

# 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>4</b>
1.1	Binary Operations . . . . .	4
1.2	Groups . . . . .	4
1.2.1	Distinct Powers of Group Elements . . . . .	4
1.2.2	Symmetric Groups . . . . .	4
1.2.3	Cyclic Groups . . . . .	4
1.2.4	Dihedral Groups . . . . .	5
1.2.5	The Infinite Cyclic/Dihedral Group . . . . .	5
1.2.6	Torsion Groups . . . . .	5
1.3	$p$ -groups . . . . .	5
1.4	Subsets of Groups . . . . .	6
1.4.1	Set Multiplication . . . . .	6
1.4.2	Centre . . . . .	6
1.4.3	Properties of Sets . . . . .	6
1.5	Order . . . . .	6
1.6	Isomorphisms . . . . .	7
1.7	Subgroups . . . . .	7
1.7.1	The Product of Subgroups . . . . .	8
1.7.2	The Subgroup Test . . . . .	8
1.7.3	The Intersection of Subgroups . . . . .	8
1.8	Generated Subgroups . . . . .	9
1.9	Cyclic Groups . . . . .	9
1.10	Cosets . . . . .	10
1.10.1	A Bijection from Left to Right Cosets . . . . .	10
1.10.2	A Equivalence Relation on Cosets . . . . .	10
1.10.3	Index . . . . .	10
1.10.4	Lagrange's Theorem . . . . .	10
1.11	Outer Direct Product . . . . .	11
1.11.1	Properties of the Outer Direct Product . . . . .	11
<b>2</b>	<b>Homomorphisms</b>	<b>12</b>
2.1	Properties of Homomorphisms . . . . .	12
2.2	Homomorphisms and Generating Sets . . . . .	12
<b>3</b>	<b>Automorphisms</b>	<b>13</b>
3.1	Inner Automorphisms . . . . .	13
3.2	Conjugation . . . . .	13

3.2.1	Conjugations on Subgroups . . . . .	13
<b>4</b>	<b>Normal and Characteristic Subgroups</b>	<b>14</b>
4.1	Properties of Normal Subgroups . . . . .	14
4.2	A Test for Normal and Characteristic Subgroups . . . . .	14
4.3	Normal Subgroups of Index 2 . . . . .	15
4.4	Properties of the Centre . . . . .	15
4.5	Simple Groups . . . . .	15
<b>5</b>	<b>Quotient Groups</b>	<b>16</b>

# 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  $1 \leq n_1 < n_2 < \cdots < n_r < n$ ,

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

- 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  $\text{Ker}(\varphi) \trianglelefteq G$ .

### 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  $G/H$ .