Warwick Mathematics Exchange

MA3K4

Introduction to Group Theory

2024, April 15th

Desync, aka The Big Ree

Contents

Introduction

ree

Disclaimer: I make *absolutely no guarantee* that this document is complete nor without error. In particular, any content covered exclusively in lectures (if any) will not be recorded here. This document was written during the 2023 academic year, so any changes in the course since then may not be accurately reflected.

Notes on formatting

New terminology will be introduced in *italics* when used for the first time. Named theorems will also be introduced in *italics*. Important points will be **bold**. Common mistakes will be underlined. The latter two classifications are under my interpretation. YMMV.

Content not taught in the course will be outlined in the margins like this. Anything outlined like this is not examinable, but has been included as it may be helpful to know alternative methods to solve problems.

The table of contents above, and any inline references are all hyperlinked for your convenience.

History

First Edition: 2024-04-06*
Current Edition: 2024-04-15

Authors

This document was written by R.J. Kit L., a maths student. I am not otherwise affiliated with the university, and cannot help you with related matters.

Please send me a PM on Discord @Desync#6290, a message in the WMX server, or an email to Warwick.Mathematics.Exchange@gmail.com for any corrections. (If this document somehow manages to persist for more than a few years, these contact details might be out of date, depending on the maintainers. Please check the most recently updated version you can find.)

If you found this guide helpful and want to support me, you can buy me a coffee!

(Direct link for if hyperlinks are not supported on your device/reader: ko-fi.com/desync.)

*Storing dates in big-endian format is clearly the superior option, as sorting dates lexicographically will also sort dates chronologically, which is a property that little and middle-endian date formats do not share. See ISO-8601 for more details. This footnote was made by the computer science gang.

1 Glossary

$H \leq G$	H is a subgroup of G.
$H \trianglelefteq G$	H is a normal subgroup of G.
gH	A coset of H in G; the set $gH = \{gh : g \in G\}$.
G/H	The set of left cosets of H in G; the set $\{gH : g \in G\}$.
G/N	The quotient or factor group of G by N; the set of left cosets of a normal subgroup N in G, equipped with the operation $gN \circ hN = ghN$
$[G : H]$	The index of H in G; the cardinality $\lvert G/H \rvert$; the number of distinct left cosets of H in G.
${}^g h$	The conjugation of h by g; the element ghg^{-1}.
${}^g H$	The conjugation of a subset $H \subseteq G$ by an element $g \in G$; the set $gHg^{-1} = \{ghg^{-1} : h \in H\}$.
$N_G(H)$	The normaliser of H in G; the set $\{g \in G : gHg^{-1} = H\}$. The normaliser is always a subgroup of G.
$C_G(x)$	The centraliser or commutant of x in G; the set of elements that commute with x; the set $\{g \in G : gx = xg\}$. The centraliser is always a subgroup of G.
$Z(G)$	The centre of G; the set of elements that commute with all elements of G; the set $\{g \in G : \forall h \in G : gh = hg\}$. The centre is always a normal subgroup in G.
$\mathrm{Cl}(x)$, ${}^G x$	The conjugacy class of x; the set $\{gxg^{-1} : g \in G\}$.
$\mathrm{Orb}_G(x)$	The orbit of x in G; the set of possible images of x under an action; the set $\{g \cdot x : g \in G\}$.
$\mathrm{Stab}_G(x)$	The stabiliser of x in G; the set of elements that fix x; the set $\{g \in G : g \cdot x = x\}$. The stabiliser is always a subgroup of G.
$\mathrm{fix}_X(g)$	The set of fixed points of g; the set $\{x \in X : g \cdot x = x\}$.
$\mathrm{Syl}_p(G)$	The set of Sylow p-subgroups of G.
$F_p(G)$	The set $\{x \in G : x \neq 1_G$ and $\lvert x \rvert$ is a power of $p\}$.

$\lvert G\rvert_p$	The highest power of p that divides G; if $\lvert G\rvert = p^n m$, then $\lvert G\rvert_p = p^n$.
$H \ltimes_\phi K$	The semidirect product of H and K; the set $H \times K$ equipped with the multiplication $(h_1,k_1) \cdot (h_2,k_2) \coloneqq (h_1 h_2, \phi_{h_2^{-1}}(k_1) k_2)$, where $\phi : H \to \mathrm{Aut}(K)$ is a homomorphism and $\phi(h) = \phi_h$.
$[g,h]$	The commutator of g and h; the element $ghg^{-1}h^{-1}$.
$[G,G]$	The commutator subgroup of G; the subgroup generated by $\langle [g,h] \mid g,h \in G \rangle$.
$[H,K]$	The commutator subgroup of H and K, given $H,K \leq G$; the subgroup generated by $\langle [h,k] \mid h \in H, k \in K \rangle$.
G^{ab}	The abelianisation of G; the abelian quotient group $G/[G,G]$.
$G^{(n)}$	The nth derived subgroup of G, where $G^{(0)} = G$ and $G^{(n)} = \left[G^{(n-1)}, G^{(n-1)}\right]$ for $n \in \mathbb{N}$.

2 Review

Recall that a *group* is a pair $(G,\circ)$, consisting of an *underlying set* G and a *group operation* $\circ : G\times G \to G$ that satisfies the following properties:

(G1) $\forall a,b,c \in G : (a\circ b)\circ c = a\circ(b\circ c)$ (associativity);

(G2) $\exists 1_G \in G, \forall g \in G : g\circ 1_G = 1_G \circ g = g$ (existence of identity);

(G3) $\forall g \in G, \exists g^{-1} \in G : g\circ g^{-1} = g^{-1}\circ g = 1_G$ (existence of inverses).

The group is furthermore *abelian* if the group operation additionally satisfies

(A) $\forall a,b \in G : a\circ b = b\circ a$ (commutativity).

When the context is clear, we will usually omit the operation and simply say that G is a group.

Sometimes, closure of $\circ$ over the set G is also included as an axiom, but this is implicit in $\circ$ being an operation over G.

It follows from these axioms that the identity element and the inverse of any given element g are unique, so we are justified in calling them *the* identity and *the* inverse of g.

The number of elements in a group G is called the *order* of G, and is denoted by $|G|$. (This coincides with the cardinality of the underlying set, so the notation is meaningful.)

Theorem 2.1 (Basic Properties of Groups)**.**

- *If $ga = gb$ or $ag = bg$, then $a = b$ (cancellative property);*
- *The identity element 1_G is unique;*
- *For every element g, the inverse g^{-1} is unique;*
- *If e_ℓ is a left identity (i.e. $e_\ell g = g$ for all $g \in G$), and/or e_r is a right identity, then $e_\ell = 1_G = e_r$;*
- *If ℓ is a left inverse for an element g (i.e. $\ell g = 1_G$), and/or r is a right inverse for g, then $\ell = g^{-1} = r$;*
- *For all $a,b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$;*
- *For all $g \in G$, $(g^{-1})^{-1} = g$.*

2.1 Symmetric Groups

Let X be a finite set. We write $\mathrm{Sym}(X)$ for the set of bijections $f : X \to X$. This set has group structure under composition:

(G1) For any functions $f,g,h \in \mathrm{Sym}(X)$ and $x \in X$, $\big((f\circ g)\circ h\big)(x) = f\big(g(h(x))\big) = \big(f\circ(g\circ h)\big)(x)$;

(G2) The identity function id_X is the identity element;

(G3) The inverse function f^{-1} for a function f is also its inverse in the group.

This group is called the *symmetric group* on X, and its elements are called *permutations*.

The symmetric group is abelian if and only if $|X| \le 2$.

2.1.1 Cycle Notation

Let $a_1,a_2,\ldots,a_r$ be distinct elements of a set X. The *cycle* $(a_1,a_2,\ldots,a_r)$ represents the permutation $f \in \mathrm{Sym}(X)$ with

- $f(a_i) = a_{i+1}$ for $1 \le i < r$;

- $f(a_r) = a_1$;
- $f(b) = b$ for $b \in X \setminus \{a_1,a_2,\dots a_r\}$;

The empty cycle () is a cycle, corresponding to the identity permutation id_X.

Two cycles $(a_1,\dots,a_r)$ and $(b_1,\dots,b_s)$ are *disjoint* if $\{a_1,\dots,a_r\} \cap \{b_1,\dots,b_s\} = \emptyset$.

Note that the representation of a permutation in cycle notation is not unique. For instance, $(1,2,3) = (3,1,2) = (2,3,1)$.

Theorem 2.2.

- $\big|\mathrm{Sym}(X)\big| = |X|!$.
- *Every permutation in* $\mathrm{Sym}(X)$ *can be expressed as a product of disjoint cycles.*

  Moreover, this product is unique in the sense that if $f \in \mathrm{Sym}(X)$ *has representations* $f = f_1 \cdots f_m = g_1 \cdots g_n$*, where the* f_i *and* g_i *are disjoint cycles of length greater than* 1*, then* $m = n$ *and* $\{f_1,\dots,f_m\} = \{g_1,\dots,g_n\}$*.*

2.2 General Linear Groups

Let K be a field and n be a positive integer. We define the set $\mathrm{GL}_n(K)$ to be the set of invertible $n \times n$ matrices with entries in K. Under the operation of matrix multiplication, this set forms a group called the *general linear group of dimension* n *over* K.

Recall that if K is a field (or more generally, a ring), then the *characteristic* of K is the smallest positive number p such that

$$p1_K = \underbrace{1_K + \cdots + 1_K}_{p} = 0_K$$

if such a number exists, and 0 otherwise. In the finite case, such a number will always exist, and moreover, this number is prime. The characteristic also satisfies

$$|K| = p^n$$

for some positive integer n.

Theorem 2.3. *Let* K *be a finite field, and let* $q = |K|$*. Then,*

$$\big|GL_n(K)\big| = q^{\binom{n}{2}} \prod_{i=1}^{n} (q^i - 1)$$

2.3 Orders of Elements

In multiplicative notation, we write g^n to mean the n-fold iteration of the group operation on g. If $n = 0$, then $g^n = 1_G$, and if $n < 0$, then $g^n = (g^{-1})^n$.

Let G be a group, and let $g \in G$. The *order* of g, denoted by $|g|$ is the smallest positive integer n such that $g^n = 1_G$, if such a number exists, and ∞ otherwise:

$$|g| := \begin{cases} \min\{n \in \mathbb{Z}^+ : g^n = 1_G\} & \exists n \in \mathbb{Z}^+ : g^n = 1_G \\ \infty & \text{otherwise} \end{cases}$$

Theorem 2.4.

- *The identity element* 1_G *is the unique element of order* 1*.*
- *For all* $g \in G$*,* $|g| = |g^{-1}|$*.*

Proof. Clearly, 1_G has order 1. Now suppose an element $e \in G$ also has order 1. Then, $e = e^1 = 1_G$, so $e = 1_G$.

Suppose $|g| = n$. Then, $(g^{-1})^n = (g^n)^{-1} = (1_G)^{-1} = 1_G$, so $|g^{-1}| = n$. ■

Lemma 2.5. *Let G be a group and let $a,b \in G$ have finite order. Then,*

(*i*) *If $\ell \in \mathbb{Z}^+$, then $a^\ell = 1_G$ if and only if n divides ℓ;*

(*ii*) *If $m \in \mathbb{Z}^+$, then $|a^m| = |a| / \gcd(|a|,m)$;*

(*iii*) *If a and b commute, then $|ab|$ divides $\operatorname{lcm}(|a|,|b|)$;*

(*iv*) *If a and b commute and $\langle a \rangle \cap \langle b \rangle = \{1_G\}$, then $|ab| = \operatorname{lcm}(|a|,|b|)$.*

2.4 Subgroups

A subset $H \subseteq G$ of a group G is a *subgroup* of $(G,\circ)$ if $(H,\circ)$ is itself a group, and we write $H \leq G$ to denote this relation.

Lemma 2.6. *Let $H \subseteq G$ be a non-empty subset. Then, $H \leq G$ if and only if for all $g,h \in H$, we have $gh^{-1} \in H$.*

Given an element $g \in G$, the (*cyclic*) *subgroup generated by* g is the subgroup defined by

$$\langle g \rangle := \{g^i : i \in \mathbb{Z}\}$$

and we say that g is a *generator* of G. Conversely, a group is called *cyclic* if it is in this form.

Lemma 2.7. *If $G = \langle g \rangle$ is cyclic, then $|G| = |g|$.*

More generally, given a non-empty subset $S \subseteq G$, the *subgroup generated by* S is the subgroup defined by

$$\langle S \rangle := \{s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_m^{\epsilon_m} : m \in \mathbb{N}, s_i \in S, \epsilon_i \in \{\pm 1\}\}$$

That is, the subgroup containing all linear combinations of elements in S. If $S = \{s_1, \ldots, s_n\}$, then we also write $\langle S \rangle = \langle s_1, \ldots, s_n \rangle$ for this subgroup.

2.4.1 Cosets

Given a subgroup $H \leq G$ of a group G and an element $g \in G$, the *left coset* gH of H in G is the set

$$gH = \{gh : h \in H\} \subseteq G$$

Lemma 2.8. *Let G be a group and $H \leq G$ a subgroup. Then, the following are equivalent for all $g,k \in G$:*

(*i*) *$k \in gH$;*

(*ii*) *$gH = kH$;*

(*iii*) *$g^{-1}k \in H$.*

Proof. (*i*) → (*ii*): Note that $hH = H$ for all $h \in H$. Now, if $k \in gH$, then $k = gh$ for some $h \in H$, so $kH = (gh)H = g(hH) = gH$.

(*ii*) → (*iii*): Because H is a subgroup, $1_G \in H$, so $k = k1_G \in kH$. If $kH = gH$, then also $k \in gH$, so for some $h \in H$, $k = gh$, so $g^{-1}k = h \in H$.

(*iii*) → (*i*): If $g^{-1}k = h \in H$, then $k = gh \in gH$. ■

Let G be a group and $H \leq G$ be a subgroup. Define the relation $\sim_H$ on G with $g \sim_H h$ if and only if $gH = hH$.

Corollary 2.8.1. *$\sim_H$ is an equivalence relation on G.*

Lemma 2.9. *Let G be a group and $H \leq G$ be a subgroup. Then,*

(i) For all g,$h \in G$, either $gH = hH$ or $gH \cap hH = \emptyset$;

(ii) If $\{g_i H\}_{i \in I}$ is the set of $\sim_H$-equivalence classes in G, then

$$G = \bigsqcup_{i \in I} g_i H$$

Proof. Since $\sim_H$ is an equivalence relation, distinct $\sim_H$-equivalence classes are pairwise disjoint and partition G. Both parts follow. ■

Theorem 2.10 (Lagrange)**.** *Let G be a finite group and let $H \leq G$ be a subgroup. Then, $|H|$ divides $|G|$. Specifically,*

$$|G| = |G : H||H|$$

Proof. The left cosets of H in G partition G by the previous lemma. Also, each left coset gH is equinumerous to H since $h \mapsto gh$ is a bijection $H \to gH$ (with inverse given by $h \mapsto g^{-1}h$), and the number of left cosets is the index $[G : H]$. The result follows. ■

Let G be a group and $H \leq G$ be a subgroup.

- The set of left cosets of H in G is denoted by $G/H \coloneqq \{gH : g \in G\}$.
- The number of distinct left cosets of H in G (i.e. the cardinality $|G/H|$) is called the *index* of H in G, and is denoted by $[G : H]$. If G is finite, then

$$[G : H] = |G|/|H|$$

Corollary 2.10.1. *Let G be a finite group and let $g \in G$. Then $|g|$ divides $|G|$.*

Proof. The subgroup $\langle g \rangle$ has order $|g|$. The result follows from Lagrange's theorem. ■

2.5 Normal Subgroups

Lemma 2.11. *Let $H \leq G$ be a subgroup of a group G, and let $g \in G$. Then, ${}^gH = gHg^{-1} = \{ghg^{-1} : h \in H\}$ is a subgroup of G.*

Let G be a group and let $H \leq G$ be a subgroup.

- H is *normal* in G if $gHg^{-1} = H$ for all $g \in G$, and we write $H \trianglelefteq G$ to denote this relation.
- The *normaliser* of H in G, is the subgroup of G defined by

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

Note that H is normal in G if and only if $N_G(H) = G$.

Theorem 2.12. *Let G be a group and let $H \leq G$ be a subgroup. Then,*

(i) H is normal in G if and only if $gHg^{-1} \subseteq H$ for all $g \in G$;

(ii) If $[G : H] = 2$, then H is normal in G;

(iii) $H \trianglelefteq N_G(H) \leq G$;

(iv) $G \trianglelefteq G$;

(v) $\{1_G\} \trianglelefteq G$.

A non-trivial group G is *simple* if the only normal subgroups of G are $\{1_G\}$ and G.

Given subsets $A,B \subseteq G$ of a group G, we write $AB \coloneqq \{ab : a \in A, b \in B\}$ for the internal product of A and B. In general, this is not a subgroup, even if A and B are both subgroups.

Lemma 2.13. *Let N be normal in G, and let $g,h \in G$. Then, $(gN)(hN) = ghN$.*

Let N be normal in G. Then, the binary operation $\circ : G/N \times G/N \to G/N$ defined by $(gN) \circ (hN) = ghN$ is called the *natural binary operation* of G/H.

With the natural binary operation $\circ$, $(G/N,\circ)$ is a group called the *quotient* or *factor* group of G by N.

2.6 Group Homomorphisms

Let $(G,\circ)$ and $(H,*)$ be groups.

A map $\phi : G \to H$ is a *group homomorphism* if $\phi(g \circ h) = \phi(g) * \phi(h)$ for all $g,h \in G$.

If ϕ is a homomorphism and has an inverse (or equivalently, is bijective), then φ is an *isomorphism*, and we say that G and H are *isomorphic*, written as $G \cong H$. An isomorphism from a group to itself is also called an *automorphism*.

We define the *kernel* and *image* of a homomorphism ϕ as the sets

$$\ker(\phi) \coloneqq \{g \in G : \phi(g) = 1_G\}$$
$$\operatorname{im}(\phi) \coloneqq \{\phi(g) : g \in G\}$$

Let N be normal in G. A the map $\pi : G \to G/N$ defined by $\pi(g) = gN$ is a surjective homomorphism called the *quotient map* or *natural homomorphism* from G to G/N.

Theorem 2.14. *If n and m are coprime, then $C_n \times C_m \cong C_{nm}$.*

Theorem 2.15 (First Isomorphism Theorem)**.** *Let G and H be groups, and let $\phi : G \to H$ be a group homomorphism. Then,*

(i) $\ker(\phi) \trianglelefteq G$;

(ii) $\operatorname{im}(\phi) \leq H$;

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

Theorem 2.16 (Second Isomorphism Theorem)**.** *Let G be a group, $H \leq G$ a subgroup, and $N \trianglelefteq G$ be normal in G. Then,*

(i) $NH = HN \leq G$;

(ii) $H \cap N \trianglelefteq H$;

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

Theorem 2.17 (Third Isomorphism Theorem)**.** *Let G be a group, and let $N,K \trianglelefteq G$ be normal in G with $N \subseteq K \subseteq G$. Then,*

(i) $K/N \trianglelefteq G/N$;

(ii) $(G/N)/(K/N) \cong G/K$.

Theorem 2.18 (Correspondence Theorem)**.** *Let G be a group, and let $N \trianglelefteq G$ be normal in G. Then, there is a bijection between the subgroups of G containing N and the subgroups of G/N. More precisely, the map*

$$f : \{S : S \leq G/N\} \to \{S : N \leq S \leq G\} : S \mapsto S/N$$

is a bijection, and moreover, this map sends normal subgroups to normal subgroups.

3 Permutation Groups

Let X be a set. A subgroup of $\mathrm{Sym}(X)$ is called a *permutation group* on X.

For $g \in \mathrm{Sym}(X)$, the *support* of g is the set

$$\mathrm{supp}(g) \coloneqq \{x \in X : g(x) \neq x\}$$

and for a permutation group G, the *support* of G is the set

$$\mathrm{supp}(G) \coloneqq \{x \in X : g(x) \neq x\}$$

If $G = \langle g \rangle \leq \mathrm{Sym}(X)$, then $\mathrm{supp}(\langle g \rangle) = \mathrm{supp}(g)$. Also note that if

$$g = (a_1, \ldots, a_{m_1}) \cdots (a_{m_{t-1}+1}, \ldots, a_{m_t})$$

is a product of disjoint cycles, then

$$\mathrm{supp}(g) = \{a_1, \ldots, a_{m_1}, a_{m_1+1}, \ldots, a_{m_{t-1}+1}, \ldots, a_{m_t}\}$$

Theorem 3.1. *Let X be a finite set. Then,*

(i) Disjoint cycles in $\mathrm{Sym}(X)$ commute;

(ii) If $f = (a_1, \ldots, a_r) \in \mathrm{Sym}(X)$ is a cycle of length r, then f has order $|f| = r$.

More generally, if $f = f_1 \cdots f_m$ is a product of disjoint cycles, then f has order

$$|f| = \mathrm{lcm}\big(|f_1|, \ldots, |f_m|\big)$$

(iii) Let $f = (a_1, \ldots, a_r) \in \mathrm{Sym}(X)$ and $g \in \mathrm{Sym}(X)$. Then,

$${}^{g}f = gfg^{-1} = \big(g(a_1), \ldots, g(a_r)\big)$$

Let $n \geq 3$ and set $X = \{1, \ldots, n\}$. Define the permutations $\sigma, \tau \in \mathrm{Sym}(X)$ by

$$\sigma \coloneqq (1, \ldots, n)$$
$$\tau \coloneqq \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} (i, n-i+1)$$

Then, the *dihedral group* D_{2n} of order $2n$ is the subgroup of $\mathrm{Sym}(X)$ generated by σ and τ.

Example. If $n = 8$, then

$$D_{16} = \big\langle \{(1,2,3,4,5,6,7,8), (1,8)(2,7)(3,6)(4,5)\} \big\rangle$$

△

Lemma 3.2. *If $H, K \leq G$ with $H = \langle A \rangle$ finite and $K = \langle B \rangle$ for some subsets $A, B \subseteq G$, then $K \subseteq N_G(H)$ if and only if ${}^{b}a \in H$ for all $a \in A$ and $b \in B$.*

Theorem 3.3. *Let $n \geq 3$ and $D_{2n} = \langle\{\sigma,\tau\}\rangle$. Then,*

(*i*) $|D_{2n}| = 2n$;

(*i*) $\langle\sigma\rangle \trianglelefteq D_{2n}$, *and* $|\langle\sigma\rangle| = n$. *In particular, D_{2n} is not simple.*

Let X be a finite set. A permutation $f \in \mathrm{Sym}(X)$ is *even* if it has an even number of cycles of even length in its decomposition into disjoint cycles, and is *odd* otherwise.

Equivalently, a permutation is even if it can be decomposed into an even number of not necessarily disjoint transpositions and odd otherwise.

The set $\mathrm{Alt}(X) \coloneqq \{f \in \mathrm{Sym}(X) : f \text{ is even}\}$ is the *alternating group* on X, and is a subgroup of $\mathrm{Sym}(X)$ of order $|X|!/2$. That is, $[\mathrm{Sym}(X) : \mathrm{Alt}(X)] = 2$.

Theorem 3.4. *If X and Y are finite sets with $|X| = |Y|$, then $\mathrm{Sym}(X) \cong \mathrm{Sym}(Y)$.*

Proof. For any bijection $F : Y \to X$, the homomorphism $\phi : \mathrm{Sym}(X) \to \mathrm{Sym}(Y)$ defined by $\phi(f) = F^{-1} \circ f \circ F$ is an isomorphism. ■

We write S_n for the symmetric group on the set $\{1,\ldots,n\}$. By the previous theorem, $\mathrm{Sym}(X) \cong S_n$ whenever $|X| = n$.

3.1 Group Actions

Let G be a group and X a set. A (*left*) *group action* of G on X is a map $\cdot : G \times X \to X$ such that

(*i*) $(gh) \cdot x = g \cdot (h \cdot x)$ for all $g,h \in G$ and $x \in X$;

(*ii*) $1_G \cdot x = x$ for all $x \in X$.

In this case, we say that G *acts on* X or that X is a *G-set*.

Three important group actions are as follows:

- **Left-multiplication**:

  Let G be a group and take $X = G$. Then, $g \cdot x \coloneqq gx$ defines an action of G on itself:

  (*i*) $(gh) \cdot x = (gh)x = g(hx) = g \cdot (h \cdot x)$;

  (*ii*) $1_G \cdot x = 1_G x = x$.

- **Conjugation**:

  Let G be a group and take $X = G$. Then, $g \cdot x \coloneqq gxg^{-1}$ defines an action of G on itself:

  (*i*) $(gh) \cdot x = (gh)x(gh)^{-1} = ghxh^{-1}g^{-1} = g \cdot (hxh^{-1}) = g \cdot (h \cdot x)$;

  (*ii*) $1_G \cdot x = 1_G x 1_G^{-1} = x$.

- **Action on Cosets**:

  Let G be a group and $H \leq G$ be a subgroup. Take $X = G/H \coloneqq \{gH : g \in G\}$ to be the set of left cosets of H in G. Then, $g \cdot (xH) = (gx)H$ defines a group action on this set of cosets:

  (*i*) $(gh) \cdot xH = g(hxH) = g \cdot (hxH) = g \cdot (h \cdot xH)$;

  (*ii*) $1_G \cdot xH = (1_G x)H = xH$.

Theorem 3.5 (Group Action Induces Homomorphism into Symmetric Group)**.** *Let $\cdot$ be an action of a group G on a set X. For $g \in G$, define the map $\phi(g) : X \to X$ by $\phi(g)(x) = g \cdot x$. Then, $\phi(g) \in \mathrm{Sym}(X)$ and $\phi : G \to \mathrm{Sym}(X)$ is a homomorphism.*

Proof. For any $g,h \in G$ and $x \in X$,

$$\begin{aligned}\phi(gh)(x) &= (gh) \cdot x \\ &= g \cdot (h \cdot x) \\ &= \big(\phi(g)\phi(h)\big)(x)\end{aligned}$$

■

Let $\cdot$ be an action of a group G on a set X. The *kernel* of the action $\cdot$, denoted $\ker(G,X,\cdot\,)$, is defined to be the kernel of the homomorphism $\phi : G \to \mathrm{Sym}(X)$ as defined above:

$$\ker(G,X,\cdot\,) \coloneqq \{g \in G : \forall x \in X, g \cdot x = x\} \subseteq G$$

The *image* of the action $\cdot$, denoted $\mathrm{im}(G,X,\cdot\,)$ is the image of ϕ:

$$\mathrm{im}(G,X,\cdot\,) \coloneqq \{\phi(g) : g \in G\} \subseteq \mathrm{Sym}(X)$$

Note that by the first isomorphism theorem, we have

- $\ker(G,X,\cdot\,) \trianglelefteq G$;
- $\mathrm{im}(G,X,\cdot\,) \leq \mathrm{Sym}(X)$.

The action $\cdot$ is *faithful* if the kernel is trivial, $\ker(G,X,\cdot\,) = \{1_G\}$, and *trivial* if the kernel is the entire group, $\ker(G,X,\cdot\,) = G$.

Example.

(*i*) The left-multiplication action of a group on itself is always faithful.

(*ii*) The conjugation action of a group on itself is trivial if and only if $gxg^{-1} = x$ for all $g,x \in G$. That is, if and only if G is abelian.

(*iii*) If G acts on the set G/H of cosets of a subgroup $H \leq G$, then the action is trivial if and only if $gH = H$ for all $g \in G$. That is, if and only if $H = G$.

So, if H is a proper subgroup of G, then $\ker(G,G/H,\cdot\,)$ is a proper normal subgroup of G.

△

Theorem 3.6. *If $\cdot$ is a faithful action of G on X, then G is isomorphic to a subgroup of* $\mathrm{Sym}(X)$.

Proof. As $\cdot$ is faithful, we have $G/\ker(G,X,\cdot\,) = G/\{1_G\} \cong G$, so by the first isomorphism theorem,

$$\begin{aligned}G &\cong G/\ker(G,X,\cdot\,) \\ &\cong \mathrm{im}(G,X,\cdot\,) \\ &\leq \mathrm{Sym}(X)\end{aligned}$$

■

Let $\cdot$ be an action of a group G on a set X, and let $x \in X$.

The *orbit* of x in G is the set of possible images of x under the action:

$$\mathrm{Orb}_G(x) \coloneqq \{g \cdot x : g \in G\} \subseteq X$$

The *stabiliser* of x in G is the set of elements of G that fix x:

$$\mathrm{Stab}_G(x) \coloneqq \{g \in G : g \cdot x = x\} \subseteq G$$

The *centraliser* or *commutant* of x in G is the set of elements that commute with x:

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

(This notion is independent from group actions.)

Lemma 3.7. *The stabiliser and centraliser of any element $g \in G$ are subgroups of G.*

The *centre* of G is the set of elements of G that commute with every element of G:

$$Z(G) = \{g \in G : \forall h \in G : gh = hg\}$$

Note that

$$Z(G) = \bigcap_{g \in G} C_G(g)$$

so, as an intersection of subgroups, the centre is itself a subgroup (and is in fact normal in G).

Example. We compute the orbits and stabilisers of the three group actions from before.

- **Left-multiplication** ($X = G$, $g \cdot x \coloneqq gx$):

  For any $y \in X = G$, we have $y^{-1}x \in G$, so $y = (y^{-1}x) \cdot x$ and $y \in \mathrm{Orb}_G(x)$, so $\mathrm{Orb}_G(x) = X$ for all $x \in X$. Also, $g \cdot x = gx = x$ if and only if $g = 1_G$, so $\mathrm{Stab}_G(x) = \{1_G\}$ for all $x \in G$.

- **Conjugation** ($X = G$, $g \cdot x \coloneqq gxg^{-1}$):

  The orbit $\mathrm{Orb}_G(x) = \{gxg^{-1} : g \in G\}$ of an element $x \in X$ under conjugation is also called the *conjugacy class* of x in G, also written as $\mathrm{Cl}(x)$ or ${}^G x$.

  For any $g \in G$, $g \cdot x = gxg^{-1} = x$ if and only if $gx = xg$, so $\mathrm{Stab}_G(x) = C_G(x)$ for all $x \in X = G$. Also,

  $$\begin{aligned} \ker(G,X,\cdot\,) &= \{g \in G : \forall x \in X : g \cdot x = x\} \\ &= \{g \in G : \forall x \in X : gxg^{-1} = x\} \\ &= Z(G) \end{aligned}$$

- **Action on Cosets** ($X = G/H$, $g \cdot (xH) = (gx)H$):

  The stabiliser of $xH \in X$ is

  $$\begin{aligned} \mathrm{Stab}_G(xH) &= \{g \in G : g \cdot xH = xH\} \\ &= \{g \in G : (gx)H = xH\} \\ &= \{g \in G : (x^{-1}gx)H = H\} \\ &= \{g \in G : (x^{-1}gx) \in H\} \\ &= xHx^{-1} \\ &= {}^x H \end{aligned}$$

  Also, if $xH,yH \in X$, then $(yx^{-1}) \cdot xH = yH$, so $\mathrm{Orb}_G(xH) = X$ for all $xH \in X$.

$\triangle$

Theorem 3.8. *Let $\cdot$ be an action of a group G on a set X, and let $x \in X$. Then,*

(i) $\mathrm{Stab}_G(X) \leq G$*;*

(ii) $\bigcap_{x \in X} \mathrm{Stab}_G(x) = \ker(G,X,\cdot\,)$.

Theorem 3.9 (Orbit-Stabiliser)**.** *Let G be a group acting on a finite set X and let $x \in X$. Then,*

$$|\mathrm{Orb}_G(x)| = [G : \mathrm{Stab}_G(x)] = \frac{|G|}{|\mathrm{Stab}_G(x)|}$$

Corollary 3.9.1. *Let G be a finite group acting on a set X. Then,*

(*i*) *For all $x,y \in X$, either $\mathrm{Orb}_G(x) = \mathrm{Orb}_G(y)$, or $\mathrm{Orb}_G(x) \cap \mathrm{Orb}_G(y) = \emptyset$. That is, orbits partition X.*

(*ii*) $|\mathrm{Orb}_G(x)|$ *divides* $|G|$.

Proof.

(*i*) Define a relation $\sim$ on X such that $x \sim y$ if and only if $y = g \cdot x$ for some $g \in G$. This relation is reflexive, by taking $g = 1_G$; symmetric, by taking inverses; and transitive, by multiplying the given g values with the group operation.

So, $\sim$ is an equivalence relation. The result then follows immediately from equivalence classes partitioning sets.

(*ii*) Follows immediately from the orbit-stabiliser theorem.

■

Theorem 3.10 (Cayley)**.** *Every finite group G is isomorphic to a subgroup of a symmetric group.*

Proof. The kernel of the left-multiplication action of G on itself is the set

$$\ker(G,G,\cdot\,) = \{g \in G : \forall x \in X : gx = x\}$$

For any $g \in G$ such that $gx = x$ for all $x \in G$, we have $g1_G = 1_G$, so $g = 1_G$, and hence the kernel is trivial, so the action is faithful. The result then follows from Theorem 3.6. ■

Theorem 3.11. *Let G be a finite group with $|G| = p^n$ for a prime p and $n \geq 1$. Then, $|Z(G)| > 1$.*

Proof. By Corollary 3.9.1, $|{}^G x| = |\mathrm{Orb}_G(x)|$ divides $|G|$, so $|{}^G x|$ is a power of p.

By definition, $Z(G) = \{x \in G : |{}^G x| = 1\}$. Suppose $|Z(G)| = 1$, so only one conjugacy class has cardinality 1, and the rest have cardinality p^{a_i}. Since orbits partition G, the cardinality of G is equal to the sum of the cardinalities of the orbits:

$$|G| = 1 + p^{a_1} + \cdots + p^{a_k}$$

However, this has residue 1 modulo p, contradicting that $|G| = p^n \equiv 0 \pmod{p}$. ■

Corollary 3.11.1. *Let G be a finite group with $|G| = p^n$ for a prime p and natural n. Then,*

(*i*) *If $n = 2$, then G is abelian.*

(*ii*) *If $n = 3$, then either G is abelian, or $|Z(G)| = p$.*

Theorem 3.12 (Cauchy)**.** *Let G be a finite group and let p be a prime divisor of $|G|$. Then, G has an element of order p. Moreover, the number of elements of G of order p is congruent to -1 modulo p.*

Theorem 3.13. *Let G be a finite group and let $H,K \leq G$. Then,*

$$|HK| = |KH| = \frac{|H||K|}{|H \cap K|}$$

Theorem 3.14. *Let G be a finite group and let $H,K \leq G$. Then,*

$$|G : H \cap K| \leq |G : H||G : K|$$

3.2 Fixed Points

Let G be a group acting on a set X, and let $g \in G$.

An element $x \in X$ is a *fixed point* if $g \cdot x = x$. The set of all fixed points for a given $g \in G$ is denoted by

$$\mathrm{fix}_X(g) \coloneqq \{x \in X : g \cdot x = x\}$$

An element $g \in G$ is *fixed point free* if $\mathrm{fix}_X(g) = \emptyset$.

Lemma 3.15 (Burnside)**.** *Let G be a finite group acting on a finite set X, and let $X/G \coloneqq \{\mathrm{Orb}_G(x) : x \in X\}$ be the set of orbits in G. Then,*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{fix}_X(g)|$$

This lemma was stated and proved by Burnside in his 1897 book on finite groups, but attributed it to Frobenius, 1887. However, even before Frobenius, the result was known to Cauchy in 1845. Consequently, this lemma is sometimes called the *lemma that is not Burnside's*, or just *the not-Burnside lemma.*

Proof. First, the sum can be rewritten as

$$\begin{aligned}\sum_{g \in G} |\mathrm{fix}_X(g)| &= \left|\left\{(g,x) \in G \times X : g \cdot x = x\right\}\right| \\ &= \sum_{x \in X} |\mathrm{Stab}_G(x)|\end{aligned}$$

Then, by the orbit-stabiliser theorem,

$$|\mathrm{Stab}_G(x)| = \frac{|G|}{|\mathrm{Orb}_G(x)|}$$

so

$$\begin{aligned}\sum_{x \in X} |\mathrm{Stab}_G(x)| &= \sum_{x \in X} \frac{|G|}{|\mathrm{Orb}_G(x)|} \\ &= |G| \sum_{x \in X} \frac{1}{|\mathrm{Orb}_G(x)|}\end{aligned}$$

Let Y be the set of distinct orbits in X. Note that X is partitioned by its orbits, so,

$$\begin{aligned}&= |G| \sum_{A \in X/G} \sum_{x \in A} \frac{1}{|\mathrm{Orb}_G(x)|} \\ &= |G| \sum_{A \in X/G} \sum_{x \in A} \frac{1}{|A|} \\ &= |G| \sum_{A \in X/G} 1 \\ &= |G||X/G|\end{aligned}$$

and the result follows. ■

The action of G on X is *transitive* if for any two points $x,y \in X$, there exists $g \in G$ such that $g \cdot x = y$. Or equivalently, if G only has one orbit, or $\mathrm{Orb}_G(x) = X$ for all $x \in X$.

Corollary 3.15.1. *If a finite group G acts transitively on a finite set X with $|X| > 1$, then G contains a fixed point free element.*

Proof. Suppose G does not contain any fixed point free elements, so $|\mathrm{fix}_X(g)| \geq 1$ for all $g \in G$. Then, G acts transitively, so $|X/G| = 1$, and Burnside's lemma gives

$$\begin{aligned}|G| &= \sum_{g \in G} |\mathrm{fix}_X(g)| \\ &= |\mathrm{fix}_X(y)| + \sum_{g \in G \setminus \{1_G\}} |\mathrm{fix}_X(g)| \\ &= |X| + \sum_{g \in G \setminus \{1_G\}} |\mathrm{fix}_X(g)| \\ &\geq |X| + |G| - 1\end{aligned}$$

so $1 \geq |X|$, contradicting that $1 < |X|$. ■

4 The Sylow Theorems

Lagrange's theorem states that if H is a subgroup of a finite group G, then $|H|$ divides $|G|$. Does the converse hold? That is, if G is a finite group, and r divides $|G|$, then does G contain a subgroup H of order r?

In general, this is not the case. For instance, if G is a non-abelian finite simple group, then G has no subgroup of order $|G|/2$. Such a subgroup H would have index 2 in G and would be a proper normal subgroup of G; also, G is non-abelian, so $|G| > 2$ and $1 < |H| < |G|$, contradicting that G is simple.

We write $|G|_p$ to denote the highest power of p that divides G. That is, if $|G| = p^n m$ with p,m coprime, then $|G|_p = p^n$.

- A subgroup $H \leq G$ is a *p-subgroup* of G if $|H|$ is a power of p.
- Let $P \leq G$ and suppose $|P| = |G|_p$. Then, P is called a *Sylow p-subgroup* of G.
- We write $\mathrm{Syl}_P(G)$ to denote the set of Sylow p-subgroups of G.

Example. Take $G = S_4$. We have $|G| = 4! = 2^3 \cdot 3$, so $|G|_2 = 2^3$ and $|G|_3 = 3$.

1. $P = \{1_G,(1,2,3),(3,2,1)\}$ has order $|P| = 3 = |G|_3$, so P is a Sylow 3-subgroup of G;
2. $K_4 = \{1_G,(1,2)(3,4),(1,3)(1,4),(1,4)(2,3)\}$ has order $|K_4| = 2 \neq |G|_2$, so K_4 is a 2-subgroup of G, but not a Sylow 2-subgroup;
3. $D_8 = \langle \sigma,\tau \rangle$ with $\sigma = (1,2,3,4)$ and $\tau = (1,4)(2,3)$ has order $|D_8| = 8 = |G|_2$, so D_8 is a Sylow 2-subgroup of G.
4. A_4 is not a p-subgroup of G for any prime p.
5. The trivial subgroup $\{1_G\}$ is a Sylow p-subgroup for all prime p.

△

Theorem 4.1 (Sylow). *Let G be a finite group with order $|G| = p^n m$ with p,m coprime. Then,*

1. *G has at least one Sylow p-subgroup.*

2. *All Sylow p-subgroups of G are conjugate. That is, if H and K are Sylow p-subgroups of G, then there exists an element $g \in G$ such that $gHg^{-1} = K$.*
3. *Any p-subgroup of G is contained in a Sylow p-subgroup of G.*
4. *The number r of Sylow p-subgroups of G satisfies $r \equiv 1 \pmod p$ and $r \mid m$.*

4.1 Applications

By Sylow theorem 2, G acts on $\mathrm{Syl}_p(G)$ by conjugation, and for any $P \in \mathrm{Syl}_p(G)$, $\mathrm{Orb}_G(P) = \mathrm{Syl}_p(G)$. The stabiliser of P under conjugation is then the normaliser:

$$\begin{aligned}\mathrm{Stab}_G(P) &= \{g \in G : g \cdot P = P\}\\ &= \{g \in G : gPg^{-1} = P\}\\ &= \{g \in G : gP = Pg\}\\ &= N_G(P)\end{aligned}$$

Corollary 4.1.1. *Let G be a finite group, p be a prime divisor of $|G|$, and $P \in \mathrm{Syl}_p(G)$. Then,*

(*i*) $|\mathrm{Syl}_p(G)| = [G : N_G(P)]$;

(*ii*) $|\mathrm{Syl}_p(G)|$ *divides* $|G|/|G|_p$;

(*iii*) $P \trianglelefteq G$ *if and only if* $|\mathrm{Syl}_p(G)| = 1$. *That is, unique Sylow p-subgroups are normal.*

Proof.

(*i*) By the orbit-stabiliser theorem

$$\begin{aligned}|\mathrm{Syl}_p(G)| &= |\mathrm{Orb}_G(P)|\\ &= [G : \mathrm{Stab}_G(P)]\\ &= [G : N_G(P)]\end{aligned}$$

(*ii*) Since $P \leq N_G(P)$, by Lagrange's theorem, $|N_G(P)| = |P||N_G(P) : P|$. Then,

$$\begin{aligned}|\mathrm{Syl}_p(G)| &= [G : N_G(P)]\\ &= \frac{|G|}{|N_G(P)|}\\ &= \frac{|G|}{|P|[N_G(P) : P]}\end{aligned}$$

which divides $\frac{|G|}{|P|} = \frac{|G|}{|G|_p}$.

(*iii*) $P \trianglelefteq G$ if and only if $G = N_G(P)$. Then, by the orbit-stabiliser theorem,

$$\begin{aligned}|\mathrm{Orb}_G(P)| &= \frac{|G|}{|\mathrm{Stab}_G(P)|}\\ |\mathrm{Syl}_p(G)| &= \frac{|G|}{|N_G(P)|}\end{aligned}$$

so $G = N_G(P)$ if and only if $|\mathrm{Syl}_P(G)| = 1$.

∎

Corollary 4.1.2. *Let G be a finite group and let p be a prime divisor of $|G|$. Define the set*

$$F_p(G) \coloneqq \{x \in G : x \neq 1_G \text{ and } |x| \text{ is a power of } p\}$$

Then,

(*i*)

$$F_p(G) = \bigcup_{P \in \mathrm{Syl}_p(G)} (P \setminus \{1_G\})$$

(*ii*) $|F_p(G)| \geq |G|_p - 1$, *with equality if and only if* $|\mathrm{Syl}_p(G)| = 1$;

(*iii*) *If* $|G|_p = p$, *then* $|F_p(G)| = |\operatorname{Syl}_p(G)|(p-1)$, *with equality if and only if* $|\mathrm{Syl}_p(G)| = 1$.

4.1.1 Proving Groups of a Particular Order are Not Simple

Example. Let G be a group of order $20 = 2^2 \times 5$. Can G be simple?

By Sylow's first theorem, G has Sylow 5-subgroups. By Sylow's fourth theorem, the number r of Sylow 5-subgroups divides 2^2 and satisfies $r \equiv 1 \pmod 5$. It follows that $r = 1$ is the only value that satifies this requirement, so G has a unique Sylow 5-subgroup, which must be normal in G and hence G cannot be simple. △

Example. Let G be a group of order $48 = 2^4 \times 3$. Can G be simple?

By Sylow theorem 1, G has Sylow 2-subgroups and Sylow 3-subgroups. By Sylow's fourth theorem, the number r of Sylow 2 subgroups divides 3 and satisfies $r \equiv 1 \pmod 2$. We must have $r = 1{,}3$, so G has either 1 or 3 Sylow 2-subgroups.

If there is only 1 Sylow 2-subgroup, then it is normal in G. Otherwise, G has 3 Sylow 2-subgroups and G acts non-trivially (and transitively) on $\mathrm{Syl}_2(G)$ by conjugation. This action induces a non-trivial homomorphism $\phi : G \to S_3$ (as in Theorem 3.5).

By the first isomorphism theorem $G/\ker(\phi) \cong \mathrm{im}(\phi)$, so by Lagrange's theorem,

$$\begin{aligned} |G/\ker(\phi)| &= |\mathrm{im}(\phi)| \\ |G|/|\ker(\phi)| &= |\mathrm{im}(\phi)| \\ |G|/|\mathrm{im}(\phi)| &= |\ker(\phi)| \end{aligned}$$

Because ϕ is non-trivial, $1 < |\operatorname{im}(\phi)| \leq |S_3| = 6$, so $\frac{48}{6} \leq |\ker(\phi)| < \frac{48}{1}$ and hence $\ker(\phi)$ is a non-trivial normal subgroup of G. △

Example. Let G be a group of order $2\,552 = 8 \times 11 \times 29$. Can G be simple?

Take $p = 11$, so $|G| = 11 \times (8 \times 29) = 11^1 \times 232$. The number of Sylow 11-subgroups, r, must divide 232 and satisfy $r \equiv 1 \pmod{11}$. Consider the factorisation $232 = 2^3 \times 29$; the factors of 232 are then: 1, 2, 4, 8, $29 \equiv 7$, $58 \equiv 3$, $116 \equiv 6$, and $232 \equiv 1$, so $r = 1{,}232$ are the possible solutions.

Now, if G has more than 1 Sylow 11-subgroup, then it must have 232 Sylow 11-subgroups. As 11 is prime, these subgroups must be cyclic, so every non-identity element generates the group. It follows that these subgroups intersect only at the identity element, so each subgroup contributes 10 elements of order 11, so there must be $232 \times 10 = 2\,320$ elements of order 11 in G.

Now, take $p = 29$, so $|G| = 29 \times (8 \times 11) = 29^1 \times 88$. By identical arguments as before, the number of Sylow 29-subgroups must be 1 or 88, and again, as 29 is prime, each subgroup must be cyclic, so if there is more than 1 Sylow 29-subgroup, then there are $88 \times 28 = 2\,464$ elements of order 28.

Now, by Sylow's first theorem, there exist Sylow 29 and 11-subgroups. If there are more than one of each, then we have 2 320 and 2 464 elements of order 11 and 29, respectively. But these values sum to more than $2\,552 = |G|$, so we cannot simultaneously have more than 1 Sylow 29 and 11-subgroups. But then, any unique Sylow p-subgroup is normal, so G cannot be simple. △

4.1.2 Proving a Particular Group is Simple

Corollary 4.1.3. *Let G be a finite group and let p be a prime divisor of $|G|$. Define the set*

$$F_p(G) \coloneqq \{x \in G : x \neq 1_G \text{ and } |x| \text{ is a power of } p\}$$

Then,

(*i*) *Let N be normal in G. If $x \in N$, then ${}^G x \subseteq N$.*

(*ii*) *Let N be normal in G and suppose p does not divide $[G : N]$. Then,*

  (*a*) $\mathrm{Syl}_p(N) = \mathrm{Syl}_p(G)$;

  (*b*) $F_p(G) = F_p(N)$.

Theorem 4.2. *A_5 is simple.*

Proof. Suppose for a contradiction that A_5 has a non-trivial proper subgroup N. By Lagrange's theorem, $|N|$ divides $|A_5| = 5!/2 = 60$, so the prime factors of $|N|$ are 2, 3 and 5.

Now, note that

- A_5 has 24 elements of order 5 – these are the 5-cycles, and there are $P^5_5 = \frac{5!}{(5-5)!} = 120$ permutations of 5 elements from {1,2,3,4,5}. Dividing by 5 to account for cyclic shifts, there are $\frac{120}{5} = 24$ such elements;
- A_5 has 20 elements of order 3 – these are the 3-cycles, and there are $P^5_5 = \frac{5!}{(5-5)!} = 120$ permutations of 5 elements from {1,2,3,4,5}. ;
- A_5 has 15 elements of order 2 – are those of the form $(ab)(cd)$ for a,b,c,d distinct elements of {1,2,3,4,5}. There are $P^5_4 = \frac{5!}{(5-4)!}$ permutations of 4 elements from 5, but 2 ways to cyclic shift within each cycle, and 2! ways to permute the cycles themselves, so there are $\frac{120}{2 \cdot 2 \cdot 2!} = 15$ elements of order 2.

Suppose p divides $|N|$ for $p = 3$ or $p = 5$. Then, p does not divide $[G : N]$, so by Corollary 4.1.3(i), $F_p(G) = F_p(N)$.

If $p = 3$, then $F_p(N) = F_p(G) = 20$, so $|N| \geq 21$. Since $|N|$ divides 60 and is less than 60, $|N| = 30$. Similarly, if $p = 5$, then $F_p(N) = F_p(G) = 24$, so $|N| \geq 25$. Again, we must have $|N| = 30$.

So, if 3 or 5 divide $|N|$, then $|N| = 30$ and both 3 and 5 divide $|N|$, so $F_3(N) = 20$ and $F_5(N) = 24$. But then, $|N| = 30 > 20 + 24$, which is a contradiction.

Now suppose neither 3 nor 5 divide $|N|$. By Lagrange's theorem, $|N|$ divides $|G| = 4 \cdot 3 \cdot 5$, so $|N|$ divides 4. By Cauchy's theorem, there exists $x \in N$ with order 2. By Corollary 4.1.3(ii), we then have $4 = |N| \geq |{}^G x| = 15$ ■

4.2 Simplicity of A_n

Lemma 4.3.

(*i*) *Let $n \geq 3$ and let X_n be the set of 3-cycles in S_n. Note that $X_n \subseteq A_n$ since 3-cycles decompose into a pair (i.e. an even number) of transpositions. Then, $A_n = \langle X_n \rangle$.*

(*ii*) *Let* $n \geq 5$*. Then, any two* 3*-cycles are conjugate in* A_n*.*

Lemma 4.4. *For* $n \geq 5$*, any non-identity permutation* $\sigma \in A_n$ *has a conjugate* σ' *such that* $\sigma \neq \sigma'$ *and* $\sigma(i) = \sigma'(i)$ *for some* $i \in \{1,2,\dots,n\}$*.*

Theorem 4.5. A_n *is simple for all* $n \geq 5$*.*

Proof. We induct on n. We already have that A_5 is simple, so assume $n \geq 6$.

A_n acts on the set $X_n = \{1,2,\dots,n\}$ in the natural way. For each $i \in X_n$, define

$$H_i := \mathrm{Stab}_{A_n}(i) \cong A_{n-1}$$

and by the inductive hypothesis, $H_i \cong A_{n-1}$ is simple. Note that H_i contains a 3-cycle containing 3 points of X_n other than i.

Suppose A has a non-trivial proper subgroup $N \lhd A_n$. Take any non-identity permutation $\sigma \in N$. By the previous lemma, there exists a conjugate $\sigma' \in N$ such that $\sigma \neq \sigma'$ and $\sigma(i) = \sigma'(i)$ for some $i \in X_n$.

Since normal subgroups are closed under conjugation, $\sigma' \in N$, so $\sigma^{-1}\sigma' \in N$, $\sigma^{-1}\sigma' \neq 1_{A_n}$, and $\sigma^{-1}\sigma'(i) = i$. Thus $\sigma^{-1}\sigma' \in H_i$ and so $N \cap H_i \neq \{1_{A_n}\}$.

Now, $N \lhd A_n$ so $N \cap H_i \lhd H_i$ by the second isomorphism theorem. But, $H_i \subseteq N$ contains a 3-cycle, so by Theorem 4.3(ii), N contains all 3-cycles of A_n. The result then follows from Theorem 4.3(i). ■

5 Classifying Groups of Small Order

5.1 Semidirect Products

Given two groups H and K, their cartesian product $H \times K$ has group structure by applying the group operations pointwise. This group is called the (*external*) *direct product* of H and K.

This extends naturally to any arbitrary collection of groups, with the product operation applied pointwise on each coordinate.

Theorem 5.1. *Let* H *and* K *be normal subgroups of a group* G *such that* $G = HK$ *and* $H \cap K = \{1_G\}$*. Then,*

(*i*) $hk = kh$ *for all* $h \in H$ *and* $k \in K$*, so if* H *and* K *are both abelian, then* G *is abelian;*

(*ii*) $G \cong H \times K$*.*

Recall that an automorphism of a group G is an isomorphism $G \to G$. The set $\mathrm{Aut}(G)$ of automorphisms of G has group structure under function composition and is called the *automorphism group* of G.

Let H and K be groups, and let $\phi : H \to \mathrm{Aut}(K)$ be a homomorphism. Write ϕ_h for $\phi(h)$ and define a binary operation $\cdot : (H \times K) \times (H \times K) \to H \times K$ by

$$(h_1,k_1) \cdot (h_2,k_2) := (h_1h_2,\phi_{h_2^{-1}}(k_1)k_2)$$

Then, $(H \times K, \cdot\,)$ has group structure and is called the (*external*) *semidirect product* of H and K with respect to ϕ, denoted by $H \ltimes_\phi K$.

Example. Three important semidirect products are generated by homomorphisms as follows:

- **The trivial homomorphism**:

  Let H and K be any groups. Then, the map $\phi : H \to \mathrm{Aut}(K)$ defined by $\phi(h) = \mathrm{id}_K$ is the trivial homomorphism, and the resulting semidirect product operation is given by

$$(h_1,k_1) \cdot (h_2,k_2) = (h_1,h_2,\phi_{h_2^{-1}}(k_1)k_2)$$

$$= (h_1 h_2, \mathrm{id}_K(k_1)k_2)$$
$$= (h_1 h_2, k_1 k_2)$$

so

$$H \ltimes_\phi K \cong H \times K$$

- **The inversion homomorphism**:

  Let $H = C_2 = \langle c \rangle$ and let K be any abelian group. Then, the map $\phi : H \to \mathrm{Aut}(K)$ defined by $\phi(1_H) = \mathrm{id}_K$ and $\phi(h) = (k \mapsto k^{-1})$ (i.e. the identity element is sent to the identity automorphism, and every other element is sent to the inversion automorphism) is a homomorphism.

  If $K \cong C_n$, then the resulting semidirect product is isomorphic to the dihedral group of order $2n$:

  $$C_2 \ltimes_\phi C_n \cong D_{2n}$$

- **The conjugation homomorphism**:

  Let G be a group and let $H \leq G$ and $K \trianglelefteq G$. Then, the map $\phi : H \to \mathrm{Aut}(K)$ defined by $\phi(h) = (k \mapsto hkh^{-1})$ is a homomorphism.

  This last homomorphism will be useful with the following lemma:

$\triangle$

Lemma 5.2. *Let G be a group and let $H \leq G$ and $K \trianglelefteq G$. If $G = HK$ and $K \cap H = \{1_G\}$, then*

$$G \cong H \ltimes_\phi K$$

Proof. $\blacksquare$

Example. Let $n \geq 3$ be an integer, and consider the dihedral group $G = D_{2n} = \langle \sigma, \tau \rangle$, where

$$\sigma := (1, \ldots, n)$$
$$\tau := \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} (i, n-i+1)$$

Let $K = \langle \sigma \rangle = \{1_G, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$ and $H = \langle \tau \rangle = \{1_G, \tau\}$. Recall that ${}^\tau\sigma = \tau\sigma\tau^{-1} = \sigma^{-1}$, so ${}^\tau k = k^{-1}$ for all $k \in K$.

Since $|\tau| = 2$, $|\sigma| = n$, and $D_{2n} = K \sqcup \tau K$, we have $G = HK$ and $H \cap K = \{1_G\}$, so by the previous lemma, we have $G \cong H \ltimes_\phi K$, where ϕ is the inversion homomorphism. $\triangle$

Lemma 5.3. *Let G be a non-abelian finite group and suppose that*

1. *G has a cyclic subgroup K of order $n := |G|/2$;*
2. *$G \setminus K$ contains an element G of order 2;*
3. *If $i \in \{0, 1, \ldots, n-1\}$ satisfies $i^2 \equiv 1 \pmod{n}$, then $i \equiv \pm 1 \pmod{n}$.*

Then,

$$G \cong D_{2n}$$

Example. The following are some examples of positive integers n that satisfy the third hypothesis of the previous lemma.

- For $n = 6$, $0^2, 1^2, 2^2, 3^2, 4^2, 5^2 \equiv 0, 1, 4, 3, 4, 1 \pmod{6}$, so $i^2 \equiv 1 \pmod{6}$ if and only if $i = 1, 5 \equiv \pm 1 \pmod{6}$.

- Let $n = p$ where p is prime. Then,

$$\begin{aligned} i^2 &= 1 \\ i^2 - 1 &= 0 \\ (i-1)(i+1) &= 0 \end{aligned}$$

  Since $\mathbb{Z}/p\mathbb{Z}$ is a field, it has no zero divisors, so either $i - 1 = 0$ or $i + 1 = 0$, so $i^2 = 1$ if and only if $i = \pm 1$ in $\mathbb{Z}/p\mathbb{Z}$.

- Let $n = p^2$ where p is prime.

  If $p = 2$, we have $0^2, 1^2, 2^2, 3^2 \equiv 0, 1, 0, 1 \pmod 4$, so $i^2 \equiv 1 \pmod 4$ if and only if $i = 1, 3 \equiv \pm 1 \pmod 4$.

  Otherwise, suppose p is odd and let $i \in \{0, 1, \ldots, p^2 - 1\}$ such that $i^2 \equiv 1 \mod p^2$. Then, p^2 divides $(i-1)(i+1)$.

  Since p is odd, it divides at most one of the factors, because if it divided both, it would also divide their difference $(i + 1) - (i - 1) = 2$, contradicting that p is odd. So, p^2 also divides at most one of the factors.

  So, p^2 divides $i - 1$ or $i + 1$. Then, since $0 \le i \le p^2 - 1$, the only possibilities are $i = 1, p^2 - 1 \equiv \pm 1 \pmod{p^2}$.

△

5.2 Semidirect Products of Abelian and Cyclic Groups

We consider the following special case of semidirect products: let G be a finite group with $|G|/2$ odd, and suppose G has an abelian normal subgroup K of order $|G|/2$.

The *commutator* of two elements $g, h \in G$ is the element $[g, h] := ghg^{-1}h^{-1}$. Similarly, we define the subgroup $[K, x] := \langle \{[k, x] : k \in K\} \rangle$.

Lemma 5.4 (Fitting)**.**

(i) ${}^x a = xax^{-1} = a^{-1}$ *for all* $a \in [K, x]$*;*

(ii) $K = C_K(x) \times [K, x]$*;*

(iii) $G \cong \big(H \ltimes_\phi [K, x]\big) \times C_K(x)$*, where* $\phi : H \to \operatorname{Aut}\big([K, x]\big)$ *is the inversion homomorphism.*

5.3 Abelian Groups

Theorem 5.5 (Fundamental Theorem of Finite Abelian Groups)**.** *Let G be a finite abelian group. Then, there exist divisors $d_1, \ldots, d_r$ of $|G|$ such that $d_1 \mid d_2 \mid \cdots \mid d_r$ and*

$$G \cong \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i}$$

5.4 Groups of order p, p^2, or $2p$, for prime p

Lemma 5.6. *If $|G| = p$ with p prime, then $G \cong C_p$.*

Proof. Take any non-identity element $g \in G$. By lagrange's theorem, $|g|$ divides $|G| = p$. Since $g \neq 1_G$, $|g| = p$ so $G = \langle g \rangle$. ■

Lemma 5.7. *If $|G| = p^2$ with p prime, then either $G \cong C_{p^2}$ or $G \cong C_p \times C_p$.*

Proof. We have already proved that all groups of order p^2 are abelian (Corollary 3.11.1), so G is abelian. The fundamental theorem of finite abelian groups then gives the result. ■

Lemma 5.8. *If $|G| = 2p$ with $p \neq 2$ prime, then either $G \cong C_{2p}$ or $G \cong D_{2p}$.*

Proof. If G is abelian, then $G \cong C_2 \times C_p \cong C_{2p}$ by the fundamental theorem of finite abelian groups.

Otherwise, G is non-abelian. Let $P \in \mathrm{Syl}_p(G)$. The number r of Sylow p-subgroups divides 2 and satisfies $r \equiv 1 \pmod p$, so since $p \neq 2$, we must have $r = 1$, so $P \trianglelefteq G$.

Since p is odd, it follows that all elements of G of order 2 lie in $G \setminus P$. Also, since $\mathbb{Z}/p\mathbb{Z}$ is a field, the only solutions of the equation $i^2 - 1 = 0$ are congruent to ± 1 modulo p. Then, Theorem 5.3 gives that $G \cong D_{2p}$, as required. ■

5.5 Groups of order $2p^2$, for odd prime p

Let $p \neq 2$ be prime, $H = C_2$, and $K = C_p \times C_p$. Let $\phi : H \to \mathrm{Aut}(K)$ be the inversion homomorphism. The group $H \ltimes_\phi K$ is then called the *generalised dihedral group of order* $2p^2$ and is denoted by GD_{2p^2}.

Lemma 5.9. *If $|G| = 2p^2$ with $p \neq 2$ prime, then G is isomorphic to one of the following:*

- C_{2p^2};
- $C_p \times C_{2p}$;
- $C_p \times D_{2p}$;
- D_{2p^2};
- GD_{2p^2}.

5.6 Groups of order pq, for prime p,q with $p < q$ and $p \nmid q - 1$

Lemma 5.10. *Let $|G| = pq$ with p,q prime, satisfying $p < q$ and $p \nmid q - 1$. Then, $G \cong C_{pq}$.*

Proof. The number r of Sylow p-subgroups divides q and satisfies $r \equiv 1 \pmod p$. If $r = q$, then $q \equiv 1 \pmod p$, so $q - 1 \equiv 0 \pmod p$, contradicting that p does not divide $q - 1$. Thus, $r = 1$.

Similarly, the number s of Sylow q-subgroups divides p and satisfies $s \equiv 1 \pmod q$. Since $p < q$, p is already a least residue modulo q, so $s = p$ leads to a contradiction $p \equiv 1 \pmod q$, so $s = 1$.

So, G has a normal Sylow p-subgroup, say H, and a normal Sylow q-subgroup, say K. By Lagrange's theorem, $H \cap K = \{1_G\}$. By Theorem 3.13,

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{pq}{1} = pq = |G|$$

so $G = HK$. Then, by Theorem 5.1, $G \cong H \times K$. Note that, being of prime order, H and K are both cyclic. Let $H = \langle h \rangle$ and $K = \langle k \rangle$. These generators commute, so $|hk| = |h||k| = pq = |G|$, so $G = \langle xy \rangle = C_{pq}$, as required. ■

We have now classified all groups of the following orders:

$$1,2,3,4,5,6,7,9,10,11,13,14,15,17,18$$

We will not classify groups of order 16, as there are too many, but we will now classify groups of order 8 and 12.

5.7 Groups of order 8

We have already seen a non-cyclic group of order 8, namely D_8. We now define another.

The *quaternion group* Q_8 is the group of unit basis quaternions under quaternion multiplication:

$$Q_8 \coloneqq \{1,i,j,k,-1,-i,-j,-k\}$$

That is,

- $1q = q1 = q$ and $(-1)q = q(-1) = -q$ for all $q \in Q_8$;
- $ij = -ji = k$, $jk = -kj = i$, and $ki = -ik = j$;
- $1^2 = 1$, and $i^2 = j^2 = k^2 = ijk = -1$.

The quaternion group can also be defined as the group with presentation

$$Q_8 \coloneqq \langle i,j,k \mid i^2 = j^2 = k^2 = ijk \rangle$$

where the identity is denoted 1, the element $i^2 = j^2 = k^2 = ijk$ is denoted -1, and the elements i^3, j^3, and k^3 are denoted $-i$, $-j$, and $-k$, respectively.

Lemma 5.11.

(i) *$Z(Q_8) = \{\pm 1\}$.*

(ii) *G has 1 element of order 2, namely -1, and 6 elements of order 4, namely $\pm i$, $\pm j$, and $\pm k$.*

(iii) *$G = \langle i,j \rangle = \langle j,k \rangle = \langle k,i \rangle$.*

(iv) *$Q_8 \ncong D_8$ since D_8 has 5 elements of order 2 and 2 elements of order 4.*

Lemma 5.12. *If $|G| = 8$, then G is isomorphic to one of the following:*

- *$C_2 \times C_2 \times C_2$;*
- *$C_4 \times C_2$;*
- *C_8;*
- *D_8;*
- *Q_8.*

5.8 Groups of order 12

We have already seen some non-cyclic groups of order 12, namely D_12 and A_4. We now define another.

Let $H = C_4 = \langle h \rangle$ and $K = C_3$. Define $\phi : H \to \mathrm{Aut}(K)$ by $\phi(h^i) = (k \mapsto k^{(-1)^i})$. The resulting semidirect product $H \ltimes_\phi K$ is called the *dicyclic group* of order 12, denoted by Dic_{12}.

Lemma 5.13. *If $|G| = 12$, then G is isomorphic to one of the following:*

- *$C_3 \times C_2 \times C_2 \cong C_6 \times C_2$;*
- *C_{12};*
- *D_{12};*
- *A_4;*
- *Dic_{12}.*

5.9 Unique Simple Group of Order 60

Theorem 5.14. *If $|G| = 60$, then $G \cong A_5$.*

6 Soluble Groups

6.1 Composition Series

We write $H < G$ or $H \lneq G$ to mean that H is a proper subgroup of G, and similarly, $H \lhd G$ or $H \ntrianglelefteq G$ to mean that H is a proper normal subgroup of G.

A *composition series* of a group G is a sequence of nested normal subgroups $(G_i)_{i=1}^r$ satisfying

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

such that G_i/G_{i-1} is simple for each $1 \leq i \leq r$, and r is called the *length* of the series.

Example.

1. Let $p \neq 2$ be prime and let $G = D_{2p} = \langle \sigma,\tau \rangle$. Let $G_0 = \{1_G\}$, $G_1 = \langle \sigma \rangle \cong C_p$, and $G_2 = G$. These groups satisfy the normality requirements, and the quotients are given by $G_1/G_0 \cong G_1 \cong C_p$, $G_2/G_1 \cong \langle \tau \rangle \cong C_2$, which are both simple. Thus,
$$\{1_G\} \ntrianglelefteq \langle \sigma \rangle \ntrianglelefteq D_{2p}$$
is a composition series of length 2.
2. Let $n \geq 5$, and let $G = S_n$. Let $G_0 = \{1_G\}$, $G_1 = A_n$, and $G_2 = S_n$. These groups satisfy the normality requirements, and the quotients are given by $G_1/G_0 \cong G_1 \cong A_n$, $G_2/G_1 \cong C_2$, which are both simple. Thus,
$$\{1_G\} \ntrianglelefteq A_n \ntrianglelefteq S_n$$
is a composition series of length 2.
3. Let $G = D_8 = \langle \sigma,\tau \rangle$. Let $G_0 = \{1_G\}$, $G_1 = \langle \sigma^2 \rangle$, $G_2 = \langle \sigma \rangle$, and $G_3 = D_8$. These groups satisfy the normality requirements, and the quotients are all isomorphic to C_2, which is simple, so
$$\{1_G\} \ntrianglelefteq \langle \sigma^2 \rangle \ntrianglelefteq \langle \sigma \rangle \ntrianglelefteq D_8$$
is a composition series of length 3.

$\triangle$

Note that if G is the trivial group, then the series

$$\{1_G\} = G_0 = G$$

is a composition series of G of length 0.

Theorem 6.1. *Every finite group has a composition series.*

Corollary 6.1.1. *Let G be a finite group and let $N \trianglelefteq G$. Suppose that*

$$\begin{aligned} \{1_G\} &= N_0 \ntrianglelefteq N_1 \ntrianglelefteq \cdots \ntrianglelefteq N_r = N \\ \{1_G\} &= \frac{X_0}{N} \ntrianglelefteq \frac{X_1}{N} \ntrianglelefteq \cdots \ntrianglelefteq \frac{X_s}{N} = \frac{G}{N} \end{aligned}$$

are composition series for N and G/N, respectively, where each X_i in the second series is a subgroup of G containing N. In particular, $X_0 = N$ and $X_s = G$.

Then,

$$\{1_G\} = N_0 \ntrianglelefteq N_1 \ntrianglelefteq \cdots \ntrianglelefteq N_r = N = X_0 \ntrianglelefteq X_1 \ntrianglelefteq \cdots \ntrianglelefteq X_s = G$$

is a composition series for G of length $r + s$.

6.2 Jordan-Hölder Theorem

Two composition series I and II of a group G

$$\begin{aligned} \{1_G\} = A_0 \subsetneq A_1 \subsetneq \cdots \subsetneq A_r = G \qquad &(\mathrm{I}) \\ \{1_G\} = B_0 \subsetneq B_1 \subsetneq \cdots \subsetneq B_s = G \qquad &(\mathrm{II}) \end{aligned}$$

are *equivalent* and write $\mathrm{I} \sim \mathrm{II}$ if $r = s$ and there is a bijection

$$f : \{A_i/A_{i-1} : 1 \leq i \leq r\} \to \{B_i/B_{i-1} : 1 \leq i \leq s\}$$

such that $A_i/A_{i-1} \cong f(A_i/A_{i-1})$ for each $1 \leq i \leq r$.

Theorem 6.2 (Jordan-Hölder)**.** *Let*

$$\begin{aligned} \{1_G\} = A_0 \subsetneq A_1 \subsetneq \cdots \subsetneq A_r = G \qquad &(\mathrm{I}) \\ \{1_G\} = B_0 \subsetneq B_1 \subsetneq \cdots \subsetneq B_s = G \qquad &(\mathrm{II}) \end{aligned}$$

be two composition series of a finite group G. Then, $\mathrm{I} \sim \mathrm{II}$.

This theorem implies that, up to isomorphism, the quotients G_i/G_{i-1} and the length r of any composition series of a finite group G are invariants of that group.

Let

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

be a composition series for a finite group G, with uniqueness up to equivalence given by the Jordan-Hölder theorem. Then, the quotient groups G_i/G_{i-1} for $1 \leq i \leq r$ are called the *composition factors* of G, and r is called the *composition length* of G.

A finite group is *soluble* if it is trivial or if its composition factors are all cyclic groups of prime order (or equivalently, simple abelian groups).

Example.

(*i*) Let G be a finite abelian group. Then, any quotient of any subgroup of G is abelian, so any composition factor of G is a simple abelian group, i.e. a cyclic group of prime order. Thus, all abelian groups are soluble.

(*ii*) Let $n \geq 5$ and consider A_n. Then, A_n is a non-abelian simple group, so it has precisely one composition factor, namely itself, which is non-abelian. Thus, A_n is not soluble for any $n \geq 5$.

△

Lemma 6.3. *Let G be a finite group and let N be normal in G. Then, G is soluble if and only if both N and G/N are soluble.*

Proof. Write $\mathrm{CF}(G)$ for the (multi)set of composition factors of G. By Corollary 6.1.1 and the Jordan-Hölder theorem,

$$\mathrm{CF}(G) = \mathrm{CF}(N) \cup \mathrm{CF}(G/N)$$

Thus, G is soluble if and only if both N and G/N are soluble. ■

Example. Let $G = D_{2n} = \langle \sigma, \tau \rangle$ and let $N = \langle \sigma \rangle \trianglelefteq G$. N is abelian and $|G/N| = 2$, so G/N is abelian, so both are soluble, and hence G is soluble. △

6.3 Commutators

Recall that the commutator of two elements $g,h \in G$ is the element $[g,h] \coloneqq ghg^{-1}h^{-1}$. Note that $[g,h] = 1_G$ if and only if g and h commute.

Example. Consider the alternating group A_5.

$$\begin{aligned}\big[(1,2,4),(1,3,5)\big] &= (1,2,4)(1,3,5)(1,2,4)^{-1}(1,3,5)^{-1} \\ &= (1,2,4)(1,3,5)(4,2,1)(5,3,1) \\ &= (1,2,3)\end{aligned}$$

More generally, if $\{x,a,b,c,d\} = \{1,2,3,4,5\}$,

$$\big[(x,a,b)(x,c,d)\big] = (x,a,b)(x,c,d)(b,a,x)(d,c,x) = (x,a,c)$$

$\triangle$

The *commutator subgroup* $[G,G]$ is the subgroup of G generated by all of its commutators:

$$[G,G] \coloneqq \big\langle [g_1,g_2] \bigm| g_1,g_2 \in G \big\rangle$$

More generally, if $H,K \leq G$, we define

$$[H,K] \coloneqq \big\langle [h,k] \bigm| h \in H, k \in K \big\rangle$$

to be the *commutator subgroup of H and K*.

Example.

1. In any abelian group G, $[g,h] = 1_G$ for all $g,k \in G$, so the commutator subgroup $[G,G] = \langle 1_G \rangle = \{1_G\}$ is trivial.
2. Let $G = A_5$. As seen in the example above, every 3-cycle in A_5 is the commutator of some pair of 3-cycles. But A_5 is generated by 3-cycles, so $[A_5,A_5] = A_5$.

$\triangle$

The *abelianisation* G^{ab} of a group G is the quotient $G/[G,G]$.

Theorem 6.4. *For any group G,*

(i) $[G,G] \trianglelefteq G$*;*

(ii) G^{ab} *is abelian.*

(iii) If N is normal in G and G/N is abelian, then $[G,G] \leq N$

Proof. (i) For all $g,h,j \in G$,

$$\begin{aligned}g[h,k]g^{-1} &= ghkh^{-1}k^{-1}g^{-1} \\ &= gh(g^{-1}g)k(g^{-1}g)h^{-1}(g^{-1}g)k^{-1}g^{-1} \\ &= (ghg^{-1})(gkg^{-1})(gh^{-1}g^{-1})(gk^{-1}g^{-1}) \\ &= (ghg^{-1})(gkg^{-1})(ghg^{-1})^{-1}(gkg^{-1})^{-1} \\ &= [ghg^{-1},gkg^{-1}] \\ &\in [G,G]\end{aligned}$$

For a general element $[h_1,k_1][h_2,k_2]\cdots[h_r,k_r] \in [G,G]$, we have,

$$g[h_1,k_1][h_2,k_2]\cdots[h_r,k_r]g^{-1} = g[h_1,k_1](g^{-1}g)[h_2,k_2](g^{-1}g)\cdots(g^{-1}g)[h_r,k_r]g^{-1}$$

$$
\begin{aligned}
&= \left(g[h_1,k_1]g^{-1}\right)\left(g[h_2,k_2]g^{-1}\right)\cdots\left(g[h_r,k_r]g^{-1}\right) \\
&\in [G,G]
\end{aligned}
$$

so $[G,G] \trianglelefteq G$.

(*ii*) We prove a more general statement: a quotient group G/N is abelian if and only if every commutator is in N. That is, if and only if $[G,G] \subseteq N$.

Let $g,h \in G$. Then,

$$
\begin{aligned}
(gN)(hN) &= (hN)(gN) \\
(gN)(hN) &= (hN)(gN)N \\
(gN)^{-1}(hN)^{-1}(gN)(hN) &= N \\
[gN,hN] &= N \\
[g,h]N &= N \\
[g,h] &\in N
\end{aligned}
$$

where we used that N is the identity in G/N on the second line. So, gH and hN commutes if and only if $[g,h] \in N$, so G/N is abelian if and only if $[g,h] \in N$ for all $g,h \in G$. In particular, if $N = [G,G]$, then every commutator is in N be definition of the commutator subgroup, so $G^{\text{ab}} = G/[G,G]$ is abelian.

(*iii*) Proved in part (*ii*).

■

Corollary 6.4.1. *A group G is abelian if and only if $[G,G] = \{1_G\}$.*

Given a group G, define $G^(0) \coloneqq G$ and recursively define the *nth derived subgroup* as

$$G^{(n)} \coloneqq \left[G^{(n-1)},G^{(n-1)}\right]$$

for each $n \in \mathbb{N}$. Then, the descending series

$$G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \cdots \geq G^{(n)} \geq G^{(n+1)} \geq \cdots$$

is called the *derived series* of G.

By definition, we have

- $\left(G^{(n)}\right)^{(m)} = G^{(n+m)}$;
- $H^{(n)} \leq G^{(n)}$ for all $H \leq G$.

Theorem 6.5. *Let G be a finite group. Then, G is soluble if and only if $G^{(n)} = \{1_G\}$ for some $n \in \mathbb{N}$.*

Proof. Suppose G is soluble. We induct on $|G|$.

If $|G| = 1$, then G is trivial, as is $G^{(0)}$. Suppose otherwise that $|G| > 1$ and define $N \coloneqq [G,G] \trianglelefteq G$. Then, N is soluble by Theorem 6.3, as it is a normal subgroup of a soluble group.

By definition of solubility, G has a composition series

$$\{1_G\} = G_0 \mathrel{\ntrianglelefteq} G_1 \mathrel{\ntrianglelefteq} \cdots \mathrel{\ntrianglelefteq} G_r = G$$

where all the composition factors G_i/G_{i-1} are cyclic with prime order. In particular, G/G_{r-1} is cyclic and hence abelian, so $[G,G] = N \leq G_{r-1}$, giving $|N| < |G|$. So, $N^{(m)} = \{1_G\}$ for some $m \in \mathbb{N}$ by the inductive hypothesis. Since $G^{(n)} = [G,G]^{(n-1)}$ by definition, it follows that $G^{m+1} = \{1_G\}$ as required.

Now, for the reverse implication, suppose that $G^{(n)} = \{1_G\}$ for some $n \in \mathbb{N}$. We induct on $|G|$.

If $|G| = 1$, then G is trivial and hence soluble. Suppose otherwise that $|G| > 1$ and again define $N \coloneqq [G,G] \trianglelefteq G$. If $N = G$, then $G^{(n)} = [G,G]^{(n-1)} = G^{(n-1)} = \cdots = G^{(1)} = G^{(0)} = G$, which contradicts the inductive hypothesis. So, $N \ntrianglelefteq G$.

Since $N^{(n-1)} = [G,G]^{(n-1)} = G^{(n)} = \{1_G\}$, N is soluble by the inductive hypothesis. Also, $G/N = G/[G,G] = G^{\mathrm{ab}}$ is abelian and hence soluble. So, G is also soluble by Theorem 6.3. ∎

A previous result gave that normal subgroups of a soluble group are soluble, but this theorem implies that *any* subgroup of a soluble group is soluble.

Corollary 6.5.1. *If G is a finite soluble group, and $H \leq G$, then H is soluble.*

Proof. Since G is soluble, $G^{(n)} = \{1_G\}$ for some $n \in \mathbb{N}$. Since $H^{(n)} \leq G^{(n)}$, we must have $H^{(n)} = \{1_G\}$, so H is soluble. ∎

6.4 Examples of Soluble Groups

Theorem 6.6. *Let G be a group of order p^n for some prime p and $n \in \mathbb{N}$. Then, G is soluble, and furthermore, all composition factors of G are isomorphic to C_p.*

Proof. We proceed by strong induction on $|G|$.

If $|G| = p^1 = p$, then $G \cong C_p$ is cyclic of prime order, so G is soluble with composition length 1, and its composition factor is C_p.

Assume that $|G| = p^n > p$ and that the result holds for all groups of order less than $|G|$. Then, by Theorem 3.11, the centre $Z \coloneqq Z(G)$ is non-trivial. The centre Z is abelian and hence soluble. Also, G/Z is soluble by the inductive hypothesis, so G is soluble by Theorem 6.3. ∎

Theorem 6.7. *Let G_1 and G_2 be finite soluble groups. Then, $G \coloneqq G_1 \times G_2$ is soluble.*

Proof. Consider the projection homomorphism $\pi_1 : G \to G_1$. Define $N \coloneqq \ker(\pi) = \{1_{G_1}\} \times G_2 \cong G_2$, so N is soluble.

Also, $\mathrm{im}(\pi) = G_1$ is soluble, so by the first isomorphism theorem,

$$\begin{gathered} G/\ker(\pi) \cong \mathrm{im}(\pi) \\ G/N \cong G_1 \end{gathered}$$

and hence G/N is soluble, so G is soluble by Theorem 6.3. ∎

Corollary 6.7.1. *Let $G_1, \ldots, G_t$ be finite soluble groups. Then, $G \coloneqq G_1 \times \cdots \times G_t$ is soluble.*

Proof. Induction on the previous result. ∎