

# Group Theory Notes

by Tyler Wright

[github.com/Fluxanoia](https://github.com/Fluxanoia)

[fluxanoia.co.uk](https://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
$\{1, 2, \dots\}$	$\mathbb{N}$
$\{0, 1, 2, \dots\}$	$\mathbb{N}_0$
The set of primes	$\mathbb{P}$
$(F \setminus \{0_F\}, \times)$	$F^*$
(invertible $n \times n$ matrices on $F, \times$ )	$GL_n(F)$

# Contents

<b>0</b>	<b>Notation</b>	<b>1</b>
<b>1</b>	<b>The Fundamentals</b>	<b>5</b>
1.1	Binary Operations . . . . .	5
1.2	Groups . . . . .	5
1.2.1	Distinct Powers of Group Elements . . . . .	5
1.2.2	Symmetric Groups . . . . .	5
1.2.3	Cyclic Groups . . . . .	5
1.2.4	Dihedral Groups . . . . .	6
1.2.5	The Infinite Cyclic/Dihedral Group . . . . .	6
1.2.6	Torsion Groups . . . . .	6
1.3	$p$ -groups . . . . .	6
1.4	Subsets of Groups . . . . .	7
1.4.1	Set Multiplication . . . . .	7
1.4.2	Centre . . . . .	7
1.4.3	Properties of Sets . . . . .	7
1.5	Order . . . . .	7
1.6	Isomorphisms . . . . .	8
1.7	Subgroups . . . . .	8
1.7.1	The Product of Subgroups . . . . .	9
1.7.2	The Subgroup Test . . . . .	9
1.7.3	The Intersection of Subgroups . . . . .	9
1.8	Generated Subgroups . . . . .	10
1.9	Cyclic Groups . . . . .	10
1.10	Cosets . . . . .	11
1.10.1	A Bijection from Left to Right Cosets . . . . .	11
1.10.2	A Equivalence Relation on Cosets . . . . .	11
1.10.3	Index . . . . .	11
1.10.4	Lagrange's Theorem . . . . .	11
1.11	Outer Direct Product . . . . .	12
1.11.1	Properties of the Outer Direct Product . . . . .	12
<b>2</b>	<b>Homomorphisms</b>	<b>13</b>
2.1	Properties of Homomorphisms . . . . .	13
2.2	Homomorphisms and Generating Sets . . . . .	13
<b>3</b>	<b>Automorphisms</b>	<b>14</b>
3.1	Inner Automorphisms . . . . .	14
3.2	Conjugation . . . . .	14

3.2.1	Conjugations on Subgroups . . . . .	14
<b>4</b>	<b>Normal and Characteristic Subgroups</b>	<b>15</b>
4.1	Properties of Normal Subgroups . . . . .	15
4.2	A Test for Normal and Characteristic Subgroups . . . . .	15
4.3	Normal Subgroups of Index 2 . . . . .	16
4.4	Properties of the Centre . . . . .	16
4.5	Simple Groups . . . . .	16
<b>5</b>	<b>Quotient Groups</b>	<b>17</b>
<b>6</b>	<b>The Homomorphism Theorem</b>	<b>18</b>
<b>7</b>	<b>The First Isomorphism Theorem</b>	<b>18</b>
7.1	The Order of the Product . . . . .	19
<b>8</b>	<b>The Second Isomorphism Theorem</b>	<b>20</b>
<b>9</b>	<b>The Correspondence Theorem</b>	<b>20</b>
<b>10</b>	<b>Commutators</b>	<b>22</b>
10.1	Commutator Subgroups . . . . .	22
10.2	Commutator Subgroup of Characteristic Subgroups . . . . .	22
10.3	Abelian Quotients . . . . .	22
10.3.1	Quotients of Abelian Groups . . . . .	23
10.4	The Abelianisation . . . . .	23
<b>11</b>	<b>Direct Products</b>	<b>24</b>
11.1	Component Groups . . . . .	24
11.2	The Commutator of Normal Subgroups . . . . .	25
11.3	Isomorphism between Products . . . . .	25
11.4	Criteria for Inner Direct Products . . . . .	26
11.4.1	By Unique Compositions . . . . .	26
11.4.2	By the Size . . . . .	27
<b>12</b>	<b>Finitely Generated Abelian Groups</b>	<b>28</b>
12.1	Classification of Cyclic Groups . . . . .	28
12.2	The Torsion Subgroup . . . . .	28
12.3	The Primary Decomposition Theorem . . . . .	29
12.4	Finitely Generated Abelian Torsion Groups . . . . .	30
12.5	Order of Elements in $p$ -groups . . . . .	30
12.6	Elements with Coset Order . . . . .	30

12.7	Decomposition of Finite Abelian $p$ -groups . . . . .	31
12.8	Homomorphism from $\mathbb{Z}^n$ to Sequences . . . . .	31
12.9	One-way Inverses on Homomorphisms to $\mathbb{Z}^n$ . . . . .	32
12.10	Abelian Groups with $\mathbb{Z}^n$ Quotients . . . . .	32
12.11	Finitely Generated Subgroups . . . . .	33
12.12	Fundamental Theorem of Finitely Generated Torsion-free Abelian Groups . . . . .	33
12.13	Fundamental Theorem of Finitely Generated Abelian Groups . . . . .	34
<b>13</b>	<b>Symmetric Groups</b>	<b>35</b>
13.1	Cycles . . . . .	35
13.2	Permutations as Disjoint Cycles . . . . .	36
13.3	Cycle Type . . . . .	36
13.4	Conjugacy in $S_n$ . . . . .	36
13.5	Conjugacy and Cycle Type . . . . .	37
13.6	Parity of Transposition Representations . . . . .	37
13.7	Signature . . . . .	37
13.8	The Signature Homomorphism . . . . .	38
13.9	Alternating Groups . . . . .	38
13.10	Subgroups of Index 2 in $S_n$ . . . . .	38
13.11	Alternating Groups generated by 3-Cycles . . . . .	39
<b>14</b>	<b>Group Actions</b>	<b>40</b>
14.1	The Orbit and Stabiliser . . . . .	40
14.2	The Orbit-Stabiliser Theorem . . . . .	40
14.3	Relation via the Orbit . . . . .	41
14.4	Fixed Points . . . . .	41
14.5	The Conjugation Action . . . . .	42
14.6	Partitioning on Conjugacy Classes . . . . .	42
14.7	The Orbit-Stabiliser Theorem for Conjugation . . . . .	42
14.8	The Class Equation . . . . .	42
<b>15</b>	<b>Sylow's Theorems</b>	<b>43</b>
15.1	Cauchy's Theorem . . . . .	43

# 1 The Fundamentals

## 1.1 Binary Operations

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

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  $X \rightarrow X$  is a group under function composition denoted by  $\text{Sym}(X)$ . We typically write  $\text{Sym}(\{1, 2, \dots, n\})$  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:

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

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:

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

then we have that:

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

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

### 1.2.5 The Infinite Cyclic/Dihedral Group

A map  $\varphi$  from  $\mathbb{Z} \rightarrow \mathbb{Z}$  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:

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

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

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

### 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:

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

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  $\{0, 1, \dots, |x| - 1\}$ . 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.  $\square$

## 1.6 Isomorphisms

For  $(G, *)$ ,  $(H, \circ)$  groups, an isomorphism  $\varphi : G \rightarrow H$  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  $X \neq \emptyset$  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  $X \neq \emptyset$ . 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  $X \neq \emptyset$  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:

$$x = x_1 x_2 \cdots x_n,$$

$$y = y_1 y_2 \cdots y_m,$$

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  $xH \cap yH = \emptyset$ ,
- 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:

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

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  $|P| = |Q| = p$ ,  $P \cap Q = \emptyset$  or  $P = Q$ .

## 1.11 Outer Direct Product

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

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

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

$$(a_1, \dots, a_n)(b_1, \dots, b_n) = (a_1b_1, \dots, a_nb_n).$$

$G$  is a group under this operation.

### 1.11.1 Properties of the Outer Direct Product

For  $G_1, \dots, G_n$  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  $\sigma$  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  $[n]$   $G \cong \prod_{i \in [n]} H_i$ .

## 2 Homomorphisms

For  $G, H$  groups, a homomorphism  $\varphi : G \rightarrow H$  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:

$$\begin{aligned}\text{Im}(\varphi) &= \{\varphi(g) : g \in G\}, \\ \text{Ker}(\varphi) &= \{g \in G : \varphi(g) = e_H\}.\end{aligned}$$

### 2.1 Properties of Homomorphisms

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

1.  $\varphi(e_G) = e_H$ ,
2.  $\text{Ker}(\varphi)$  is a subgroup of  $G$ ,
3.  $\text{Im}(\varphi)$  is a subgroup of  $H$ ,
4.  $\varphi$  is injective if and only if  $\text{Ker}(\varphi) = \{e_G\}$ ,
5.  $\varphi(x^{-1}) = \varphi(x)^{-1}$  for every  $x$  in  $G$ ,
6. For  $x_1, \dots, x_n$  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  $\varphi : G \rightarrow H$ , and  $X \subseteq G$ , we have that  $\varphi(\langle X \rangle) = \langle \varphi(X) \rangle$ .

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

### 3 Automorphisms

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

#### 3.1 Inner Automorphisms

For a group  $G$ , we have that  $\varphi : G \rightarrow G$  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  $\varphi$  is a homomorphism. We can see that  $g^{-1}xg = e_G$  implies that  $x = gg^{-1} = e_G$  so  $\text{Ker}(\varphi) = \{e_G\}$ . Finally, we see that  $x = g^{-1}(gxg^{-1})g$  so  $\varphi$  is surjective as  $x$  is arbitrary in  $G$ . Thus,  $\varphi$  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  $\varphi$  in  $\text{Aut}(G)$ ,  $\varphi(H) = H$  (denoted by  $H \trianglelefteq_{\text{char}} G$ ). We know characteristic subgroups are normal as  $\text{Aut}(G)$  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  $\varphi : G \rightarrow H$  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  $\text{Ker}(\varphi) \trianglelefteq G$ . 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  $\varphi$  in  $\text{Aut}(G)$ ,  $\varphi(H) \subseteq H$  then  $H \trianglelefteq_{\text{char}} G$ .

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

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

### 4.3 Normal Subgroups of Index 2

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

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

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

### 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  $\varphi$  in  $\text{Aut}(G)$  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  $\varphi$  is a homomorphism. Furthermore,  $\varphi(z)h = h\varphi(z)$  for every  $h$  in  $G$  as  $\varphi$  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  $G$ .  $\square$

### 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  $\pi : G \rightarrow G/H$  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.

$\pi$  is trivially surjective, for  $g$  in  $\text{Ker}(\pi)$ ,  $gH = H$  which means  $g$  is in  $H$ . The converse is true as  $H$  is a subgroup. Thus,  $\pi$  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  $\pi$  on this quotient group the quotient homomorphism from  $G$  to  $G/H$ .

## 6 The Homomorphism Theorem

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

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

*Proof.* We set  $I = \text{Im}(\varphi)$  and  $K = \text{Ker}(\varphi)$ , and define  $\psi : G/K \rightarrow I$  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  $\psi$  is a homomorphism and is trivially surjective as required.  $\square$

## 7 The First Isomorphism Theorem

For a group  $G$  with  $N \trianglelefteq G$ ,  $\pi : G \rightarrow G/N$  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  $\pi$  to  $H$ . Note that  $\pi|_H : H \rightarrow G/N$  is a homomorphism. Furthermore:

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

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

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

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

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

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

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

so  $\varphi$  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:

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

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  $\pi : G \rightarrow G/N$  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  $\varphi$  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  $H, K \trianglelefteq_{\text{char}} G$ ,  $[H, K] \trianglelefteq_{\text{char}} G$ . Furthermore,  $[G, G] \trianglelefteq_{\text{char}} G$ .

*Proof.* We take  $\varphi$  in  $\text{Aut}(G)$ :

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

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  $\pi : G \rightarrow G/H$  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 arbitrary,  $[G, G] \subseteq H$ .

( $\Leftarrow$ ) 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  $H \trianglelefteq_{\text{char}} G$  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  $[G, G] \trianglelefteq_{\text{char}} G$ .

## 11 Direct Products

We have already seen the outer direct product as:

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

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

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:

- $G = H_1 \times \cdots \times H_n$ ,
- $H_i \cap (H_1 \times \cdots \times H_{i-1} \times H_{i+1} \times \cdots \times H_n) = \{e_G\}$  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:

$$\widehat{G}_i = \{(e, \dots, e, g_i, e, \dots, e) : g_i \in G_i\}.$$

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  $\widehat{G}_1, \dots, \widehat{G}_n$ .

*Proof.* (1) We can see that:

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

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

(2) We can see that:

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

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

(3) We have that  $G = \widehat{G}_1 \cdots \widehat{G}_n$  as:

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

Furthermore,  $\widehat{G}_i \cap G'_i = \{e\}$  where  $G'_i = \widehat{G}_1, \dots, \widehat{G}_{i-1}, \widehat{G}_{i+1}, \dots, G_n$  as the elements of  $G'_i$  are of the form  $(g_1, \dots, g_{i-1}, e, g_{i+1}, \dots, g_n)$  whereas elements of  $\widehat{G}_i$  are of the form  $(e, \dots, e, g_i, e, \dots, e)$ . 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  $H_1, \dots, H_n$ ,  $G \cong H_1 \times \cdots \times H_n$ .

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

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

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  $(h_1, \dots, h_n) \in \text{Ker}(\varphi)$ :

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

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

## 11.4 Criteria for Inner Direct Products

### 11.4.1 By Unique Compositions

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 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  $H_1, \dots, H_n$  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  $H_1, \dots, H_n \leq G$  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  $i^{\text{th}}$  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  $\varphi : \mathbb{Z} \rightarrow G$  to be defined as  $\varphi(m) = x^m$ . We can see that  $\varphi$  is a surjective homomorphism. If  $|x| = \infty$  then  $\text{Ker}(\varphi) = \{0\}$ , otherwise,  $\text{Ker}(\varphi) = |x|\mathbb{Z}$ . By the homomorphism theorem:

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

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

### 12.2 The Torsion Subgroup

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

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

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

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

### 12.3 The Primary Decomposition Theorem

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

*Proof.* We take  $x$  in  $G$ , by Lagrange's Theorem, we have that  $x = p_1^{l_1} \dots p_k^{l_k}$  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  $G_{p_i}$ . Clearly  $\gcd(n_1, \dots, n_k) = 1$ , so by the Euclidean algorithm there exists  $m_1, \dots, m_k$  such that  $m_1 n_1 + \dots + m_k n_k = 1$ . 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,  $G = G_{p_1} + \dots + G_{p_k}$ .

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

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

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

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

$$\begin{aligned} &ar_i + bp_i^{d_i} = 1, \\ \implies &y_i = (ar_i + bp_i^{d_i})y_i, \\ \implies &y_i = ar_i y_i + bp_i^{d_i} y_i, \\ \implies &y_i = 0 + 0 = 0, \end{aligned}$$

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

## 12.4 Finitely Generated Abelian Torsion Groups

A finitely generated torsion group is finite.

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

$$G = \{l_1x_1 + \dots + l_nx_n : 0 \leq l_i < |x_i|\},$$

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

## 12.5 Order of Elements in $p$ -groups

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

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

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

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

## 12.6 Elements with Coset Order

For  $G$  a finite abelian  $p$ -group for some prime  $p$ . We take  $g$  in  $G$  to have maximum order. For every  $x$  in  $G$ , there exists  $y$  in  $x + \langle g \rangle$  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  $p^m \cdot x$  is in  $\langle g \rangle$  so  $p^m \cdot x = l \cdot g$  for some  $l$  in  $\mathbb{N}_0$  (if  $l = 0$  we are done). We write  $l = np^r$  with  $n, p$  coprime. If  $p^r \geq |g|$  then  $l \cdot g = 0$  and  $|x| = p^m$  and we are done. Otherwise, we use the result above to see that  $|l \cdot g| = \frac{|g|}{p^r}$  and  $|p^m x| = \frac{|x|}{p^m}$  so  $\frac{|g|}{p^r} = \frac{|x|}{p^m}$ . The maximality of  $g$  implies that  $|g| \geq |x|$  so  $r \geq m$  and thus  $p^m$  divides  $l$ . We define:

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

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

## 12.7 Decomposition of Finite Abelian $p$ -groups

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

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

$$G = \langle x_1 \rangle \oplus \dots \oplus \langle x_k \rangle. \quad (*)$$

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

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

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

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

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

which combined with Lagrange's theorem means that:

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

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

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

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

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

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

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

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

For an abelian group  $G$  and  $\alpha : G \rightarrow \mathbb{Z}^n$  is a surjective homomorphism, there exists an injective homomorphism  $\beta : \mathbb{Z}^n \rightarrow G$  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  $g_1, \dots, g_n$  in  $G$  such that  $\alpha(g_i) = e_i$  for all  $i$  as  $\alpha$  is surjective. The previous result states that there exists a homomorphism  $\beta$  from  $\mathbb{Z}^n$  to  $G$  such that  $\beta(e_i) = g_i$  for all  $i$ . This gives us that  $(\alpha \circ \beta)(e_i) = e_i$  which defines  $\alpha \circ \beta$  as homomorphisms are defined by the images of a set of generators. Thus,  $\alpha \circ \beta = \iota_{\mathbb{Z}^n}$ .

We can see that:

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

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

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

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

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

Given  $g$  in  $G$ :

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

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



## 12.11 Finitely Generated Subgroups

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

*Proof.* We know that  $G \cong H \oplus \mathbb{Z}^n$  by the previous result. The projection  $\pi$  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  $\pi$ .  $\square$

## 12.12 Fundamental Theorem of Finitely Generated Torsion-free Abelian Groups

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

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

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

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

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

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

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

### 12.13 Fundamental Theorem of Finitely Generated Abelian Groups

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

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

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

## 13 Symmetric Groups

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

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

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

as required. □

### 13.1 Cycles

For  $k$  in  $\mathbb{N}$ , a permutation  $f$  in  $S_n$  is called  $k$ -cycle if there are  $k$  distinct members  $i_1, \dots, i_k$  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  $f = (i_1, \dots, i_k)$ . A 2-cycle is called a transposition and cycles  $(i_1, \dots, i_k), (j_1, \dots, j_l)$  are disjoint if  $\{i_1, \dots, i_k\} \cap \{j_1, \dots, j_l\} = \emptyset$ . Furthermore:

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

## 13.2 Permutations as Disjoint Cycles

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

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

## 13.3 Cycle Type

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

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

## 13.4 Conjugacy in $S_n$

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

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

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

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

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

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

as required. □

### 13.5 Conjugacy and Cycle Type

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

*Proof.* We take the cycle type of  $x$  be  $(l_1, \dots, l_k)$  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 to some  $a_j^{(r)}$ . For  $g$  in  $S_n$ :

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

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

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

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

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

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

using the previous result. □

### 13.6 Parity of Transposition Representations

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

### 13.7 Signature

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

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

## 13.8 The Signature Homomorphism

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

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

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

□

## 13.9 Alternating Groups

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

*Proof.*  $A_n = \text{Ker}(\varepsilon)$ .

□

## 13.10 Subgroups of Index 2 in $S_n$

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

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

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

meaning  $\pi$  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,  $H = \text{Ker}(\pi) = \text{Ker}(\varepsilon) = A_n$ .

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

### 13.11 Alternating Groups generated by 3-Cycles

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

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

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

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

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

a 3-cycle.

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

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

a product of two 3-cycles.

□

## 14 Group Actions

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

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

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

### 14.1 The Orbit and Stabiliser

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

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

are the orbit and stabiliser of  $x$ , respectively.

### 14.2 The Orbit-Stabiliser Theorem

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

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

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

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

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

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

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



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

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

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

### 14.3 Relation via the Orbit

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

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

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

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

### 14.4 Fixed Points

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

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

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

*Proof.* We have that:

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

$\square$

## 14.5 The Conjugation Action

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

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

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

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

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

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

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

## 14.6 Partitioning on Conjugacy Classes

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

## 14.7 The Orbit-Stabiliser Theorem for Conjugation

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

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

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

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

## 14.8 The Class Equation

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

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

## 15 Sylow's Theorems

### 15.1 Cauchy's Theorem

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

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

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

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

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

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

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

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

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

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