal normal subgroup of G/N. By Proposition 6.6, M/N is a p-group for some prime p. Let $P \in \mathrm{Syl}_p(M)$, so $M = PN$. Let $X = N_G(P)$. Then bya previous proposition,

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

since $P \leq N_G(P) = X$.

- **Case 1:** $X < G$. Apply induction to the group X. Note:
  - X is solvable,
  - $N \cap X \triangleleft X$,
  - $X/(N \cap X) \cong G/N$,
  - $|N \cap X|$ and $|X/(N \cap X)|$ are coprime.
- **Case 2:** $X = G$. Then $P \triangleleft G$. Apply induction to G/P. Note that:
  - $M/P \triangleleft G/P$,
  - $\gcd(|M/P|, |G/M|) \mid \gcd(|N|, |G/N|) = 1$.

  So the induction hypothesis gives a subgroup $K/P \leq G/P$ such that

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

  Lift this to G: Then $G = MK = NPK = NK$, since $P \leq K$, and $M \cap K = P$. Finally, we show $N \cap K = 1$: since $p \mid |G/N|$, and $\gcd(|N|, |G/N|) = 1$, it follows that $p \nmid |N|$. Hence $N \cap K \leq M \cap K = P$, but $P \cap N = 1$, so $N \cap K = 1$. Therefore, $G = NK$ and $N \cap K = 1$, so the extension splits.

This completes the proof by induction. □

Definition 6.30. If G is a finite group, then a **Hall π-subgroup** H of G is a subgroup whose order and index are coprime; that is $\gcd(|H|, |G : H|) = 1$.

Theorem 6.31 (Hall's theorem)
Let π be any set of primes, and G a finite soluble group. Write $|G| = nm$, where n is a π-number and m a π'-number. Then G has a subgroup of order n i.e. it has a Hall π-subgroup.

Remark 6.32. This theorem is an analogue of Sylow I.

Proof. Let G be a finite solvable group and let π be a set of primes. We aim to 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, the solvable quotient group G/M has a Hall π-subgroup H/M. So:

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

By a previous proposition, 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 suppose $p \notin \pi$. Then $\gcd(|M|, |H/M|) = 1$. Hence by the previous theorem, H splits as an extension of M, so there exists a subgroup $K \leq H$ such that

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

Then:

$$|K| = |H/M| \quad \text{(a } \pi\text{-number)}, \quad |G : K| = |G : H| \cdot |H : K| = |G : H| \cdot |M|$$

is a π'-number. Hence K is a Hall π-subgroup of G, completing the proof. □

Example 6.33

Some examples of Hall π-subgroups:

1. If G is abelian, then G has a unique Hall π-subgroup for any set of primes π. This subgroup is defined as

$$G_\pi = \{g \in G : o(g) \text{ is a } \pi\text{-number}\}.$$

2. Let G be the group of upper triangular matrices in $SL_2(p)$, as in Example (2) on p.24. Then $G \cong \mathbb{F}_p^+ \rtimes \mathbb{F}_p^\times$, 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 subgroup is not normal in G, and thus not unique.
   - If $p \in \pi$, then G has a Hall π-subgroup of the form

$$\mathbb{F}_p^+ \rtimes H_{\pi \setminus \{p\}},$$

     which is normal in G and hence unique.

3. If G is non-solvable, then G may have Hall π-subgroups for some sets π, but not others. For example, the alternating group A_5 has order $60 = 2^2 \cdot 3 \cdot 5$, and:
   - A_5 has a Hall $\{2, 3\}$-subgroup, namely $A_4 \subset A_5$, of order 12.
   - However, A_5 has no Hall $\{2, 5\}$- or $\{3, 5\}$-subgroups, as such subgroups would have index 3 or 4 respectively — but no such subgroups exist (e.g., by Sylow or index arguments).

7 Nilpotent groups

Definition 7.1. 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

- $G_i \triangleleft G$, and
- $G_{i+1}/G_i \leq Z(G/G_i)$.

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

Example 7.2. Abelian groups are nilpotent with central series $1 \leq G$.

Corollary 7.3. Let G be a nilpotent group, then $Z(G) \neq 1$.

Proof. From the condition of the central series we have that, $G_1/G_0 \leq Z(G/G_0)$. Since $G_0 = 1$ this means $G_1 \leq Z(G)$. □

Corollary 7.4. Nilpotent groups are soluble.

Proof. The condition $G_{i+1}/G_i \leq Z(G/G_i)$ implies that G_{i+1}/G_i is Abelian. □

Proposition 7.5
Every finite p-group (for p prime) is nilpotent.

Proof. We use the fact that $Z(G) \neq 1$ for a p-group $G \neq 1$. Let $P \neq 1$ be a p-group, and define a series of subgroups

$$1 = P_0 < P_1 < P_2 < \cdots$$

where

- $P_1 = Z(P)$,
- P_2 is the subgroup containing P_1 such that $P_2/P_1 = Z(P/P_1)$,
- recursively define P_{i+1} to the subgroup such that $P_{i+1}/P_i = Z(P/P_i)$.

This is a strictly increasing series since each centre is non-trivial (as all the quotients must be p-group by considering their orders) so, it must terminate at $P_r = P$. By definition this is a central series for P. □

Example 7.6

We present some common examples and non-examples of nilpotent groups, along with brief justifications.

Examples of Nilpotent Groups:

- **All abelian groups**: Every abelian group is nilpotent of class 1 since the commutator subgroup is trivial, i.e. $[G, G] = \{1\}$.
- **Quaternion group $\mathbf{Q_8}$**: This group has center $Z(Q_8) = \{\pm 1\}$, and $Q_8/Z(Q_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ is abelian. Thus, the upper central series terminates in two steps.
- **Unitriangular matrices**: The group of upper unitriangular matrices over a field, e.g.
$$\left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\} \subset \mathrm{GL}_3(\mathbb{F}_p)$$
is nilpotent, since it is a p-group.
- **Direct products of nilpotent groups**: If G and H are nilpotent, then $G \times H$ is also nilpotent.

Non-Examples:

- **Symmetric group S_n for $n \geq 3$**: These groups have trivial center and nonabelian structure. For example, $[S_3, S_3] = A_3 \cong \mathbb{Z}_3$, so the lower central series does not terminate at the identity quickly.
- **Alternating group A_n for $n \geq 5$**: These are simple and nonabelian, hence cannot be nilpotent.
- **General linear groups $\mathrm{GL}_n(\mathbb{F}_q)$, $n \geq 2$**: These contain nonabelian simple subgroups and have trivial center.
- **Dihedral group D_n for n not a power of a prime**: These are not p-groups and often have trivial centers.

Definition 7.7. Let G be a finite group, and define

- $Z_0(G) = 1$,
- $Z_1(G) = Z(G)$, and
- recursively define $Z_{i+1}(G)$ to be such that $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$.

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

Proposition 7.8. The upper central series is a central series.

Proof. Each $Z_i(G)$ is characteristic in G, and the centrality property holds by the definition of $Z_{i+1}(G)$. □

Definition 7.9. 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 $[k, h] = [h, k]^{-1}$).

Definition 7.10. Define

- $\gamma_0(G) = G$,
- $\gamma_1(G) = [G, G] = G'$, and
- recursively, $\gamma_{i+1}(G) = [\gamma_i(G), G]$.

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.

Proposition 7.11. The lower central series is a central series.

Proof. 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

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

□

Example 7.12

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 $1 < \langle \rho^2 \rangle < G$.

Proposition 7.13

Let G be a finite group, and let $X, Y \leq G$.

1. $Y \leq N_G(X) \iff [X, Y] \leq X$.
2. Suppose $Y \triangleleft G$ and $Y \leq X$, then

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

Note 7.14. This is a powerful statement that allows us to switch between commutators and relations between groups.

Proof. We prove each statement in turn.

1. Suppose $Y \leq N_G(X)$. Then for all $x \in X, y \in Y$, we have:

$$[x, y] = xyx^{-1}y^{-1} \in X,$$

so $[X, Y] \leq X$.

Conversely, suppose $[x, y] \in X$ for all $x \in X, y \in Y$. Then:

$$yxy^{-1} = [x, y]x \in X,$$

since both $[x, y] \in X$ and $x \in X$. So $y \in N_G(X)$, and hence $Y \leq N_G(X)$.

2. Assume $Y \triangleleft G$ and $Y \leq X$. Then for $x \in X$, the condition $xY \in Z(G/Y)$ means:

$$xY \cdot gY = gY \cdot xY \quad \forall g \in G,$$

which is equivalent to:

$$[x,g]Y = Y \quad \forall g \in G \quad \iff \quad [x,g] \in Y \quad \forall g \in G.$$

So $[x,g] \in Y$ for all $x \in X$, $g \in G$, i.e. $[X,G] \leq Y$. Hence, the equivalence

$$X/Y \leq Z(G/Y) \quad \iff \quad [X,G] \leq Y$$

follows, completing part (2).

□

Theorem 7.15

Let G be a finite group, and let $n \in \mathbb{Z}_{>0}$. The following are equivalent:

1. $Z_n(G) = G$
2. $\gamma_n(G) = 1$.

Moreover, G is nilpotent if and only if both these conditions hold for some n.

Note 7.16. We only need for one of these conditions to hold for G to be nilpotent, as one implies the other.

Proof. If either (i) or (ii) holds, then G is nilpotent. So we assume G is nilpotent, and aim to show that (i) and (ii) hold for exactly the same set of positive integers n.

Let

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

be a central series for G. By Proposition 7.3(ii), for each i, we have

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

In particular:

$$\gamma_0(G) = G = N_k, \quad \gamma_1(G) = [G,G] \leq [N_k, G] \leq N_{k-1},$$

and inductively,

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

Since $N_0 = 1$, we conclude that $\gamma_k(G) = 1$. Thus (ii) holds with $n = k$.

To show (i) $\Rightarrow$ (ii): Suppose $Z_n(G) = G$. Take the central series with $N_i = Z_i(G)$. Then $N_k = G$, so again $\gamma_k(G) = 1$, proving (ii).

So (i) $\Rightarrow$ (ii), and we have shown both directions.

Now let us prove the reverse implication: Assume again that G is nilpotent with central series (7.2), and we aim to show

$$N_i \leq Z_i(G) \quad \text{for all } i. \tag{7.3}$$

We proceed by induction.

For $i = 0$, both $N_0 = 1$ and $Z_0(G) = 1$, so the base case holds.

Now suppose $N_{i-1} \leq Z_{i-1}(G)$ for some $i \geq 1$. By Proposition 7.3(ii), we get:

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

and since for $n \in N_i, z \in Z_{i-1}(G)$, we have $[nz, g] = [n, zg][z, g] \in [N_i, G]Z_{i-1}(G) \leq Z_{i-1}(G)$, it follows that

$$[N_i Z_{i-1}, G] \leq Z_{i-1}(G),$$

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

$$N_i \leq Z_i.$$

Thus (7.3) holds by induction.

In particular, $Z_k(G) = N_k = G$, so (i) holds with $n = k$. If $\gamma_n(G) = 1$, then taking the central series with $N_i = \gamma_{n-i}(G)$, the same argument shows $Z_n(G) = G$.

This completes the proof. □

Definition 7.17. For a nilpotent group G, the smallest integer n such that $Z_n(G) = G$ (or equivalently $\gamma_n(G) = 1$) is called the **nilpotence class** (or **class**) of G.

Example 7.18

The dihedral group $D_{2^{c+1}}$ has nilpotency class c.

Proof. This follows from the structure of the dihedral group $D_{2^{c+1}}$, which is a group of order 2^{c+1}. It is known that D_{2^n} has nilpotency class $n - 1$ for $n \geq 3$. Setting $n = c + 1$, we conclude the nilpotency class is c. □

Example 7.19

Some examples.

1. Abelian groups have class 1.
2. A non-Abelian group G has class 2 if and only if $G' \leq Z(G)$, for examples D_8, Q_8 and the group of upper unitriangular matrices in $\mathrm{GL}_3(p)$ of order p^3.

Proposition 7.20

Let $G = G_1 \times G_2 \times \cdots \times G_k$ be a direct product of nilpotent groups. Then the nilpotency class of G is equal to the maximum of the nilpotency classes of the G_i.

Proof. The lower central series $\gamma_i(G)$ of the direct product satisfies:

$$\gamma_i(G) = \gamma_i(G_1) \times \gamma_i(G_2) \times \cdots \times \gamma_i(G_k).$$

Hence, $\gamma_c(G) = 1$ if and only if $\gamma_c(G_i) = 1$ for all i, which occurs exactly when the nilpotency class of each $G_i \leq c$. Therefore, the nilpotency class of the product is the maximum of the nilpotency classes of the factors. □

Exam Questions 7.21 (Q4 Exam 2014)

The questions.

(c) Let $c > 1$. Show that there is no group of order p^c with nilpotency class c.

(d) Let G be a non-abelian group of order p^3. Show that $G' = Z(G)$.

(e) Show that if $1 \leq c < a$, then there is a group of order 2^a with nilpotency class c.

Solution. We provide the solution to each part.

(c) If G has class c, then the subgroups $\gamma_1(G), \ldots, \gamma_{c+1}(G)$ are distinct. Since $\gamma_{i+1}(G) \leq \gamma_i(G)$ for all i, we see that these subgroups must have orders $p^c, p^{c-1}, \ldots, p, 1$. In particular, $\gamma_3(G)$ is a normal subgroup of order p^{c-2}. But now $G/\gamma_3(G)$ has order p^2, and so is Abelian. Hence, $G' \leq \gamma_3(G)$. But $G' = \gamma_2(G)$, and so we must have $\gamma_3(G) = \gamma_2(G)$, which is a contradiction.

(d) $Z(G)$ is non-trivial, and not equal to G since G is non-abelian. But it is a fact seen in the course that $Z(G)$ cannot have index p, and so we must have $|Z(G)| = p$. Since G is non-abelian and has nilpotency class less than 3 by (c), G must have nilpotency class 2. So $[G, G']$ is trivial, and so $G' \leq Z(G)$. But G' is not trivial since G is non-abelian, and so $G' = Z(G)$.

(e) From lectures, the dihedral group $D = D_{2^{c+1}}$ has nilpotency class c. The cyclic group C of order p^{a-c-1} has nilpotency class 1. So the direct product $D \times C$ has order p^a and nilpotency class c.

Exam Questions 7.22 (Q3 Exam 2016)

The questions.

(b) Let p be a prime number and a an integer greater than 1, and let G be a group of order p^a. Show that G is nilpotent of class at most $a-1$.

(c) Let G be a finite nilpotent group. Show that the nilpotency class of G is the maximum of the nilpotency classes of its Sylow subgroups. (You may use any results from the course without proof, but you should state them clearly.)

Solution. We provide a solution to each part.

(b) We use the fact that every non-trivial p-group P has a non-trivial centre. (For the conjugacy classes of P partition P, and all have p-power size; since p divides $|P|$, we see that the number of conjugacy classes of size 1 is divisible by p, and is non-zero since $\{1\}$ is one such class. The classes of size 1 contain central elements.)

We also use the fact from lectures that for any surjective homomorphism $\theta : G \to H$, we have $\phi(\gamma_a(G)) = \gamma_a(H)$ (proved by an easy induction on a).

We work by induction on a. If $a = 2$, then G is abelian. Suppose that every group of order p^a is nilpotent of class at most $a-1$. Suppose that G has order p^{a+1}. Since G has non-trivial centre, it has a central subgroup K of order p. Now G/K has order p^a, and so G/K is nilpotent of class at most $a-1$. Hence $\gamma_a(G/K) = \{e\}$. Now if θ is the canonical map $G \to G/K$, then $\gamma_a(G/K) = \theta(\gamma_a(G))$. Hence we see that $\gamma_a(G) \leq \ker\theta = K$. So $\gamma_{a+1}(G) \leq [K, G] = \{e\}$, since K is central. Hence G is nilpotent of class at most a, completing the induction.

(c) We use the following facts from lectures: every finite nilpotent group is isomorphic to a direct product of its Sylow subgroups. If A is nilpotent of class c and B is nilpotent of class d, then $A \times B$ is nilpotent of class $\max(c, d)$.

It follows from the second of these statements that if $P_1, \ldots, P_k$ are nilpotent groups of class $c_1, \ldots, c_k$ respectively, then $P_1 \times \cdots \times P_k$ is nilpotent of class $\max(c_1, \ldots, c_k)$ (by straightforward induction on k). Now if G is a finite nilpotent group, it is a direct product of its Sylow subgroups, which are nilpotent groups; the result follows immediately.

Corollary 7.23

Subgroups and quotients of nilpotent groups are nilpotent.

Proof. Let G be nilpotent, so $\gamma_n(G) = 1$ for some n.

If $H \leq G$, then by monotonicity of the lower central series,

$$\gamma_n(H) \leq \gamma_n(G) = 1,$$

so $\gamma_n(H) = 1$, and H is nilpotent.

Let $N \trianglelefteq G$, and let $\varphi : G \to G/N$ be the canonical projection. Then for all i,

$$\varphi(\gamma_i(G)) = \gamma_i(\varphi(G/N)),$$

since homomorphisms preserve commutator structure. In particular,

$$\gamma_n(G/N) = \varphi(\gamma_n(G)) = \varphi(1) = 1.$$

Hence, the lower central series of G/N also terminates in the trivial subgroup after at most n steps, so G/N is nilpotent.

□

Theorem 7.24

For a finite group G, the following are equivalent:

1. G is nilpotent.
2. For any $H < G$, we have $H < N_G(H)$.
3. Every maximal subgroup of G is normal.
4. Every Sylow subgroup of G is normal.
5. $G = P_1 \times \cdots \times P_k$ where P_i is a p_i-subgroup and $p_1, \ldots, p_k$ are distinct primes.

Note 7.25. The P_i tend to be the Sylow subgroups of G.

Exam Questions 7.26 (Q3 Exam 2010)

Show that if a and b are two elements of coprime orders in a nilpotent group G, then a and b commute. Hence or otherwise prove that if the dihedral group D_{2n} is nilpotent, then $n = 2^k$ for some integer k.

Solution. We will use the theorem that every nilpotent group G is isomorphic to the direct product $P_1 \times P_2 \times \cdots \times P_s$ of all its Sylow subgroups P_i. Here $|P_i| = p_i^{v_i}$ $(v_i \in \mathbb{N})$ and $p_1, p_2, \ldots, p_s$ are the distinct primes dividing $|G|$. Let now $a = (a_1, \ldots, a_s)$, $b = (b_1, \ldots, b_s)$ be two elements of $P_1 \times \cdots \times P_s$ of coprime orders. I claim that for every index i between 1 and s, either $a_i = 1$ or $b_i = 1$. Suppose $a_i \neq e \neq b_i$ for some i. Then since P_i is a p_i-group, the prime p_i divides both the order $o(a_i)$ and $o(b_i)$. On the other hand, $o(a)$ is the least common multiple of $o(a_1), o(a_2), \ldots, o(a_s)$, and so $p_i \mid o(a)$. Similarly, $p_i \mid o(b)$, which is a contradiction. This proves my claim. Hence $[a, b] = 1$ for every index i, and therefore

$$[a, b] = ([a_1, b_1], \ldots, [a_s, b_s]) = (1, 1, \ldots, 1) = 1_G,$$

i.e., a and b commute.
For the final part, suppose that there is an odd prime p dividing n and D_{2n} is nilpotent. D_{2n} is generated by a rotation ρ of order n and a reflection τ of order 2 such that $\tau\rho\tau^{-1} = \rho^{-1}$. Let $n = pm$ for some integer m and consider $a = \rho^m$ and $b = \tau$. The order of a is the odd prime p, and by the above result, a and b must commute. However,

$$[a, b] = \rho^m \tau \rho^{-m} \tau = \rho^m (\tau \rho^{-m} \tau) = \rho^m (\rho^m) = \rho^{2m} = a^2 \neq e$$

since $o(a) = p$. This is a contradiction. Therefore, n must be a power of 2.

Exam Questions 7.27 (Q4(a) Exam 2022)

Let $F = \mathbb{Z}/3\mathbb{Z}$ be the field with 3 elements, and let

$$G = \{(a_{ij})_{3\times 3} \in GL_3(F) \mid a_{21} = a_{31} = a_{32} = 0\}$$

be the group of upper triangular matrices in $GL_3(F)$. Let

$$H = \{(a_{ij})_{3\times 3} \in G \mid a_{11} = a_{22} = a_{33} = 1\}$$

be the group of uni-triangular matrices.

Find the orders of G and H. Which of the groups G and H are solvable and which are nilpotent? Justify your answer.

Solution. An element of H has three off-diagonal entries which can contain any element of F, which gives $|H| = 3^3$. An element of G in addition can have ± 1 on the diagonal entries, which gives $|G| = 2^3 \cdot 3^3$. If we assign to an element of G an element of $C_2 \times C_2 \times C_2 = \{(x, y, z) : x, y, z \in \{1, -1\}\}$ equal to (a_{11}, a_{22}, a_{33}), we obtain a surjective homomorphism with kernel H. Since H is a 3-group, it is nilpotent. Since G/H is a 2-group, G is solvable.

If the Sylow 2-subgroup of diagonal matrices in G were normal, the whole G would be the direct product of its Sylow subgroups. Then every diagonal matrix would commute with every upper triangular matrix, which is not the case by a direct check. Hence G is not a nilpotent group.

7.1 Soluble radical and the Fitting subgroup

Proposition 7.28

Let G be a finite group with normal subgroups M and N (thus, $MN \triangleleft G$).

1. If M and N are soluble, so is MN.
2. If M and N are nilpotent, so is MN.

Proof. We prove each statement in turn.

1. We have the isomorphism:

$$MN/N \cong M/M \cap N,$$

which is solvable by a proposition. Hence MN is solvable by a proposition.

2. This is more subtle. Suppose $M, N \triangleleft G$ are both nilpotent. We aim to show every Sylow subgroup of MN is normal, and hence MN is nilpotent by the previous theorem.

Let p be a prime, and let $S \in \mathrm{Syl}_p(MN)$. Then $S \cap M \in \mathrm{Syl}_p(M)$, and since M is nilpotent, it has a unique Sylow p-subgroup. So $S \cap M \trianglelefteq M$, and hence $S \cap M \trianglelefteq MN$ since $M \trianglelefteq MN$. Likewise, $S \cap N \trianglelefteq MN$.

Now observe:

$$|MN|_p = \frac{|M|_p|N|_p}{|M \cap N|_p} \quad \text{and} \quad |S| \geq \frac{|S \cap M| \cdot |S \cap N|}{|S \cap M \cap N|},$$

so:

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

Thus all inequalities are equalities, so:

$$S = (S \cap M)(S \cap N).$$

Since both $S \cap M$ and $S \cap N$ are normal in MN, so is S. Hence all Sylow subgroups of MN are normal, and MN is nilpotent.

□

Corollary 7.29. Every finite group G, has a unique largest soluble normal subgroup and a unique largest nilpotent normal subgroup, denoted by $R(G)$ and $F(G)$ respectively.

Proof. Choose $R \trianglelefteq G$, maximal subject to being solvable. If $S \trianglelefteq G$ is any other solvable normal subgroup, then RS is solvable by Proposition 7.6, and is also normal in G. By maximality of R, it must be that $RS = R$, hence $S \leq R$. So R is the unique largest such subgroup. The nilpotent case is proven identically, using part (2) of the previous proposition. □

Definition 7.30. We call $F(G)$ the **fitting subgroup**.

Example 7.31

Example of fitting subgroups.

1. $F(S_3) = A_3$.
2. $F(S_4) = V_4$.
3. Let $G = \mathrm{SL}_2(p)$, for $p \geq 5$ we have $F(G) = R(G) = Z(G) = \{\pm I\}$.

Proposition 7.32

If G is soluble, then $C_G(F(G)) \leq G$ (hence, $C_G(F(G)) = Z(F(G))$).

Proof. Exercise. □

Note 7.33. The point is that G acts by conjugation on its Fitting subgroup $F = F(G)$, giving a homomorphism

$$\pi : G \longrightarrow \mathrm{Aut}(F).$$

The kernel of this homomorphism is $C_G(F)$, the centraliser of F in G. But by a proposition above (or its earlier corollaries), $C_G(F) = Z(F)$. Hence, we have:

$$G/Z(F) \hookrightarrow \mathrm{Aut}(F),$$

so $G/Z(F)$ is isomorphic to a subgroup of $\mathrm{Aut}(F)$.

This is often a useful piece of structural information about a solvable group G.

Example 7.34. Suppose G is solvable and $F = F(G) \cong (C_p)^n$ for some prime p. Then $F = Z(F)$ and:

$$\mathrm{Aut}(F) \cong \mathrm{GL}_n(p).$$

So we conclude that:

$$G/Z(F) \leq \mathrm{GL}_n(p),$$

i.e., G is an extension of an elementary abelian p-group $(C_p)^n$ by a (solvable) subgroup of $\mathrm{GL}_n(p)$.

8 The Frattini subgroup

Definition 8.1. Let $G \neq 1$. A subgroup $1 \neq M \leq G$ is said to be a **maximal subgroup** of G if there is no subgroup L such that $M \leq L \leq G$.

Proposition 8.2 ([1, Page 51, 140(v)])
If $M < G$ and $|G : M| = p$ for some prime p, then M is a maximal subgroup of G.

Definition 8.3. Let G be a finite group. The intersection of all the maximal subrgoups of G is called the **Frattini subgroup** of G, denoted by $\Phi(G)$.

Example 8.4
We have that

- Consider the group $C_2 \times C_2$, its maximal subgroups are $\langle a \rangle, \langle b \rangle$, and $\langle a, b \rangle$ thus $\Phi(C_2 \times C_2) = 1$.
- The maximal subgroups are the ones of order 4 so $\langle \rho \rangle, \langle \sigma, \rho^2 \rangle$ and $\langle \rho\sigma, \rho^2 \rangle$. Hence, $\Phi(D_8) = \langle \rho^2 \rangle = Z(D_8)$.

Proposition 8.5. Let $x \in \Phi(G)$. Then for any subset $S \subseteq G$,

$$G = \langle S, x \rangle \Rightarrow G = \langle S \rangle.$$

Conversely, if $x \in G$ and has the property as above, 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 $x \in \Phi(G) \subseteq M$, so $G = \langle S, x \rangle \leq M$, a contradiction. Hence $G = \langle S \rangle$.
Conversely, suppose $x \in G$ has the property. 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 the assumption of the property (with $S = M$). Hence $x \in \Phi(G)$. □

□

Definition 8.6. In light of the property outlined above, we say that $\Phi(G)$ consists of the **non-generators** of G.

Note 8.7. This means that $\Phi(G)$ is generated by all the elements in G which do not generate G.

Proposition 8.8
$\Phi(G)$ is 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 $P \in \mathrm{Syl}_p(\Phi(G))$. By the Frattini argument, we have

$$G = N_G(P)\Phi(G),$$

and hence $G = N_G(P)$ by the non-generation property (above proposition). So $P \triangleleft G$, hence certainly $P \triangleleft \Phi(G)$. We have now shown that every Sylow subgroup of $\Phi(G)$ is normal, and so $\Phi(G)$ is nilpotent by one of the equivalent definitions to be nilpotent. □

Corollary 8.9. We have that $\Phi(G) < F(G)$.

Proposition 8.10
The Frattini subgroup of elementary Abelian groups is trivial i.e. for p prime $\Phi((C_n)^p) = 1$.

Proof. Regard the group $(C_p)^n \cong (\mathbb{F}_p^n, +)$ as a vector space over $\mathbb{F}_p$. Let $0 \neq v \in \mathbb{F}_p^n$, we can extend to a basis $\{v_1, \ldots, v_n\}$ then $\langle v_2 \ldots, v_n\rangle \cong \mathbb{F}_p^{n-1}$ which is a maximal subgroup not containing p. Therefore, $v \notin \Phi((C_n)^p)$ which implies $\Phi((C_n)^p) = 1$. □

Theorem 8.11 (Burnside Basis Theorem)
Let P be a p-group with $|P| = p^n$ and $|\Phi(P)| = p^{n-d}$, where $d \geq 1$.

1. Then $P/\Phi(P) \cong (C_p)^d$, an elementary Abelian group of order p^d.
2. If $N \triangleleft P$ and P/N is an elementary Abelian group, then $\Phi(P) \leq N$.
3. Let $P \to P/\Phi(P)$ such that $x \mapsto \overline{x}$ be the canonical surjection. Regard $P/\Phi(P)$ as the vector space $\mathbb{F}_p^d$, then for $x_1, \ldots, x_d \in P$ we have that

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

Proof. We prove each statement in turn.

1. Let M be a maximal subgroup of P. Then $M \triangleleft P$ by Theorem 7.5, and $|P : M| = p$. By definition, $P' \leq M$, and $x^p \in M$ for all $x \in P$. So:

$$P' \leq \Phi(P), \quad \text{and hence } P/\Phi(P) \text{ is abelian with } \bar{x}^p = 1.$$

Thus $P/\Phi(P)$ is an elementary abelian p-group of order p^d, i.e., $P/\Phi(P) \cong (C_p)^d$.

2. Suppose $N \triangleleft P$ and P/N is elementary abelian. Then $\Phi(P/N) = 1$, by Proposition 8.3. Maximal subgroups of P/N are of the form M/N, where M is maximal in P and contains N. Hence:
$$\Phi(P/N) = \bigcap M/N = N.$$
So $\Phi(P) \leq N$.

3. Let $P = \langle x_1, \ldots, x_d \rangle$. Then $\bar{x}_1, \ldots, \bar{x}_d$ span $\mathbb{F}_p^d$, hence form a basis.

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

□

Corollary 8.12

As per the notation above. Let $d(P)$ denote the minimum number of generators of P, then $d(P) = d$.

Example 8.13

Consider the dihedral group D_{16}. We aim to determine its Frattini subgroup. Since $|D_{16}| = 16 = 2^4$, we know that $|\Phi(D_{16})| = 2^{4-d}$, where d is the minimum number of generators of D_{16}. By applying the earlier proposition, we find that D_{16} has exactly 2 generators, so $d(D_{16}) = 2 = d$. Consequently, $|\Phi(D_{16})| = 2^2$, which implies that $\Phi(D_{16}) = \langle \rho^2 \rangle$.

Exam Questions 8.14 (Q3 Exam 2023)

The questions.

(b) (i) Let p be an odd prime. Prove that the dihedral group D_{2p} is not nilpotent.

(ii) Deduce that for any $n \in \mathbb{N}$, the dihedral group D_{2n} is nilpotent if and only if n is equal to a power of 2.

(c) Now let G be a finite nilpotent group.

(i) Let M be a maximal subgroup of G. Assuming the standard result that $M \triangleleft G$, prove that G/M is cyclic of prime order.

(ii) Prove that $G' \leq \Phi(G)$.

(iii) Hence prove that if G/G' is cyclic, then G must be cyclic.

Solution. We provide the solution to each part in turn.

(b) (i) Let $G = D_{2p} = \langle x, y : x^p = y^2 = 1, y^{-1}xy = x^{-1}\rangle$. If G is nilpotent, then by definition $Z(G) \neq 1$. However, $Z(D_{2p}) = 1$ (the non-identity powers x^i do not commute with y, the other elements $x^i y$ do not commute with x). So D_{2p} is not nilpotent.

(ii) Consider $G = D_{2n}$. If $n = 2^a$, then G is a 2-group, which is nilpotent (standard result). If not, then n has an odd prime factor p, and then G has a subgroup $\langle x^{n/p}, y\rangle \cong D_{2p}$. This is non-nilpotent by (i), so G has a non-nilpotent subgroup, hence is itself not nilpotent (standard result).

(c) (i) Let G be nilpotent, and M a maximal subgroup. As stated in the question, $M \triangleleft G$. Since M is maximal, G/M can have no nontrivial subgroups, hence $G/M \cong C_p$ for some prime p.

(ii) By (i), G/M is cyclic, hence abelian, for every maximal subgroup M. Hence $G' \leq M$ for every maximal subgroup, and so $G' \leq \Phi(G)$.

(iii) Suppose G/G' is cyclic. Then by (ii), $G/\Phi(G)$ is cyclic, so $G/\Phi(G) = \langle g\Phi(G)\rangle$ for some $g \in G$. Then $G = \langle g, \Phi(G)\rangle$. Hence by the 'non-generation' property of $\Phi(G)$, we have that $G = \langle g\rangle$, cyclic.

8.1 Groups of order p^3

Note 8.15. We can use the possible orders of $P/\Phi(P)$ as a framework to classify p-groups.

Theorem 8.16. Groups of order p^2 are abelian.

We know the classification of groups of order 2^3, and also the abelian groups of order p^3, namely C_{p^3}, $C_{p^2} \times C_p$, $C_p \times C_p \times C_p$. Thus, our interest lies in non-abelian groups of order p^3, particularly when p is odd.

In the proof of the classification theorem, we will need the following identity.

Proposition 8.17. Let G be a group such that $G' \leq Z(G)$. Then for all $x, y \in G$ and integers $n \geq 1$,

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

Proof. We use induction on n, and the identity

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

Note that $[x^{-1}, y^{-1}] \in Z(G)$ since $G' \leq Z(G)$. This means that these commutators commute with everything, simplifying our manipulation.

Assume the formula holds for n. Then:

$$\begin{aligned} x^{n+1}y^{n+1} &= x^n y^n xy \\ &= (xy)^n [x^{-1}, y^{-1}]^{n(n-1)/2} \cdot xy \quad \text{(by induction)} \\ &= (xy)^n xy [x^{-1}, y^{-1}]^{n(n-1)/2} \quad \text{(since the commutator is central)} \\ &= (xy)^n xy [x^{-1}, y^{-1}]^n \\ &= (xy)^{n+1} [x^{-1}, y^{-1}]^{n(n-1)/2+n} = (xy)^{n+1} [x^{-1}, y^{-1}]^{(n+1)n/2}, \end{aligned}$$

as required. □

Theorem 8.18

Let p be a prime. We classify the non-Abelian groups of order p^3.

- For $p = 2$ there are 2 non-Abelian groups which are D_8 and Q_8.
- For an odd p, up to isomorphism, there are exactly 2 non-Abelian groups:
  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. $P_2 = \langle a, b : a^{p^2} = b^p = 1,\ [a, b] = a^p \rangle \cong C_{p^2} \rtimes C_p$.

Remark 8.19. P_1 is isomorphic to the group of upper unitriangular matrices in $GL_3(p)$, via the map:

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

We can also view $P_i = NH$ as semidirect products with $N \trianglelefteq P_i$, $N \cap H = 1$, for:

- $i = 1$: $N = \langle a, c \rangle \cong C_p \times C_p$, $H = \langle b \rangle \cong C_p$
- $i = 2$: $N = \langle a \rangle \cong C_{p^2}$, $H = \langle b \rangle \cong C_p$

Proof. Let $|P| = p^3$ with P non-abelian. By Theorem 8.4, $P/\Phi(P) \cong (C_p)^d$ with $d = 1, 2, 3$. If $d = 1$, then P is cyclic, and if $d = 3$, then $P \cong (C_p)^3$ (abelian). Hence, for P non-abelian, we must have $d = 2$. So:

$$P = \langle a, b \rangle, \quad \Phi(P) = \langle c \rangle, \quad \text{where } c = [a, b].$$

Also, since $\Phi(P) = Z(P) = P'$, the group is nilpotent class 2.

- **Case 1.** Suppose $a^p = b^p = 1$. Then since $[a, b] \neq 1$, we can take $c = [a, b]$. All relations of P_1 are satisfied, so $P \cong P_1$.
- **Case 2.** Now suppose a has order p^2, so $a^{p^2} = 1$, but $a^p \neq 1$. Then $a^p \in \Phi(P) = \langle a^p \rangle$, so:
  - **(2a)** If $b^p = 1$, then $[a, b] = a^p$ and we have the relations for P_2, so $P \cong P_2$.
  - **(2b)** If b has order p^2, we can modify a, b such that $a^p = c, b^p = c^{-1}$. Then by Prop 8.6,
    $$1 = a^p b^p = (ab)^p [a^{-1}, b^{-1}]^{p(p-1)/2}.$$
    Since $p \mid p(p-1)/2$, this implies $[a^{-1}, b^{-1}]^{p(p-1)/2} = 1$ and hence $(ab)^p = 1$. Replacing b by ab, we return to Case (2a), so $P \cong P_2$.

□

8.2 Groups of order 16 (and more generally of order 2^n)

There are 15 groups of order 16, and a complete classification is quite involved. We give a partial classification using the theory we have developed so far. Many of the groups are constructed as semidirect products, leveraging new automorphisms introduced below.

Proposition 8.20 (Automorphisms for Semidirect Products)
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:

1. $\alpha_1(x) = x^{p^{n-1}+1}$,
2. If $p = 2$: $\alpha_2(x) = x^{-1}$,
3. If $p = 2$: $\alpha_3(x) = x^{2^{n-1}-1}$.

Proof. These are easily checked to be homomorphisms; we verify they have order p. For example:
$$\alpha_1^p(x) = x^{(p^{n-1}+1)^p} \equiv x \mod p^n$$
The binomial expansion and reduction modulo p^n confirms the claim. Similar arguments apply for α_2 and α_3. □

Definition 8.21. We now define four classes of groups of order p^n (for $n \geq 3$):

1. **Modular group:**
$$\mathrm{Mod}_{p^n} = C_{p^{n-1}} \rtimes_{\alpha_1} C_p = \langle x, y : x^{p^{n-1}} = y^p = 1, y^{-1}xy = x^{p^{n-2}+1} \rangle$$
2. **Dihedral group:**
$$D_{2^n} = C_{2^{n-1}} \rtimes_{\alpha_2} C_2 = \langle x, y : x^{2^{n-1}} = y^2 = 1, y^{-1}xy = x^{-1} \rangle$$
3. **Semidihedral group:**
$$\mathrm{SD}_{2^n} = C_{2^{n-1}} \rtimes_{\alpha_3} C_2 = \langle x, y : x^{2^{n-1}} = y^2 = 1, y^{-1}xy = x^{2^{n-2}-1} \rangle$$

4. **Generalised quaternion group:**

$$Q_{2^n} = \langle x, y : x^{2^{n-1}} = y^4 = 1, x^{2^{n-2}} = y^2, y^{-1}xy = x^{-1} \rangle$$

Remark 8.22. Note that for odd p, Mod_{p^3} is isomorphic to the group P_2 from a previous theorem. All four classes have cyclic subgroups of index p, which is useful for classifying non-abelian p-groups.

8.3 Classifying groups of order 16

We shall achieve a partial classification. Let $|P| = 16$. Using a previous theorem, we divide the analysis into cases as follows:

1. $P/\Phi(P) \cong C_2$
2. $P/\Phi(P) \cong C_2^2$ and $\Phi(P) \cong C_4$
3. $P/\Phi(P) \cong C_2^2$ and $\Phi(P) \cong C_2^2$
4. $P/\Phi(P) \cong C_2^3$
5. $P/\Phi(P) \cong C_2^4$

In Case 1, P is cyclic, and in Case 4, we have $P \cong C_2^4$. The other cases require substantial effort. We shall just deal with Case 2a:

Theorem 8.23

Let P be as in Case 2a. Then P is isomorphic to one of the groups

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

Sketch of proof. We'll give a sketch and leave some of the details to Q4, Sheet 4. We have:

$$P/\Phi(P) \cong C_2^2 \quad \text{and} \quad \Phi(P) = \langle a \rangle \cong C_4.$$

The main step is to prove that there is an element $x \in P$ such that $x^2 = a$, i.e. x has order 8. Define:

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

Then K is characteristic and hence normal. Every non-identity element of P/K has order 2, so P/K is elementary abelian. Hence $\Phi(P) \leq K$. But since $x^2 \in \Phi(P)$ for all x, we get $K \leq \Phi(P)$, so:

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

Therefore, one of the generators x^2 must be equal to a, i.e. there exists $x \in P$ such that $x^2 = a$, so x has order 8. Then $\langle x \rangle \trianglelefteq P$. For $y \in P \setminus \langle x \rangle$, we define:

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

for some $s, r \in \mathbb{Z}$. As $x^4 = a^2$ has order 2, this implies $s \in \{1, 3, 5, 7\}$, and we leave it as an exercise to verify the resulting group is:

- $s = 1$: $P \cong C_8 \times C_2$
- $s = 3$: $P \cong SD_{16}$
- $s = 5$: $P \cong \mathrm{Mod}_{16}$
- $s = 7$: $P \cong D_{16}$ or Q_{16}

□

Note 8.24. This classification leverages the Burnside Basis Theorem, which tells us that $P/\Phi(P)$ behaves like a vector space over $\mathbb{F}_2$. In Case IIa, we know $P/\Phi(P) \cong C_2^2$ and $\Phi(P) \cong C_4$, which already gives a powerful structural constraint: P is generated by 2 elements, and all nontrivial relations are encoded in $\Phi(P)$. The proof shows that P has a normal cyclic subgroup of order 8, and the different ways a second generator can act by conjugation determine the isomorphism type of P. This case covers many of the most interesting and common groups of order 16, including the dihedral, quaternion, and semidihedral groups.

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.

Definition 9.1. Let G be a finite group, and $H \leq G$ with $|G : H| = n$. Choose right coset representatives $y_1, \ldots, y_n$, so that:

$$G = \bigcup_{i=1}^{n} Hy_i.$$

For each $x \in G$, 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:

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

Definition 9.2. The **transfer map** $\tau : G \to H/H'$ is defined by:

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

Example 9.3

Let $G = D_6 = \langle \rho, \sigma \rangle$, and let $H = \langle \sigma \rangle$. Choose coset representatives e, ρ, ρ^2. Then $h_i(\rho) = e$, and $h_i(\sigma) = \sigma$ for all i. So:

$$\tau(\rho) = e, \quad \tau(\sigma) = \sigma.$$

Proposition 9.4
The transfer map τ satisfies:

1. τ is a homomorphism $G \to H/H'$.
2. τ is independent of the choice of coset representatives $y_1, \dots, y_n$.

Proof. We prove each statement in turn.

1. Let $x_1, x_2 \in G$. From (9.1), we have:

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

On the other hand:

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

As H/H' is abelian, it follows that:

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

2. Let $y_1', \dots, y_n'$ be another set of coset representatives, say $y_i' = z_i y_i$, where $z_i \in H$. Then by (9.1),

$$y_i' x = z_i y_i x = z_i h_i(x) y_{\sigma_x(i)} = h_i'(x) y'_{\sigma_x'(i)}.$$

So $h_i'(x) = z_i h_i(x) z^{-1}_{\sigma_x(i)}$, and:

$$\prod_i h_i'(x) H' = \left(\prod_i z_i\right)\left(\prod_i h_i(x)\right)\left(\prod_i z^{-1}_{\sigma_x(i)}\right) H' = \prod_i h_i(x) H'.$$

Hence part (2) follows.

□

Note 9.5. The transfer map τ captures a kind of "averaged" behaviour of group elements over cosets. Given a subgroup H, we can't always map the entire group G nicely into H, but we *can* map into H/H', an abelian quotient. This is particularly useful when studying whether $G' \subsetneq G$, since τ is trivial on commutators. The technical condition involving coset representatives ensures that the map is well-defined and independent of how we choose them. The real power of τ comes in theorems where it helps show that certain elements must lie outside the commutator subgroup.

9.1 How to compute $\tau(x)$

Let $\tau : G \to H/H'$ be the transfer homomorphism defined above. Let $\Omega = \{Hg : g \in G\}$ be 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 rather than the left-action used previously, but it suits the transfer map notation.) Let the disjoint cycles of this action be:

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

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

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

Note 9.6. The transfer homomorphism collects how x "twists" the cosets of H in G. The cycle decomposition tells us how each coset is permuted by x, and this twisting is encoded by the conjugates $x_ix^{r_i}x_i^{-1}$. When all such twists are multiplied, we obtain $\tau(x)$, modulo H'.

Proposition 9.7

For $x \in G$ we have

$$\tau(x) = \left(\prod_{i=1}^{t} x_ix^{r_i}x_i^{-1} \right) H',$$

where:

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

Note 9.8. Each conjugate $x_ix^{r_i}x_i^{-1}$ accounts for how x^{r_i} acts within the corresponding coset. Since the action is by conjugation, the total transfer accumulates these internal symmetries over all cosets, giving a well-defined element of H/H'.

Corollary 9.9. Let $|G/Z(G)| = m$, and let $\tau : G \to Z(G)$ be the transfer. Then

$$\tau(x) = x^m \quad \text{for all } x \in G.$$

Proof. By the previous proposition, $\tau(x) = \left(\prod_{i=1}^{t} x_ix^{r_i}x_i^{-1}\right)$, where $x_ix^{r_i}x_i^{-1} \in Z(G)$, hence is equal to x^{r_i}. So $\tau(x) = \prod x^{r_i} = x^m$. □

9.2 Fusion and the Focal Subgroup

In our main applications of transfer, we consider the transfer homomorphism

$$\tau : G \to P/P',$$

where P is a Sylow p-subgroup of G. We need to introduce some terminology regarding conjugacy.

Definition 9.10.

1. For $H \leq G$ and $x, y \in H$, we write $x \sim^H y$ if x and y are H-conjugate; that is, $y = hxh^{-1}$ for some $h \in H$.

   Note: $x \sim^H y \Rightarrow x \sim^G y$, but not conversely.

2. A subgroup $H \leq G$ is said to **have no fusion in** G if, for all $x, y \in H$,

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

Note 9.11. Fusion describes how conjugacy in the whole group G relates to conjugacy within a subgroup H. If $x \sim^G y$ but $x \not\sim^H y$, it means the group G "fuses" elements of H that are not conjugate within H itself. When H has no fusion, G's conjugation preserves the internal structure of H.

Example 9.12

Let $G = A_4$. The 3-Sylow subgroup $P_3 = \langle (123) \rangle \in \mathrm{Syl}_3(G)$ has no fusion in G, as any conjugates of (123) within G lie in P_3 and are already conjugate in it.

On the other hand, the 2-Sylow subgroup $P_2 = V_4 \in \mathrm{Syl}_2(G)$ does have fusion in G. For $x, y \in P_2 \setminus \{1\}$ with $x \neq y$, we can have $x \sim^G y$ but $x \not\sim^{P_2} y$.

Definition 9.13. Let $P \leq G$. The **focal subgroup** of P in G is defined as:

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

Note 9.14. The focal subgroup captures the "difference" between elements of P that are conjugate in G, but possibly not in P. The elements xy^{-1} measure how far the group P is from having no fusion in G: the smaller the focal subgroup, the less fusion.

Proposition 9.15

Let $P \leq G$. Then the following hold:

1. We have $P' \leq F_G(P) \leq P \cap G'$.
2. If P has no fusion in G, then $F_G(P) = P'$.

Proof. We prove each statement in turn.

1. For $x \in P, g \in G$ and $y = gxg^{-1}$, we compute

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

   Taking $g \in P$, we see that $P' \leq F_G(P)$. Since all such commutators lie in G', we have $F_G(P) \leq G'$, and being generated inside P, we have $F_G(P) \leq P \cap G'$.

2. If P has no fusion in G, then for all $x, y \in P$, $x \sim^G y$ implies $x \sim^P y$, i.e. conjugation by G inside P coincides with conjugation by P. Hence,

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

□

Example 9.16. Some examples.

1. Let $G = A_4$, and let P_2, P_3 be the subgroups defined in the previous example. Then $F_G(P_3) = P_3' = 1$, while $F_G(P_2) = P_2$.
2. Let $G = A_5$, and $P_5 = \langle x \rangle \in \mathrm{Syl}_5(G)$, where $x = (12345)$. Then $x \sim^G x^{-1}$, so P_5 has fusion in G and $F_G(P_5) \supseteq x^2$. Hence $F_G(P_5) = P_5$.

Theorem 9.17 (Focal Subgroup theorem)
Let $P \in \mathrm{Syl}_p(G)$, and let $\tau : G \to P/P'$ be the transfer homomorphism. Then

$$F_G(P) = P \cap G' = P \cap \ker(\tau).$$

Proof. We know from a previous proposition that $F_G(P) \leq P \cap G'$. Also, since $G/G' \cong \mathrm{Im}(\tau)$ is abelian, we have $G' \leq \ker(\tau)$. Hence:

$$F_G(P) \leq P \cap G' \leq P \cap \ker(\tau).$$

So it suffices to prove the reverse inclusion:

$$P \cap \ker(\tau) \leq F_G(P).$$

Let $x \in P \cap \ker(\tau)$. By a previous proposition (transfer formula), we have:

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

where $\sum r_i = |G : P| = n$, and each $x_i x^{r_i} x_i^{-1} \in P$. Since conjugates of x lie in P, the product lies in $F_G(P)$, so:

$$\tau(x) = x^n f P', \quad \text{for some } f \in F_G(P).$$

But $x \in \ker(\tau)$, so $\tau(x) \in P'$. Therefore,

$$x^n f \in P' \Rightarrow x^n \in F_G(P).$$

Now $x \in P$, so x has p-power order, and n is coprime to p, so $\langle x \rangle = \langle x^n \rangle$. Thus $x \in F_G(P)$, completing the proof. □

Corollary 9.18. Suppose $P \in \mathrm{Syl}_p(G)$ has no fusion in G. Then

$$P \cap G' = P'.$$

Remark 9.19. The corollary tells us that if $P \in \mathrm{Syl}_p(G)$ is nontrivial and has no fusion in G, then the derived subgroup G' intersects P exactly in its own derived subgroup: $P \cap G' = P'$. In particular, if $P' < P$, then $G' < G$, so G is not simple unless $G \cong C_p$. This result is a classic "local-to-global" phenomenon: properties of a Sylow subgroup (a local condition) give information about the global structure of G.

Proposition 9.20. Let $P \in \mathrm{Syl}_p(G)$. Then for any $x, y \in C_G(P)$,

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

Proof. Suppose $x, y \in C_G(P)$ and $x \sim^G y$. Then $y = gxg^{-1}$ for some $g \in G$. So $P \leq C_G(x), C_G(y)$, and is a Sylow p-subgroup of each. Now $P \sim^G {}^gP \leq C_G(y)$, and both are Sylow p-subgroups of $C_G(y)$, so by Sylow IV, they are conjugate in $C_G(y)$: ${}^gP = {}^cP$ for some $c \in C_G(y)$. Then $cg \in N_G(P)$ and $y = cxc^{-1}$, showing $x \sim^{N_G(P)} y$. □

Theorem 9.21 (Burnside's Transfer theorem)
Let $P \in \mathrm{Syl}_p(G)$, and suppose that $P \leq Z(N_G(P))$. Then there exists $N \trianglelefteq G$ such that

$$G = PN \quad \text{and} \quad P \cap N = 1.$$

Note 9.22. The result guarantees the existence of a normal complement N to a Sylow p-subgroup P, provided P lies in the centre of its normaliser. This means that G splits as a semidirect product of P and N, where N is a p'-subgroup. This is powerful for simplifying the structure of G: instead of trying to understand all of G, we can understand P and N separately. The key condition $P \leq Z(N_G(P))$ ensures P is abelian and fixed under conjugation by its normaliser—this tames how elements in G move elements of P.

Proof. Assume $P \in \mathrm{Syl}_p(G)$ and $P \leq Z(N_G(P))$. Then

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

Claim: $F_G(P) = 1$.

Proof. Recall $F_G(P) = \langle xy^{-1} : x, y \in P, x \sim^G y \rangle$. Suppose $x \sim^G y$. Then by Prop. 9.8, $x \sim^{N_G(P)} y$, so $y = nxn^{-1}$ for some $n \in N_G(P)$. Since $P \leq Z(N_G(P))$, we have $nxn^{-1} = x$, so $x = y$, and hence $xy^{-1} = 1$, proving the claim.

Now let $\tau : G \to P$ be the transfer map. By the Focal Subgroup Theorem,

$$P \cap \ker(\tau) = F_G(P) = 1.$$

Set $N = \ker(\tau)$. Then $P \cap N = 1$. Also, $|PN| = |P||N|$, so $|G : N| = |P|$, and $G/N \cong \mathrm{Im}(\tau) \leq P$, so G/N is a p-group. This means $|N|$ is coprime to p, so N is a p'-group and $G = PN$. □

Example 9.23
Some examples.

1. If $G = A_4$ and $P = P_3 = \langle (123) \rangle \in \mathrm{Syl}_3(G)$, then clearly $P = C_G(P) = N_G(P)$, and so $P \leq Z(N_G(P))$.
2. In general, if $G = PN$ where P is abelian and $N \trianglelefteq G$ is a p'-group, then $P \in \mathrm{Syl}_p(G)$ and $P \leq Z(N_G(P))$.

Theorem 9.24

Let p be the smallest prime dividing $|G|$, and suppose that $P \in \mathrm{Syl}_p(G)$ is cyclic. Then G has a normal p-complement (i.e. a finite normal group of order coprime to p).

Note 9.25. A cyclic Sylow p-subgroup is highly structured and easy to understand—it has no nontrivial commutator structure. When it's also the smallest prime dividing $|G|$, this limits how G can act on it, making it easier to isolate the p-part of the group. This isolation allows Burnside's theorem to be applied, giving a normal complement N of order coprime to p, so that $G = PN$. This is a beautiful bridge between the structure of small subgroups and the whole group.

Proof. Since P is cyclic, it is abelian, so $P \leq C_G(P)$. By a previous proposition $N_G(P)/C_G(P)$ embeds into $\mathrm{Aut}(P)$, which is a p'-group because $P \cong C_{p^a}$ and $|\mathrm{Aut}(C_{p^a})| = p^{a-1}(p-1)$. Thus $N_G(P)/C_G(P)$ is a p'-group, and so the whole of $N_G(P)$ is equal to $C_G(P)$. Then

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

and Burnside's theorem applies, giving a normal p-complement. □

Corollary 9.26

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

Proof. Proceed by induction on $|G|$. If $|G| = 1$, the result is clear. Otherwise, let p be the smallest prime dividing $|G|$ and let $P \in \mathrm{Syl}_p(G)$. By Theorem 9.9, G has a normal p-complement $N \trianglelefteq G$ such that $G = PN$ and $P \cap N = 1$. So $G/N \cong P$ is cyclic, and hence solvable. Also, N is smaller than G and by assumption all its Sylow subgroups are cyclic, so by induction N is solvable. Thus G is an extension of solvable groups, and hence solvable. □

Corollary 9.27

If $|G|$ is square-free, i.e., $|G| = p_1 \cdots p_k$ for distinct primes p_i, then G is solvable.

Proof. Each Sylow subgroup of G is cyclic of prime order, hence cyclic. So Corollary 9.10 applies, and G is solvable. □

Corollary 9.28. Let $|G| = p^2qr$, where p, q, r are distinct primes, and suppose G is simple. Then $|G| = 60$ (hence $G \cong A_5$).

Proof. By a previous theorem, p must be the smallest of the primes p, q, r. Let $P \in \mathrm{Syl}_p(G)$, so that $|P| = p^2$. Then P is not cyclic by a previous corollary, so $P \cong C_p \times C_p$.

By Burnside's theorem we must have $P < N_G(P)$, and so $|N_G(P)| = p^2q$ or p^2r. Swapping q, r if necessary, we may take $|N_G(P)| = p^2q$. Write $N = N_G(P)$ and let $Q \in \mathrm{Syl}_q(N)$. Then $|Q| = q$ and $N_G(P) = PQ = P \rtimes_\iota Q$, where $\iota : Q \to \mathrm{Aut}(P)$.

If ι is trivial then $N_G(P) = P \times Q$ and $P \leq Z(N_G(P))$, which is not possible by Burnside.

Hence $\iota : Q \to \mathrm{Aut}(P)$ is nontrivial, which means that $\mathrm{Aut}(P)$ contains the image $\iota(Q)$, a subgroup of order q. Hence q divides $|\mathrm{Aut}(P)| = |\mathrm{Aut}(C_p \times C_p)| = |\mathrm{GL}_2(p)|$. Since

$$|\mathrm{GL}_2(p)| = p(p^2-1)(p-1) = p(p+1)(p-1)^2,$$

it follows that q divides $p-1$ or $p+1$. On the other hand, p is the smallest of the primes p, q, r, so $q > p$. Therefore $q = p+1$, and so we must have $p = 2, q = 3$. Thus $|G| = 12r$ with $r > 3$.

Now $n_r(G) \equiv 1 \mod r$ and divides 12. Hence $r = 5$ or 11. If $r = 11$ then $n_r(G) = 12 = |G : N_G(R)|$, so we have $R = C_G(R) = N_G(R)$, giving a contradiction by Burnside. So finally $r = 5$ and we have $|G| = 12r = 60$. □

Note 9.29. The goal is to prove that any simple group of order p^2qr (with distinct primes) must actually have order 60. The argument works by:

- Applying Burnside's Transfer Theorem to guarantee a normal p-complement if the Sylow p-subgroup is cyclic, hence showing that P must be non-cyclic.
- Analysing the structure of $N_G(P)$ when $P \cong C_p \times C_p$, and using properties of automorphism groups to restrict possible orders.
- Finally, applying arithmetic restrictions (such as divisibility and minimality of p) to pin down the possible values of p, q, r, leading to the unique solution $|G| = 60$.

This demonstrates how Burnside's theorem links local group structure (Sylow subgroups and their normalisers) to the global classification of finite simple groups.

10 Mastery material

10.1 The General and Special linear groups

Proposition 10.1
$\mathrm{GL}_n(r)/\mathrm{SL}_n(r) \cong \mathbb{Z}_r^\times$

10.2 Primitive Group Actions

Definition 10.2. An equivalence relation $\sim$ on Ω is said to be G**-invariant** if for all $\alpha, \beta \in \Omega$ with $\alpha \sim \beta$, and for all $g \in G$, we have

$$g \cdot \alpha \sim g \cdot \beta.$$

In other words, the equivalence classes are preserved under the action of G.

Definition 10.3. Let G be a group acting on a set Ω. We say that the action of G on Ω is **primitive** if:

- The action is **transitive**, i.e., for all $\alpha, \beta \in \Omega$, there exists $g \in G$ such that $g \cdot \alpha = \beta$; and
- There is **no non-trivial** G-invariant equivalence relation on Ω.

Equivalently, G acts primitively on Ω if the stabiliser G_α of a point $\alpha \in \Omega$ is a **maximal subgroup** of G.

10.3 Symplectic Groups

Number of Points in Projective Space $\mathbb{P}^n(\mathbb{F}_q)$

Formula:

$$|\mathbb{P}^n(\mathbb{F}_q)| = \frac{q^{n+1} - 1}{q - 1}$$

Note: The expression is a geometric series:

$$|\mathbb{P}^n(\mathbb{F}_q)| = 1 + q + q^2 + \cdots + q^n$$

10.3.1 The Pfaffian

Definition 10.4. A square matrix $A \in \mathbb{R}^{n \times n}$ is called **skew-symmetric** if

$$A^\top = -A,$$

This means that for all i, j,

$$a_{ij} = -a_{ji}.$$

Proposition 10.5
In particular, all diagonal entries of a skew-symmetric matrix must be zero.

Proof. Since $a_{ii} = -a_{ii}$ implies $a_{ii} = 0$. □

Theorem 10.6. We have the following.

1. The determinant of a skew-symmetric matrix is square.
2. The determinant of a skew-symmetric matrix of odd size is zero.
3. There is a unique polynomial $\mathrm{Pf}(A)$ in the inderterminates a_{ij} such that if A is a skew-symmetric $2n \times 2n$ matrix then $\det(A) = \mathrm{Pf}(A)^2$.

Theorem 10.7
If A is a skew-symmetric matrix and P any invertibel matrix, then

$$\mathrm{Pf}(PAP^\top) = \det(P)\mathrm{Pf}(A).$$

10.4 The Symplectic groups

Definition 10.8. The **symplectic group** $\mathrm{Sp}(2n, F)$ is the group of $2n \times 2n$ invertible matrices over a field F that preserve a fixed non-degenerate alternating bilinear form. That is, it is the set of matrices $P \in \mathrm{GL}(2n, F)$ such that

$$P^\top A P = A,$$

where A is a fixed invertible skew-symmetric matrix. A standard choice for A is

$$A = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \quad \text{or} \quad A = \mathrm{diag}\left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right).$$

Definition 10.9. The **projective symplectic group** $\mathrm{PSp}(2n, F)$ is defined as the quotient group

$$\mathrm{PSp}(2n, F) = \mathrm{Sp}(2n, F)/\{\pm I\}.$$

Proposition 10.10

We have the following

(a) $\mathrm{Sp}(2n, F)$ is a subgroup of $\mathrm{SL}(2n, F)$.

(b) $\mathrm{PSp}(2n, F) \cong \mathrm{Sp}(2n, F)/\{\pm I\}$.

Proof. We prove each statement in turn.

(a) Let $P \in \mathrm{Sp}(2n, F)$. Then using the property of the Pfaffian, we compute

$$\mathrm{Pf}(A) = \mathrm{Pf}(PAP^\top) = \det(P)\mathrm{Pf}(A),$$

which implies $\det(P) = 1$. Therefore, $P \in \mathrm{SL}(2n, F)$.

(b) Suppose $P = cI$ satisfies $PAP^\top = A$. Then

$$(cI)A(cI) = c^2 A = A \Rightarrow c^2 = 1 \Rightarrow c = \pm 1.$$

So the only scalar matrices in $\mathrm{Sp}(2n, F)$ are $\pm I$, and hence

$$\mathrm{PSp}(2n, F) \cong \mathrm{Sp}(2n, F)/\{\pm I\}.$$

□

10.5 Orders and isomorphisms

Proposition 10.11.

$$|\mathrm{Sp}(2n, q)| = \prod_{i=1}^{n} (q^{2i} - 1) q^{2i-1} = q^{n^2} \prod_{i=1}^{n} (q^{2i} - 1).$$

For $PSp(2n, q)$, divide the above by $\gcd(2, q - 1)$.

Proposition 10.12

Let F be a field. Then:

1. $\mathrm{Sp}(2, F) \cong \mathrm{SL}(2, F)$.
2. $\mathrm{PSp}(2, F) \cong \mathrm{PSL}(2, F)$.

Proof. We prove each statement in turn.

1. We show this by exhibiting a non-degenerate bilinear form on F^2 preserved by $\mathrm{SL}(2, F)$. Define:
$$B(x, y) = \det \begin{pmatrix} x \\ y \end{pmatrix},$$
for all $x, y \in F^2$, where the matrix has x and y as rows. This is an alternating bilinear form and hence a symplectic form.

   Let $P \in \mathrm{SL}(2, F)$. For any $x, y \in F^2$, observe that
$$\begin{pmatrix} xP \\ yP \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} P, \quad \text{so} \quad B(xP, yP) = \det \begin{pmatrix} xP \\ yP \end{pmatrix} = \det \begin{pmatrix} x \\ y \end{pmatrix} \det(P) = B(x, y),$$
since $\det(P) = 1$. So all elements of $\mathrm{SL}(2, F)$ preserve B, and hence $\mathrm{SL}(2, F) \subseteq \mathrm{Sp}(2, F)$. They are equal as subgroups of $\mathrm{GL}(2, F)$.

2. Part (2) follows immediately by quotienting both groups by their centres $\{\pm I\}$.

□

Remark 10.13. In particular $\mathrm{PSp}(2, F)$ is simple if and only if $|F| > 3$,

Proposition 10.14

An example of a non-simple symplectic group.
$$\mathrm{PSp}(4, 2) \cong S_6.$$

Proof. Let $F = \mathbb{F}_2$ and $V = F^6$. Define the standard inner product:
$$x \cdot y = \sum_{i=1}^{6} x_i y_i.$$
Let $j = (1, 1, 1, 1, 1, 1)$ be the all-1 vector. Then for all $x \in V$, we have:
$$x \cdot x = x \cdot j.$$
Hence, the inner product induces a degenerate alternating form on the hyperplane:
$$j^\perp = \{x \in V : x \cdot j = 0\},$$

but it becomes non-degenerate on the quotient space $j^\perp/\langle j\rangle$ of rank 4. This space admits a symplectic form B, and S_6 acts as isometries of B by permuting coordinates. Hence,

$$S_6 \leq \mathrm{Sp}(4,2) = \mathrm{PSp}(4,2).$$

Since

$$|S_6| = 6! = 720 = 15 \cdot 8 \cdot 3 \cdot 2 = |\mathrm{Sp}(4,2)|,$$

we conclude that $S_6 \cong \mathrm{PSp}(4,2)$. □

10.6 Generation and simplicity

We follow the analogy with $\mathrm{PSL}(n,F)$ to show that the symplectic group $\mathrm{Sp}(2n,F)$ is generated by *symplectic transvections*. Moreover, it equals its own derived group, and its projective version $\mathrm{PSp}(2n,F)$ is simple for $n \geq 2$, except in the special case $\mathrm{PSp}(4,2)$.

Transvections and Elations

Definition 10.15. Let F be a commutative field, and let V be an F-vector space. A **transvection** is a linear map $T : V \to V$ such that:

$$\mathrm{rank}(T - I) = 1 \quad \text{and} \quad (T - I)^2 = 0.$$

This implies T can be written in the form:

$$T(x) = x + (f(x))a,$$

for some $a \in V$ and $f \in V^*$ such that $f(a) = 0$.

Definition 10.16. We define the following.

- The **axis** of the transvection is $\ker(T - I) = \ker(f)$, a hyperplane fixed pointwise by T.
- The **centre** of the transvection is $\mathrm{Im}(T - I) = \langle a\rangle$; any subspace containing this is fixed as a set by T.

Definition 10.17. In projective geometry, the transformation induced by a transvection is called an **elation**. All elations lie inside $\mathrm{PSL}(n,F)$.

Symplectic Transvections

Let B be a symplectic form on a vector space V. We seek transvections that preserve B. A general transvection has the form

$$x \mapsto x + (f(x))a,$$

where $a \in V$, $f \in V^*$, and $f(a) = 0$ (i.e., $a \in \ker(f)$).

To preserve B, we require:

$$B(x + (f(x))a, y + (f(y))a) = B(x,y).$$

Expanding and using bilinearity of B, we get:

$$B(x,y) + (f(x))B(a,y) - (f(y))B(a,x) = B(x,y),$$

which simplifies to:

$$(f(x))B(a,y) = (f(y))B(a,x).$$

Assuming $B(a,x) \neq 0$, define $\lambda = \frac{f(x)}{B(a,x)}$. Then we must have:

$$f(y) = \lambda B(a,y) \quad \text{for all } y,$$

so that the map becomes:

$$x \mapsto x + \lambda B(x,a)a.$$

Definition 10.18. A **symplectic transvection** is a transvection that preserves the symplectic form B, and has the form

$$x \mapsto x + \lambda B(x,a)a.$$

Proposition 10.19

The **centre** of this map is $\langle a \rangle$ and the **axis** is:

$$a^{\perp} = \{x \in V : B(x,a) = 0\}.$$

Lemma 10.20

For $r \geq 3$, and for $r = 2$ and $F \neq \mathbb{F}_2$, the group $\mathrm{PSp}(2r, F)$ is equal to its derived group.

Proof. If $F \neq \mathbb{F}_2, \mathbb{F}_3$, we know from Lemma 2.8 that any element inducing a transvection on a hyperbolic plane and the identity on the complement is a commutator, so the result follows. The same argument completes the proof provided that we can show it holds for $\mathrm{PSp}(6,2)$ and $\mathrm{PSp}(4,3)$.

To handle these two groups, we introduce a standard notation. Reorder the rows and columns of the standard skew-symmetric matrix so that

$$J = \begin{pmatrix} O & I \\ -I & O \end{pmatrix},$$

where O and I are $r \times r$ zero and identity matrices, respectively. A matrix C belongs to the symplectic group if and only if $C^{\top} J C = J$.

We find:

(a) For all invertible $r \times r$ matrices A, we have

$$\begin{pmatrix} A^{-1} & O \\ O & A^{\top} \end{pmatrix} \in \mathrm{Sp}(2r, F).$$

(b) For all symmetric $r \times r$ matrices B, we have

$$\begin{pmatrix} I & B \\ O & I \end{pmatrix} \in \mathrm{Sp}(2r, F).$$

A straightforward computation shows that the commutator of the two matrices in (a) and (b) is

$$\begin{pmatrix} I & B - ABA^\top \\ O & I \end{pmatrix},$$

and it suffices to choose A and B such that A is invertible, B is symmetric, and $B - ABA^\top$ has rank 1.

Suitable choices:

(a) $r = 2$, $F = \mathrm{GF}(3)$, with

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

(b) $r = 3$, $F = \mathrm{GF}(2)$, with

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

□

Appendix

A Table of factorials

n	$n!$
0	1
1	1
2	2
3	6
4	24
5	120
6	720
7	5040

References

[1] J.S. Rose. *A Course on Group Theory*. A course on group theory. Dover Publications, 1994.

[2] J.J. Rotman. *An Introduction to the Theory of Groups*. Graduate Texts in Mathematics. Springer New York, 2012.