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
$\{1, 2, \ldots\}$	$\mathbb{N}$
$\{0, 1, 2, \ldots\}$	$\mathbb{N}_0$
The set of primes	$\mathbb{P}$
$(F \backslash \{0_F\}, \times)$	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 Distinct Powers of Group Elements

For an element x in a group G, we have that the powers of x are distinct up to the order of x.

1.2.2 Symmetric Groups

For a set X, the set of bijections $X \to X$ is a group under function composition denoted by $\mathrm{Sym}(X)$. We typically write $\mathrm{Sym}(\{1, 2, \ldots, n\})$ as S_n.

1.2.3 Cyclic Groups

If we consider a regular n-gon P_n, we take rotations of $\frac{2\pi}{n}$ radians about the centre to be r and can define:

$$C_n = \{e, r, r^2, \ldots, r^{n-1}\},$$

to be the group of rotational symmetries of P_n, the cyclic group on P_n.

1.2.4 Dihedral Groups

If we consider again, a regular n-gon P_n and take:

$$r = \text{a rotation of } \frac{2\pi}{n} \text{ radians about the centre,}$$
$$s = \text{reflection in some fixed line of symmetry,}$$

then we have that:

$$\mathrm{Sym}(P_n) = \{e, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\},$$

called the dihedral group, denoted by D_{2n}.

1.2.5 The Infinite Cyclic/Dihedral Group

A map φ from $\mathbb{Z} \to \mathbb{Z}$ is a symmetry if for some n and m in $\mathbb{Z}$:

$$|\varphi(m) - \varphi(n)| = |m - n|.$$

Taking r to be the symmetry $n \mapsto n + 1$, we can define the infinite cyclic group:

$$C_\infty = \{\ldots, r^{-2}, r^{-1}, e, r, r^2, \ldots\}.$$

Taking s to be the symmetry $n \mapsto -n$, we can define the infinite dihedral group:

$$D_\infty = \{\ldots, r^{-2}, r^{-1}, e, r, r^2, \ldots, r^{-2}s, r^{-1}s, s, rs, r^2s\}.$$

1.2.6 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.

1.3 p-groups

For p in $\mathbb{P}$, we say that a group G is a p-group if the order of each element of G is a power of p.

1.4 Subsets of Groups

1.4.1 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 $\{e_G\}$.

1.4.2 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.

1.4.3 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 Order

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

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

Taking x in X, if x has finite order, then:

1. $x^n = e_G$ if and only if $|x|$ divides n,
2. $x^n = x^m$ if and only if $|x|$ divides $m - n$,

and if x has infinite order:

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

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

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

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

For (2) and (3), we take x to have any order and consider:

$$\begin{aligned} x^n &= x^m, \\ x^{m-n} &= e_G. \end{aligned}$$

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

1.6 Isomorphisms

For $(G, *)$, $(H, \circ)$ groups, an isomorphism $\varphi : G \to H$ is a bijection such that $\varphi(x * y) = \varphi(x) \circ \varphi(y)$ for all x, y in G. If such a map exists, we say G is isomorphic to H, denoted by $G \cong H$.

We can restrict isomorphisms to subgroups, compose them, or take the inverse and the result will be an isomorphism.

1.7 Subgroups

A subset X of a group $(G, *)$ is a subgroup if and only if $(X, *)$ (with $*$ restricted to X, for which X must be closed under $*$) is a group, denoted by $X \leq G$ (or if $X \neq G$, $X < G$).

Alternatively, we have that X is a subgroup if and only if:

- e_G is in X,
- X is closed under $*$,
- X is symmetric under $*$.

1.7.1 The Product of Subgroups

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

Proof. By the alternate definition of a subgroup above, we know that for a subgroup X of G, X contains e_G, and X is closed and symmetric under $*$.

Suppose $HK \leq G$, thus:

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

Now, suppose $HK = KH$:

- $e_G = e_G e_G$ is in HK,
- $(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK$,
- $(HK)^{-1} = K^{-1}H^{-1} = KH = HK$,

so HK is a subgroup. □

1.7.2 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. Suppose $X \leq G$, then e_G is in X so $X \neq \varnothing$. For x, y in X, x^{-1} is also in X by the inverse rule of subgroups, so $x^{-1}y$ is also in X by the closure of subgroups.

Suppose $X \neq \varnothing$ and for each x, y in X, $x^{-1}y$ is also in X. Taking x, y in X, we have that $x^{-1}x = e_G$ is also in X. Also, $x^{-1}e_G = x^{-1}$ is in X. Finally, $xy = (x^{-1})^{-1}y$. □

1.7.3 The Intersection of Subgroups

We have that for a group G with $\mathcal{A}$ a set of subgroups of G:

$$\bigcap_{a \in \mathcal{A}} a,$$

is a subgroup of G.

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

1.8 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 $X \cup X^{-1}$ by closure and existence of inverses.

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 and taking x, y in $\Gamma(X)$, for some n, m in $\mathbb{N}$, we have 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 x_i with 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 $\Gamma(X)$ by its definition. Thus, $\Gamma(X)$ is a subgroup as required. $\square$

1.9 Cyclic Groups

A group G is cyclic if it is generated by a single element. Elements in G that generate G are called generators. Supposing G is cyclic:

- For x a generator of G, $G = \{x^n : n \in \mathbb{Z}\}$,
- G is abelian,
- $G \cong C_{|G|}$,
- For $X \leq G$, X is cyclic.

1.10 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. We have some properties of left cosets:

- For h in H, $hH = H = Hh$,
- For g in $G \setminus H$ we cannot say $gH = Hg$ in general,
- G is the union of all the left cosets,
- For x, y in G, $xH = yH$ if and only if x is in yH,
- For x, y in G, either $xH = yH$ or $xH \cap yH = \varnothing$,
- For all x in G, $|xH| = |H|$.

1.10.1 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.

1.10.2 A Equivalence Relation on Cosets

We can define an equivalence relation $\sim$ on a group G with $H \leq G$ by setting:

$$x \sim y \Longleftrightarrow y \in xH,$$

where xH is the equivalence class containing x.

1.10.3 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 $[G : H]$ (the choice of left cosets here is arbitrary due to the bijection between the coset types).

1.10.4 Lagrange's Theorem

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

This means, for any subgroup $H \leq G$, its index and order divide the order of G. Thus, for G a finite group:

- For x in G, $|x|$ divides $|G|$,
- If G has prime order, G is cyclic and every non-identity element is a generator,
- For p in $\mathbb{P}$ with $P, Q \leq G$ and $|P| = |Q| = p$, $P \cap Q = \varnothing$ or $P = Q$.

1.11 Outer Direct Product

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

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

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

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

G is a group under this operation.

1.11.1 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, G_i is cyclic for each i in $[n]$,
- 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 $\mathrm{Aut}(G)$ 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 $\mathrm{Ker}(\varphi) = \{e_G\}$. 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. $\square$

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, $xH = G \backslash H$. 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. □

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 $\pi(H) \cong H/H \cap N$. □

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:

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

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:

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

Note that for a homomorphism φ with domain G, we have that $\varphi([x, y]) = [\varphi(x), \varphi(y)]$.

10.1 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, $[G, G] = \{e_G\}$.

10.2 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. □

10.3 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. $\square$

10.3.1 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. $\square$

10.4 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. $\square$

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 $\mathbb{Z}^n = \{(m_1, \dots, m_n) : m_1, \dots, m_n \in \mathbb{Z}\}$ and $e_i = (0, \dots, 1, \dots, 0) \in \mathbb{Z}^n$ 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. $\square$

12.2 Fundamental Theorem of Finitely Generated Abelian Groups

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

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