Group Theory Notes

by Tyler Wright

github.com/Fluxanoia fluxanoia.co.uk

These notes are not necessarily correct, consistent, representative of the course as it stands today, or rigorous. Any result of the above is not the author's fault.

These notes are in progress.

0 Notation

We commonly deal with the following concepts in Group Theory which I will abbreviate as follows for brevity:

Term	Notation
$(F \setminus \{0_F\}, \times)$	F^*
(invertible $n \times n$ matrices on $F, \times$)	$GL_n(F)$

Contents

1 The Fundamentals

1.1 Binary Operations

A binary operation on a set X is a map $X \times X \to X$.

Take a binary operation $*$ on a set X, we say that $*$ is associative if for all x, y, z in X:

$$x * (y * z) = (x * y) * z.$$

Furthermore, we say e in X is an identity element of $*$ if for all x in X:

$$e * x = x * e,$$

and we say that y in X is the inverse to x if $x * y$ and $y * x$ are both identities of $*$.

1.2 Groups

A group $(G, *)$ is a non-empty set G combined with a binary operation $*$ such that:

- $*$ is associative,
- G contains an identity for $*$,
- for each element in G, there exists some inverse in G with respect to $*$.

1.2.1 Cyclic Groups

A group G is cyclic if it is generated by a single element. Elements in G that generate G are called generators. Cyclic groups are abelian, subgroups of cyclic groups are cyclic.

1.2.2 Dihedral Groups

The dihedral group D_{2n} is the set of symmetries of the regular n-gon, with a rotation r by $\frac{2\pi}{n}$ radians and a reflection s, $D_{2n} = C_n \cup sC_n$.

1.2.3 Torsion Groups

A group is a torsion group if every element has finite order and torsion-free if every non-identity element has infinite order.

1.2.4 p-groups

For p a prime, we say that a group G is a p-group if the order of each element of G is a power of p.

1.3 Set Multiplication

For X, Y subsets of a group $(G, *)$, we define:

$$X * Y = \{x * y : x \in X, y \in Y\},$$

the product set of X and Y (which is a subset of G). We have that $*$ is an associative binary operation on $\mathcal{P}(G)$. Additionally, we define:

$$X^{-1} = \{x^{-1} : x \in X\}.$$

However, these definitions do not define a group on $\mathcal{P}(G)$ as an inverse does not necessarily exist for each element, despite the existence of an identity $\{e\}$.

1.4 Centre

For a group G, the centre of G is the set of elements that commute with all elements of G, denoted by $Z(G)$:

$$Z(G) = \{z \in G : gz = zg, \forall\, g \in G\}.$$

We have that $Z(G)$ is a subgroup of G.

1.5 Properties of Sets

For a group $(G, *)$ with $X \subseteq G$, we have some defined properties:

- X is symmetric if for each x in X, x^{-1} is also in X,
- X is closed under $*$ if for all x, y in X, $x * y$ is in X.

1.6 Order

For a group $G = (X, *)$, G has order $|X|$. The order of an element x of X is defined as follows:

$$\begin{array}{rcll} |x| & = & \infty & \text{if } x^n \neq e \text{ for any } n \text{ in } \mathbb{N}, \\ |x| & = & \min\{n \in \mathbb{N} \mid x^n = e\} & \text{otherwise.} \end{array}$$

Taking x in X:

1. $x^i = x^j$ if and only if $i \equiv j \bmod |x|$,

if x has finite order, then:

2. $x^n = e$ if and only if $|x|$ divides n,
3. $x^n = x^m$ if and only if $|x|$ divides $m - n$,

and if x has infinite order, then:

4. $x^n = x^m$ if and only if $n = m$.

Proof. (1) This trivially holds for the identity, we consider $x \neq e$. If $x^i = x^j$ for some $i \not\equiv j \bmod |x|$, we take $i < j$ without loss of generality and see that:

$$x^i = x^j \Longleftrightarrow e \equiv x^{j-i},$$

but this contradicts the minimality of $|x|$.

(2) For n in $\mathbb{N}$, we take $n = q|x| + r$ for some q in $\mathbb{Z}$, r in $\{0, 1, \ldots, |x| - 1\}$ by the division algorithm. Thus:

$$\begin{aligned} x^n &= x^{q|x|}x^r, \\ &= e^q x^r, \\ &= x^r, \end{aligned}$$

and we can see that $x^r = e$ if and only if $r = 0$ as $r < |x|$ and $|x|$ is minimal. Thus, $x^n = e$ if and only if $r = 0$ which occurs if and only if $|x|$ divides n.

((3) and (4)), We take x to have any order so:

$$x^n = x^m \Longleftrightarrow x^{m-n} = e.$$

Thus, if $|x| < \infty$ then $|x|$ divides $m - n$ by (1) and if $|x| = \infty$ then $m - n = 0$ by the definition of order. $\square$

1.7 Homomorphisms

For $(G, *)$ and $(H, \circ)$ groups, a homomorphism $\varphi : G \to H$ is a map such that $\varphi(x * y) = \varphi(x) \circ \varphi(y)$ for all x and y in G.

1.8 Isomorphisms

An isomorphism from G to H is a bijective homomorphism from G to H. If such a map exists, we say G is isomorphic to H, denoted by $G \cong H$.

1.9 Subgroups

A subset X of a group $(G, *)$ is a subgroup if and only if $(X, *)$ is a group, denoted by $X \leq G$ (if X is a proper subset, this is denoted by $X < G$).

1.9.1 The Product of Subgroups

For H and K subgroups of a group G, HK is a subgroup of G if and only if $HK = KH$.

Proof. $(\Rightarrow)$ If $HK \leq G$:

$$\begin{aligned} HK &= (HK)^{-1} \\ &= K^{-1}H^{-1} \\ &= KH. \end{aligned}$$

$(\Leftarrow)$ If $HK = KH$:

$$\begin{aligned} ee &= e \text{ in } HK, \\ (HK)(HK) &= H(KH)K = H(HK)K = (HH)(KK) = HK, \\ (HK)^{-1} &= K^{-1}H^{-1} = KH = HK, \end{aligned}$$

so HK is a subgroup. □

1.10 The Intersection of Subgroups

For a group G with $\mathcal{X}$ a set of subgroups of G:

$$\bigcap_{X \in \mathcal{X}} X \leq G.$$

Proof. We take A to be the intersection of the subgroups in $\mathcal{X}$, A must be non-empty as each subgroup must contain e. Taking x and y in A, for each X in $\mathcal{X}$ we know that x and y are in X. As X is a subgroup, x^{-1} and thus $x^{-1}y$ are in X. As X is arbitrary, $x^{-1}y$ must be in A. Thus, A is a subgroup of G by the subgroup test. □

1.11 The Subgroup Test

For X a subset of a group G, X is a subgroup if and only if $X \neq \varnothing$ and $x^{-1}y$ is in X for each x, y in X.

Proof. ($\Rightarrow$) If $X \leq G$, then e is in X so $X \neq \varnothing$. For x and y in X, x^{-1} is in X, so $x^{-1}y$ is also in X as X is closed.

($\Leftarrow$) Supposing the latter and taking x and y in X, we have that $x^{-1}x = e$, $x^{-1}e = x^{-1}$, $xy = (x^{-1})^{-1}y$ are all in X. $\square$

1.12 Generated Subgroups

For a group G with $X \subseteq G$ non-empty, we define the subgroup generated by X as:

$$\langle X \rangle = \bigcap_{A \leq G : X \subseteq A} A,$$

the intersection of all the subgroups containing X. This can also be called the smallest subgroup containing X. Alternatively, we have that:

$$\langle X \rangle = \Gamma(X) = \{x_1 x_2 \cdots x_n : x_i \in X \cup X^{-1}, m \in \mathbb{N}\}.$$

Proof. We can see that $\Gamma(X) \subseteq \langle X \rangle$ as $\langle X \rangle$ contains X and is a subgroup so it contains all the finite products of elements of $X \cup X^{-1}$.

If we can show that $\Gamma(X)$ is a subgroup, then that would mean $\langle X \rangle \subseteq \Gamma(X)$ as $\Gamma(X)$ contains X so would have been included in the intersection used to generate $\langle X \rangle$. We know that $\Gamma(X)$ is non-empty as X is non-empty. We take x and y in $\Gamma(X)$, and some n and m in $\mathbb{N}$ and see that:

$$\begin{aligned} x &= x_1 x_2 \cdots x_n, \\ y &= y_1 y_2 \cdots y_m, \end{aligned}$$

by the definition of $\Gamma(X)$. For each i in $[n]$, we know that x_i^{-1} is in $\Gamma(X)$ as $X^{-1} \subseteq \Gamma(X)$ so:

$$\begin{aligned} x^{-1}y &= (x_1 x_2 \cdots x_n)^{-1} y \\ &= x_n^{-1} x_{n-1}^{-1} \cdots x_1^{-1} y_1 y_2 \cdots y_m, \end{aligned}$$

is in $\Gamma(X)$. Thus, $\Gamma(X)$ is a subgroup as required. $\square$

1.13 Cosets

For a group G with $H \leq G$ and x in G, the subset xH is a left coset of H in G and similarly, Hx is a right coset. For x and y in G:

- $xH = yH$ if and only if x is in yH,
- either $xH = yH$ or $xH \cap yH = \varnothing$,
- $|xH| = |H|$.

1.13.1 A Bijection from Left to Right Cosets

For a group G with $H \leq G$, the map $xH \mapsto Hx^{-1}$ is a bijection from the set of left cosets to the set of right cosets.

1.13.2 Index

For a group G with $H \leq G$, the number of distinct left cosets of H in G is called the index of H in G, denoted by $[G : H]$.

1.14 Lagrange's Theorem

For a finite group G with $H \leq G$, $|G| = [G : H]|H|$. Thus, for any subgroup $H \leq G$:

- $[G : H]$ and $|H|$ divide $|G|$,
- for x in G, $|x|$ divides $|G|$,
- if $|G|$ is prime, G is cyclic,
- for a prime p and P and Q subgroups of G with order p, $P \cap Q = \varnothing$ or $P = Q$.

1.15 Outer Direct Product

For $G_1, \dots, G_n$ groups, we set:

$$G_1 \times \cdots \times G_n = \{(a_1, \dots, a_n) : a_i \in G_i, i \in [n]\},$$

and define a binary operation on $G = G_1 \times \cdots \times G_n$ by:

$$(a_1, \dots, a_n)(b_1, \dots, b_n) = (a_1 b_1, \dots, a_n b_n).$$

G is a group under this operation.

1.16 Properties of the Outer Direct Product

For $G_1, \ldots, G_n$ groups, with $G = \prod_{i \in [n]} G_i$:

- $|G| = \prod_{i \in [n]} |G_i|$,
- $Z(G) = \prod_{i \in [n]} Z(G_i)$,
- if G is cyclic, for each i in $[n]$, G_i is cyclic,
- for all σ in S_n, $G \cong \prod_{i \in [n]} G_{\sigma(i)}$,
- for the integers $1 \leq n_1 < n_1 < \cdots < n_r < n$,

$$G \cong (G_1 \times \cdots \times G_{n_1}) \times (G_{n_1+1} \times \cdots \times G_{n_2}) \times \cdots \times (G_{n_r+1} \times \cdots \times G_n),$$

- for $H_1, \ldots, H_n$ groups with $G_i \cong H_i$ for each i in $[n]$ $G \cong \prod_{i \in [n]} H_i$.

2 Homomorphisms

For G, H groups, a homomorphism $\varphi : G \to H$ is a map that for all x, y in G satisfies:

$$\varphi(xy) = \varphi(x)\varphi(y).$$

The image and kernel are defined as expected:

$$\mathrm{Im}(\varphi) = \{\varphi(g) : g \in G\},$$
$$\mathrm{Ker}(\varphi) = \{g \in G : \varphi(g) = e_H\}.$$

2.1 Properties of Homomorphisms

For G, H groups and $\varphi : G \to H$ a homomorphism, we have that:

1. $\varphi(e_G) = e_H$,
2. $\mathrm{Ker}(\varphi)$ is a subgroup of G,
3. $\mathrm{Im}(\varphi)$ is a subgroup of H,
4. φ is injective if and only if $\mathrm{Ker}(\varphi) = \{e_G\}$,
5. $\varphi(x^{-1}) = \varphi(x)^{-1}$ for every x in G,
6. For $x_1, \ldots, x_n$ in G, $\varphi(x_1 \cdots x_n) = \varphi(x_1) \cdots \varphi(x_n)$.

These properties lead us to the following:

- For a finitely ordered element g in G, $|\varphi(g)|$ divides $|g|$ by (6),
- If G is a p-group for p in $\mathbb{P}$, the image of every homomorphism on G is a p-group also.

We can restrict homomorphisms to subgroups or compose them and the result will be a homomorphism.

2.2 Homomorphisms and Generating Sets

For G, H groups, a homomorphism $\varphi : G \to H$, and $X \subseteq G$, we have that $\varphi(\langle X \rangle) = \langle \varphi(X) \rangle$.

Furthermore, for another homomorphism $\psi : G \to H$ with X being a generating set for G, if $\varphi(x) = \psi(x)$ for each x in X, then $\varphi = \psi$.

3 Automorphisms

An automorphism is an isomorphism from a group to itself. The set of all automorphisms on a group G is denoted by $\text{Aut}(G)$ which is a group under composition.

3.1 Inner Automorphisms

For a group G, we have that $\varphi : G \to G$ defined for some g in G as $x \mapsto g^{-1}xg$ is an automorphism. Any automorphism of this form is called an inner automorphism.

Proof. For x, y in G:

$$\begin{aligned}\varphi(xy) &= g^{-1}xyg \\ &= g^{-1}xe_Gyg \\ &= g^{-1}xgg^{-1}yg \\ &= \varphi(x)\varphi(y),\end{aligned}$$

so φ is a homomorphism. We can see that $g^{-1}xg = e_G$ implies that $x = gg^{-1} = e_G$ so $\text{Ker}(\varphi) = \{e_G\}$. Finally, we see that $x = g^{-1}(gxg^{-1})g$ so φ is surjective as x is arbitrary in G. Thus, φ is an automorphism. □

3.2 Conjugation

The operation performed by inner automorphisms is called conjugation by an element. For a group G with x, y, g in G and $X \subseteq G$:

- $g^{-1}xg$ is the conjugation of x by g,
- $g^{-1}xg$ is denoted by x^g,
- $g^{-1}Xg$ is similarly denoted by X^g,
- x and y are said to be conjugate if there exists some g in G such that $x = y^g$.

3.2.1 Conjugations on Subgroups

For G a group with $H \leq G$ and g in G, H^g is a subgroup of G and $H^g \cong H$.

Two subgroups $H, K \leq G$ are said to be conjugate if there exists some g in G with $H = K^g$.

4 Normal and Characteristic Subgroups

For a group G, a subgroup H of G is normal if for each g in G, $gH = Hg$. This is denoted by $H \trianglelefteq G$.

We say H is a characteristic subgroup if for every φ in $\mathrm{Aut}(G)$, $\varphi(H) = H$ (denoted by $H \underset{\text{char}}{\trianglelefteq} G$). We know characteristic subgroups are normal as $\mathrm{Aut}(G)$ contains inner automorphisms.

4.1 Properties of Normal Subgroups

We have that for a group G, the set of normal subgroups on G is closed under set multiplication and intersection. For G, H. groups with $\varphi : G \to H$ a homomorphism, we have that:

1. If $K \leq G$ then $\varphi(K) \leq H$,
2. If $K \trianglelefteq G$ then $\varphi(K) \trianglelefteq \varphi(G)$,
3. If $K \leq H$ then $\varphi^{-1}(K) \leq G$,
4. If $K \trianglelefteq H$ then $\varphi^{-1}(K) \trianglelefteq G$.

Using $K = \{e_H\}$ in (4), we can see that $\mathrm{Ker}(\varphi) \trianglelefteq G$. Furthermore, every normal subgroup is the kernel of some homomorphism.

4.2 A Test for Normal and Characteristic Subgroups

Let G be a group with $H \leq G$:

1. If for every g in G, $H^g \subseteq H$ then $H \trianglelefteq G$,
2. If for every φ in $\mathrm{Aut}(G)$, $\varphi(H) \subseteq H$ then $H \underset{\text{char}}{\trianglelefteq} G$.

Proof. (2) Suppose that $\varphi(H) \subseteq H$ for each φ in $\mathrm{Aut}(G)$. We take φ in $\mathrm{Aut}(G)$, φ^{-1} is also an isomorphism so is also in $\mathrm{Aut}(G)$. We have that $\varphi^{-1}(H) \subseteq H$ by our assumption, applying φ to both sides, we see that $H \subseteq \varphi(H)$ so combined with our assumptions, $H = \varphi(H)$ as required.

(1) We can perform the same argument as (2) by using the fact that the inverse of an inner automorphism is also an inner automorphism. $\square$

4.3 Normal Subgroups of Index 2

For a group G with $H \leq G$ and $[G : H] = 2$, $H \trianglelefteq G$.

Proof. Taking x in G, suppose x is in H, then $xH = H = Hx$.

Suppose x is not in H, then $xH \neq H$ as x is in xH. Thus, xH and H are disjoint cosets of H and as $[G : H] = 2$, $G = H \cup xH$ the disjoint union of these cosets. So, $xH = G \setminus H$. We can apply this reasoning to the right coset and deduce that $xH = Hx$ as required. □

4.4 Properties of the Centre

For a group G, $Z(G)$ is a characteristic subgroup of G and every subgroup of $Z(G)$ is normal.

Proof. We know that $Z(G) \leq G$. We take φ in $\mathrm{Aut}(G)$ and take z in $Z(G)$. We take an arbitrary g in G, as z is in $Z(G)$, $zg = gz$, thus $\varphi(z)\varphi(g) = \varphi(g)\varphi(z)$ as φ is a homomorphism. Furthermore, $\varphi(z)h = h\varphi(z)$ for every h in G as φ is surjective. Thus, $\varphi(z)$ is in $Z(G)$ as required.

Taking $H \leq Z(G)$, we know that for all g in G, h in H, $gh = hg$ as h is in $Z(G)$. Thus, $gH = Hg$ for all g in G. □

4.5 Simple Groups

A non-trivial group is simple if its only normal subgroups are itself and the trivial subgroup.

5 Quotient Groups

For a group G with $H \trianglelefteq G$, G/H is a group under set multiplication and for every a, b in G satisfies:

$$(aH)(bH) = (ab)H.$$

Furthermore, we have $\pi : G \to G/H$ the mapping $g \mapsto gH$ is a surjective homomorphism with kernel H.

Proof. We know set multiplication is associative so, we take a, b in G, and see that:

$$\begin{aligned}
(aH)(bH) &= aHbH \\
&= (ab)(HH) && (H \text{ is normal}) \\
&= (ab)H. && (H \text{ is a subgroup})
\end{aligned}$$

Thus, G/H is closed under the operation. We take the identity to be $e_G H$ and for g in G, the inverse of gH is $g^{-1}H$. So, G/H is a group under set multiplication.

π is trivially surjective, for g in $\mathrm{Ker}(\pi)$, $gH = H$ which means g is in H. The converse is true as H is a subgroup. Thus, π is a homomorphism. $\square$

The group G/H with the operation of set multiplication is called the quotient group of G by H. We call π on this quotient group the quotient homomorphism from G to G/H.

6 The Homomorphism Theorem

For G, H groups with $\varphi : G \to H$ a homomorphism, we let $\pi : G \to G/\operatorname{Ker}(\varphi)$ be the quotient homomorphism. There exists an isomorphism $\psi : G/\operatorname{Ker}(\varphi) \to \operatorname{Im}(\varphi)$ such that $\varphi = \psi \circ \pi$.

If φ is injective, this shows that $G \cong \operatorname{Im}(\varphi)$.

Proof. We set $I = \operatorname{Im}(\varphi)$ and $K = \operatorname{Ker}(\varphi)$, and define $\psi : G/K \to I$ by $gK \mapsto \varphi(g)$. We then consider:

$$\begin{aligned}(gK = hK) &\iff (g^{-1}h \in K)\\ &\iff (\varphi(g^{-1}h) = e_H)\\ &\iff (\varphi(g)^{-1}\varphi(h) = e_H)\\ &\iff (\varphi(g) = \varphi(h)).\end{aligned}$$

So, the map is well-defined and injective. Furthermore, $\psi(\pi(g)) = \psi(gK) = \varphi(g)$. Consider:

$$\begin{aligned}\psi(ghK) &= \varphi(gh)\\ &= \varphi(g)\varphi(h)\\ &= \psi(gK)\psi(hK),\end{aligned}$$

so ψ is a homomorphism and is trivially surjective as required. $\square$

7 The First Isomorphism Theorem

For a group G with $N \trianglelefteq G$, $\pi : G \to G/N$ the quotient homomorphism, and $H \leq G$:

1. $H \cap N \trianglelefteq H$,
2. $\pi(H) \cong H/(H \cap N)$.

Proof. We write $\pi|_H$ for the restriction of π to H. Note that $\pi|_H : H \to G/N$ is a homomorphism. Furthermore:

$$\begin{aligned}\operatorname{Im}(\pi|_H) &= \pi(H),\\ \operatorname{Ker}(\pi|_H) &= H \cap \operatorname{Ker}(\pi) = H \cap N.\end{aligned}$$

As the kernel of a homomorphism is a normal subgroup in the domain, $H \cap N \trianglelefteq H$. The homomorphism says that $\pi(H) \cong H/H \cap N$. $\square$

Additionally, we have that $HN \leq G$ and $\pi(H) = HN/N$.

Proof. We know that $HN \leq G$ if and only if $HN = NH$ which is implied by the normality of N. We consider the group:

$$\begin{aligned} HN/N &= \Big(\{hnN : h \in H, n \in N\}, \times\Big), \\ &= \Big(\{hN : h \in H\}, \times\Big), && (N \text{ is a subgroup}) \\ &= \pi(H). \end{aligned}$$

As required. □

7.1 The Order of the Product

Let G be a group with $N \trianglelefteq G$, and $H \leq G$. If HN is finite, then:

$$|HN| = \frac{|H||N|}{|H \cap N|}.$$

Proof. We can see that:

$$\begin{aligned} \frac{|HN|}{|N|} &= [HN : N] && \text{(By Lagrange's Theorem)} \\ &= |\pi(H)| && \text{(By the above)} \\ &= [H : H \cap N] && \text{(By the First Isomorphism Theorem)} \\ &= \frac{|H|}{|H \cap N|}, && \text{(By Lagrange's Theorem)} \end{aligned}$$

as required. □

8 The Second Isomorphism Theorem

For a group G with $N \leq H \leq G$, and $N, H \trianglelefteq G$, we have that $H/N \trianglelefteq G/N$ and $(G/N)/(H/N) \cong G/H$.

Proof. We let $\varphi : G/N \to G/H$ be defined by $gN \mapsto gH$. We have that:

$$aN = bN \Rightarrow ab^{-1} \in N \subseteq H \Rightarrow aH = bH,$$

so φ is well-defined. It is a homomorphism because:

$$\begin{aligned}
\varphi(aNbN) &= \varphi(abN) \\
&= abH \\
&= aHbH \\
&= \varphi(aN)\varphi(bN),
\end{aligned}$$

and is trivially surjective. Considering:

$$\begin{aligned}
\operatorname{Ker}(\varphi) &= \{gN : gH = eH\} \\
&= \{gN : g \in H\} \\
&= H/N,
\end{aligned}$$

we have that $H/N \trianglelefteq G/N$ as it is the kernel of a homomorphism and that $(G/N)/(H/N) \cong G/H$ by the homomorphism theorem. $\square$

9 The Correspondence Theorem

For a group G with $N \trianglelefteq G$ and $\pi : G \to G/N$ the quotient homomorphism. We have that:

1. If $K \subseteq G/N$ then:
   (a) $K \leq G/N$ if and only if $K = H/N$ for some $H \leq G$ containing N,
   (b) $K \trianglelefteq G/N$ if and only if $K = H/N$ for some $H \trianglelefteq G$ containing N,
2. If $N \subseteq H \subseteq G$ then:
   (a) $H \leq G$ if and only if $H = \pi^{-1}(K)$ for some $K \leq G/N$,
   (b) $H \trianglelefteq G$ if and only if $H = \pi^{-1}(K)$ for some $K \trianglelefteq G/N$.

Proof. We have already proved the ($\Leftarrow$) direction in (4.1).

(1)(a) Note that $K = \pi(\pi^{-1}(K))$. By the ($\Rightarrow$) direction of (2)(a), we know that $\pi^{-1}(K)$ is a subgroup of G and contains N as it's a subgroup. So, $\pi(\pi^{-1}(K)) = \pi^{-1}(K)/N$. Taking $H = \pi^{-1}(K)$ proves the ($\Rightarrow$) direction of (1)(a).

(1)(b) To prove the ($\Rightarrow$) direction of (1)(b), we just need to prove that $K \trianglelefteq G/N$ implies that $\pi^{-1}(K) \trianglelefteq G$ which we proved in the ($\Leftarrow$) direction of (2)(b).

(2) We know that H is a union of left cosets of N as it's a subgroup, this means that $H = \pi^{-1}(\pi(H))$. We apply (4.1) again with $\phi = \pi$ and get the ($\Rightarrow$) direction of (2). $\square$

10 Commutators

For x, y in a group G, we define the commutator of x and y as:

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

This can be considered as the 'cost' of commuting x and y:

$$xy = yx[x, y].$$

10.1 Commutators under Homomorphisms

For x, y in a group G with a homomorphism φ from G to H, we have that $\varphi([x, y]) = [\varphi(x), \varphi(y)]$.

10.2 Commutator Subgroups

For a group G with $H, K \leq G$, we define a subgroup $[H, K]$ by:

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

The subgroup $[G, G]$ is called the commutator subgroup. Furthermore, if G is abelian, $[G, G] = \{e_G\}$.

10.3 Commutator Subgroup of Characteristic Subgroups

For a group G with $H, K \underset{\text{char}}{\trianglelefteq} G$, $[H, K] \underset{\text{char}}{\trianglelefteq} G$. Furthermore, $[G, G] \underset{\text{char}}{\trianglelefteq} G$.

Proof. We take φ in $\mathrm{Aut}(G)$:

$$\begin{aligned}
\varphi([H, K]) &= \varphi(\langle [h, k] : h \in H, k \in K \rangle) \\
&= \langle \varphi([h, k]) : h \in H, k \in K \rangle \\
&= \langle [\varphi(h), \varphi(k)] : h \in H, k \in K \rangle \\
&= \langle [h, k] : h \in H, k \in K \rangle && (H, K \underset{\text{char}}{\trianglelefteq} G) \\
&= [H, K],
\end{aligned}$$

as required. $\square$

10.4 Abelian Quotients

For a group G with $H \trianglelefteq G$, G/H is abelian if and only if $[G, G] \leq H$. Furthermore, this shows that a quotient of G is abelian if and only if it is isomorphic to a quotient of $G/[G, G]$ (by the second isomorphism theorem).

Proof. We take $\pi : G \to G/H$ to be the quotient homomorphism.

($\Rightarrow$) If G/H is abelian then we take x, y arbitrary in G. We have that $\pi([x, y]) = [\pi(x), \pi(y)] = e_G H$. Thus, $[x, y]$ is in H. Thus, as x, y are arbitary, $[G, G] \subseteq H$.

($\Leftarrow$) If $[G, G] \subseteq H$ then for every xH, yH in G/H we have that:

$$\begin{aligned} [xH, yH] &= (x^{-1}H)(y^{-1}H)(xH)(yH) \\ &= [x, y]H \\ &= H. \end{aligned}$$

Thus, G/H is abelian. $\square$

10.4.1 Quotients of Abelian Groups

Every quotient of an abelian group is abelian.

Proof. If G is abelian then $[G, G] = \{e_G\}$. So, for each $H \underset{\text{char}}{\trianglelefteq} G$ we have $[G, G] \subseteq H$ and so G/H is abelian by the above. $\square$

10.5 The Abelianisation

For a group G, the abelianisation of G is the quotient group $G/[G, G]$. This group is always abelian and is the largest possible abelian quotient of G.

It can be that $G/[G, G] = \{e_G\}$ ($[G, G] = G$). These groups are called perfect. An example is non-abelian simple groups as $[G, G] \underset{\text{char}}{\trianglelefteq} G$.

11 Direct Products

We have already seen the outer direct product as:

$$G_1 \times \cdots \times G_n = \{(g_1, \ldots, g_n) : g_i \in G_i\},$$

for groups $G_1, \ldots, G_n$ which forms a group with component-wise group operations.

For a group G with $H_1, \ldots, H_n \trianglelefteq G$. We say G is the inner direct product of $H_1, \ldots, H_n$ if:

- $G = H_1 \times \cdots \times H_n$,
- $H_i \cap (H_1 \times \cdots \times H_{i-1} \times H_{i+1} \times \cdots \times H_n) = \{e_G\}$ for all i in $[n]$.

We have that $|G| = \prod_i H_i$.

11.1 Component Groups

We let $G = G_1 \times \cdots \times G_n$, for each i in $[n]$, we set:

$$\widehat{G_i} = \{(e, \ldots, e, g_i, e, \ldots, e) : g_i \in G_i\}.$$

We have that:

1. For each i in $[n]$, $\widehat{G_i} \trianglelefteq G$,
2. For each i in $[n]$, $\widehat{G_i} \cong G_i$,
3. G is the inner direct product of $\widehat{G_1}, \ldots, \widehat{G_n}$.

Proof. (1) We can see that:

$$\psi((g_1, \ldots, g_n)) = (g_1, \ldots, g_{i-1}, e, g_{i+1}, \ldots g_n),$$

is a homomorphism with kernel $\widehat{G_i}$. Thus, $\widehat{G_i} \trianglelefteq G$.

(2) We can see that:

$$\varphi_i((e, \ldots, e, g_i, e, \ldots, e)) = g_i,$$

is an isomorphism. Thus, $\widehat{G_i} \cong G_i$.

(3) We have that $G = \widehat{G_1} \cdots \widehat{G_n}$ as:

$$(g_1, \ldots, g_n) = (g_1, e, \ldots)(e, g_2, e, \ldots) \cdots (e, \ldots, e, g_n).$$

Furthermore, $\widehat{G_i} \cap G_i' = \{e\}$ where $G' = \widehat{G_1}, \ldots, \widehat{G_{i-1}}, \widehat{G_{i+1}}, \ldots G_n$ as the elements of G_i' are of the form $(g_1, \ldots, g_{i-1}, e, g_{i+1}, \ldots, g_n)$ whereas elements of $\widehat{G_i}$ are of the form $(e, \ldots, e, g_i, e, \ldots, e)$. Thus, the only element in common is e_G. $\square$

11.2 The Commutator of Normal Subgroups

For a group G with $H, K \trianglelefteq G$, $[H, K] \subseteq H \cap K$.

Proof. For h in H and k in K, $[h, k] = h^{-1}k^{-1}hk$. But:

- $h^{-1}k^{-1}h$ is in $h^{-1}Kh = K$,
- $k^{-1}hk$ is in $k^{-1}Hk = H$,

so $[h, k]$ is in $H \cap K$. □

Furthermore, if $G = H_1 \times \cdots \times H_n$ is an inner direct product, then for $i \neq j$ both in $[n]$, we have that the elements of H_i commute with the elements of H_j.

Proof. The definition of the inner direct product means that $H_i \cap H_j = \{e\}$. This means that $[H_i, H_j] = \{e\}$ as required. □

11.3 Isomorphism between Products

For a group G the inner direct product of subgroups $H_1, \ldots, H_n$, $G \cong H_1 \times \cdots \times H_n$.

Proof. We define $\varphi : H_1 \times \cdots \times H_n \to G$ by:

$$\varphi((h_1, \ldots, h_n)) = h_1 \cdots h_n,$$

which is a homomorphism by the commutativity of H_i and H_j (where $i \neq j$). The definition of the inner direct product implies that it is surjective. We take $(h_1, \ldots, h_n) \in \mathrm{Ker}(\varphi)$:

$$\begin{aligned}
& h_1 \cdots h_n = e \\
\implies \quad & h_i^{-1} = h_1 \cdots h_{i-1}h_{i+1} \cdots h_n \\
\implies \quad & h_i^{-1} \in H_i \cap (H_1 \cdots H_{i-1}H_{i+1} \cdots H_n) \\
\implies \quad & h_i^{-1} = e.
\end{aligned}$$

Thus, as i was chosen arbitrarily, $(h_1, \ldots, h_n) = (e, \ldots, e)$. Thus, φ is an isomorphism. □

11.4 Criteria for Inner Direct Products

11.4.1 By Unique Compositions

For a group G with $H_1, \ldots, H_n$ normal subgroups of G, G is an inner direct product of $H_1, \ldots, H_n$ if and only if for all g in G, there exists a unique h_i in each H_i such that $g = \prod_i h_i$.

Proof. ($\Rightarrow$) By the definition, we have $g = \prod_i h_i$ for some h_i in each H_i so it suffices to show this product is unique. We suppose that:

$$\prod_i k_i = g = \prod_i h_i,$$

for some k_i, h_i in each H_i. We fix i and see that:

$$\begin{aligned}
e &= g^{-1}g \\
&= h_n^{-1} \cdots h_1^{-1} k_1 \cdots k_n \\
&= h_1^{-1} k_1 \cdots h_n^{-1} k_n \\
&= h_i^{-1} k_i h_1^{-1} k_1 \cdots h_{i-1}^{-1} k_{i-1} h_{i+1}^{-1} k_{i+1} \cdots h_n^{-1} k_n \\
k_i^{-1} h_i &= h_1^{-1} k_1 \cdots h_{i-1}^{-1} k_{i-1} h_{i+1}^{-1} k_{i+1} \cdots h_n^{-1} k_n \\
&\in H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_n) \\
&= \{e\}.
\end{aligned}$$

as G is the direct product of $H_1, \ldots, H_n$ which means elements from differing subgroups commute. Thus, for each i, $h_i = k_i$.

($\Leftarrow$) Clearly $G = H_1 \cdots H_n$ so it suffices to show that:

$$H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_n) = \{e\}$$

for each i. We take x in this intersection:

$$\begin{aligned}
x = h_i &= h_1 \cdots h_{i-1} h_{i+1} \cdots h_n \\
e \cdots e h_i e \cdots e &= h_1 \cdots h_{i-1} e h_{i+1} \cdots h_n,
\end{aligned}$$

which, by the uniqueness of the composition of x, means that $x = e$ as required. □

11.4.2 By the Size

For G a finite group with $H_1, \dots, H_n \trianglelefteq G$ such that $G = H_1 \cdots H_n$. G is an inner direct product if and only if $|G| = \prod_i |H_i|$.

Proof. ($\Rightarrow$) As G is an inner direct product we have the result.

($\Leftarrow$) As $|G| = \prod_i |H_i|$, each $h_1 \cdots h_n$ product of elements in $H_1 \cdots H_n$ are distinct. By the above, this means G is an inner direct product. $\square$

12 Finitely Generated Abelian Groups

We will write $\mathbb{Z}^n = \{(m_1, \ldots, m_n) : m_1, \ldots, m_n \in \mathbb{Z}\}$ and $e_i = (0, \ldots, 1, \ldots, 0) \in \mathbb{Z}^n$ with 1 in the i^{th} entry. These are the standard generators for $\mathbb{Z}^n$.

For some n in $\mathbb{N}$, we write $\mathbb{Z}_n$ to be the integers modulo n which is a group under addition. Additionally, $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ and $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$.

12.1 Classification of Cyclic Groups

For a cyclic group G, if $|G| = n$ finite, we have that $G \cong \mathbb{Z}_n$. Otherwise, $G \cong \mathbb{Z}$.

Proof. We choose x as a generator of G. We take $\varphi : \mathbb{Z} \to G$ to be defined as $\varphi(m) = x^m$. We can see that φ is a surjective homomorphism. If $|x| = \infty$ then $\operatorname{Ker}(\varphi) = \{0\}$, otherwise, $\operatorname{Ker}(\varphi) = |x|\mathbb{Z}$. By the homomorphism theorem:

$$G = \operatorname{Im}(\varphi) \cong \mathbb{Z}/\operatorname{Ker}(\varphi).$$

The result follows as $\mathbb{Z}/\operatorname{Ker}(\varphi) = \mathbb{Z}$ if $|x| = \infty$ and $\mathbb{Z}_{|x|}$ otherwise. □

12.2 The Torsion Subgroup

For an abelian group G with $T \subseteq G$ the set of elements in G of finite order and a prime p with $G_p \subseteq T$ the set of elements in T of with order equal to a power of p. We have that $G_p \leq T \leq G$ and G/T is torsion-free with T called the torsion subgroup of G and G_p called the p-primary component of G.

Proof. We suppose x and y are in T with $|x| = k$, $|y| = m$. We know that $km(x - y) = 0$ so $|x - y| \leq km < \infty$, thus $(x - y)$ is in T so T is a subgroup of G by the subgroup test.

Furthermore, $|x - y|$ must divide km so if x and y are in G_p then km is a power of p. Thus, $|x - y|$ is a power of p so $(x - y)$ is in G_p. Again, by the subgroup test, G_p is a subgroup of T.

Suppose $z + T$ has finite order for some z in G. If so, there exists some m in $\mathbb{N}$ with $mx + T = T$, in particular mx is in T. By the definition of T, there exists some n in $\mathbb{N}$ with $nmx = 0$. But, this would mean x has finite order so x is in T. Thus, G/T is torsion-free. □

12.3 The Primary Decomposition Theorem

For a finite abelian group G, we take $p_1, \ldots, p_k$ to be the prime factors of $|G|$. We have that $G = G_{p_1} \oplus \cdots \oplus G_{p_k}$.

Proof. We take x in G, by Lagrange's Theorem, we have that $x = p_1^{l_1} \cdots p_k^{l_k}$ for some $l_1, \ldots, l_k$ in $\mathbb{N}_0$. For each i in $[k]$, we set:

$$n_i = \prod_{j \in [k] \setminus \{i\}} p_j^{l_j},$$

and note that $|n_i x| = p_i^{l_i}$ so $n_i x$ is in G_{p_i}. Clearly $\gcd(n_1, \ldots, n_k) = 1$, so by the Euclidean algorithm there exists $m_1, \ldots, m_k$ such that $m_1 n_1 + \cdots + m_k n_k = 1$. Thus:

$$\begin{aligned} x &= \left(\sum_{i=1}^{k} m_i n_i \right) \cdot x \\ &= \sum_{i=1}^{k} m_i (n_i x) \\ &\in \sum_{i=1}^{k} G_{p_i}. \end{aligned}$$

Thus, $G = G_{p_1} + \cdots + G_{p_k}$.

We now consider x_i, x_i' in G_{p_i} for each i in $[k]$ such that $\sum_{i \in [k]} x_i = \sum_{i \in [k]} x_i'$. We write $y_i = x_i - x_i'$ so that $\sum_{i \in [k]} y_i = 0$. Furthermore, we say $|y_i| = p_i^{d_i}$ and set:

$$r_i = \prod_{j \in [k] \setminus \{i\}} |y_i| = \prod_{j \in [k] \setminus \{i\}} p_j^{d_j}.$$

As $|y_i|$ divides $|r_j|$ for all $j \in [k] \setminus \{i\}$, we know that $r_i y_j = 0$. This implies that $r_i y_i = 0$ as $\sum_{i=1}^{k} y_i = 0$.

Moreover, as r_i and p_i are coprime by definition, the Euclidean algorithm implies that there exists a, b in $\mathbb{Z}$ such that:

$$\begin{aligned} & a r_i + b p_i^{d_i} = 1, \\ \implies \quad & y_i = (a r_i + b p_i^{d_i}) y_i, \\ \implies \quad & y_i = a r_i y_i + b p_i^{d_i} y_i, \\ \implies \quad & y_i = 0 + 0 = 0, \end{aligned}$$

so $x_i = x_i'$ for each i in $[k]$. Thus, our compositions are unique as required. $\square$

12.4 Finitely Generated Abelian Torsion Groups

A finitely generated torsion group is finite.

Proof. We take $x_1, \ldots, x_n$ to be the finite generating set for an abelian torsion group G so:

$$G = \{l_1 x_1 + \cdots + l_n x_n : 0 \leq l_i < |x_i|\},$$

which is finite since $|x_i| < \infty$ for all i in $[n]$. □

12.5 Order of Elements in p-groups

For a prime p and a p-group G, we take g in G. We set k in $\mathbb{N}$ to np^r with n, p coprime and r in $\mathbb{N}_0$. If $p^r \leq |g|$ then $|g^k| = \frac{|g|}{p^r}$.

Proof. We know that $|g| = p^m$ for some m as G is a p-group. For d in $\mathbb{N}$:

$$\begin{aligned} & (g^k)^d = e \\ \iff \quad & g^{dnp^r} = e \\ \iff \quad & p^m \text{ divides } dnp^r \\ \iff \quad & p^m \text{ divides } dp^r \\ \iff \quad & p^{m-r} \text{ divides } d, \end{aligned}$$

thus, $|g^k| = p^{m-r} = \frac{|g|}{p^r}$ as required. □

12.6 Elements with Coset Order

For G a finite abelian p-group for some prime p. We take g in G to have maximum order. For every x in G, there exists y in $x + \langle g \rangle$ sich that the order of y in G is equal to the order of $x + \langle g \rangle$ in $G/\langle g \rangle$.

Proof. We write $x + \langle g \rangle = p^m$ for some m, noting that $p^m \cdot x$ is in $\langle g \rangle$ so $p^m \cdot x = l \cdot g$ for some l in $\mathbb{N}_0$ (if $l = 0$ we are done). We write $l = np^r$ with n, p coprime. If $p^r \geq |g|$ then $l \cdot g = 0$ and $|x| = p^m$ and we are done. Otherwise, we use the result above to see that $|l \cdot g| = \frac{|g|}{p^r}$ and $|p^m x| = \frac{|x|}{p^m}$ so $\frac{|g|}{p^r} = \frac{|x|}{p^m}$. The maximality of g implies that $|g| \geq |x|$ so $r \geq m$ and thus p^m divides l. We define:

$$y = x - \frac{l}{p^m} \cdot g,$$

thus $p^m y = p^m(x - np^{r-m} g) = 0$ so $|y| \leq p^m$. But, as y is in $x + \langle g \rangle$, $|y| \geq p^m$ so $|y| = p^m$ as required. □

12.7 Decomposition of Finite Abelian p-groups

For a finite abelian p-group G with p prime, there exists a k in $\mathbb{N}_0$ and $m_1, \dots, m_k$ in $\mathbb{N}$ such that $G \cong \mathbb{Z}_{p^{m_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{m_k}}$.

Proof. It is sufficient to show that for $x_1, \dots, x_k$ in G, G is an inner direct sum:

$$G = \langle x_1 \rangle \oplus \cdots \oplus \langle x_k \rangle. \tag{$*$}$$

If $G = \{0\}$ then this is trivial so we assume $|G| > 1$. By strong induction, we assume every group of order lesser to that of G is of the form shown in $(*)$.

We take g in G to have maximum order, $g \neq e$ as our group is non-trivial so $|G/\langle g \rangle| < |G|$ so by induction, there exists $x_1, \dots, x_k$ in G such that:

$$G/\langle g \rangle = \langle x_1 + \langle g \rangle \rangle \oplus \cdots \oplus \langle x_k + \langle g \rangle \rangle.$$

The previous result implies that we can assume that $|x_i| = |x_i + \langle g \rangle|$, so:

$$\begin{aligned} |G/\langle g \rangle| &= |\langle x_1 + \langle g \rangle \rangle| \cdots |\langle x_k + \langle g \rangle \rangle| \\ &= |x_1| \cdots |x_k|, \end{aligned}$$

which combined with Lagrange's theorem means that:

$$\begin{aligned} |G| &= [G : \langle g \rangle] \\ &= |G/\langle g \rangle| \cdot |g| \\ &= |x_1| \cdots |x_k| \cdot |g|. \end{aligned}$$

We want to show that $G = \langle x_1 \rangle + \cdots + \langle x_k \rangle + \langle g \rangle$ so for all h in G, $h = ng + \sum_{i=1}^{k} l_i x_i$ for some $l_1, \dots, l_k, n$ in $\mathbb{N}_0$. By $(*)$ we know that:

$$\begin{aligned} & h + \langle g \rangle = (l_1 x_1 + \cdots + l_k x_k) + \langle g \rangle \\ \implies \quad & h \in (l_1 x_1 + \cdots + l_k x_k) + \langle g \rangle \\ \implies \quad & h = l_1 x_1 + \cdots + l_k x_k + ng \text{ for some } n. \end{aligned}$$

As we have that G is a sum of $\langle x_1 \rangle, \dots, \langle x_k \rangle, \langle g \rangle$ and its size is a product of the size of these groups, G is an inner direct product of said elements as required. $\square$

12.8 Homomorphism from $\mathbb{Z}^n$ to Sequences

For n in $\mathbb{N}$ and an abelian group G, and every $g_1, \dots, g_n$ in G, there exists a unique homomorphism $\varphi : \mathbb{Z}^n \to G$ satisfying $\varphi(e_i) = g_i$ for all i. In particular, $\varphi((m_1, \dots, m_1)) = m_1 g_1 + \cdots + m_n g_n$.

Proof. This is trivially a homomorphism and is unique as homomorphisms are defined by the images of a set of generators. $\square$

12.9 One-way Inverses on Homomorphisms to $\mathbb{Z}^n$

For an abelian group G and $\alpha : G \to \mathbb{Z}^n$ is a surjective homomorphism, there exists an injective homomorphism $\beta : \mathbb{Z}^n \to G$ such that $\alpha \circ \beta = \iota_{\mathbb{Z}^n}$ (the identity on $\mathbb{Z}^n$).

Proof. If $n = 0$, this is trivial. Otherwise, there exists $g_1, \ldots, g_n$ in G such that $\alpha(g_i) = e_i$ for all i as α is surjective. The previous result states that there exists a homomorphism β from $\mathbb{Z}^n$ to G such that $\beta(e_i) = g_i$ for all i. This gives us that $(\alpha \circ \beta)(e_i) = e_i$ which defines $\alpha \circ \beta$ as homomorphisms are defined by the images of a set of generators. Thus, $\alpha \circ \beta = \iota_{\mathbb{Z}^n}$.

We can see that:

$$\begin{aligned}\ker(\beta) &\subseteq \ker(\alpha \circ \beta) \\ &= \ker(\iota_{\mathbb{Z}^n}) \\ &= \{0\}.\end{aligned}$$

Thus, $\ker(\beta) = \{0\}$ so β is injective as required. $\square$

12.10 Abelian Groups with $\mathbb{Z}^n$ Quotients

For an abelian group G with $H \leq G$ satisfying $G/H \cong \mathbb{Z}^n$ for some n in $\mathbb{N}_0$, we have that $G = H \oplus K$ for some $K \leq G$ satisfying $K \cong \mathbb{Z}^n$.

Proof. We consider $\pi : G \to G/H$ the quotient homomorphism and $\psi : G/H \to \mathbb{Z}^n$ an isomorphism. We set $\alpha = \psi \circ \pi$ from G to $\mathbb{Z}^n$, which is a surjective homomorphism. The previous result gives us $\beta : \mathbb{Z}^n \to G$ an injective homomorphism with $\alpha \circ \beta = \iota_{\mathbb{Z}^n}$. We note that $H = \ker(\alpha) \leq G$ and set $K = \beta(\mathbb{Z}^n) \leq G$. Furthermore, as β is injective, $K \cong \mathbb{Z}^n$.

Given g in G:

$$\begin{aligned}\alpha(g - (\beta \circ \alpha)(g)) &= \alpha(g) - \alpha((\beta \circ \alpha)(g)) \\ &= \alpha(g) - ((\alpha \circ \beta) \circ \alpha)(g) \\ &= \alpha(g) - \alpha(g) \\ &= 0,\end{aligned}$$

therefore $(g - (\beta \circ \alpha)(g))$ is in $\ker(\alpha) = H$ so g is in $(\beta \circ \alpha)(g) + H$ in particular, g is in $K + H = H + K$. As $\alpha \circ \beta = \iota_{\mathbb{Z}^n}$, $\ker(\alpha) \cap \beta(\mathbb{Z}^n) = \{0\}$ which means $H \cap K = \{0\}$. Thus, $G = H \oplus K$ as required. $\square$

12.11 Finitely Generated Subgroups

For a finitely generated abelian group G with $H \leq G$ satisfying $G/H \cong \mathbb{Z}^n$ for some n in $\mathbb{N}_0$, H is finitely generated.

Proof. We know that $G \cong H \oplus \mathbb{Z}^n$ by the previous result. The projection π from $H \oplus \mathbb{Z}^n$ onto H defined by $(h, z) \mapsto h$ is a homomorphism. Since $H \oplus \mathbb{Z}^n$ is finitely generated, H is finitely generated by these generators under π. $\square$

12.12 Fundamental Theorem of Finitely Generated Torsion-free Abelian Groups

For n in $\mathbb{N}$ and G a finitely generated torsion-free abelian group generated by at most n elements, $G \cong \mathbb{Z}^k$ for some $k \leq n$.

Proof. We take $\{g_1, \ldots, g_n\}$ to be a generating set of G. If $n = 1$, G is cyclic and has infinite order so $G \cong \mathbb{Z}$. Otherwise, we set:

$$H = \{x \in G : \exists\, m \in \mathbb{N} \text{ such that } mx \in \langle g_n \rangle\},$$

and observe that H is a subgroup via the subgroup test. We consider the quotient G/H and the quotient homomorphism $\pi : G \to G/H$. We know that G/H is torsion-free as:

$$\begin{aligned} k\pi(x) = 0 &\implies \pi(kx) \\ &\implies kx \in H \\ &\implies lkx \in \langle g_n \rangle \text{ for some } l \\ &\implies x \in H \\ &\implies \pi(x) = 0. \end{aligned}$$

So 0 is the only element of finite order in G/H as π is surjective. Furthermore, g_n is also in H so G/H is generated by $\{\pi(g_1), \ldots, \pi(g_{n-1})\}$. By induction on n, $G/H \cong \mathbb{Z}^k$ for some $k \leq n - 1$. By a previous result, $G \cong H \oplus \mathbb{Z}^k$ so it's sufficient to show that $H \cong \{0\}$ or $\mathbb{Z}$.

We know that H is torsion-free as it's a subgroup of G, we consider $H/\langle g_n \rangle$ which is finitely generated via π and the quotient homomorphism to $H/\langle g_n \rangle$ and a torsion group as for all h in H, there's some l such that $l(h + \langle g_n \rangle) = \langle g_n \rangle$. In particular, $H/\langle g_n \rangle$ is finite with size m for instance. Thus, for all h in H, $m(h + \langle g_n \rangle) = \langle g_n \rangle$ so mh is in $\langle g_n \rangle$. We define $\varphi : H \to \langle g_n \rangle$ by $h \mapsto mh$ which is clearly a homomorphism and injective as H is torsion-free (so $mh = 0$ implies that $h = 0$). So, $H \cong \varphi(H) \leq \langle g_n \rangle$, in particular, H is cyclic. Thus, $H \cong \mathbb{Z}$ because H has infinite order and is cyclic as required. $\square$

12.13 Fundamental Theorem of Finitely Generated Abelian Groups

Suppose G is a finitely generated abelian group, there exists non-negative integers n and k, primes $p_1, \ldots, p_k$, and natural numbers $n_1, \ldots, n_k$ such that:

$$G \cong \mathbb{Z}_{p_1^{m_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{m_k}} \oplus \mathbb{Z}^n$$

Proof. We take $T \leq G$ to be the torsion subgroup. As G is finitely generated, G/T is also and by the previous result, $G/T \cong \mathbb{Z}^n$ for some n. By more previous results, we know that $G \cong T \oplus \mathbb{Z}^n$ and T is finitely generated and hence finite. Again, we know that there are finitely many primes $p_1, \ldots, p_m$ such that $G_{p_i} \neq \{0\}$, each G_{p_i} is finite, and $T = G_{p_1} \oplus \cdots \oplus G_{p_m}$. We know that each $G_{p_i} = \mathbb{Z}_{p_i^{m_1}} \oplus \cdots \oplus \mathbb{Z}_{p_i^{m_d}}$ which gives us the result. $\square$

13 Symmetric Groups

For a set X, a permutation of X is a bijection from X to X, the set of all permutations of X forms a group under composition denoted by $\mathrm{Sym}(X)$. For n in $\mathbb{N}$, we write $\mathrm{Sym}([n])$ as S_n. Note that $|\mathrm{Sym}(X)| = |X|!$.

Proof. We prove this by considering the number of bijections between sets X, Y of size n. For $n = 1$, $f = \{(x, y) : x \in X, y \in Y\}$ has only one pair. For $n > 1$:

$$\begin{aligned} m &= \sum_{y \in Y} |\{\text{bijections from } X \text{ to } Y : x \mapsto y\}| \\ &= \sum_{y \in Y} |\{\text{bijections from } X \setminus \{x\} \text{ to } Y \setminus \{y\}\}| \\ &= \sum_{y \in Y} (n-1)! \\ &= n \cdot (n-1)! \\ &= n!, \end{aligned}$$

as required. □

13.1 Cycles

For k in $\mathbb{N}$, a permutation f in S_n is called k-cycle if there are k distinct members $i_1, \ldots, i_k$ in $[n]$ such that:

$$f(i_j) = \begin{cases} i_{j+1} & j \in [k-1] \\ i_1 & j = k, \end{cases}$$

in which case, we write $f = (i_1, \ldots, i_k)$. A 2-cycle is called a transposition and cycles $(i_1, \ldots, i_k)$, $(j_1, \ldots, j_l)$ are disjoint if $\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_l\} = \varnothing$. Furthermore:

- A k-cycle has order k,
- $(i_1, \ldots, i_k) = (i_2, \ldots, i_k, i_1)$,
- $(i_1, \ldots, i_k)^{-1} = (i_k, \ldots, vi_1)$,
- $(i_1, \ldots, i_k) = (i_1, i_2)(i_2, i_3) \cdots (i_{k-1}, i_k)$,
- Disjoint cycles commute.

13.2 Permutations as Disjoint Cycles

For n in $\mathbb{N}$, each element of S_n can be written as a product of disjoint cycles with lengths summing to n which is unique up to reordering. Every element can also be written as a product of transpositions.

From this, we can see that S_n is generated by the set of transpositions on 1, $\{(1,2),(1,3),\dots,(1,n)\}$ as $(1,i)(1,j)(1,i)=(i,j)$.

13.3 Cycle Type

For f in S_n written as a product of disjoint cycles with lengths summing to n, we take $l_1,\dots,l_k$ be the lengths of these cycles in descending order. The k-tuple $(l_1,\dots,l_k)$ is the cycle type of f.

From this, we can see that $|f| = \operatorname{lcm}(l_1,\dots,l_k)$.

13.4 Conjugacy in S_n

For all g in S_n with $i_1,\dots,i_k$ distinct elements of $[n]$:

$$g(i_1,\dots,i_k)g^{-1} = (g(i_1),\dots,g(i_k)).$$

Proof. For $k=1$, $(i_1)=e$ so $g(i_1)g^{-1}=gg^{-1}=e=(g(i_1))$. For $k=2$ and x in $S_n\setminus\{g(i_1),g(i_2)\}$:

$$\begin{aligned} g(i_1,i_2)g^{-1}(g(i_1)) &= g(i_2), \\ g(i_1,i_2)g^{-1}(g(i_2)) &= g(i_1), \\ g(i_1,i_2)g^{-1}(x) &= gg^{-1}(x) \\ &= x, \end{aligned}$$

so $g(i_1,i_2)g^{-1}=(g(i_1),g(i_2))$. For $k>2$, $(i_1,\dots,i_k)=(i_1,i_2)\cdots(i_{k-1},i_k)$ so:

$$\begin{aligned} g(i_1,\dots,i_k)g^{-1} &= g(i_1,i_2)\cdots(i_{k-1},i_k)g^{-1} \\ &= g(i_1,i_2)g^{-1}g\cdots g^{-1}g(i_{k-1},i_k)g^{-1} \\ &= (g(i_1),g(i_2))\cdots(g(i_{k-1}),g(i_k)) \\ &= (g(i_1),\dots,g(i_k)), \end{aligned}$$

as required. $\square$

13.5 Conjugacy and Cycle Type

For x, y in S_n, x and y are conjugate if and only if they have the same cycle type.

Proof. We take the cycle type of x be $(l_1, \ldots, l_k)$ so:

$$x = (a_1^{(1)}, \ldots, a_{l_1}^{(1)}) \cdots (a_1^{(k)}, \ldots, a_{l_k}^{(k)}),$$

with each value in $[n]$ corresponding to some $a_j^{(r)}$. For g in S_n:

$$\begin{aligned} gxg^{-1} &= g(a_1^{(1)}, \ldots, a_{l_1}^{(1)})g^{-1}g \cdots g^{-1}g(a_1^{(k)}, \ldots, a_{l_k}^{(k)})g^{-1} \\ &= (g(a_1^{(1)}), \ldots, g(a_{l_1}^{(1)})) \cdots (g(a_1^{(k)}), \ldots, g(a_{l_k}^{(k)})), \end{aligned}$$

with the disjoint property of the cycles preserved as the contrary would contradict the disjoint property of the cycles of x. Thus, all conjugates of x have the same cycle type as x.

For y in S_n with cycle type equal to $(l_1, \ldots, l_k)$:

$$y = (b_1^{(1)}, \ldots, b_{l_1}^{(1)}) \cdots (b_1^{(k)}, \ldots, b_{l_k}^{(k)}),$$

with each value in $[n]$ corresponding to some $b_j^{(r)}$. We define g in S_n by $g(a_i^{(j)}) = b_i^{(j)}$ and see that:

$$gxg^{-1} = y,$$

using the previous result. $\square$

13.6 Parity of Transposition Representations

For x in S_n with $x = t_1 \cdots t_r = s_1 \cdots s_k$ and each t_i, s_i a transposition, $r \equiv k \bmod 2$.

13.7 Signature

For x in S_n with $x = t_1 \cdots t_r$ and each t_i a transposition, the signature of x is defined as:

$$\varepsilon(x) = \begin{cases} 1 & r \equiv 0 \bmod 2 \\ -1 & \text{otherwise.} \end{cases}$$

13.8 The Signature Homomorphism

For n in $\mathbb{N}$, $\varepsilon : S_n \to (\{-1, 1\}, \times)$ is a homomorphism.

Proof. For x, y in S_n with $x = x_1 \cdots x_r$ and $y = y_1 \cdots y_s$ where each x_i and y_j is a transposition:

$$\begin{aligned}\varepsilon(xy) &= \varepsilon(x_1 \cdots x_r y_1 \cdots y_s) \\ &= (-1)^{r+s} \\ &= (-1)^r(-1)^s \\ &= \varepsilon(x)\varepsilon(y).\end{aligned}$$

$\square$

13.9 Alternating Groups

We define the alternating group A_n to be the set of even permutations in S_n. Thus, $A_n \trianglelefteq S_n$.

Proof. $A_n = \operatorname{Ker}(\varepsilon)$. $\square$

13.10 Subgroups of Index 2 in S_n

For $n > 1$, $H \leq S_n$ has index 2 if and only if $H = A_n$.

Proof. ($\Rightarrow$) We know that $H \trianglelefteq S_n$ so we consider S_n/H which must have order 2 as H has index 2. Thus, $S_n/H \cong C_2 \cong (\{-1, 1\}, \times)$ so there's a surjective homomorphism π from S_n to $(\{-1, 1\}, \times)$ with kernel H. For t_1, t_2 transpositions, there exists g such that $t_1 = g^{-1}t_2g$ so:

$$\begin{aligned}\pi(t_1) &= \pi(g)^{-1}\pi(t_2)\pi(g) \\ &= \pi(t_2)\pi(g)^{-1}\pi(g) && ((\{-1,1\}, \times) \text{ is abelian}) \\ &= \pi(t_2),\end{aligned}$$

meaning π takes the same value k on all transpositions. The set of transpositions T generates S_n so $\pi(T)$ generates $(\{-1, 1\}, \times)$ but $\pi(T) = \{k\}$ so $k = -1$. Thus, for $x = x_1 \cdots x_r$ a product of transpositions, $\pi(x) = (-1)^r = \varepsilon(x)$ so $\pi = \varepsilon$. As such, $H = \operatorname{Ker}(\pi) = \operatorname{Ker}(\varepsilon) = A_n$.

($\Leftarrow$) By the homomorphism theorem, $\operatorname{Im}(\varepsilon) \cong S_n/\operatorname{Ker}(\varepsilon) = S_n/A_n$. So, $[S_n : A_n] = |\{-1, 1\}| = 2$. $\square$

13.11 Alternating Groups generated by 3-Cycles

For n in $\mathbb{N}$, A_n is generated by its subset of 3-cycles.

Proof. Each element of A_n is a product of an even number of transpositions, so a product of permutations of the form $(i, j)(k, l)$. It suffices to show that these permutations must be 3-cycles.

Case 1 If $\{i, j\} = \{k, l\}$, as $(i, j) = (j, i)$, $(i, j)(k, l) = e$, a product of zero 3-cycles.

Case 2 If $|\{i, j\} \cap \{k, l\}| = 1$, we take $j = k$ without loss of generality so:

$$\begin{aligned}(i, j)(k, l) &= (i, j)(j, l) \\ &= (i, j, l),\end{aligned}$$

a 3-cycle.

Case 3 If i, j, k, and l are all distinct then:

$$\begin{aligned}(i, j)(k, l) &= (i, j)(j, k)(j, k)(k, l) \\ &= (i, j, k)(j, k, l),\end{aligned}$$

a product of two 3-cycles.

□

14 Group Actions

For a group G and a non-empty set X, an action of G on X is a homomorphism $\varphi : G \to \mathrm{Sym}(X)$. We say that:

- the action is faithful if φ is injective,
- the action is transitive if for all x, y in X, there exists g in G such that $\varphi(g)(x) = y$.

We will abbreviate $\varphi(g)(x)$ to $g \cdot x$.

14.1 The Orbit and Stabiliser

For a group G acting on a set X, for each x in X:

$$\begin{aligned} \mathrm{Orb}_G(x) &= G \cdot x = \{g \cdot x : g \in G\}, \\ \mathrm{Stab}_G(x) &= G_x = \{g \in G : g \cdot x = x\}, \end{aligned}$$

are the orbit and stabiliser of x, respectively.

14.2 The Orbit-Stabiliser Theorem

For a group G acting on a set X with x in X, $\mathrm{Stab}_G(x)$ is a subgroup of G and there is a well-defined bijection φ from $\mathrm{Orb}_G(x)$ to $G/\mathrm{Stab}_G(x)$ defined by:

$$\varphi(g \cdot x) = g\,\mathrm{Stab}_G(x).$$

If G is finite, $|G| = |\mathrm{Orb}_G(x)| \cdot |\mathrm{Stab}_G(x)|$.

Proof. We want to show that $\mathrm{Stab}_G(x) \leq G$. As the action is a homomorphism, $e \cdot x = x$, so e is in $\mathrm{Stab}_G(x)$. For g, h in $\mathrm{Stab}_G(x)$, then:

$$\begin{aligned} (gh) \cdot x &= g \cdot (h \cdot x) && \text{(action is homomorphic)} \\ &= g \cdot (x) \\ &= x. \end{aligned}$$

For g in $\mathrm{Stab}_G(x)$:

$$\begin{aligned} g^{-1} \cdot (g \cdot x) = x &\iff g^{-1} \cdot x = x \\ &\iff g^{-1} \in \mathrm{Stab}_G(x), \end{aligned}$$

so $\mathrm{Stab}_G(x) \leq G$. We know that φ is well-defined and injective as:

$$\begin{aligned}
\big[g \cdot x = h \cdot x\big] &\iff h^{-1} g \cdot x = x \\
&\iff h^{-1} g \in \mathrm{Stab}_G(x) \\
&\iff g \in h \, \mathrm{Stab}_G(x) \\
&\iff g \, \mathrm{Stab}_G(x) = h \, \mathrm{Stab}_G(x).
\end{aligned}$$

As φ is trivially surjective, it is a well-defined bijection as required. $\square$

14.3 Relation via the Orbit

For a group G acting on a set X, we define an equivalence relation on X by $x \sim y$ if y is in $\mathrm{Orb}_G(x)$. The orbits of elements x in G are the equivalence classes of this relation, so they partition X.

Proof. **Reflexivity** For all x in X, we have that $e \cdot x = x$ so $x \sim x$.

Symmetry If $g \cdot x = y$ then $g^{-1} \cdot y = x$.

Transitivity If $x \sim y \sim z$ then there exists g such that $y = g \cdot x$ and h such that $z = h \cdot y$ so $z = (hg) \cdot x$ so $x \sim z$. $\square$

14.4 Fixed Points

For a group G acting on a set X, x in X is a fixed point for this action if $\mathrm{Orb}_G(x) = \{x\}$. We write $\mathrm{Fix}_G(X)$ for the set of fixed points of this action.

For X finite, we write $\mathcal{O}_G(X)$ for the set of orbits of X under this action. For each orbit O in $\mathcal{O}_G(X)$, we pick can arbitrary element $x_O \in O$ and see that:

$$|X| = |\mathrm{Fix}_G(X)| + \sum_{O \in \mathcal{O}_G(X),\, |O|>1} [G : \mathrm{Stab}_G(x_O)].$$

Proof. We have that:

$$\begin{aligned}
|X| &= \sum_{O \in \mathcal{O}_G(X)} |O| && \text{(Relation via the Orbit)} \\
&= |\mathrm{Fix}_G(X)| + \sum_{O \in \mathcal{O}_G(X),\, |O|>1} |O| \\
&= |\mathrm{Fix}_G(X)| + \sum_{O \in \mathcal{O}_G(X),\, |O|>1} [G : \mathrm{Stab}_G(x_O)]. && \text{(Orbit-Stabiliser)}
\end{aligned}$$

$\square$

14.5 The Conjugation Action

For a group G, acting on itself via the conjugacy action ($g \cdot x = gxg^{-1}$), we take x in G. The conjugacy class of x, denoted by x^G, is defined by:

$$x^G = \{gxg^{-1} : g \in G\} = \mathrm{Orb}_G(x).$$

The centraliser of x, denoted by $C_G(x)$, is defined by:

$$C_G(x) = \{g \in G : gxg^{-1} = x\} = \mathrm{Stab}_G(x).$$

For $H \leq G$, the normaliser of H in G, denoted by $N_G(H)$, is defined by:

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

We note that this is the stabiliser of H under the conjugation action of G onto the set of subgroups of G.

14.6 Partitioning on Conjugacy Classes

For a group G, the conjugacy classes of G partition G.

14.7 The Orbit-Stabiliser Theorem for Conjugation

For a group G with x in G, $C_G(x) \leq G$ and there exists a well-defined bijection φ from x^G to $G/C_G(x)$ defined by:

$$\varphi(gxg^{-1}) = gC_G(x).$$

If G is finite, $|G| = |x^G||C_G(x)|$. If we apply this to the conjugation action of G onto the set of its subgroups, we get that:

$$|\{K \leq G : K \text{ is conjugate to } H\}| = [G : N_G(H)].$$

14.8 The Class Equation

For a finite group G, we write $\mathcal{C}$ for the set of conjugacy classes of G, for each conjugacy class C, we can pick an arbitrary element g_C and see that:

$$|G| = |Z(G)| + \sum_{C \in \mathcal{C}(G),\, |C|>1} [G : C_G(g_C)].$$

15 Sylow's Theorems

15.1 Cauchy's Theorem

For a finite group G and a prime p such that p divides $|G|$, G contains an element of order p.

Proof. We first prove the theorem for abelian groups, then for all groups.

Abelian Case Suppose G is abelian. If $|G| = p$, then G is cyclic with a generator of order p. So, we consider $|G| > p$ and proceed by induction on $|G|$. We take g in $G \setminus \{e\}$, if p divides $|g|$, we take $g^{\frac{|g|}{p}}$. Otherwise, by Lagrange's theorem, $|G| = |g| \cdot [G : \langle g\rangle]$ so p divides $[G : \langle g\rangle]$. Thus, $G/\langle g\rangle$ is an abelian group of order strictly less than $|G|$, so by induction, it contains an element of order p, $h\langle g\rangle$. We write $n = |h|$, we have that:

$$(h\langle g\rangle)^n = h^n\langle g\rangle = e\langle g\rangle = \langle g\rangle,$$

so p divides n. Thus, $h^{\frac{n}{p}}$ has order p in G as required. □

We remove our supposition that G is abelian. As before, if $|G| = p$, then G is cyclic with a generator of order p. So, we consider $|G| > p$ and proceed by induction on $|G|$. If p divides $|Z(G)|$, as $Z(G)$ is abelian, we are done. Otherwise, we consider the class equation:

$$|G| = |Z(G)| + \sum_{C \in \mathcal{C}(G),\, |C|>1} [G : C_G(g_C)].$$

As p divides $|G|$ but not $|Z(G)|$, there is some term of the summation that is not divisible by p. Thus, there exists g in G such that $g \in C$ where C is a conjugacy class of size at least 2 and $[G : C_G(g)]$ is not divisible by p. But, Lagrange's theorem implies that $|C_G(g)|$ is divisible by p as:

$$|G| = |C_G(g)|[G : C_G(g)].$$

Since $|C| \geq 2$, g is not central in G, so $C_G(g) \neq G$. By induction, $C_G(g)$ contains an element of order p. Hence, G does. □

15.2 Order of p-groups

For a prime p and a finite group G, G is a p-group if and only if $|G| = p^m$ for some m in $\mathbb{N}$.

Proof. If $|G| = p^m$ for some m in $\mathbb{N}$ then every element has order dividing p^m by Lagrange's theorem. As such, G is a p-group. Conversely, if $|G|$ is divisible by some prime $q \neq p$, then Cauchy's theorem imples that G has an element of order q, which is not a power of p. $\square$

15.3 Sylow's First Theorem

We consider a prime p and a finite group G with $|G| = p^r m$ for some r in $\mathbb{N}_0$ and some m in $\mathbb{N}$ such that p does not divide m. We have that for every k in $\mathbb{N}_0$, there exists a subgroup of G of order p^k if and only if $k \leq r$.

Proof. We note that when $k > r$, p^k cannot divide $p^r m$ as we've defined it so by Lagrange's theorem, there's no subgroup of size p^k. Thus, we consider k in $[r]_0$. The theorem is trivial when $G = \{e\}$, so we assume $|G| > 1$ and proceed by induction on $|G|$.

Case 1 We suppose that p divides $|Z(G)|$. Cauchy's theorem implies that there is a central element x of order p, thus $\langle x \rangle \trianglelefteq G$. We consider $G/\langle x \rangle$ which has size $p^{r-1}m$ so by induction has subgroups of order p^k for k in $[r-1]_0$ denoted by $H_0, \ldots, H_{r-1}$ with each i in $[r-1]_0$ yielding $|H_i| = p^i$.

We take π from G to $G/\langle x \rangle$ to be the quotient homomorphism and note that by the correspondence theorem, for all i in $[r-1]_0$, $\pi^{-1}(H_i) \leq G$ and so:

$$|\pi^{-1}(H_i)| = |\langle x \rangle| \cdot |H_i| = p|H_i| = p^{i+1}.$$

Thus, since we have the trivial subgroup of order 1, we have subgroups of order $1, p, \ldots, p^r$ as required.

Case 2 We suppose that p does not divide $|Z(G)|$. We take $\mathcal{C}$ to be the set of conjugacy classes in G and for each c in $\mathcal{C}$, we pick an element g_C in C and use the class equation:

$$|G| = |Z(G)| + \sum_{C \in \mathcal{C}, |C| \geq 2} [G : C_G(g_C)].$$

Thus, there must be some g not in $Z(G)$ such that $[G : C_G(g)]$ is not divisible by p so:

$$\frac{|G|}{|C_G(g)|},$$

is not divisible by p. However, since $|G|$ is divisible by p^r, $|C_G(g)|$ must be also. As g is not in $Z(G)$, $C_G(g) \neq G$ so $|C_G(g)| < |G|$. By induction, $C_G(g)$ contains subgroups of order $1, p, \ldots, p^r$ which are also subgroups of G. $\square$

15.4 Sylow Subgroups

For a prime p and a group G, a p-subgroup $H \leq G$ is a Sylow p-subgroup if it is not a subgroup of any other p-subgroup of G. We write $\mathrm{Syl}_p(G)$ for the set of these subgroups and $n_p(G)$ for the quantity of them.

15.5 Closure of p-groups under Conjugacy

For a prime p and a group G with $H \leq G$ a p-group, for every g in G, H^g is also a p-group. If H is a Sylow p-group, so is H^g.

Proof. As conjugacy is an automorphism, H^g is another p-group. If H is a Sylow p-subgroup and H^g is not, then H^g must be a proper subgroup of some other p-group $K \leq G$. But, K^g is another p-subgroup and:

$$H = g^{-1}(gHg^{-1})g < g^{-1}Kg,$$

which contradicts the fact that H is a Sylow p-group. $\square$

15.6 Sylow's Second Theorem

For a prime p and a finite group G, the Sylow p-groups of G are all conjugate to each other.

Proof. We write $|G| = p^r m$ with p not dividing m. By Sylow's first theorem, we have that there exists a Sylow p-subgroup $P \leq G$ with $|P| = p^r$. We will show P is conjugate to an arbitrary Sylow p-subgroup H. We take H to act on G/P via $h \cdot gP = (hg)P$ and $\mathcal{O}$ to be the set of orbits of this action. The orbits partition G/P so $m = [G : P] = \sum_{O \in \mathcal{O}} |O|$. But, m is not divisible by p so there must be some orbit O with $|O|$ not divisible by p. The orbit-stabiliser theorem gives us that:

$$|H| = |O| \cdot |\mathrm{Stab}_H(x)|,$$

for some x in G/P, so $|O|$ divides $|H|$. Since H is a p-group, $|O|$ must be a power of p. Thus, $|O| = 1$ and as such, the action of H on G/P has a fixed point, for some g in G and for all h in H:

$$\begin{aligned} HgP = gP &\iff g^{-1}HgP = P \\ &\iff g^{-1}Hg \subseteq P. \end{aligned}$$

By the closure of Sylow p-subgroups under conjugacy and the definition of Sylow p-subgroups, $g^{-1}Hg$ must be equal to P. $\square$

A consequence of this is that the conjugation action of G on the Sylow p-subgroups gives us that $|\operatorname{Orb}_G(P)| = n_p(G)$. So, by the orbit-stabiliser theorem:

$$|\operatorname{Stab}_G(P)| = N_G(P) = \frac{|G|}{n_p(G)}.$$

15.7 Order of Sylow Subgroups

For a prime p and a finite group G with $|G| = p^r m$ where r is in $\mathbb{N}_0$, m is in $\mathbb{N}$, and p doesn't divide m, every Sylow p-subgroup of G has order p^r.

Proof. This is a consequence of Sylow's first and second theorems. $\square$

15.8 The Quantity of Sylow Subgroups

For a finite group G and $P \leq G$ a Sylow p-subgroup, $n_p(G) = [G : N_G(P)]$. In particular, $P \trianglelefteq G$ if and only if P is the unique Sylow p-subgroup of G.

Proof. By Sylow's second theorem:

$$\begin{aligned} n_p(G) &= |\{H \leq G : H \text{ is conjugate to } P\}| \\ &= [G : N_G(P)], \end{aligned}$$

as required. $\square$

15.9 Sylow Subgroups of Abelian Groups

For a finite abelian group G, $n_p(G) = 1$ for all primes p.

Proof. We have that $n_p(G) = [G : N_G(P)] = 1$ as $N_G(P) = G$. $\square$

15.10 Fixed Point of Conjugation on Sylow Subgroups

We consider a finite group G and $P \leq G$ a Sylow p-subgroup with P acting on $\operatorname{Syl}_p(G)$ by conjugation, $g \cdot Q = gQg^{-1}$. We have that $\operatorname{Fix}_p(\operatorname{Syl}_p(G)) = \{P\}$.

Proof. We know that P is in $\operatorname{Fix}_p(\operatorname{Syl}_p(G))$ as $gPg^{-1} = P$ for some g in P. For Q in $\operatorname{Fix}_p(\operatorname{Syl}_p(G))$, by definition, $gQg^{-1} = Q$ for all g in P. Thus, $P \leq N_G(Q)$, $Q \trianglelefteq N_G(Q)$, and $PQ = QP$ so $PQ \leq G$. By (7.1), $|PQ|$ divides $|P||Q|$, but as P and Q are p-groups, they must have an order that is a power of p. Thus, $|PQ|$ is also a power of p so PQ is a p-group. However, $P, Q \leq PQ$ are both Sylow p-subgroups, so $P = PQ = Q$, as required. $\square$

15.11 Sylow's Third Theorem

For a prime p and a finite group G with $|G| = p^r m$ for some where p doesn't divide m, $n_p(G)$ divides m and $n_p(G) \equiv 1 \bmod p$.

Proof. We take P to be a Sylow p-subgroup with P acting on $\mathrm{Syl}_p(G)$ by conjugation. By (14.4), we have that for $\mathcal{O}$ the set of orbits and Q_O in O for each O in $\mathcal{O}$:

$$|\mathrm{Syl}_p(G)| = |\mathrm{Fix}_P(\mathrm{Syl}_p(G))| + \sum_{O \in \mathcal{O}_G(X),\, |O|>1} [P : \mathrm{Stab}_P(Q_O)].$$

If an ordbit has size greater than one, its elements are not fixed. So, none of the stabilisers are equal to P, so each index is greater than 1 and divides $|P|$ (so is a power of p). As such:

$$\begin{aligned} n_p(G) = |\mathrm{Syl}_p(G)| &\equiv |\mathrm{Fix}_P(\mathrm{Syl}_p(G))| \bmod p \\ &\equiv 1 \bmod p, \end{aligned} \tag{15.10}$$

Thus, by (15.8), for a Sylow p-subgroup P:

$$n_p(G) = [G : N_G(P)],$$

so $n_p(G)$ divides $|G|$ and by the above, does not divide p^r. Thus, $n_p(G)$ divides m. ☐

16 Finite Simple Groups

16.1 Classification of Abelian Simple Groups

For an abelian group G, G is simple if and only if $G \cong \mathbb{Z}_p$ for some prime p.

Proof. ($\Rightarrow$) Supposing the antecedent, for some non-identity element x in G, $\langle x \rangle \trianglelefteq G$ so $\langle x \rangle = G$ as G is simple. As such, G is cyclic. If G is infinite, $\langle x^2 \rangle$ is a non-trivial proper normal subgroup of G, a contradiction of the simplicity of G. If $|G|$ is not prime, $|G| = mn$ for some m and n in $\mathbb{N}_{>1}$. Then $\langle x^m \rangle$ is, again, a non-trivial proper normal subgroup of G. As such, G is a finite cyclic group of prime order, so $G \cong \mathbb{Z}_p$ for some prime p.

($\Leftarrow$) By Lagrange's theorem, $\mathbb{Z}_p$ has no non-trivial proper subgroups. □

16.2 Bound on the Order of Centres of Finite p-groups

For a prime p and G a non-trivial finite p-group, $|Z(G)| \geq p$.

Proof. By (15.2), $|G| = p^m$ for some m in $\mathbb{Z}$. For some g in G, if the conjugacy class of g contains more than one element, then $C_G(g) \neq g$ so $[G : C_G(g)] > 1$. By Lagrange's theorem, $[G : C_G(g)]$ must be a multiple of p. Since $|G|$ is also a multiple of p, $|Z(G)|$ must be too. As $Z(G)$ contains the identity, $|Z(G)| \geq p$. □

16.3 Existence of Non-abelian Finite Simple p-groups

There are no non-abelian finite simple p-groups.

Proof. The centre of a finite simple p-group G has size at least p, so for G to be simple, $Z(G) = G$ so G is abelian. □

16.4 Classification of Simple p-groups

For a prime p and a finite simple p-group, G is simple if and only if $G \cong \mathbb{Z}_p$.

Proof. By (16.3), G is abelian. We apply (16.1) and we are done. □

16.5 Bound on the Quantity of Sylow p-subgroups in Non-abelian Finite Simple Groups

For a non-abelian finite simple group G and a prime p dividing $|G|$, $n_p(G) > 1$.

Proof. Sylow's first theorem implies that G has at least one non-trivial Sylow p-subgroup P. By (16.4), there are no non-abelian finite simple p-groups so P is a non-trivial proper subgroup of G. As G is simple, $P \ntrianglelefteq G$ so there exists some conjugation of P not equal to P which would also be a Sylow p-subgroup. Thus, $n_p(G) > 1$. □

16.6 Simple Groups of Order 56

There are no simple groups of order 56.

Proof. We appeal to the contrary and take G to be a simple group of order $56 = 7 \cdot 2^3$. We know that G is not abelian by (16.1). We know that $n_7(G) > 1$ by (16.5) and by Sylow's third theorem, $n_7(G) \equiv 1 \bmod 7$ and $n_7(G)$ divides 8. Thus, $n_7(G)$ must be 8.

By Cauchy's theorem, every Sylow 7-subgroup has size 7, so must be isomorphic to C_7. As these subgroups are distinct, their intersection must be $\{e\}$. This gives us $48 = 7 \cdot 6$ distinct elements of order 7 in G. This leaves 8 elements not of order 7, which must form a Sylow 2-subgroup of order 8 by Sylow's first theorem. This accounts for all 56 elements of G, there can be no other Sylow 2-subgroups, contradicting (16.5). □

16.7 Simple Groups of Order consisting of 2 or 3 Factors

For p, q, r primes, there are no finite simple groups of order pq or pqr.

Proof. We suppose that G is a finite simple group, we note that $|G|$ is pq or pqr, G cannot be abelian by (16.1)

Case 1 We suppose that $|G| = pq$. By (16.4), $p \neq q$. Sylow's third theorem implies that $n_p(G)$ divides q and $n_q(G)$ divides p but this means:

$$n_p(G) \in \{1, q\},$$
$$n_q(G) \in \{1, p\}.$$

But, by (16.5), $n_p(G)$ and $n_q(G)$ must be greater than 1, so $n_p(G) = q$ and $n_q(G) = p$. Again, by Sylow's third theorem, we have that:

$$p \equiv 1 \bmod q,$$
$$q \equiv 1 \bmod p.$$

But, if we suppose that $q < p$, then $q \equiv q \bmod p$ and similarly for $q > p$. This is a contradiction.

Case 2 We suppose that $|G| = pqr$. By (16.4), we have that either $pqr = p^2q$ with p and q distinct (**2a**) or p, q, and r are all distinct (**2b**).

Case 2a Sylow's third theorem implies that:

$$n_p(G) \in \{1, q\},$$
$$n_q(G) \in \{1, p, p^2\},$$

and with (16.5), they both must be greater than 1. If $n_q(G) = p$, we have a contradiction by the reasoning in **Case 1**. Otherwise, $n_q(G) = p^2$. So, we have p^2 distinct subgroups of order q which admit $q - 1$ unique elements of order q. Thus, there are $p^2(q-1) = p^2q - p^2 = |G| - p^2$ elements of order q in G. This leaves p^2 elements not of order q, which must form a unique Sylow p-subgroup. But, we know that $n_p(G) > 1$, so this is a contradiction.

Case 2b We suppose that $p < q < r$ without loss of generality. Sylow's third theorem implies that $n_r(G)$ divides pq and is congruent to 1 mod r combined with (16.5) again, $n_r(G)$ is in $\{p, q, pq\}$. But, as $r > q > p$, $n_r(G)$ must be equal to pq as otherwise:

$$n_r(G) = p \not\equiv 1 \bmod r,$$
$$n_r(G) = q \not\equiv 1 \bmod r.$$

By a similar argument, $n_q(G)$ is in $\{r, pr\}$ and $n_p(G)$ is in $\{q, r, qr\}$. Thus, in G, there are:

$$pq(r-1) \text{ elements of order } r,$$
$$\text{at least } r(q-1) \text{ elements of order } q,$$
$$\text{at least } q(p-1) \text{ elements of order } p.$$

This accounts for:

$$\begin{aligned} pq(r-1) + r(q-1) + q(p-1) &= pqr - pq + rq - r + qp - q \\ &= pqr + (rq - r - q), \end{aligned}$$

elements in G, but this is greater than $pqr = |G|$, a contradiction. □

16.8 Simplicity of the First Alternating Groups

We have that $A_1 = A_2 = \{e\}$, $A_3 \cong C_3$ is simple, and A_4 is not simple.

Proof. We can see that $S_1 = \{e\}$ and $S_2 = \{e, (1,2)\}$, so $A_1 = A_2 = \{e\}$. Also, $A_3 = \{e, (1,2,3), (1,3,2)\} \cong C_3$, and A_4 has a normal subgroup:

$$\{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

□

16.9 Conjugacy of 3-cycles in Alternating Groups

For $n \geq 5$, all the 3-cycles in A_n are conjugate.

Proof. By (13.4), we know that for $i_1, \ldots, i_k$ distinct in $[n]$ and g in S_n:

$$g(i_1, \ldots, i_k)g^{-1} = (g(i_1), \ldots, g(i_k)).$$

For i, j, k arbitrary in $[n]$, we have that if there's some g in A_n such that:

$$g(1) = i, \qquad g(2) = j, \qquad g(3) = k, \tag{$*$}$$

then $g(1,2,3)g^{-1} = (i,j,k)$. Thus, it's sufficient to show such g exists in A_n. We take g_0 to be the element of S_n with property $(*)$. We suppose that g_0 is not in A_n, so is a composition of an odd number of transpositions. As such, $(4,5)g_0$ is in A_n and adheres to the property $(*)$ as required. □

16.10 Simple Alternating Groups

The alternating group A_n is simple for $n = 3$ and $n \geq 5$.

Proof. For $n < 5$, we have (16.8). We suppose $n \geq 5$ and take $N \trianglelefteq A_n$ with $N \neq \{e\}$ and $a \neq e$ in N. We note that it is sufficient to show that N contains a 3-cycle as by (16.9) and the properties of normal subgroups, N would then equal A_n, showing there are no proper normal subgroups. We write a as a product of disjoint cycles $a_1, \ldots, a_t$, assuming each a_i is not a 1-cycle:

$$a = a_1 \cdots a_t. \tag{$*$}$$

For all b in A_n, as a^{-1} is also in N and N is normal, we see that $aba^{-1}b^{-1}$ is in N.

Case 1 We suppose $(*)$ contains an r-cycle with $r \geq 4$, without loss of generality, we set $a_1 = (i_1, \ldots, i_r)$ and then take $b = (i_1, i_2, i_3)$ in A_n. We know that:

$$\begin{aligned} aba^{-1}b^{-1} &= (a(i_1), a(i_2), a(i_3))(i_3, i_2, i_1) \\ &= (i_2, i_3, i_4)(i_3, i_2, i_1) \\ &= (i_2, i_4, i_2), \end{aligned}$$

is a 3-cycle.

Case 2 We suppose $(*)$ contains at least two 3-cycles, (i_1, i_2, i_3) and (i_4, i_5, i_6), we take $b = (i_1, i_2, i_4)$ in A_n. We know that:

$$\begin{aligned} aba^{-1}b^{-1} &= (a(i_1), a(i_2), a(i_4))(i_4, i_2, i_1) \\ &= (i_2, i_3, i_5)(i_4, i_2, i_1) \\ &= (i_1, i_4, i_3, i_5, i_2), \end{aligned}$$

is a 5-cycle. This induces a 3-cycle in N by **Case 1**.

Case 3 We suppose $(*)$ contains exactly one 3-cycle (i_1, i_2, i_3) and at least one transposition (i_4, i_5). We take $b = (i_1, i_2, i_4)$ in A_n. We know that:

$$\begin{aligned} aba^{-1}b^{-1} &= (a(i_1), a(i_2), a(i_4))(i_4, i_2, i_1) \\ &= (i_1, i_4, i_3, i_5, i_2), \end{aligned}$$

inducing a 3-cycle in N by **Case 2**.

Case 4 We suppose that $(*)$ contains only transpositions. As such, t must be even as at least 2, we take (i_1, i_2) and (i_3, i_4) to be two of these transpositions. As $n \geq 5$, there's some i_5 in $[n] \setminus \{i_1, \dots, i_4\}$. We take $b = (i_1, i_3, i_5)$. We know that:

$$\begin{aligned} aba^{-1}b^{-1} &= (a(i_1), a(i_3), a(i_5))(i_5, i_3, i_1) \\ &= (i_2, i_4, a(i_5))(i_5, i_3, i_1) \\ &= \begin{cases} (i_1, i_2, i_4, i_5, i_3) & a(i_5) = i_5 \\ (i_1, i_2, i_6)(i_5, i_3, i_1) & \text{otherwise.} \end{cases} \end{aligned}$$

In the former case, we use **Case 2**. In the latter case, i_6 is in $[n] \setminus \{i_1, \dots, i_5\}$ (as a is formed by disjoint cycles) so we have two disjoint 3-cycles, which we use **Case 2** on. □

16.11 Faithful Non-trivial Actions on Simple Groups

For a simple group G and a non-empty set X with φ from G to $\mathrm{Sym}(X)$ a non-trivial action, φ is faithful and G is isomorphic to a subgroup of $\mathrm{Sym}(X)$.

Proof. We have that $\ker(\varphi) \neq G$ as the action is non-trivial, and as $\ker(\varphi) \trianglelefteq G$ and G is simple, $\ker(\varphi) = \{e\}$. Thus, φ is faithful. The homomorphism theorem implies that $\varphi(G)$ is isomorphic to some subgroup of $\mathrm{Sym}(X)$. □

16.12 Alternating Subgroups of Index n

For $n \geq 5$, if $H \leq A_n$ has index n, then $H \cong A_{n-1}$.

Proof. We take φ from A_n to $\mathrm{Sym}(A_n/H)$ to be the left multiplication action. This action is transitive, so non-trivial and we know that A_n is simple by (16.10) so it must be a faithful action by (16.11). We take ψ from H to $\mathrm{Sym}(A_n/H)$ to be the restriction of φ, noting that H is a fixed point for ψ. We define an action on $X = (A_n/H) \setminus \{H\}$ as ψ' from H to $\mathrm{Sym}(X)$ as the restriction of ψ.

We want to show that ψ' is faithful, we take h in H with $h \neq e$ so $\psi(h)(xH) \neq xH$ for some x in A_n (as ψ is faithful). But, since $\psi(h)(H) = H$ for all h in H, $xH \neq H$. As such, $\psi'(h)(xH) \neq xH$ so ψ' is faithful. But, ψ' acts on X of size $n-1$, so with the homomorphism theorem, we have that $H \cong \psi'(H) \leq \mathrm{Sym}(X) \cong S_{n-1}$. By Lagrange's theorem:

$$\begin{aligned} |A_n| = |H| \cdot [A_n : H] &\iff \frac{n!}{2} = n|H| \\ &\iff |H| = \frac{(n-1)!}{2}, \end{aligned}$$

and the only subgroup of S_{n-1} of index 2 is A_{n-1} by (13.10). □

16.13 Simple Groups of Order 60

All simple groups of order 60 are isomorphic to A_5.

Proof. We take G to be a simple group of order 60. We know that G is not abelian as 60 is not prime (by (16.1)). We then use (16.5) to show that $n_p(G) > 1$ for all primes dividing 60. Sylow's third theorem implies that $n_5(G) \equiv 1 \bmod 5$ and divides 12 so $n_5(G) = 6$. Sylow's second theorem implies that G acts transitively by conjugation on $\mathrm{Syl}_5(G)$ and by (16.11), this action is faithful and G is isomorphic to a subgroup of $\mathrm{Sym}(\mathrm{Syl}_5(G))$. As $n_5(G) = 6$, $\mathrm{Sym}(\mathrm{Syl}_5(G)) \cong S_6$ so G is isomorphic to some subgroup $G' \leq S_6$.

We want to show that $G' \cap A_6 = G'$, we let π from S_6 to S_6/A_6 be the quotient homomorphism. The first isomorphism theorem implies that $\pi(G') \cong G'/(A_6 \cap G')$ but as G' is simple, $G'/(A_6 \cap G')$ must have order 1 or 60. However, S_6/A_6 has order 2, so $|G'/A_6 \cap G'| = 1$. As such, $A_6 \cap G' = G'$. In particular, $G' \leq A_6$. As $|A_6| = 360$ and $|G'| = 60$, it must be that $G' \cong A_5$ by (16.12). □

16.14 The Smallest Non-abelian Finite Simple Group

The smallest non-abelian finite simple group has order 60.

Proof. We take the smallest non-abelian finite simple group to be G. By (16.13), $|G| \leq 60$ as A_5 is a non-abelian finite simple group. By (16.4), $|G|$ can't be a prime power, by (16.6), $|G| \neq 56$, and by (16.7), $|G|$ can't be the product of two or three primes. Thus:

$$|G| \in \{24, 36, 40, 48, 54, 60\}.$$

We reason on a case-by-case basis:

- By Sylow's third theorem and (16.5), if $|G| = 24$ or 48 then $n_2(G) = 3$. However, Sylow's second theorem and (16.11) implies that G is isomorphic to a subgroup of S_3 which is impossible as $|S_3| = 6$,
- By Sylow's third theorem and (16.5), if $|G| = 36$ then $n_3(G) = 4$. However, Sylow's second theorem and (16.11) implies that G is isomorphic to a subgroup of S_4 which is impossible as $|S_4| = 24$,
- By Sylow's third theorem, if $|G| = 40$ then $n_5(G) = 1$, contradicting (16.11),
- By Sylow's third theorem, if $|G| = 54$ then $n_3(G) = 1$, contradicting (16.11).

Thus, $|G| = 60$. $\square$

17 Soluble and Nilpotent Groups

17.1 Normal and Subnormal Series

For a group G, a subnormal series of G is a finite sequence:

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G.$$

If each G_i is such that $G_i \trianglelefteq G$ then this is a normal series. The length of the series is n and we call each G_{i+1}/G_i a factor of the series.

17.2 Soluble Groups

A group is soluble if it has a subnormal series in which every factor is abelian. The length of the shortest such series is the derived length.

17.3 Insolubility of Non-abelian Simple Groups

For a non-abelian simple group G, G is not soluble.

Proof. If we have a subnormal series $G_0, G_1, \dots, G_n$ for G, we take m to be maximal such that $G_m \neq G$ and see that $G_m \trianglelefteq G_{m+1} = G$ so $G_m = \{e\}$ as G is simple. As such, $G/\{e\} \cong G$ is a non-abelian factor of G, contradicting the solubility of G. $\square$

17.4 Derived Series

For a group G, the derived series of G is:

$$G \geq G^{(0)} \geq G^{(1)} \geq \cdots,$$

where for each i in $\mathbb{N}$, we define:

$$\begin{aligned} G^{(0)} &= G, \\ G^{(i)} &= [G^{(i-1)}, G^{(i-1)}]. \end{aligned}$$

We say that $G^{(m)}$ is the m^{th} derived subgroup of G.

17.5 Derived and Subnormal Series

For a group G, G is soluble of derived length at most n if and only if $G^{(n)} = \{e\}$.

Proof. ($\Longrightarrow$) We have $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$ a subnormal series for G with abelian factors. We want to show that $G^{(i)} \leq G_{n-i}$ for each i in $[n]$. This shows that $G^{(n)} \leq G_0 = \{e\}$ and hence $G^{(n)} = \{e\}$ as required. If $i = 0$, then this is true by definition. We proceed by induction with $i > 0$, by our hypothesis, we have that $G^{(i-1)} \leq G_{n-i+1}$. Since G_{n-i+1}/G^{n-i} is abelian by assumption, (10.4) implies that $[G_{n-i+1}, G_{n-i+1}] \subseteq G_{n-i}$ so we have that $G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \leq G_{n-i}$.

($\Longleftarrow$) We know that $G^{(n)} \trianglelefteq G^{(n-1)} \trianglelefteq \cdots \trianglelefteq G^{(0)} = G$ is a subnormal series for G by (10.3) and the factors are abelian by (10.4). Thus, G is soluble of derived length at most n. $\square$

17.6 Derived Groups under Homomorphisms

For G and H groups with a homomorphism φ from G to H, we have that $\varphi(G^{(k)}) = \varphi(G)^{(k)}$ for all k in $\mathbb{Z}_{\geq 0}$.

Proof. We have the $k = 0$ case by definition, we proceed by induction assuming $k > 0$:

$$\begin{aligned}
\varphi(G)^{(k)} &= [\varphi(G)^{(k-1)}, \varphi(G)^{(k-1)}] \\
&= \langle [x, y] : x, y \in \varphi(G)^{(k-1)} \rangle \\
&= \langle [x, y] : x, y \in \varphi(G^{(k-1)}) \rangle && \text{(IH)} \\
&= \langle [\varphi(g), \varphi(h)] : g, h \in G^{(k-1)} \rangle \\
&= \langle \varphi([g, h]) : g, h \in G^{(k-1)} \rangle && (10.1) \\
&= \varphi(\langle [g, h] : g, h \in G^{(k-1)} \rangle) && (2.2) \\
&= \varphi(G^{(k)}),
\end{aligned}$$

as required. $\square$

17.7 Solubility of Subgroups and Quotients

For a soluble group G of derived length at most n, every subgroup and quotient of G is soluble of derived length at most n.

Proof. By (17.5), $G^{(n)} = \{e\}$ so for $H \leq G$ then $H^{(n)} \leq G^{(n)} = \{e\}$ so H is soluble of derived length at most n by (17.5). For $N \trianglelefteq G$ with π from G to G/N the quotient homomorphism, (17.6) implies that:

$$(G/N)^{(n)} = \varphi(G)^{(n)} = \pi(G^{(n)}) = \pi(\{e\}) = N. \qquad (8.4)$$

Thus, by (17.5), G/N is soluble of derived length at most n. $\square$

17.8 Commutator of Symmetric Groups

For n in $\mathbb{N}$, $[S_n, S_n] = A_n$.

Proof. The cases for $n < 3$ are trivial as $A_n = \{e\}$, so we consider $n \geq 3$. We know that $[S_n, S_n] \leq A_n$ as $S_n/A_n \cong C_2$ which is abelian so we can invoke (10.4). Thus, it is sufficient to show that $A_n \leq [S_n, S_n]$. For a 3-cycle (x, y, z), we know that:

$$(x, y, z) = [(x, y), (y, z)] \in [S_n, S_n],$$

and as the 3-cycles generate A_n and (x, y, z) was arbitrary, we are done. $\square$

17.9 Insolubility of Symmetric Groups

For n in $\mathbb{N}$, S_n is soluble if and only if $n \leq 4$.

Proof. As $S_1 \leq S_2 \leq S_3 \leq S_4$, (17.7) shows that the cases for $n \leq 4$ all follow from the case $n = 4$ where:

$$\{e\} \trianglelefteq \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \trianglelefteq A_4 \trianglelefteq S_4,$$

has abelian factors so S_4 is soluble. For $n > 4$, A_n is a non-abelian simple group so by (17.3), it is not soluble. So, by (17.7), S_n is not soluble. $\square$

17.10 Central Series

For a group G, we define a finite series $G = Z_k \geq \cdots \geq Z_0 = \{e\}$ of subgroups of G to be central if for every i in $[k]$, we have that $[G, Z_i] \leq Z_{i-1}$. The length of the series is k.

17.11 Nilpotent Groups

A group that admits a central series is nilpotent. The length of the shortest such series is called the step of G.

17.12 Lower Central Series

For a group G, the lower central series of G is:

$$G_1 \geq G_2 \geq \cdots,$$

where for each i in $\mathbb{N}$, we define:

$$G_1 = G,$$
$$G_{i+1} = [G, G_i].$$

17.13 Lower Central and Central Series

For a group G with a lower central series $G = G_1 \geq G_2 \geq \cdots$, G is nilpotent of step at most s if and only if $G_{s+1} = \{e\}$.

Proof. ($\Longrightarrow$) As G is nilpotent of step at most s, it has a central series:

$$G = Z_s \geq \cdots \geq Z_0 = \{e\}.$$

We want to show that $G_i \leq Z_{s+1-i}$ for all i in $[s]$. This shows that $G_{s+1} = \{e\}$ as required. If $i = 1$, then this is true by definition. We proceed by induction with $i > 0$:

$$\begin{aligned} G_i &= [G, G_{i-1}] \\ &\leq [G, Z_{s+2-i}] \qquad \text{(IH)} \\ &\leq Z_{s+1-i}. \end{aligned}$$

($\Longleftarrow$) We have that:

$$G = G_1 \geq G_2 \geq \cdots \geq G_{s+1} = \{e\},$$

is a central series of length s as for all k in $[s]$, $[G, G_k] = [G, G_{k+1}]$ by definition. $\square$

17.14 The Normaliser Condition

For a nilpotent group G with $H < G$, we have that $H \neq N_G(H)$.

Proof. We take $G = Z_k \geq \cdots \geq Z_0 = \{e\}$ to be a central series for G and set $n = \max(\{m \in [k]_0 : Z_m \leq H\})$. It must be that $n < k$ as $H \neq G$, so we consider some z in Z_{n+1} and h in H. By definition, $h^{-1}z^{-1}hz = [h, z]$ is in Z_n so $z^{-1}hz$ is in hZ_n. But, as $Z_n \leq H$, $hZ_n \subseteq H$. Since h was arbitrary, $z^{-1}Hz = H$ so z is in $N_G(H)$ and thus, as z was arbitrary, $Z_{n+1} \leq N_G(H)$. By the maximality of n, $H \not\leq Z_{n+1} \leq N_G(H)$ so $N_G(H) \neq H$. $\square$