MA2202 Algebra I

Thang Pang Ern and Malcolm Tan Jun Xi

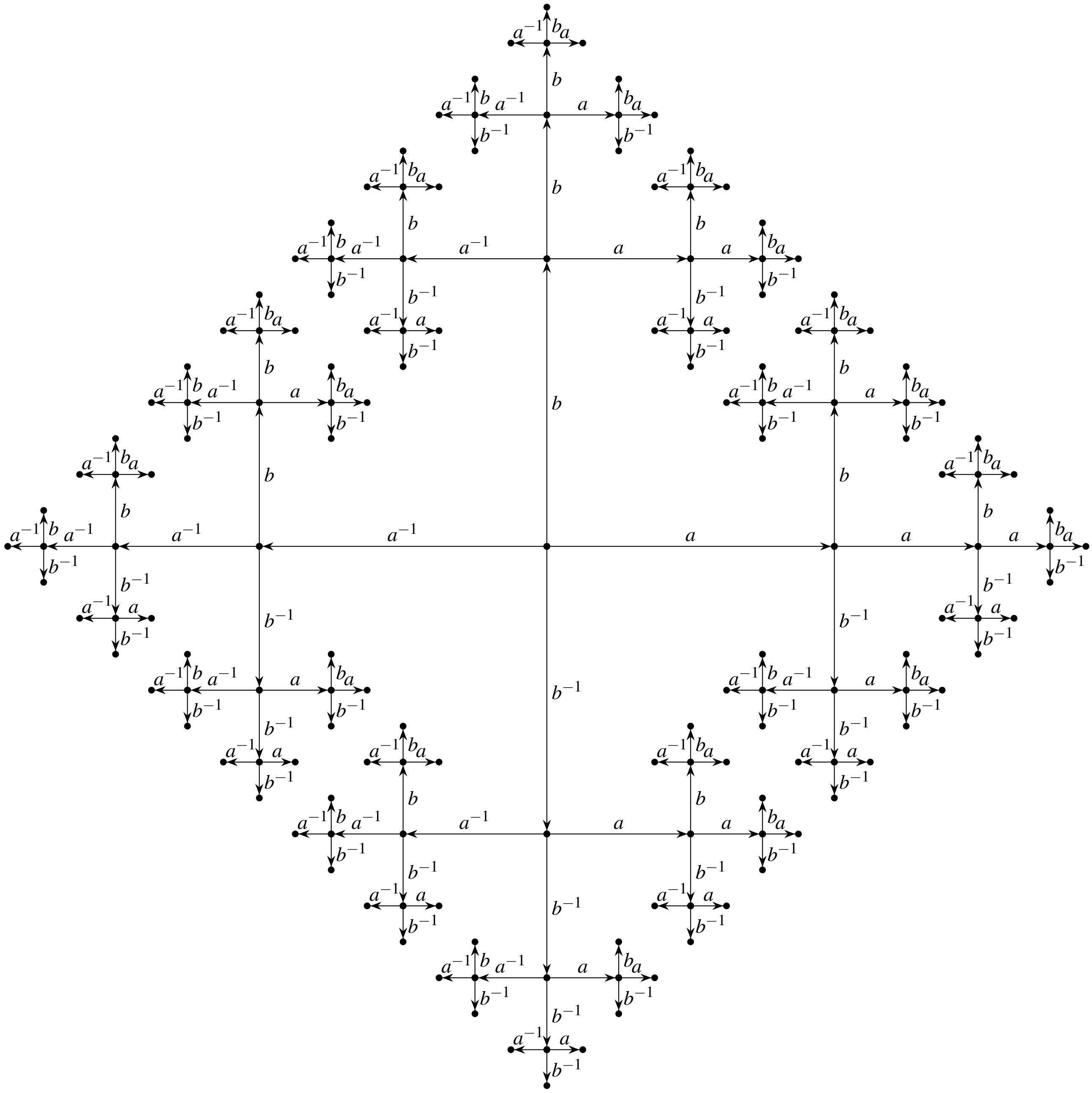
Contents

References

1 Dummit, D. S. and Foote, R. M. (2003). *Abstract Algebra 3rd Edition*. Wiley.

2 Gallian, J. (2009). *Contemporary Abstract Algebra 7th Edition*. Cengage Learning.

3 Carter, N. (2009). *Visual Group Theory*. American Mathematical Society. Mathematical Association of America.



Cayley graph of the free group on two generators a and b

Chapter 1
Introduction to Groups

1.1
Basic Axioms and Examples

Definition 1.1 (group axioms). A group consists of an underlying set G, equipped with a multiplication map $\cdot$, where

$$\cdot : G \times G \to G \quad \text{such that} \quad (a,b) \mapsto a \cdot b \text{ or } ab,$$

the identity element $e \in G$ (usually the identity e is 1), and an inversion map, where

$$(\ )^{-1} : G \to G \quad \text{such that} \quad a \mapsto a^{-1}.$$

Moreover, the following group axioms must be satisfied:

(i) Associativity of $\cdot$: for all $a,b,c \in G$, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(ii) Existence of identity element: for all $a \in G$, there exists $e \in G$ such that $a \cdot e = e \cdot a = a$

(iii) Existence of inverse element: for all $a \in G$, we have $a \cdot a^{-1} = a^{-1} \cdot a = e$

Definition 1.2 (Abelian group). A group G is Abelian or commutative if the elements commute, i.e.

$$\text{for all } a,b \in G, \quad \text{we have } a \cdot b = b \cdot a.$$

Example 1.1 (Dummit and Foote p. 21 Question 7). Let $G = \{x \in \mathbb{R} : 0 \leq x < 1\}$ and for $x,y \in G$, let $x * y$ be the fractional part of $x + y$, i.e. $x * y = x + y - [x+y]$, where $[a]$ is the greatest integer less than or equal to a. Prove that $*$ is a well-defined binary operation on G and that G is an Abelian group under $*$ (called the *real numbers* mod 1).

Solution. To show that $*$ is a binary operation, we need to show that

$$\text{for any } 0 \leq x,y < 1 \quad \text{we have} \quad 0 \leq x + y - [x+y] < 1.$$

Since $0 \leq x + y < 2$ and $[x+y] \in \{0,1\}$, it follows that $0 \leq x + y - [x+y] < 1$, so $*$ is a binary operation. Well-definedness of $*$ follows from here too.

We then prove that $(G,*)$ forms a group. Closure was already established; the existence of the identity element $0 \in G$, and for every $x \in G$, $1 - x \in G$ is an inverse because

$$x * (1-x) = x + (1-x) - [x + 1 - x] = 0.$$

Proving associativity is slightly tedious. Suppose $x,y,z \in G$. Then,

$$(x*y)*z = (x + y - [x+y]) * z = x + y + z - [x+y] - [x+y+z-[x+y]]$$

and

$$x*(y*z) = x*(y+z-[y+z]) = x+y+z-[y+z] - [x+y+z-[y+z]]$$

Hence, it suffices to show that

$$[x+y]+[x+y+z-[x+y]]=[y+z]+[x+y+z-[y+z]].$$

There are four cases to consider, which are as follows: 2

(i) $[x+y]=0$ and $[y+z]=0$

(ii) $[x+y]=1$ and $[y+z]=1$

(iii) $[x+y]=0$ and $[y+z]=1$

(iv) $[x+y]=1$ and $[y+z]=0$

Cases **(i)** and **(ii)** are obvious. Since **(iii)** and **(iv)** are symmetric, we will only prove for Case **(iii)**. We have

$$[x+y]+[x+y+z-[x+y]]=[x+y+z]$$

and

$$[y+z]+[x+y+z-[y+z]]=1+[x+y+z-1].$$

Using the substitution $t=x+y+z$, where we note that $0\le t<3$, it suffices to prove that $[t]=1+[t-1]$, which is obviously true. We conclude that G is a group equipped with the binary operation $*$.

Lastly, we need to show that G is Abelian. Suppose $g_1,g_2\in G$. Then,

$$g_1*g_2=g_1+g_2-[g_1+g_2]=g_2+g_1-[g_2+g_1]=g_2*g_1,$$

so G is Abelian. □

Example 1.2 (Dummit and Foote p. 22 Question 25)**.** Prove that if $x^2=1$ for all $x\in G$, then G is Abelian.

Solution. Suppose $x,y\in G$. Then, $(xy)^2=1$, which implies $xyxy=1$. Hence, $xy=y^{-1}x^{-1}$. Since $x^2=1$, then $x=x^{-1}$, so it follows that $xy=yx$. As such, G is Abelian. □

Example 1.3 (Dummit and Foote p. 22 Question 24)**.** If a and b are commuting elements of G, prove that $(ab)^n=a^nb^n$ for all $n\in\mathbb{Z}$. (*Hint:* Do this by induction for positive n first.)

Solution. We will only prove the inductive step. Given that $a,b\in G$ are commuting elements such that $(ab)^k=a^kb^k$, then

$$(ab)^{k+1}=(ab)(ab)^k=aba^kb^k=baa^kb^k=ba^{k+1}b^k=a^{k+1}bb^k=a^{k+1}b^{k+1}.$$

So, $(ab)^n=a^nb^n$ for all $n\in\mathbb{Z}^+$ by induction. The proof for negative integers is similar by replacing n with $-n$. Also, the proof for the case when $n=0$ is trivial. □

Remark 1.1. In Example 1.2, such elements $x\in G$ are said to be *idempotent*. There is an analogous concept in Linear Algebra, i.e. a square matrix $\mathbf{A}$ is idempotent if and only if $\mathbf{A}^2=\mathbf{I}$.

Proposition 1.1. Let G be a group. Then, the following hold:

(i) The identity element e of G is uniquely determined by $\cdot$

(ii) For any $a\in G$, the inverse a^{-1} of a is uniquely determined by a, $\cdot$ and e

(iii) **Idempotence of inverse operation:** For any $a\in G$, $\left(a^{-1}\right)^{-1}=a$

(iv) **Shoe-socks property:** For any $a,b\in G$, $(a\cdot b)^{-1}=\left(b^{-1}\right)\cdot\left(a^{-1}\right)$

(v) Generalised associativity law: For any $n \in \mathbb{N}$ and for any $a_1, \ldots, a_n \in G$,

$$\text{the value of } a_1 \cdot \ldots \cdot a_n \in G \quad \text{is independent of} \quad \text{how the expression is bracketed}$$

Proof. We will only prove **(i)** and **(ii)**. The proofs of **(iii)** and **(iv)** are quite straightforward. Lastly, **(v)** can be proven using strong induction but it is rather tedious.

We first prove **(i)**. Assume $f \in G$ is also an identity element. Then, by **(ii)** of Definition 1.1, we have $a \cdot f = f \cdot a = a$. Replacing a with e, we have $f = f \cdot e = e$, where the first equality $f = f \cdot e$ follows because $e \in G$ is an identity element. As $e = f$, we conclude that the identity element is uniquely determined by $\cdot$.

We then prove that **(ii)** holds. Assume $b \in G$ is also an inverse element. Then, by **(iii)** of Definition 1.1, b also satisfies $a \cdot b = b \cdot a = e$. As such,

$$b = b \cdot e = b \cdot \left(a \cdot a^{-1}\right) = (b \cdot a) \cdot a^{-1} = e \cdot a^{-1} = a^{-1}$$

so $b = a^{-1}$, implying that the inverse of a is unique. □

As such, by **(i)** and **(ii)** of Proposition 1.1, it is common to specify a group simply by giving the underlying set G and the multiplication map $\cdot : G \times G \to G$. The identity element $e \in G$ and the inversion map are then understood *implicitly*.

Corollary 1.1 (generalised shoe-socks property)**.** The shoe-socks property in **(iv)** of Proposition 1.1 can be generalised as follows:

$$(a_1 a_2 \ldots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \ldots a_1^{-1} \quad \text{for all} \quad a_1, a_2, \ldots, a_n \in G.$$

Corollary 1.1 is presented as a question on p. 22 Question 15 of the Dummit and Foote textbook.

Example 1.4 (trivial group)**.** Any singleton $\{e\}$ is a group. This is known as the trivial group.

Example 1.5 (additive groups)**.** Under $+$, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are groups. However, $\mathbb{N}$ under $+$ is not a group since it does not have an identity element. Although obvious, to deduce rigorously, suppose on the contrary that e is the additive identity of $\mathbb{N}$. Then,

$$\text{for any } a \in \mathbb{N}, \quad \text{there exists } e \in \mathbb{N} \quad \text{such that } a + e = a.$$

This means that $e = 0$, but $0 \notin \mathbb{N}$. Moreover, one recalls the subset inclusion

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C} \quad \text{so because } \mathbb{Z} \text{ is a group,} \quad \text{then } \mathbb{Q}, \mathbb{R}, \mathbb{C} \text{ are groups.}$$

Example 1.6 (multiplicative groups)**.** Under $\times$ (or $\cdot$), the following sets are groups:

$$\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\} \quad \text{and} \quad \mathbb{R}^\times = \mathbb{R} \setminus \{0\} \quad \text{and} \quad \mathbb{C}^\times = \mathbb{C} \setminus \{0\}$$

These are known as multiplicative groups. Also, although $\times$ and $\cdot$ practically denote the same thing, we use the superscript $\times$ instead of $\cdot$ when denoting the respective multiplicative groups, i.e. we write $\mathbb{Q}^\times$ instead of $\mathbb{Q}^\cdot$.

To get a sense of what is going on in these groups, we take $\mathbb{R}^\times$ as an example. By the closure property of groups as mentioned at the start of Definition 1.1, for any $x, y \in \mathbb{R}^\times$, we must have $xy \in \mathbb{R}^\times$. To put it in plain

English, this means that

$$\text{the product of two non-zero real numbers} \quad \text{is also a non-zero real number.}$$

This is obviously true.

Having said all these, $\mathbb{Z} \setminus \{0\}$ under $\times$ does not form a group. This is because **(iii)** of Definition 1.1 is not satisfied, i.e. there does not exist an inverse element in this set. To see why, say we have

$$a \in \mathbb{Z} \setminus \{0\}, \quad \text{and suppose there exists } b \in \mathbb{Z} \setminus \{0\} \quad \text{such that } ab = 1.$$

Say $a = 2$, then $b = 1/2 \notin \mathbb{Z}$, so $\mathbb{Z} \setminus \{0\}$ does not form a group under multiplication.

Example 1.7 (multiplicative group of $\mathbb{Z}$). Although $\mathbb{Z} \setminus \{0\}$ under $\times$ is not a multiplicative group (Example 1.6), we see that $\mathbb{Z}^\times = \{\pm 1\}$ under $\times$ is a group. One can easily verify this property using the group axioms in Definition 1.1.

Here is a brief taster on rings, although we will introduce them formally in MA3201. Anyway, we say that a set R is a ring if the following properties are satisfied:

(i) R is a group under $+$, which is known as the additive group of R

(ii) $A^* = \{a \in A : \text{there exists } b \in A \text{ such that } ab = 1_R = ba\}$ is a group under $\times$, which is known as the multiplicative group of R

Example 1.8 (integers modulo n). For any $n \in \mathbb{Z}^+$, define $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\}$ to be the set of integers modulo n, i.e. this set comprises the remainders when any integer is divided by n.

Under $+$, $\mathbb{Z}/n\mathbb{Z}$ is an additive group. Moreover, it is said to be a *cyclic group* of *order* n. To those who wish to jump the gun, the concepts of cyclic subgroups of a group and the order of a group will be discussed in Definitions 1.3 and 2.10 respectively.

Example 1.9 (group of roots of unity in $\mathbb{C}$). Let

$$G = \left\{ z \in \mathbb{C} : z^n = 1 \text{ for some } n \in \mathbb{Z}^+ \right\}.$$

Then, G is a group under multiplication, known as the group of roots of unity in $\mathbb{C}$. For those who have prior knowledge in H2 Further Mathematics, you would know that the elements of the group G are $z = e^{2k\pi i/n}$, where $0 \le k \le n-1$ is an integer. Having said all these, note that G is not a group under addition.

Example 1.9 appears as an exercise question (p. 22 Question 8) of the Dummit and Foote textbook. One can attempt to verify that $(G, \cdot)$ is indeed a group.

Example 1.10 (Gallian p. 92 Question 16). Let

$$G = \left\{ a + b\sqrt{2} : a, b \in \mathbb{Q} \text{ and } a, b \text{ are both non-zero} \right\}.$$

Prove that G is a group under ordinary multiplication.

Solution. We first prove that the closure property is satisfied. Let $a_1, a_2, b_1, b_2 \in \mathbb{Q}$, with a_1, b_1 both non-zero and a_2, b_2 both non-zero. Then, given that

$$a_1 + b_1\sqrt{2}, a_2 + b_2\sqrt{2} \in G, \quad \text{we have} \quad \left(a_1 + b_1\sqrt{2}\right)\left(a_2 + b_2\sqrt{2}\right) = a_1a_2 + 2b_1b_2 + (a_1b_2 + a_2b_1)\sqrt{2} \in G.$$

Although tedious, one is able to deduce that associativity of $\cdot$ holds in G, so **(i)** of Definition 1.1 is satisfied. The identity element in the set G is 1, so **(ii)** of Definition 1.1 is satisfied. Lastly, we construct the multiplicative inverse of $a+b\sqrt{2} \in G$.

Suppose there exists $c \in G$ such that $\left(a+b\sqrt{2}\right)c = 1$. Then, by conjugation, we have

$$c = \frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} \quad \text{which is defined since } a,b \text{ both non-zero} \quad \text{implies } a^2-2b^2 \neq 0.$$

As such, **(iii)** of Definition 1.1 is satisfied. ☐

Example 1.11 (Dummit and Foote p. 22 Question 18). Let x and y be elements of G. Then,

$$xy = yx \quad \text{if and only if} \quad y^{-1}xy = x \quad \text{if and only if} \quad x^{-1}y^{-1}xy = 1.$$

Solution. We have

$$\begin{aligned} xy = yx \quad & \text{if and only if} \quad y^{-1}xy = y^{-1}yx = x \\ & \text{if and only if} \quad x^{-1}y^{-1}xy = x^{-1}x = 1 \end{aligned}$$

and the result follows. ☐

Definition 1.3 (finite group and its order). A finite group is a group whose underlying set is a finite set. The order of a finite group G is the cardinality $|G|$ of the set G.

Definition 1.4 (Cayley table). Let $G = \{g_1, \ldots, g_n\}$ be a finite group with $g_1 = 1$. The Cayley table of G is the $n \times n$ matrix whose i,j-entry is g_ig_j.

Other than the term 'Cayley table', one can also refer to it as a multiplication table or a group table. As inferred from its name, a Cayley table describes the structure of a finite group by arranging all the possible products of all the group's elements in a square table which is reminiscent of an addition or a multiplication table. Many properties of a group (i.e. whether it is Abelian, identifying which elements are inverses of another) can be deduced from its Cayley table.

We shall construct Cayley tables for some groups of small order.

Example 1.12 (Cayley table of G, where $|G| = 1$). Let G be a group such that $G = \{e\}$, where e is the identity element of G. Then, the following is the Cayley table of G:

$\cdot$	e
e	e

Table 1: Cayley table of G, where $|G| = 1$

Example 1.13 (Cayley table of G, where $|G| = 2$)**.** Let G be a group such that $G = \{e, a\}$, where $a \neq e$ and e is the identity element of G. Then, the following is the Cayley table of G:

$\cdot$	e	a
e	e	a
a	a	e

Table 2: Cayley table of G, where $|G| = 2$

Example 1.14 (Cayley table of G, where $|G| = 3$)**.** Let G be a group such that $G = \{e, a, b\}$, where e, a, b are distinct and e is the identity element of G. Then, the following is a Cayley table of G (try to spot a couple of nice features):

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Table 3: Cayley table of G, where $|G| = 3$

Note that we used the article 'a' to describe the Cayley table, which shows that the Cayley table of a group G, where $|G| = 3$, is not unique. It is easy to see that the following is also a Cayley table of G:

$\cdot$	e	a	b
e	e	a	b
a	a	e	b
b	b	a	e

Table 4: Cayley table of G, where $|G| = 3$

What is the difference between the two Cayley tables?

Example 1.15 (Dummit and Foote p. 22 Question 10)**.** Prove that a finite group is Abelian if and only if its group table is a symmetric matrix.

Solution. We first prove the forward direction. Suppose G is a finite group, say $|G| = n$. Then, $G = \{1_G, g_1, g_2, \ldots, g_{n-1}\}$, where g_i are distinct and neither is the identity element for all $1 \leq i \leq n-1$.

Suppose the group table is some $n \times n$ array, with the $(1,1)$-entry being at the top left and the (n,n)-entry being at the bottom right. For $i \neq j$, the (i, j)-entry is $a_i a_j$, whereas the (j,i)-entry is $a_j a_i$. Since G is Abelian, then $g_i g_j = g_j g_i$ for all distinct i, j. We conclude that the group table is symmetric.

In fact, proving the reverse direction is simple — just work out the steps in reverse. $\square$

Proposition 1.2. Let G be a group. For any $a,b \in G$,

$$\text{there exist unique } x,y \in G \quad \text{such that} \quad ax = b \text{ and } ya = b.$$

Proof. We first prove the existence claim. Set $x = a^{-1}b$. Then, $ax = b$. Similarly, by setting $y = ba^{-1}$, we have $ya = b$. We then prove the uniqueness claim. Here, we will only prove that $x \in G$ such that $ax = b$ is unique. Suppose there exist $x,x' \in G$ such that $ax = b = ax'$. It follows that $x = a^{-1}b = x'$. □

Corollary 1.2 (cancellation laws). Let G be a group. Then, the following hold:

(i) For any $a,u,v \in G$, if $au = av$, then $u = v$

(ii) For any $b,u,v \in G$, if $ub = vb$, then $u = v$

Proof. We will only prove **(i)** as **(ii)** can be proven similar. Given that $au = av$, then multiplying both sides on the left by a^{-1}, it follows that $u = v$. □

Corollary 1.3. For any $a \in G$, the maps

$$G \to G \text{ where } x \mapsto ax \quad \text{and} \quad G \to G \text{ where } x \mapsto xa \quad \text{are bijective.}$$

Definition 1.5 (direct product). Let $(A,\cdot)$ and $(B,*)$ be groups, where $\cdot$ and $*$ are the operations on A and B respectively. The direct product of A and B is the group $A \times B$ with an underlying set

$$A \times B = \{(a,b) : a \in A, b \in B\},$$

equipped with a multiplication map

$$(A \times B) \times (A \times B) \to A \times B \quad \text{where} \quad ((a_1,b_1),(a_2,b_2)) \mapsto (a_1 \cdot a_2, b_1 * b_2),$$

the identity element $1_{A\times B} = (1_A, 1_B)$, and an inversion map

$$A \times B \to A \times B \quad \text{where} \quad (a,b) \mapsto (a,b)^{-1} = \left(a^{-1}, b^{-1}\right).$$

Example 1.16. Take $A = G$ to be any group and $B = \{1\}$ be the trivial group ($B = \{e\}$ works too). Then,

$$A \times B = G \times \{1\} = \{(g,1) : g \in G\}$$

with multiplication for the left component be given by that in G.

Example 1.17. Let $A = B = S_2$ be the symmetric group on 2 elements. In fact, since $|S_2| = 2$, we can also consider A and B to be any group of 2 elements (in fact, 2 is a nice number since it is prime and groups of order prime p, in general, have similar structure — we say that the groups are *isomorphic* and we will learn this in due course).

As $G = \{1, x\}$, then

$$G \times G = \{(1,1),(1,x),(x,1),(x,x)\} \quad \text{which is a group with 4 elements.}$$

Letting $e = (1,1)$, $a = (1,x)$, $b = (x,1)$, $c = (x,x)$, we can construct a Cayley table for $G \times G$ as follows:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Table 5: Group table for $G \times G$

Example 1.18 (Dummit and Foote p. 22 Question 28)**.** Let $(A, \star)$ and $(B, \diamond)$ be groups and let $A \times B$ be their direct product. Verify all the group axioms for $A \times B$:

(a) Prove that the associative law holds: for all $(a_i, b_i) \in A \times B$, $i = 1,2,3$,

$$(a_1,b_1)[(a_2,b_2)(a_3,b_3)] = [(a_1,b_1)(a_2,b_2)](a_3,b_3).$$

(b) Prove that $(1,1)$ is the identity of $A \times B$.

(c) Prove that the inverse of (a,b) is (a^{-1}, b^{-1}).

Solution.

(a) We have

$$\begin{aligned}(a_1,b_1)[(a_2,b_2)(a_3,b_3)] &= (a_1,b_1)(a_2 \star a_3, b_2 \diamond b_3)\\ &= (a_1 * (a_2 * a_3), b_1 \diamond (b_2 \diamond b_3))\\ &= ((a_1 \star a_2) \star a_3, (b_1 \diamond b_2) \diamond b_3) \quad \text{by associativity of } \star \text{ and } \diamond\\ &= [(a_1 \star a_2),(b_1 \diamond b_2)](a_3,b_3)\\ &= [(a_1,b_1)(a_2,b_2)](a_3,b_3)\end{aligned}$$

(b) Suppose (a_0, b_0) is the identity of $A \times B$. Then, for any $(a,b) \in A \times B$, we must have

$$(a_0,b_0)(a,b) = (a,b)(a_0,b_0) = (a,b).$$

This yields

$$a_0 \star a = a \star a_0 = a \text{ and } b_0 \diamond b = b \diamond b_0 = b \quad \text{so} \quad a$$

Since A and B are groups, by the cancellation law (Corollary 1.2), we have $a_0 = b_0 = 1$, so $(1,1)$ is indeed the identity of $A \times B$.

(c) Let $(a,b) \in A \times B$. Suppose the inverse of (a,b) is (c,d). Then,

$$(a,b)(c,d) = (1,1) \quad \text{so} \quad (a \star c, b \diamond d) = (1,1).$$

We must have $a \star c = 1$ and $b \diamond d = 1$. Since A and B are groups, the inverses of a and b exist, which are a^{-1} and b^{-1} respectively. □

Example 1.19 (Dummit and Foote p. 23 Question 29). Prove that

$$A \times B \text{ is an Abelian group} \quad \text{if and only if} \quad \text{both } A \text{ and } B \text{ are Abelian.}$$

Solution. We first prove the forward direction. Suppose $A \times B$ is an Abelian group, i.e.

$$\text{for any } (a_1,b_1),(a_2,b_2) \in A \times B \quad \text{we have} \quad (a_1a_2, b_1b_2) = (a_2a_1, b_2b_1)$$

So, $a_1a_2 = a_2a_1$ and $b_1b_2 = b_2b_1$. We conclude that both A and B are Abelian.

We then prove the reverse direction. Suppose A and B are Abelian groups. Then, for any $a_1, a_2 \in A$ and $b_1, b_2 \in B$, we have

$$a_1a_2 = a_2a_1 \quad \text{and} \quad b_1b_2 = b_2b_1.$$

It follows that

$$\text{for any } (a_1,b_1),(a_2,b_2) \in A \times B \quad \text{we have} \quad (a_1a_2, b_1b_2) = (a_2a_1, b_2b_1),$$

which concludes that $A \times B$ is Abelian. □

Definition 1.6. For any $x \in G$, define

$$x^0 = 1 \quad \text{to be the identity of } G$$

and for any $n \in \mathbb{Z}_{\geq 0}$, we define

$$x^{n+1} = x^n \cdot x \quad \text{and} \quad x^{-n} = (x^n)^{-1} \quad \text{recursively.}$$

Definition 1.6 provides a formal way of recursively defining exponentiation — the informal way is as follows: for any $n \in \mathbb{Z}^+$, we define

$$x^n = x \cdot x \cdot \ldots \cdot x \quad \text{and} \quad x^{-n} = (x^n)^{-1} = x^{-1} \cdot x^{-1} \cdot \ldots \cdot x^{-1}$$

Definition 1.7 (order of group). Let $x \in G$. If

$$\text{there exists } n \in \mathbb{Z}^+ \quad \text{such that } x^n = 1, \quad \text{then } x \text{ is of finite order}$$

and the order of x is the smallest $n \in \mathbb{Z}^+$ such that $x^n = 1$. We denote this by $|x|$ or $\operatorname{ord}(x)$.

Otherwise, if

$$\text{for any } n \in \mathbb{Z}^+ \quad \text{we have } x^n \neq 1, \quad \text{then } x \text{ is of infinite order}$$

as no positive power of x is the identity.

Remark 1.2. One should not

confuse	the notion of	the order of an element $x \in G$	with the
	the notion of	the order of a finite group G	

We return to Examples 1.12, 1.13, and 1.14.

Example 1.20 (Cayley table of G, where $|G| = 1, 2, 3$)**.** We first consider the case when $|G| = 1$. Then, G has a single element e. It is of order 1 since $e^1 = 1$.

$\cdot$	e
e	e

Table 6: Cayley table of G, where $|G| = 1$

Next, we consider the case when $|G| = 2$. Then, G has two distinct elements e and a. Again, the identity element e is of order 1, whereas a is of order 2 since $a^2 = e$.

$\cdot$	e	a
e	e	a
a	a	e

Table 7: Cayley table of G, where $|G| = 2$

When $|G| = 3$, G has three distinct elements e, a, and b. Again, the identity element e is of order 1, whereas a and b are of order 3.

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Table 8: Cayley table of G, where $|G| = 3$

Example 1.21 (Dummit and Foote p. 22 Question 16)**.** Let x be an element of G. Prove that $x^2 = 1$ if and only if $|x|$ is either 1 or 2.

Solution. We only prove the forward direction as the proof of the reverse direction is trivial. Suppose $x^2 = 1_G$. Then, $|x| \leq 2$. By definition, $|x| \geq 1$. Hence, $|x|$ is either 1 or 2. $\square$

Example 1.22 (Dummit and Foote p. 22 Question 17)**.** Let x be an element of G. Prove that if $|x| = n$ for some positive integer n, then $x^{-1} = x^{n-1}$.

Solution. Given that $|x| = n$, then there exists $n \in \mathbb{Z}^+$ such that $x^n = 1_G$. Since $x \in G$, then its inverse $x^{-1} \in G$ exists, i.e. $x \cdot x^{-1} = 1_G$. Left multiplying both sides by x^{n-1}, we obtain

$$\begin{aligned} x^{n-1} \cdot x \cdot x^{-1} &= x^{n-1} \cdot 1_G \\ \left(x^{n-1} \cdot x\right) \cdot x^{-1} &= x^{n-1} \quad \text{by associativity} \end{aligned}$$

Since $x^{n-1} \cdot x = 1_G$, it follows that $x^{n-1} = x^{-1}$. □

Example 1.23 (Dummit and Foote p. 22 Question 21). Let G be a finite group and let x be an element of order n. Prove that if n is odd, then $x = \left(x^2\right)^k$ for some k.

Solution. Since n is odd, there exists $k \in \mathbb{Z}$ such that $n = 2k - 1$. As $x^n = 1$, then $x^{2k-1} = 1$, so $x = x^{2k}$. □

Example 1.24 (Dummit and Foote p. 22 Question 22). If x and g are elements of the group G, prove that $|x| = \left|g^{-1}xg\right|$. Deduce that $|ab| = |ba|$ for all $a, b \in G$.

Solution. Suppose $|x| = n$. Then, there exists $n \in \mathbb{Z}^+$ such that $x^n = 1$. So,

$$\left(g^{-1}xg\right)^n = \left(g^{-1}xg\right) \cdot \left(g^{-1}xg\right) \cdot \ldots \cdot \left(g^{-1}xg\right) = g^{-1}gx^ng = g^{-1}g = 1.$$

So, $\left|gxg^{-1}\right| \geq n$.

Next, suppose $\left|gxg^{-1}\right| = n$. Then, there exists $n \in \mathbb{Z}^+$ such that $\left(gxg^{-1}\right)^n = 1$. So, $x^n = 1$. It follows that $|x| \geq n$. As such, $|x| = \left|gxg^{-1}\right|$.

If $|x|$ or $\left|gxg^{-1}\right|$ is infinite, the statement is trivial. Lastly, replace x with ab. Then, suppose $g^{-1}xg = ba$, i.e. $g^{-1}abg = ba$. We can set $g = a$, so it follows that $|ab| = |ba|$ for all $a, b \in G$. □

Example 1.25 (Dummit and Foote p. 22 Question 23). Suppose $x \in G$ and $|x| = n < \infty$. If

$$n = st \text{ for some positive integers } s \text{ and } t, \quad \text{prove that } |x^s| = t.$$

Solution. Say $|x| = n = st$ for some positive integers s and t. Then, $x^{st} = 1$, i.e. $(x^s)^t = 1$. The result follows. □

Example 1.26 (Dummit and Foote p. 22 Question 20). For x an element in G, show that x and x^{-1} have the same order.

Solution. We shall consider two cases — if $|x|$ is finite and if $|x|$ is infinite.

If $|x|$ is finite, i.e. $|x| = n$, then we have $x^n = 1_G$. So,

$$x^n \cdot \left(x^{-1}\right)^n = 1_G \cdot \left(x^{-1}\right)^n \quad \text{which implies} \quad x^n \cdot x^{-n} = \left(x^{-1}\right)^n.$$

As such, $\left(x^{-1}\right)^n = 1_G$, which implies x^{-1} is also of finite order.

For the second case, if $|x|$ is infinite, we shall prove by contradiction that $\left|x^{-1}\right|$ is also infinite. Suppose on the contrary that $\left|x^{-1}\right|$ is finite. Then, there exists $k \in \mathbb{Z}^+$ such that $\left(x^{-1}\right)^k = 1_G$. So, $\left(x^k\right)^{-1} = 1_G$. This implies $x^k = 1_G$ as the only element in a group which has the inverse as its identity is the identity element 1_G, leading to a contradiction! □

Example 1.27 (Dummit and Foote p. 60 Question 20). Let p be a prime and $n \in \mathbb{Z}^+$. Show that if x is an element of the group G such that $x^{p^n} = 1$, then

$$|x| = p^m \quad \text{for some } m \leq n.$$

Solution. We know that $|x| \leq p^n$, so either $|x| = p^m$ or $|x| = p^{n-m}$. Note that $n \geq m$ implies $n - m \geq 0$, so the latter is valid too. As such, the order of x is either p^m or p^{n-m}. Since $n - m$ is arbitrary, it can be replaced by $\widetilde{m}$, where $\widetilde{m} \leq n$. □

Lemma 1.1. Let G be a group. Suppose $x \in G$ has infinite order. For distinct $j, k \in \mathbb{Z}$, we have $x^j \neq x^k$.

Corollary 1.4. Every element of a finite group G has finite order.

The converse of Corollary 1.4 is not true. That is, if every element of G has finite order, it is possible for G to be an infinite group. For example, consider the infinite group $G = (\mathbb{Q}/\mathbb{Z}, +)$. The elements are of the form $\mathbb{Z} + p/q$, where $p, q \in \mathbb{Z}$ but $q \neq 0$. The order of each element in G is at most q since

$$q\left(\mathbb{Z} + \frac{p}{q}\right) = q\mathbb{Z} + p \quad \text{which is an integer.}$$

However, there are infinitely many numbers which are in $\{\mathbb{Z} + p/q\}$.

Example 1.28 (Dummit and Foote p. 23 Question 30)**.** Prove that the elements $(a, 1)$ and $(1, b)$ of $A \times B$ commute and deduce that the order of (a, b) is the least common multiple of $|a|$ and $|b|$.

Solution. Suppose $(A, \star)$ and $(B, \diamond)$ are groups. Then,

$$(a,1)(1,b) = (a \star 1, 1 \diamond b) = (a,b) = (1 \star a)(b \diamond 1) = (1,b)(a,1)$$

so $(a, 1)$ and $(1, b)$ commute. For the second part, we note that $a^{|a|} = 1_A$ and $b^{|b|} = 1_B$. Suppose the order of (a, b) is n. Then, $(a,b)^n = 1_{A \times B}$, i.e. $(a^n, b^n) = (1_A, 1_B)$. It follows that $n = \operatorname{lcm}(|a|, |b|)$. □

Example 1.29 (Dummit and Foote p. 23 Question 31)**.** Prove that any finite group G of even order contains an element of order 2.

Hint: Let $t(G)$ be the set $\{g \in G : g \neq g^{-1}\}$. Show that $t(G)$ has an even number of elements and every non-identity element of $G \setminus t(G)$ has order 2.

Solution. As mentioned, let $t(G) = \{g \in G : g \neq g^{-1}\}$. Then, $t(G)$ must have an even number of elements since

$$g \in t(G) \quad \text{if and only if} \quad g^{-1} \in t(G)$$

where g, g^{-1} are distinct. Since G has an even number of elements, then $G \setminus t(G)$ also has an even number of elements. Since $e \notin t(G)$, then $G \setminus t(G)$ is non-empty, i.e. there exists a non-identity element $a \in G \setminus t(G)$, so $a = a^{-1}$. Hence, $a^2 = e$. □

Example 1.30 (Dummit and Foote p. 23 Question 32)**.** If x is an element of finite order n in G, prove that the elements $1, x, x^2, \ldots, x^{n-1}$ are all distinct. Deduce that $|x| \leq |G|$.

Solution. Let $x \in G$ be such that $|x| = n$. Suppose on the contrary that $1, x, x^2, \ldots, x^{n-1}$ are not all distinct. Then, there exist distinct $i, j \in \{1, \ldots, n-1\}$ such that $x^i = x^j$. So, $x^{i-j} = 1_G$. However, $i - j \leq n - 1$, which is a contradiction. Thus, the elements are all distinct. Since G is a group and it must contain all powers of x (by closure property), it follows that $|x| \leq |G|$. □

Example 1.31 (Dummit and Foote p. 23 Question 33)**.** Let x be an element of finite order n in G.

(a) Prove that if n is odd, then $x^i \neq x^{-i}$ for all $i = 1, 2, \ldots, n-1$.

(b) Prove that if $n = 2k$ and $1 \leq i < n$, then $x^i = x^{-i}$ if and only if $i = k$.

Solution.

(a) Suppose on the contrary that there exists $1 \leq i \leq n-1$ such that $x^i = x^{-i}$. So, $x^2 = 1_G$. If $2i > n$, then there exists $k \in \mathbb{Z}$ such that $2i = n+k$. So, $x^{n+k} = 1_G$, which implies $x^k = 1_G$. As

$$n = 2i - k \leq 2(n-1) - k = 2n - 2 - k < 2n - k,$$

then $n > k$. As such, the order of x is at most k, where $k < n$. This leads to a contradiction.

(b) We first prove the forward direction. Suppose $x^i = x^{-i}$, which implies $x^{2i} = 1_G$. Since $x^n = x^{2k} = 1_G$, then $2i = 2k$, so $i = k$.

For the reverse direction, suppose $n = 2k$, $1 \leq i < n$ and $i = k$. Then, $x^i \cdot x^i = x^{2i} = x^{2k} = x^n = 1_G$. □

Example 1.32 (Dummit and Foote p. 23 Question 34)**.** If x is an element of infinite order in G, prove that the elements x^n, $n \in \mathbb{Z}$, are all distinct.

Solution. Suppose on the contrary that there exists a pair of identical elements, i.e. distinct $i, j \in \mathbb{Z}$ such that $x^i = x^j$. Then, $x^{i-j} = 1_G$, which contradicts the fact that $x \in G$ is finite. □

Example 1.33 (Dummit and Foote p. 23 Question 35)**.** If x is an element of finite order n in G, use the division algorithm to show that any integral power of x equals one of the elements in the set $\{1, x, x^2, \ldots, x^{n-1}\}$ (so these are all the distinct elements of the cyclic subgroup of G generated by x).

Solution. Let $k \in \mathbb{Z}$ be arbitrary. By the division algorithm, there exist $q, r \in \mathbb{Z}$, where $0 \leq r < n$, such that $k = qn + r$. So,

$$x^k = x^{qn+r} = (x^n)^q \cdot x^r = x^r.$$

Since $0 \leq r < n$, then $x^r \in \left\{1, x, x^2, \ldots, x^{n-1}\right\}$. □

Example 1.34 (Dummit and Foote p. 23 Question 36)**.** Assume $G = \{1, a, b, c\}$ is a group of order 4 with identity 1. Assume also that G has no elements of order 4 (so by Example 1.30, every element has order ≤ 3). Use the cancellation laws to show that there is a unique group table for G. Deduce that G is abelian.

Solution. The non-identity elements of G are either of order 2 or 3. In Example 1.29, we mentioned that every finite group of even order contains an element of order 2. Without loss of generality, suppose this element is a. Then, $a^2 = 1$. Note that $ab \neq 1$, otherwise it would imply that $b = a^{-1} = a$. In a similar fashion, $ab \neq b$, otherwise $a = 1$. Hence, it forces $ab = c$.

In a similar fashion, one can deduce that $ba = c$ and $ac = ca = b$. We now obtain an alternative expression for b^2. It can either be 1 or a. If it is a, then it implies $b^4 = 1$, which is a contradiction since every element must have order at most 3. So, $b^2 = 1$ ($c^2 = 1$ similarly).

As such, the group table is unique. We are now in position to construct the group/Cayley table for G.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	e	b	a	e

Table 9: Cayley table of G

Since the group table is symmetric about the main diagonal, we infer that G is Abelian. □

1.2 Dihedral Groups

Definition 1.8 (dihedral group). Let $n \in \mathbb{Z}^+$. The dihedral group of order $2n$ is the group D_{2n} (some authors would write D_n) with underlying set

$$D_{2n} = \left\{1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\right\} \quad \text{which has } 2n \text{ pairwise distinct elements.}$$

So, every element of D_{2n} can be uniquely written as

$$s^k r^i \quad \text{with} \quad k = 0 \text{ or } 1 \quad \text{and } 0 \leq i \leq n-1$$

with product determined by the following relations:

$$r^n = s^2 = 1 \quad \text{and} \quad rs = sr^{-1}$$

For $n \geq 3$, we have a nice geometric interpretation of the dihedral group D_{2n}. D_{2n} is the group of rigid motions (or symmetries) of a regular n-gon. On a plane, we fix a regular n-gon centred at the origin. Label the vertices consecutively from 1 to n clockwise/anticlockwise. Then, r and s denote the following:

$$r = \text{rotation clockwise/anticlockwise respectively about the origin} \quad \text{through } 2\pi/n \text{ radians}$$
$$s = \text{reflection about the fixed line} \quad \text{through a vertex and the origin}$$

Figure 1 depicts rotation and reflection in a regular pentagon, D_{10}.

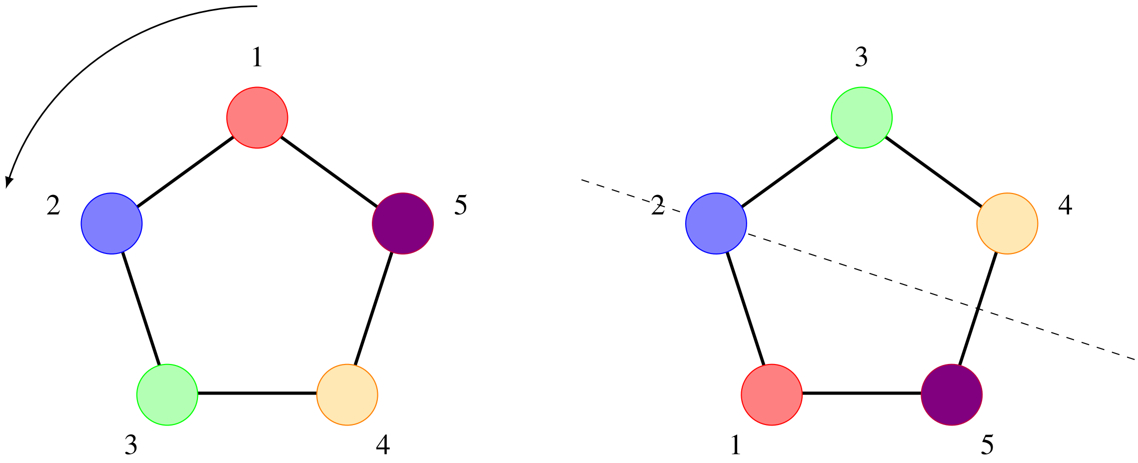


Figure 1: Rotation and reflection in a regular pentagon, D_{10}

For those who have difficult remembering the relation $rs = sr^{n-1}$ in the dihedral group D_{2n}, try to think of either $rs = sr^{n-1}$ or $sr = rs^{n-1}$ first. So, each expression contains an rs, an sr (*commute the elements informally*), and an exponent of $n-1$ somewhere. The question is where do we insert this exponent? If we consider the latter, then it definitely leads to a problem because if let's say $n = 5$, then $n-1 = 4$ so $s^{n-1} = s^4 = \left(s^2\right)^2 = e$. However, when we write the relations of the group, they must be *simplified*, i.e. instead of writing $s^4 = e$, having $s^2 = e$ is sufficient†!

Proposition 1.3. In D_{2n}, the following properties hold:

(i) $1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}$ are pairwise distinct

(ii) $r^n = s^2 = 1$

(iii) $rs = sr^{-1}$

Example 1.35 (dihedral group of an equilateral triangle D_6)**.** The dihedral group D_6 represents the symmetries of an equilateral triangle. This group has six elements: three rotations e, r, r^2 and three reflections s, sr, sr^2. Here,

r denotes a clockwise rotation about the origin through an angle of 120° and

s denotes a reflection across a vertical axis

Two obvious ways in which the elements interact are $r^3 = e$ and $s^2 = e$. Moreover, one should verify that sr and sr^2 are indeed reflections.

On page 27 of the Dummit and Foote textbook, Question 1**(a)** asks the reader to compute the order of each element in D_6. It is obvious that we have the following:

$$|e| = 1 \quad |r| = 3 \quad \left|r^2\right| = 3 \quad |s| = 2 \quad |sr| = 2 \quad \left|sr^2\right| = 2$$

Example 1.36 (Dummit and Foote p. 27 Question 2)**.** Show that if x is any element of D_{2n} which is not a power of r, then $rx = xr^{-1}$.

† Geometrically, this just means reflecting about the same axis two times yields the original figure.

$\cdot$	e	r	r^2	s	sr	sr^2
e	e	r	r^2	s	sr	sr^2
r	r	r^2	e	sr^2	s	sr
r^2	r^2	e	r	sr	sr^2	s
s	s	sr	sr^2	e	r^2	r
sr	sr	sr^2	s	r	e	r^2
sr^2	sr^2	s	sr	r^2	r	e

Table 10: Cayley table of D_6

Solution. Since x is not a power of r, then we can write $x = sr^q$. Note that we do not have to attach any exponent to s since the exponent can either take the value 0 or 1. So,

$$rx = rsr^q = (rs)\,r^q = \left(sr^{-1}\right)r^q = sr^{q-1} = (sr^q)\,r^{-1} = xr^{-1}$$

so it follows that $rx = xr^{-1}$. $\square$

Example 1.37 (Dummit and Foote p. 27 Question 3)**.** Show that every element of D_{2n} which is not a power of r has order 2. Deduce that D_{2n} is generated by the two elements s and sr, both of which have order 2.

Solution. By Example 1.36, we can write such an element $x \in D_{2n}$ as $x = sr^q$. One can use induction to deduce the first claim, i.e. $|x| = 2$. Alternatively, observe that

$$(sr^q)\,(sr^q) = \left(sr^{q-1}\right)(rsr^q) = \left(sr^{q-1}\right)\left(sr^{q-1}\right) = \ldots = s^2 = 1.$$

Now, the elements of D_{2n} are

$$1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}.$$

Each r^q can be written as $(s\,(sr))^q$. Also, each sr^q can be written as $(s\,(sr))^q$. Since $|s| = 2$, it follows that $|sr| = 2$ as well. $\square$

Example 1.38 (Dummit and Foote p. 28 Question 6)**.** Let x and y be elements of order 2 in any group G. Prove that if $t = xy$, then $tx = xt^{-1}$ (so that if $n = |xy| < \infty$, then x and t satisfy the same relations in G as s and r do in D_{2n}).

Solution. Since x and y are elements of order 2, then $x^2 = y^2 = 1_G$. As such, $x = x^{-1}$ and $y = y^{-1}$. Given that $t = xy$, then

$$tx = xyx = x\,(yx) = x\left(y^{-1}x^{-1}\right) = x\,(xy)^{-1} = xt^{-1}$$

and the result follows. $\square$

1.3
Symmetric Groups

Recall from MA1100 the following definitions (Definitions 1.9 and 1.10):

Definition 1.9 (bijective map)**.** Let X and Y be sets. A map $\sigma : X \to Y$ is bijective if and only if

it is injective, i.e. for all $x_1, x_2 \in X$ and $\sigma(x_1) = \sigma(x_2)$ in Y implies $x_1 = x_2$ in X and

it is surjective, i.e. for all $y \in Y$, there exists $x \in X$ such that $\sigma(x) = y$

Definition 1.10 (invertible map)**.** Let X and Y be sets. A map $\sigma : X \to Y$ is invertible if and only if

$$\text{there exists a map } \tau : Y \to X \quad \text{such that } \tau \circ \sigma = \mathrm{id}_X \text{ and } \sigma \circ \tau = \mathrm{id}_Y$$

in which case τ is uniquely determined by σ, called the inverse of σ and denoted by σ^{-1}. Thus,

$$\sigma^{-1} \circ \sigma = \mathrm{id}_X \quad \text{and} \quad \sigma \circ \sigma^{-1} = \mathrm{id}_Y .$$

We have the following theorem based on Definitions 1.9 and 1.10:

Theorem 1.1. For any sets X and Y and any $\sigma \in \mathrm{Maps}(X,Y)$, we have

$$\sigma \text{ is invertible} \quad \text{if and only if} \quad \sigma \text{ is bijective.}$$

Definition 1.11 (permutation group $\mathrm{Perm}(\Omega)$)**.** Let Ω be any set. Define

$$\mathrm{Perm}(\Omega) = S_\Omega = \{\sigma \in \mathrm{Maps}(\Omega,\Omega) : \sigma \text{ is bijective}\} \quad \text{to be the set of bijections from } \Omega \text{ to itself.}$$

The elements of $\mathrm{Perm}(\Omega)$ are called the permutations of Ω.

Proposition 1.4 (permutation group $\mathrm{Perm}(\Omega)$)**.** Under the composition of maps, $\mathrm{Perm}(\Omega)$ is a group, which forms a group. This is known as the composition of the set Ω.

Proof. We verify **(i)**, **(ii)**, and **(iii)** of Definition 1.1. Firstly, composition $\circ$ is associative so **(i)** is satisfied. Next, id_Ω, which is the identity map on Ω, is the identity element of the permutation group so **(ii)** is satisfied. Lastly, $\sigma \mapsto \sigma^{-1}$ is the inverse operation, so **(iii)** is satisfied. □

Definition 1.12 (symmetric group S_n)**.** For any positive integer n, define

$$S_n = \mathrm{Perm}(\{1,\ldots,n\}) \quad \text{to be the symmetric group of degree } n.$$

By Definition 1.11, S_n is the set of all bijections from $\{1,\ldots,n\}$ to itself.

Definition 1.13 (Cauchy's two-line notation)**.** For any permutation $\sigma \in S_n$, we write

$$\sigma = \begin{pmatrix} 1 & \ldots & n \\ \sigma(1) & \ldots & \sigma(n) \end{pmatrix}$$

so under σ, we have $1 \mapsto \sigma(1)$, and so on, up to and including the relationship between the entries in the last column, where $n \mapsto \sigma(n)$. This way of representing any permutation σ is known as Cauchy's two-line notation.

Example 1.39. The matrix

$$\begin{pmatrix} 1 & \ldots & n \\ a_1 & \ldots & a_n \end{pmatrix} \quad \text{denotes the permutations of } \{1,\ldots,n\} \quad \text{where } i \mapsto a_i.$$

As an exercise, one can construct the Cayley tables for the symmetric groups S_1, S_2, S_3. In relation to Definition 1.3, one notes that

$$|S_1| = 1 \quad \text{and} \quad |S_2| = 2 \quad \text{and} \quad |S_3| = 6$$

since S_n denotes the set of permutations of $\{1, \ldots, n\}$. As each Cayley table of a finite group with n elements is an $n \times n$ square (Definition 1.4), then we would expect the table to have

$$n^2 \text{ elements} \quad \text{other than the row and column headers.}$$

We now introduce the notion of the cycle decomposition of a permutation.

Definition 1.14 (cycle decomposition)**.** Let

$$a_1, \ldots, a_m \quad \text{be} \quad \text{an ordered list of pairwise distinct elements of} \quad \{1, \ldots, n\}, \quad \text{where } m \leq n.$$

The cycle $(a_1\ a_2\ \ldots\ a_m) \in S_n$ is the permutation which sends

$$a_i \text{ to } a_{i+1} \text{ for } 1 \leq i \leq m-1 \quad \text{and} \quad a_m \text{ to } a_1$$

and fixes all other integers in $\{1, \ldots, n\} \setminus \{a_1, \ldots, a_m\}$. This can be represented visually as follows:

$$\begin{tikzcd} a_1 \arrow[r] & a_2 \arrow[r] & \cdots \arrow[r] & a_m \arrow[lll, bend left] \end{tikzcd}$$

Example 1.40. $(2\ 1\ 3) \in S_3$ can be described as follows using Cauchy's two-line notation:

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \text{where} \quad 2 \mapsto 1 \quad 1 \mapsto 3 \quad 3 \mapsto 2$$

It is important that we mention that $(2\ 1\ 3) \in S_3$. If suppose $(2\ 1\ 3) \in S_4$, then it would imply that the element 4 is fixed, i.e. $4 \mapsto 4$. Here is the Cauchy two-line notation denoting the permutation.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \quad \text{where} \quad 2 \mapsto 1 \quad 1 \mapsto 3 \quad 3 \mapsto 2$$

The composition of permutations in S_n is carried out from right to left.

Example 1.41 (composition of permutations)**.** Consider the permutations $(1\ 2), (1\ 3) \in S_3$. Then, for the permutation $(1\ 2) \circ (1\ 3)$, we have the following sequence of maps:

$$1 \mapsto 3 \quad \text{and} \quad 3 \mapsto 1 \mapsto 2 \quad \text{and} \quad 2 \mapsto 1$$

so using Cauchy's two-line notation, the permutation can be written as

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2).$$

In fact, the symbol $\circ$ can be omitted, i.e. we can write

$$(1\ 2)(1\ 3) \quad \text{in place of} \quad (1\ 2) \circ (1\ 3).$$

Similarly, we have

$$(1\ 3) \circ (1\ 2) = (1\ 3)(1\ 2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3).$$

So, we see that $(1\ 2), (1\ 3) \in S_3$ do not commute. In general, Theorem 1.2 mentions a generalisation of this result, where the subscript 3 can be replaced with some arbitrary positive integer $n \geq 3$.

Theorem 1.2. For all $n \geq 3$, S_n is a non-Abelian group.

Note that the numbers in a cycle can be cyclically permuted without altering the permutation, i.e.

$$\begin{aligned}(a_1\ a_2\ \dots\ a_m) &= (a_2\ a_3\ \dots\ a_m\ a_1) \\ &= (a_3\ a_4\ \dots\ a_m\ a_1\ a_2) \\ &= \dots \\ &= (a_m\ a_1\ a_2\ \dots\ a_{m-1})\end{aligned}$$

for which the above expressions hold in S_n, where $m \leq n$. By convention, the smallest number in the cycle is usually written first.

Example 1.42. It is preferred to write $(1\ 3\ 2)$ instead of $(3\ 2\ 1)$ or $(2\ 1\ 3)$.

Definition 1.15 (length of cycle)**.** The length of a cycle is the number of integers that appear in it. We say that

$$\text{an } l\text{-cycle} \quad \text{is} \quad \text{a cycle of length } l.$$

By convention, the identity permutation of S_n, is written simply as id or ε. Moreover, 1-cycles such as $(1), (2), \dots (n)$ are not written.

Example 1.43 (Dummit and Foote p. 33 Question 10)**.** Prove that if σ is the m-cycle $(a_1\, a_2\, \dots\, a_m)$, then for all $i \in \{1, 2, \dots, m\}$, $\sigma^i(a_k) = a_{k+i}$, where $k+i$ is replaced by its least residue mod m when $k+i > m$. Deduce that $|\sigma| = m$.

Solution. To prove the first claim that $\sigma^i(a_k) = a_{k+i}$, we shall use induction. When $i = 1$, it is clear that $\sigma(a_k) = a_{k+1}$ since σ cyclically permutes $a_1, \dots, a_m$. So, the base case is true. Now, suppose that the proposition holds for some positive integer $i = r$, i.e. $\sigma^r = (a_k) = a_{k+r}$. We wish to prove that $\sigma^{r+1}(a_k) = a_{k+r+1}$.

So,

$$\sigma^{r+1}(a_k) = \sigma(\sigma^r(a_k)) = \sigma(a_{k+r}) = a_{k+r+1},$$

where we have used the subtle yet important fact that $k+r$ and $k+r+1$ are replaced by their least residues modulo m. So, the statement is proven by induction.

We then justify that $|\sigma| = m$. Note that for $1 \leq i < m$, we have $\sigma^i(a_k) = a_{k+i} \neq a_k$, so σ^i is not equal to the identity permutation. However, $\sigma^m(a_k) = a_k$ since the index $k+m$ is replaced by its least residue modulo m, which is k. It follows that $|\sigma| = m$. □

Example 1.44 (Dummit and Foote p. 33 Question 11)**.** Let σ be the m-cycle $(1\,2\, \dots\, m)$. Show that

$$\sigma^i \text{ is also an } m\text{-cycle} \quad \text{if and only if} \quad i \text{ is relatively prime to } m.$$

Solution. For the forward direction, suppose σ^i is an m-cycle. Note that $\sigma^i(1) = i+1$, $\sigma^i(2) = i+2$ and so on. Moreover, $\sigma^i(m-i) = m$, so $\sigma^i(m+1-i) = 1$. Hence, for any $1 \leq k \leq m$,

$$\sigma^i : S_m \to S_m \quad \text{where} \quad k \mapsto k+i \pmod m$$

These elements are distinct if and only if $k+ia$ and $k+ib$ are distinct for any distinct a and b, i.e. if and only if $k+ia$ is not congruent to $k+ib$ modulo m for any $1 \leq a, b \leq m$. Hence, m does not divide $i(a-b)$. This is equivalent to saying that $\gcd(i,m) = 1$. ☐

Definition 1.16 (transposition). A transposition is a 2-cycle.

Example 1.45 (Dummit and Foote p. 33 Question 16). Show that if $n \geq m$, then the number of m-cycles in S_n is given by

$$\frac{n(n-1)(n-2)\ldots(n-m+1)}{m}.$$

Hint: Count the number of ways of forming an m-cycle and divide by the number of representations of a particular m-cycle.

Solution. By Definition 1.15, an m-cycle is defined to be a cycle of length m, i.e.

$$(a_1 \ldots a_m) \quad \text{where} \quad a_1, \ldots, a_m \in \{1, \ldots, n\} \text{ which are all distinct.}$$

There are n choices for a_1. Consequently, there are $n-1$ choices for a_2. Repeating this, there are $n-m+1$ choices for a_m. By the multiplication principle, the number of ways to form an m-cycle is

$$n(n-1)(n-2)\ldots(n-m+1),$$

which is precisely the numerator of the expression we wish to deduce. Now, it suffices to show that the number of representations of a particular m-cycle is m. It is not difficult to see that the m-cycles

$$(a_1\, a_2 \ldots a_{m-1}\, a_m), (a_2\, a_3 \ldots a_{m-1}\, a_m\, a_1), \ldots (a_m\, a_1\, a_2 \ldots a_{m-2}\, a_{m-1}) \quad \text{are the identical,}$$

and there are m of them. Hence, dividing the earlier expression by m, the result follows. ☐

Definition 1.17 (disjoint cycles). Two cycles are

$$\text{disjoint} \quad \text{if and only if} \quad \text{they have no numbers in common.}$$

Example 1.46. In S_4, the transpositions $(1\ 2)$ and $(3\ 4)$ are disjoint.

Proposition 1.5 (disjoint cycles commute). Let σ and τ be two disjoint cycles of S_n. Then,

$$\sigma \text{ and } \tau \quad \text{commute.}$$

To put it more explicitly, if $a_1, \ldots, a_{m_1}, a_{m_1+1}, \ldots, a_{m_2} \in \{1, \ldots, n\}$ are pairwise distinct, then

$$(a_1\ \ldots\ a_{m_1})(a_{m_1+1}\ \ldots\ a_{m_2}) = (a_{m_1+1}\ \ldots\ a_{m_2})(a_1\ \ldots\ a_{m_1}),$$

where we can let $\sigma = (a_1\ \ldots\ a_{m_1})$ and $\tau = (a_{m_1+1}\ \ldots\ a_{m_2})$.

Example 1.47 (Dummit and Foote p. 33 Question 14). Let p be a prime. Show that an element has order p in S_n if and only if its cycle decomposition is a product of commuting p-cycles. Show by an explicit example that this need not be the case if p is not prime.

Solution. We first prove the forward direction. Suppose $\sigma \in S_n$ is of order p. Consider the cycle decomposition of σ, say there exist $\tau_1, \ldots, \tau_m \in S_n$ such that

$$\sigma = \tau_1 \ldots \tau_m \quad \text{where the } \tau_i\text{'s are disjoint.}$$

By Proposition 1.5, we know that disjoint cycles commute. So,

$$\sigma^2 = (\tau_1 \ldots \tau_m)^2 = \tau_1^2 \ldots \tau_m^2 \quad \text{so in general} \quad \sigma^p = \tau_1^p \ldots \tau_m^p.$$

Since $|\sigma| = p$, then σ^p is the identity permutation of S_n, i.e. τ_i^p is the identity permutation on S_n for all $1 \leq i \leq n$. So, the length of each cycle τ_i divides p, which means each τ_i is either the identity permutation or of order p. The forward direction follows.

As for the reverse direction, suppose the cycle decomposition of σ is a product of commuting p-cycles, where p is prime, i.e.

$$\sigma = \tau_1 \ldots \tau_m \quad \text{where the } \tau_i\text{'s are disjoint.}$$

So, $\sigma^p = \tau_1^p \ldots \tau_m^p$ since the p-cycles commute. As each τ_i is a p-cycle, it follows that τ_i is the identity permutation on S_n. Hence, $|\sigma| \leq p$. However, τ_i^j is not the identity permutation for all $j < p$, so $|\sigma| \geq p$. It follows that $|\sigma| = p$.

We then prove that the original statement may not hold if p is not prime. Choose $p = 6$ and $n = 6$. Then, $\sigma = (1\,2)(3\,4\,5)$ is of order 6 in S_6. However, $(1\,2)(3\,4\,5)$ cannot be written as a product of commuting 6-cycles since each 6-cycle must utilise all 6 elements of $\{1, \ldots, 6\}$, however 6 does not appear in the permutation $(1\,2)(3\,4\,5)$. □

Example 1.47 is a generalisation of Question 13 of the exercise set in the Dummit and Foote textbook as the case where $p = 2$ is discussed. Since 2 is a prime, both implications hold.

Example 1.48 (Dummit and Foote p. 34 Question 17)**.** Show that if $n \geq 4$, then the number of permutations in S_n which are the product of two disjoint 2-cycles is

$$\frac{n(n-1)(n-2)(n-3)}{8}.$$

Solution. Let $(a_r\,a_s), (a_i\,a_j) \in S_n$ be two disjoint 2-cycles. Their product is $(a_r\,a_s)(a_i\,a_j)$. All other elements are fixed under the permutation. Note the following sequence of events:

$$\begin{aligned} &\text{there are } n \text{ choices for } r \quad \text{so} \quad \text{there are } n-1 \text{ choices for } s \\ &\text{there are } n-2 \text{ choices for } i \quad \text{so} \quad \text{there are } n-3 \text{ choices for } j \end{aligned}$$

Note that the choice of the pair (r, s) is independent of (i, j) but the choice of each element in the pair is dependent on the choice of the other element.

Since each pair (r, s) and (i, j) can be arranged in 2 ways each (divide by a factor of 2×2) and the order of the 2-cycles does not matter, we divide by another factor of 2. Hence, the total quantity that we divide by is $2 \times 2 \times 2 = 8$. The result follows. □

Theorem 1.3 (cycle decomposition). Every element $\sigma \in S_n$ can be written as a product of pairwise disjoint cycles (called a cycle decomposition of σ) which is unique up to the following properties:

(i) Cyclic permutation of the numbers in each cycle

(ii) Rearranging the cycles in the product

How do we determine the cycle decomposition of σ^{-1}? Recall that $\sigma \circ \sigma^{-1} = \varepsilon$, where ε denotes the identity permutation. Then, the cycle decomposition of σ^{-1} is obtained by writing the numbers in each cycle in the reverse order.

Example 1.49. Consider $\sigma = (1\ 3\ 2) \in S_3$. Then, in σ^{-1}, we must have the following:

$$3 \mapsto 1 \quad \text{and} \quad 2 \mapsto 3 \quad \text{and} \quad 1 \mapsto 2.$$

Hence, $\sigma^{-1} = (2\ 3\ 1)$.

We now introduce the cycle decomposition algorithm. Although it seems somewhat complicated, we will provide an example so knowing the abstract details of the algorithm is not necessary.

Algorithm 1.1 (cycle decomposition algorithm). The steps are as follows:

1. Pick the smallest element of $\{1, 2, \ldots, n\}$ which has not yet appeared in a previous cycle. Begin the new cycle: $(a$
2. Read off $\sigma(a)$ from the given description of σ — call it b.
   - If $b = a$, close the cycle without writing b down, return to Step 1.
   - If $b \neq a$, write b next to a in this cycle, i.e. $(a\ b$.
3. Read off $\sigma(b)$ from the given description of σ — call it c.
   - If $c = a$, close the cycle without writing c down, return to Step 1.
   - If $c \neq a$, write c next to b in this cycle, i.e. $(a\ b\ c$. Repeat this step using the number c as the new value for b until the cycle closes.
4. Remove all cycles of length 1.

Example 1.50. Consider the permutation $\sigma \in S_{13}$ defined as follows:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 3 & 1 & 11 & 9 & 5 & 10 & 6 & 4 & 7 & 8 & 2 \end{pmatrix}$$

We wish to decompose σ into a product of cycles. The idea here is as follows. We see that $1 \mapsto 12 \mapsto 8 \mapsto 10 \mapsto 4 \mapsto 1$, so one of the cycles is $(1\ 12\ 8\ 10\ 4)$. We see that 2 is not in this cycle, and $2 \mapsto 13 \mapsto 2$, so we obtain the transposition $(2\ 13)$. Since 3 is fixed under σ, then we have the 1-cycle (3), which we would omit when we are done with the decomposition.

We see that 4 was previously in a cycle, so we move on to 5. As $5 \mapsto 7 \mapsto 7 \mapsto 5$, then we obtain our fourth cycle $(5\ 11\ 7)$. It is then easy to deduce that the last cycle is the transposition $(6\ 9)$. Hence, σ can be written as

$$\sigma = (1\ 12\ 8\ 10\ 4)\,(2\ 13)\,(5\ 11\ 7)\,(6\ 9)\,.$$

By Proposition 1.5, we know that disjoint cycles commute, so it is valid to write

$$\sigma = (2\ 13)\,(6\ 9)\,(1\ 12\ 8\ 10\ 4)\,(5\ 11\ 7)\,.$$

However, the former approach is preferred since, when denoting the decomposition of a permutation, we prioritize smaller numbers from left to right. It is then easy to deduce that

$$\sigma^{-1} = (1\ 4\ 10\ 8\ 12)\,(2\ 13)\,(5\ 7\ 11)\,(6\ 9)\,.$$

We pose the following question: what is the largest order of an element in S_n? When I first learnt Group Theory, I jumped to a conclusion too quickly and claimed that the largest order is n. Clearly it is not! In fact, in S_5, the largest order of an element is actually 6, and not 5.

Consider the permutation $\sigma = (1\,3)\,(2\,5\,4) \in S_5$. Then,

$$\begin{aligned}\sigma^2 &= (2\,4\,5)\\ \sigma^3 &= (1\,3)\\ \sigma^4 &= (2\,5\,4)\\ \sigma^5 &= (1\,3)\,(2\,4\,5)\end{aligned}$$

and σ^6 is the identity permutation. As such, $|\sigma| = 6$. If we let $g(n)$ (universally known notation) denote the largest order of permutation of n elements, one can deduce that

$$g(1) = 1 \quad g(2) = 2 \quad g(3) = 3 \quad g(4) = 4 \quad g(5) = 6 \quad g(6) = 6 \quad g(7) = 12.$$

Also, $g(40) = 27720$. This is known as Landau's function.

When we write a permutation as a product of disjoint cycles, the important consequence is that these cycles act independently on disjoint subsets of $\{1, \ldots, n\}$. The order of a permutation (the number of times you must apply it to get back to the identity arrangement) is precisely the lcm of the lengths of its disjoint cycles. Thus, to find the maximum possible order of any permutation on n elements, we seek a way to split $\{1, \ldots, n\}$ into cycles of lengths that give us the largest lcm.

A closed formula for Landau's function $g(n)$ is

$$g(n) = \prod_{p \le n} p^{\lfloor \log_p n \rfloor} \quad \text{where} \quad \text{the product is taken over all primes } p \le n.$$

This happens to coincide with the maximal lcm one can arrange via cycle decompositions. Clearly, this topic deals with Partition Theory. The interested reader can search this topic for more information.

1.4 Matrix Groups

Let F be a field, such as the real numbers $\mathbb{R}$ or the complex numbers $\mathbb{C}$. A field can be regarded as a *ring* such that every non-zero element $x \in F$ has a multiplicative inverse, i.e.

$$\text{for every } x \in F \setminus \{0\}, \quad \text{there exists } y \in F \text{ such that } xy = 1_F.$$

Definition 1.18 (general linear group)**.** For any $n \in \mathbb{N}$, define the general linear group of $n \times n$ invertible matrices over F (also known as the general linear group of degree n) as follows:

$$\mathrm{GL}_n(F) = \{\mathbf{A} \in \mathcal{M}_{n\times n}(F) : \det(\mathbf{A}) \neq 0\}$$

Here, $\mathcal{M}_{n\times n}(F)$ denotes the set of $n \times n$ matrices with entries in F.

Proposition 1.6. $\mathrm{GL}_n(F)$ is a group under multiplication.

Proof. Recall that matrix multiplication is associative. The identity element in the group is the identity matrix of order n, denoted by $\mathbf{I}_n$. Lastly, $\mathbf{A} \mapsto \mathbf{A}^{-1}$ is the inverse operation. Hence, the three axioms of Definition 1.1 are satisfied. $\square$

Definition 1.19 (special linear group). For any $n \in \mathbb{N}$, define the special linear group of $n \times n$ invertible matrices over F as follows:

$$\mathrm{SL}_n(F) = \{\mathbf{A} \in \mathrm{GL}_n(F) : \det(\mathbf{A}) = 1\}.$$

In Question 9 of Page 48 of the Dummit and Foote textbook, the reader is asked to prove that $\mathrm{SL}_n(F) \leq \mathrm{GL}_n(F)$. In other words, $\mathrm{SL}_n(F)$ is a *subgroup* of $\mathrm{GL}_n(F)$. Although subgroups will be covered in Definition 2.1, and proving that a group is a subgroup is taught in Proposition 2.1, we will briefly state what the question means here.

Intuitively, any matrix $\mathbf{A}$ in the special linear group must also be in the general linear group as a matrix of determinant 1 is invertible. In order to verify the subgroup criteria, one first needs to show that $\mathrm{SL}_n(F)$ is non-empty, for which we can take the $n \times n$ identity matrix $\mathbf{I}_n$, where the elements of the matrix are the identity elements of the field F, i.e. $a_{ij} = 1_F$ for all $1 \leq i, j \leq n$. We then need to show that

$$\text{for any } \mathbf{A}, \mathbf{B} \in \mathrm{SL}_n(F) \quad \text{we have} \quad \mathbf{A}\mathbf{B}^{-1} \in \mathrm{SL}_n(F).$$

This is obvious because $\mathbf{A}\mathbf{B}^{-1}$ is of determinant 1! Hence, $\mathrm{SL}_n(F) \leq \mathrm{GL}_n(F)$.

Definition 1.20 (Heisenberg group). Let F be a field. Let

$$H(F) = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} : a, b, c \in F \right\} \quad \text{denote} \quad \text{the Heisenberg group over } F.$$

After introducing the Heisenberg group over an arbitrary field F (Definition 1.20), Example 1.51 develops some of its basic properties. As mentioned in the Dummit and Foote textbook, when $F = \mathbb{R}$, this group plays an important role in Quantum Mechanics and signal theory by giving a group theoretic interpretation (due to Hermann Weyl) of Heisenberg's uncertainty principle. Note that $\mathbb{Z}$ is not a field (as not every element has a multiplicative inverse) but the Heisenberg group may be defined more generally — for example, with entries in $\mathbb{Z}$[†].

Example 1.51 (Dummit and Foote p. 35 Question 11). Let

$$\mathbf{X} = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \text{ and } \mathbf{Y} = \begin{bmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{bmatrix} \quad \text{be elements of } H(F).$$

(a) Compute the matrix product $\mathbf{XY}$ and deduce that $H(F)$ is closed under matrix multiplication. Exhibit explicit matrices such that $\mathbf{XY} \neq \mathbf{YX}$ (so that $H(F)$ is always non-abelian).

(b) Find an explicit formula for the matrix inverse $\mathbf{X}^{-1}$ and deduce that $H(F)$ is closed under inverses.

(c) Prove the associative law for $H(F)$ and deduce that $H(F)$ is a group of order $|F|^3$. (Do not assume that matrix multiplication is associative.)

[†] The Heisenberg group $H(\mathbb{Z})$ is known as the discrete Heisenberg group.

(d) Find the order of each element of the finite group $H(\mathbb{Z}/2\mathbb{Z})$.
(e) Prove that every non-identity element of the group $H(\mathbb{R})$ has infinite order.

Solution.

(a) We have

$$\mathbf{XY} = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+d & b+af+e \\ 0 & 1 & e+f \\ 0 & 0 & 1 \end{bmatrix} \in H(F).$$

So, $H(F)$ is closed under matrix multiplication.

For the next part, we can take

$$\mathbf{X} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \text{ and } \mathbf{Y} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{so} \quad \mathbf{XY} = \begin{bmatrix} 1 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix} \text{ but } \mathbf{YX} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix}$$

As such, $\mathbf{XY} \neq \mathbf{YX}$.

(b) This is a very simple exercise using techniques taught in MA2001. We have

$$\mathbf{X}^{-1} = \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix} \in H(F).$$

This shows that $H(F)$ is closed under inverses.

(c) The first part on proving associativity in $H(F)$ is easy but tedious so we omit the solution. As for the second part, suppose $|H(F)|$ is finite. Consider $\mathbf{X} \in H(F)$. Since each of the a, b, c that appears as an entry in $\mathbf{X}$ has $|F|$ possible choices (as $a, b, c \in F$), then $|H(F)| = |F|^3$.

(d) Suppose $a, b, c \in \mathbb{Z}/2\mathbb{Z}$. Note that

$$\mathbf{X}^2 = \begin{bmatrix} 1 & 2a & 2b+ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & ac \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

We shall consider three cases.

- **Case 1:** Suppose $a = c = 0$. Then, $\mathbf{X}^2 = \mathbf{I}$, so $|\mathbf{X}| = 2$.
- **Case 2:** Without loss of generality, suppose $a = 0$ and $c = 1$ (the case where $a = 1$ and $c = 0$ is symmetric). Then, $\mathbf{X}^2 = \mathbf{I}$, so $|\mathbf{X}| = 2$.
- **Case 3:** Suppose $a = c = 1$. Then,

$$\mathbf{X}^2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{which implies} \quad \mathbf{X}^4 = \mathbf{I}.$$

As such, $|\mathbf{X}| = 4$.

(e) From **(d)**, we have

$$\mathbf{X}^2 = \begin{bmatrix} 1 & 2a & 2b+ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{bmatrix} \quad \text{so} \quad \mathbf{X}^4 = \begin{bmatrix} 1 & 4a & 4b+6ac \\ 0 & 1 & 4c \\ 0 & 0 & 1 \end{bmatrix}.$$

Also, one can compute

$$\mathbf{X}^3 = \begin{bmatrix} 1 & 3a & 3b+3ac \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{bmatrix}.$$

It is clear that for any $n \in \mathbb{N}$,

$$\mathbf{X}^n = \begin{bmatrix} 1 & an & bn+u_n ac \\ 0 & 1 & cn \\ 0 & 0 & 1 \end{bmatrix},$$

where u_n is a sequence of numbers whose general term is to be determined. We know that the first few terms of u_n are $0,1,3,6,\ldots$ which is precisely the sequence of triangular numbers (but translated)! Recall that

$$T_n \text{ is a triangular number} \quad \text{if and only if} \quad T_n = 1+2+\ldots+n = \frac{n(n+1)}{2}.$$

As such,

$$u_n = \frac{n(n-1)}{2}$$

which implies

$$\mathbf{X}^n = \begin{bmatrix} 1 & an & bn+\frac{n(n-1)}{2}ac \\ 0 & 1 & cn \\ 0 & 0 & 1 \end{bmatrix}.$$

Suppose $\mathbf{X}^n = \mathbf{I}$. Then, this would force $an = 0$, $cn = 0$ and $nb + n(n-1)ac/2 = 0$. This forces $a = b = c = 0$ since $n \geq 1$. As such, we see that every non-identity element of $H(\mathbb{R})$ has infinite order. □

1.5 The Quaternion Group

Definition 1.21 (quaternion group Q_8)**.** The quaternion group is the group Q_8 with underlying set

$$Q_8 = \{1,-1,i,-i,j,-j,k,-k\} \quad \text{which are pairwise distinct.}$$

The product $\cdot$ is computed as follows:

(1) $1 \cdot a = a \cdot 1 = a$ for all $a \in Q_8$

(2) $(-1)\cdot(-1) = 1$

(3) $(-1)\cdot a = a \cdot (-1) = -a$ for all $a \in Q_8$

The elements of Q_8 satisfy the following properties:

(i) $i \cdot i = j \cdot j = k \cdot k = -1$ (i.e. i,j,k are square roots of -1)

(ii) $i \cdot j = k$ and $j \cdot i = -k$

(iii) $j \cdot k = i$ and $k \cdot j = -i$

(iv) $k \cdot i = j$ and $i \cdot k = -j$

Other than Q_8, the set of quaternions is often denoted by $\mathbb{H}$, which is named after the Irish mathematician William Roman Hamilton. Quaternions were first described by Hamilton in 1843 and he applied them to mechanics in three-dimensional space. Recall that we had the inclusion

$$\mathbb{R} \subseteq \mathbb{C} \quad \text{and we can now extend it to} \quad \mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{H},$$

i.e. the complex numbers are a subset of the quaternions. Although we mentioned that $\mathbb{R}$ and $\mathbb{C}$ are rings (or rather, groups under both addition and multiplication), we see that the nice property of multiplication being commutative is *gone* when we go from $\mathbb{C}$ to $\mathbb{H}$! In fact, $\mathbb{H}$ cannot be referred to as a field since multiplication is non-commutative so one would refer to it as a division algebra.

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Table 11: Cayley table for the quaternion group Q_8

Example 1.52. The order of $-1 \in Q_8$ is 2 since $(-1)\cdot(-1) = 1$.

Example 1.53. The order of $k \in Q_8$ is 4. To see why, recall that $k \cdot k = -1$. Hence, the order of k, *assuming it exists*, is at least 2. From Example 1.52, we know that the order of -1 is 2, so we can conclude that $k^4 = 1$.

We can interpret the elements of Q_8 as matrices, i.e.

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad i = \begin{bmatrix} i & 0 \\ 0 & i \end{bmatrix} \quad \text{and} \quad j = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad k = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

One checks that **(i)**, **(ii)**, **(iii)**, and **(iv)** of Definition 1.21 are satisfied. It follows that the associativity of multiplication in Q_8 follows from the associativity of matrix multiplication.

1.6 Generators and Relations

Definition 1.22 (generators)**.** Let G be a group. A set of generators of G is a subset S of G such that every element of G can be written as

$$\text{a finite product of elements of } S \quad \text{and} \quad \text{their inverses.}$$

When this holds, we say that

$$G \text{ is generated by } S \quad \text{or} \quad S \text{ generates } G \quad \text{and we write } G = \langle S \rangle .$$

Example 1.54 (trivial example)**.** Any group G is generated by the subset G of G.

Example 1.55. The trivial group $S_1 = \{1\}$ is generated by $\{1\}$ and also by $\emptyset$.

Example 1.56 (S_2)**.** $S_2 = \{1, (1\ 2)\}$ is generated by $\{1, (1\ 2)\}$ and $\{(1\ 2)\}$. It is clear that the first set $\{1, (1\ 2)\}$ generates S_2; to see why $\{(1\ 2)\}$ generates S_2 as well, note that $(1\ 2)(1\ 2)$ is the identity permutation ε on S_2!

Example 1.57 (S_3)**.** S_3 is generated by $\{(1\ 2), (1\ 2\ 3)\}$. To reiterate, any permutation of S_3 can be written as the finite product of these permutations in the set.

Example 1.58. By cycle decomposition, S_n is generated by the set of all cycles in S_n.

Example 1.59 ($\mathbb{Z}$ under addition)**.** The additive group $\mathbb{Z}$ under $+$ is generated by $\{+1\}$. This means that starting from 0, we can obtain any integer n by adding or subtracting 1 finitely many times.

Example 1.60 ($\mathbb{R}^+$ under addition)**.** The additive group of the positive real numbers $\mathbb{R}^+$ under addition is generated by $(0,1]$.

Example 1.61 (Q_8)**.** The quaternion group Q_8 is generated by

$$\{i,j\} \quad \text{or} \quad \{j,k\} \quad \text{or} \quad \{k,i\}$$

Example 1.62 (D_{2n})**.** The dihedral group D_{2n} is generated by $\{r,s\}$.

Definition 1.23 (relation)**.** A relation in G with respect to a set of generators S is an equation in the elements of $S \cup \{1\}$ which is satisfied in G.

Example 1.63 (D_{2n})**.** Recall Definition 1.8, where we mentioned that $r^n = s^2 = 1$ and $rs = sr^{-1}$, which are relations with respect to $\{r,s\}$.

Example 1.64 (Q_8)**.** Recall Definition 1.21, where we mentioned that $i \cdot i = -1$ and $j \cdot j = -1$, so it follows that $i^4 = j^4 = 1$. Moreover, one checks that $ij = i^2 ji = j^3 i$.

Definition 1.24 (presentation)**.** A presentation of G, written as

$$G = \langle S \mid R_1, R_2, \ldots \rangle$$

consists of

$$\text{a set } S \text{ of generators of } G \quad \text{and} \quad \text{a set } \{R_1, R_2, \ldots\} \text{ of relations with respect to } S$$

such that any other relation among the elements of S can be deduced from $\{R_1, R_2, \ldots\}$.

Example 1.65 (D_{2n})**.** We have

$$D_{2n} = \left\langle r,s \mid r^n = s^2 = 1, rs = sr^{-1} \right\rangle$$

However, it may be difficult (or even impossible) to tell the following: when two elements of the group (which are expressed in terms of the given generators) are equal, whether the group is finite or infinite, and whether the group is trivial. This is known as the Adian-Rabin theorem (Theorem 1.4).

Theorem 1.4 (Adian-Rabin theorem)**.** Most *reasonable* properties of finitely presentable groups are algorithmically undecidable.

Example 1.66 (finite group; Klein four-group)**.** The group with presentation

$$\left\langle x_1, y_1 \mid x_1^2 = y_1^2 = (x_1 y_1)^2 = 1 \right\rangle \quad \text{is of order } 4.$$

One would eventually know that this is the group representation of the Klein four-group (the group is denoted by V). We will mention in Definition 2.3 that V is an Abelian group with four elements e,a,b,c, in which each element is involutory/self-inverse, i.e. composing it with itself produces the identity. Moreover, composing any two of the three non-identity elements produces the third one.

Example 1.67 (infinite group)**.** The group with presentation

$$\left\langle x_2, y_2 \mid x_2^3 = y_2^3 = (x_2y_2)^3 = 1 \right\rangle \quad \text{is an infinite group!}$$

We call this the von Dyck group $D(3,3,3)$[†]. In fact, if we consider a general case where we have a group with the following presentation

$$\left\langle x_2, y_2 \mid x_2^p = y_2^p = (x_2y_2)^p = 1 \right\rangle,$$

where p is an odd prime, then the group is infinite!

Example 1.68. There may be *hidden* or implicit relations, which are consequences of the specified ones. Say we consider the group with presentation

$$X_{2n} = \left\langle x, y \mid x^n = y^2 = 1, xy = yx^2 \right\rangle.$$

Then, albeit not obvious, one can deduce that $x = x^4$, which consequently implies $x^3 = 1$. Such a property is non-trivial. Moreover, we see that the order of $x \in X_{2n}$ is 3.

Example 1.69 (trivial group)**.** The group with presentation

$$\left\langle u, v \mid u^4 = v^3 = 1, uv = v^2u^2 \right\rangle \quad \text{is trivial.}$$

In Example 1.71, we will deduce that this group is indeed trivial.

Example 1.70 (Q_8; Dummit and Foote p. 36 Question 3)**.** In Examples 1.61 and 1.64, we discussed the generators and relations of the quaternion group Q_8. Now, we deduce with justification that Q_8 admits the following group presentation:

$$Q_8 = \left\langle i, j, k \mid i^2 = j^2 = k^2 = ijk \right\rangle$$

Recall Definition 1.21, where we mentioned that

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}.$$

Also, it is known that the elements of Q_8 satisfy the following properties:

(i) $i \cdot i = j \cdot j = k \cdot k = -1$ (i.e. i, j, k are square roots of -1)

(ii) $i \cdot j = k$ and $j \cdot i = -k$

(iii) $j \cdot k = i$ and $k \cdot j = -i$

(iv) $k \cdot i = j$ and $i \cdot k = -j$

Clearly, Q_8 has 3 generators. In order to deduce the most *compact-looking relation*, recall from **(i)** that $i^2 = j^2 = k^2 = -1$. By **(i)**, we have

$$(i \cdot j) \cdot (j \cdot i) = k \cdot (-k) \quad \text{so} \quad i \cdot j^2 \cdot i = -k^2 = 1.$$

As such, $ij(-ji) = -1$. By **(ii)** again, we see that $j \cdot i = -k$ so $-ji = k$. As such, $ijk = -1$. One should see that given the relation $i^2 = j^2 = k^2 = ijk$, we can deduce **(iii)** and **(iv)**.

Example 1.71 (Dummit and Foote p. 28 Question 18)**.** Let Y be the group with presentation

$$\left\langle u, v \mid u^4 = v^3 = 1, uv = v^2u^2 \right\rangle.$$

(a) Show that $v^2 = v^{-1}$.
Hint: Use the relation $v^3 = 1$.

[†]The interested reader can look up ‘wallpaper groups’ to see some nice visual applications of von Dyck groups.

(b) Show that v commutes with u^3.

Hint: Show that $v^2u^3v = u^3$ by writing the LHS as $\left(v^2u^2\right)(uv)$ and using the relations to reduce this to the RHS. Then, use **(a)**.

(c) Show that v commutes with u.

Hint: Show that $u^9 = u$ and then use **(b)**.

(d) Show that $uv = 1$.

Hint: Use **(c)** and the last relation.

(e) Show that $u = 1$, deduce that $v = 1$, and conclude that $Y = 1$.

Hint: Use **(d)** and the equation $u^4v^3 = 1$.

Solution.

(a) This is trivial as $v^3 = 1$ implies $v \cdot v^2 = 1$. Hence, $v^2 = v^{-1}$.

(b) We first prove the hint. Note that

$$v^2u^3v = v\left(vu^2\right)(uv) = v\left(vu^2\right)\left(v^2u^2\right) = v^2u^2v^2u^{-1}u^3 = uv^3u^{-1}u^3 = u^3.$$

Hence, $v^{-1}u^3v = u^3$, which implies $u^3v = vu^3$.

(c) The hint is obvious. So,

$$\begin{aligned} uv &= u^9v \quad \text{since } u^8 = 1 \\ &= u^3u^3\left(u^3v\right) \\ &= u^3vu^3u^3 \quad \text{by } \textbf{(b)} \\ &= vu^9 \quad \text{by } \textbf{(b)} \\ &= vu \quad \text{since } u^8 = 1 \end{aligned}$$

(d) We have

$$\begin{aligned} uv &= vu \quad \text{by } \textbf{(c)} \\ v^2u^2 &= vu \quad \text{by the last relation } uv = v^2u^2 \end{aligned}$$

So, $vuvu = vu$, which implies $vu = 1$. Since u and v commute, the result follows.

(e) By **(d)**, we have $u = v^{-1}$. As $uv = v^2u^2$, then $e = v^{-1}u^2$, where we used **(a)** on the RHS. So, $u^2 = v$. Since $u = v^{-1}$ and $u^2 = v$, then $u^3 = 1$. However, we know that $u^4 = 1$ by the group presentation, so $u = 1$. Consequently, $v = 1$. As such, $uv = 1$ as well. This implies 1 is the only element of Y, so we conclude that Y is the trivial group. □

1.7 Homomorphisms and Isomorphisms

Someone ever asked what a homomorphism is in MA5204.

Definition 1.25 (group homomorphism)**.** Let G and H be groups. A group homomorphism (or homomorphism if it is explicitly known that the map is between two groups) from $(G,\cdot)$ to $(H,*)$ is a map $\varphi : G \to H$ such that the following properties are satisfied:

(i) φ **respects multiplication:** for all $x, y \in G$, we have $\varphi(x \cdot y) = \varphi(x) * \varphi(y)$ and note that

$$x \cdot y \text{ involves the operation in } G \quad \text{whereas} \quad \varphi(x) * \varphi(y) \text{ involves the operation in } H$$

(ii) φ **respects identity:** one has $\varphi(1_G) = 1_H$

(iii) φ**respects inversion:** for all $x \in G$, we have $\varphi\left(x^{-1}\right) = (\varphi(x))^{-1}$

Proposition 1.7. Let $\varphi : G \to H$ be a map. Then,

$$\varphi \text{ is a homomorphism} \quad \text{if and only if} \quad \varphi \text{ respects multiplication.}$$

Proposition 1.8. For any group G, the identity map $\mathrm{id}_G : G \to G$ is a homomorphism.

Example 1.72 (Dummit and Foote p. 39 Question 1)**.** Let $\varphi : G \to H$ be a homomorphism.

(a) Prove that $\varphi(x^n) = [\varphi(x)]^n$ for all $n \in \mathbb{Z}^+$.

(b) Do part **(a)** for $n = -1$ and deduce that $\varphi(x^n) = [\varphi(x)]^n$ for all $n \in \mathbb{Z}$.

Solution.

(a) We will prove this by induction. For any $n \in \mathbb{Z}^+$, let the proposition $P(n)$ denote $\varphi(x^n) = [\varphi(x)]^n$. We will first prove that $P(1)$ is true, which is obvious as $\varphi\left(x^1\right) = \varphi(x) = [\varphi(x)]^1$.

Suppose $P(k)$ is true for some $k \in \mathbb{Z}^+$. Notice that $\varphi\left(x^{k+1}\right) = \varphi(x \cdot \ldots \cdot x)$, where there are $k+1$ x's on the RHS. Since φ is a homomorphism, we can write

$$\varphi\left(x^{k+1}\right) = \varphi\left(x^k \cdot x\right) = [\varphi(x)]^k \varphi(x) = [\varphi(x)]^{k+1}.$$

It follows that $P(n)$ is true for any $n \in \mathbb{Z}^+$.

(b) Suppose $n = -1$, we have $\varphi(x^n) = \varphi\left(x^{-1}\right)$. Since φ is a homomorphism, by **(iii)** of Definition 1.25, we have

$$\varphi\left(x^{-1}\right) = [\varphi(x)]^{-1}.$$

It now suffices to prove the result in **(a)** for $n = 0$ and $n \in \mathbb{Z}^-$. When $n = 0$, we have

$$\varphi\left(x^0\right) = \varphi(1_G) = 1_H = [\varphi(x)]^0.$$

So, the statement holds for $n = 0$.

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

We have considered the case where $n \in \mathbb{Z}^+$ in **(a)**, so now we will consider $n = 0$ and $n \in \mathbb{Z}^-$. When $n = 0$, we have

$$\varphi(x^0) = \varphi(1) = 1_G = 1 = \varphi(x)^0$$

As such the statement holds true for $n = 0$. For $n \in \mathbb{Z}^-$, similar to how we proved for the case when $n = -1$, as φ is a homomorphism, we shall set $n = -k$ where $k \in \mathbb{Z}^+$. Then,

$$\varphi\left(x^{-k}\right) = \varphi\left[\left(x^k\right)^{-1}\right] = \left[\varphi\left(x^k\right)\right]^{-1} = [\varphi(x)]^{-k}.$$

so the statement holds for all $n \in \mathbb{Z}$. □

Proposition 1.9. Let G, H, K be groups. If

$$\varphi : G \to H \quad \text{and} \quad \psi : H \to K \quad \text{are homomorphisms,}$$

then

$$\text{the composite map } \psi \circ \varphi : G \to K \quad \text{is a homomorphism.}$$

Proof. Let $x, y \in G$. Then,

$$\mathrm{id}_G(xy) = xy = \mathrm{id}_G(x)\,\mathrm{id}_G(y) \quad \text{so} \quad \mathrm{id}_G \text{ respects multiplication.}$$

We then show that $\psi \circ \varphi$ respects multiplication. We have

$$\begin{aligned}
(\psi \circ \varphi)(xy) &= \psi(\varphi(xy)) \\
&= \psi(\varphi(x)\varphi(y)) \quad \text{since } \varphi \text{ respects multiplication} \\
&= \psi(\varphi(x))\psi(\varphi(y)) \quad \text{since } \psi \text{ respects multiplication} \\
&= (\psi \circ \varphi)(x)(\psi \circ \varphi)(y)
\end{aligned}$$

so we see that $\psi \circ \varphi$ respects multiplication. □

In the proof of Proposition 1.9, we did not explicitly state the operations in the respective groups G, H, K. For example, say the operations on G and H are $\cdot$ and $*$ respectively. These can actually be omitted.

At this juncture, it appears that the concept of a group homomorphism may seem abstract, but we have actually been encountering them for quite some time. Here is an example to make the concept more concrete.

Example 1.73. Let

$$G = H = K = \mathbb{R} \quad \text{be additive groups.}$$

In the context of additive groups, we would expect f and g to be linear if they are group homomorphisms, i.e. they satisfy

$$f(x+y) = f(x) + f(y) \quad \text{and} \quad g(x+y) = g(x) + g(y) \quad \text{for all } x, y \in \mathbb{R}.$$

For those who have prior experience in Olympiads, you would know that the only solution to the functional equation $f(x+y) = f(x) + f(y)$, where $x, y \in \mathbb{R}$ is $f(x) = ax$, where $a \in \mathbb{R}$. In fact, this functional equation is known as Cauchy's functional equation.

By Proposition 1.9, we recall that the composition of group homomorphism is also a group homomorphism, i.e.

$$(f \circ g)(x) = (g \circ f) = abx \quad \text{preserves the additive structure.}$$

This is indeed not surprising! Moreover, non-linear functions such as $\sqrt{x}$ and $\cos x$ do not satisfy the requirements of an additive group homomorphism in $\mathbb{R}$.

Example 1.74. Let G be a group. Then, the following hold:

$$\begin{aligned}
&1 \to G \quad \text{where} \quad 1 \mapsto 1_G \quad \text{is a homomorphism} \quad \text{and} \\
&G \to 1 \quad \text{where} \quad G \ni x \mapsto 1 \quad \text{is a homomorphism}
\end{aligned}$$

and they are the unique homomorphisms from 1 to G and G to 1 respectively.

Example 1.75. The exponential map

$$\exp : \mathbb{R} \to \mathbb{R}^{+} \text{ where } \exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \quad \text{is a homomorphism from } (\mathbb{R},+) \text{ to } \left(\mathbb{R}^{+},\times\right).$$

Try to see how this result is analogous to the following law of indices:

$$e^{x+y} = e^x \cdot e^y \quad \text{or} \quad \exp(x+y) = \exp(x) \cdot \exp(y),$$

where addition is taking place in $\exp(x+y)$ and multiplication is taking place in $\exp(x) \cdot \exp(y)$.

Next, consider the natural logarithm

$$\log_e : \mathbb{R}^{+} \to \mathbb{R} \text{ where } \log_e(x) = \int_1^x \frac{1}{t}\, dt \quad \text{is a homomorphism from } \left(\mathbb{R}^{+},\times\right) \text{ to } (\mathbb{R},+).$$

Again, try to see how this result is analogous to the following law of indices:

$$\log_e(xy) = \log_e(x) + \log_e(y)$$

where multiplication is taking place in $\log_e(xy)$ and addition is taking place in $\log_e(x) + \log_e(y)$.

Hence,

$$\begin{aligned} \log_e \circ \exp = \mathrm{id}_{\mathbb{R}} \quad &\text{as} \quad \text{for all } x \in \mathbb{R}, \text{ we have } \log_e(e^x) = x \quad \text{and} \\ \exp \circ \log_e = \mathrm{id}_{\mathbb{R}^{+}} \quad &\text{as} \quad \text{for all } x \in \mathbb{R}_{>0}, \text{ we have } e^{\log_e(x)} = x \end{aligned}$$

Example 1.76 (Dummit and Foote p. 40 Question 17). Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is Abelian.

Solution. We first prove the forward direction. Suppose

$$\varphi : G \to G \quad \text{where} \quad \varphi(g) = g^{-1} \quad \text{is a homomorphism.}$$

Then,

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) \quad \text{which implies} \quad (g_1 g_2)^{-1} = g_1^{-1} g_2^{-1}.$$

Hence, $g_2^{-1} g_1^{-1} = g_1^{-1} g_2^{-1}$. Taking inverses on both sides, we have $g_1 g_2 = g_2 g_1$, which shows that any two elements of G commute, i.e. G is Abelian. In fact, the proof of the reverse direction follows by performing all the steps in reverse. □

Example 1.77 (Dummit and Foote p. 40 Question 18). Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^2$ is a homomorphism if and only if G is Abelian.

Solution. Similar to the nature of Example 1.76, we will only prove the forward direction as the proof of the reverse direction follows by performing all the steps in reverse. Suppose

$$\varphi : G \to G \quad \text{where} \quad \varphi(g) = g^2 \quad \text{is a homomorphism.}$$

Then,

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) \quad \text{which implies} \quad (g_1 g_2)^2 = g_1^2 g_2^2.$$

Hence, $g_1 g_2 g_1 g_2 = g_1 g_1 g_2 g_2$. Since G is group, for any $g_1, g_2 \in G$, their respective inverses exist, i.e. there exist $g_1^{-1}, g_2^{-1} \in G$ such that $g_1 \cdot g_1^{-1} = 1_G$ and $g_2 \cdot g_2^{-1} = 1_G$. Hence, $g_2 g_1 = g_1 g_2$, for which similar to Example 1.76, shows that G is Abelian. □

Example 1.78 (Dummit and Foote p. 41 Question 25). Let $n \in \mathbb{Z}^+$ and let r and s be the usual generators of D_{2n}, and let $\theta = 2\pi/n$.

(a) Prove that the matrix
$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$
is the matrix of the linear transformation which rotates the xy-plane about the origin in a counterclockwise direction by θ radians.

(b) Prove that the map $\varphi : D_{2n} \to \mathrm{GL}_2(\mathbb{R})$ defined on generators by
$$\varphi(r) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \quad \text{and} \quad \varphi(s) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$
extends to a homomorphism of D_{2n} into $\mathrm{GL}_2(\mathbb{R})$.

(c) Prove that the homomorphism φ in **(b)** is injective.

Solution.

(a) This is a simple exercise involving polar coordinates. We omit the solution.

(b) Geometrically, $\varphi(s)$ represents a reflection across the line $y = x$, so $[\varphi(s)]^2 = \mathbf{I}$. Since the rotation matrix in **(a)** denotes a rotation about the origin in a counterclockwise direction by θ radians, then applying the map n times yields the identity map, or rather $\mathbf{I}$. That is, $[\varphi(r)]^n = \mathbf{I}$.

Lastly, we shall justify that
$$\varphi(r)\varphi(s) = \varphi(s)[\varphi(r)]^{-1}.$$
$\varphi(r)\varphi(s)$ means that we reflect across the line $y = x$ first, then rotate by θ radians counterclockwise. This is the same as a rotation of θ radians clockwise first, then a reflection across the line $y = x$, which is represented by $\varphi(s)[\varphi(r)]^{-1}$.

(c) Let H denote the subgroup of $\mathrm{GL}_2(\mathbb{R})$ generated by $\varphi(r)$ and $\varphi(s)$. Then, the map $\psi : D_{2n} \to H$ defined by restricting the codomain of φ is surjective. Since $|H| = 2n = |D_{2n}|$, then ψ must be injective. Consequently, φ must also be injective. □

Definition 1.26 (group isomorphism). Let $\varphi : G \to H$ be a bijective group homomorphism. Then,
$$\varphi \text{ is an isomorphism} \quad \text{and} \quad G \text{ and } H \text{ are isomorphic,} \quad \text{where we write} \quad G \cong H.$$
Hence, an isomorphism from G to H is
$$\text{a homomorphism } \varphi : G \to H \quad \text{such that} \quad \text{there exists a homomorphism } \psi : H \to G$$
such that
$$\psi \circ \varphi = \mathrm{id}_G \quad \text{and} \quad \varphi \circ \psi = \mathrm{id}_H.$$

Proposition 1.10. A homomorphism $\varphi : G \to H$ is an isomorphism if and only if φ is bijective.

Definition 1.27 (group isomorphism). We say that
$$G \cong H \quad \text{if and only if} \quad \text{there exists an isomorphism from } G \text{ to } H.$$
Note that the isomorphism is usually not unique.

Remark 1.3. Saying that two groups G and H are isomorphic is generally quite *useless* — it is better if we can state what the isomorphism $\varphi : G \to H$ is.

Example 1.79 (Dummit and Foote p. 40 Question 5)**.** Prove that the additive groups $\mathbb{R}$ and $\mathbb{Q}$ are not isomorphic.

Solution. Suppose on the contrary that $\mathbb{R}$ and $\mathbb{Q}$ are isomorphic, with the group operation being $+$. Recall from MA1100 that $\mathbb{Q}$ is countable and $\mathbb{R}$ is uncountable so there does not exist a bijective function from $\mathbb{R}$ to $\mathbb{Q}$. By Proposition 1.10, the additive groups $(\mathbb{R},+)$ and $(\mathbb{Q},+)$ are not isomorphic. □

Example 1.80 (Dummit and Foote p. 40 Question 7)**.** Prove that D_8 and Q_8 are not isomorphic[†].

Solution. Based on the mentioned links in the footnote, we see that Q_8 has only 1 element of order 2, whereas D_8 has 5 elements of order 2. By **(b)** of Proposition 1.14, D_8 and Q_8 are not isomorphic. One checks the following:

$$\begin{aligned} &\text{the element of order 2 in } Q_8 && \text{is} && -1 && \text{and} \\ &\text{the elements of order 2 in } D_8 && \text{are} && r^2, s, rs, r^2s, r^3s && \end{aligned}$$

so indeed, D_8 and Q_8 are not isomorphic. □

Example 1.81 (Dummit and Foote p. 40 Question 8)**.** Prove that if $n \neq m$, then S_n and S_m are not isomorphic.

Solution. $|S_n| = n!$ and $|S_m| = m!$ which are not equal. □

Example 1.82 (Dummit and Foote p. 40 Question 9)**.** Prove that D_{24} and S_4 are not isomorphic.

Solution. Note that $r \in D_{24}$ which is of order 12, but there does not exist any element of order 12 in S_4. □

Proposition 1.11. $\cong$ is an equivalence relation. That is,

$$\cong \quad \text{is} \quad \text{reflexive, symmetric, transitive.}$$

Proof. We first prove that $\cong$ is reflexive. Let G be a group. Then,

$$\text{the identity map } \mathrm{id}_G : G \to G \quad \text{defined by} \quad \mathrm{id}_G(g) = g \text{ for all } g \in G$$

is a bijective homomorphism. To see why id_G is a homomorphism, we have for any $g_1, g_2 \in G$,

$$\mathrm{id}_G(g_1 \cdot g_2) = g_1 \cdot g_2 = \mathrm{id}_G(g_1) \cdot \mathrm{id}_G(g_2).$$

Also, id_G is clearly bijective since every element in G maps uniquely to itself. As such, $G \cong G$.

We then prove that $\cong$ is symmetric. Suppose $G \cong H$, where H is also a group. Then,

$$\text{there exists a group isomorphism} \quad \varphi : G \to H.$$

Since φ is bijective, it is invertible by Theorem 1.1, φ^{-1} exists. As such,

$$\text{there exists a group isomorphism} \quad \varphi^{-1} : H \to G \quad \text{which implies} \quad H \cong G \text{ so } \cong \text{ is symmetric.}$$

[†]I looked at the element structure of Q_8 and the element structure of D_8.

Lastly, we prove that $\cong$ is transitive. Suppose $G \cong H$ and $H \cong K$, where K is also a group. Then,

$$\text{there exist group isomorphisms} \quad \varphi : G \to H \text{ and } \psi : H \to K.$$

We need to show that $\psi \circ \varphi : G \to K$ is an isomorphism, so two properties need to be established — $\psi \circ \varphi$ is a homomorphism (follows from Proposition 1.9) and $\psi \circ \varphi$ is a bijective map. The latter is a simple result from MA1100, where it is known that the composition of bijective maps is also bijective. So, $G \cong K$, implying that $\cong$ is transitive. ☐

Example 1.83. Recall Example 1.75, where we mentioned the exponential map and the natural logarithm as group homomorphisms. One would know from MA1100 that these functions are injective and surjective, hence bijective, which shows that we can construct the following group isomorphisms:

$$(\mathbb{R}, +) \cong \left(\mathbb{R}^+, \times\right) \quad \text{and} \quad \left(\mathbb{R}^+, \times\right) \cong (\mathbb{R}, +)$$

which correspond to the exponential function and the natural logarithm respectively.

Example 1.84. We have the isomorphism

$$D_6 \cong S_3.$$

Although $|D_6| = |S_3| = 6$, we cannot use this fact to conclude that the groups are isomorphic. Instead, the only way out is by constructing a group homomorphism $\varphi : S_3 \to D_6$ and checking that it is indeed an isomorphism. We omit the details.

Example 1.85 (Dummit and Foote p. 40 Question 3)**.** If $\varphi : G \to H$ is an isomorphism, prove that

$$G \text{ is Abelian} \quad \text{if and only if} \quad H \text{ is Abelian.}$$

If $\varphi : G \to H$ is a homomorphism, what additional conditions on φ (if any) are sufficient to ensure G is abelian, then so is H?

Solution. We first prove the first result. Starting with the forward direction, assume that G is Abelian. Take two elements $h_1, h_2 \in H$. Then, there exist $g_1, g_2 \in G$ (this follows as φ is bijective, hence surjective) such that

$$\varphi(g_1) = h_1 \quad \text{and} \quad \varphi(g_2) = h_2.$$

Then,

$$\begin{aligned} h_1 h_2 &= \varphi(g_1)\varphi(g_2) \\ &= \varphi(g_1 g_2) \quad \text{since } \varphi \text{ is a homomorphism} \\ &= \varphi(g_2 g_1) \quad \text{since } G \text{ is Abelian} \\ &= \varphi(g_2)\varphi(g_1) \quad \text{since } \varphi \text{ is a homomorphism} \\ &= h_2 h_1 \end{aligned}$$

so H is Abelian.

We then prove the reverse direction. Suppose $g_1, g_2 \in G$. Then,

$$\begin{aligned} \varphi(g_1 g_2) &= \varphi(g_1)\varphi(g_2) \quad \text{since } \varphi \text{ is a homomorphism} \\ &= \varphi(g_2)\varphi(g_1) \quad \text{since } H \text{ is Abelian} \\ &= \varphi(g_2 g_1) \quad \text{since } \varphi \text{ is a homomorphism} \end{aligned}$$

Since φ is bijective, it is injective so $g_1g_2 = g_2g_1$. So, G is Abelian.

We proceed with the second result. Suppose $\varphi : G \to H$ is a homomorphism. Say G is Abelian. As mentioned in the forward direction of the proof of the first result, if φ is surjective, then H is Abelian. $\square$

Proposition 1.12 (Dummit and Foote p. 40 Question 11)**.** Let A and B be groups. Prove that

$$A \times B \cong B \times A.$$

Proof. Define

$$\varphi : A \times B \to B \times A \quad \text{where} \quad \varphi : (a,b) \mapsto (b,a).$$

Here, note that $(A,\cdot)$ and $(B,*)$ are groups. We first show that φ is a homomorphism. Suppose we have $(a_1,b_1),(a_2,b_2) \in A \times B$ such that

$$\varphi((a_1,b_1)) = (b_1,a_1) \quad \text{and} \quad \varphi((a_2,b_2)) = (b_2,a_2).$$

Then,

$$\varphi((a_1,b_1)(a_2,b_2)) = \varphi((a_1a_2,b_1b_2)) = (b_1b_2,a_1a_2) = (b_1,a_1)(b_2,a_2) = \varphi(a_1,b_1)\varphi(a_2,b_2).$$

So, φ is indeed a homomorphism.

We then prove that φ is bijective. Suppose we have $\varphi((a_1,b_1)) = \varphi((a_2,b_2))$. Then, $(b_1,a_1) = (b_2,a_2)$, so by equality of ordered pairs ,we have $a_1 = a_2$ and $b_1 = b_2$. This implies φ is injective.

Then, note that for every $(b,a) \in B \times A$, we can choose $(a,b) \in A \times B$ such that $\varphi((a,b)) = (b,a)$, which implies φ is surjective. It follows that φ is a bijective homomorphism so φ is an isomorphism. $\square$

Example 1.86 (Dummit and Foote p. 40 Question 12)**.** Let A, B, and C be groups and let

$$G = A \times B \quad \text{and} \quad H = B \times C.$$

Prove that $G \times C \cong A \times H$.

Solution. Define

$$\varphi : G \times C \to A \times H \quad \text{where} \quad \varphi : (g,c) \mapsto (a,h)$$

Let $g = (a,b)$ and $h = (b,c)$, where $a \in A, b \in B, c \in C$, so $\varphi : ((a,b),c) \mapsto (a,(b,c))$. The proof that φ is a homomorphism is similar to that in Example 1.12.

We then prove that φ is injective. Suppose $(a_1,(b_1,c_1)) = (a_2,(b_2,c_2))$ in $A \times H$. Then, $a_1 = a_2$ and $(b_1,c_1) = (b_2 = c_2)$. The latter implies $b_1 = b_2$ and $c_1 = c_2$, so φ is injective. Also, it is clear that φ is surjective because for every $(a,(b,c)) \in A \times H$, there exists $((a,b),c) \in G \times C$ such that $\varphi((a,b),c) = (a,(b,c))$. We conclude that φ is an isomorphism. $\square$

Example 1.87 (Dummit and Foote p. 40 Question 19)**.** Let

$$G = \left\{z \in \mathbb{C} : z^n = 1 \text{ for some } n \in \mathbb{Z}^+\right\}.$$

Prove that for any fixed integer $k > 1$, the map from G to itself defined by $z \mapsto z^k$ is a surjective homomorphism but is not an isomorphism.

Solution. Let the map be

$$\varphi : G \to G \quad \text{where} \quad z \mapsto z^k.$$

We first prove that φ is a homomorphism. Let $x, y \in G$ (referring to the domain). Then,

$$\varphi(xy) = (xy)^k = x^k y^k = \varphi(x)\varphi(y),$$

so φ is a homomorphism. To see why φ is surjective, let $a, n \in \mathbb{Z}^+$, and choose

$$z^k = e^{2a\pi i/n} \quad \text{in } G,$$

where G here refers to the codomain. One checks that

$$\left(z^k\right)^n = e^{2a\pi i} = \left(e^{2\pi i}\right)^a = 1.$$

The preimage of $e^{2a\pi i/n}$ in G is $e^{2a\pi i/nk}$. Again, one checks that $\left(e^{2a\pi i/nk}\right)^{nk} = 1$, so indeed, this element is in G. So, φ is surjective.

However, φ is not an isomorphism because it is not injective. To see why, let $\zeta_1, \zeta_2 \in \mathbb{C}$ such that $|\zeta_1| = |\zeta_2| = 1$. Consider $\varphi(\zeta_1) = \varphi(\zeta_2)$. Say we define $\zeta_1 = e^{2a\pi i/k}$ and $\zeta_2 = e^{2b\pi i/k}$, where $a, b \in \mathbb{Z}^+$. Then, the equation $\varphi(\zeta_1) = \varphi(\zeta_2)$ holds but ζ_1 may not be equal to ζ_2. In particular, we can simply choose distinct a and b. □

Proposition 1.13. For any sets Δ and Ω,

$$\text{if } |\Delta| = |\Omega| \quad \text{then} \quad S_\Delta \cong S_\Omega.$$

Proof. Suppose $|\Delta| = |\Omega|$. Then, by definition, there exists a bijective (or equivalently, invertible) map

$$\theta : \Delta \to \Omega \quad \text{with inverse map} \quad \theta^{-1} : \Omega \to \Delta.$$

We define the map $\varphi : S_\Delta \to S_\Omega$ as follows:

$$\text{for any } \sigma \in S_\Delta, \quad \text{set} \quad \varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1} \text{ which is known as the conjugation map.}$$

We will discuss more about conjugation in due course (Definition 2.6), particularly when we talk about *normal subgroups*. Note that $\varphi(\sigma)$ is a permutation of Ω since it is a map from Ω to Ω and it is the composition of invertible maps, which implies it is also invertible. So, we have shown that φ is bijective.

We then show that $\varphi : S_\Delta \to S_\Omega$ is a homomorphism. Let $\tau, \sigma \in S_\Delta$. Then,

$$\begin{aligned}
\varphi(\sigma \circ \tau) &= \theta \circ (\tau \circ \sigma) \circ \theta^{-1} \\
&= \theta \circ \tau \circ \mathrm{id}_\Delta \circ \sigma \circ \theta^{-1} \\
&= \theta \circ \tau \circ \theta^{-1} \circ \theta \circ \sigma \circ \theta^{-1} \\
&= \left(\theta \circ \tau \circ \theta^{-1}\right) \circ \left(\theta \circ \sigma \circ \theta^{-1}\right) \\
&= \varphi(\tau) \circ \varphi(\sigma)
\end{aligned}$$

Similarly, one can deduce that

$$\psi : S_\Omega \to S_\Delta \quad \text{defined by} \quad \psi(\alpha) = \theta^{-1} \circ \alpha \circ \theta \text{ for any } \alpha \in S_\Omega$$

is a homomorphism. As such,

$$\psi \circ \varphi = \mathrm{id}_{S_\Delta} \quad \text{and} \quad \varphi \circ \psi = \mathrm{id}_{S_\Omega},$$

implying that φ is an isomorphism with inverse $\varphi^{-1} = \psi$. □

Proposition 1.14. Let $\varphi : G \to H$ be an isomorphism. Then, the following hold:

(a) $|G| = |H|$

(b) for all $x \in G$, we have $|x| = |\varphi(x)|$

Proof. By Proposition 1.10, φ is bijective, so **(a)** follows.

For **(b)**, the result holds if G is an infinite group (consequently, H is an infinite group). So, consider the case when G is a finite group, say of order n. As any isomorphism is a homomorphism, then $\varphi(1_G) = 1_H$. Since G is finite, then there exists $n \in \mathbb{N}$ such that $x^n = 1_G$. Hence, $\varphi(x^n) = (\varphi(x))^n$, which implies $(\varphi(x))^n = 1_H$. This shows that $|\varphi(x)| \mid n$.

Conversely, if $(\varphi(x))^m = 1_H$ for some $m \in \mathbb{N}$, then taking φ^{-1} on both sides, we have $x^m = 1_G$. By the minimality of $|x| = n$, we have $m \geq n$, so we conclude that $|x| = |\varphi(x)|$. □

Example 1.88 (Dummit and Foote p. 40 Question 4)**.** Prove that the multiplicative groups

$$\mathbb{R} \setminus \{0\} \text{ and } \mathbb{C} \setminus \{0\} \quad \text{are not isomorphic.}$$

Solution. Recall **(b)** of Proposition 1.14, which mentions that if there really exists an isomorphism $\varphi : \mathbb{R} \setminus \{0\} \to \mathbb{C} \setminus \{0\}$, then for all $x \in \mathbb{R} \setminus \{0\}$, we have $|x| = |\varphi(x)|$. Note that $i \in \mathbb{C} \setminus \{0\}$ is of order 4. However, there does not exist any element in $\mathbb{R} \setminus \{0\}$ of order 4. We shall argue this rigorously.

Let $x \in \mathbb{R} \setminus \{0\}$. Then, either $x = \pm 1$ or $x \neq \pm 1$. For the former, if $x = 1$, then $|x| = 1$; if $x = -1$, then $|x| = 2$ since $(-1)^2 = 1$. For the latter, as $x \neq \pm 1$ but $|x| = 1$, then x must be a root of unity, i.e. there exists $n \geq 3$ such that $x = e^{2\pi i/n}$, but these elements are not purely real. As such, if such an isomorphism φ were to really exist, it has to preserve the order of the element under φ, but it does not. So, $\mathbb{R} \setminus \{0\}$ $\mathbb{C} \setminus \{0\}$ are not isomorphic. □

Example 1.89 (Dummit and Foote p. 41 Question 24)**.** Let G be a finite group and let x and y be distinct elements of order 2 in G that generate G. Prove that $G \cong D_{2n}$, where $n = |xy|$.

Solution. Recall Example 1.38, which mentions that if x and y are elements of order 2 in a group G,

$$t = xy \quad \text{implies} \quad tx = xt^{-1}.$$

Let $t = r$ and $x = s$ so that $y = tx^{-1} = rs^{-1}$. Here, r and s denote the usual rotation and reflection as mentioned in Definition 1.8 on the dihedral group D_{2n}. So,

$$x^2 = s^2 = e \quad \text{and} \quad y^2 = rs^{-1}rs^{-1} = rsrs = sr^{-1}rs = s^2 = e.$$

We have shown that x and y are of order 2. Lastly, we will prove that x and y are distinct. Suppose on the contrary that they denote the same transformation, i.e. $x = y$, or equivalently $s = rs^{-1}$. Then, $s^2 = r$, which implies $r = e$, which is a contradiction.

We conclude that G and D_{2n} are isomorphic. □

Definition 1.28 (automorphism group)**.** Let G be a group and let $\mathrm{Aut}(G)$ be the set of all isomorphisms from G onto G.

Proposition 1.15 (Dummit and Foote p. 41 Question 20). $\mathrm{Aut}(G)$ is a group under function composition.

In Proposition 1.15, the elements of $\mathrm{Aut}(G)$ are automorphisms of G. We now prove this result.

Proof. Suppose there exist maps $\varphi, \psi \in (G)$. Then,

$$\varphi, \psi : G \to G \quad \text{are isomorphisms.}$$

We will first prove that $\mathrm{Aut}(G)$ satisfies the closure property. Take any $x, y \in G$. Then,

$$\begin{aligned}(\varphi \circ \psi)(xy) &= \varphi(\psi(xy)) \\ &= \varphi(\psi(x)\psi(y)) \quad \text{since } \psi \text{ is a homomorphism} \\ &= \varphi(\psi(x))\varphi(\psi(y)) \quad \text{since } \varphi \text{ is a homomorphism} \\ &= ((\varphi \circ \psi)(x))((\varphi \circ \psi)(y))\end{aligned}$$

As such $\varphi \circ \psi$ is a homomorphism. From MA1100, we know that the composition of bijective functions φ and ψ, denoted by $\varphi \circ \psi$, is also bijective. So, $\varphi \circ \psi : G \to G$ is an isomorphism, which implies $\varphi \circ \psi \in \mathrm{Aut}(G)$.

Note that the composition of maps satisfies associativity, reason being if we have $\varphi, \psi, \omega \in \mathrm{Aut}(G)$, then

$$\varphi \circ (\psi \circ \Omega) = (\varphi \circ \psi) \circ \Omega.$$

The identity element of $\mathrm{Aut}(G)$ is clearly id_G.

Lastly, given $\varphi \in \mathrm{Aut}(G)$, as φ is bijective, it is invertible so $\varphi^{-1} : G \to G$ exists and it is also bijective. Take any $a, b \in G$. Then, $\varphi^{-1}(ab) = \varphi^{-1}(a)\varphi^{-1}(b)$ which shows that φ^{-1} is a homomorphism. As such, $\varphi^{-1} \in \mathrm{Aut}(G)$. To conclude, $\mathrm{Aut}(G)$ is a group. □

Example 1.90 (Dummit and Foote p. 41 Question 21). Prove that for each fixed non-zero $k \in \mathbb{Q}$, the map

$$\text{from } \mathbb{Q} \text{ to itself} \quad \text{defined by} \quad q \mapsto kq \quad \text{is an automorphism of } \mathbb{Q}.$$

Solution. We have $\varphi(q) = kq$. Consider $q_1, q_2 \in \mathbb{Q}$ such that $\varphi(q_1) = kq_1$ and $\varphi(q_2) = kq_2$. Then,

$$\varphi(q_1 + q_2) = k(q_1 + q_2) = kq_1 + kq_2 = \varphi(q_1) + \varphi(q_2).$$

As such, φ is a homomorphism. Next, we ill show that φ is bijective. We first prove that φ is injective. Consider $\varphi(q_1) = \varphi(q_2)$, which implies $kq_1 = kq_2$. Since $k \neq 0$, then $q_1 = q_2$, so φ is injective. Next, we prove that φ is surjective. For any $y \in \mathbb{Q}$, we can choose $x = y/k$ such that $\varphi(x) = k(y/k) = y$, which implies φ is surjective. The result follows. □

Example 1.91 (Dummit and Foote p. 41 Question 22). Let A be an Abelian group and fix some $k \in \mathbb{Z}$. Prove that the map $a \mapsto a^k$ is a homomorphism from A to itself. If $k = -1$ prove that this homomorphism is an isomorphism (i.e. is an automorphism of A).

Solution. Define $\varphi : A \to A$, where $\varphi(a) = a^k$ for some $k \in \mathbb{Z}$. So, for any $a, b \in A$

$$\varphi(ab) = (ab)^k = a^k b^k = \varphi(a)\varphi(b),$$

where the second equality uses the fact that A is Abelian (see Example 1.3). Hence, φ is a homomorphism.

When $k = -1$, we have the homomorphism $\varphi(a) = a^{-1}$. Since φ is its own inverse function, then φ is bijective so it is an isomorphism. □

Example 1.92 (Dummit and Foote p. 41 Question 23). Let G be a finite group which possesses an automorphism σ such that

$$\sigma(g) = g \quad \text{if and only if} \quad g = 1.$$

If σ^2 is the identity map from G to G, prove that G is Abelian. Such an automorphism σ is called *fixed-point free* of order 2.
Hint: Show that every element of G can be written in the form $x^{-1}\sigma(x)$ and apply σ to such an expression.

Solution. Define a map

$$\varphi : G \to G \quad \text{where} \quad \varphi(x) = x^{-1}\sigma(x).$$

We first prove that φ is injective. Suppose $\varphi(x) = \varphi(y)$. Then,

$$\begin{aligned} x^{-1}\sigma(x) &= y^{-1}\sigma(y) \\ \sigma(y) &= yx^{-1}\sigma(x) \end{aligned}$$

Hence,

$$y = \sigma(\sigma(y)) = \sigma\left(yx^{-1}\right)x \quad \text{which implies} \quad yx^{-1} = \sigma\left(yx^{-1}\right).$$

Since σ is fixed-point free, then $yx^{-1} = 1$, so $x = y$. Hence, φ is injective. Since G (referring to the domain) is a finite set, then φ is surjective. So, φ is bijective. From here, we deduce the hint — let $g \in G$, where G here refers to the codomain. As such, $g = x^{-1}\sigma(x)$, so for any $g \in G$, we can write it as $x^{-1}\sigma(x)$.

Let $g_1, g_2 \in G$ be arbitrary. Then, there exist $x_1, x_2 \in G$ such that $g_1 = x_1^{-1}\sigma(x_1)$ and $g_2 = x_2^{-1}\sigma(x_2)$. Hence,

$$\sigma(g_1) = \sigma\left(x_1^{-1}\right)\sigma^2(x_1) = \sigma\left(x_1^{-1}\right)x_1 = g_1^{-1}.$$

As such,

$$g_1g_2 = \sigma\left(g_1^{-1}\right)\sigma\left(g_2^{-1}\right) = \sigma\left(g_1^{-1}g_2^{-1}\right) = \sigma\left((g_2g_1)^{-1}\right) = \sigma(\sigma(g_2g_1)) = g_2g_1,$$

so we conclude that G is Abelian. □

Chapter 2
Subgroups

2.1
Definition and Examples

Definition 2.1 (subgroup). Let G be a group. A subgroup of G is a subset H of G (i.e. $H \subseteq G$) such that the following properties are satisfied:

(i) Closure under multiplication: for all $x, y \in H$, we have $xy \in H$

(ii) Closure under identity: $1_G \in H$

(iii) Closure under inversion: for all $x \in H$, we have $x^{-1} \in H$

We write

$$H \leq G \quad \text{if and only if} \quad H \text{ is a subgroup of } G.$$

When $H \leq G$, the multiplication map

$$* : G \times G \to G \text{ of } G \quad \text{restricts to} \quad \text{a map } * : H \times H \to H$$

known as the multiplication map of H. We say that $1_H = 1_G \in H$ is the identity of H.

Also, the inversion map

$$(\,)^{-1} : G \to G \text{ of } G \quad \text{restricts to} \quad \text{a map } (\,)^{-1} : H \to H$$

known as the inversion map of H.

Moreover, the following properties continue to satisfy the axioms for H to be a group (recall Definition 1.1):

(i) Associativity of $*$: for all $a, b, c \in H$, we have $(a * b) * c = a * (b * c)$

(ii) Existence of identity element: $a * 1_H = 1_H * a = a$

(iii) Existence of inverse element: for all $a \in H$, there exists $a^{-1} \in H$ such that $a * a^{-1} = a^{-1} * a = 1_H$

Hence, we can conclude that H is also a group, where

$$\text{the canonical inclusion map} \quad \iota : H \hookrightarrow G \text{ with } \iota(h) = h \quad \text{is a homomorphism.}$$

The hook in $H \hookrightarrow G$ means that ι is an injective map. To put things abstractly,

any injective homomorphism is known as a *monomorphism*.

Example 2.1 (canonical examples). For any group G,

$$H = \{1\} \leq G \quad \text{and } H \text{ is known as the trivial subgroup of } G.$$

Also,

$$H = G \leq G \quad \text{and } H \text{ is known as the improper subgroup of } G.$$

Definition 2.2 (proper subgroup). We say that H is a proper subgroup of G and

$$\text{we write } H < G \quad \text{if and only if} \quad H \leq G \text{ and } H \neq G.$$

Proposition 2.1 (subgroup criterion). A subset H of G is a subgroup if and only if the following properties are satisfied:

(i) $H \neq \emptyset$

(ii) for all $x, y \in H$, one has $xy^{-1} \in H$

Proof. We first prove the forward direction. Suppose $H \leq G$. Then, because $1_H = 1_g \in H$, then $H \neq \emptyset$ so **(i)** holds. Also, **(ii)** holds because for all $x, y \in H$, we have

$$y^{-1} \in H \text{ as } H \text{ is closed under inversion} \quad \text{so} \quad xy^{-1} \in H \text{ as } H \text{ is closed under multiplication.}$$

We now prove the reverse direction. Suppose H satisfies **(i)** and **(ii)**. Since $H \neq \emptyset$ by **(i)**, then there exists $b \in H$. Letting $x = y = b$, we obtain

$$1_G = bb^{-1} \in H \quad \text{so} \quad H \text{ is closed under identity.}$$

Next, for any $a \in H$, letting $x = 1_G$ and $y = a$, we obtain

$$a^{-1} = 1_G \cdot a^{-1} \in H \quad \text{so} \quad H \text{ is closed under inversion.}$$

Lastly, for any $a, b \in H$, letting $x = a$ and $y = b^{-1}$, we have

$$ab = a \cdot \left(b^{-1}\right)^{-1} \in H \quad \text{so} \quad H \text{ is closed under multiplication.}$$

It follows that $H \leq G$. □

Proposition 2.2 (finite subgroup criterion). A finite subset H of G is a subgroup if and only if the following properties are satisfied:

(i) $H \neq \emptyset$

(ii) for all $x, y \in H$, one has $xy \in H$

Proof. The proof is similar to that of the forward direction of Proposition 2.1. We only prove the reverse direction. Let $x \in H$. By setting $x = y$, we have $x^2 \in H$. As such,

$$\text{by an inductive argument,} \quad \text{for any } a \in \mathbb{N} \text{ we have } x^a \in H.$$

Set $n = |H| + 1$. By the pigeonhole principle,

$$\text{the map } \{1, \ldots, n\} \to H \quad \text{where} \quad a \mapsto x^a \quad \text{is not injective.}$$

Hence, there exist distinct positive integers a and b such that $x^b = x^a$. Without loss of generality, suppose $a < b$. Applying **(ii)** again, it follows that $x^{b-a} = 1_G \in H$, so H is closed under identity.

Lastly, we verify that H is closed under inversion. To see why this is true, for any $a \in \mathbb{Z}_{\geq 0}$ (the subscript can include 0 since we previously established that H is closed under identity), we have $x^a \in H$, so $x^{b-a-1} \in H$. It follows that

$$x \cdot x^{b-a-1} = x^{b-a} = 1_G \quad \text{so} \quad x^{-1} = x^{b-a-1} \in H,$$

which implies H is closed under inversion. Hence, $H \leq G$. □

Example 2.2. We have $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ under addition.

Example 2.3. We have $\mathbb{Z}^\times \leq \mathbb{Q}^\times \leq \mathbb{R}^\times \leq \mathbb{C}^\times$ under multiplication.

Having said all these, note that $\mathbb{Q}^\times$ and $\mathbb{R}^\times$ are not subgroups of $\mathbb{R}$ even though these sets are subsets of $\mathbb{R}$. For example, to see why, we see that $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ so $\mathbb{R}^\times$ excludes the additive identity of $\mathbb{R}$ which is 0. Moreover, $\mathbb{R}^\times$ is not closed under addition, so it does not satisfy the subgroup criterion (Proposition 2.1).

Moreover, $\mathbb{Z}^+$ is not a subgroup of $\mathbb{Z}$ under addition even though $\mathbb{Z}^+$ is closed under addition. This is because $\mathbb{Z}^+$ does not contain the additive identity of $\mathbb{Z}$ which is 0.

Example 2.4 (subgroups of $\mathbb{Z}$). We shall discuss some subgroups of $\mathbb{Z}$. For any $n \in \mathbb{Z}_{\geq 0}$, define the subset

$$n\mathbb{Z} \quad \text{to be} \quad \text{the set of integer multiples of } n.$$

Equivalently, we have

$$\begin{aligned} n\mathbb{Z} &= \{nk \in \mathbb{Z} : k \in \mathbb{Z}\} \\ &= \{a \in \mathbb{Z} : \text{there exists } k \in \mathbb{Z} \text{ such that } a = nk\} \end{aligned}$$

We shall verify that that $n\mathbb{Z} \leq \mathbb{Z}$ using the subgroup criterion (Proposition 2.1). Firstly, note that $0 \in n\mathbb{Z}$ which follows by setting $k = 0$, so $n\mathbb{Z}$ is non-empty. Then, let $x, y \in n\mathbb{Z}$, i.e.

$$\text{there exist } k_1, k_2 \in \mathbb{Z} \quad \text{such that} \quad x = nk_1 \text{ and } y = nk_2.$$

Note that $y^{-1} = -nk_2$, which is the additive inverse of y in $\mathbb{Z}$. Hence,

$$x * y^{-1} = nk_1 + (-nk_2) = n(k_1 - k_2 \in n\mathbb{Z} \quad \text{since } k_1 - k_2 \in \mathbb{Z}.$$

Here, our choice of the symbol $*$ is apt since it is arbitrary, but keep in mind that the group operation is addition.

For example,

$$0\mathbb{Z} = \{0\} \quad 1\mathbb{Z} = \mathbb{Z} \quad 2\mathbb{Z} = \{\text{all even integers}\}.$$

Theorem 2.1. For any $H \leq \mathbb{Z}$,

$$\text{there exists a unique } n \in \mathbb{Z}_{\geq 0} \quad \text{such that} \quad H = n\mathbb{Z}.$$

Proof. Let $H \leq \mathbb{Z}$. Then, by Proposition 2.1, $H \neq \emptyset$. Hence, $0 \in H$. If $H = \{0\}$, then we are done since $H = 0\mathbb{Z}$.

On the other hand, if $H \neq \{0\}$, by the well-ordering principle, H contains a least element, say n. We claim that $H = n\mathbb{Z}$, starting by proving the reverse inclusion $n\mathbb{Z} \subseteq H$. Since $n \in H$ and H is closed under addition and inverses, then any integer multiple of n, say kn for $k \in \mathbb{Z}$, is also contained in H. So, the reverse inclusion follows.

We then prove the forward inclusion $H \subseteq n\mathbb{Z}$. Suppose $x \in H$. By the division algorithm, there exist $q, r \in \mathbb{Z}$ such that

$$x = qn + r \quad \text{where } 0 \leq r < n.$$

Since $n \in H$, then as H is closed under multiplication, we have $qn \in H$. So, $r = x - qn \in H$ as H is closed under subtraction (combination of closure under addition and inverse). By the minimality of n, we have $r = 0$, otherwise r would be a smaller positive element in H. Hence, $x = qn \in n\mathbb{Z}$, proving that $H \subseteq n\mathbb{Z}$. ☐

Example 2.5 (subgroups of groups of small order)**.** Let G be a group of small order.

(i) If $|G| = 1$, then the only subgroup of G is the trivial group $\{e\}$.

(ii) If $|G| = 2$, say $G = \{e,a\}$, then the only subgroups of G are the trivial group $\{e\}$ and $\{e,a\}$.

(iii) If $|G| = 3$, say $G = \{e,a,b\}$, then the only subgroups of G are the trivial group $\{e\}$ and $\{e,a,b\}$.

(iv) We give a glimpse of groups of order 4, and in fact, there are two possibilities up to isomorphism. Say $G = \{e,a,b,c\}$.

In Table 12, we have the Cayley table for $G = \mathbb{Z}/4\mathbb{Z}$ (we will explain what this means in a moment; as of now, appreciate the structure of the group table). Just to recap, we see that a and c are generators, but b is not (because we can neither obtain a nor c from b).

We see that the subgroups of $G = \mathbb{Z}/4\mathbb{Z}$ are

$$\{1\}, G, \{1,a\}, \{1,b\}, \{1,c\}.$$

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Table 12: Cayley table for $\mathbb{Z}/4\mathbb{Z}$ (cyclic group of order 4)

We mentioned that Table 12 is the Cayley table for $G = \mathbb{Z}/4\mathbb{Z}$. This is known as the *quotient group* $\mathbb{Z}$ modulo $4\mathbb{Z}$ (will be covered in Definition 3.12), but this simply means the set of possible remainders when an integer is divided by 4, so

$$\mathbb{Z}/4\mathbb{Z} = \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\right\}$$

The bar notation represents the equivalence classes of integers modulo 4. Specifically, $\overline{a} = \{\ldots, -2a, -a, 0, a, 2a, \ldots\}$ denotes the set of integers that have the same remainder as a when divided by 4. Similarly, we see that $\overline{1}$ and $\overline{3}$ are the only generators of the group.

Moreover, here is a fun fact. Let $e = 1$, $b = -1$, $a = i$ and $c = -i$. Then, we obtain the following Cayley table. This corresponds to the multiplicative group of the fourth roots of unity (i.e. solutions to $z^4 = 1$, where $z \in \mathbb{C}$) generated by $i = \sqrt{-1}$ (similar to the previous setups, $-i$ is also a generator)!

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Table 13: A *familiar* Cayley table?

In Table 14, we have the Cayley table for $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which refers to the direct product (recall Definition 1.5) of the quotient groups $\mathbb{Z}/2\mathbb{Z}$ and itself. Observe that every non-identity element satisfies the relation $a^2 = e$ (we say that the element a is an *involution* since it is equal to its inverse). A less-obvious relation is $(ab)^2 = e$.

The subgroups of $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are

$$\{1\}, G, \{1, b\}.$$

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Table 14: Cayley table for $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (Klein four-group V)

At the end of Example 2.5, we mentioned that the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is known as the Klein four-group V.

Definition 2.3 (Klein four-group)**.** The Klein four-group V is an Abelian group with four elements e, a, b, c, in which each element is involutory/self-inverse, i.e. composing it with itself produces the identity. Moreover, composing any two of the three non-identity elements produces the third one.

V can be defined by the following group presentation (recall Example 1.66):

$$V = \left\langle a, b \mid a^2 = b^2 = (ab)^2 = e \right\rangle$$

Example 2.6 (Dummit and Foote p. 48 Question 5)**.** Prove that G cannot have a subgroup H with $|H| = n - 1$, where $n = |G| > 2$.

Solution. Suppose on the contrary that such a subgroup H exists. Then, there exists a non-identity element $x \in H$ and an element $y \notin H$. Consider the product xy. If $xy \in H$, then $x^{-1} \in H$, so $y \in H$ (since $H \leq G$), which leads to a contradiction. On the other hand, if $xy \notin H$, then $xy = y$, which implies $x = 1$, which again is a contradiction[†]. $\square$

Example 2.7 (Dummit and Foote p. 48 Question 8)**.** Let H and K be subgroups of G. Prove that

$$H \cup K \text{ is a subgroup} \quad \text{if and only if} \quad \text{either } H \subseteq K \text{ or } K \subseteq H.$$

Solution. We first prove the forward direction. Suppose on the contrary that neither $H \subseteq K$ nor $K \subseteq H$. Then, choose $h \in H \setminus K$ and $k \in K \setminus H$, which implies $h \notin K$ and $k \notin H$. Since $hk \in H \cup K$ (given that $H \cup K \leq G$), we shall consider two cases.

- **Case 1:** Suppose $hk \in H$. Then, because $h^{-1} \in H$, then $h^{-1}hk = k$, which contradicts the closure property of subgroups as we earlier mentioned that $k \notin H$.
- **Case 2:** Suppose $hk \in K$. Same as Case 1, we reach a contradiction.

We now prove the reverse direction. Suppose either $H \subseteq K$ or $K \subseteq H$. Then, $H \cup K = K$ or $H \cup K = H$ respectively. Note that in each case, $K \leq G$ and $H \leq G$, which implies $H \cup K \leq G$. $\square$

Example 2.8 (Dummit and Foote p. 48 Question 10)**.**

(a) Prove that if H and K are subgroups of G then so is their intersection $H \cap K$.

(b) Prove that the intersection of an arbitrary non-empty collection of subgroups of G is again a subgroup of G (do not assume the collection is countable)

Solution.

(a) First, note that the intersection is non-empty since $1 \in H$ and $1 \in K$ implies $1 \in H \cap K$.

Next, consider $x, y \in H \cap K$. Then, $x, y \in H$ and $x, y \in K$. Since $y \in H$, then $y^{-1} \in H$, so $xy^{-1} \in H$. Similarly, $xy^{-1} \in K$, so $xy^{-1} \in K$. By the subgroup criterion (Proposition 2.1), $H \cap K \leq G$.

(b) Same as **(a)**, the intersection is non-empty. Now, let $H_1, \ldots \leq G$. Define their intersection as follows:

$$X = \bigcap_i H_i \quad \text{where } H_i \leq G \text{ for all } i.$$

Consider $a, b \in X$. Then, $a, b \in H_i$ for all i. Since each $H_i \leq G$, then $ab^{-1} \in H_i$ for all i, which implies

$$ab^{-1} \in \bigcap_i H_i = X.$$

By the subgroup criterion (Proposition 2.1), the intersection is a subgroup of G. $\square$

Example 2.9 (Dummit and Foote p. 49 Question 15)**.** Let $H_1 \leq H_2 \leq \ldots$ be an ascending chain of subgroups of G. Prove that

$$\bigcup_{i=1}^{\infty} H_i \quad \text{is} \quad \text{a subgroup of } G.$$

Solution. Let H denote the union. Since $1_G \in H_i$ for all $i \in \mathbb{N}$, then $1_G \in H$, so H is non-empty. Next, let $a, b \in H$, so there exist $i, j \in \mathbb{N}$ such that $a \in H_i$ and $b \in H_j$. Take $k = \max\{i, j\}$ so $a, b \in H_k$. Hence, $ab^{-1} \in H_k$, and we conclude that $ab^{-1} \in H$. By the subgroup criterion (Proposition 2.1), $H \leq G$. $\square$

We then discuss the kernel and image of a homomorphism. These are analogous to the nullspace and column space of the matrix representation of a linear transformation respectively (recall MA2001).

[†] In fact, one can use Lagrange's theorem (Theorem 3.1) and make the same conclusion. That is, assuming that $H \leq G$, we must have $(n-1) \mid n$, which clearly does not.

Definition 2.4 (kernel and image). Let $\varphi : G \to H$ be a homomorphism. The kernel of ϕ and image of φ are defined as follows respectively:

$$\ker \varphi = \{g \in G : \varphi(g) = 1_H\}$$
$$\operatorname{im} \varphi = \{\varphi(g) \in H : g \in G\}$$

Equivalently, $\operatorname{im}(\varphi)$ is the set of all $h \in H$ where there exists $g \in G$ such that $h = \varphi(g)$.

Proposition 2.3. Let $\varphi : G \to H$ be a homomorphism. Then,

$$\ker \varphi \text{ is a subgroup of } G \quad \text{and} \quad \operatorname{im} \varphi \text{ is a subgroup of } H.$$

Again, recall that there is an analogous result in MA2001, which mentions that if V and W are vector spaces and

$$T : V \to W \text{ is a linear transformation from } V \text{ to } W \quad \text{with} \quad \text{matrix representation } \mathbf{A},$$

then the nullspace of $\mathbf{A}$ is a subspace of V and the column space of $\mathbf{A}$ is a subspace of W. We now prove Proposition 2.3.

Proof. We first prove that $\ker \varphi \leq G$. Iti s clear that $1_G \in \ker \varphi$, so $\ker \varphi \neq \emptyset$. Next, let $x, y \in \ker \varphi \subseteq G$. Then,

$$\varphi\left(xy^{-1}\right) = \varphi(x)\varphi\left(y^{-1}\right) = \varphi(x)[\varphi(y)]^{-1} = 1_H 1_H^{-1} = 1_H$$

where the second last equality follows from the fact that φ respects identity, i.e. $1_H = \varphi(1_G) \in \operatorname{im} \varphi$. It follows that $xy^{-1} \in \ker \varphi$, so by the subgroup criterion (Proposition 2.1), $\ker \varphi \leq G$.

We then prove that $\operatorname{im} \varphi \leq H$. By definition of im, we see that it is non-empty. Let $x, y \in \operatorname{im} \varphi \subseteq H$. Then, by definition,

$$\text{there exist } a, b \in G \quad \text{such that} \quad x = \varphi(a) \text{ and } y = \varphi(b) \text{ in } H.$$

Hence,

$$xy^{-1} = \varphi(a)[\varphi(b)]^1 = \varphi(a)\varphi\left(b^{-1}\right) = \varphi\left(ab^{-1}\right)$$

with $ab^{-1} \in G$, which follows that $xy^{-1} \in \operatorname{im} \varphi$. Again, by the subgroup criterion (Proposition 2.1), we conclude that $\operatorname{im} \varphi \leq G$[†]. □

Example 2.10. Consider the identity homomorphism

$$\mathrm{id}_G : G \to G,$$

where it is clear that $\ker(\mathrm{id}_G) = \{1_G\}$, which is the trivial subgroup of G, and $\operatorname{im}(\mathrm{id}_G) = G$, which is the improper subgroup of G.

[†] $\operatorname{im}(\varphi) \leq H$ appears as a problem in Question p. 40 Question 13 of the Dummit and Foote textbook. Moreover, the reader is asked to deduce that if φ is injective, then $G \cong \varphi(G)$. This can also be seen as an application of the first isomorphism theorem (Theorem 3.6) which we will encounter in due course.

Example 2.11. Let

$$\varphi : G \to H \quad \text{be an isomorphism.}$$

Then, $\ker \varphi = \{1_G\}$, which is the trivial subgroup of G, and $\operatorname{im} \varphi = H$, which is the improper subgroup of H.

We give a generalisation of this example. Let

$$\varphi : G \hookrightarrow H \text{ be an injective homomorphism} \quad \text{and} \quad \psi : G \twoheadrightarrow H \text{ be a surjective homomorphism.}$$

Then, $\ker \varphi = \{1_G\}$ and $\operatorname{im} \psi = H$. Also, we recall that an injective homomorphism is known as a monomorphism, whereas a surjective homomorphism is known as an *epimorphism*.

Example 2.12. Consider the homomorphisms

$$\begin{aligned} \varphi : 1 \to G &\quad \text{which has} \quad \ker = 1 \text{ and } \operatorname{im} = \{1_G\} \\ \psi : G \to 1 &\quad \text{which has} \quad \ker = G \text{ and } \operatorname{im} = 1 \end{aligned}$$

Example 2.13. We shall find the homomorphism from S_2 to S_3 and determine the kernels and images. First, note that any homomorphism $\varphi : S_2 \to S_3$ must map the identity in S_2 to S_3.

Let $a = (1\ 2)$ denote the non-identity element in S_2, i.e. the transposition. Since $a \cdot a = e$, then applying φ to both sides yields

$$\varphi(a \cdot a) = \varphi(e) \quad \text{so} \quad [\varphi(a)]^2 = e$$

So, $\varphi(a)$ must have order dividing 2 in S_3, i.e. $\varphi(a)$ can only be mapped to elements of S_3 with order 2 or the identity. The elements in S_3 with order 2 are the transpositions $(1\ 2)$, $(1\ 3)$, and $(2\ 3)$. We can define three homomorphism by mapping a to each of these transpositions. Each choice gives a valid homomorphism since a single non-identity element in S_2 generates the group. Hence,

$$\ker \varphi = \{1_{S_2}\} \quad \text{and} \quad \operatorname{im} \varphi = \{e, (1\ 2)\} \text{ or } \{e, (1\ 3)\} \text{ or } \{e, (2\ 3)\}$$

Here, $e = \varepsilon$ denotes the identity permutation on S_3 (recall that this can be applied to S_n in general).

Example 2.14. One checks that the map $S_3 \to S_2$, where

$$1, (1\ 2\ 3) \mapsto 1_{S_2} \quad \text{and} \quad (1 2), (1 3), (2 3) \mapsto a$$

is a homomorphism with kernel $\{1, (123), (132)\} \subseteq S_3$ and image S_2.

Example 2.15 (Dummit and Foote p. 40 Question 15)**.** Define a map

$$\pi : \mathbb{R}^2 \to \mathbb{R} \quad \text{by} \quad \pi((x,y)) = x.$$

Prove that π is a homomorphism and find the kernel of π.

Solution. We first prove that π is a homomorphism. Suppose $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$. Then,

$$\pi((x_1 + x_2, y_1 + y_2)) = x_1 + x_2 = \pi((x_1, y_1)) + \pi((x_2, y_2)),$$

where we used the fact that the structure we are working with is additive. We then determine $\ker \pi$. Suppose $\pi((x,y)) = 0$, where 0 is the additive identity of $\mathbb{R}$. Then, we must have $x = 0$, while $y \in \mathbb{R}$ is arbitrary. We conclude that

$$\ker \pi = \left\{(x,y) \in \mathbb{R}^2 : x = 0\right\},$$

which is precisely the y-axis! $\square$

It turns out that the map

$$\pi : \mathbb{R}^2 \to \mathbb{R} \quad \text{where} \quad \pi((x,y)) = x$$

defined in Example 2.15 is known as a projection map. The fact that (x,y) is mapped to x for every projection map π means that π maps a 2-tuple to its first coordinate. The geometric interpretation is as follows: consider a point in $\mathbb{R}^2$. Then, π returns the x-coordinate of this point.

Example 2.16 (Dummit and Foote p. 40 Question 16)**.** Let A and B be groups and let G be their direct product, $A \times B$. Prove that the maps

$$\pi_1 : G \to A \text{ and } \pi_2 : G \to B \quad \text{defined by} \quad \pi_1((a,b)) = a \text{ and } \pi_2((a,b)) = b$$

are homomorphisms and find their kernels.

Solution. The proof that π_1 and π_2 are homomorphisms uses the same idea as mentioned in Example 2.15, and we note that π_1 denotes projection onto the first coordinate, whereas π_2 denotes projection onto the second coordinate. Again, similar to Example 2.15, $\ker \pi_1$ is the y-axis, whereas $\ker \pi_2$ is the x-axis. □

Definition 2.5 (torsion subgroup)**.** Let G be an Abelian group. Then, the set

$$G_T = \{g \in G : |g| < \infty\}$$

is known as the torsion subgroup of G.

Proposition 2.4. The torsion subgroup G_T of an Abelian group G is indeed a subgroup.

Proof. See the first part of Example 2.17. □

Example 2.17 (Dummit and Foote p. 48 Question 6)**.** Let G be an Abelian group. Prove that $\{g \in G : |g| < \infty\}$ is a subgroup of G (called the torsion subgroup of G). Give an explicit example where this set is not a subgroup when G is non-Abelian.

Solution. Note that G_T (notation used in Definition 2.5) is the set of all elements of G with finite order. Clearly, $G_T \neq \emptyset$ since $e \in G$ which is of order 1. Next, let $g_1, g_2 \in G_T$. Then, there exist $m, n \in \mathbb{Z}^+$ such that

$$g_1^m = e \quad \text{and} \quad g_2^n = e.$$

Without loss of generality, assume that $m \geq n$. So,

$$\begin{aligned}
\left(g_1 g_2^{-1}\right)^{mn} &= (g_1)^{mn} \left(g_2^{-1}\right)^{mn} \quad \text{since } G \text{ is Abelian} \\
&= [(g_1)^m]^n \cdot \left[\left(g_2^{-1}\right)^n\right]^m
\end{aligned}$$

which is equal to $e \cdot e = e$. By the subgroup criterion (Proposition 2.1), $G_T \leq G$.

For the second part, consider the group of invertible functions from $\mathbb{R}$ to $\mathbb{R}$ under function composition. Let

$$f, g : \mathbb{R} \to \mathbb{R} \quad \text{where} \quad f(x) = -x \text{ and } g(x) = 1 - x.$$

Then, $|f| = |g| = 2$ but $f \circ g$, given by $x \mapsto x - 1$, has infinite order. □

Example 2.18 (Dummit and Foote p. 85 Question 8)**.** Let $\varphi : \mathbb{R}^\times \to \mathbb{R}^\times$ be the map sending x to the absolute value of x. Prove that φ is a homomorphism and find the image of φ. Describe the kernel and the fibers of φ.

Solution. We have $\varphi(x) = |x|$. Since $|xy| = |x||y|$, it follows that $\varphi(xy) = \varphi(x)\varphi(y)$, so φ is a homomorphism. Also, note that $\operatorname{im}\varphi = \mathbb{R}^+$. Also, one checks that $\ker\varphi = \{-1,1\}$ since $\varphi(1) = \varphi(-1) = 1$. Lastly, for any $a \in \mathbb{R}$, the fiber over $a \in \mathbb{R}$ is $\{-a,a\}$. $\square$

Example 2.19. For any $n \in \mathbb{Z}$, the multiplication-by-n map

$$n^* : \mathbb{Z} \to \mathbb{Z} \quad \text{where} \quad a \mapsto na$$

is a homomorphism. This respects addition in $\mathbb{Z}$ due to the distributive law $n \cdot (a+b) = n \cdot a + n \cdot b$.

We also note that

$$\ker n^* = \begin{cases} \{0\} \subseteq \mathbb{Z} & \text{if } n \neq 0; \\ \mathbb{Z} & \text{if } n = 0 \end{cases} \quad \text{and} \quad \operatorname{im} n^* = n\mathbb{Z}.$$

We first verify that the result on $\ker n^*$ holds. If $n = 0$, then any $a \in \mathbb{Z}$ is mapped to 0 (important to recognise that this is the additive identity of $\mathbb{Z}$) under $n0^*$; if $n \neq 0$, say $a \mapsto na$ under n^*. Setting $na = 0$ (additive identity of $\mathbb{Z}$), we have

$$a = 0 \quad \text{or} \quad n = 0 \quad \text{but we can conclude that} \quad a = 0.$$

In fact, there is a *hidden* property of $\mathbb{Z}$ which we implicitly used here, which is that it is an integral domain (will encounter in MA3201 formally), i.e. an algebraic structure whereby

$$\text{the product of non-zero elements} \quad \text{is non-zero.}$$

Note that the contraposition of this statement is that

$$\text{if the product of two elements is zero,} \quad \text{then at least one of the elements is zero.}$$

To see why $\operatorname{im} n^* = |n|\mathbb{Z}$, recall by definition of im that

$$\operatorname{im} n^* = \{na : a \in \mathbb{Z}\} \quad \text{which is the set of all multiples of } n.$$

Theorem 2.2. For any homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}$,

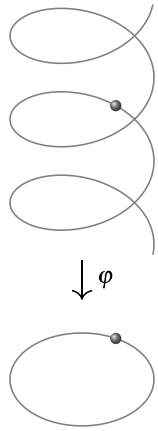
$$\text{there exists a unique } n \in \mathbb{Z} \quad \text{such that} \quad \varphi = n^*.$$

Note that this is similar to Theorem 2.1.

Example 2.20 (Dummit and Foote p. 86 Question 12)**.** Let G be the additive group of real numbers, let H be the multiplicative group of complex numbers of absolute value 1 (the unit circle $\mathbb{S}^1$ in the complex plane) and let

$$\varphi : G \to H \quad \text{be the homomorphism} \quad \varphi : r \mapsto e^{2\pi i r}.$$

Draw the points on a real line which lie in the kernel of φ. Describe similarly the elements in the fibers of φ above the points -1, i, and $e^{4\pi i/3}$ of H.



Solution. Note that the identity element of H is 1_H. Let $\varphi : r \mapsto e^{2\pi ir}$ be a homomorphism. Then, if $\varphi(r) = 1_H$, then $\cos 2\pi r = 1$ and $\sin 2\pi r = 0$ (in fact, these two statements are equivalent). Solving yields $r \in \mathbb{Z}$, which implies $\ker \varphi = \mathbb{Z}$ (sketching the points on $\mathbb{R}$ is trivial).

Next, say $\varphi(r) = -1$. Then, $\cos 2\pi r = -1$ and $\sin 2\pi r = 0$. Hence, $2r$ must be an odd integer, i.e. there exists $n \in \mathbb{Z}$ such that $2r = 2n+1$. Hence, $r = n + 1/2$, where $n \in \mathbb{Z}$, i.e.

$$\varphi * (1) = \left\{ n + \frac{1}{2} : n \in \mathbb{Z} \right\}$$

If $\varphi(r) = i$, then $\cos 2\pi r = 0$ and $\sin 2\pi r = 1$. Solving yields $r = n + 1/4$ for some $n \in \mathbb{Z}$. Hence,

$$\varphi^*(i) = \left\{ n + \frac{1}{4} : n \in \mathbb{Z} \right\}.$$

Lastly, if $\varphi(r) = e^{4\pi i/3}$, then $\cos 2\pi r = \cos 4\pi/3$ and $\sin 2\pi r = \sin 4\pi/3$. From the first equation, $2\pi r = 2\pi n + 4\pi/3$ for some $n \in \mathbb{Z}$. Hence, $r = n \pm 2/3$. However, the second equation would imply $r = n + 2/3$. To conclude,

$$\varphi^*\left(e^{4\pi i/3}\right) = \left\{ n + \frac{2}{3} : n \in \mathbb{Z} \right\}.$$

We give a remark that Question 13 from the same exercise set in the Dummit and Foote textbook is a slight modification of the question, where the homomorphism is now changed to $\varphi : r \mapsto e^{4\pi ir}$. □

Example 2.21 (Dummit and Foote p. 49 Question 13). Let H be a subgroup of the additive group of rational numbers with the property that $1/x \in H$ for every non-zero element x of H. Prove that $H = 0$ or $\mathbb{Q}$.

Solution. Since $H \leq \mathbb{Q}$, then H itself is a group so $0 \in H$. If there does not exist any non-zero element in H, then we can take $H = 0$.

On the other hand, if H contains at least one non-zero element x, it must be rational. Without loss of generality, say there exist $p, q \in \mathbb{N}$, with $q \neq 0$ such that $x = p/q$. Since $(\mathbb{Q}, +)$ is an additive group, then it is closed under addition, i.e.

$$qx = \underbrace{\frac{p}{q} + \ldots + \frac{p}{q}}_{q \text{ times}} = p \quad \text{is also } \in H.$$

We use the fact that H contains at least one non-zero element to deduce that $p \neq 0$. So, $1/p \in H$. In a similar vein, we deduce that

$$p\left(\frac{1}{p}\right) = \underbrace{\frac{1}{p} + \ldots + \frac{1}{p}}_{p \text{ times}} = 1$$

so $1 \in H$. Since H is closed under addition and inverses, we deduce that $\mathbb{Z} \subseteq H$.

We now prove that $\mathbb{Q} \subseteq H$. Let $r \in \mathbb{Q}$ be an arbitrary non-zero rational number. Then, there exist $p, q \in \mathbb{Z}$ with $q \neq 0$ such that $r = p/q$. Since $q \in H$, then $1/q \in H$. As such, $r \in H$, which implies $\mathbb{Q} \subseteq H$. As $H \subseteq \mathbb{Q}$ as well, we deduce that $H = \mathbb{Q}$. □

2.2 Centralizers and Normalizers, Stabilizers and Kernels

Definition 2.6 (conjugate and conjugacy class). Let G be a group and $a \in G$ be any element of G. For any $g \in G$,

$$\text{the element } gag^{-1} \in G \quad \text{is called} \quad \text{the } g\text{-conjugate of } a.$$

Some would also refer to this as the conjugate of a by g.

The conjugates of a in G are the gag^{-1} for $g \in G$, and we define this set to be the G-conjugacy class of a. One sees that this is equivalent to the following set:

$$\left\{x \in G : \text{there exists } g \in G \text{ such that } x = gag^{-1}\right\}$$

Definition 2.7 (centralize and centralizer). The element $g \in G$ centralizes a

$$\text{if and only if} \quad gag^{-1} \text{ or equivalently, } ga = ag.$$

So, $g \in G$ centralizes a if and only if g commutes with a.

The centralizer of a in G is the set

$$C_G(a) = \{g \in G : g \text{ centralizes } a\} = \left\{g \in G : gag^{-1} = a\right\}.$$

The centralizer of A in G is the set

$$\begin{aligned} C_G(A) &= \{g \in G : g \text{ centralizes } A\} \\ &= \left\{g \in G : \text{for all } a \in A, \text{ we have } gag^{-1} = a\right\} \end{aligned}$$

Example 2.22 (Dummit and Foote p. 52 Question 1). Prove that

$$C_G(A) = \left\{g \in G : g^{-1}ag = a \text{ for all } a \in A\right\}.$$

Solution. Recall Definition 2.7. Replacing g with g^{-1} yields the desired result. □

Definition 2.8 (normalize and normalizer). The element $g \in G$ normalizes a

$$\text{if and only if} \quad gAg^{-1} = A \text{ as a subset of } G.$$

The normalizer of $a \in G$ is the set

$$N_G(A) = \{g \in G : g \text{ normalizes } A\} = \left\{g \in G : gAg^{-1} = A\right\}.$$

Definition 2.9 (center). The center of a group G is the set

$$\begin{aligned} Z(G) &= \left\{g \in G : \text{for all } a \in G : gag^{-1} = a\right\} \\ &= \{g \in G : \text{for all } a \in G : ga = ag\} \end{aligned}$$

Example 2.23 (Dummit and Foote p. 52 Question 7). Let $n \in \mathbb{Z}$ with $n \geq 3$. Prove the following:

(a) $Z(D_{2n}) = 1$ if n is odd

(b) $Z(D_{2n}) = \left\{1, r^{2k}\right\}$ if $n = 2k$

Solution.

(a) Suppose $r^k \in Z(D_{2n})$ for $k \in \mathbb{Z}^+$. Since $sr^k = r^{-k}s$ (obtained by repeatedly applying $rs = sr^{-1}$), we have $r^k = r^{-k}$. Hence, $r^{2k} = e$ and we see that $2 \mid n$, which is a contradiction.

s cannot be in the center since it does not commute with r. Now suppose $sr^k \in Z(D_{2n})$, with $k \in \mathbb{Z}^+$. In order to commute with r, we must have $\left(sr^k\right) r = r\left(sr^k\right)$, so $sr^{k+1} = sr^{k-1}$. As such, $r^{k+1} = r^{k-1}$ and we see that $r^2 = e$, which means $n \leq 2$, another contradiction. The result follows.

(b) From the proof of **(a)**, we know that the only possible candidates are e and r^k where $n = 2k$. Since $r^{2k} = e$, then$r^k = r^{-k}$. Any element x in D_{2n} can be written as $x = s^i r^j$ for $i \in \{0, 1\}$ and $j \geq 0$, so,

$$r^k\left(s^i r^j\right) = s^i r^{-k} r^j = s^i r^k r^j = s^i r^{k+j} = \left(s^i r^j\right) r^k.$$

The result follows. □

Proposition 2.5. We have the following obvious results, which need not be memorised:

(i) For any $a \in G$, we have $C_G(a) = C_G(\{a\}) = N_G(\{a\})$

(ii) For any $A \subseteq G$, we have

$$C_G(A) = \bigcap_{a \in A} C_G(a) \quad \text{and} \quad C_G(A) \subseteq N_G(A)$$

(iii) We have

$$Z(G) = C_G(G) = \bigcap_{a \in G} C_G(a) \quad \text{and} \quad N_G(G) = G$$

(iv) We have

$$C_G(1_G) = N_G(\{1_G\}) = G \quad \text{or equivalently} \quad 1_G \in Z_G$$

(v) G is Abelian if and only if $Z(G) = G$

Example 2.24 (Dummit and Foote p. 52 Question 2). Prove that

$$C_G(Z(G)) = G \quad \text{and deduce that} \quad N_G(Z(G)) \leq G$$

Solution. Recall Definitions 2.7 and 2.9 on the centralizer and center of a group. We have

$$\begin{aligned} C_G(Z(G)) &= \left\{g \in Z(G) : \text{for all } a \in Z(G)\text{, we have } gag^{-1} = a\right\} && \text{by Definition 2.7} \\ &= \left\{g \in G : \text{for all } a \in G\text{, we have } agg^{-1} = a\right\} && \text{by Definition 2.9} \\ &= \{g \in G : \text{for all } a \in G\text{, we have } a = a\} \end{aligned}$$

which is equal to G.

We then prove the second result. Since $C_G(A), N_G(A) \subseteq G$ (this is actually a consequence of Proposition 2.6 which we will mention in due course; we will also use the fact that $H \leq G$ implies $H \subseteq G$) and $C_G(A) \subseteq N_G(A)$ ((**ii**) of Proposition 2.5), the second result follows. □

Proposition 2.6. For any $A \subseteq G$, we have

$$C_G(A), N_G(A) \leq G.$$

Proof. The proofs are quite easy to establish. We first prove that $C_G(A) \leq G$. It is clear that $1_G \in C_G(A)$ since for any $a \in A$, $1_G \cdot a \cdot 1_G^{-1} = a$. Next, let $x, y \in C_G(A)$. Then,

$$y^{-1} \in C_G(A) \quad \text{since for any } a \in A \text{ we have } yay^{-1} = a \text{ so } a = y^{-1}ay$$

So,

$$xy^{-1} \in C_G(A) \quad \text{since for any } a \in A \text{ we have } (xy)a(xy)^{-1} = xyay^{-1}x^{-1} = x\left(yay^{-1}\right) = xax^{-1} = a$$

so by the subgroup criterion, we conclude that $C_G(A) \leq G$.

We then prove that $N_G(A) \leq G$. Again, it is clear that $1_G \in N_G(A)$ since $1_G \cdot A \cdot 1_G^{-1} = A$. Next, let $x, y \in N_G(A)$. Then, similar to our proof that $C_G(A) \leq G$, one can easily do the same for $N_G(A)$. □

Example 2.25 (Dummit and Foote p. 52 Question 3)**.** Prove that if A and B are subsets of G with $A \subseteq B$, then

$$C_G(B) \quad \text{is a subgroup of} \quad C_G(A)$$

Solution. Suppose $x \in C_G(B)$. Then, for every $b \in B$, we have $xbx^{-1} = b$. Since $A \subseteq B$, then for any $a \in A$, we have $xax^{-1} = a$. Hence, $x \in C_G(A)$. It follows that $C_G(B) \subseteq C_G(A)$. By Proposition 2.6, $C_G(A)$ is a group, so the result follows. □

Example 2.26 (Dummit and Foote p. 52 Question 6)**.** Let H be a subgroup of the group G.

(a) Show that $H \leq N_G(H)$. Give an example to show that this is not necessarily true if H is not a subgroup.

(b) Show that $H \leq C_G(H)$ if and only if H is Abelian.

Solution.

(a) By Definition 2.8, the normalizer $N_G(H)$ is defined as follows:

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

Take $g \in H$ and $x \in gHg^{-1}$. Then, there exists $h \in H$ such that $x = ghg^{-1}$. Since $H \leq G$, then $x \in H$ so $gHg^{-1} \subseteq H$. The other inclusion $H \subseteq gHg^{-1}$ holds too, so it follows that $gHg^{-1} = H$. Hence, $g \in N_G(H)$. As $H \subseteq N_G(H)$, we conclude that $H \leq N_G(H)$ by Definition 2.1.

However, if H is not a subgroup, the aforementioned property may not hold. Take for example the dihedral group $G = D_8$ (symmetries of a square) and $H = \{1, r, s\}$. Note that H is not a subgroup of G as we have $r, s \in H$ but $rs \notin H$. We shall prove that $sHs \neq H$[†]. We have

$$sHs = \{s1s, srs, sss\} = \left\{s^2, srs, s^3\right\} = \left\{1, r^2, s\right\} \neq H.$$

[†]Throughout this chapter, we have been exploring the concept of the normalizer. Formally, the notation sHs can be interpreted as a *coset*. This idea will be revisited in Definition 3.1.

(b) We first prove the forward direction. Suppose $H \le C_G(H)$. Take $a,b \in H$ with $a \in C_G(H)$. So,

$$aba^{-1} = b$$

which implies $ab = ba$, showing that H is Abelian.

The proof of the reverse direction is pretty much the same — given $a,b \in H$ where $ab = ba$, we have $aba^{-1} = b$, so $a \in C_G(H)$. The result follows. □

Example 2.27 (Dummit and Foote p. 53 Question 9)**.** For any subgroup H of G and any non-empty subset A of G, define

$$N_H(A) = \left\{h \in H : hAh^{-1} = A\right\}.$$

Show that $N_H(A) = N_G(A) \cap H$ and deduce that $N_H(A)$ is a subgroup of H (note that A need not be a subset of H).

Solution. We first prove that

$$N_H(A) = N_G(A) \cap H.$$

We start by proving the forward inclusion $N_H(A) \subseteq N_G(A) \cap H$. Note that $N_H(A) \subseteq N_G(A)$ since every $h \in N_H(A)$ is also an element of G for which $hAh^{-1} = A$. Moreover, as $N_H(A) \subseteq H$, the inclusion holds.

As for the reverse inclusion, choose $h \in N_G(A) \cap H$. Since $h \in N_G(A)$, we have $hAh^{-1} = A$. Also, since $h \in H$, then $h \in N_H(A)$, which proves this inclusion.

It follows that $N_H(A) = N_G(A) \cap H$. Since $N_G(A)$ and H are subgroups, by **(a)** of Example 2.8 on the intersection of two subgroups also being a subgroup, we conclude that $N_H(A) \le H$. □

Example 2.28 (Dummit and Foote p. 53 Question 10)**.** Let H be a subgroup of order 2 in G. Show that $N_G(H) = C_G(H)$. Deduce that if $N_G(H) = G$, then $H \le Z(G)$.

Solution. Since H is of order 2, then it has two elements. Say $H = \{e, a\}$, where e is the identity element.

Take $x \in N_G(H)$, so $xex^{-1} = e$ and $xax^{-1} = a$. As such, $x \in C_G(H)$. Similarly, take $y \in C_G(H)$, so $yey^{-1} = e$ and $yay^{-1} = a$. As such, $y \in N_G(H)$. It follows that $N_G(H) = C_G(H)$.

Now, suppose $N_G(H) = G$. Then, we have $G = C_G(H)$. So, for every $g \in G$ and $h \in H$, we have $ghg^{-1} = h$, so $gh = hg$. This implies $h \in Z(G)$, so $H \subseteq Z(G)$. We conclude that $H \le Z(G)$. □

Example 2.29 (Dummit and Foote p. 53 Question 11)**.** Prove that $Z(G) \le N_G(A)$ for any $A \subseteq G$.

Solution. Let $A \subseteq G$. Suppose $a \in A$ and $g \in Z(G)$. Then, $gag^{-1} = a$ for all $a \in A$. Equivalently, $gAg^{-1} = A$, and the result follows. □

2.3
Cyclic Groups and Cyclic Subgroups

Definition 2.10 (cyclic subgroup)**.** Let G be a group. Let $x \in G$ be any element of G. The cyclic subgroup of G generated by x is the subgroup H that can be defined either of the two ways, where appropriate, as follows:

(i) multiplicative notation: H is a cyclic subgroup of G if

$$H = \{x^n : x \in \mathbb{Z}\} = \{g \in G : \text{there exists } n \in \mathbb{Z} \quad \text{such that } g = x^n\}$$

(ii) additive notation: H is a cyclic subgroup of G if

$$H = \{nx : n \in \mathbb{Z}\} = \{g \in G : \text{there exists } n \in \mathbb{Z} \quad \text{such that } g = nx\}$$

We then say that

$$H \text{ is generated by } x \quad \text{or} \quad x \text{ is a generator of } H \quad \text{and we write } H = \langle x \rangle .$$

Definition 2.11 (cyclic group)**.** A group G if cyclic if and only if

$$\text{there exists } x \in G \quad \text{such that} \quad G = \langle x \rangle .$$

If G is cyclic of order n, we say that $G = C_n$.

Example 2.30. The group of integers under addition, i.e. $(\mathbb{Z}, +)$, is cyclic and generated by ± 1.

Example 2.31 (integers modulo n)**.** For any $n \in \mathbb{Z}^+$, the additive group $\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}$, which denotes the set of remainders when divided by n, is cyclic and generated by $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ such that $\gcd(a,n) = 1$ (fact from Number Theory). The group $\mathbb{Z}/n\mathbb{Z}$ is known as the integers modulo n.

Recall the following fact from MA1100: for any $a \in \mathbb{Z}$, the congruence class of a modulo n is

$$\begin{aligned}\overline{a} = a + n\mathbb{Z} &= \{a + kn : k \in \mathbb{Z}\} \\ &= \{a, a \pm n, a \pm 2n, \ldots\}\end{aligned}$$

which is an element of $\mathbb{Z}/n\mathbb{Z}$. As such, we see that $\mathbb{Z}/n\mathbb{Z}$ has precisely n elements, which follows by the division algorithm. Also, note that for any $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$, their sum is

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{in } \mathbb{Z}/n\mathbb{Z}$$

for which the sum is well-defined.

Example 2.32 (Dummit and Foote p. 40 Question 6)**.** Prove that the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic.

Solution. Suppose on the contrary that $(\mathbb{Z}, +) \cong (\mathbb{Q}, +)$. Then, both groups should share common structural properties. However, we know from Example 2.30 that $(\mathbb{Z}, +)$ is cyclic and we will prove that $(\mathbb{Q}, +)$ is not cyclic, which leads to a contradiction.

Say we have some $q \in \mathbb{Q}$, i.e. there exist $a, b \in \mathbb{Z}$ with $b \neq 0$ such that $q = a/b$. However, $a/2b$ cannot be generated by a/b since there does not exist $k \in \mathbb{Z}$ such that

$$\frac{a}{2b} = k\left(\frac{a}{b}\right).$$

This leads to a contradiction, so $(\mathbb{Q}, +)$ is not a cyclic group. Hence, $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ are not isomorphic. □

Example 2.33 (Dummit and Foote p. 22 Question 11)**.** Find the orders of each element of the additive group $\mathbb{Z}/12\mathbb{Z}$.

Element	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$
Order	0	12	6	4	3	12	2	12	3	4	6	12

Table 15: Order of each element of the additive group $\mathbb{Z}/12\mathbb{Z}$

Solution. We shall present our answer in Table 15.
We have a couple of interesting observations. If $\gcd(k,12)=1$, then the order of the element k is 12. Also, the order of the additive group $\mathbb{Z}/12\mathbb{Z}$ is 12 and we see that the order of each element in $\mathbb{Z}/12\mathbb{Z}$ is a factor of 12. This is not surprising, as we would see in a useful corollary of Lagrange's theorem (Corollary 3.2). □

Example 2.34 (Dummit and Foote p. 22 Question 12)**.** Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/12\mathbb{Z})^{\times}:\overline{1},\overline{-1},\overline{5},\overline{7},\overline{-7},\overline{13}$.

Solution. We construct the following table:

Element	$\overline{1}$	$\overline{-1}$	$\overline{5}$	$\overline{7}$	$\overline{-7}$	$\overline{13}$
Order	1	1	5	7	5	1

Table 16: Order of each element of the multiplicative group $(\mathbb{Z}/12\mathbb{Z})^{\times}$

One notes that $\overline{-1}=\overline{11}$ so $\left(\overline{-1}\right)^2=\overline{1}$, $\overline{13}=\overline{1}$, and $\overline{-7}=\overline{5}$. □

Example 2.35 (Gallian p. 82 Question 19)**.** List the cyclic subgroups of $\mathbb{Z}/30\mathbb{Z}$.

Solution. One can construct a Cayley table describing $\mathbb{Z}/30\mathbb{Z}$ with the row and column headers being k, where $\gcd(k,30)=1$.

Such k satisfying this equation are $1,7,11,13,17,19,23$ and 29. The subgroup $\langle 1\rangle$ is cyclic since $1^m=1$ for all $m\in\mathbb{N}$. $\langle 7\rangle$ is also cyclic since the powers of 7 form a periodic sequence. One can verify that the subgroups $\langle 11\rangle,\langle 17\rangle,\langle 19\rangle$ and $\langle 29\rangle$ are also subgroups of $\mathbb{Z}/30\mathbb{Z}$. □

Example 2.36 (Dummit and Foote p. 60 Question 12)**.** Prove that the following groups are not cyclic:

(a) $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$
(b) $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}$
(c) $\mathbb{Z}\times\mathbb{Z}$

Solution.

(a) Recall that $\mathbb{Z}/2\mathbb{Z}$ consists of the possible remainders when an integer is divided by 2, so

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}=\left\{\left(\overline{0},\overline{0}\right),\left(\overline{1},\overline{0}\right),\left(\overline{0},\overline{1}\right),\left(\overline{1},\overline{1}\right)\right\}$$

The order of $\left(\overline{1},\overline{1}\right)\in\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ is 2 since

$$\left(\overline{1},\overline{1}\right)+\left(\overline{1},\overline{1}\right)=\left(\overline{0},\overline{0}\right).$$

However, we are unable to generate $\left(\overline{1},\overline{0}\right)$ using $\left(\overline{1},\overline{1}\right)$. Alternatively, one notes that the orders of $\left(\overline{1},\overline{0}\right),\left(\overline{0},\overline{1}\right)\in\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ are both 2, but they do not generate $\left(\overline{1},\overline{1}\right)$. Hence, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ does not have a generator, so it is not cyclic.

(b) We have

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}=\left\{\left(\overline{0},n\right):n\in\mathbb{Z}\right\}\sqcup\left\{\left(\overline{1},n\right):n\in\mathbb{Z}\right\}.$$

Clearly, elements of the form $(\overline{0}, n)$ cannot generate $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ since we will never obtain an element with $\overline{1}$ in the first component.

(c) Note that $(1,0), (0,1) \in \mathbb{Z} \times \mathbb{Z}$, but there does not exist $k \in \mathbb{Z}$ such that $k \cdot (1,0) = (0,1)$. $\square$

We give a nice geometric interpretation of **(c)** of Example 2.36. Refer to Figure 2 for a diagram that depicts $\mathbb{Z} \times \mathbb{Z}$, i.e. these refer to *lattice points* on the Cartesian plane $\mathbb{R} \times \mathbb{R}$. Suppose $\langle (n,m) \rangle$ is a generator for the group, where $(n,m) \in \mathbb{Z} \times \mathbb{Z}$. So, $\langle n,m \rangle$ is contained in the line $mx = ny$ (since the line has slope m/n), so the line cannot cover all of $\mathbb{Z} \times \mathbb{Z}$.

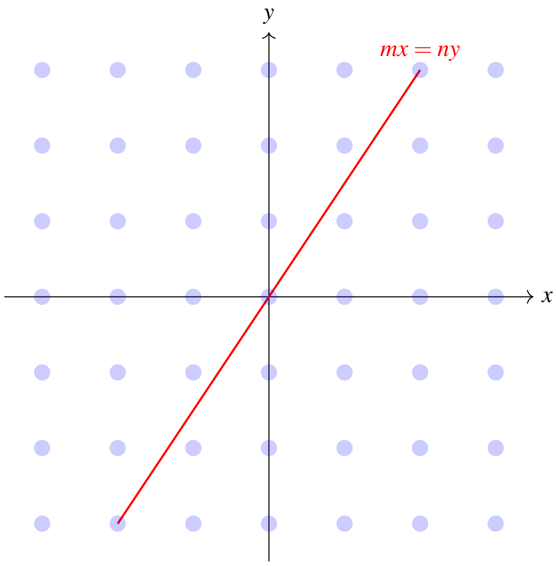


Figure 2: The line $mx = ny$ embedded in $\mathbb{Z} \times \mathbb{Z}$

Example 2.37 (Dummit and Foote p. 60 Question 13)**.** Prove that the following groups are not isomorphic:

(a) $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}$

(b) $\mathbb{Q} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Q}$

Solution.

(a) By Example 2.36, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ is not a cyclic group. However, by Example 2.30, $\mathbb{Z}$ is a cyclic group. As such, these groups cannot be isomorphic.

(b) Every non-identity element in $\mathbb{Q}$ is of infinite order but every element of the form $(0, \overline{1}) \in \mathbb{Q} \times \mathbb{Z}/2\mathbb{Z}$ is of order 2. By **(b)** of Proposition 1.14, there does not exist an isomorphism between these two groups. $\square$

Theorem 2.3 (universal property of $\mathbb{Z}$ as a group)**.** For any group G and element $x \in G$,

$$\text{there exists a unique homomorphism } \varphi : \mathbb{Z} \to G \quad \text{such that} \quad \varphi(1_{\mathbb{Z}}) = x.$$

In fact, φ is defined as follows: for any $n \in \mathbb{Z}$, we have $\varphi(n) = x^n$.

Example 2.38. Take $G = \mathbb{Z}$ to be the additive group of integers and $x = n$ to be any integer. Then, by Theorem 2.3, there exists a unique homomorphism

$$\varphi_n : \mathbb{Z} \to \mathbb{Z} \quad \text{such that} \quad \varphi_n(1_{\mathbb{Z}}) = n.$$

Given $n \in \mathbb{Z}$, recall that we have the multiplication-by-n map (Example 2.19) defined as follows:

$$n^* : \mathbb{Z} \to \mathbb{Z} \quad \text{such that} \quad a \mapsto na.$$

Since $n^*(1_{\mathbb{Z}}) = n = \varphi_n(1_{\mathbb{Z}})$, by uniqueness, it follows that $\varphi_n = n^*$ is the multiplication-by-n map.

Example 2.39. A familiar law of indices

$$(x^a)^b = x^{ab} \quad \text{for every } x \in G \text{ and } a, b \in \mathbb{Z}$$

follows from Theorem 2.3 too. To see why, let $a, b \in \mathbb{Z}$ be arbitrary and define

$$\varphi_a : \mathbb{Z} \to \mathbb{Z} \text{ such that } x \mapsto ax \quad \text{and} \quad \varphi_b : \mathbb{Z} \to \mathbb{Z} \text{ such that } x \mapsto bx.$$

Then,

$$\varphi_a \circ \varphi_b : \mathbb{Z} \to \mathbb{Z} \text{ where } x \mapsto a(bx) = abx \quad \text{is equal to} \quad \varphi_{ab} : \mathbb{Z} \to \mathbb{Z} \text{ where } x \mapsto (ab)x = abx$$

due to the uniqueness of the universal property. Here, we let

$$\psi : \mathbb{Z} \to G \text{ be the unique homomorphism} \quad \text{such that} \quad \psi(1_{\mathbb{Z}}) = x$$

So, the following diagram commutes:

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, "\varphi_b"] \arrow[dr, "\varphi_a \circ \varphi_b = \varphi_{ab}"'] & \mathbb{Z} \arrow[d, "\varphi_a"] \arrow[dr, "\psi \circ \varphi_a"] & \\
 & \mathbb{Z} \arrow[r, "\psi"'] & \mathcal{G}
\end{tikzcd}$$

This shows that

$$(\psi \circ \varphi_a) \circ \varphi_b = \psi \circ \varphi_{ab},$$

where $(\psi \circ \varphi_a) \circ \varphi_b : \mathbb{Z} \to G$ is a homomorphism sending $1_{\mathbb{Z}}$ to $(\psi \circ \varphi_a)(b) = (x^a)^b$; $\psi \circ \varphi_{ab} : \mathbb{Z} \to G$ is a homomorphism sending $1_{\mathbb{Z}}$ to $\psi(ab) = x^{ab}$. By the above commutative diagram, it follows that $(x^a)^b = x^{ab}$.

Example 2.40 (Dummit and Foote p. 60 Question 9). Let $\mathbb{Z}_{36} = \langle x \rangle$. For which integers a does the map ψ_a defined by $\psi_a : \bar{1} \mapsto x^a$ extend to a *well-defined homomorphism* from $\mathbb{Z}/48\mathbb{Z}$ into $\mathbb{Z}_{36}$. Can ψ_a ever be a surjective homomorphism?

Solution. Note that $\mathbb{Z}_{36} = \{0, 1, \ldots, 36\}$. Consider the map

$$\psi_a : \mathbb{Z}/48\mathbb{Z} \to \mathbb{Z}_{36} \quad \text{where} \quad \psi_a(\bar{y}) = x^{ay}.$$

Consider $b, c \in \mathbb{Z}/48\mathbb{Z}$ such that $\bar{b} = \bar{c}$. For ψ_a to be well-defined, we must have $\psi_a(\bar{b}) = \psi_a(\bar{c})$. As such,

$$x^{ab} = x^{ac} \quad \text{which implies} \quad x^{a(b-c)} = 1.$$

Since $\mathbb{Z}_{36} = \langle x \rangle$, then $36 \mid a(b-c)$. We also know that $48 \mid (b-c)$ which implies there exists $k \in \mathbb{Z}$ such that $b - c = 48k$. Hence, $36 \mid 48ak$. Since $\gcd(48, 36) = 12$, then $3 \mid 4ak$. Regardless of the choice of k, we must have $3 \mid 4a$, so $3 \mid a$, i.e. a must be divisible by 3.

Next, we claim that ψ_a can never be surjective. Suppose on the contrary that it is. Then, for $x \in \mathbb{Z}_{36}$, there exists $\bar{y} \in \mathbb{Z}/48\mathbb{Z}$ such that $\psi_a(\bar{y}) = x = x^{ay}$. For ψ_a to be a well-defined homomorphism, we mentioned that a must be divisible by 3, i.e. write $a = 3k$ for some $k \in \mathbb{Z}$. So, $x = x^{3ky}$ which implies $x^{3ky-1} = 1$. We must have $36 \mid (3ky - 1)$. This is a contradiction as it would imply $3 \mid 1$. $\square$

Proposition 2.7. Let $\varphi : G \to H$ be a homomorphism. Then,

$$\varphi \text{ is injective} \quad \text{if and only if} \quad \ker\varphi = \{1_G\} \quad \text{and}$$
$$\varphi \text{ is surjective} \quad \text{if and only if} \quad \operatorname{im}\varphi = H$$

Proposition 2.8. Let G be a group and let $x \in G$. Let $\varphi : \mathbb{Z} \to G$ be the unique homomorphism such that $\varphi(1_{\mathbb{Z}}) = x$, i.e. for any $k \in \mathbb{Z}$, we have $\varphi(k) = x^k$. Then, the following hold:

$$\operatorname{im}\varphi = \langle x \rangle \quad \text{which is a cyclic subgroup of } G \text{ generated by } x$$
$$\ker\varphi = \begin{cases} 0 = 0\mathbb{Z} & \text{if } x \text{ is of infinite order;} \\ n\mathbb{Z} & \text{if } x \text{ is of finite order } n \in \mathbb{Z}^+ \end{cases}$$

Corollary 2.1. Let G be a group and $x \in G$. Then, the following hold:

$$\text{if } x \text{ is of infinite order} \quad \text{then} \quad \langle x \rangle \text{ is an infinite cyclic group}$$
$$\text{if } x \text{ is of finite order } n \in \mathbb{Z}^+ \quad \text{then} \quad \langle x \rangle \text{ is a finite cyclic group of order } n.$$

Corollary 2.2. Any two infinite cyclic groups are isomorphic.

Proof. Let $G = \langle x \rangle$ be an infinite cyclic group with generator x. By Corollary 2.1, x is of infinite order. Define

$$\varphi : \mathbb{Z} \to G \text{ to be the unique homomorphism} \quad \text{such that} \quad \varphi(1_{\mathbb{Z}}) = x.$$

One checks that $\ker\varphi = 0\mathbb{Z}$ and $\operatorname{im}\varphi = \langle x \rangle$, which respectively show that φ is injective and surjective by Proposition 2.7. Hence, φ is bijective, hence it is an isomorphism. □

We shall investigate some properties of the cyclic group $\mathbb{Z}/n\mathbb{Z}$. Recall that this refers to the set of integers modulo n. Let

$$\pi : \mathbb{Z} \to n\mathbb{Z} \text{ be the unique homomorphism} \quad \text{such that} \quad \pi(1_{\mathbb{Z}}) = 1.$$

This means that for any $a \in \mathbb{Z}$, $\pi(a) = a \cdot \overline{1} = \overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$. π is typically called a projection map, or some would call it a *reduction map* or a *quotient map* because it maps elements of $\mathbb{Z}$ to a subset like $n\mathbb{Z}$, particularly in terms of congruences.

Since $\overline{1} \in \mathbb{Z}/n\mathbb{Z}$ is a generator of $\mathbb{Z}/n\mathbb{Z}$ is of finite order n, we know that

$$\operatorname{im}\pi = \mathbb{Z}/n\mathbb{Z} \quad \text{or equivalently} \quad \pi : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z} \text{ is an epimorphism.}$$

ALso, $\ker\pi = n\mathbb{Z} \subseteq \mathbb{Z}$.

Proposition 2.9. Let G be a group and $x \in G$. Suppose $a, b \in \mathbb{Z}$ such that $x^a = 1_G = x^b$. Then, $x^c = 1_G$, where $c = \gcd(a, b)$.

There is an analogous result in Number Theory, i.e. if $a, b \in \mathbb{Z}$ are both divisible by a positive integer n, then their gcd, or any linear combination, will also be divisible by n. Note that by Bézout's lemma, the gcd of two integers is a linear combination of a and b.

Theorem 2.4 (universal property of $\mathbb{Z}/n\mathbb{Z}$). For any group G and any element $x \in G$ such that $x^n = 1_G$,

$$\text{there exists a unique homomorphism } \varphi : \mathbb{Z}/n\mathbb{Z} \to G \quad \text{such that} \quad \varphi\left(\overline{1}\right) = x.$$

So, for any $\xi \in \mathbb{Z}/n\mathbb{Z}$, one can choose $a \in \mathbb{Z}$ such that $\xi = \pi(a) = \overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$ so that $\varphi(\xi) = x^a$.

As such, given any group G and element $x \in G$ such that $x^n = 1_G$, let

$$\varphi : \mathbb{Z}/n\mathbb{Z} \text{ be the unique homomorphism} \quad \text{such that} \quad \varphi(1) = x.$$

Also, let

$$\Phi : \mathbb{Z} \to G \text{ be the unique homomorphism} \quad \text{such that} \quad \Phi(1_{\mathbb{Z}}) = x.$$

Lastly, let

$$\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \text{ be the unique homomorphism} \quad \text{such that} \quad \pi(1_{\mathbb{Z}}) = 1.$$

Then, $\Phi = \varphi \circ \pi$, i.e. the following diagram commutes:

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, "\Phi"] \arrow[d, "\pi"'] & G \\
\mathbb{Z}/n\mathbb{Z} \arrow[ur, "\varphi"']
\end{tikzcd}$$

This is a classic example of the *first isomorphism theorem* (we will explore this in due course in Theorem 3.6). Simply said, if we have a group homomorphism $\varphi : G \to H$, then $G/\ker\varphi \cong \operatorname{im}\varphi$. Here, the reduction map $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ tells us that $\ker\varphi = n\mathbb{Z}$ as shown in the commutative diagram. Not surprising!

Proposition 2.10. Let G be a group and $x \in G$ such that $x^n = 1_G$. Let

$$\varphi : \mathbb{Z}/n\mathbb{Z} \to G \text{ be the unique homomorphism} \quad \text{such that} \quad \varphi\left(\overline{1}\right) = x.$$

Let $d \in \mathbb{Z}^+$ be the finite order of x. Then, the following hold:

$$\begin{aligned}
\operatorname{im}\varphi &= \langle x \rangle \quad \text{which is the cyclic subgroup of } G \text{ generated by } x \\
\ker\varphi &= \left\langle \overline{d} \right\rangle = d\mathbb{Z}/n\mathbb{Z} \text{ in } \mathbb{Z}/n\mathbb{Z}
\end{aligned}$$

Corollary 2.3. Any two finite cyclic groups of the same order are isomorphic.

We then investigate the subgroups of $\mathbb{Z}$.

Theorem 2.5. For any $H \leq \mathbb{Z}$, there exists a unique $n \in \mathbb{Z}_{\geq 0}$ such that $H = n\mathbb{Z}$. If $H \neq 0$, then $n \in \mathbb{Z}^+$ is characterised as the smallest element of $H \cap \mathbb{Z}^+$.

Proposition 2.11. Let $\varphi : G \to H$ be a homomorphism. Then, the following hold:

(i) For any $H_0 \leq H$, its φ-preimage

$$\varphi^{-1}(H_0) = \{g \in G : \varphi(g) \in H_0\} \quad \text{is a subgroup of } G$$

(ii) For any $G_0 \leq G$, its φ-image

$$\varphi(G_0) = \{\varphi(g) \in H : g \in G_0\} \quad \text{is a subgroup of } H$$

Example 2.41 (Dummit and Foote p. 85 Question 1)**.** Let $\varphi : G \to H$ be a homomorphism and let E be a subgroup of H. Prove that $\varphi^{-1}(E) \leq G$ (i.e., the pre-image or pullback of a subgroup under a homomorphism is a subgroup). If $E \trianglelefteq H$, prove that $\varphi^{-1}(E) \trianglelefteq G$. Deduce that $\ker\ \varphi \trianglelefteq G$.

Solution. Since $\varphi(1_G) = 1_E$, then $\varphi^{-1}(1_E) = 1_G \in \varphi^{-1}(E)$ so $\varphi^{-1}(E)$ is non-empty.

Next, let $a, b \in \varphi^{-1}(E)$ and suppose $x, y \in E$ such that

$$\varphi(a) = x \quad \text{and} \quad \varphi(b) = y.$$

Then, $\varphi\left(b^{-1}\right) \in E$ since $E \leq H$. Since $\varphi : G \to H$ is a homomorphism, then

$$\varphi\left(ab^{-1}\right) = \varphi(a)\varphi\left(b^{-1}\right) = \varphi(a)[\varphi(b)]^{-1} \in E$$

which implies $ab^{-1} \in \varphi^{-1}(E)$. By the subgroup criterion (Proposition 2.1), $\varphi^{-1}(E) \leq G$.

Next, if we further assume that $E \trianglelefteq H$, suppose we have $g \in G$ and $a \in \varphi^{-1}(E)$ such that

$$\varphi(a) = x \text{ and } \varphi(g) = y \quad \text{for some } x \in E, y \in H.$$

We have

$$\varphi\left(gag^{-1}\right) = \varphi(g)\varphi(a)\varphi\left(g^{-1}\right) = yxy^{-1} \in E$$

so $gag^{-1} \in \varphi^{-1}(E)$. Lastly, if we let $E = \{1_H\}$, which is the trivial subgroup of H, then we have $\ker\varphi = \varphi^{-1}(E)$. We conclude that $\ker\varphi \trianglelefteq G$. □

Example 2.42 (Dummit and Foote p. 85 Question 2)**.** Let $\varphi : G \to H$ be a homomorphism of groups with kernel K and let $a, b \in \varphi(G)$. Let $X \in G/K$ be the fiber above a and let Y be the fiber above b, i.e. $X = \varphi^{-1}(a), Y = \varphi^{-1}(b)$.

Fix an element u of X (so $\varphi(u) = a$). Prove that if $XY = Z$ in the quotient group G/K and w is any member of Z, then

$$\text{there is some } v \in Y \quad \text{such that} \quad uv = w.$$

Hint: show that $u^{-1}w \in Y$.

Solution. Since φ is a homomorphism, then

$$\varphi(XY) = \varphi(X)\varphi(Y) \quad \text{which implies} \quad \varphi(Z) = ab.$$

Hence, $Z = \varphi^{-1}(ab)$. Consider $v = u^{-1}w$, where $\varphi(u) = a$ and $\varphi(v) = b$. Hence,

$$\varphi(v) = \varphi\left(u^{-1}w\right) = \varphi\left(u^{-1}\right)\varphi(w) = a^{-1}(ab) = \left(a^{-1}a\right)b = b$$

which shows that there exists $v \in Y$ such that $u^{-1}w \in Y$. Hence, $uv = w$. □

Theorem 2.6. For any $H \leq \mathbb{Z}/n\mathbb{Z}$, there exists a unique $a \in \mathbb{Z}^+$ dividing n such that $H = \pi(a\mathbb{Z}) = \langle \overline{a} \rangle$. In fact, $a \in \mathbb{Z}^+$ is characterised as the smallest positive integer such that $\overline{a} \in H$.

Corollary 2.4. Every subgroup of a cyclic group G is cyclic.

Corollary 2.5. Let G be a cyclic group. Then, the following hold:

(i) If G is an infinite cyclic group and $x \in G$ is a generator, then

$$\mathbb{Z}_{\geq 0} \to \{\text{subgroups of } G\} \text{ where } n \mapsto \langle x^n \rangle \quad \text{is a bijection.}$$

The inverse map is

$$\begin{aligned} \{\text{subgroups of } G\} &\to \mathbb{Z}_{\geq 0} \\ K &\mapsto \begin{cases} 0 & \text{if } K = 1; \\ n & \text{if } K \neq 1 \text{ and } n \in \mathbb{Z}^+ \text{ is the smallest such that } x^n \in K \end{cases} \end{aligned}$$

(ii) On the other hand, if G is a finite cyclic group of order $n \in \mathbb{Z}^+$ and $x \in G$ is a generator, then

$$\left\{a \in \mathbb{Z}^+ : a \mid n\right\} \to \{\text{subgroups of } G\} \text{ where } a \mapsto \langle x^a \rangle \quad \text{is a bijection.}$$

The inverse map is

$$\begin{aligned} \{\text{subgroups of } G\} &\to \left\{a \in \mathbb{Z}^+ : a \mid n\right\} \\ K &\mapsto \text{the smallest } a \in \mathbb{Z}^+ \text{ such that } x^a \in K \end{aligned}$$

Proposition 2.12 (generators of $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$)**.** We have the following:

(i) For any $a \in \mathbb{Z}$, we have $\mathbb{Z} = \langle a \rangle$ if and only if $a = \pm 1$

(ii) For fixed $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$, we have $\mathbb{Z}/n\mathbb{Z} = \langle \overline{a} \rangle$ if and only if $\gcd(a,b) = 1$

Corollary 2.6 (generators of a cyclic group)**.** Let G be a cyclic group and $x \in G$ be a generator.

(i) If G is infinite, then for any $a \in \mathbb{Z}$, we have

$$G = \langle x^a \rangle \quad \text{if and only if} \quad a = \pm 1$$

(ii) If G is finite of order $n \in \mathbb{Z}^+$, then for any $a \in \mathbb{Z}$, we have

$$G = \langle x^a \rangle \quad \text{if and only if} \quad \gcd(a,n) = 1$$

Example 2.43. Find a collection of distinct subgroups $\langle m_1 \rangle, \langle m_n \rangle$ of $\mathbb{Z}/124\mathbb{Z}$ such that

$$\langle m_1 \rangle \leq \ldots \leq \langle m_n \rangle \leq \mathbb{Z}/124\mathbb{Z},$$

where n is as large as possible.

Solution. Note that the divisors of 124 are $1, 2, 4, 31, 62, 124$. So, to find the longest chain, we have

$$\langle 124 \rangle \leq \langle 4 \rangle \leq \langle 2 \rangle \leq \langle 1 \rangle = \langle \mathbb{Z}/124\mathbb{Z} \rangle,$$

where $n = 4$. □

2.4
Subgroups generated by Subsets of a Group

Example 2.44 (Dummit and Foote p. 65 Question 13)**.** Prove that the multiplicative group of positive rational numbers is generated by the set

$$\left\{\frac{1}{p} : p \text{ is a prime}\right\}.$$

Solution. By definition of $\mathbb{Q}^+$, every positive rational number x can be uniquely written as

$$x = \frac{a}{b} \quad \text{where } a, b \in \mathbb{Z}^+ \text{ and } \gcd(a, b) = 1.$$

By the fundamental theorem of arithmetic, there exist primes $p_1, \ldots, p_s, q_1, \ldots, q_t$ such that

$$a = p_1^{\alpha_1} \ldots p_s^{\alpha_s} \quad \text{and} \quad b = q_1^{\beta_1} \ldots q_t^{\beta_t} \quad \text{where } \alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t \geq 0.$$

So,

$$x = p_1^{\alpha_1} \ldots p_s^{\alpha_s} \left(\frac{1}{q_1}\right)^{\beta_1} \ldots \left(\frac{1}{q_t}\right)^{\beta_t}.$$

Each term of the form $p_i^{\alpha_i}$ is the power of some prime p_i, which is permitted since any integer power of a prime is included in a generated group. Also, we can take each of the $1/q_j$'s to be a generator. The result follows. □

Proposition 2.13 (intersection of subgroups)**.** Let $\mathcal{C}$ be a non-empty collection of subgroups of G. Then,

$$\bigcap_{H \in \mathcal{C}} H \quad \text{is also a subgroup of } G.$$

Proof. We have

$$1_G \in \bigcap_{H \in \mathcal{C}} H \quad \text{since} \quad \text{for any } H \in \mathcal{C} \text{ we have } 1_G \in H.$$

Next, let

$$x, y \in \bigcap_{H \in \mathcal{C}} H.$$

Then, for any $H \in \mathcal{A}$, we have $x, y \in H$ so $xy^{-1} \in H$. Hence,

$$xy^{-1} \in \bigcap_{H \in \mathcal{A}} H.$$

By the subgroup criterion, the aforementioned intersection is also a subgroup of H. □

Definition 2.12. Let $A \subseteq G$. Define

$$\langle A \rangle = \bigcap_{\substack{A \subseteq H \\ H \leq G}} H \quad \text{to be the intersection of all } H \leq G \text{ that contain A.}$$

This is a subgroup of G containing A known as the subgroup of G generated by A.

Example 2.45 (Dummit and Foote p. 65 Question 1)**.** Prove that if $H \le G$ then $\langle H \rangle = H$.

Solution. Clearly, $H \subseteq \langle H \rangle$ since $H \le G$. To prove the reverse inclusion, replacing A with H in Definition 2.12 yields

$$\langle H \rangle = \bigcap_{\substack{H \subseteq H \\ H \le G}} H = \bigcap_{H \le G} H$$

which follows that $\langle H \rangle \subseteq H$. Hence, $\langle H \rangle = H$. □

Example 2.46 (Dummit and Foote p. 65 Question 2)**.** Prove that if A is a subset of B, then $\langle A \rangle \le \langle B \rangle$. Give an example where $A \subseteq B$ with $A \neq B$ but $\langle A \rangle = \langle B \rangle$.

Solution. Suppose $x \in A$. Then, $x \in \langle A \rangle$. Since $A \subseteq B$, then $x \in B$ so $x \in \langle B \rangle$. The first result follows.

We then construct some $A \subseteq B$ with $A \neq B$ but $\langle A \rangle = \langle B \rangle$. Take $A = \{x\}$ and $B = \left\{x, x^3\right\}$. One checks that $A \subseteq B$ with $A \neq B$ and $\langle A \rangle = \langle B \rangle$. □

Definition 2.13 (normal closure)**.** Let

$$\overline{A} = \mathrm{ncl}_G(A) = \left\{ \prod_{i=1}^{n} a_i^{\varepsilon_i} : n \in \mathbb{Z}_{\ge 0} \text{ and } a_i \in A, \varepsilon_i = \pm 1 \right\}.$$

This is called the normal closure of A in G.

After learning about *normal subgroups* in Definition 3.7, you will come to realise that the normal closure of a group G is the smallest normal subgroup of G containing S, where $S \subseteq G$.

Example 2.47 (Dummit and Foote p. 65 Question 3)**.** Prove that if H is an Abelian subgroup of a group G, then $\langle H, Z(G) \rangle$ is Abelian. Give an explicit example of an Abelian subgroup H of a group G such that $\langle H, C_G(H) \rangle$ is not Abelian.

Solution. Suppose H is an Abelian subgroup of a group G. We shall consider the set $\langle H, Z(G) \rangle$. Every element of this set can be written as a finite product of elements each lying in either H or $Z(G)$. As such,

$$x \in \langle H, Z(G) \rangle \quad \text{can be written as} \quad x = h_1 z_1 \ldots h_k z_k \text{ where } h_i \in H \text{ and } z_i \in Z(G).$$

Since H is Abelian, then h_i and h_j commute. By definition of the center $Z(G)$, every element $z \in Z(G)$ commutes with every element of G, and in particular with every element of $H \subseteq G$. That is,

$$zh = hz \quad \text{for all } z \in Z(G), h \in H.$$

Now, putting everything together, multiplying two elements

$$x = h_1 z_1 \ldots h_k z_k \quad \text{and} \quad y = h_1' z_1' \ldots h_l' z_l',$$

one may rearrange the factors freely as they all commute pairwise. This implies $xy = yx$ so $\langle H, Z(G) \rangle$ is Abelian.

For the second part, consider the dihedral group D_8 with $H = \left\{e, r^2\right\}$. Since $e, r^2 \in Z(D_8)$, we have $C_G(H) = D_8$. Although H is Abelian, we see that $\langle H, C_G(H) \rangle = D_8$ is not Abelian. □

Example 2.48 (Dummit and Foote p. 65 Question 4)**.** Prove that if H is a subgroup of G, then H is generated by the set $H - \{1\}$.

Solution. First, note that $H - \{1\} = H \setminus \{e\}$. We shall consider two cases.

- **Case 1:** Suppose $H = \{e\}$. Then, $H \setminus \{e\} = \emptyset$ which is a generator of the trivial subgroup.
- **Case 2:** Suppose $|H| > 1$. We first prove that

$$\langle H \setminus \{e\} \rangle \subseteq H.$$

Clearly, every element of $H \setminus \{e\}$ also lies in H. Since H is a subgroup, it is closed under taking products and inverses, i.e. $e = hh^{-1}$. So, the inclusion holds.

We then prove the reverse inclusion. Consider some $h \in H$. If $h = e$, the result follows. If h is non-identity, then h is already one of the generators in $H \setminus \{e\}$, so $h \in \langle H \setminus \{e\} \rangle$. The reverse inclusion holds as a result.

Combining both cases, the result follows. □

Definition 2.14 (finitely generated group)**.** A group H is finitely generated if

$$\text{there exists a finite set } A \quad \text{such that} \quad H = \langle A \rangle .$$

Example 2.49 (Dummit and Foote p. 65 Question 14)**.** A group H is finitely generated if

$$\text{there exists a finite set } A \quad \text{such that} \quad H = \langle A \rangle .$$

(a) Prove that every finite group is finitely generated.

(b) Prove that $\mathbb{Z}$ is finitely generated.

(c) Prove that every finitely generated subgroup of the additive group $\mathbb{Q}$ is cyclic.
Hint: If H is a finitely generated subgroup of $\mathbb{Q}$, show that $H \leq \langle 1/k \rangle$, where k is the product of all denominators which appear in a set of generators for H.

(d) Prove that $\mathbb{Q}$ is not finitely generated.

Solution.

(a) Every finite group H is cyclic with generator H, i.e. $H = \langle H \rangle$.

(b) Note that $\mathbb{Z}$ is cyclic with generators ± 1, and the result follows.

(c) Suppose H is generated by $\{h_1, \ldots, h_n\}$, where each $h_i \in \mathbb{Q}$. Write

$$h_i = \frac{p_i}{q_i} \quad \text{where } p_i, q_i \in \mathbb{Z}, q_i \neq 0 \text{ and } \gcd(p_i, q_i) = 1.$$

Define $k = q_1 \ldots q_n$. Then, we shall rewrite each generator h_i in terms of $1/k$, i.e.

$$h_i = \frac{p_i}{q_i} = p_i \cdot \frac{q_1 \ldots q_n}{q_i} \cdot \frac{1}{k} = \left(p_i \cdot \frac{q_1 \ldots q_n}{q_i} \right) \cdot \frac{1}{k}.$$

Essentially, we deduced the hint. Also, $\langle 1/k \rangle \leq H$ so combining both results, we see that H is generated by a single element $1/k$, implying that H is a cyclic subgroup of $\mathbb{Q}$. Note that $q_1 \ldots q_n / q_i \in \mathbb{Z}$ so h_i is indeed an integer multiple of $1/k$. So, $h_i \in \langle 1/k \rangle$. We deduce that $H \leq \langle 1/k \rangle$.

(d) Suppose on the contrary that $\mathbb{Q}$ is finitely generated. Then, there exists a finite set A such that $\mathbb{Q} = \langle A \rangle$, i.e. $\mathbb{Q}$ is cyclic. Let $p/q \in A$, where $q \neq 0$ and $\gcd(p,q) = 1$. So for every $x \in \mathbb{Q}$, there exists $k \in \mathbb{Z}$ such that $x = k(p/q)$. Since p/q is the generator, then there exists $r \in \mathbb{Z}$ such that $1/r \in \langle p/q \rangle$.

So, $q = pkr$ which implies $q \mid p$. This is a contradiction as we assumed that $\gcd(p,q) = 1$. □

Definition 2.15 (divisible group). A non-trivial Abelian group A (written multiplicatively) is said to be divisible if

$$\text{for every } a \in A \text{ and each } k \in \mathbb{Z} \setminus \{0\} \quad \text{there exists } x \in A \text{ such that } x^k = a.$$

This means that each element has a k^{th} root in A.

Example 2.50 (Dummit and Foote p. 66 Question 19). A non-trivial Abelian group A (written multiplicatively) is said to be divisible if

$$\text{for every } a \in A, k \in \mathbb{Z} \setminus \{0\} \quad \text{there exists } x \in A \text{ such that } x^k = a.$$

This means that each element has a k^{th} root in A. In additive notation, each element is the k^{th} multiple of some element of A.

(a) Prove that the additive group of rational numbers, $\mathbb{Q}$, is divisible.

(b) Prove that no finite Abelian group is divisible.

Solution.

(a) Let $a \in \mathbb{Q}$ and $a \in \mathbb{Z} \setminus \{0\}$. Then, choose $x = a/k \in \mathbb{Q}$ so that $kx = a$. So, $\mathbb{Q}$ is divisible.

(b) First, note that although the trivial group $\{e\}$ is Abelian, it does not satisfy the condition of a divisible group since k must be non-zero.

Now, suppose on the contrary that there exists a finite Abelian group G that is divisible. Suppose $|G| = n$. Choose two non-identity elements $x, y \in G$ such that $y^n = e$ (actually, this choice is attributed to a useful corollary of Lagrange's theorem in Corollary 3.2 which we will explore in due course). Then, for $x \in G$, the equation $y^n = x$ does not hold. □

Example 2.51 (Dummit and Foote p. 66 Question 20). Prove that if A and B are non-trivial Abelian groups, then

$$A \times B \text{ is divisible} \quad \text{if and only if} \quad \text{both } A \text{ and } B \text{ are divisible groups.}$$

Solution. We first prove the forward direction. Suppose $A \times B$ is a divisible group. Then, for any $(a,b) \in A \times B$ and $k \in \mathbb{Z} \setminus \{0\}$, we have

$$(x,y)^k = (a,b) \quad \text{which implies} \quad \left(x^k, y^k\right) = (a,b).$$

By equality of ordered pairs, we have $x^k = a$ and $y^k = b$, so A and B are divisible groups.

We then prove the reverse direction. Suppose A and B are divisible groups. Then, take $a, x \in A$ and $b, y \in B$, as well as $k \in \mathbb{Z} \setminus \{0\}$ such that

$$x^k = a \quad \text{and} \quad y^k = b.$$

This implies that $(x,y)^k = (a,b)$, showing that $A \times B$ is divisible. □

Example 2.52 (Dummit and Foote p. 86 Question 15). Prove that a quotient of a divisible Abelian group by any proper subgroup is also divisible. Deduce that $\mathbb{Q}/\mathbb{Z}$ is divisible.

Solution. Let G be a divisible Abelian group and let H be a proper subgroup of G. Suppose $g \in G$ and $k \in \mathbb{Z}^+$. Since G is divisible, then

$$\text{there exists } k \in \mathbb{Z} \setminus \{0\} \quad \text{such that} \quad x^k = g.$$

So, $x^k H = gH$, which implies that $(xH)^k = gH$. So, G/H is divisible. As for the second part, take $G = \mathbb{Q}$ and $H = \mathbb{Z}$. □

Example 2.53 (Dummit and Foote p. 86 QUestion 16). Let G be a group, let N be a normal subgroup of G and let $\overline{G} = G/N$. Prove that if $G = \langle x, y \rangle$ then $\overline{G} = \langle \overline{x}, \overline{y} \rangle$. Prove more generally if

$$G = \langle S \rangle \quad \text{for any subset } S \text{ of } G,$$

then $\overline{G} = \langle \overline{S} \rangle$.

Solution. Suppose we have $g \in G$. Then, $gN \in \overline{G}$. So,

$$\text{there exist } x_i \in \{x, y\} \text{ and } a_i \in \mathbb{Z} \quad \text{such that} \quad g = x_1^{a_1} \ldots x_k^{a_k}.$$

So,

$$gN = \left(x_1^{a_1} \ldots x_k^{a_k}\right) N = \left(x_1^{a_1} N\right) \ldots \left(x_k^{a_k} N\right) = (x_1 N)^{a_1} \ldots (x_k N)^{a_k} = \overline{x_1}^{a_1} \ldots \overline{x_k}^{a_k}.$$

Here, $\overline{x_i} \in \{\overline{x}, \overline{y}\}$. As such, for any $gN \in \overline{G}$, we have $\overline{G} = \langle \overline{x}, \overline{y} \rangle$.

More generally, if $S \subseteq G$, suppose $s_i \in S$ for all $1 \leq i \leq k$ such that

$$g = s_1 \ldots s_k.$$

Similar to the above, we can write gN as

$$gN = \overline{s_1}^{a_1} \ldots \overline{s_k}^{a_k}$$

so $\overline{G} = \overline{S}$. □

2.5 The Lattice of Subgroups of a Group

Algorithm 2.1 (lattice construction). The lattice of subgroups of G is constructed as follows:

1. Plot all subgroups of G with

$$1 \text{ at the bottom} \quad \text{and} \quad G \text{ at the top},$$

   and subgroups of larger order positioned higher.
2. Draw a line upward from A to B if and only if $A \leq B$ and there are no subgroups properly contained between A and B.

We will encounter this topic of lattice construction in Galois Theory (MA4203) again. This concept of lattice construction is fundamental to understanding the Galois correspondence, which elegantly connects what is called *field extensions* to subgroup structures in the Galois group of the extension. Interestingly, in this structure, we will encounter an inversion of inclusion, where larger subgroups correspond to smaller field extensions. This inverse relationship between subgroups and subfields makes the lattice construction particularly useful for organising these dependencies.

Proposition 2.14. For any $d, n \in \mathbb{Z}_{\geq 0}$, one has

$$n\mathbb{Z} \subseteq d\mathbb{Z} \quad \text{if and only if} \quad d \mid n \text{ in } \mathbb{Z}.$$

Proof. Since $n\mathbb{Z}$ is cyclic generated by n, it is the smallest subgroup of $\mathbb{Z}$ generated by n. Hence, $n\mathbb{Z} \subseteq d\mathbb{Z}$ if and only if $n \in d\mathbb{Z}$, which is equivalent to saying that there exists $k \in \mathbb{Z}$ such that $n = dk$. □

Proposition 2.15. For fixed $n \in \mathbb{Z}^+$ and any $a, b \in \mathbb{Z}^+$ dividing n, we have

$$\langle \overline{a} \rangle \subseteq \langle b \rangle \text{ in } \mathbb{Z}/n\mathbb{Z} \quad \text{if and only if} \quad b \mid a \text{ in } \mathbb{Z}.$$

Proof. We have

$$\begin{aligned} \langle \overline{a} \rangle \subseteq \langle \overline{b} \rangle \quad & \text{if and only if} \quad \overline{a} \in \langle \overline{b} \rangle \\ & \text{if and only if} \quad \text{there exists } k \in \mathbb{Z} \text{ such that } \overline{a} = k\overline{b} \text{ in } \mathbb{Z}/n\mathbb{Z} \\ & \text{if and only if} \quad a \in b\mathbb{Z} + n\mathbb{Z} = b\mathbb{Z} \text{ since } b \mid n \\ & \text{if and only if} \quad b \mid a \text{ in } \mathbb{Z} \end{aligned}$$

□

Example 2.54 (lattice of subgroups of G when $|G| = 1$)**.** This example is uninteresting as $\mathbb{Z}/1\mathbb{Z} = \langle 1 \rangle = \{0\}$.

Example 2.55 (lattice of subgroups of G when $|G| = 2$)**.** If $|G| = 2$, we obtain the following lattice of subgroups:

$$\begin{array}{c} \mathbb{Z}/2\mathbb{Z} \\ | \\ 2\mathbb{Z}/2\mathbb{Z} \end{array}$$

Example 2.56 (lattice of subgroups of G when $|G| = 3$)**.** If $|G| = 3$, we obtain the following lattice of subgroups:

$$\begin{array}{c} \mathbb{Z}/3\mathbb{Z} \\ | \\ 3\mathbb{Z}/3\mathbb{Z} \end{array}$$

Example 2.57 (lattice of subgroups of G when $|G| = 4$)**.** If $|G| = 4$, recall that there are two possibilities of G up to isomorphism, namely the cyclic group of order 4 ($\mathbb{Z}/4\mathbb{Z}$) and the Klein four-group V. For the former, we obtain the following lattice of subgroups:

$$\begin{array}{c} \mathbb{Z}/4\mathbb{Z} \\ | \\ 2\mathbb{Z}/4\mathbb{Z} \\ | \\ 4\mathbb{Z}/4\mathbb{Z} \end{array}$$

The Klein four-group has the following lattice of subgroups:

$$\begin{tikzcd} & V = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(0,0),(0,1),(1,0),(1,1)\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \langle (1,0) \rangle \arrow[dr, dash] & \langle (1,1) \rangle \arrow[d, dash] & \langle (0,1) \rangle \arrow[dl, dash] \\ & \langle (0,0) \rangle & \end{tikzcd}$$

Example 2.58 (lattice of subgroups of G when $|G| = 5$)**.** If $|G| = 5$, we obtain the following lattice of subgroups:

$$\begin{array}{c} \mathbb{Z}/5\mathbb{Z} \\ | \\ 5\mathbb{Z}/5\mathbb{Z} \end{array}$$

Example 2.59 (lattice of subgroups of groups of prime order). Suppose G is a group, where $|G| = p$, where p is prime. Based on our examples of the lattices of subgroups for the cases when $p = 2, 3, 5$, we generalise to the following lattice for some arbitrary p:

$$\begin{tikzcd} \mathbb{Z}/p\mathbb{Z} \arrow[d, dash] \\ p\mathbb{Z}/p\mathbb{Z} \end{tikzcd}$$

We state an interesting theorem in Number Theory regarding primes.

Theorem 2.7 (Wilson's theorem). Let p be a prime. Then, $(p-1)! \equiv -1 \pmod{p}$.

Proof. We pair the elements of $(\mathbb{Z}/p\mathbb{Z})^{\times}$ with their respective inverses. The elements which cannot be paired up are those which are self-invertible. These elements satisfy $x^2 \equiv 1 \pmod{p}$. There are only two elements which satisfy this congruence, which are 1 and $p-1$. Therefore, in the product $(p-1)! \in (\mathbb{Z}/p\mathbb{Z})^{\times}$, all the other elements cancel out, leaving $p-1$. $\square$

Example 2.60 (lattice of subgroups of G when $|G| = 6$). Similar to groups of order 4, we note that there are 2 groups of order 6, up to isomorphism. These are

$$C_6, \text{ the cyclic group of order 6} \quad \text{and} \quad S_3, \text{ the symmetric group on 3 letters.}$$

We first discuss subgroups of $C_6 \cong \mathbb{Z}/6\mathbb{Z}$. We note that $2\mathbb{Z}/6\mathbb{Z}, 3\mathbb{Z}/6\mathbb{Z} \leq \mathbb{Z}/6\mathbb{Z}$. To see what the elements of each subgroup look like, we have

$$2\mathbb{Z}/6\mathbb{Z} = \left\{\overline{0}, \overline{2}, \overline{4}\right\} \quad \text{and} \quad 3\mathbb{Z}/6\mathbb{Z} = \left\{\overline{0}, \overline{3}\right\}.$$

Hence, $2\mathbb{Z}/6\mathbb{Z}$ should be placed above (but not directly) $3\mathbb{Z}/6\mathbb{Z}$ since the former is of a larger order. However, $2\mathbb{Z}/6\mathbb{Z}$ and $3\mathbb{Z}/6\mathbb{Z}$ are *not comparable* since one is clearly not a subset of the other.

$$\begin{tikzcd} & \mathbb{Z}/6\mathbb{Z} \arrow[dl, dash] \arrow[ddr, dash] & \\ 2\mathbb{Z}/6\mathbb{Z} \arrow[ddr, dash] & & \\ & & 3\mathbb{Z}/6\mathbb{Z} \arrow[dl, dash] \\ & 6\mathbb{Z}/6\mathbb{Z} & \end{tikzcd}$$

On the other hand, the following is the lattice of subgroups of S_3:

$$\begin{tikzcd} & & & S_3 \cong D_6 \arrow[dlll, dash] \arrow[dll, dash] \arrow[dl, dash] \arrow[dr, dash] & \\ \langle (12) \rangle \arrow[drrr, dash] & \langle (13) \rangle \arrow[drr, dash] & \langle (23) \rangle \arrow[dr, dash] & & \langle (123) \rangle \arrow[dl, dash] \\ & & & 1 & \end{tikzcd}$$

Example 2.61 (lattice of subgroups of G when $|G| = 8$). There are 5 groups of order 8, up to isomorphism. These are the cyclic group $\mathbb{Z}/8\mathbb{Z}$, the direct product $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, the direct product $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, the dihedral group D_8, the quaternion group Q_8.

We first discuss the lattice of subgroups of $\mathbb{Z}/8\mathbb{Z}$, which are as follows:

$$\begin{tikzcd}[arrows=dash]
\mathbb{Z}/8\mathbb{Z} \arrow[d] \\
2\mathbb{Z}/8\mathbb{Z} \arrow[d] \\
4\mathbb{Z}/8\mathbb{Z} \arrow[d] \\
8\mathbb{Z}/8\mathbb{Z}
\end{tikzcd}$$

We then discuss the lattice of subgroups of $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which are as follows:

$$\begin{tikzcd}[arrows=dash]
& \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \arrow[dl] \arrow[d] \arrow[dr] & \\
\langle (1,0) \rangle \arrow[d] \arrow[dr] & \langle (2,0),(0,1) \rangle \arrow[dl] \arrow[d] \arrow[dr] & \langle (1,1) \rangle \arrow[dl] \arrow[d] \\
\langle (2,1) \rangle \arrow[dr] & \langle (2,0) \rangle \arrow[d] & \langle (0,1) \rangle \arrow[dl] \\
& \langle (0,0) \rangle &
\end{tikzcd}$$

The lattice of subgroups of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is complicated, so we will not discuss it. We then discuss the lattice of subgroups of D_8.

$$\begin{tikzcd}[arrows=dash]
& & D_8 = \langle r,s \rangle \arrow[dl] \arrow[d] \arrow[dr] & & \\
& \langle s, r^2 \rangle \arrow[dl] \arrow[d] \arrow[dr] & \langle r \rangle \arrow[d] & \langle rs, r^2 \rangle \arrow[dl] \arrow[d] \arrow[dr] & \\
\langle s \rangle \arrow[ddrr] & \langle r^2 s \rangle \arrow[ddr] & \langle r^2 \rangle \arrow[dd] & \langle rs \rangle \arrow[ddl] & \langle r^3 s \rangle \arrow[ddll] \\
& & & & \\
& & 1 & &
\end{tikzcd}$$

Lastly, we discuss the lattice of subgroups of Q_8.

$$\begin{tikzcd}[arrows=dash]
& Q_8 \arrow[dl] \arrow[d] \arrow[dr] & \\
\langle i \rangle \arrow[dr] & \langle j \rangle \arrow[d] & \langle k \rangle \arrow[dl] \\
& \langle -1 \rangle \arrow[d] & \\
& 1 &
\end{tikzcd}$$

Chapter 3
Quotient Groups and Homomorphisms

3.1
Definitions and Examples

Definition 3.1 (cosets and representatives)**.** Let G be a group and $H \leq G$. For any $g \in G$,

$$gH = \{gh \in G : h \in H\} \quad \text{is the left } g\text{-coset of } H \text{ in G}$$
$$Hg = \{hg \in G : h \in H\} \quad \text{is the right } g\text{-coset of } H \text{ in G}$$

Any element of the coset is known as a representative.

Example 3.1. $g = g \cdot 1_G$ is a representative for gH; $g = 1_G \cdot g$ is a representative for Hg.

We will only discuss left cosets from now, although similar properties hold for right cosets by symmetry. Also, there is no difference between left and right cosets if G is Abelian, i.e. if $a \in G$, then $a \in aH$ and $a \in Ha$.

Definition 3.2 (coset space)**.** The set of left cosets of H in G is denoted by G/H. So,

$$G/H = \{X \subseteq G : \text{there exists } g \in G \text{ such that } X = gH\}.$$

Definition 3.3 (projection map)**.** Let

$$\pi : G \to G/H \quad \text{denote the map} \quad g \mapsto gH.$$

Note that π is surjective (by definition) but not injective in general, i.e. there possibly exist distinct $g_1, g_2 \in G$ such that $g_1H = g_2H$ in G/H.

Example 3.2. Suppose $H = G$. Then, for any $g \in G$, we have $gG = G = Gg$ and

$$G/G = \{G\} \text{ which is a singleton} \quad \text{and} \quad \pi : G \to G/G \text{ is the trivial map.}$$

Example 3.3. If $H = 1$, then for any $g \in G$, we have $g1 = \{g\} = 1_g$ and

$$G/1 = \{\{g\} \in \mathcal{P}(G) : g \in G\} \quad \text{and} \quad \pi : G \to G/1 \text{ where } g \mapsto \{g\} \text{ is the obvious bijection.}$$

Example 3.4. Fix $n \in \mathbb{Z}^+$. Take $G = \mathbb{Z}$ and $H = n\mathbb{Z}$, where we see that $H \leq G$. We have the familiar set of cosets of $n\mathbb{Z}$ in $\mathbb{Z}$, denoted by $\mathbb{Z}/n\mathbb{Z}$!

For any $a \in \mathbb{Z}$, the a-coset of $n\mathbb{Z}$ in $\mathbb{Z}$ is the congruence class of a modulo n, i.e.

$$\bar{a} = a + n\mathbb{Z} = \{a + kn : k \in \mathbb{Z}\}.$$

The projection map

$$\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \text{ where } a \mapsto a + n\mathbb{Z} \quad \text{is the reduction mod } n \text{ map.}$$

Example 3.5 (Dummit and Foote p. 85 Question 7)**.** Define

$$\pi : \mathbb{R}^2 \to \mathbb{R} \quad \text{by} \quad \pi((x,y)) = x+y.$$

Prove that π is a surjective homomorphism and describe the kernel and fibers of π geometrically.

Solution. Suppose $(x_1,y_1),(x_2,y_2) \in \mathbb{R}^2$. Then,

$$\begin{aligned}
\pi((x_1,y_1)+(x_2,y_2)) &= \pi(x_1+x_2,y_1+y_2) \\
&= x_1+x_2+y_1+y_2 \\
&= x_1+y_1+x_2+y_2 \\
&= \pi((x_1,y_1))+\pi((x_2,y_2))
\end{aligned}$$

so π is a homomorphism. To show that π is surjective, suppose $x+y=z \in \mathbb{R}$. Then, we can choose $(x,z-x) \in \mathbb{R}^2$ such that $\pi((x,z-x)) = x+z-x = z$, so π is surjective.

$\ker\pi$ denotes the set of all $(x,y) \in \mathbb{R}^2$ such that $x+y=0$. In other words, the kernel represents the line $y=-x$. Lastly, for $a \in \mathbb{R}$, the fiber over a is a line with equation $x+y=a$. □

Example 3.6. Let $G = S_3$ and $H = \langle(1\,2)\rangle$. The following are the left cosets of H in G:

$$\begin{aligned}
(1)H &= H \\
(1\,2)H &= H \\
(1\,3)H &= \{(1\,3),(1\,2\,3)\} \\
(1\,2\,3)H &= \{(1\,3),(1\,2\,3)\} \\
(2\,3) &= \{(2\,3),(1\,3\,2)\} \\
(1\,3\,2)H &= \{(2\,3),(1\,3\,2)\}
\end{aligned}$$

We leave the enumeration of all right H-cosets in G as an exercise. Also, one sees that in general, the left and right cosets are different, i.e. $gH \neq Hg$.

Proposition 3.1. For any $g_1,g_2 \in G$, the following are equivalent:

(i) $g_1H = g_2H$ in G/H

(ii) $g_1H \subseteq g_2H$

(iii) $g_1 \in g_2H$

(iv) $g_2^{-1}g_1 \in H$

Corollary 3.1. Let G be a group and $H \leq G$. Then, the following hold:

(i) The relation $\sim$ on G defined by

$$g_1 \sim g_2 \quad \text{if and only if} \quad g_2^{-1}g_1 \in H$$

is an equivalence relation

(ii) The set G/H is the quotient set of the equivalence relation in **(i)**

(iii) The map

$$\pi : G \to G/H \quad \text{where} \quad g \mapsto gH \quad \text{is the quotient map of the equivalence relation in } \textbf{(i)}$$

(iv) The set of left cosets of H in G form a partition of G

Proof. **(i)** is trivial. We prove **(ii)**, **(iii)**, **(iv)** concurrently. Note that $X \subseteq G$ is an equivalence class (with relation $\sim$) if and only if there exists $g \in G$ such that

$$X = \{x \in G : x \sim g\} = \left\{x \in G : g^{-1}x \in H\right\} = gH.$$

The result follows. $\square$

Example 3.7 (Dummit and Foote p. 89 Question 36)**.** Prove that if $G/Z(G)$ is cyclic then G is abelian. (*Hint:* If $G/Z(G)$ is cyclic with generator $xZ(G)$, show that every element of G can be written in the form $x^a z$ for some integer $a \in \mathbb{Z}$ and some element $z \in Z(G)$.)

Solution. Suppose $G/Z(G)$ is cyclic. Then, elements of this quotient group are of the form $xZ(G)$, where $x \in G$. So, we can write

$$G = \bigcup_{n=0}^{\infty} x^n Z(G).$$

Take $a, b \in G$. Then, there exist $n, m \in \mathbb{Z}_{\geq 0}$ such that

$$a = x^n y \text{ and } b = x^m z \quad \text{where} \quad y, z \in Z(G).$$

So,

$$ab = x^n y x^m z = x^m z x^n y = ba \quad \text{via repeated use of the fact that } y, z \in Z(G).$$

So, G is an Abelian group. $\square$

Definition 3.4 (index of subgroup)**.** Let $H \leq G$. The index of H in G is

$$|G : H| = |G/H| \quad \text{which is the cardinality of the set } G/H.$$

Definition 3.5 (commutator and commutator subgroup)**.** Let $x, y \in G$, where G is a group. The element $x^{-1}y^{-1}xy$ is called the commutator of x and y and it is denoted by $[x, y]$. Also, the group

$$\{[x,y] : x, y \in G\} = \left\{x^{-1}y^{-1}xy : x, y \in G\right\} \quad \text{is the commutator subgroup of } G.$$

3.2
More on Cosets and Lagrange's Theorem

Proposition 3.2. For any $g \in G$, the map

$$H \to gH \text{ defined by } h \mapsto gh \quad \text{is a well-defined bijection.}$$

This is known as left multiplication by g.

Proof. The well-definedness and surjective nature of the map follows by the definition of the left coset gH. The map is injective by performing left multiplication by g^{-1}, i.e. cancellation law. $\square$

Example 3.8 (Dummit and Foote p. 95 Question 6)**.** Let $H \leq G$ and let $g \in G$. Prove that if the right coset Hg equals some left coset of H in G then it equals the left coset gH and g must be in $N_G(H)$.

Solution. Suppose we have $Hg = aH$ for some $a \in G$. Since $g \in Hg$, then we have $g \in aH$. We know that the right cosets partition G, thus $aH = gH$. Therefore, $Hg = gH$ which follows that $gHg^{-1} = H$. We conclude that $g \in N_G(H)$. $\square$

Example 3.9 (Dummit and Foote p. 95 Question 5)**.** Let H be a subgroup of G and fix some element $g \in G$.

(a) Prove that gHg^{-1} is a subgroup of G of the same order as H.

(b) Deduce that if $n \in \mathbb{Z}^+$ and H is the unique subgroup of G of order n, then $H \trianglelefteq G$.

Solution.

(a) We know that $1 \in gHg^{-1}$ so gHg^{-1} is non-empty. Next, consider $h_1, h_2 \in H$ and $g \in G$ as usual such that $x, y \in gHg^{-1}$, i.e.

$$x = gh_1g^{-1} \quad \text{and} \quad y = gh_2g^{-1}.$$

So,

$$xy^{-1} = \left(gh_1g^{-1}\right)\left(gh_2g^{-1}\right)^{-1} = gh_1g^{-1}gh_2^{-1}g^{-1} = gh_1h_2^{-1}g^{-1}.$$

Since $H \leq G$, then $h_1h_2^{-1} \in H$, so $xy^{-1} \in gHg^{-1}$. As such, $gHg^{-1} \leq G$.

For the second part, define

$$\varphi : H \to gHg^{-1} \quad \text{such that} \quad \varphi(h) = ghg^{-1}.$$

For any $x \in gHg^{-1}$, we can choose $h = x$ so that $\varphi(h) = ghg^{-1} = x$ so φ is surjective. Next, suppose there exist $h_1, h_2 \in H$ such that $f(h_1) = f(h_2)$. So,

$$gh_1g^{-1} = gh_2g^{-1} \quad \text{which implies} \quad h_1 = h_2.$$

As such, φ is injective. We conclude that φ is a bijective map and $|H| = \left|gHg^{-1}\right|$.

(b) From **(a)**, we know that

$$gHg^{-1} \leq G \quad \text{and} \quad \left|gHg^{-1}\right| = |H|.$$

Since H is the unique subgroup of order n, then $H = gHg^{-1}$ for all $g \in G$, and it follows that $H \trianglelefteq G$.

We then move on to our first big theorem of Group Theory, called Lagrange's theorem.

Theorem 3.1 (Lagrange's theorem)**.** Let G be a finite group. Then,

$$\text{for any } H \leq G, \quad \text{we have } |H| \mid |G|.$$

Moreover, $|G| = |G : H|\,|H|$.

Proof. The left cosets of H in G form the partition

$$G = \bigsqcup_{X \in G/H} X \quad \text{so} \quad |G| = \sum_{X \in G/H} |X|.$$

Note that the symbol $\sqcup$ denotes that the union of X over all $X \in G/H$ denotes a disjoint union. By Proposition 3.2, for each $X \in G/H$, we have $|X| = |H|$, and the result follows. $\square$

Example 3.10 (Dummit and Foote p. 95 Question 4)**.** Show that if $|G| = pq$ for some primes p and q (not necessarily distinct) then either G is abelian or $Z(G) = 1$.

Solution. Note that $Z(G) \leq G$ so by Lagrange's theorem (Theorem 3.1), $|Z(G)| \mid |G|$ so $|Z(G)|$ is either 1 or p or q. We shall consider two cases.

- **Case 1:** Suppose $Z(G)$ is the trivial group. Then, $|Z(G)| = 1$.
- **Case 2:** Without loss of generality, suppose $|Z(G)| = p$. Then, consider the quotient group $G/Z(G)$. By Lagrange's theorem (Theorem 3.1),

$$|G/Z(G)| = \frac{|G|}{|Z(G)|} = \frac{pq}{p} = q.$$

Since the order of this quotient group is prime, then it is cyclic. By Example 3.7, G is Abelian.

The result follows. □

Example 3.11 (Dummit and Foote p. 95 Question 8)**.** PRove that if

$$H \text{ and } K \text{ are finite subgroups of } G \text{ whose orders are relatively prime} \quad \text{then} \quad H \cap K = 1.$$

Solution. Suppose $|H| = m$ and $|K| = n$ such that $\gcd(m,n) = 1$. Let $|H \cap K| = a$. Since $H \cap K \leq H$ and $H \cap K \leq K$, then

$$\text{by Lagrange's theorem} \quad \text{we have} \quad |H \cap K| \mid |H| \text{ and } |H \cap K| \mid |K|.$$

Thus, $a \mid m$ and $a \mid n$. So, $a \mid \gcd(m,n)$. Since $\gcd(m,n) = 1$, then $a = 1$. □

Corollary 3.2. Let G be a finite group. For any $x \in G$, we have

$$|x| \mid |G| \quad \text{or equivalently} \quad x^{|G|} = 1_G.$$

Corollary 3.2 is a useful corollary of Lagrange's theorem. It can be used to deduce some interesting results in Number Theory like Euler's theorem and Fermat's little theorem. We start with some preliminaries.

Definition 3.6 (Euler φ-function)**.** The Euler φ-function (not to be confused with group homomorphism) or totient function can be described as follows:

$$\varphi(n) = |\{a : a \leq n \text{ and } \gcd(a,n) = 1\}|$$

We can also think of the Euler φ-function from a group-theoretic point-of-view. Take $G = (\mathbb{Z}/n\mathbb{Z})^{\times}$, which refers to the multiplicative group of $\mathbb{Z}/n\mathbb{Z}$. One sees that $|G| = \varphi(n)$.

Theorem 3.2 (Euler's theorem)**.** For any $x \in \mathbb{Z}$ such that $\gcd(x,n) = 1$, we have $x^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof. By Corollary 3.2, we see that for any $x \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, we have $x^{\varphi(n)} = \overline{1}$ in $\mathbb{Z}/n\mathbb{Z}$. □

Theorem 3.3 (Fermat's little theorem)**.** Let p be a prime. Then, for any $x \in \mathbb{Z}$, we have $x^{p-1} \equiv 1 \pmod{p}$.

Proof. One should see this as a proof of Euler's theorem (Theorem 3.2) by setting $n = p$, where p is prime. □

Note that the converse of Lagrange's theorem is false, i.e. if G is finite and $n \mid |G|$, there need not exist a subgroup of G of order n. A classic counterexample to the converse is about the alternating group of degree 4, denoted by A_4 (will mention more in due course, particularly once we have covered Definition 3.16). We briefly mention the details here but a formal explanation will be given in Example 3.38. The alternating group A_n is related to the symmetric group S_n. We will mention in Definition 3.16 that $|A_n| = |S_n|/2$, so it is clear that $|A_4| = 12$. Although 6 divides 12, we will see in Example 3.38 that A_4 does not have any subgroup of order 12.

Corollary 3.3. Let G be a finite group, where $|G| = p$ for some prime p. Then,

$$G \text{ is cyclic} \quad \text{and hence} \quad G \cong \mathbb{Z}/p\mathbb{Z}.$$

Proof. Choose any non-identity element $x \in G$. Then, $\langle x \rangle \leq G$, where $|x| \mid |G| = p$ and $|x| > 1$. Hence, $|\langle x \rangle| = p$, which implies $\langle x \rangle = G$.

We conclude that

$$\text{the unique homomorphism } \varphi : \mathbb{Z}/p\mathbb{Z} \to G \quad \text{such that} \quad \varphi\left(\overline{1}\right) = x$$

is an isomorphism. □

Theorem 3.4 (tower theorem)**.** Suppose $H \leq G$ and $K \leq H$. Then,

$$[G : K] = [G : H]\,[H : K].$$

We will encounter a variant of Theorem 3.4 in Galois Theory, in particular when discussing field extensions. Also, this problem appears on p. 96 of the Dummit and Foote textbook (Question 11).

Proof. Note that we cannot assume that G is a finite group. So, we write G as the disjoint union of left cosets of H as follows:

$$G = \bigsqcup_{g \in T} gH$$

where $T \subseteq G$ is a set of coset representatives for G/H. Note that $|T| = [G : H]$.

Similarly, within H, we can form its cosets using K, i.e.

$$H = \bigsqcup_{h \in R} hK,$$

where $R \subseteq H$ is a set of coset representatives for H/K. Note that $|R| = [H : K]$ similarly. As such,

$$G = \bigsqcup_{g \in T} gH = \bigsqcup_{g \in T} \bigsqcup_{h \in R} (gh)\,K.$$

Here, each gH breaks into $[H : K]$ cosets of K, and there are $[G : H]$ distinct cosets gH. As the total number of cosets of K in G is $[G : K]$, the result follows. □

Example 3.12 (Dummit and Foote p. 96 Question 10)**.** Suppose H and K are subgroups of finite index in the (possible infinite) group G with $[G : H] = m$ and $[G : K] = n$. Prove that

$$\operatorname{lcm}(m, n) \leq [G : H \cap K] \leq mn.$$

Deduce that if m and n are relatively prime, then

$$[G : H \cap K] = [G : H] \cdot [G : K].$$

Solution. Suppose we have $g \in G$. Then, consider the cosets $gH, gK, g(H \cap K)$. If $x \in g(H \cap K)$, then $x \in gH$ and $x \in gK$ so $g(H \cap K) \subseteq gH \cap gK$. Similarly, if $x \in gH$ and $x \in gK$, then $xg^{-1} \in H \cap K$ so $x \in g(H \cap K)$. This shows that $gH \cap gK = g(H \cap K)$.

For each coset of $H \cap K$, it is the intersection of one coset from H and one coset from K. So, $[G : H \cap K] \leq mn$. Also, we note that

$$[G:H] \mid [G:H\cap K] \quad \text{and} \quad [G:K] \mid [G:H\cap K].$$

As such, $[G : H \cap K] \geq \operatorname{lcm}(m,n)$. Combining both inequalities yields the first result.

For the second part, if m and n are relatively prime, then $\operatorname{lcm}(m,n) = mn$ so $[G : H \cap K] = mn$. □

3.3 Normal Subgroups and Quotient Groups

Definition 3.7 (normal subgroup). A subgroup N of G is a normal subgroup if and only if any of the following equivalent conditions is satisfied:

- **(i)** for any $g \in G$, one has $gNg^{-1} = N$, i.e. every element of G normalizes N
- **(ii)** $N_G(N) = G$
- **(iii)** for any $g \in G$, one has $gN = Ng$
- **(iv)** for any $g \in G$, one has $gNg^{-1} \subseteq N$

If either of these holds, we write $N \trianglelefteq G$.

Example 3.13. Some trivial examples include $1 \trianglelefteq G$ and $G \trianglelefteq G$.

Example 3.14. Let G be an Abelian group and $H \leq G$. Then $H \trianglelefteq G$. This follows from Definitions 2.7 and 2.8, where we discussed the definitions of the centralizer and normalizer of a group, i.e. G is Abelian

$$G \text{ is Abelian} \quad \text{if and only if} \quad \text{for any } A \subseteq G \text{ we have } C_G(A) = N_G(A) = G.$$

Example 3.15. If $H \subseteq Z(G)$, then H is normal since this implies $gHg^{-1} = H$. It follows that $Z(G) \trianglelefteq G$.

Proposition 3.3. In the quotient group G/N, we have

$$(gN)^\alpha = g^\alpha N \quad \text{for all } \alpha \in \mathbb{Z}.$$

Proposition 3.3 appears in Dummit and Foote p. 85 Question 4. One can prove this result using induction.

Example 3.16 (Dummit and Foote p. 85 Question 5). Prove that the order of the element gN in G/N is n, where n is the smallest positive integer such that $g^n \in N$ (and gN has infinite order if no such positive integer exists). Give an example to show that the order of gN in G/N may be strictly smaller than the order of g in G.

Solution. For the first part, suppose we have $gN \in G/N$ and $g^n \in N$. Then, we have $g^nN = 1N$. From Proposition 3.3, we have $(gN)^n = g^nN$, so $(gN)^n = 1N$. As such, $|G/N| \leq n$. Next, suppose there exists $m \in \mathbb{N}$ such that $(gN)^m = 1N$. Then, $(gN)^m = g^mN$, which follows that $g^m \in N$. So, $|G/N| = m$. However, since n was defined to be the smallest positive integer, then $m \geq n$ so we conclude that $|gN| = n$.

Next, assuming that there does not exist such a positive integer, then for each $k \in \mathbb{N}$, we have $g^k \notin N$. Suppose on the contrary that $|gN|$ is finite. Then, there exists $p \in \mathbb{Z}$ such that $(gN)^p = 1N$, which follows that $g^p \in N$. This is a contradiction!

For the last part, suppose $G = \mathbb{Z}/4\mathbb{Z}$ which is a group of order 4. Let $N = \langle x^2 \rangle$ and $G = \langle x \rangle$. So, $x^2N = 1N$ which is of order 1. $\square$

Example 3.17 (Dummit and Foote p. 88 Question 22).

(a) Prove that if H and K are normal subgroups of a group G, then

$$\text{their intersection } H \cap K \quad \text{is} \quad \text{also a normal subgroup of } G.$$

(b) Prove that the intersection of any arbitrary non-empty collection of normal subgroups of a group is a normal subgroup (do not assume the collection is countable).

Solution.

(a) By Proposition 2.13, we know that the arbitrary intersection of subgroups is also a subgroup. In particular, if $H, K \trianglelefteq G$, then $H \cap K \trianglelefteq G$. So, it suffices to show that $H \cap K$ satisfies the normal subgroup criterion (Definition 3.7).

Suppose we have $g \in G$ and $x \in H \cap K$. Then, by definition, we have $x \in H$ and $x \in K$. Since $H, K \leq G$, then $gxg^{-1} \in H$ and $gxg^{-1} \in K$, which follows that $gxg^{-1} \in H \cap K$. Hence, $H \cap K \trianglelefteq G$.

(b) Again, we make use of Proposition 2.13. Define X to be the collection of normal subgroups X_i, i.e.

$$X = \bigcap_{i \in I} X_i \quad \text{where} \quad X_i \trianglelefteq G.$$

Suppose we have $g \in G$ and $x \in X$. Then, $x \in X_i$ for all $i \in I$. Since $X_i \leq G$, then $gxg^{-1} \in X_i$, so $gxg^{-1} \in X$. The result follows. $\square$

Example 3.18 (Dummit and Foote p. 88 Question 24). Prove that if

$$N \trianglelefteq G \text{ and } H \text{ is any subgroup of G} \quad \text{then} \quad N \cap H \trianglelefteq H.$$

Solution. By a special case of Proposition 2.13, we know that the intersection of two subgroups is also a subgroup of a group. So, $N \cap H \leq H$. Suppose $h \in H$ and $x \in N \cap H$. Then, $x \in N$ and $x \in H$. Since $N \trianglelefteq G$, then there exists $g \in G$ such that $gxg^{-1} \in N$.

Set $h = g$ so that $hxh^{-1} \in N$. Since $x \in H$, then $hxh^{-1} \in H$ as well. It follows that $hxh^{-1} \in N \cap H$, proving that $N \cap H \trianglelefteq H$. $\square$

Definition 3.8. For any $A, B \subseteq G$, we write

$$\begin{aligned} AB &= \{ab \in G : a \in A, b \in B\} \\ &= \{x \in G : \text{there exist } a \in A, b \in B \text{ such that } x = ab\} \end{aligned}$$

Observe that this is precisely the image of $A \times B$ under the multiplication map $G \times G \to G$.

Example 3.19 (Dummit and Foote p. 89 Question 39). Suppose A is the non-abelian group S_3 and D is the diagonal subgroup $\{(a,a) \mid a \in A\}$ of $A \times A$. Prove that D is not normal in $A \times A$.

Solution. Note that $(1\,2\,3) \in S_3$. Let $a = (1\,3)$ and $b = (1\,2\,3)$ be two permutations in S_3. Then, $a^{-1} = a$ since a is a transposition, and $b^{-1} = (1\,3\,2)$. Suppose

$$x = (a,b) \in A \times A \quad \text{and} \quad y = (a,a) \in D.$$

Then,

$$xyx^{-1} = \left(a^3, bab^{-1}\right) = \left(a, bab^{-1}\right).$$

If $D \trianglelefteq A \times A$, then we must have $xyx^{-1} \in D$ so $a = bab^{-1}$. However, one checks that $bab^{-1} = (2\,3)$ but $a = (1\,3)$ which implies D is not normal in $A \times A$. $\square$

Definition 3.9. For any $A \subseteq G$, define

$$\begin{aligned} A^{-1} &= \left\{a^{-1} \in G : a \in A\right\} \\ &= \left\{x \in G : \text{there exist } a \in A \text{ such that } x = a^{-1}\right\} \end{aligned}$$

This is precisely the image of A under the inversion map $G \to G$.

One sees that

$$(AB)\,C = A\,(BC) \quad \text{since multiplication in } G \text{ is associative.}$$

Example 3.20. Suppose $H \leq G$ and $g \in G$. Then,

$$\begin{aligned} HH &= \{ab \in G : a \in H, b \in H\} = H \\ H^{-1} &= \left\{a^{-1} \in G : a \in H\right\} = H \end{aligned}$$

Example 3.21 (absorption property)**.** Let $N \trianglelefteq G$. Then, for any $g_1, g_2 \in G$, we obtain $g_1N, g_2N \subseteq G$, and

$$\begin{aligned} (g_1N)\,(g_2N) &= g_1\,(Ng_2)\,N && \text{by associativity} \\ &= g_1\,(g_2N)\,N && \text{since } N \trianglelefteq G \\ &= (g_1g_2)\,(NN) && \text{by associativity} \\ &= (g_1g_2)\,N \end{aligned}$$

In a similar fashion, one is able to deduce that $(gN)^{-1} = g^{-1}N$.

We are now in a position to define the product of cosets and the inversion of a coset.

Definition 3.10 (product of cosets)**.** Let $X_1, X_2 \in G/N$. We can compute their product by first

$$\text{choosing any representative } g_1 \text{ of } X \quad \text{and} \quad \text{choosing any representative } g_2 \text{ of } X_2.$$

So, $X_1 = g_1N$ and $X_2 = g_2N$ respectively. We then multiply g_1 and g_2 in G, and

$$\text{form the coset} \quad X_1X_2 = g_1g_2N \in G/N.$$

Definition 3.11 (inversion of coset)**.** Let $X \in G/N$. We can compute the inversion of X by

$$\text{choosing any representative } g \text{ of } X \quad \text{so} \quad X = gN,$$

then inversing g in G and forming the coset $X^{-1} = g^{-1}N \in G/N$.

The results in Definitions 3.10 and 3.11 are well-defined, i.e. independent of the choice of representatives for the cosets.

Example 3.22 (Dummit and Foote p. 85 Question 3). Let A be an Abelian group and let B be a subgroup of A. Prove that A/B is Abelian. Give an example of a non-Abelian group G containing a proper normal subgroup N such that G/N is Abelian.

Solution. For the first result, suppose we have $xB, yB \in A/B$, where $x, y \in A$. Then,

$$xByB = xyBB = xyB = yxB = yBxB$$

so A/B is Abelian.

For the second part, consider $G = D_8$ which is non-Abelian. It has a normal subgroup $N = \langle r^2 \rangle$. However, $G/N \cong V_4$ (the Klein four-group in Definition 2.3) which is Abelian. □

Example 3.23 (Dummit and Foote p. 89 Question 40). Let G be a group, let N be a normal subgroup of G and let $\overline{G} = G/N$. Prove that $\overline{x}$ and $\overline{y}$ commute in $\overline{G}$ if and only if $x^{-1}y^{-1}xy \in N$. Here, the element $x^{-1}y^{-1}xy$ is called the *commutator* of x and y and is denoted by $[x, y]$ (recall Definition 3.5).

Solution. Say $\overline{x} = xN$ and $\overline{y} = yN$, where $x, y \in G$. We first prove the forward direction. Suppose $\overline{x}$ and $\overline{y}$ commute in $\overline{G}$. Then,

$$\overline{x} \cdot \overline{y} = (xN) \cdot (yN) = (xy)N \quad \text{and} \quad \overline{y} \cdot \overline{x} = (yx)N \quad \text{similarly}.$$

So, $(xy)N = (yx)N$, which implies $(yx)^{-1}(xy) \in N$, i.e. $x^{-1}y^{-1}xy \in N$.

We then prove the reverse direction. Suppose $x^{-1}y^{-1}xy \in N$. Then, $(xy)N = (yx)N$, so in $\overline{G}$, if we define $\overline{x} = xN$ and $\overline{y} = yN$ for some $x, y \in G$, it follows that

$$\overline{x} \cdot \overline{y} = (xy)N = (yx)N = \overline{y} \cdot \overline{x},$$

showing that $\overline{x}$ and $\overline{y}$ commute in G. □

Example 3.24 (Dummit and Foote p. 89 Question 41). Let G be a group. Prove that $N = \{x^{-1}y^{-1}xy : x, y \in G\}$ is a normal subgroup of G and G/N is abelian. Here, N is called the *commutator subgroup of* G (recall Definition 3.5).

Solution. $x^{-1}y^{-1}xy \in N$ by definition of the commutator subgroup. Let $g \in G$ be arbitrary too. Then,

$$\begin{aligned} g * x^{-1}y^{-1}xy * g^{-1} &= gx^{-1}y^{-1}xyg^{-1} \\ &= \left(gxg^{-1}\right)^{-1}\left(gyg^{-1}\right)\left(gxg^{-1}\right)\left(gyg^{-1}\right) \in N \end{aligned}$$

so $N \trianglelefteq G$. The fact that G/N is Abelian was established in Example 3.23, where we mentioned that if $\overline{G} = G/N$, then $\overline{x}, \overline{y}$ commute in $\overline{G}$ if and only if $x^{-1}y^{-1}xy \in N$, where N denotes the commutator subgroup. □

Example 3.25 (Dummit and Foote p. 89 Question 42). Assume both H and K are normal subgroups of G with $H \cap K = 1$. Prove that $xy = yx$ for all $x \in H$ and $y \in K$. (*Hint:* Show $x^{-1}y^{-1}xy \in H \cap K$)

Solution. Since $H \trianglelefteq G$, then for any $g \in G$ and $h \in H$, we have $ghg^{-1} \in H$. In particular, we can choose $g \in K$, so set $y \in K$. As such,

$$yxy^{-1} \in H \quad \text{where} \quad x \in H, y \in K.$$

So, $y^{-1}xy \in H$, which implies $x^{-1}y^{-1}xy \in H$. Similarly, one can deduce that $x^{-1}y^{-1}xy \in K$ as well. So, $x^{-1}y^{-1}xy \in H \cap K$. However, as $H \cap K = 1$, it forces $x^{-1}y^{-1}xy = 1$, so $xy = yx$. □

Lemma 3.1. Let G be a group. Then, every subgroup H of index 2 is normal.

Proof. Suppose $[G:H]=2$ and $g \in G$. Then, H has 2 left cosets in G. If $gH=H$, then $g \in H$ and so $gH=H=Hg$. $gH=Hg$ satisfies condition **(iii)** in Definition 3.7 and the result follows.

On the other hand, if $gH \neq H$, then H and gH are the only two left cosets of H in G. As $g \notin H$, then H and Hg are the only two right cosets of H in G, so $Hg = G \setminus H = gH$. Thus, $gH=Hg$ so the result follows by **(iii)** of Definition 3.7. □

Definition 3.12 (quotient group)**.** Let G be a group and $N \trianglelefteq G$. The quotient group of G modulo N is the group G/N with underlying set

$$\begin{aligned} G/N &= \text{set of left/right cosets of } N \text{ in G} \\ &= \{X \subseteq G : \text{there exists } g \in g \text{ such that } X = gN = Ng\} \end{aligned}$$

having the following properties:

(a) Equipped with a **multiplication map:**

$$G/N \times G/N \to G/N \quad \text{defined by} \quad (g_1N, g_2N) \mapsto (g_1N)(g_2N) = g_1g_2N$$

(b) **Existence of identity element:** $1_{G/N} = 1_GN = N \in G/N$

(c) Equipped with an **inversion map**

$$G/N \to G/N \quad \text{defined by} \quad gN \mapsto (gN)^{-1} = g^{-1}N$$

One checks that the quotient group is a group, i.e. the group axioms in Definition 1.1 indeed hold. These are easy to check and are induced by their validity in G.

Proposition 3.4. Suppose $H \leq G$. Then,

$$\text{the multiplication of left cosets } G/H \times G/H \to G/H \quad \text{is well-defined}$$

if and only if $H \trianglelefteq G$.

Example 3.26. Some obvious examples include $1 \trianglelefteq G$ and $G \trianglelefteq G$, as well as $n\mathbb{Z} \trianglelefteq \mathbb{Z}$.

3.4 The Isomorphism Theorems

We first state an important fact before delving into the isomorphism theorems. If H is a group and $H_0 \leq H$, we say that

$$\text{the inclusion map } i : H_0 \to H \quad \text{where} \quad h_0 \mapsto h_0 \quad \text{is a monomorphism}$$

called the inclusion homomorphism, and $\operatorname{im} i = H_0$.

Proposition 3.5 (universal property of subgroup)**.** Let $\varphi : G \to H$ be a homomorphism from another group G to H such that $\operatorname{im} \varphi \subseteq H_0$, where $H_0 \leq H$. The, there exists a unique homomorphism $\varphi_0 : G \to H_0$

such that the following diagram commutes, i.e. $\varphi = i \circ \varphi_0$:

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[dr, dashed, "\varphi_0"'] & H \\ & H_0 \arrow[u, "i"'] \end{tikzcd}$$

The shaded line to denote $\varphi_0 : G \to H_0$ indicates that φ_0 is unique. In fact, φ_0 is defined as follows:

$$\text{for any } g \in G \quad \text{set } \varphi_0(g) = \varphi(g) \text{ which is regarded as an element of } H_0.$$

Proposition 3.6. The quotient map

$$\pi : G \to G/N \quad \text{where} \quad g \mapsto gN$$

is an epimorphism, with $\ker \pi = N$. The map π is known as the quotient mod N homomorphism.

Proof. For any $g_1, g_2 \in G$, we have

$$\pi(g_1 g_2) = (g_1 g_2) N = (g_1 N)(g_2 N) = \pi(g_1) \pi(g_2)$$

which shows that π is a homomorphism. Also,

$$\ker \pi = \pi\left(1_{G/N}\right) = \pi^{-1}(N) = \{g \in G : gN = N\} = N$$

and the result follows. $\square$

Theorem 3.5 (universal property of quotient group)**.** Let $\varphi : G \to H$ be a homomorphism from G to another group H such that $N \subseteq \ker \varphi$. Then, there exists a unique homomorphism $\overline{\varphi} : G/N \to H$ such that the following diagram commutes, i.e. $\varphi = \overline{\varphi} \circ \pi$:

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, two heads, "\pi"'] & H \\ G/N \arrow[ur, dashed, "\overline{\varphi}"'] & \end{tikzcd}$$

Example 3.27. Set $G = \mathbb{Z}$ and $N = n\mathbb{Z}$, for which we obtain the universal property of $\mathbb{Z}/n\mathbb{Z}$ (Theorem 2.4).

Theorem 3.6 (first isomorphism theorem)**.** Let $\varphi : G \to H$ be a homomorphism. Then, let

$$\varphi = i \circ \widetilde{\varphi} \circ \pi \quad \text{denote the canonical factorisation of } \varphi,$$

where

$$\pi : G \twoheadrightarrow G/\ker \varphi \text{ is the quotient homomorphism} \quad \text{and}$$
$$i : \operatorname{im} \varphi \hookrightarrow H \text{ is the inclusion homomorphism}$$

Also,

$$\widetilde{\varphi} : G/\ker \varphi \to \operatorname{im} \varphi \quad \text{is an isomorphism induced by } \varphi,$$

meaning the following diagram commutes:

$$\begin{tikzcd}
G \arrow[r, "\varphi"] \arrow[d, two heads, "\pi"'] & H \\
G/\ker(\varphi) \arrow[r, "\widetilde{\varphi}"'] & \operatorname{im}(\varphi) = \varphi(G) \arrow[u, "i"']
\end{tikzcd}$$

Proof. Let $\widetilde{\varphi} : G/\ker\varphi \to \varphi(G)$, where $\psi(g\ker\varphi) = \widetilde{\varphi}(g)$. We shall prove that $\widetilde{\varphi}$ is well-defined and injective. We have

$$\begin{aligned} g\ker\varphi = h\ker\varphi \quad &\text{if and only if} \quad h^{-1}g \in \ker\varphi \\ &\text{if and only if} \quad \varphi\left(h^{-1}g\right) = 1_G \\ &\text{if and only if} \quad \varphi(g) = \varphi(h) \end{aligned}$$

so it follows that $\widetilde{\varphi}(g\ker\varphi) = \widetilde{\varphi}(h\ker\varphi)$. In particular, the idea behind showing that a map is well-defined is to justify uniqueness, i.e. for each element in $\widetilde{\varphi}$, there must be exactly one element in $G/\ker(\phi)$ that it maps to. As such, there cannot be ambiguity or multiple possible mappings for a single element.

To show that $\widetilde{\varphi}$ is surjective, suppose there exists $g \in G$ such that $\varphi(g) = h$. Then, $\widetilde{\varphi}(g\ker\varphi) = \varphi(g) = h$ and the result follows. $\square$

Example 3.28 (Dummit and Foote p. 89 Question 37)**.** Let A and B be groups. Show that $\{(a,1) \mid a \in A\}$ is a normal subgroup of $A \times B$ and the quotient of $A \times B$ by this subgroup is isomorphic to B.

Solution. Let $S = \{(a,1) \mid a \in A\}$. Note that $(a,1) \in S$ and $(x,y) \in A \times B$. So,

$$g * s * g^{-1} = (x,y) * (a,1) * (x,y)^{-1} = \left(xax^{-1}, yy^{-1}\right) = \left(xax^{-1}, 1\right) \in S.$$

It follows that $S \trianglelefteq A \times B$.

We then wish to prove that $(A \times B)/S \cong B$. Define a map

$$\varphi : A \times B \to B \quad \text{where} \quad \varphi((a,b)) = b.$$

φ is a well-defined surjective homomorphism. We then compute $\ker\varphi$. Suppose $\varphi((x,y)) = 1_B$. Then, x can be arbitrarily set and $y = 1_B$. So, $\ker\varphi = \{(a,1) : A \in A\} = S$. By the first isomorphism theorem (Theorem 3.6), there exists an isomorphism $\varphi : A \times B \to B$ such that $\ker\varphi = S$. $\square$

Example 3.29 (Dummit and Foote p. 89 Question 38)**.** Let A be an abelian group and let D be the (diagonal) subgroup $\{(a,a) \mid a \in A\}$ of $A \times A$. Prove that D is a normal subgroup of $A \times A$ and $(A \times A)/D \cong A$.

Solution. This question is similar to Example 3.28. Anyway, let $(a,a) \in D$ and $(x,x) \in A \times A$. Then,

$$(x,x) * (a,a) * (x,x)^{-1} = \left(xax^{-1}, xax^{-1}\right) \in D,$$

where the inclusion $\in D$ follows from the fact that $xax^{-1} \in A$.

To prove the second result, define a map

$$\varphi : A \times A \to A \quad \text{where} \quad \varphi((a,a)) = a.$$

Again, one checks that φ is a well-defined surjective homomorphism. We then compute $\ker\varphi$, which turns out to be D. By the first isomorphism theorem (Theorem 3.6), φ is an isomorphism with $\ker\varphi = D$. □

We then discuss the second and third isomorphism theorems. These should be seen as corollaries of the first isomorphism theorem.

Corollary 3.4 (second isomorphism theorem)**.** Let G be a group. Suppose $H \le G$ and $K \trianglelefteq G$. Then, HK is a subgroup of G containing H and K and

$$\text{the composite homomorphism} \quad H \hookrightarrow HK \twoheadrightarrow HK/K \quad \text{induces an isomorphism } H/H\cap K \cong HK/K.$$

In particular, $K \trianglelefteq HK$ and $H\cap K \trianglelefteq H$.

Proof. Consider the map $\varphi : H \to HK/K$ with $\varphi(h) = hK$. One can show that φ is a well-defined surjective homomorphism with $\ker\varphi = H\cap K$. □

Example 3.30. We know that there is a fundamental result in Number Theory that

$$\text{for any } m,n \in \mathbb{Z} \quad \text{we have } \gcd(m,n)\cdot \operatorname{lcm}(m,n) = mn.$$

Use the second isomorphism theorem to deduce this result.

Solution. We will use N in place of K (Corollary 3.4) to denote the normal subgroup of G. Let

$$G = \mathbb{Z}, H = m\mathbb{Z}, N = n\mathbb{Z} \quad \text{where it is clear that} \quad H \le G \text{ and } N \trianglelefteq G.$$

Since $G = \mathbb{Z}$ is an additive group, then $HN = H+N = m\mathbb{Z}+n\mathbb{Z}$. These comprise elements of the form $mx+ny$, where $x,y \in \mathbb{Z}$. Note that

$$\{mx+ny : x,y \in \mathbb{Z}\} = \gcd(m,n)\mathbb{Z} \quad \text{follows by Bézout's lemma.}$$

Consider $H\cap N = m\mathbb{Z}\cap n\mathbb{Z}$. Here, $m\mathbb{Z}$ refers to all multiples of m; $n\mathbb{Z}$ is defined similarly. Hence, $H\cap N = \operatorname{lcm}(m,n)\mathbb{Z}$. Let $d = \gcd(m,n)$ and $\operatorname{lcm}(m,n) = l$. By the second isomorphism theorem,

$$d\mathbb{Z}/n\mathbb{Z} = HN/N \cong H/H\cap K = m\mathbb{Z}/l\mathbb{Z}.$$

Define $\varphi : d\mathbb{Z} \to \mathbb{Z}/\left(\frac{n}{d}\mathbb{Z}\right)$, for which $\ker\varphi = n\mathbb{Z}$. One can deduce that $m\mathbb{Z}/l\mathbb{Z} \cong \mathbb{Z}/\left(\frac{l}{m}\mathbb{Z}\right)$. So,

$$\left|\mathbb{Z}/\left(\frac{n}{d}\mathbb{Z}\right)\right| = \left|\mathbb{Z}/\left(\frac{l}{m}\mathbb{Z}\right)\right| \quad \text{which implies} \quad \frac{n}{d} = \frac{l}{m}.$$

As such, $mn = dl$ and the result follows. □

Example 3.31 (Dummit and Foote p. 101 Question 3)**.** Prove that if H is a normal subgroup of G of prime index p, then for all $K \le G$, either

(i) $K \le H$ or

(ii) $G = HK$ and $|K : K\cap H| = p$

Solution. Suppose $H \trianglelefteq G$ such that $|G : H| = p$. Suppose $K \le G$, then either $K \le H \le G$ or $H \le K \le G$. The former establishes **(i)**. We now work with $H \le K \le G$. By the tower theorem (Theorem 3.4), we have

$$|G : H| = |G : HK|\cdot|HK : H|$$

Since $|G : H| = p$ which is prime, then $|G : HK| = 1$ or p. If $|G : HK| = p$, then $|HK : H| = 1$, so $H = HK$. This implies $K \le H$ (which is just **(i)**). On the other hand, if $|G : HK| = 1$, then $|HK : H| = p$. By the second isomorphism theorem (Theorem 3.4), we have

$$K/H\cap K \cong HK/H \quad \text{where} \quad H \trianglelefteq G.$$

Since the groups are isomorphic, then $|K : H\cap K| = |HK : H|$, so $|K : H\cap K| = p$, and the result follows. □

Corollary 3.5 (third isomorphism theorem). Let G be a group and let $N, K \trianglelefteq G$ with $N \subseteq K \subseteq G$. Then, $K/N \trianglelefteq G/N$ and

$$\begin{aligned}&\text{the composite homomorphism } G \twoheadrightarrow G/N \twoheadrightarrow (G/N)/(K/N)\\ &\text{induces an isomorphism } G/K \cong (G/N)/(K/N)\end{aligned}$$

Proof. Consider the map $\varphi : G/N \to G/K$ with $\varphi(gK) = gH$. One can show that φ is a well-defined surjective homomorphism with $\ker\varphi = H/N$. □

Example 3.32 (Dummit and Foote p. 101 Question 4). Let C be a normal subgroup of the group A and D be a normal subgroup of the group B. Prove that

$$(C\times D) \trianglelefteq (A\times B) \quad \text{and} \quad (A\times B)/(C\times D) \cong (A/C)\times(B/D).$$

Solution. Define a map

$$\varphi : A\times B \to (A/C)\times(B/D) \quad \text{where} \quad \varphi((a,b)) = (aC, bD)$$

We first show that φ is a homomorphism. We have

$$\begin{aligned}\varphi((a_1,b_1)(a_2,b_2)) &= \varphi((a_1a_2, b_1b_2))\\ &= (a_1a_2C, b_1b_2D) = (a_1C, b_1D)(a_2C, b_2D)\\ &= \varphi((a_1,b_1))\,\varphi((a_2,b_2))\end{aligned}$$

This shows that φ is a homomorphism. Showing that φ is surjective is trivial; also $\ker\varphi = C\times D$. Hence, φ induces an isomorphism, with $(C\times D) \trianglelefteq (A\times B)$, which follows by the third isomorphism theorem (Theorem 3.5). □

Theorem 3.7 (lattice isomorphism theorem). Let G be a group and $N \trianglelefteq G$. Let $\pi : G \to G/N$ be the quotient homomorphism. Then, the maps

$$\{\text{subgroups of } G \text{ containing } N\} \leftrightarrow \{\text{subgroups of } G/N\}$$

where $H \mapsto \pi(H)$ and $\pi^{-1}(X)X$ are well-defined inclusion-preserving and normality-preserving bijections, inverses of each other.

Lemma 3.2 (Zassenhaus' lemma). Let $A_1 \trianglelefteq A_2$ and $B_1 \trianglelefteq B_2$ be four subgroups of a group G. Then,

$$A_1(A_2\cap B_1) \trianglelefteq A_1(A_2\cap B_2) \quad \text{and} \quad B_1(A_2\cap B_2) \trianglelefteq B_1(A_1\cap B_2),$$

and we have the following isomorphism:

$$\frac{A_1(A_2\cap B_2)}{A_1(A_2\cap B_1)} \cong \frac{A_2\cap B_2}{(A_1\cap B_2)(A_2\cap B_1)} \cong \frac{B_1(A_2\cap B_2)}{B_1(A_1\cap B_2)}$$

Proof. Due to symmetry, we only prove one of the isomorphisms. First, we prove that $A_1(A_2\cap B_1) \trianglelefteq A_1(A_2\cap B_2)$. In other words, if $c \in A_2\cap B_1$ and $x \in A_2\cap B_2$, then $xcx^{-1} \in A_2\cap B_2$. This is trivial (recall that $B_1 \trianglelefteq B_2$). Now, it suffices to show that there exists an isomorphism

$$\frac{A_1(A_2\cap B_2)}{A_1(A_2\cap B_1)} \cong \frac{A_2\cap B_2}{(A_1\cap B_2)(A_2\cap B_1)}.$$

Set $D = (A_1\cap B_2)(A_2\cap B_1)$. Define

$$\phi : A_1(A_2\cap B_2) \to (A_2\cap B_2)/D \quad \text{where} \quad \phi : a_1 x \mapsto xD$$

Here, $a_1 \in A_1$ and $x \in A_2\cap B_2$. One checks that ϕ is well-defined and is a homomorphism. Surjectivity is clear. Now, we need to show that $\ker(\phi) = A_1(A_2\cap B_1)$. Suppose $a_1 x \in \ker(\phi)$. Then, $x \in D = (A_1\cap B_2)(A_2\cap B_1)$. Hence, $x = a_1' x'$, where $a_1' \in A_1\cap B_2$ and $x' \in A_2\cap B_1$. As such, $a_1 x = a_1 a_1' x'$.

By considering $x' \in A_2\cap B_1$ and $(A_1\cap B_2) \subseteq A_1$, we have

$$a_1 \in A_1\cap A_1\cap (A_2\cap B_1) = A_1(A_2\cap B_1)$$

which concludes the proof. □

3.5 Transpositions and the Alternating Group

Lemma 3.3. Any cycle in S_n can be written as a product of transpositions.

Proof. Suppose $m \leq n$. Note that

$$(a_1\, a_2\, a_m) \quad \text{is an } m\text{-cycle.}$$

One observes that

$$(a_1\, a_2\, a_m) = (a_1\, a_m)(a_1\, a_{m-1})\ldots(a_1\, a_3)(a_1\, a_2) \quad \text{which is a product of transpositions.}$$

The result follows. □

Proposition 3.7. Every element of S_n can be written as a product of transpositions.

Proof. We proceed with strong induction on $n \in \mathbb{Z}^+$. The base case $n = 1$ is trivial since S_1 only contains the identity permutation. Suppose $n > 1$ is arbitrary and regard

$$S_{n-1} \leq S_n \quad \text{via} \quad S_{n-1} = \{\sigma \in S_n : \sigma(n) = n\}.$$

Consider $\sigma \in S_n$. Define

$$\tau = \begin{cases} \text{the transposition } (\sigma(n)\; n) \in S_n & \text{if } \sigma(n) \neq n; \\ \text{identity} \in S_n & \text{if } \sigma(n) = n. \end{cases}$$

Then, $\tau\circ\sigma$ maps n to n, so $\tau\circ\sigma \in S_{n-1}$. By the induction hypothesis,

$$\text{there exist transpositions } \tau_1,\ldots,\tau_k \in S_{n-1} \subseteq S_n \quad \text{such that} \quad \tau\circ\sigma = \tau_1\ldots\tau_k,$$

which implies $\sigma = \tau\tau_1\ldots\tau_k$ is a product of transpositions in S_n. □

Corollary 3.6. S_n is generated by the $n-1$ transpositions

$$(1\,2),(1\,3),\dots,(1\,n).$$

Proof. For any $a,b \in \{2,3,\dots,n\}$ with $a \neq b$, we have

$$(a\,b) = (1\,b)\,(1\,a)\,(1\,b)$$

and the result follows. □

Corollary 3.7. S_n is generated by the $n-1$ adjacent transpositions

$$(1\,2),(2\,3),\dots,(n-1\,n).$$

Proof. If $b \in \{2,3,\dots,n\}$, where $b < n$, then

$$(1\,b+1) = (b\,b+1)\,(1\,b)\,(b\,b+1)$$

so by induction, the transpositions $(1\,2),(1\,3),\dots,(1\,n)$ are in G. □

Corollary 3.8. S_n is generated by $(1\,2)$ and the n-cycle $(1\,2\,\dots\,n)$.

Proof. If $b \in \{1,\dots,n\}$ and $b < n$, then

$$(1\,2\,\dots\,n)\,(b\,b+1)\,(1\,2\,\dots\,n)^{-1} = (b+1\,b+2)$$

so by induction, the adjacent transpositions are in the subgroup of S_n generated by $(1\,2)$ and $(1\,2\,\dots\,n)$. □

Definition 3.13 (reversal of permutation)**.** A reversal of $\sigma \in S_n$ is an ordered pair (a,b) with $a,b \in \{1,\dots,n\}$ such that

$$a < b \quad \text{and} \quad \sigma(a) > \sigma(b).$$

Let $\mathcal{R}(\sigma)$ denote the following set:

$$\mathcal{R}(\sigma) = \left\{(a,b) \in \{1,\dots,n\}^2 : (a,b) \text{ is a reversal of } \sigma\right\}$$

Proposition 3.8. For any $\sigma \in S_n$, we have $0 \leq |\mathcal{R}(\sigma)| \leq \binom{n}{2}$.

Definition 3.14 (sign homomorphism)**.** The sign homomorphism of S_n is the map $\varepsilon : S_n \to \{\pm 1\}$ defined as follows:

$$\text{for any } \sigma \in S_n \quad \text{we have} \quad \varepsilon(\sigma) = (-1)^{|\mathcal{R}(\sigma)|} = \begin{cases} 1 & \text{if } \sigma \text{ has an even number of reversals;} \\ -1 & \text{if } \sigma \text{ has an odd number of reversals.} \end{cases}$$

Definition 3.15. The permutation $\sigma \in S_n$ is called an even permutation if $\varepsilon(\sigma) = 1$, and it is an odd permutation if $\varepsilon(\sigma) = -1$.

Example 3.33. Clearly, $\mathcal{R}(1) = \emptyset$. Also, $\varepsilon(1) = 1$.

Example 3.34. Let $\sigma = (i\,j)$. Then,

$$\mathcal{R}(\sigma) = \{(i\,j)\} \sqcup \{(i\,b) : i < b < j\} \sqcup \{(a\,j) : i < a < j\}.$$

Hence, $\mathcal{R}(\sigma)$ collects all transpositions related to $(i\,j)$ in the sense that they either directly swap i with j, or involve one of the endpoints (i or j) and another element in the interval (i, j). Moreover, we have $\varepsilon(\sigma) = -1$.

Example 3.35. Let

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ n & n-1 & \ldots & 1 \end{pmatrix}.$$

Then,

$$\mathcal{R}(\sigma) = \left\{(a,b) \in \{1,\ldots,n\}^2 : a < b\right\}.$$

We also have

$$\varepsilon(\sigma) = \begin{cases} 1 & \text{if } n \equiv 0,1 \pmod 4; \\ -1 & \text{if } n \equiv 2,3 \pmod 4. \end{cases}$$

Definition 3.16 (alternating group)**.** The alternating group of degree n is the kernel of the sign homomorphism ε, i.e.

$$A_n = \ker \varepsilon \trianglelefteq S_n.$$

In simpler terminologies, A_n is the set of even permutations on n letters.

Example 3.36. $A_3 = \{(1), (1,2,3), (1,3,2)\}$

Proposition 3.9. For $n > 1$,

$$A_n \text{ is a proper normal subgroup of } S_n \quad \text{and} \quad |A_n| = \frac{1}{2}n!.$$

Proof. For the first result, we will only prove that $A_n \leq S_n$ as A_n being a normal subgroup follows from there. Since $(1) = (1\,2)(1\,2)$, it implies that $(1) \in A_n$ so $A_n \neq \emptyset$. Suppose

$$\sigma \text{ and } \tau \quad \text{can be} \quad \text{expressed as a product of an even number of permutations}$$

Then, τ^{-1} can also be expressed as a product of an even number of permutations. Hence, the same can be said for $\sigma\tau^{-1}$, implying that $\sigma\tau^{-1} \in A_n$. By Proposition 2.1, the first result follows.

For the second result, define

$$\varphi : A_n \to S_n \setminus A_n \text{ such that } \varphi(\sigma) = (1\,2)\,\sigma, \quad \text{which}$$
$$\text{has inverse} \quad \varphi^{-1} : S_n \setminus A_n \to A_n \text{ such that } \varphi^{-1}(\tau) = (1\,2)\,\tau$$

Since φ is bijective, then $|A_n| = |S_n| - |A_n|$ and the result follows. $\square$

Lemma 3.4. A_n is generated by 3-cycles.

Proof. It suffices to prove that a product of two transpositions can be expressed as a product of 3-cycles. For $1 \leq a < b < c < d \leq n$, we have

$$(a,b)(c,d) = (a,b,c)(b,c,d) \quad \text{and} \quad (a,b)(a,c) = (a,c,b)$$

and the result follows. □

Example 3.37. Prove that A_n is generated by $\{(1,2,3),(1,2,4),\ldots,(1,2,n)\}$.

Solution. Motivated by Lemma 3.4, observe that

$$(1,2,3)(1,2,4) = (1,3)(2,4) \quad \text{and} \quad (1,2,5)(1,2,6) = (1,5)(2,6) \quad \text{and so on.}$$

In general,

$$(1,2,k)(1,2,k+1) = (1,k)(2,k+1) \quad \text{for all } k \geq 3.$$

Hence, $(1,2,3),(1,2,4),\ldots,(1,2,n)$ is a product of $2n$ transpositions which is even and so it generates A_n. □

Example 3.38 (classic counterexample to converse of Lagrange's theorem)**.** We note that $|A_4| = 12$ but A_4 does not contain any subgroup of order 6. This is a classic counterexample to the converse of Lagrange's theorem. Let us see why this is so.

By Lemma 3.4, we know that A_n is generated by 3-cycles. In particular, A_4 is generated by 3-cycles (for those interested in the elements of A_4, please refer to Example 3.39). For example,

$$(1\,3)\,(2\,4) \text{ is an even permutation in } A_4 \quad \text{and} \quad (1\,3)\,(2\,4) = (1\,2\,3)\,(1\,2\,4)$$

which is a product of 3-cycles. Suppose there exists $H \leq A_4$ such that $|H| = 6$. We claim that H contains all 3-cycles, which would imply that $H = A_4$, a contradiction. To see why, suppose $\sigma \in A_4 \setminus H$ is a 3-cycle. Then,

$$\sigma H \neq H \text{ is in the quotient group } AH/H \quad \text{so} \quad \sigma^2 H = (\sigma H)(\sigma H) \text{ must be } H \text{ in } AH/H.$$

So, $\sigma^2 \in H$. Since σ is a 3-cycle, then $\sigma^{-1} \in H$, so $\sigma \in H$ since H is a subgroup so it is closed under multiplication, i.e. $\sigma = \sigma^2 \cdot \sigma^{-1}$. Hence, all 3-cycles are contained in H, so $H = A_4$, resulting in a contradiction.

Example 3.39 (MA2202S AY24/25 Sem 2 Tutorial 2)**.**

(i) List all the elements of A_4.

(ii) Let H be a subgroup of S_4 with the property that $\sigma^2 \in H$, for any $\sigma \in S_4$. Show that H contains A_4, and further deduce that H is either A_4 or S_4.

Solution.

(i) A_4 contains all even permutations on four letters, so they are as follows: 4

(1) $()$

(2) $(1\,2\,3)$

(3) $(1\,2\,4)$

(4) $(1\,3\,2)$

(5) $(1\,3\,4)$

(6) $(1\,4\,2)$

(7) $(1\,4\,3)$

(8) $(2\,3\,4)$

(9) $(2\,4\,3)$

(10) $(1\,2)\,(3\,4)$

(11) $(1\,3)\,(2\,4)$

(12) $(1\,4)\,(2\,3)$

One can easily check that each permutation mentioned is even.

(ii) We first prove that $A_4 \subseteq H$. Choose some arbitrary permutation $\tau \in A_4$. Then, there exists $\sigma \in S_4$ such that $\tau = \sigma^2$ (by Definition of the alternating group). So, $\tau = \sigma^2 \in H$, implying that $A_4 \subseteq H$.

For the second part, we note that $[S_4 : A_4] = 2$ by considering the orders of each group. Recall Lemma 3.1, which states that if $H \le G$ such that $[G : H] = 2$, then $H \trianglelefteq G$. As such, $A_4 \trianglelefteq S_4$. From the first part of **(ii)**, we deduced that

$$A_4 \subseteq H \subseteq S_4$$

so by the tower theorem (Theorem 3.4), we have

$$[S_4 : A_4] = [S_4 : H] \cdot [H : A_4] \quad \text{so} \quad 2 = [S_4 : H] \cdot [H : A_4]\,.$$

As such, either $[S_4 : H] = 1$ or 2. If the index is 1, then $H = S_4$; if the index is 2, then $[H : A_4] = 1$, implying that $H = A_4$. $\square$

Chapter 4
Group Actions

4.1
Group Actions and Permutation Representations

When we discuss the problems from the Dummit and Foote textbook, the set A is taken to be non-empty.

Definition 4.1 (action map and action homomorphism). Let G be a group and A be a set. An action map of G on A is a map

$$\alpha : G \times A \to A \quad \text{where} \quad (g,a) \mapsto ga$$

satisfying the following properties:

(i) Associativity of $\cdot$: For all $g_1, g_2 \in G$ and $a \in A$, we have $g_1 \cdot (g_1 \cdot a) = (g_1 g_2) \cdot a$

(ii) 1_G acts as identity for $\cdot$: for al $a \in A$, we have $1_G \cdot a = a$

An action homomorphism of G on A is a homomorphism

$$\varphi : G \to S_A = \{\text{all bijections } A \to A\}.$$

Lemma 4.1. Suppose

$$\alpha : G \times A \to A \quad \text{is an action map.}$$

For any $g \in G$, define

$$\sigma_g : A \to A \quad \text{to be the map} \quad a \mapsto \sigma_g(a) = \alpha(g,a) = ga.$$

Define the map

$$\varphi_\alpha : G \to S_A \quad \text{by setting} \quad g \mapsto \sigma_g.$$

Then, φ_α is a well-defined homomorphism called the action homomorphism induced by α.

Proof. We first prove that φ_a is well-defined. It suffices to show that for any $g \in G$, the map σ_g is in S_A. Indeed, $\sigma_g : A \to A$ is a bijection with inverse $\sigma_{g^{-1}} : A \to A$, where $\sigma_{g^{-1}} : a \mapsto g^{-1}a$. To see why, one can verify that

$$\sigma_{g^{-1}} \circ \sigma_g = a \quad \text{and} \quad \sigma_g \circ \sigma_{g^{-1}} = a.$$

We then prove that φ_a is a homomorphism. It suffices to prove that

$$\text{for any } g_1, g_2 \in G, \quad \text{we have } \varphi_a(g_1 g_2) = \varphi(g_1) \circ \varphi_a(g_2).$$

Indeed, this is true because

$$\sigma_{g_1 g_2} : a \mapsto (g_1 g_2) \cdot a \quad \text{and} \quad \sigma_{g_1} \circ \sigma_{g_2} : a \mapsto g_1 \cdot (g_2 a)$$

which are equal in S_A. □

Lemma 4.2. Suppose $\varphi : G \to S_A$ is a homomorphism. For any $g \in G$ and $a \in A$, define $g \cdot a = \varphi(g)(a) \in S_A$. Define the map

$$\alpha_\varphi : G \times A \to A \quad \text{by setting} \quad (g,a) \mapsto g \cdot a = \varphi(g)(a).$$

Then, α_φ is an action map called the action map induced by φ.

Proposition 4.1. The maps

$$\{\text{action maps of } G \text{ on } A\} \leftrightarrow \{\text{action homomorphism of } G \text{ on } A\}$$

where

$$\alpha \mapsto \varphi_\alpha \quad \text{and} \quad \alpha_\varphi \varphi \quad \text{are bijections, inverses of each other.}$$

Proof. We only prove the forward direction as the proof of the reverse direction is similar. Start with an action map α. Then, we obtain an action homomorphism φ_α, which induces an action map α_{φ_α}. So, for any $g \in G$ and any $a \in A$, we have

$$\alpha_{\varphi_\alpha}(g,a) = \varphi_\alpha(g)(a) = \alpha(g,a)$$

which is an action homomorphism on $a \in A$. □

Example 4.1 (trivial action). For any group G and any set A, the trivial action of G on A is defined by

$$\begin{aligned} &\text{the trivial action homomorphism} \quad G \to S_A \quad \text{where} \quad g \mapsto \mathrm{id}_A \quad \text{and} \\ &\text{the trivial action map} \quad G \times A \to A \quad \text{where} \quad (g,a) \mapsto a \end{aligned}$$

Example 4.2 (tautological action). For any set A, the tautological action of the group S_A on A is defined by

$$\begin{aligned} &\text{the identity action homomorphism} \quad S_A \to S_A \quad \text{where} \quad g \mapsto g \quad \text{and} \\ &\text{the tautological action map} \quad S_A \times A \to A \quad \text{where} \quad (g,a) \mapsto g(a) \end{aligned}$$

Example 4.3. For any $n \in \mathbb{Z}_{\geq 0}$, the symmetric group S_n acts tautologically on $\{1,\ldots,n\}$.

To see why, given an arbitrary permutation $\sigma \in Sn$, we can apply σ directly to any element $i \in \{1,\ldots,n\}$, resulting in a new element $\sigma(i)$ from the same set. Hence, S_n defines a group action on $\{1,\ldots,n\}$ by mapping each i to $\sigma(i)$ for every $\sigma \in S_n$. The explanation *tautological* action is due to the fact that the action uses the definition of S_n directly without any further modifications —

$$\text{the elements of } S_n \quad \text{are precisely} \quad \text{the maps that permute } \{1,\ldots,n\},$$

and the action on $\{1,\ldots,n\}$ is exactly what these maps are designed to do.

Definition 4.2 (multiplication action). Let R be a ring. This ring need not be commutative, i.e.

$$\text{for any } x,y \in R \quad \text{it is not necessary that} \quad x \cdot y = y \cdot x.$$

The multiplicative group $A^\times$ is defined as follows:

$$A^\times = \{a \in A : \text{there exists } b \in A \text{ such that } ab = 1_A = ba\}$$

The multiplication action of $A^\times$ on A is defined by

$$\text{restricting the multiplication map } A\times A\to A \quad \text{to} \quad A^\times \times A \to A.$$

We shall see several examples of Definition 4.2 in action.

Example 4.4. Note that $\mathbb{Z},\mathbb{R},\mathbb{C}$ are rings. We have

$$\begin{aligned} \text{the group } \mathbb{Z}^\times = \{\pm 1\} &\quad \text{acts by multiplication on } \mathbb{Z}\\ \text{the group } \mathbb{R}^\times = \mathbb{R}\setminus\{0\} &\quad \text{acts by multiplication on } \mathbb{R}\\ \text{the group } \mathbb{C}^\times = \mathbb{C}\setminus\{(0,0)\} &\quad \text{acts by multiplication on } \mathbb{C}\end{aligned}$$

Example 4.5. For any $n \in Z_{\geq 0}$,

$$\text{the group } (\mathbb{Z}/n\mathbb{Z})^\times \quad \text{acts by multiplication on } \mathbb{Z}/n\mathbb{Z}.$$

Example 4.6. For any $n\in\mathbb{Z}$ and any commutative ring R,

$$\text{the group } \mathrm{GL}_n(R) = (\mathcal{M}_{n\times n}(R))^\times \quad \text{acts by multiplication on } \mathcal{M}_{n\times n}(R).$$

To see why, recall from Definition 1.18 that $\mathrm{GL}_n(R)$ refers to the general linear group of degree n over a commutative ring R. This group consists of all invertible $n\times n$ matrices with entries from R. More formally,

$$\mathrm{GL}_n(R) = \{\mathbf{A}\in\mathcal{M}_{n\times n}(R) : \text{there exists } \mathbf{B}\in\mathcal{M}_{n\times n}(R) \text{ such that } \mathbf{AB}=\mathbf{BA}=\mathbf{I}_n\},$$

where $\mathcal{M}_{n\times n}(R)$ denotes the set of all $n\times n$ matrices with entries in R and $\mathbf{I}_n$ is the $n\times n$ identity matrix. The notation $(\mathcal{M}_{n\times n}(R))^\times$ denotes the group of invertible elements within the ring $\mathcal{M}_{n\times n}(R)$, which is precisely $\mathrm{GL}_n(R)$ because an element in $\mathcal{M}_{n\times n}(R)$ is invertible if and only if it is in $\mathrm{GL}_n(R)$.

$\mathrm{GL}_n(R)$ acts on $\mathcal{M}_{n\times n}(R)$ by left (or right) matrix multiplication. Specifically, for any invertible matrix $\mathbf{A}\in\mathrm{GL}_n(R)$ and any matrix $\mathbf{B}\in\mathcal{M}_{n\times n}(R)$, the action of $\mathbf{A}$ on $\mathbf{B}$ is given by:

$$\mathbf{A}\cdot\mathbf{B} = \mathbf{AB} \quad \text{for which the action is well-defined since} \quad \mathbf{AB}\in\mathcal{M}_{n\times n}(R).$$

Example 4.7. We have

$$\begin{aligned} \mathbb{R}^\times \text{ acts on} &\quad \text{any } \mathbb{R}\text{-vector space by scalar multiplication}\\ \mathbb{C}^\times \text{ acts on} &\quad \text{any } \mathbb{C}\text{-vector space by scalar multiplication}\end{aligned}$$

4.2 Groups acting on themselves by Left Multiplication

Definition 4.3 (left multiplication action). For any group G, the left multiplication action of G on itself is defined by

$$\text{the group multiplication map } G\times G\to G \quad \text{where} \quad (g,a)\mapsto g\cdot a.$$

The corresponding action homomorphism

$$G\to \mathrm{Perm}(G) \quad \text{which is} \quad g\mapsto (a\mapsto g\cdot a)$$

is injective. By the first isomorphism theorem, it induces an isomorphism of G with its image in $\text{Perm}(G)$.

Theorem 4.1 (Cayley's theorem)**.** Let G be a finite group of order n. Then,

$$G \cong H \quad \text{where} \quad H \leq S_n.$$

4.3 Groups acting on themselves by Conjugation

Definition 4.4 (inner automorphism)**.** An inner automorphism of G is an automorphism $\sigma \in \text{Aut}(G)$ such that there exists $g \in G$ with $\sigma = a \mapsto gag^{-1}$. The subgroup of $\text{Aut}(G)$

$$\text{consisting of all inner automorphisms} \quad \text{is denoted by } \text{Inn}(G).$$

Definition 4.5 (conjugation action)**.** For any group G, the conjugation action of G on itself is defined by

$$\text{the conjugation map } G \times G \to G \quad \text{where} \quad (g,a) \mapsto g \cdot a \cdot g^{-1}.$$

The corresponding action homomorphism

$$G \to \text{Aut}(G) \subseteq \text{Perm}(G) \quad \text{which is} \quad g \mapsto \left(a \mapsto gag^{-1}\right)$$

with kernel $Z(G)$. Thus, the following diagram commutes:

$$\begin{tikzcd} G \arrow[r] \arrow[d, two heads] & \text{Aut}(G) \\ G/Z(G) \arrow[r] & \text{Inn}(G) \arrow[u, hook] \end{tikzcd}$$

We give some examples of groups acting on themselves by conjugation and the associated inner automorphism groups (Examples 4.8, 4.9, 4.10, and 4.11).

Example 4.8 (conjugation action on S_3)**.** Let $G = S_3$, the symmetric group on 3 elements, i.e.

$$S_3 = \{e, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}.$$

Then, the center $Z(S_3) = \{e\}$ since no non-trivial element commutes with all others. As such, $\text{Inn}(S_3) \cong S_3/Z(S_3) \cong S_3$. Also, the conjugacy classes are

$$\{e\} \quad \text{and} \quad \{(1\,2), (1\,3), (2\,3)\} \quad \text{and} \quad \{(1\,2\,3), (1\,3\,2)\}.$$

This conjugation action permutes elements within each conjugacy class.

Example 4.9 (conjugation action on $\mathbb{Z}$)**.** Let $G = \mathbb{Z}$, the additive group of integers. Since $\mathbb{Z}$ is Abelian, then conjugation is trivial, i.e.

$$g * a * g^{-1} = g + a + (-g) = a \quad \text{for all } g, a \in \mathbb{Z}.$$

As such, every conjugation map is the identity. Also, $\text{inn}(\mathbb{Z}) = \{e\}$ and $Z(\mathbb{Z}) = \mathbb{Z}$. In fact, for any Abelian group, $\text{Inn}(G)$ is trivial.

Example 4.10 (conjugation action on D_8). Consider $G = D_8$, the dihedral group of order 8, which has presentation

$$D_8 = \left\langle r, s \mid r^4 = s^2 = e \text{ and } rs = sr^{-1} \right\rangle.$$

Note that $Z(D_8) = \{e, r^2\}$ (by manually verifying). As such, $\mathrm{Inn}(D_8) \cong D_8/Z(D_8) \cong V_4$, where V_4 is the Klein four-group. Also, the conjugacy classes are

$$\{e\}, \{r, r^3\}, \{r^2\}, \{s, sr^2\}, \{sr, sr^3\}.$$

The conjugation action reflects the group's rotational and reflectional symmetries.

Example 4.11 (conjugation action on $\mathrm{GL}_n(\mathbb{R})$). Let $G = \mathrm{GL}_n(\mathbb{R})$. Conjugation here refers to matrix similarity — elements in the same conjugacy class are similar matrices (i.e. they represent the same linear transformation up to basis change). Note that $Z(\mathrm{GL}_n(\mathbb{R}))$ are the scalar matrices $\lambda \mathbf{I}$, where $\lambda \neq 0$.

A fun fact is that the projective general linear group $\mathrm{PGL}_n(\mathbb{R})$ is defined as follows:

$$\mathrm{PGL}_n(\mathbb{R}) = \mathrm{GL}_n(\mathbb{R}) / Z(\mathrm{GL}_n(\mathbb{R})),$$

i.e. to obtain $\mathrm{PGL}_n(\mathbb{R})$, we mod out non-zero multiples of the identity matrix. Some applications of the projective linear group can be found in areas like Number Theory, Algebraic Geometry and Dynamical Systems.

4.4 Orbits and Stabilisers

Proposition 4.2. Let G be a group acting on a set A. The relation $\sim$ on A is defined as follows:

$$a \sim b \quad \text{if and only if} \quad \text{there exists } g \in G \text{ such that } ga = b.$$

The relation $\sim$ is an equivalence relation.

For any $a \in A$, define the G-orbit of a to be the $\sim$ equivalence class containing a, which is denoted by

$$G \cdot a = \{g \cdot a \in A : g \in G\}.$$

The set of G-orbits of A form a partition of A.

Proof. We first verify that $\sim$ is an equivalence relation. Note that

$$\begin{aligned} \sim \text{ is reflexive} \quad &\text{as} \quad 1_G \cdot a = a \\ \sim \text{ is symmetric} \quad &\text{as} \quad ga = b \text{ implies } g^{-1}b = a \\ \sim \text{ is transitive} \quad &\text{as} \quad g_1 a = b \text{ and } g_2 b = c \text{ implies } (g_2 g_1) a = c \end{aligned}$$

so it follows that $\sim$ is an equivalence relation.

We then prove the second part of the proposition. Note that a subset $X \subseteq A$ is an $\sim$-equivalence class if and only if there exists $a \in A$ such that $X = \{b \in A : a \sim b\} = G \cdot a$. It follows that the $\sim$-equivalence classes in A, i.e. the G-orbits in A, form a partition of A. $\square$

Definition 4.6 (transitive action). The action of G on A is transitive if and only if there is only one orbit, which is A itself, i.e. if and only if

$$\text{there exists } a \in A \quad \text{such that} \quad A = G \cdot a.$$

Definition 4.7 (stabilizer). For any $a \in A$, the stabilizer of a is the subgroup

$$G_a = \{g \in G : ga = a\} \quad \text{of } G.$$

Example 4.12. For the trivial action of G on A, the G-orbits in A are $\{a\}$ for every $a \in A$. So, the action is not transitive unless $|A| = 1$. The stabilizer of any $a \in A$ is $G_a = G$.

Example 4.13. For the tautological action of the group $\mathrm{Perm}(A)$ on A, its action is transitive, i.e. the only orbit is A. Also, the stabilizer of any $a \in A$ is the subgroup $\mathrm{Perm}(A)_{\{a\}}$.

Example 4.14. For the left multiplication action of G on itself, the action is transitive as the only orbit is $G \cdot 1_G = G$. The stabilizer of any $a \in G$ is the trivial subgroup $\{1_G\}$.

Example 4.15. For the left multiplication of G on G/H, where $H \leq G$, the action is transitive as the only orbit is $G \cdot 1_G H = G/H$. The stabilizer of $1_G H$ is the subgroup H; the stabilizer of xH is the subgroup xHx^{-1}.

For the latter, to see why, we see that $gxH = xH$ is equivalent to $x^{-1}gxH = H$, so $x^{-1}gx \in H$, and we conclude that $g \in xHx^{-1}$.

Example 4.16. For the conjugation of G on itself, the G-orbit of 1_G is $\{1_G\}$, so the action is not transitive unless $|G| = 1$. The orbit of $a \in G$ is the conjugacy class of a. Recall from Definition 2.6 that this is precisely the set of conjugates of a in G, which is

$$\left\{gag^{-1} \in G : g \in G\right\}.$$

The stabilizer of $a \in G$ is the centralizer of a in G, i.e.

$$C_G(a) = \left\{g \in G : gag^{-1} = a\right\}.$$

Example 4.17. For the conjugation action of G on the subsets of G, the G-orbit of a subset $A \subseteq G$ is the set of conjugates of A in G, i.e.

$$\left\{gAg^{-1} : g \in G\right\}.$$

The stabilizer of A is the normalizer of A in G, i.e.

$$N_G(A) = \left\{g \in G : gAg^{-1} = A\right\}.$$

Example 4.18 (Dummit and Foote p. 96 Question 15). Let $G = S_n$ and for fixed $i \in \{1, \ldots, n\}$, let G_i be the stabiliser of i. Prove that $G_i \cong S_{n-1}$.

Solution. Consider some permutation $\sigma \in G_i$. Then, σ is the product of disjoint cycles. Note that if $i \notin \sigma$ as i needs to be fixed. So, G_i consists of $\{1, \ldots, n\} \setminus \{i\}$ so $|G_i| = |S_{n-1}|$. The result follows. $\square$

Example 4.19 (Dummit and Foote p. 116 Question 1). Let G act on the set A. Prove that

$$\text{if } a, b \in A \text{ and } b = g \cdot a \text{ for some } g \in G \quad \text{then} \quad G_b = gG_ag^{-1} \ (G_a \text{ is the stabilizer of } a).$$

Deduce that if G acts transitively on A then the kernel of the action is

$$\bigcap_{g\in G} gG_ag^{-1}.$$

Solution. Recall that for any $a \in A$, the subgroup G_a is the stabilizer of a in G, i.e. $G_a = \{g \in G : ga = a\}$. Suppose $x \in G_b$. Then, $xb = b$, so

$$g^{-1}xg\cdot a = g^{-1}xb = g^{-1}b = a$$

which shows that $g^{-1}xg \in G_a$, so $x \in gG_ag^{-1}$.

Next, suppose $x \in G_a$. Then, $xa = a$, so

$$gxg^{-1}\cdot b = gxg^{-1}b = gxa = ga = b$$

which shows that $gxg^{-1} \in G_b$. We conclude that $G_b = gG_ag^{-1}$.

Recall that if G acts transitively on A, then there exists only one orbit, which is A itself. Let K denote the kernel of this action. We wish to prove that

$$K = \bigcap_{g\in G} gG_ag^{-1}.$$

We first prove the forward inclusion. Suppose $x \in K$. Then, $x\cdot a = a$ for all $a \in A$. One can show that $g^{-1}xg = a$ so that $g^{-1}xg \in G_a$ for all $g \in G$. As such, $x \in gG_ag^{-1}$ for all $g \in G$, which implies

$$x \in \bigcap_{g\in G} gG_ag^{-1}.$$

We then prove the reverse inclusion. Suppose x is contained in the intersection. Then, $x = gG_ag^{-1}$ for some $g \in G$. Since the group action is transitive, then there exists $b \in A$ such that $b = g\cdot a$ for some $g \in G$. As such,

$$\begin{aligned} x\cdot b &= gyg^{-1}b \quad \text{for some } y \in G_a \\ &= gyg^{-1}ga \\ &= gya \\ &= ga \quad \text{since } y \in G_a \end{aligned}$$

which is equal to b. Since $x\cdot b = b$, then x stabilizes b, implying that $x \in K$. So, the kernel K is indeed the aforementioned intersection. □

Example 4.20 (Dummit and Foote p. 116 Question 2)**.** Let G be a *permutation group* on the set A (i.e., $G \le S_A$), let $\sigma \in G$ and let $a \in A$. Prove that $\sigma G_a\sigma^{-1} = G_{\sigma(a)}$. Deduce that if G acts transitively on A then

$$\bigcap_{\sigma\in G} \sigma G_a\sigma^{-1} = 1.$$

Solution. Suppose $x \in \sigma G_a\sigma^{-1}$. Then, there exists $y \in G_a$ such that $x = \sigma y\sigma^{-1}$. As such,

$$x\cdot a = \sigma y\sigma^{-1}\sigma\cdot a = \sigma y\cdot a = \sigma\cdot a = \sigma(a).$$

So, $x \in G_{\sigma(a)}$.

Conversely, suppose $x \in G_{\sigma(a)}$. Then, $x \cdot a = \sigma(a)$. As such,

$$\sigma^{-1}x\sigma \cdot a = \sigma^{-1}x \cdot \sigma(a) = \sigma^{-1} \cdot \sigma(a) = a.$$

So, $\sigma^{-1}x\sigma \in G_a$, which implies $x \in \sigma G_a \sigma^{-1}$.

Next, suppose G acts transitively on A. Recall Definition 4.6, which states that for any $x, y \in A$, there exists $g \in G$ such that $y = g \cdot x$. By Example 4.19, we must have

$$\text{kernel of action} = \bigcap_{\sigma \in G} \sigma G_a \sigma^{-1}.$$

As such, it suffices to prove that the kernel is trivial. Since $G \leq S_A$, then the homomorphism $\varphi : G \to S_A$ is injective, so its kernel is trivial. □

Example 4.21 (Dummit and Foote p. 116 Question 3). Assume that G is an abelian, transitive subgroup of S_A. Show that $\sigma(a) \neq a$ for all $\sigma \in G - \{1\}$ and all $a \in A$. Deduce that $|G| = |A|$. (*Hint:* Use Example 4.20)

Solution. Suppose $G \leq S_A$ and G acts transitively on A. So, we have

$$\begin{aligned} 1 &= \bigcap_{\sigma \in G} \sigma G_a \sigma^{-1} && \text{by Example 4.20} \\ &= \bigcap_{\sigma \in G} \sigma \sigma^{-1} G_a && \text{since } G \text{ is Abelian} \\ &= \bigcap_{\sigma \in G} G_a \end{aligned}$$

which is independent of σ. So, $1 = G_a$, i.e. the stabilizer of a in G is trivial. So, $\sigma(a) \neq a$ for all $\sigma \in G \setminus \{1\}$ and for all $a \in A$.

We then prove $|G| = |A|$. Since the action of G on A is transitive, then for any $a, b \in A$, there exists $\sigma \in G$ such that $b = \sigma \cdot a$. Suppose $\tau \in G$ such that $\sigma \cdot a = \tau \cdot a$, so $\tau^{-1}\sigma \cdot a = a$, i.e. $\tau^{-1}\sigma \in G_a = 1$. This implies $\sigma = \tau$. As such, if we define a map $\varphi : A \to G$, we must have $\ker \varphi = 1$, i.e. φ is injective, so $|A| \leq |G|$.

Conversely, if $a \in A$ is fixed, we can define a map $\psi : G \to A$ via $\psi(\sigma) = \sigma \cdot a$. Again, this map is injective, so $|G| \leq |A|$, so we conclude that $|G| = |A|$. □

Example 4.22 (Dummit and Foote p. 117 Question 10). Let H and K be subgroups of the group G. For each $x \in G$ define the HK *double coset* of x in G to be the set

$$HxK = \{hxk \mid h \in H, k \in K\}.$$

(a) Prove that HxK is the union of the left cosets $x_1K, \ldots, x_nK$ where $\{x_1K, \ldots, x_nK\}$ is the orbit containing xK of H acting by left multiplication on the set of left cosets of K.

(b) Prove that HxK is a union of right cosets of H.

(c) Show that HxK and HyK are either the same set or are disjoint for all $x, y \in G$. Show that the set of HK double cosets partitions G.

(d) Prove that $|HxK| = |K| \cdot |H : H \cap xKx^{-1}|$.

(e) Prove that $|HxK| = |H| \cdot |K : K \cap x^{-1}Hx|$.

Solution.

(a) Suppose $hxk \in HxK$. Then,

$$hxK = h \cdot xK \in H \cdot xK \quad \text{and} \quad hxk \in hxK.$$

As such,

$$hxk \in \bigcup_{yK \in H \cdot xK} yK \quad \text{which implies} \quad HxK \subseteq \bigcup_{yK \in H \cdot xK} yK.$$

Conversely, let

$$g \in \bigcup_{yK \in H \cdot xK} yK.$$

Then, $g \in yK$ for some $yK \in H \cdot xK$. So, $yK = h \cdot xK$ for some $h \in H$. As such, $g = hxk$ for some $k \in K$. We have

$$\bigcup_{yK \in H \cdot xK} yK \subseteq HxK \quad \text{so we conclude that} \quad HxK = \bigcup_{yK \in H \cdot xK} yK.$$

(b) Proof is similar to **(a)**.

(c) Observe that every element is in some double coset, i.e. $x \in HxK$ for all $x \in G$. As such,

$$G = \bigcup_{x \in G} HxK.$$

Note that if $y \in HxK$, then $HyK \subseteq HxK$.

Next, suppose $x, y \in G$ such that $HxK \cap HyK = \emptyset$. Then, there exist $h_i \in H, k_i \in K$ such that $h_1xk_1 = h_2yk_2$. As such,

$$x = h_1^{-1}h_2yk_2k_1^{-1} \in HyK.$$

This implies $HxK \subseteq HyK$. Similarly, $HyK \subseteq HxK$. As such, the two double cosets are either disjoint or equal. It follows that the set of HK double cosets partitions G.

(d) We recall **(a)**. Also, we shall use $\text{stab}_H(xK)$ to denote the stabilizer of xK in H. It suffices to show that $\text{stab}_H(xK) = H \cap xKx^{-1}$.

We first prove the forward inclusion. Suppose $h \in \text{stab}_H(xK)$. Then, $hxK = h \cdot xK = xK$ and we have $x^{-1}hx \in K$. So, $h \in xKx^{-1}$, and we conclude that $h \in H \cap xKx^{-1}$.

To prove the reverse inclusion, suppose $h \in H \cap xKx^{-1}$. Then, $x^{-1}hx \in K$, so that $h \cdot xK = hxK = xK$. As such, $h \in \text{stab}_H(xK)$. It follows that $\text{stab}_H(xK) = H \cap xKx^{-1}$.

In **(a)**, we showed that

$$HxK = \bigcup_{yK \in H \cdot xK} yK.$$

In fact, this union is disjoint since the yK are distinct left cosets of K, each of order $|K|$. Hence,

$$|HxK| = |K| \cdot |H \cdot xK| = |K| \cdot [H : \text{stab}_H(xK)] = |K| \cdot \left[H : H \cap xKx^{-1}\right]$$

and the result follows.

(e) Proof is similar to **(d)**. □

Corollary 4.1. Let G be a finite group. Let p be the smallest prime dividing $|G|$. Then, any subgroup of G of index p is normal.

Proof. Suppose $H \leq G$ and $[G:H] = p$. Consider the left multiplication action of G on G/H. Let K be the kernel of

$$\text{the action homomorphism } G \to \text{Perm}\,(G/H) \quad \text{where} \quad g \mapsto (xH \mapsto gxH)\,.$$

By the first isomorphism theorem, G/K is isomorphic to a subgroup of $\text{Perm}\,(G/H) \cong S_p$. Since $|S_p| = p!$, then

$$[G:K] \mid p! \quad \text{by Lagrange's theorem.}$$

Since $K \subseteq H \subseteq G$, by the tower theorem (Theorem 3.4), we have

$$[H:K] = \frac{[G:K]}{[G:H]} \quad \text{divides} \quad \frac{p!}{p} = (p-1)!.$$

By Lagrange's theorem, $[H:K] \mid |G|$, so its prime divisors must be $\geq p$. This forces $[H:K] = 1$, so H exactly one coset of K, implying that $K = H \trianglelefteq G$. $\square$

Proposition 4.3. Let G be a group acting on a set A. For any $a \in A$, the map

$$G/G_a \to G \cdot a \quad \text{where} \quad gG_a \mapsto g \cdot a \quad \text{is a well-defined bijection.}$$

In particular, $|G \cdot a| = [G:G_a]$.

Proof. Suppose $g_1, g_2 \in G$ are such that $g_1 G_a = g_2 G_a$ in G/G_a. We need to show that $g_1 \cdot a = g_2 \cdot a$ in $G \cdot a$. To see why this holds, there exists $h \in G_a$ such that $g_1 h = g_2$ in G, so

$$g_2 \cdot a = g_1 h \cdot a = g_1 \cdot (h \cdot a) = g_1 \cdot a.$$

Hence, the map is well-defined. By definition of $G \cdot a$ as the G-orbit of a, the map is surjective. It now suffices to prove that the map is injective. Suppose for any $g_1, g_2 \in G$, we have $g_1 \cdot a = g_2 \cdot a$ in $G \cdot a$.

Then,

$$g_2^{-1} g_1 \cdot a = g_2^{-1} \cdot (g_1 \cdot a) = g_2^{-1} \cdot (g_2 a) = g_2^{-1} g_2 \cdot a = a.$$

Hence, $g_2^{-1} g_1 \in G_a$, which implies $g_1 G_a = g_2 g_2^{-1} g_1 G_a = g_2 G_a$ in G/G_a. We conclude that the map is injective. $\square$

Example 4.23. The number of conjugates of a subset S in G is

$$[G : N_G(S)] \quad \text{which is the index of the normalizer of } S \text{ in } G.$$

The number of conjugates of an element s in G is

$$[G : C_G(s)] \quad \text{which is the index of the centralizer of } s \text{ in } G.$$

Corollary 4.2 (orbit-stabilizer theorem)**.** Let G be a group acting on a finite set A. Let $\{a_i \in A\}$ be representatives of the distinct G-orbits in A. Then,

$$A = \bigsqcup_i G \cdot a_i \quad \text{is in bijection with} \quad \bigsqcup_i G/G_{a_i}.$$

Definition 4.8 (fixed point)**.** A fixed point of A under the action of G is an element $a \in A$ such that

$$\text{for any } g \in G \quad \text{we have} \quad g \cdot a = a \text{ in } A.$$

The subset of fixed points of A is denoted by

$$A^G = \{a \in A : \text{for any } g \in G, \text{ we have } ga = a\} \subseteq A.$$

Remark 4.1. The fixed points of an *interesting* action are usually also *interesting*.

Example 4.24. For the left multiplication action of a finite subgroup $H \leq G$ on the coset space G/H,

$$xH \in G/H \quad \text{is a fixed point under } H \quad \text{if and only if} \quad x \in N_G(H).$$

Example 4.25. For the conjugation action of G on itself,

$$a \in G \quad \text{is a fixed point under } G \quad \text{if and only if} \quad a \in Z(G).$$

Example 4.26. For the conjugation action of G on the subgroups of G,

$$H \text{ is a fixed point under } G \quad \text{if and only if} \quad H \trianglelefteq G.$$

We then discuss an important theorem, known as the class equation (Theorem 4.2). To obtain it, we use the fact that each element $g \in G$ belongs to exactly one conjugacy class. The class equation expresses the order of G by summing the sizes of these conjugacy classes.

We first discuss the elements in the center $Z(G)$. These form a conjugacy class of size 1 (since each element commutes with all elements of G, making its conjugacy class trivial). So, the contribution from $Z(G)$ to the order of G is $|Z(G)|$.

On the other hand, for each conjugacy class not contained in $Z(G)$, we select a representative g_i. The size of the conjugacy class of g_i is given by $[G : C_G(g_i)]$, the index of the centralizer $C_G(g_i)$ in G, because the elements conjugate to g_i are precisely those in G that can be obtained by conjugating g_i by elements of G. Thus, $[G : C_G(g_i)]$ measures the size of the conjugacy class of g_i.

Theorem 4.2 (the class equation)**.** Let G be a finite group. Let $g_1, \ldots, g_r$ be representatives of the distinct conjugacy classes of G not contained in $Z(G)$. Then,

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)].$$

Example 4.27 (Burnside's theorem for p-groups)**.** Let G be a finite p-group. We will formally introduce p-groups when talking about the Sylow theorems (Definition 4.9) but we briefly discuss its definition here. We say that a finite p-group is a group of order p^n, where p is prime and $n > 0$. Then, prove that

$$G \quad \text{has a non-trivial center.}$$

Will encounter this result again in MA5218 Representation Theory.

Solution. Note that the order of any conjugacy class of G must divide the order of G. To see why, we have

$$C_G(g_i) \le G \quad \text{so} \quad [C_G(g_i)] \mid |G| \text{ by Lagrange's theorem.}$$

So, our claim is established. As such, the conjugacy class H_i that is not in the center also has order some power of p^{k_i}, where $0 < k_i < n$, i.e. $|H_i| = [G : C_G(g_i)] = p^{k_i}$. By the class equation (Theorem 4.2), we have

$$|G| = p^n = |Z(G)| + \sum_{i=1}^{r} p^{k_i} \quad \text{which implies} \quad |Z(G)| = -p^n + \sum_{i=1}^{r} p^{k_i}.$$

So, $p \mid |Z(G)|$, which implies $|Z(G)| > 1$, i.e. the center is non-trivial since it contains more than 1 element. □

Theorem 4.3 (Cauchy's theorem)**.** Let G be a finite group. Let p be a prime dividing $|G|$. Then, there exists an element in G of order p.

After learning about Sylow p-subgroups (Definition 4.10) and Sylow's first theorem (Theorem 4.4), you would come to realise that Sylow's first theorem is a stronger statement compared to Cauchy's theorem. Briefly speaking, if we have a group $|G|$ of order $p^\alpha m$, where $\alpha \ge 1$ and p does not divide m, then there exists a subgroup of order p^α. In contrast, Cauchy's theorem only tells us that there exists a subgroup of order p (use Lagrange's theorem to deduce this statement from Theorem 4.3).

4.5 The Sylow Theorems and their Applications to Groups of Order ≤ 200

Definition 4.9 (p-group)**.** Let p be a prime. A p-group is a finite group of order p^α, where $\alpha \ge 1$.

Definition 4.10 (p-subgroup and Sylow p-subgroup)**.** Let G be a finite group.

(i) A p-subgroup of G is a subgroup of G which is a p-group

(ii) A Sylow p-subgroup of G is a p-subgroup of G of index prime to p, i.e. if

$$|G| = p^\alpha m \quad \text{where } \alpha \ge 1 \text{ and } p \text{ does not divide } m,$$

then a Sylow p-subgroup of G is a subgroup of order p^α.

$\mathrm{Syl}_p(G)$ denotes the set of Sylow p-subgroups of G, and $n_p(G)$ is the number of Sylow p-subgroups of G when G is clear from the context.

Theorem 4.4 (Sylow's theorems)**.** Let G be a finite group of order $p^\alpha m$, where p does not divide m and $a \ge 1$.

(1) Sylow p-subgroups of G exist, i.e. $\mathrm{Syl}_p(G) \ne \emptyset$.

(2) Any two Sylow p-subgroups of G are conjugate in G, i.e.

$$\text{for any } P, Q \in \mathrm{Syl}_p(G) \quad \text{there exists } g \in G \text{ such that } gPg^{-1} = Q$$

(3) $n_p(G) \mid m$ and $n_p(G) \equiv 1 \pmod p$

Sylow's theorems (Theorem 4.4) are very important to the extent that each of the indices **(1)**, **(2)**, and **(3)** are given the names Sylow's first theorem, Sylow's second theorem, and Sylow's third theorem respectively. Moreover, it is crucial to know how Sylow's theorems can be applied, compared to their proofs.

We then see how Sylow's theorems can be applied.

Corollary 4.3. For the same prime p, any two Sylow p-subgroups of a group G are isomorphic.

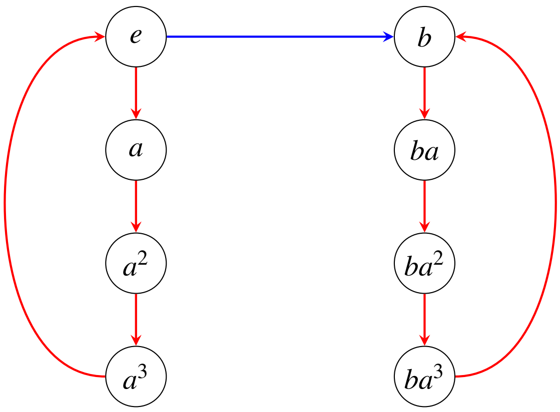
Proof. Direct consequence of Sylow's second theorem (Theorem 4.4) and the fact that if $K \leq G$ and $g \in G$, then $K \cong gKg^{-1}$. The latter simply means that conjugate elements and conjugate subgroups have the same order. □

I highly recommend the reader to read Nathan Carter's 'Visual Group Theory' for great explanations of the applications of Sylow's theorems. We first classify groups of order 8 using Sylow's theorems (Theorem 4.4).

Example 4.28 (groups of order 8)**.** By Sylow's first theorem, there exists at least one subgroup of order 4 (since $8 = 2^3$ and $2^{2=4}$, where $2 \leq 3$). Note that such subgroups must be isomorphic to the Klein four-group V_4 or C_4 (isomorphic to $\mathbb{Z}/4\mathbb{Z}$. If all the subgroups were $\cong V_4$, then the group would have no elements of order 4 (recall the identity $a^2 = b^2 = (ab)^2 = e$ in V_4), and therefore only elements of order 2.

If the subgroup only has elements of order 2, then it must be Abelian. This is easy to see by the definition of V_4. Since C_4 is not Abelian, then any non-Abelian group of order 8 has a copy of C_4 in it. For this copy of C_4, say it is generated by a. As such, we can deal with the subgroup $\langle a \rangle$ and its one left coset, which together form all eight elements of the group. Call the coset $b\langle a \rangle$ for some $b \notin \langle a \rangle$. We wish to determine the possibilities for how a and b relate, and so determine the structures possible in non-Abelian groups of order 8. At this juncture, we only know that the order of b is either 2 or 4[†].

- **Case 1:** Suppose b has order 2. Consider the following diagram. We wish to determine where the arrows involving b (in blue) send the element a to. Any such decision can be expressed as an equation relating a and b.

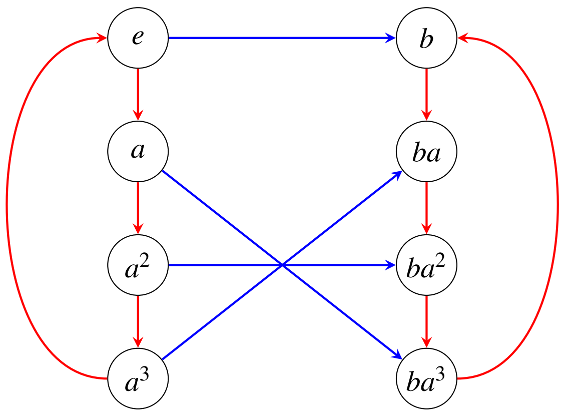


First, note that the arrow for b (in blue) cannot send a to the top row of the diagram because there are already b arrows touching both such elements. Similarly, because $b \notin \langle a \rangle$, the b arrow cannot send a within the left column.

[†]A possible misconception is that people might think it is not permissible for b to be of order 4. In the first place, an order of 2 or 4 is valid by Lagrange's theorem (Theorem 3.1) since the order of any element must divide 8. However, as $b \notin \langle a \rangle$, then b cannot have order 1 or 4 coming from a. Moreover, b is *outside* the cyclic group C_4 so it is perfectly fine if b generates a different cyclic subgroup of order 4.

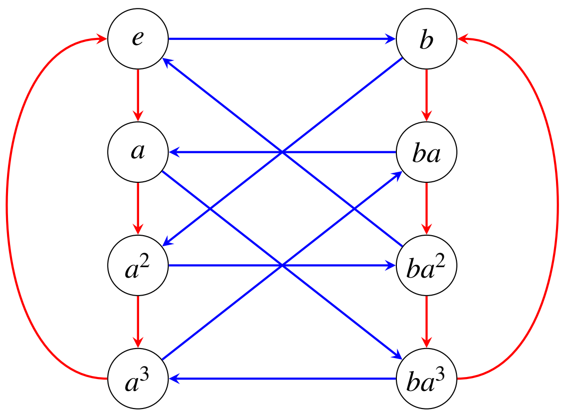
Next, if the b arrow were to send a to ba, then we would have $ab = ba$, but this means that the group is Abelian. As we have already listed the Abelian groups, we are now only seeking the non-Abelian ones. If the b arrow were to connect a to ba^2, we would have $ab = ba^2$. This means that the paths ab and ba^2 should lead to the same output regardless of where in the diagram we start. Say we start from a. This requires drawing a b arrow from a^2 to b. However, b already has an oncoming b arrow from e, so we cannot have $ab = ba^2$.

The only remaining choice is to connect a to ba^3, and all other b connections are then determined by the equation $ab = ba^3$. As such, we obtain the Cayley diagram of the dihedral group D_8 as follows:



We can determine the relationship between a and b by asking where the b cycle continues from b. By process of elimination, we shall determine which element is $= b^2$. Note that b^2 is not any of the elements in the right column because $b \notin \langle a \rangle$ so $b^2 \notin \langle a \rangle$. Moreover, $b^2 \neq e$, otherwise it would imply $|b|$ and we already considered this. Next, $b^2 \neq a$, otherwise $b^8 = a^4 = e$ so b is of order 8. The group is cyclic, hence Abelian, for which we have already considered. Lastly, if $b^2 = a^3$, then $b^8 = a^{12} = \left(a^4\right)^3 = e$ so b is of order 8, which is a contradiction again.

We are only left with the relation $b^2 = a^2$. We obtain the following Cayley diagram of Q_8.



- **Case 2:** Then, suppose b has order 4. We leave this as an exercise.

One can conclude that the two non-Abelian groups of order 8 are D_8 and Q_8. There are three Abelian groups $C_2 \times C_2 \times C_2$, $C_4 \times C_2$, and C_8 — in fact, one can deduce this using the fundamental theorem of finitely generated Abelian groups too (Theorem 5.1, so there are 5 groups of order 8 up to isomorphism.

Most of the applications of Sylow's Theorem use it to prove that a group of a particular order is not simple.

Definition 4.11 (simple group). A simple group is a group G with $|G| > 1$ such that the only normal subgroups of G are 1 and G.

For Examples 4.29 to 4.35 [†], let p, q, r denote distinct primes and n be a positive integer. We shall discuss a broad classification of groups of order ≤ 200.

Order of group	Simple
p	Yes (Example 4.29)
p^n with $n > 1$	No (Example 4.30)
mp^n	No (Example 4.31)
p^2q	No (Example 4.32)
pqr	No (Example 4.33)
$2^n \cdot 3$ with $n > 1$	No (Example 4.34)
$3^n \cdot 4$ with $n > 1$	No (Example 4.35)

Table 17: Simplicity of groups of certain orders

For groups of order ≤ 200, Table 17 takes care of all orders except the following:

$$40, 56, 60, 66, 72, 80, 84, 90, 112, 120, 126, 132, 140, 144, 150, 160, 168, 176, 180, 196, 198, 200$$

We will discuss some of these in due course.

Order of group	Simple	Order of group	Simple
40	No (Example 4.36)	132	No
56	No (Example 4.37)	140	No
60	Depends (Example 4.38)	144	No
66	No	150	No
72	No	160	No
80	No	168	Depends
84	No	176	No
90	No	180	No
112	No	196	No
120	No	198	No
126	No	200	No

Table 18: Simplicity of groups of certain orders

Example 4.29 (groups of order p). This is merely an application of Lagrange's theorem (Theorem 3.1). Suppose p is a prime and $|G|\, p$. Let $H \leq G$. Then, by Lagrange's theorem, either $|H| = 1$ or $|H| = p$. In either case, H is a trivial subgroup of G (Example 1.4), which implies that G is simple and there is no non-trivial normal subgroup of G.

[†]These are taken from Aryaman Maithani's GitHub's post. It offers a concise compilation of the broad classifications of groups of certain order, but we will explain them here in greater detail.

We conclude that any group of prime order is simple.

Example 4.30 (groups of order p^n with $n > 1$). Let G be be a group of order p^n, where $n \geq 2$ and p is prime. We will prove that G is not simple. Recall Example 4.27 on Burnside's theorem for p-groups, where we used the class equation (Theorem 4.2) to deduce that if a finite p-group is of order p^n, then $Z(G) \neq \{e\}$ (i.e. the center is non-trivial).

We shall consider two cases — namely if $Z(G) \neq G$ and $Z(G) = G$. For the first case, we note that $Z(G)$ is a proper non-trivial normal subgroup of G so G is not simple (Definition 4.11).

For the second case, suppose $Z(G) = G$. This means that G is Abelian (in fact, this is an 'if and only if' statement) since every element in the group commutes with every other element. Let $1 \neq x \in G$. Then, $|x| = p^m$ for some $1 \leq m \leq n$. Choose $y = x^{p^m}$. Then $|y| = p$. Let $H = \langle y \rangle$, which implies that H is a proper non-trivial subgroup of G which is normal as G is Abelian.

Example 4.31 (groups of order mp^n). Let G be a group of order mp^n, where p is prime and $1 < m < p$. We will prove that G is not simple. By Sylow's third theorem (Theorem 4.4), $n_p \mid m$ and $n_p \equiv 1 \pmod p$. This means that there exists $\lambda \in \mathbb{Z}$ such that $n_p = \lambda p + 1$. Since $(\lambda p + 1) \mid m$ and $m < p$, then $\lambda = 0$. As such, $n_p = 1$, so there is 1 Sylow p-subgroup of G. By Sylow's second theorem (Theorem 4.4), this subgroup is normal since any two Sylow p-subgroups of G are conjugate in G.

Example 4.32 (groups of order p^2q). Let p and q be distinct primes. If $|G| = p^2q$, then we claim that G is not simple.

First, consider the case where $p > q$. By Sylow's third theorem (Theorem 4.4), $n_p \mid q$ and $n_p \equiv 1 \pmod p$. The latter implies that there exists $\lambda \in \mathbb{Z}$ such that $n_p = \lambda p + 1$. As $(\lambda p + 1) \mid q$ and $p > q$, then $\lambda = 0$, which implies $n_p = 1$, so by Sylow's second theorem, G is not simple.

Next, consider the case where $p < q$ (slightly longer argument). By Sylow's third theorem (Theorem 4.4), $n_q \in \{1, p, p^2\}$. If $n_q = 1$, then G is not simple. If $n_q = p$, then as $n_q \equiv 1 \pmod q$, then $q \mid (p-1)$ which is impossible since $p < q$.

As such, we consider the case where $n_q = p^2$. This means that there are p^2 Sylow q-subgroups of G. Since each of these subgroups is of order q, which is prime, the intersection of any two Sylow q-subgroups is trivial. To see why, let these subgroups be P and Q. By defining $H = P \cap Q$, note that $H \leq P$ and $H \leq Q$. By Lagrange's theorem (Theorem 3.1), we must have $|H| \mid q$. As such, either $|H| = 1$ or $|H| = q$. However, if $|H| = q$, then both Sylow q-subgroups are equal, contradicting the fact that they are distinct.

At this juncture, recall that we are still working with the case $n_q = p^2$ but we established that the intersection of any Sylow q-subgroups is trivial. Since each Sylow q-subgroup contains q elements (including the identity), then their union contains $p^2(q-1)$ non-identity elements. Since $|G| = p^2q$, then there are $p^2q - p^2(q-1) = p^2$ elements not contained in the union of the Sylow q-subgroups. We know that $n_p \geq 1$ and none of the $p^2(q-1)$ elements can be part of a Sylow p-subgroup. Thus, the remaining p^2 elements must form a Sylow p-subgroup, which implies $n_p = 1$. Again, by Sylow's second theorem (Theorem 4.4), G is not simple.

Example 4.33 (groups of order pqr). Let p, q, r be distinct primes. Without loss of generality, assume that $p < q < r$. Suppose G is a group such that $|G| = pqr$. By Sylow's third and second theorems (Theorem 4.4), if

$n_p = 1$ or $n_q = 1$ or $n_r = 1$, then G is not simple.

Suppose on the contrary that $n_r > 1$. As $n_r \mid pq$ and $p < q < r$, then $n_r = pq$ (also because $n_r > 1$). That is, there are pq Sylow r-subgroups of G. Similar to Example 4.32, as each such Sylow r-subgroup is of order r, which is prime, then the intersection of any two Sylow r-subgroups is trivial. Hence, the number of elements of order r is $pq(r-1)$. Now, recall that $n_q > 1$ and by Sylow's third theorem (Theorem 4.4), $n_q \mid pr$. Hence, $n_q \in \{p, r, pr\}$. Since $n_q \equiv 1 \pmod{q}$, then $n_q \neq p$. This implies $n_q \geq r$, i.e. the number of elements of order q is $\geq r(q-1)$. Lastly, as $n_p \equiv 1 \pmod{p}$ and $n_p \mid qr$, then $n_p \in \{q, r, qr\}$. Since $n_p \geq q$, then the number of elements of order p is $\geq q(p-1)$.

Combining the red parts and noting that they are counting distinct non-identity elements, we have

$$|G| \geq pq(r-1) + r(q-1) + q(p-1) + 1$$

where the 1 on the rightmost side denotes the identity element. Hence,

$$pqr = |G| \geq pqr + qr - q - r + 1 = pqr + (q-1)(r-1) > pqr$$

which is a contradiction as $|G| = pqr$!

Example 4.34 (groups of order $2^n \cdot 3$ with $n > 1$)**.** We shall prove that such groups G are not simple. By Sylow's third theorem (Theorem 4.4), $n_2 \mid 3$ and $n_2 \equiv 1 \pmod{2}$, so either $n_2 = 1$ or $n_2 = 3$. If $n_2 = 1$, then by a similar argument as the previous examples using Sylow's second and third theorems (Theorem 4.4), G is not simple.

If $n_2 = 3$, then let $\mathrm{Syl}_2(G)$ denote the set of Sylow 2-subgroup of G. Naturally, G acts on $\mathrm{Syl}_2(G) = \{P_1, P_2, P_3\}$ via conjugation. A natural trick for examples on Sylow theory is to consider a natural homomorphism $\varphi : G \to S_3$ (codomain will always be a symmetric group S_n, where n is the number of Sylow p-subgroups). By Sylow's second theorem (Theorem 4.4), any two Sylow 2-subgroups are conjugates in G, i.e.

$$\text{there exists } g \in G \text{ such that } gP_ig^{-1} = P_j \quad \text{for distinct } i, j \in \{1, 2, 3\}.$$

Note that the group action is transitive so $\ker \varphi \neq G$. Suppose on the contrary that $\ker \varphi = \{e\}$. Then, φ is injective (simple fact from MA2001) which implies $\varphi(G)$ has $2^n \cdot 3 \geq 12$ elements (since $n \geq 2$). Since $\varphi(G) \leq S_3$ and $|S_3| = 6$, then we have a contradiction. Hence, $\ker \varphi$ is a proper non-trivial subgroup of G. As $\ker \varphi \trianglelefteq G$ (recall Example 2.41), then we conclude that G is not simple.

Example 4.35 (groups of order $3^n \cdot 4$ with $n > 1$)**.** The idea here is similar to Example 4.34. By Sylow's third theorem (Theorem 4.4), we have $n_3 \mid 4$ and $n_3 \equiv 1 \pmod{3}$, so either $n_3 = 1$ or $n_3 = 4$. If $n_3 = 1$, then G is not simple.

On the other hand, if $n_3 = 4$, then let $\mathrm{Syl}_3(G) = \{P_1, \ldots, P_4\}$ denote the Sylow 3-subgroups of G. Let G act on $\mathrm{Syl}_3(G)$ via conjugation, which is a transitive action so $\ker \varphi \neq G$. Consider the natural corresponding homomorphism $\varphi : G \to S_4$. Suppose on the contrary that $\ker \varphi = \{e\}$. Then, φ is injective which implies $|\varphi(G)| = |G| \geq 3^2 \cdot 4 = 36$. However, $|S_4| = 24$ which is a contradiction as there does not exist an injective map from a group of order ≥ 36 into S_4.

We now discuss the simplicity of some groups of specific orders in Table 18.

Example 4.36 (groups of order 40)**.** Let G be a group of order 40. We will prove that G is not simple Since $40 = 2^3 \cdot 5$, by Sylow's third theorem (Theorem 4.4), we have $n_5 \mid 8$ and $n_5 \equiv 1 \pmod{5}$. By considering the divisors of 8, it follows that $n_5 = 1$ so by Sylow's second theorem (Theorem 4.4), G is not simple.

Example 4.37 (groups of order 56)**.** Let G be a group of order 56. We will prove that G is not simple. Note that $56 = 2^3 \cdot 7$. By Sylow's third theorem (Theorem 4.4), we have $n_7 \mid 8$ and $n_7 \equiv 1 \pmod 7$, so $n_7 = 1$ or $n_7 = 8$. If $n_7 = 1$, then by Sylow's second theorem (Theorem 4.4), G is not simple.

We then consider the case when $n_7 = 8$. Since each Sylow 7-subgroup is of order 7, which is prime, then the intersection of any two Sylow 7-subgroups is trivial. Thus, there are $8 \cdot (7-1) = 48$ elements of order 7. Since $|G| = 56$, then there are $56 - 48 = 8$ elements not contained in any Sylow 7-subgroup. By Sylow's first theorem (Theorem 4.4), $n_2 \geq 1$. However, no non-identity element can belong to a Sylow 2-subgroup or a Sylow 7-subgroup. As such, the remaining 8 elements belong to a Sylow 2-subgroup, so $n_2 = 1$, and we are done.

It is interesting to note that there exist some groups of order 60 which are simple (Example 4.38).

Example 4.38 (groups of order 60)**.** Let G be a group of order 60. Then, it is possible for G to not be a simple group. Take for example $G = \mathbb{Z}/60\mathbb{Z}$ and we can easily verify that $H = \{0, 30\} \trianglelefteq G$ because G is Abelian.

Having said that, let $G = A_5$, i.e. the alternating group on 5 elements. It is known that A_n is simple for $n \geq 5$, so G is simple and is of order $5!/2 = 60$. Interestingly, one can show that A_5 is the only simple group of order 60 up to isomorphism.

Chapter 5
More Abstract Group Theory

5.1
Solvable Groups

5.2
Products

Theorem 5.1 (fundamental theorem of finitely generated Abelian groups)**.** Let G be a finitely generated Abelian group. Then,

$$G \cong Z_{n_1} \times Z_{n_2} \times \dots Z_{n_s}$$

for some $r, n_1, \dots, n_s \in \mathbb{Z}$ satisfying the following conditions:

(i) $r \geq 0$ and $n_j \geq 2$ for all j;

(ii) $n_{i+1} \mid n_i$ for all $1 \leq i \leq s-1$

Moreover, the representation of G as the mentioned product is unique, i.e. if

$$G \cong Z_{m_1} \times \dots Z_{m_u}$$

for some $t, m_1, \dots, m_u \in \mathbb{Z}$ satisfying **(i)** and **(ii)**, then $t = r$, $u = s$ and $m_i = n_i$ for all i.

5.3
Free Groups