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.

Contents

1 The Fundamentals

1.1 Binary Operations

A binary operation on a set X is a map $X \times X \to X$. For a binary operation $*$ on a set X, we say that $*$ is associative if for all x, y, and 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 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, $D_{2n} = C_n \cup sC_n$.

1.2.2 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. The infinite dihedral group is neither a torsion or a torsion-free group.

1.2.3 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.

1.2.4 Simple Groups

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

1.3 Set Multiplication (1.5)

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 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.

1.5 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 $X < G$).

1.5.1 Centre (1.8)

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.

1.5.2 The Product of Subgroups (1.9)

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

Proof. ($\Longrightarrow$) We can see that $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$.

($\Longleftarrow$) We have that:

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

so $HK \leq G$. □

1.6 The Intersection of Subgroups (1.11)

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

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

Proof. We have that A must be non-empty as each element of $\mathcal{X}$ must contain e. Taking x and y in A, for each X in $\mathcal{X}$ we know that x and y are also 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. Hence, A is a subgroup of G by the subgroup test. □

1.7 The Subgroup Test (1.10)

For a subset X 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. ($\Longrightarrow$) 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.

($\Longleftarrow$) 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. □

1.8 Generated Subgroups (1.12)

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:

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

Key Insights
We show $\Gamma(X)$ is included in the intersection forming $\langle X \rangle$ so $\langle X \rangle \subseteq \Gamma(X)$.

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. □

1.9 Cyclic Groups (1.13-16)

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. For a generator x of a cyclic group G, $|G| = |x|$.

1.10 Order (1.3)

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

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

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:

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

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 $[|x| - 1]_0$ 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:

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

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

1.11 Cosets (1.18)

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:

1. $G = \bigcup_{x \in G} xH$,
2. $xH = yH$ if and only if x is in yH,
3. either $xH = yH$ or $(xH \cap yH) = \varnothing$,
4. $|xH| = |H|$.

Proof. (1) H contains the identity, so this is trivial.

(2) From the former, xe is in $xH = yH$. From the latter, $x = yh$ for some h in H so $xH = yhH = yH$.

(3) For g in $(xH \cap yH) \neq \varnothing$, $gH = xH = yH$ by (2).

(4) The map from H to xH defined by $h \mapsto xh$ is bijective. □

1.11.1 A Bijection from Left to Right Cosets (1.17)

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

1.11.2 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 $[G : H]$.

1.12 Lagrange's Theorem (1.19)

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

Proof. By (1.11), $G = \bigcup_{x \in G} xH$ is the disjoint union of $[G : H]$ left cosets of H, each of order $|H|$. □

1.12.1 Consequences of Lagrange's Theorem (1.20-22)

For a group G:

1. for all x in G, $|x|$ divides $|G|$,
2. if $|G|$ is prime, G is cyclic,
3. for a prime p, and P and Q subgroups of G with order p, $(P \cap Q) = \varnothing$ or $P = Q$.

Proof. (1) $\langle x \rangle \leq G$ of order $|x|$, so $|G| = [G : \langle x \rangle]|x|$.

(2) For all x in G, $|\langle x \rangle|$ must be p or 1. Thus, every non-identity element in G has order p so generates G.

(3) For $g \neq e$ in $(P \cap Q)$, $|g| = p$ so $P = \langle g \rangle = Q$. $\square$

2 Morphisms

2.1 Homomorphisms

For G and H groups, a homomorphism φ from G to H is a map that for all x and y in G satisfies:

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

The image and kernel are defined as:

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

2.1.1 Properties of Homomorphisms (2.2-6)

For G and H groups, and φ from G to H a homomorphism, we have that:

1. $\varphi(e) = e$,
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 $\mathrm{Ker}(\varphi) = \{e\}$,
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, 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 (2.7-8)

For G and H groups, a homomorphism φ from G to H, and $X \subseteq G$, we have that $\varphi(\langle X \rangle) = \langle \varphi(X) \rangle$. Furthermore, for another homomorphism ψ from G to H with X a generating set for G, if $\varphi(x) = \psi(x)$ for each x in X, then $\varphi = \psi$.

Proof. We have that:

$$\begin{aligned}
\varphi(\langle X\rangle) &= \{\varphi(x_1\cdots x_n) : x_1,\cdots,x_n \in (X\cup X^{-1}), n\in\mathbb{N}\}\\
&= \{\varphi(x_1)\cdots\varphi(x_n) : x_1,\cdots,x_n \in (X\cup X^{-1}), n\in\mathbb{N}\} \qquad (2.1.1)\\
&= \{x_1\cdots x_n : x_1,\cdots,x_n \in (\varphi(X)\cup\varphi(X^{-1})), n\in\mathbb{N}\}\\
&= \{x_1\cdots x_n : x_1,\cdots,x_n \in (\varphi(X)\cup\varphi(X)^{-1}), n\in\mathbb{N}\} \qquad (2.1.1)\\
&= \langle\varphi(X)\rangle.
\end{aligned}$$

By (2.1.1), $\varphi(x^{-1}) = \psi(x^{-1})$ for every x in X so $\varphi = \psi$ on all members of $X \cup X^{-1}$. But, as every element of G can be written as a finite product of elements in X, $\varphi = \psi$ in general by (2.1.1). □

2.3 Isomorphisms

An isomorphism is a bijective homomorphism. Groups admitting an isomorphism are isomorphic.

2.4 Conjugation

For a group G containing some x, y, and g, $x^g = g^{-1}xg$ is the conjugation of x by g, similarly defined for sets. Also, x and y are said to be conjugate if there exists some h in G such that $x = y^h$.

2.4.1 Conjugations on Subgroups (2.10)

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

Proof. By (2.5.1), conjugation is an isomorphism. □

2.5 Automorphisms

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

2.5.1 Inner Automorphisms (2.9)

For a group G, we have that φ from 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 any x and y in G, $\varphi(xy) = g^{-1}xyg = g^{-1}xgg^{-1}g = \varphi(x)\varphi(y)$ so φ is a homomorphism. We have that $g^{-1}xg = e$ implies that $x = gg^{-1} = e$ so $\mathrm{Ker}(\varphi) = \{e\}$. 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 Normal, Characteristic, and Quotient Groups

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.

3.1 Properties of Normal Subgroups (2.14-17)

For a group G, the set of normal subgroups on G is closed under set multiplication and intersection. For G and H groups with φ from 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 $K = \{e\}$ in (4), we can see that $\mathrm{Ker}(\varphi) \trianglelefteq G$.

Proof. For P and Q normal subgroups of G, $PQ = QP$ by normality so $PQ \leq G$ by (1.5.2). We know that PQ is normal as for all g in G, $g^{-1}PQg = g^{-1}Pgg^{-1}Qg = HK$ by the normality of P and Q. Then, we know that the intersection of subgroups is a subgroup by (1.6), for a set of normal subgroups of $\mathcal{A} \subseteq \mathcal{P}(G)$ and g in G:

$$\left(\bigcap_{A \in \mathcal{A}} A\right)^g = \bigcap_{A \in \mathcal{A}} A^g = \bigcap_{A \in \mathcal{A}} A,$$

so this intersection is normal.

(1) For $\varphi(x)$ and $\varphi(y)$ in $\varphi(K)$, $\varphi(x)^{-1}\varphi(y) = \varphi(x^{-1}y)$ which is in $\varphi(K)$ as K is a subgroup. The result follows from the subgroup test.

(2) For every g in G, we have that $\varphi(g)^{-1}\varphi(K)\varphi(g) = \varphi(K^g) = \varphi(K)$.

(3) For x and y in $\varphi^{-1}(K)$, $\varphi(x^{-1}y) = \varphi(x)^{-1}\varphi(y)$ is in K so $x^{-1}y$ is in $\varphi^{-1}(K)$. The result follows from the subgroup test.

(4) For g in G, $\varphi(g^{-1}\varphi^{-1}(K)g) = \varphi(g)^{-1}K\varphi(g) = K$ so $g^{-1}\varphi^{-1}(K)g \subseteq \varphi^{-1}(K)$. The result follows from (3.2). $\square$

3.2 A Test for Normal and Characteristic Subgroups (2.12)

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) We suppose that $\varphi(H) \subseteq H$ for each φ in $\mathrm{Aut}(G)$. For φ in $\mathrm{Aut}(G)$, φ^{-1} 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 $H = \varphi(H)$ as required.

(1) We can perform the same argument as (2) as conjugation is an inner automorphism. □

3.3 Normal Subgroups of Index 2 (2.11)

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

Proof. For x in H, $xH = H = Hx$. For x in $G \setminus H$, $xH \neq H$ by (1.11). Thus, xH and H are disjoint cosets of H and as $[G : H] = 2$, $G = H \cup xH$ is a disjoint union. We can apply the same argument to the right coset and deduce that $xH = Hx$ as required. □

3.4 Properties of the Centre (2.13)

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

> **Key Insights**
> We have that $\varphi(Z(G))$ commutes with $\mathrm{Im}(\varphi)$ but this is just G as φ is an isomorphism. Then, we just use (3.2).

Proof. We note that $Z(G) \leq G$ by (1.5.1). For φ in $\mathrm{Aut}(G)$ and z in $Z(G)$, we take some g in G, so $zg = gz$ and thus $\varphi(z)\varphi(g) = \varphi(g)\varphi(z)$ as φ is a homomorphism. Thus, as g was arbitrary and φ is surjective, $\varphi(z)$ must be in $Z(G)$. Since z was arbitrary, $Z(G)$ is a characteristic subgroup by (3.2).

Every subgroup of $Z(G)$ contains only elements that commute with all elements of G, so must be normal. □

3.5 Quotient Groups (2.18)

For a group G with $H \trianglelefteq G$, the quotient of G by H, G/H, is a group under set multiplication and for every a and b in G satisfies $(aH)(bH) = (ab)H$. Furthermore, the map π from G to G/H defined by $g \mapsto gH$ is a surjective homomorphism with kernel H, called the quotient homomorphism.

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

$$\begin{aligned}(aH)(bH) &= aHbH \\ &= (ab)(HH) && (H \trianglelefteq G) \\ &= (ab)H.\end{aligned}$$

Thus, π is a homomorphism, G/H is closed under this operation, eH is the identity, and for g in G, the inverse of gH is $g^{-1}H$. So, G/H is a group under set multiplication. We have that π is trivially surjective and for g in $\mathrm{Ker}(\pi)$, $\varphi(g) = gH = H$ which means that g is in H by (1.11). □

4 The Morphism Theorems

4.1 The Homomorphism Theorem (2.19-21)

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

- every subset of a group is a normal subgroup if and only if it is the kernel of some homomorphism,
- if φ is injective, $G \cong \operatorname{Im}(\varphi)$.

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

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

So, ψ is well-defined and injective. We also have that ψ is trivially surjective and $(\psi \circ \pi)(g) = \psi(gK) = \varphi(g)$. Now, we consider:

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

so ψ is a homomorphism. $\square$

4.2 The First Isomorphism Theorem (2.22)

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

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

> **Key Insights**
> This theorem essentially states that normal subgroups are normal in other subgroups.

Proof. We write $\pi|_H$ for the restriction of π to H and note that:

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

As the kernel of a homomorphism is a normal subgroup in the domain group (3.1), $(H \cap N) \trianglelefteq H$. The Homomorphism Theorem implies that $H/(H \cap N) \cong \pi(H)$. □

4.3 Normal Subgroup Products (2.23)

For a group G with $H \leq G$, $N \trianglelefteq G$, and π from G to G/N the quotient homomorphism, we have that $HN \leq G$ and $\pi(H) = HN/N$.

Proof. We know that $HN \leq G$ if and only if $HN = NH$ by (1.5.2) which is implied by the normality of N. We consider the group:

$$\begin{aligned} HN/N &= \{hnN : h \in H, n \in N\} \\ &= \{hN : h \in H\} \\ &= \pi(H), \end{aligned}$$

as required. □

4.4 The Order of Normal Subgroup Products (2.24)

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:

$$\begin{aligned}
\frac{|HN|}{|N|} &= [HN : N] && \text{(Lagrange's Theorem)} \\
&= |\pi(H)| && (4.3) \\
&= [H : H \cap N] && \text{(First Isomorphism Theorem)} \\
&= \frac{|H|}{|H \cap N|}, && \text{(Lagrange's Theorem)}
\end{aligned}$$

as required. □

4.5 The Second Isomorphism Theorem (2.25)

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

Proof. We take φ from G/N to G/H to be defined by $gN \mapsto gH$. We have that:

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

so φ is well-defined. We have that φ is a homomorphism because:

$$\varphi(aNbN) = \varphi(abN) = abH = aHbH = \varphi(aN)\varphi(bN),$$

and is trivially surjective as:

$$\mathrm{Ker}(\varphi) = \{gN : gH = eH\} = \{gN : g \in H\} = H/N.$$

Thus, $H/N \trianglelefteq G/N$ by (3.1) and $(G/N)/(H/N) \cong G/H$ by the Homomorphism Theorem. □

4.6 The Correspondence Theorem (2.26)

For a group G with $N \trianglelefteq G$, and π from 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 can show the ($\Longleftarrow$) directions by (3.1) applied with π.

(1)(a) We take $H = \pi^{-1}(K)$ and thus by the ($\Longleftarrow$) direction of (2) we have that $H \leq G$ and thus $K = \pi(H) = H/N$.

(1)(b) For this case, it is sufficient to show that given $K \trianglelefteq G/N$, $\pi^{-1}(K) \trianglelefteq G$. But, this is already shown in the ($\Longleftarrow$) direction of (2)(b).

(2) We have that $N \leq H \leq G$ so H is a union of cosets of N so $H = \pi^{-1}(\pi(H))$. We apply (3.1) again with π to get the result. $\square$

5 Commutators

For x and y in a group G, we define the commutator of x and y as $[x, y] = x^{-1}y^{-1}xy$. This can be interpreted as the 'cost' of commuting x and y as $xy = yx[x, y]$.

5.1 Commutators under Homomorphisms

For x and y in a group G with a homomorphism φ from G to H, we have that:

$$\varphi([x, y]) = [\varphi(x), \varphi(y)].$$

Proof. Trivial from the definitions. □

5.2 Commutator Subgroups

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

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

The subgroup $[G, G]$ is the commutator subgroup of G. If G is abelian, $[G, G] = \{e\}$.

5.3 Commutator of Normal Subgroups (2.32)

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

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

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

Hence, $[h, k]$ is in $(H \cap K)$. □

5.4 Commutators of Characteristic Subgroups (2.27)

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

Proof. For φ in $\mathrm{Aut}(G)$:

$$\begin{aligned}
\varphi([H, K]) &= \varphi(\langle [h, k] : h \in H, k \in K \rangle) \\
&= \langle \varphi([h, k]) : h \in H, k \in K \rangle && (2.2) \\
&= \langle [\varphi(h), \varphi(k)] : h \in H, k \in K \rangle && (5.1) \\
&= \langle [h, k] : h \in H, k \in K \rangle && (H \text{ and } K \underset{\text{char}}{\trianglelefteq} G) \\
&= [H, K],
\end{aligned}$$

as required. □

5.5 Abelian Quotients (2.28)

For a group G with $H \trianglelefteq G$, G/H is abelian if and only if $[G, G] \leq H$. Furthermore, a quotient of G is abelian if and only if it is isomorphic to $G/[G, G]$.

Proof. We take π from G to G/H to be the quotient homomorphism.

($\Longrightarrow$) We take x and y in G, we have that $\pi([x, y]) = [\pi(x), \pi(y)] = eH$, thus $[x, y]$ is in H. Thus, as x and y are arbitary, $[G, G] \subseteq H$.

($\Longleftarrow$) For every xH and 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. So, G/H is abelian if and only if $[G, G] \leq H$ which is true if and only if G/H is isomorphic to a quotient to $G/[G, G]$ as this implies:

$$(G/[G, G])/(H/[G, G]) \cong G/H,$$

by the Second Isomorphism Theorem. □

5.5.1 Quotients of Abelian Groups (2.29)

Every quotient of an abelian group is abelian.

Proof. If G is abelian then $[G, G] = \{e\}$. So, for each $H \underset{\text{char}}{\trianglelefteq} G$ we have $[G, G] \leq H$ and so G/H is abelian by (5.5). □

5.6 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.

6 Direct Products

6.1 Outer Direct Product

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

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

this is a group under component-wise group operations.

6.1.1 Properties of the Outer Direct Product (1.23)

For groups $G_1, \dots, G_n$, 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 $H_1, \dots, H_n$ groups with $G_i \cong H_i$ for each i in $[n]$ $G \cong \prod_{i \in [n]} H_i$.

6.2 Inner Direct Product

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

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

6.3 Component Groups (2.30)

For $G = G_1 \times \cdots \times G_n$ an outer direct product, 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 $\widehat{G_i}$ so, $\widehat{G_i} \trianglelefteq G$ by (3.1).

(2) We can see that:

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

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

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

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

Furthermore, taking i in $[n]$ and $G' = \widehat{G_1} \cdots \widehat{G_{i-1}} \widehat{G_{i+1}} \cdots G_n$, we have that $(\widehat{G_i} \cap G') = \{e\}$ as the elements of G' 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. This is sufficient to prove the result as i was chosen arbitrarily. □

6.4 Commuting Normal Elements of Inner Direct Products (2.33)

For a group G with $H_1, \ldots, H_k \trianglelefteq G$ such that $G = H_1 \cdots H_k$ is an inner direct product, and i and j in $[k]$ whenever $i \neq j$, the elements of H_i commute with the elements of H_j.

Proof. As G is an inner direct product, $(H_i \cap H_j) = \{e\}$. Thus, $[H_i, H_j] = \{e\}$ by (5.3). □

6.5 Isomorphism between Products (2.31)

For a group G such that it is the inner direct product of subgroups $H_1, \dots, H_n$ of G, $G \cong H_1 \times \cdots \times H_n = H$.

Proof. We define φ from H to G by:

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

which is a homomorphism by (6.4) and is surjective as $G = H_1 \cdots H_n$. Taking $(h_1, \dots, h_n)$ in $\mathrm{Ker}(\varphi)$ and some i in $[n]$:

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

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

6.6 Criteria for Inner Direct Products

6.6.1 By Unique Compositions (2.34)

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

Proof. ($\Longrightarrow$) We have $g = \prod_{i \in [n]} h_i$ for some h_i in each H_i by the definition of the inner direct product, so it suffices to show this product is unique. We suppose that:

$$g = \prod_{i \in [n]} k_i = \prod_{i \in [n]} h_i,$$

for some k_i and h_i in each H_i. For i in $[n]$, it must be that $k_i = h_i$ as:

$$\begin{aligned} e &= g^{-1} g \\ &= h_n^{-1} \cdots h_1^{-1} k_1 \cdots k_n \\ &= h_1^{-1} k_1 \cdots h_n^{-1} k_n && (6.4) \\ &= h_i^{-1} k_i h_1^{-1} k_1 \cdots h_{i-1}^{-1} k_{i-1} h_{i+1}^{-1} k_{i+1} \cdots h_n^{-1} k_n, && (6.4) \\ k_i^{-1} h_i &= h_1^{-1} k_1 \cdots h_{i-1}^{-1} k_{i-1} h_{i+1}^{-1} k_{i+1} \cdots h_n^{-1} k_n \\ &\in H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_n) = \{e\}. \end{aligned}$$

($\Longleftarrow$) We trivially have $G = H_1 \cdots H_n$, so it suffices to show that for each i in $[n]$:

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

Taking i in $[n]$ and x in $\mathcal{H}_i$, we have that:

$$h_i = x = h_1 \cdots h_{i-1} h_{i+1} \cdots h_n,$$

for some h_i in each H_i. But by the uniqueness of the composition of x, this means that $x = e$ as required. $\square$

6.6.2 By the Size (2.35)

For a finite group G with $H_1, \ldots, H_n \trianglelefteq G$ such that $G = H_1 \cdots H_n$. G is an inner direct product if and only if $|G| = \prod_{i \in [n]} |H_i|$.

Proof. ($\Longrightarrow$) Follows trivially from the definitions.

($\Longleftarrow$) As $|G| = \prod_i |H_i|$, each product of elements $h_1 \cdots h_n$ in $H_1 \cdots H_n$ is distinct. By (6.6.1), G is an inner direct product. $\square$

7 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 $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$.

7.1 Classification of Cyclic Groups (3.1)

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

Proof. For a generator of G, x, We take φ from $\mathbb{Z}$ to G to be defined by $\varphi(m) = x^m$. Trivially, 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. □

7.2 Torsion Subgroup and p-components (3.3)

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. We have that 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 also a power of p so $(x - y)$ is in G_p. Again, by the subgroup test, G_p is a subgroup of T.

If we suppose that for some z in G, $z + T$ has finite order, there must exist some m in $\mathbb{N}$ with $mx + T = T$, so mx is in T. By the definition of T, there exists some n in $\mathbb{N}$ with $nmx = 0$. This means x has finite order so is in T. Thus, G/T is torsion-free. □

7.3 The Primary Decomposition Theorem (3.4)

For a finite abelian group G, we take $p_1, \dots, p_k$ 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, $|x|$ divides $|G|$ so $|x| = p_1^{l_1} \cdots p_k^{l_k}$ for some $l_1, \dots, l_k$ 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}. It must be that $\gcd(n_1, \dots, n_k) = 1$ as they are powers of distinct primes, so by the Euclidean Algorithm there exists $m_1, \dots, m_k$ 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, $G = G_{p_1} + \cdots + G_{p_k}$. Now, for each i in $[k]$, we consider x_i and x_i' in G_{p_i} such that $\sum_{i \in [k]} x_i = \sum_{i \in [k]} x_i'$. We write $y_i = x_i - x_i'$ so that $\sum_{i \in [k]} y_i = 0$, take d_i such that $|y_i| = p_i^{d_i}$, 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 and b in $\mathbb{Z}$ such that:

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

so $x_i = x_i'$ for each i in $[k]$. Thus, the composition of each element of G in our sum is unique, implying G is the direct sum of $G_{p_1}, \dots, G_{p_k}$ by (6.6.1). □

7.4 Order of Finitely Generated Abelian Torsion Groups (3.5)

A finitely generated torsion group is finite.

Proof. For $x_1, \ldots, x_n$ the finite generating set of an abelian torsion group G:

$$G = \{k_1 x_1 + \cdots + k_n x_n : 0 \leq k_i < |x_i|\},$$

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

7.5 Order of Powers of Elements in p-groups (3.6)

For a prime p and a p-group G, we take g in G and set k in $\mathbb{N}$ to np^r with n and 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 $\mathbb{N}$:

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

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

7.6 Elements with Coset of Maximal Cyclic Subgroup Order (3.7)

For some prime p and a finite abelian p-group G, we take g in G to have maximum order. For every x in G, there exists y in $x + \langle g \rangle$ such 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 $p^m x$ is in $\langle g \rangle$ so $p^m x = kg$ for some k in $\mathbb{N}_0$. We write $k = np^r$ with n and p coprime. If $p^r = 0$ or $p^r > |g|$ then $kg = 0$ so $|x| = p^m = |x + \langle g \rangle|$. Otherwise, by (7.5), $|kg| = \frac{|g|}{p^r}$ and $|p^m x| = \frac{|x|}{p^m}$ as p^m is minimal so $p^m \leq |x|$. Thus, $\frac{|g|}{p^r} = \frac{|x|}{p^m}$ as $p^m x = kg$. The maximality of g implies that $|g| \geq |x|$ so $r \geq m$ and thus p^m divides k. We define:

$$y = x - \frac{k}{p^m} g.$$

Hence, $p^m y = p^m x - kg = 0$ so $|y|$ divides p^m. But, as y is in $x + \langle g \rangle$, (2.1.1) applied to the quotient homomorphism from G to $G/\langle g \rangle$ implies that p^m divides $|y|$ so $|y| = p^m$ as required. $\square$

7.7 Decomposition of Finite Abelian p-groups (3.8)

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 the 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 can be written in 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:

$$G/\langle g \rangle = \langle x_1 + \langle g \rangle \rangle \oplus \cdots \oplus \langle x_k + \langle g \rangle \rangle. \tag{$\bullet$}$$

By (7.6), 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:

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

We want to show that $G = \langle x_1 \rangle + \cdots + \langle x_k \rangle + \langle g \rangle$ and 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 $(\bullet)$ we know that:

$$\begin{aligned} h + \langle g \rangle = (l_1 x_1 + \cdots + l_k x_k) + \langle g \rangle &\implies h \in (l_1 x_1 + \cdots + l_k x_k) + \langle g \rangle \qquad (1.11) \\ &\implies h = l_1 x_1 + \cdots + l_k x_k + ng. \end{aligned}$$

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 by (6.6.2). □

7.8 Homomorphism from $\mathbb{Z}^n$ to Group Subsets (3.10)

For n in $\mathbb{N}$ and an abelian group G, for 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 by (2.2). □

7.9 One-way Inverses on Homomorphisms to $\mathbb{Z}^n$ (3.11)

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. By (7.8), we know 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 completely defines $(\alpha \circ \beta)$ by (2.2). Thus, $(\alpha \circ \beta) = \iota_{\mathbb{Z}^n}$. We can see that:

$$\begin{aligned} \mathrm{Ker}(\beta) &\subseteq \mathrm{Ker}(\alpha \circ \beta) && (2.1.1) \\ &= \mathrm{Ker}(\iota_{\mathbb{Z}^n}) \\ &= \{0\}. \end{aligned}$$

Thus, $\mathrm{Ker}(\beta) = \{0\}$ so β is injective as required. □

7.10 Abelian Groups with $\mathbb{Z}^n$ Quotients (3.9)

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 take π from G to G/H to be the quotient homomorphism and ψ from G/H to $\mathbb{Z}^n$ to be an isomorphism. We set $\alpha = (\psi \circ \pi)$ which is a surjective homomorphism from G to $\mathbb{Z}^n$. By (7.9), we have β from $\mathbb{Z}^n$ to G an injective homomorphism with $(\alpha \circ \beta) = \iota_{\mathbb{Z}^n}$. We note that $H = \mathrm{Ker}(\alpha) \leq G$ and set $K = \beta(\mathbb{Z}^n) \leq G$. As β is injective, $K \cong \mathbb{Z}^n$. For some 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 $\mathrm{Ker}(\alpha) = H$ so g is in $(\beta \circ \alpha)(g) + H$. In particular, g is in $K + H = H + K$. As $(\alpha \circ \beta) = \iota_{\mathbb{Z}^n}$, $(\mathrm{Ker}(\alpha) \cap \beta(\mathbb{Z}^n)) = \{0\}$ which means $(H \cap K) = \{0\}$. Thus, $G = H \oplus K$ as required. □

7.11 $\mathbb{Z}^n$ Subgroups of Finitely Generated Groups (3.12)

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 (7.10). 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. $\square$

7.12 Fundamental Theorem of Finitely Generated Torsion-free Abelian Groups (3.13)

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 proceed by induction, 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 π from G to G/H. We know that G/H is torsion-free as:

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

Thus, 0 is the only element of finite order in G/H as π is surjective. Clearly g_n is in H, so G/H is generated by $\{\pi(g_1), \ldots, \pi(g_{n-1})\}$. By induction, $G/H \cong \mathbb{Z}^k$ for some $k < n$. By (7.10), $G \cong H \oplus \mathbb{Z}^k$ so it's sufficient to show that $H \cong \{0\}$ or $\mathbb{Z}$.

We consider $H/\langle g_n \rangle$ which is finitely generated by (2.2) and a torsion group as for all h in H, there's some l such that $lh + \langle g_n \rangle = \langle g_n \rangle$. By (7.4), $H/\langle g_n \rangle$ is finite, we write m for its order. Thus, for all h in H, $mh + \langle g_n \rangle = \langle g_n \rangle$ as $|h|$ must divide m by Lagrange's Theorem so mh is in $\langle g_n \rangle$. We define φ from H to $\langle g_n \rangle$ by $\varphi(h) = mh$ which is an injective homomorphism as $H \leq G$ is torsion-free so $mh = 0$ implies that $h = 0$. Hence, $H \cong \varphi(H) \leq \langle g_n \rangle$, so H is cyclic. Thus, $H \cong \mathbb{Z}$ because H has infinite order and is cyclic. $\square$

7.13 Fundamental Theorem of Finitely Generated Abelian Groups (3.2)

For a finitely generated abelian group G, 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 by (2.2), and $G/T \cong \mathbb{Z}^n$ for some n by (7.12). Then, 7.10 gives us that $G \cong T \oplus \mathbb{Z}^n$ and (7.4 and 7.11) imply that T is finite. By (7.3), there are finitely many primes $p_1, \ldots, p_m$ such that $G_{p_i} \neq \{0\}$, each G_{p_i} is finite, and $T = G_{p_1} \oplus \cdots \oplus G_{p_m}$. Then, (7.7) and $G \cong T \oplus \mathbb{Z}^n$ gives us that $G_{p_i} = \mathbb{Z}_{p_i^{m_1}} \oplus \cdots \oplus \mathbb{Z}_{p_i^{m_d}}$ for each i in $[m]$, leading to the result. $\square$

8 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 which is 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 and Y of size n. For $n = 1$, there's only one bijection from X to Y. For $n > 1$, some x_0 in X and y_0 in Y:

$$\begin{aligned}
|\{\text{bijections from } X \text{ to } Y\}| &= \sum_{y \in Y} |\{\text{bijections from } X \text{ to } Y : x_0 \mapsto y\}| \\
&= \sum_{y \in Y} |\{\text{bijections from } X \setminus \{x_0\} \text{ to } Y \setminus \{y_0\}\}| \\
&= \sum_{y \in Y} (n-1)! \\
&= n \cdot (n-1)! \\
&= n!,
\end{aligned}$$

proving the result by induction. □

8.1 Cycles

For k in $\mathbb{N}$, a permutation f in S_n is called k-cycle if there are k distinct $i_1, \ldots, i_k$ 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.

8.2 Permutations as Disjoint Cycles (4.1)

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 $(1,i)(1,j)(1,i)=(i,j)$.

8.3 Cycle Type (4.2)

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 $|f| = \operatorname{lcm}(l_1,\dots,l_k)$.

8.4 Conjugacy in S_n (4.4)

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 $k=2$ we take (i,j) in S_n and r in $[n]$, then:

$$(g(i,j)g^{-1})(r) = \begin{cases} r & \text{if } g^{-1}(r)\notin\{i,j\} \\ g(i) & \text{if } g^{-1}(r)=j \\ g(j) & \text{if } g^{-1}(r)=i. \end{cases}$$

Thus, $g(i_1,i_2)g^{-1}=(g(i_1),g(i_2))$. For $k>2$, $(i_1,\dots,i_k)=(i_1,i_2)(i_2,i_3)\cdots(i_{k-1},i_k)$ 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. □

8.5 Conjugacy and Cycle Type (4.3)

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

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

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

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

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

these are still disjoint cycles creating an element of cycle type $(l_1, \dots, l_k)$ so, all conjugates of x have the same cycle type as x. For any y in S_n with cycle type equal to $(l_1, \dots, l_k)$:

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

with each value in $[n]$ corresponding uniquely to some $b_j^{(r)}$. We define g in S_n by $g\big(a_i^{(j)}\big) = b_i^{(j)}$ and see that $gxg^{-1} = y$ by $(*)$. $\square$

8.6 Parity of Transposition Representations (4.5)

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

8.7 Signature (4.6)

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:

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

We have that ε is a homomorphism from S_n to $(\{-1, 1\}, \times)$.

Proof. For x and 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:

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

as required. $\square$

8.8 Alternating Groups (4.7)

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

Proof. The result follows from (3.1) and $A_n = \operatorname{Ker}(\varepsilon)$. $\square$

8.9 Subgroups of Index 2 in S_n (4.8)

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

Proof. ($\Longrightarrow$) We know that $H \trianglelefteq S_n$ by (3.3) so we consider S_n/H which must be isomorphic to C_2 and thus $(\{-1, 1\}, \times)$ by (1.12.1). Hence, there is a surjective homomorphism π from S_n to $(\{-1, 1\}, \times)$ with kernel H. For t_1 and t_2 transpositions, there exists g such that $t_1 = g^{-1}t_2g$ by (8.5) 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, $H = \operatorname{Ker}(\pi) = \operatorname{Ker}(\varepsilon) = A_n$.

($\Longleftarrow$) By the Homomorphism Theorem, $\operatorname{Im}(\varepsilon) \cong S_n/\operatorname{Ker}(\varepsilon) = S_n/A_n$. Thus, $[S_n : A_n] = 2$. $\square$

8.10 Generating Alternating Groups by 3-Cycles (4.9)

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:

$$(i, j)(k, l) = (i, j)(j, l) = (i, j, l),$$

a 3-cycle.

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

$$(i, j)(k, l) = (i, j)(j, k)(j, k)(k, l) = (i, j, k)(j, k, l),$$

a product of two 3-cycles. $\square$

9 Group Actions

For a group G and a non-empty set X, an action of G on X is a homomorphism φ from 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 $\varphi(g)(x) = y$.

9.1 The Orbit and Stabiliser

For an action φ on a group G and a set X, for each x in X:

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

are the orbit and stabiliser of x, respectively.

9.2 The Orbit-Stabiliser Theorem (5.1)

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

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

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 φ is a homomorphism, $\varphi(e) = e$, so e is in $\mathrm{Stab}_G(x)$. For g and h in $\mathrm{Stab}_G(x)$:

$$\begin{aligned}\varphi(gh)(x) &= (\varphi(g) \circ \varphi(h))(x)\\ &= \varphi(g)(x)\\ &= x,\end{aligned}$$

so $\mathrm{Stab}_G(x)$ is closed. For inverses, we see that:

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

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

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

As ψ is trivially surjective, it is a bijection as required. $\square$

9.3 Relation via the Orbit (5.2)

For an action φ on a group G and 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. We consider the conditions for equivalence relations:

Reflexivity For all x in X, we have that $\varphi(e)(x) = x$ so $x \sim x$.

Symmetry If $\varphi(g)(x) = y$ then $\varphi(g^{-1})(y) = x$.

Transitivity If $x \sim y \sim z$ then there exists g such that $y = \varphi(g)(x)$ and h such that $z = \varphi(h)(y)$. Thus, $z = \varphi(hg)(x)$ so $x \sim z$. □

9.4 Fixed Points (5.3)

For an action φ on a group G and a set X, x in X is a fixed point for φ if $\mathrm{Orb}_G(x) = \{x\}$. We write $\mathrm{Fix}_G(X)$ for the set of fixed points of φ. We write $\mathcal{O}_G(X)$ for the set of orbits of X under φ. For each orbit O in $\mathcal{O}_G(X)$, we pick can arbitrary element $x_O \in O$ and see that for X finite:

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

Proof. We first note that the fixed points of φ are just the singleton orbits in $\mathcal{O}_G(X)$. Thus:

$$\begin{aligned}\mathcal{O}_G(X) &= \mathrm{Fix}_G(X) \cup \{O \in \mathcal{O}_G(X) : |O| > 1\} \\ &= \mathrm{Fix}_G(X) \cup \mathcal{O}_G^{(1)}(X),\end{aligned}$$

is a disjoint union. We have that:

$$\begin{aligned}|X| &= \sum_{O \in \mathcal{O}_G(X)} |O| && (9.3) \\ &= |\mathrm{Fix}_G(X)| + \sum_{O \in \mathcal{O}_G^{(1)}(X)} |O| \\ &= |\mathrm{Fix}_G(X)| + \sum_{O \in \mathcal{O}_G^{(1)}(X)} |G/\mathrm{Stab}_G(x_O)| && (9.2) \\ &= |\mathrm{Fix}_G(X)| + \sum_{O \in \mathcal{O}_G^{(1)}(X)} [G : \mathrm{Stab}_G(x_O)].\end{aligned}$$

□

9.5 The Conjugation Action

For a group G acting on itself via conjugacy ($\varphi(g)(x) = gxg^{-1}$), where φ is this action and x in G, the conjugacy class of x, denoted by x^G, is defined by:

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

The centraliser of x is defined by:

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

For $H \leq G$, the normaliser of H in G is defined by:

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

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

9.6 Partitioning on Conjugacy Classes (5.4)

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

Proof. The conjugacy classes are the orbits of this action leading to the result by (9.3). □

9.7 The Orbit-Stabiliser Theorem for Conjugation (5.5)

For a group G with x in G where we take φ to be the conjugacy action on G, we have that $\mathrm{Stab}_G(x) = C_G(x) \leq G$ and there exists a well-defined bijection ψ from $\mathrm{Orb}_G(x) = x^G$ to $G/C_G(x)$ defined by:

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

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

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

Proof. This follows directly from (9.2). □

9.8 The Class Equation (5.6)

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:

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

Proof. This follows directly from (9.4) as for g in G and z in $Z(G)$, $g^{-1}zg = z$. □

10 Sylow's Theorems

10.1 Cauchy's Theorem (6.1-2)

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 $g^{\frac{|g|}{p}}$ and we are done. Otherwise, by Lagrange's theorem, $|G| = |g| \cdot [G : \langle g\rangle]$ so p divides $[G : \langle g\rangle]$. We have that $G/\langle g\rangle$ is an abelian group by (5.5.1) and has 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.

General Case 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 by the first case. 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. We have that 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. □

10.2 Order of p-groups (6.3)

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 implies that G has an element of order q, which is not a power of p. $\square$

10.3 Sylow's First Theorem (6.4)

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 $p^r m$ 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, so $\langle x \rangle \trianglelefteq Z(G) \underset{\text{char}}{\trianglelefteq} G$ (by (3.4)). 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. $\square$

10.4 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.

10.5 Closure of p-groups under Conjugacy (6.5)

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 $K \leq G$. However, K^g should be another p-subgroup but:

$$H = g^{-1}(gHg^{-1})g < g^{-1}Kg, \tag{2.5.1}$$

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

10.6 Sylow's Second Theorem (6.6)

For a prime p and a finite group G, the Sylow p-groups of G are all conjugate to each other. Thus, the conjugation action of G on the Sylow p-subgroups gives us that $|\mathrm{Orb}_G(P)| = n_p(G)$. So, by the Orbit-Stabiliser Theorem:

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

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 by $\varphi(h)(gP) = (hg)P$ and $\mathcal{O}$ to be the set of orbits of this action. By (9.3), the orbits partition G/P so $m = |G/P| = [G : P] = \sum_{O \in \mathcal{O}} |O|$. But, m cannot be 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 (10.5), $g^{-1}Hg = P$. $\square$

10.7 Order of Sylow Subgroups (6.7)

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 direct from Sylow's First and Second Theorem. □

10.8 The Quantity of Sylow Subgroups (6.8)

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:

$$\begin{aligned} n_p(G) &= |\{H \leq G : H \text{ is conjugate to } P\}| \\ &= [G : N_G(P)]. \end{aligned} \tag{9.7}$$

If $n_p(G) = 1$, then $P^g = P$ for all g in G by Sylow's Second Theorem. □

10.9 Sylow Subgroups of Abelian Groups (6.9)

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

Proof. As G is abelian, $N_G(P) = G$ so we have that $n_p(G) = [G : N_G(P)] = 1$. □

10.10 Fixed Point of Conjugation on Sylow Subgroups (6.11)

For a finite group G and a Sylow p-subgroup P where P acts on $\mathrm{Syl}_p(G)$ by conjugation via φ, we have that $\mathrm{Fix}_P(\mathrm{Syl}_p(G)) = \{P\}$.

Proof. We know that P is in $\mathrm{Fix}_P(\mathrm{Syl}_p(G))$ as $gPg^{-1} = P$ for any g in P. For Q in $\mathrm{Fix}_P(\mathrm{Syl}_p(G))$, by definition, $gQg^{-1} = Q$ for all g in P so, $P \subseteq N_G(Q)$. As we know $Q \trianglelefteq N_G(Q)$, (4.3) shows that $PQ \leq G$, and by (4.4), $|PQ|$ 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, since P and Q are both Sylow p-subgroups in PQ, $P = PQ = Q$, as required. □

10.11 Sylow's Third Theorem (6.10)

For a prime p and a finite group G with $|G| = p^r m$ for some prime p that 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 Lagrange's Theorem, p divides $[P : \mathrm{Stab}_P(Q)]$ for every Q in $\mathrm{Syl}_p(G)$ that is not in $\mathrm{Fix}_P(G)$. So, we have that:

$$\begin{aligned} n_p(G) &\equiv |\mathrm{Fix}_P(\mathrm{Syl}_p(G))| \bmod p && (9.4) \\ &\equiv 1. && (10.10) \end{aligned}$$

By (10.8) and Lagrange's Theorem, $n_p(G)$ must divide $|G|$ and as $n_p(G) \equiv 1 \bmod p$, $n_p(G)$ is not divisible by p. Thus, $n_p(G)$ divides m. $\square$

11 Finite Simple Groups

11.1 Classification of Abelian Simple Groups (7.2)

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

Proof. ($\Longrightarrow$) 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.

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

11.2 Bound on the Order of Centres of Finite p-groups (7.3)

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

Proof. By (10.2), $|G| = p^m$ 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, $|Z(G)| \geq p$. □

11.3 Existence of Non-abelian Finite Simple p-groups (7.4)

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

Proof. The centre of a finite simple p-group G has size at least p by (11.2), so for G to be simple, $Z(G) = G$ so G is abelian. □

11.4 Classification of Simple p-groups (7.5)

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

Proof. By (11.3), G is abelian. By (11.1), we have the result. □

11.5 Bound on the Quantity of Sylow p-subgroups in Non-abelian Finite Simple Groups (7.6)

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 (11.4), 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, $n_p(G) > 1$. □

11.6 Simple Groups of Order 56 (7.7)

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 (11.1). We know that $n_7(G) > 1$ by (11.5) 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 (11.5). □

11.7 Simple Groups of Order consisting of 2 or 3 Factors (7.8)

For p, q, and 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 (11.1)

Case 1 We suppose that $|G| = pq$. By (11.4), $p \neq q$. 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 (11.5), $n_p(G)$ 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 (11.4), 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:

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

and with (11.5), they both must be greater than 1. If $n_q(G) = p$, we have a contradiction by the reasoning in **Case 1**. So, it must be that $n_q(G) = p^2$. Hence, 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 (11.5), so $n_r(G)$ is in $\{p, q, pq\}$. But, as $r > q > p$, $n_r(G)$ must be equal to pq as otherwise:

$$\begin{aligned} n_r(G) &= p \not\equiv 1 \bmod r, \\ n_r(G) &= q \not\equiv 1 \bmod r. \end{aligned}$$

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:

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

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. $\square$

11.8 Simplicity of the First Alternating Groups (7.10)

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:

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

as required. □

11.9 Conjugacy of 3-cycles in Alternating Groups (7.11)

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

Proof. By (8.4), for i, j, and 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. □

11.10 Simple Alternating Groups (7.9)

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

Proof. For $n < 5$, we have (11.8). 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 definition, it would then contain every conjugate of that 3-cycle so with (11.9 N would equal A_n, showing there are no proper non-trivial normal subgroups of A_n. 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 have that $aba^{-1}b^{-1}$ is also 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 $[n] \setminus \{i_1, \ldots, i_4\}$. 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 $[n] \setminus \{i_1, \ldots, i_5\}$ (as a is formed by disjoint cycles) so we have two disjoint 3-cycles, which we use **Case 2** on. □

11.11 Faithful Non-trivial Actions on Simple Groups (7.13)

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

11.12 Alternating Subgroups of Index n (7.12)

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 (11.10) so it must be a faithful action by (11.11). 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 (8.9). $\square$

11.13 Simple Groups of Order 60 (7.14)

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 (11.1)). We then use (11.5) 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 (11.11), 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 (11.12). $\square$

11.14 The Smallest Non-abelian Finite Simple Group (7.15)

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

Proof. We take the smallest non-abelian finite simple group to be G. By (11.13), $|G| \leq 60$ as A_5 is a non-abelian finite simple group. By (11.4), $|G|$ can't be a prime power, by (11.6), $|G| \neq 56$, and by (11.7), $|G|$ 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 (11.5), if $|G| = 24$ or 48 then $n_2(G) = 3$. However, Sylow's Second Theorem and (11.11) implies that G is isomorphic to a subgroup of S_3 which is impossible as $|S_3| = 6$,
- By Sylow's Third Theorem and (11.5), if $|G| = 36$ then $n_3(G) = 4$. However, Sylow's Second Theorem and (11.11) 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 (11.11),
- By Sylow's Third Theorem, if $|G| = 54$ then $n_3(G) = 1$, contradicting (11.11).

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

12 Soluble and Nilpotent Groups

12.1 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.

12.2 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.

12.3 Insolubility of Non-abelian Simple Groups (8.1)

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

Proof. If we suppose G is soluble and take a subnormal series $G_0, G_1, \dots, G_n$ for G and m to be maximal such that $G_m \neq G$, we 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. □

12.4 Derived Series

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

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

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

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

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

12.5 Derived and Subnormal Series (8.3)

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, (5.5) 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 $\{e\} = G^{(n)} \trianglelefteq G^{(n-1)} \trianglelefteq \cdots \trianglelefteq G^{(0)} = G$ is a subnormal series for G by (5.4) and the factors are abelian by (5.5). Thus, G is soluble of derived length at most n. $\square$

12.6 Derived Groups under Homomorphisms (8.4)

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 $k > 0$:

$$\begin{aligned}
\varphi(G)^{(k)} &= [\varphi(G)^{(k-1)}, \varphi(G)^{(k-1)}] \\
&= \langle [x, y] : x, y \in \varphi(G)^{(k-1)} \rangle \\
&= \langle [x, y] : x, y \in \varphi(G^{(k-1)}) \rangle && \text{(IH)} \\
&= \langle [\varphi(g), \varphi(h)] : g, h \in G^{(k-1)} \rangle \\
&= \langle \varphi([g, h]) : g, h \in G^{(k-1)} \rangle && (5.1) \\
&= \varphi(\langle [g, h] : g, h \in G^{(k-1)} \rangle) && (2.2) \\
&= \varphi(G^{(k)}),
\end{aligned}$$

as required. $\square$

12.7 Solubility of Subgroups and Quotients (8.5)

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 (12.5), $G^{(n)} = \{e\}$ so for $H \leq G$ then $H^{(n)} \leq G^{(n)} = \{e\}$ so H is soluble of derived length at most n by (12.5). For $N \trianglelefteq G$ with π from G to G/N the quotient homomorphism, (12.6) implies that:

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

Thus, by (12.5), G/N is soluble of derived length at most n. $\square$

12.8 Commutator of Symmetric Groups (8.7)

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 $n \geq 3$. As $S_n/A_n \cong C_2$ we have $[S_n, S_n] \leq A_n$ by (5.5). 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. □

12.9 Insolubility of Symmetric Groups (8.6)

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

Proof. As $S_1 \leq S_2 \leq S_3 \leq S_4$, (12.7) 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 (12.3), it is not soluble. So, by (12.7), S_n is not soluble. □

12.10 Central Series

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

12.11 Nilpotent Groups

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

12.12 Lower Central Series

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

$$\cdots \leq G_2 \leq G_1 = G,$$

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

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

12.13 Lower Central and Central Series (8.8)

For a group G with a lower central series $\cdots \leq G_2 \leq G_1 = G$, 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:

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

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

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

($\Longleftarrow$) We have that:

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

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

12.14 The Normaliser Condition (8.9)

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

Proof. We take $\{e\} = Z_0 \leq \cdots \leq Z_k = G$ 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 $N_G(H) \neq H$. $\square$