Contents

1 Introduction to Groups

1.1 Groups

A group is a higher abstraction for a structure which supports a certain arithmetic operation. To fully specify a group, we need to abstract the notion of an "arithmetic operation".

Definition 1.1.1 ▸ Binary Operation

A **binary operation** $\star$ on a set G is a function $f\colon G \times G \to G$.

Conventionally, the notations $a \star b$ and $\star((a, b))$ are equivalent. For the sake of simplicity, we will not use the latter.

Recall that there are some commonly used properties of operations. We shall abstract those as well. First, we pay attention to whether the order of execution matters in a sequence of repeated applications of an operation.

Definition 1.1.2 ▸ Associativity

A binary operation $\star$ on G is **associative** if for all $a, b, c \in G$, we have

$$a \star (b \star c) = (a \star b) \star c.$$

Similarly, we will next focus on whether the order of operands matters when an operation is applied.

Definition 1.1.3 ▸ Commutativity

Let G be a set with a binary operation $\star$, then $a, b \in G$ **commute** if $a \star b = b \star a$. We say that $\star$ or G is **commutative** if all elements in G commute pair-wisely with respect to $\star$.

Note that both addition and multiplication are associative and commutative over $\mathbb{N}$, but subtraction is not. In fact, subtraction is not even a binary operation over $\mathbb{N}$ because $\mathbb{N}$ is not closed under subtraction.

A more complex example is cross product in $\mathbb{R}^n$, which is neither associative nor commutative. Recall that we used the word "closed" when arguing that subtraction is not a binary operation over $\mathbb{N}$. We shall further formalise this notion.

Definition 1.1.4 ▸ Closure

Let $\star$ be a binary operation on G, then $H \subseteq G$ is **closed under $\star$** if for all $a, b \in H$, we have $a \star b \in H$.

In particular, this means that $\star$ on G is still a binary operation on any $H \subseteq G$ which is closed under $\star$. Intuitively, both associativity and commutativity can be inherited by these subsets.

Proposition 1.1.5 ▸ Presevation of Associativity and Commutativity

Let $\star$ be a binary operation on G and $H \subseteq G$ be closed under $\star$, then

- *if $\star$ is associative on G, then $\star$ is associative on H;*
- *if $\star$ is commutative on G, then $\star$ is commutative on H.*

Proof. Left as exercise to the reader. □

Next, we will introduce the fundamental axioms which define the abstract mathematical notion of groups, as well as some simple results derived from these axioms.

Definition 1.1.6 ▸ Group

A **group** is a pair $(G, \star)$ where G is a set and $\star$ is a binary operation on G such that

- $\star$ is associative;
- there exists some $e \in G$ with $a \star e = e \star a = a$ for all $a \in G$, where e is known as an **identity** of G;
- for all $a \in G$, there exists some $a^{-1} \in G$ such that $a \star a^{-1} = a^{-1} \star a = e$, where a^{-1} is known as the **inverse** of a.

In Definition 1.1.6, the map $\star$ is often called *multiplication* by convention. Moreover, we can define a map $^{-1}\colon G \to G$ known as the *inversion* map as an alternative way to construct the inverses.

Therefore, a group can be defined as a set in which:

1. any two elements can be multiplied,
2. every element has an inverse in the set itself, and
3. there exists an identity element which equals the product of any element multiplied by its inverse and multiplied by which any element equals itself.

The very first thing to take note here is that the order of multiplication matters in groups! In other words, $a \star b \neq b \star a$ in general.

Definition 1.1.7 ▸ Abelian Group

A group G is called an **Abelian** or **commutative** group if it is commutative.

Another important thing to remember here is that, although we call the map $\star$ "multiplication" conventionally, it does not have to be referring to the multiplication between real numbers or vectors or anything that we commonly take to be able to be multiplied together in elementary mathematics.

In fact, we will see that by taking $\mathbb{Z}$ as the set and addition $+$ as the multiplication map, we get a group that satisfies Definition 1.1.6 perfectly! Furthermore, this group $(\mathbb{Z}, +)$, known as the *additive group* of $\mathbb{Z}$, is an Abelian group. The same holds for $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$.

Consider $(\mathbb{Q} - \{0\}, +)$, which is not a group due to the missing identity. However, we can turn it into a group, specifically into a *multiplicative group*, by changing the operation to $\times$. In fact, $(\mathbb{Q} - \{0\}, \times)$ is also Abelian. The same holds for $(\mathbb{R} - \{0\}, \times)$ and $(\mathbb{C} - \{0\}, \times)$.

> *Remark.* Writing $\frac{b}{a}$ is not a good notation in the context of this course because it could mean either $a^{-1} \star b$ or $b \star a^{-1}$, which are completely different for non-Abelian groups.

Note that further $(\mathbb{Z} - \{0\}, \times)$ is not a group because all elements except 1 do not have inverses. Therefore, we define $\mathbb{Z}^\times := \{-1, 1\}$ which under $\times$ is a multiplicative group.

A group can be finite or infinite. To define those we need to define a measurement for the "size" of a group.

Definition 1.1.8 ▸ Order of a Group

Let $(G, \star)$ be a group, then $|G|$ is known as the **order** of the group. G is said to be a **finite** group if G is finite, and **infinite** group otherwise.

Let us consider some extreme cases here. Note that a group cannot be empty, so the most extreme case is a singleton group.

Proposition 1.1.9 ▸ Singleton Sets Are Abelian Groups

Every singleton set $\{e\}$ is an Abelian group under any binary operation. In particular, the only binary operation under which the set is a group is $(e, e) \mapsto e$.

Proof. Trivial. □

Next is a more complex example based on the *roots of unity*.

Definition 1.1.10 ▸ Root of Unity

An **n-th root of unity** is a complex number $z \in \mathbb{C}$ such that $z^n = 1$.

We can collect all such roots and realise that they form a group.

Proposition 1.1.11 ▸ n-th Root of Unity Group

Let $\mathbb{Z}_n := \{0, 2, \cdots, n-1\}$ *and define*

$$U_n := \left\{ \exp\left(\frac{2k\pi\mathrm{i}}{n}\right) : k \in \mathbb{Z}_n \right\},$$

then $(U_n, \cdot)$ *is a group.*

Proof. We first prove that U_n is closed under multiplication. Take any $z_1, z_2 \in U_n$, then there exist $k_1, k_2 \in \mathbb{Z}_n$ such that $z_1 = \exp\left(\frac{2k_1\pi\mathrm{i}}{n}\right)$ and $z_2 = \exp\left(\frac{2k_2\pi\mathrm{i}}{n}\right)$. Notice that there exists some $q \in \mathbb{N}$ and $r \in \mathbb{Z}_n$ such that $k_1 + k_2 = nq + r$, so

$$\begin{aligned} z_1 \cdot z_2 &= \exp\left(\frac{2(k_1+k_2)\pi\mathrm{i}}{n}\right) \\ &= \exp\left(\frac{2(nq+r)\pi\mathrm{i}}{n}\right) \\ &= \exp\left(2q\pi\mathrm{i} + \frac{2r\pi\mathrm{i}}{n}\right) \\ &= \exp(2q\pi\mathrm{i}) \exp\left(\frac{2r\pi\mathrm{i}}{n}\right). \end{aligned}$$

Observe that $\exp(2q\pi\mathrm{i}) = 1$, so $z_1 \cdot z_2 = \exp\left(\frac{2r\pi\mathrm{i}}{n}\right) \in U_n$. It is obvious that multiplication is associative over $\mathbb{C}$ and $1 \in U_n$ is an identity, so it suffices to prove the existence of inverses. Take any $z \in U_n$, then there exists some $k \in \mathbb{Z}_n$ such that $z = \exp\left(\frac{2k\pi\mathrm{i}}{n}\right)$. Consider

$$\begin{aligned} z' &:= \exp\left(\frac{-2k\pi\mathrm{i}}{n}\right) \\ &= \exp(2\pi\mathrm{i}) \exp\left(\frac{-2k\pi\mathrm{i}}{n}\right) \\ &= \exp\left(\frac{2(n-k)\pi\mathrm{i}}{n}\right). \end{aligned}$$

Note that $n - k \in \mathbb{Z}_n$ and $z' \cdot z = z \cdot z' = 1$, so $z' = z^{-1}$. Therefore, $(U_n, \cdot)$ is a group. □

We shall prove some trivial results directly from the definition of groups.

Theorem 1.1.12 ▸ Uniqueness of Identity and Inverse in Groups

Let G be a group under $\star$ with identity e, then e is unique and for all $a \in G$, a^{-1} is unique. Furthermore,

- $\left(a^{-1}\right)^{-1} = a$ *for all* $a \in G$;
- $(a \star b)^{-1} = b^{-1} \star a^{-1}$ *for all* $a, b \in G$.

Proof. Suppose there exists $f \in G$ such that $a \star f = f \star a = a$ for all $a \in G$. Since $e \in G$, we have $e \star f = e$, but e is the identity and $f \in G$, so $f \star e = f$. Therefore,

$$f = f \star e = e \star f = e,$$

which means that e is unique. Suppose that there is some $a \in G$ such that there is some $b \in G$ with $a \star b = b \star a = e$, then

$$\begin{aligned} b &= b \star e \\ &= b \star \left(a \star a^{-1}\right) \\ &= (b \star a) \star a^{-1} \\ &= e \star a^{-1} \\ &= a^{-1}. \end{aligned}$$

Therefore, a^{-1} is unique for all $a \in G$. □

Theorem 1.1.12 shows that if the map $\star$ is such that an identity exists in the set G, then it is unique, which also uniquely determines the inversion map as there cannot be different $a, b \in G$ such that $ac = bc = e$ for some $c \in G$. In other words, **a group is uniquely determined by the multiplication map** given a set G.

Theorem 1.1.13 ▸ Generalised Associative Law

Let $(G, \star)$ be a group, then $a_1 \star a_2 \star \cdots \star a_n$ is well-defined for any $a_1, a_2, \cdots, a_n \in G$ and all $n \in \mathbb{N}^+$ and $n \geq 3$.

Proof. We shall proceed with induction on n. The case where $n = 3$ is immediate from Definition 1.1.6. Suppose that there exists some $k \in \mathbb{N}^+$ with $k \geq 3$ such that

$$a_1 \star a_2 \star \cdots \star a_k$$

is well-defined for any $a_1, a_2, \cdots, a_k \in G$. Take any $a_1, a_2, \cdots, a_{k+1} \in G$ and write

$$a_1 \star a_2 \star \cdots \star a_k = K \in G,$$

then clearly $K \star a_{k+1} \in G$ and so $a_1 \star a_2 \star \cdots \star a_{k+1}$ is well-defined. □

The above results justify some short-hand notations in a group G.

- We denote the identity of any group by 1.
- If the binary operation is clear, we can omit it by writing $a \star b = a \cdot b = ab$.
- For all $a \in G$ and any $n \in \mathbb{Z}$,

$$a^n = \begin{cases} a \cdot a \cdot \cdots \cdot a & \text{if n > 0} \\ 1 & \text{if n = 0} \\ a^{-1} \cdot a^{-1} \cdot \cdots \cdot a^{-1} & \text{if n < 0} \end{cases}$$

Note that the last notation here can be confusing when our group is an additive group, so we may consider the following alternative instead:

$$n \cdot a = \begin{cases} a + a + \cdots + a & \text{if n > 0} \\ 0 & \text{if n = 0} \\ a^{-1} + a^{-1} + \cdots + a^{-1} & \text{if n < 0} \end{cases}$$

Theorem 1.1.14 ▸ Left and Right Cancellation Laws

Let G be a group, then for any $a, b, u, v \in G$,

- *if $au = av$, then $u = v$;*
- *if $ub = vb$, then $u = v$.*

Proof. Suppose that $au = av$, then

$$u = 1 \cdot u = \left(a^{-1}a\right) u = a^{-1} \left(au\right) = a^{-1} \left(av\right) = \left(a^{-1}a\right) v = 1 \cdot v = v.$$

The other case is similar. □

A direct consequence of the cancellation laws is the following:

Corollary 1.1.15 ▸ Existence and Uniqueness of Solutions in Groups

Let G be a group, then for any $a, b, x, y \in G$, the equations $ax = b$ and $ya = b$ have unique solutions.

Proof. The uniqueness is obvious from Theorem 1.1.14, so it suffices to prove the existence. Take $x = a^{-1}b$, the obviously

$$ax = a\left(a^{-1}b\right) = \left(aa^{-1}\right)b = 1 \cdot b = b.$$

Therefore, $x = a^{-1}b$ is a solution to the equation $ax = b$. The other case is similar. □

A further consequence leads to the following way to identify the identity and inverses in a group:

Corollary 1.1.16 ▸ Characterisation of Identity and Inverses

Let G be a group. For any $a, b \in G$, if $ab = 1$ or $ba = 1$, then $b = a^{-1}$ and if $ab = a$ or $ba = a$, then $b = 1$.

Proof. Suppose that $ab = 1$, then by Corollary 1.1.15 we have $b = a^{-1} \cdot 1 = a^{-1}$. Similarly, suppose that $ab = a$, then we have $b = a^{-1}a = 1$. The other cases are similar. □

Lastly, note that we can take Cartesian product over groups.

Definition 1.1.17 ▸ Direct Product

Let $(A, \star)$ and $(B, \diamond)$ be groups. The **direct product** $A \times B$ is defined by the set

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

where

$$(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2).$$

One may check that for any groups A and B, the direct product $A \times B$ is always a group with identity $(1_A, 1_B)$ and inversion map $(a, b) \mapsto (a^{-1}, b^{-1})$.

We will discuss the structure of matrix groups. However, as matrices are closely related to vector spaces and vector spaces are closely related to fields, it is helpful to first define what a field is.

Definition 1.1.18 ▸ Field

A **field** is a set $\mathbb{F}$ together with two binary operations $+$ and $\cdot$ such that

- $(\mathbb{F}, +)$ is an Abelian group with identity 0,
- $(\mathbb{F} - \{0\}, \cdot)$ is an Abelian group with identity 1, and

- $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all $a, b, c \in \mathbb{F}$.

Remark. We use $\mathbb{F}^\times$ to denote the multiplication group $(\mathbb{F} - \{0\}, \cdot)$.

The next proposition is an attempt in constructing a field of a fixed cardinality.

Proposition 1.1.19 ▸ Construction of a Finite Field

Let p be a prime number and $\sim$ be the equivalence relation on $\mathbb{Z}$ such that $a \sim b$ if and only if $a \equiv b \mod p$. Define $\mathbb{F}_p := \mathbb{Z}/\sim$ and

$$\begin{aligned} [x]_\sim + [y]_\sim &= [x + y]_\sim, \\ [x]_\sim \cdot [y]_\sim &= [x \cdot y]_\sim \end{aligned}$$

for all $[x]_\sim, [y]_\sim \in \mathbb{F}_p$, then $(\mathbb{F}_p, +, \cdot)$ is a field with $|\mathbb{F}_p| = p$.

Proof. Let $X := \{0, 1, \cdots, p - 1\}$ and define $f : X \to \mathbb{F}_p$ by $f(x) = [x]_\sim$. We claim that f is bijective. Suppose that $f(x) = f(y)$ for some $x, y \in X$, then $[x]_\sim = [y]_\sim$, which means $x \equiv y \mod p$. Without loss of generality, assume that $x \leq y$, then since $0 \leq y - x \leq p - 1$ we must have $y - x = 0$, so $x = y$. Therefore, f is injective. Take any $[x]_\sim \in \mathbb{F}_p$, then there exists some $b \in \mathbb{Z}$ and $r \in X$ such that $x = bp + r$, and so $x \equiv r \mod p$. This means that $\{x\}_\sim = [r]_\sim = f(r)$. Therefore, f is surjective and so is a bijection. Therefore, $|\mathbb{F}_p| = |X| = p$. □

Now we can fix some arbitrary field $\mathbb{F}$ and consider some matrices.

Definition 1.1.20 ▸ General Linear Group

Let $\mathbb{F}$ be a field, then for each $n \in \mathbb{Z}^+$, the **general linear group** of degree n on $\mathbb{F}$ is defined as

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

with respect to matrix multiplication.

Remark. In other words, the matrix group on $\mathbb{F}$ is the set of all non-singular $n \times n$ matrices on $\mathbb{F}$.

The reader might find it an interesting exercise to show that $\mathrm{GL}_n(\mathbb{F})$ is indeed a group. In particular, $\mathrm{GL}_1(\mathbb{F}) = \mathbb{F}^\times$.

Note that given a set of elements, we can consider all possible products between the elements. Based on these products, we can “generate” a group.

Definition 1.1.21 ▸ Generators

Let G be a group. A set of **generators** of G is a set $S \subseteq G$ such that every element of G can be written as a finite product of elements of S and their inverses.

We say that G is *generated* by S or S *generates* G, which is denoted by $G = \langle S \rangle$. We introduce some basic examples and conventions.

First, every group is generated by itself. In particular, every singleton group is generated by $\{1\}$ and $\varnothing$ (by convention). It is also clear that the addition group $(\mathbb{Z}, +)$ is generated by $\{1\}$ and that D_{2n} is generated by $\{r, s\}$. However, $(\mathbb{R}, +)$ is generated by $\mathbb{R}_{\geq 0}$ and not $\mathbb{Q}$ because irrationals cannot be written as a finite sum of rationals and their inverses. By Theorem 1.2.11, we also know that every symmetric group is generated by all of its cycles.

We also need to define how the elements in the generators should multiply with each other to properly "generate" the group. To do this, we make use of relations.

Definition 1.1.22 ▸ Relation in a Group

Let G be a group with generators S. A **relation** in G is a relation R on $S \cup \{1\}$.

Remark. Conventionally, it is useful to think of a relation in a group G as an equation to relate its generators to 1.

Roughly speaking, relations define how the generators can be combined together to derive all the other elements in a group. Therefore, we can fully specify a group using generators and relations.

Definition 1.1.23 ▸ Presentation

A **presentation** of a group $G = \langle S \mid R \rangle$ is a set of generators S and a set of relations R on S such that any other relation on S can be deduced from R.

1.2 Permutations

Next, we examine a more complicated example of groups known as *symmetric groups*. First, we shall prove a preliminary theorem.

Proposition 1.2.1 ▸ Bijectivity and Invertibility Are Equivalent

Let X, Y be any sets and let $\sigma \in Y^X$ be a map, then σ is invertible if and only if it is bijective.

Proof. Suppose that σ is invertible. Let $x_1, x_2 \in X$ be such that $\sigma(x_1) = \sigma(x_2)$, then

$$x_1 = \sigma^{-1}(\sigma(x_1)) = \sigma^{-1}(\sigma(x_2)) = x_2,$$

so σ is injective. Take some $y \in Y$, then there exists $\sigma^{-1}(y) \in X$ with $\sigma(\sigma^{-1}(y)) = y$, so σ is surjective. Therefore, σ is a bijection.

Conversely, suppose that σ is bijective. Define a map $\tau\colon Y \to X$ by $\tau(y) = x$ if and only if $\sigma(x) = y$. Since σ is injective, for every $y \in Y$ there is a unique x with $\sigma(x) = y$, so τ is well-defined. Take any $x \in X$ with $\sigma(x) = y$, we have

$$\tau(\sigma(x)) = \tau(y) = x,$$

so $\tau \circ \sigma = \mathrm{id}_X$. Similarly, $\sigma \circ \tau = \mathrm{id}_Y$. Therefore, σ is invertible. □

Now, the above proposition gives a way to quickly justify the existence of "inverses" for bijections, which we will use to prove the following result:

Proposition 1.2.2 ▸ Group of Bijections

Let Ω be a non-empty set and define $S_\Omega \subseteq \Omega^\Omega$ to be the set of all bijections from Ω to itself, then $(S_\Omega, \circ)$ is a group.

Proof. Trivial. □

Intuitively, if we label each element in Ω, the every map $\sigma \in S_\Omega$ is essentially a re-labelling of all elements via a one-to-one correspondence. Therefore, such bijections correspond exactly to the permutations of Ω.

Definition 1.2.3 ▸ Symmetric Group

For any non-empty set Ω, the set S_Ω of all bijective maps from Ω to itself is called the **symmetric group** under $\circ$. Each $\sigma \in S_\Omega$ is called a **permutation** of Ω.

Remark. In particular, for any $n \in \mathbb{Z}^+$, the group $S_n : S_{\{1,2,\cdots,n\}}$ is called the *symmetric group of degree* n.

Let us investigate a little bit about the cardinality of symmetric groups.

Proposition 1.2.4 ▸ Cardinality of Sets of Bijections

For any finite set Σ with $|\Sigma| = n$, define $S_{n,\Sigma}$ to be the set of all bijections from $\mathbb{Z}_n^+$ to Σ, where $\mathbb{Z}_n^+ = \{1, 2, \cdots, n\}$, then $\left|S_{n,\Sigma}\right| = n!$.

Proof. We shall proceed with induction on n. The case where $n = 1$ is obvious. Suppose that there exists some $k \in \mathbb{N}^+$ such that any finite set Σ_k with $|\Sigma_k| = k$ satisfies $\left|S_{k,\Sigma_k}\right| = k!$. Let Σ_{k+1} be any finite set such that $|\Sigma_{k+1}| = k+1$ and consider

$$S_{k+1,\Sigma_{k+1}} = \bigsqcup_{a \in \Sigma_{k+1}} \left\{\sigma \in S_{k+1,\Sigma_{k+1}} : \sigma(k+1) = a\right\}.$$

It is clear that for each $a \in \Sigma_{k+1}$,

$$\left|\left\{\sigma \in S_{k+1,\Sigma_{k+1}} : \sigma(k+1) = a\right\}\right| = \left|S_{k,\Sigma_{k+1}-\{a\}}\right| = k!.$$

Therefore,

$$\left|S_{k+1,\Sigma_{k+1}}\right| = |\Sigma_{k+1}| \cdot k! = (k+1)!.$$

□

By fixing $\Sigma = \{1, 2, \cdots, n\}$ in the above Proposition, we can easily deduce the following corollary:

Corollary 1.2.5 ▸ Cardinality of Symmetric Groups

For any $n \in \mathbb{N}^+$, we have $|S_n| = n!$.

Proof. Trivial. □

Note that this is exactly the same as the combinatorial argument that the total number of permutations over n elements is $n!$. Basically, to fix any bijection from Σ to $\mathbb{Z}_n^+$, we just need to take each element in Σ and "match" it to a unique unmatched element in $\mathbb{Z}_n^+$. In doing so, we are in fact applying the multiplication principle and it is not surprising that we can arrive at the same conclusion.

Notice that sometimes, if we apply a certain permutation repeatedly to a set, we might be able to restore the original arrangement of its elements. Such a situation is very peculiar and so we define the notion of *order* to describe it.

Definition 1.2.6 ▸ Order of a Group

Let G be a group. The **order** of $x \in G$, denoted by $|x|$, is the smallest $n \in \mathbb{N}^+$ such that $x^n = 1$. If for all $n \in \mathbb{N}^+$, we have $x^n \neq 1$, then we say that x has order ∞.

It is clear that all finite sets of cardinality n are equinumerous to S_n, so it suffices to study the behaviour of S_n's for all $n \in \mathbb{N}^+$. We first consider a special type of permutations which shift each element by one position.

Definition 1.2.7 ▸ Cycle

Let $m \leq n$ be positive integers. An **m-cycle** on S_n is the permutation over $\{a_1, a_2, \cdots, a_m\} \subseteq S_n$ such that

$$\sigma\colon a_i \mapsto \begin{cases} a_{i+1} & \text{if } 1 \leq i \leq m-1 \\ a_1 & \text{if } i = m \\ a_i & \text{otherwise} \end{cases},$$

denoted by $(a_1, a_2, \cdots, a_m)$.

To demonstrate that the cycle notation is a good notation, we offer the following proposition:

Proposition 1.2.8 ▸ Characterisation of Abelian Symmetric Groups

A symmetric group of degree n is not Abelian if and only if $n \geq 3$.

Proof. Let S_Ω be a non-Abelian symmetric group of degree n for some finite set Ω, then there exists $a, b \in S_\Omega$ such that $ab \neq ba$. Clearly, this means that $a \neq b$. Notice that a is not the identity because otherwise $ab = b = ba$, which is a contradiction. Similarly, b is not the identity, and so there must exists some $e \in S_\Omega$ which is the identity. Therefore, $n = |S_\Omega| \geq 3$.

Conversely, it suffices to prove that S_n is not Abelian if $n \geq 3$. Take $(1,2), (1,3) \in S_n$ and consider

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

Clearly, $(1,3,2) \neq (1,2,3)$ and so $(1,2)$ and $(1,3)$ do not commute. Therefore, S_n is not Abelian. □

Remark. In fact, all non-Abelian groups must have cardinality at least 3.

Some rough observation shows that the reason that some cycles do not permute is that they contain overlapping elements which will get swapped to different positions if the order of the permutations is different. However, if two cycles are disjoint, then intuitively it should not matter which one is executed first.

Proposition 1.2.9 ▸ Commutativity of Cycles

Let $(a_1, a_2, \cdots, a_m), (b_1, b_2, \cdots, b_k) \in S_n$ *be cycles, then*

$$(a_1, a_2, \cdots, a_m) \circ (b_1, b_2, \cdots, b_k) = (b_1, b_2, \cdots, b_k) \circ (a_1, a_2, \cdots, a_m)$$

if $\{a_1, a_2, \cdots, a_m\} \cap \{b_1, b_2, \cdots, b_k\} = \varnothing$.

Proof. Define

$$\begin{aligned} \sigma_{ab} &= (a_1, a_2, \cdots, a_m) \circ (b_1, b_2, \cdots, b_k), \\ \sigma_{ba} &= (b_1, b_2, \cdots, b_k) \circ (a_1, a_2, \cdots, a_m), \end{aligned}$$

then it is equivalent to proving that $\sigma_{ab}(x) = \sigma_{ba}(x)$ for all $x \in \mathbb{Z}_n^+$. Take any $x \in \mathbb{Z}_n^+$, if $x \notin \{a_1, a_2, \cdots, a_m\} \cup \{b_1, b_2, \cdots, b_k\}$, then $\sigma_{ab}(x) = x = \sigma_{ba}(x)$. If $x = a_i \in \{a_1, a_2, \cdots, a_m\}$, then

$$\begin{aligned} (a_1, a_2, \cdots, a_m)(x) &= \begin{cases} a_{i+1} & \text{if } 1 \leq i \leq m-1 \\ a_1 & \text{if } i = m \end{cases}, \\ (b_1, b_2, \cdots, b_k)(x) &= x \end{aligned}$$

because $\{a_1, a_2, \cdots, a_m\} \cap \{b_1, b_2, \cdots, b_k\} = \varnothing$. Therefore, $\sigma_{ab}(x) = \sigma_{ba}(x)$. The same argument applies to $x = b_j \in \{b_1, b_2, \cdots, b_k\}$. □

Those with the intuition or training in programming may realise that since a permutation of a set is essentially constructed by repeatedly swapping elements in pairs, we can naturally find a finite number of cycles in a permutation.

Definition 1.2.10 ▸ Cycle Decomposition

Let $\sigma \in S_n$ be any permutation, then a **cycle decomposition** of σ is a finite product in the form of

$$\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_k$$

where $\sigma_1, \sigma_2, \cdots, \sigma_k \in S_n$ are cycles.

Remark. Note that the cycle decomposition of a permutation is not unique in general.

Now, let us justify our programming intuition from a mathematical perspective.

Theorem 1.2.11 ▸ Existence of Cycle Decompositions

Every $\sigma \in S_n$ admits a cycle decomposition.

Proof. For each $\sigma \in S_n$, let us define D_σ to be a digraph with $V(D_\sigma) = \mathbb{Z}_n^+$ such that $x \to y \in E(D_\sigma)$ if and only if $\sigma(x) = y$. Fix any $v_0 \in V(D_\sigma)$. For every $i \in \mathbb{N}$, it is clear that $d^+(v_i) = 1$ and so we can take v_{i+1} as the unique out-neighbour of v_i. We claim that there exists some $v_k \in V(D_\sigma)$ such that $v_{k+1} = v_0$ because otherwise the graph is of an infinite order, which is not possible. Remove all edges $v_i \to v_{i+1}$ for $i = 1, 2, \cdots, k$ and let D'_σ be the resultant graph. We can repeat the same process again on D'_σ and we claim that eventually the graph will become empty. Suppose on contrary that the edge-minimal graph obtained through this algorithm is non-empty, then it must be acyclic and contains a longest directed path $u_0 u_1 \cdots u_k$. Let $\sigma(u_k) = w$, then $u_k \to w$ has been removed in a previous iteration, which means that $u_k \to w$ is contained in some cycle $\vec{C} \subseteq D$. Note that $u_0 u_1 \cdots u_k \nsubseteq \vec{C}$ because otherwise the path would have been removed, so there must exists a vertex $u_m \in u_0 u_1 \cdots u_k$ such that

$$u_m u_{m+1} \cdots u_k \subseteq \vec{C} \quad \text{but} \quad u_{m-1} \to u_m \notin E\left(\vec{C}\right).$$

However, this is not possible because this means that there exists some $u' \neq u_{m-1}$ such that $u', u_{m-1} \in N_D^-(u_m)$ and so $\sigma(u') = \sigma(u_{m-1}) = u_m$, which is a contradiction because σ is a bijection. Now, let $\vec{C_i}$ be the directed cycle removed at the i-th iteration, then by taking its vertices in clockwise order we form a cycle σ_i, where $i = 1, 2, \cdots, k$. It is clear that these cycles are pairwise disjoint and

$$\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_k.$$

□

The name “symmetric group” suggests a relation to geometry. We will now introduce a special group with some geometric interpretation.

Definition 1.2.12 ▸ Dihedral Group

For $n \in \mathbb{Z}_{\geq 3}$, the **dihedral group** of order $2n$, denoted by D_{2n}, is the group formed by $1, r, s$ such that

$$D_{2n} := \{1, r, r^2, \cdots, r^{n-1}, s, sr, sr^2, \cdots, sr^{n-1}\}$$

and

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

The multiplication rule for a diheral group is a bit obscure, so we may wish to use the following technique to produce some readable notation:

Definition 1.2.13 ▸ Multiplication Table

Let $G := \{g_1, g_2, \cdots, g_n\}$ be a finite group. The **multiplication table** of G is an $n \times n$ matrix whose (i, j) entry is $g_i g_j$.

With "some" computation, one may notice that the multiplication tables of D_6 and S_3 look quite similar, which gives as the motivation to visualise D_{2n} using some geometric representation.

Consider a regular n-sided polygon P and define r as "clockwise rotation of P about its centre by $\frac{2\pi}{n}$" and s as "reflection of P about an axis through a fixed point in P and the origin". Surprisingly, such a definition is coherent with the multiplication rule in Definition 1.2.12! Indeed, doing r for n times and doing s twice both means that the polygon remains what it was originally, and a rotation followed by reflection is exactly the same as a reflection followed by a rotation in the opposite direction.

> *Remark.* Note that for $n > 3$, the multiplication tables of D_{2n} and S_n no longer coincide because $|D_{2n}| = 2n \neq n! = |S_n|$.

Intuitively, a permutation can be achieved by a sequence of swaps, which are essentially 2-cycles.

Definition 1.2.14 ▸ Transposition

A **transposition** is a 2-cycle.

Clearly, since every permutation can be decomposed into swaps, transpositions generate a symmetric group.

Proposition 1.2.15 ▸ Transpositions Decomposition of Symmetric Groups

Let S_n be a symmetric group and T_n be the collection of all transpositions in S_n, then $S_n = \langle T_n \rangle$.

Proof. We proceed with induction on n. The case where $n = 1$ is trivial. Suppose that there exists some $k \in \mathbb{Z}^+$ such that $S_k = \langle T_k \rangle$. For any $\sigma \in S_{k+1}$, define

$$\tau_\sigma := \begin{cases} (\sigma(k+1), k+1) & \text{if } \sigma(k+1) \neq k+1 \\ \mathrm{id} & \text{otherwise} \end{cases}.$$

Therefore, $k+1$ is the unique element mapped to $k+1$ by $\tau_\sigma \circ \sigma$. Clearly, $\tau_\sigma \circ \sigma$ is a bijection and so $(\tau_\sigma \circ \sigma) \in S_k$. Therefore, there exists transpositions $\tau_1, \tau_2, \cdots, \tau_r \in S_k$ such that

$$(\tau_\sigma \circ \sigma) = \prod_{i=1}^{r} \tau_i.$$

Since $\tau_\sigma^{-1} = \tau_\sigma$,

$$\sigma = \tau_\sigma \circ \tau_\sigma \circ \sigma = \tau_\sigma \circ \prod_{i=1}^{r} \tau_i.$$

Therefore, $S_{k+1} = \langle T_{k+1} \rangle$. □

Alternatively, observe that every cycle can be written as

$$(a_1, a_2, \cdots, a_m) = \prod_{i=2}^{m} (a_1, a_i),$$

so by applying Theorem 1.2.11, we can first decompose every permutation into cycles and then into transpositions, followed by merging repeated transpositions. Applying the same reasoning on every transposition leads to the following corollary:

Corollary 1.2.16 ▸ Simplified Transposition Decomposition

Every symmetric group S_n is generated by $\{(1k) \in S_n : k = 2, 3, \cdots, n\}$.

Notice further that every transposition in the form of $(1n)$ can be achieved by first swapping n with $n-1$, then swapping 1 and $n-1$, and lastly swapping $n-1$ and n again, which leads to the following alternative decomposition:

Corollary 1.2.17 ▸ Decomposition by Adjacent Transpositions of Symmetric Groups

Every symmetric group S_n is generated by $\{(i, i+1) : i = 1, 2, \cdots, n-1\}$.

Observe also that to swap 1 and n, it is equivalent to rotating the list towards the right by an offset of 1, swapping 1 and 2, followed by a rotation in the reverse direction by aan offset of 1.

Corollary 1.2.18 ▸ Decomposition by Rotation and Transposition of Symmetric Groups

Every symmetric group S_n *is generated by* $\{(12), (12 \cdots n)\}$.

Remark. While there are many ways to generate a symmetric group with transpositions, it is not true in general that any transpositions and cycles can generate a symmetric group. For example, $\{(12), (1324)\}$ generates a subgroup of S_4 isomorphic to D_8.

Consider any permutation $\sigma \in S_n$. A possible visualisation is to view σ as a "labelling" of $\{1, 2, \cdots, n\}$. In other words, the permutation imposes an ordering onto the set, which can be somewhat related to *sorting*. Here, we introduce a notion that is a generalisation of *inversions* in sorting.

Definition 1.2.19 ▸ Reversal

Let $\sigma \in S_n$. A **reversal** of σ is an ordered pair $(a, b) \in \{1, 2, \cdots, n\}^2$ such that $a < b$ but $\sigma(a) > \sigma(b)$. We denote the set of all reversals of σ by $R(\sigma)$.

Remark. It is clear that $0 \leq |R(\sigma)| \leq \frac{n(n-1)}{2}$ for any $\sigma \in S_n$.

1.3 Group Homomorphisms

Previously, we have seen how S_Ω and S_n are essentially "the same" if $|\Omega| = n$. This is exactly because of the fact that these groups have the same structure. We shall now formalise the notion of "having the same structure". In the context of groups, since every group can be completely defined by a binary operation, it is natural to define a structure-preserving transformation as one which preserves the binary operation.

Definition 1.3.1 ▸ Group Homomorphism

Let $(G, \star)$ and $(H, \diamond)$ be groups. A **homomorphism** from G to H is a map $\varphi \colon G \to H$ such that

$$\varphi(a \star b) = \varphi(a) \diamond \varphi(b)$$

for all $a, b \in G$.

Recall that the notions of identity and inverses are induced by the binary operation on a group, so naturally a group homomorphism should respect these structures as well.

Proposition 1.3.2 ▸ Properties of Group Homomorphisms

Let $\varphi\colon G \to H$ be a homomorphism, then

$$\varphi(1_G) = \varphi(1_H) \quad \text{and} \quad \varphi(a^{-1}) = \varphi(a)^{-1}$$

for all $a \in G$.

Proof. Notice that

$$\varphi(1_G)\varphi(1_G) = \varphi\left({1_G}^2\right) = 1_H\varphi(1_G),$$

so by 1.1.14, we have $\varphi(1_G) = 1_H$. Consider

$$\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(1_G) = 1_H.$$

Similarly, $\varphi(a)\varphi(a^{-1}) = 1_H$, so $\varphi(a^{-1}) = \varphi(a)^{-1}$ for all $a \in G$. □

Clearly, for any group G, the identity map $\mathrm{id}_G\colon G \to G$ is a homomorphism. Moreover, by denoting $\mathbb{1} := \{1\}$, the maps $\psi\colon \mathbb{1} \to G$ and $\varphi\colon G \to \{1\}$ with $\psi(1) = 1_G$ and $\varphi(a) = 1$ for all $a \in G$ are the unique homomorphisms for any group G. It is also clear from the above fact that "the" singleton group is unique up to homomorphisms.

Intuitively, since a homomorphism does not change the group's structure, the group's structure will not change after undergoing any sequence of homomorphisms.

Proposition 1.3.3 ▸ Composition of Homomorphisms Is a Homomorphism

For any groups G, H, K, if $\varphi\colon G \to H$ and $\psi\colon H \to K$ are homomorphisms, then

$$\psi \circ \varphi\colon G \to K$$

is a homomorphism.

Proof. Left to the reader as an exercise. □

We introduce a special homomorphism on symmetric groups.

Definition 1.3.4 ▸ Sign Homomorphism

The **sign homomorphism** on S_n is the map $\epsilon\colon S_n \to \{\pm 1\}$ defined by

$$\epsilon(\sigma) = (-1)^{|R(\sigma)|}.$$

A permutation $\sigma \in S_n$ is called an **even permutation** if $\epsilon(\sigma) = 1$, and an **odd permutation** otherwise.

Intuitively, for each reversal (i, j), the signs of $i - j$ and $\sigma(i) - \sigma(j)$ are reversed. Therefore, if

$$\Delta := \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

is a polynomial, by defining

$$\sigma(\Delta) := \prod_{1 \leq i < j \leq n} \left(x_{\sigma(i)} - x_{\sigma(j)}\right),$$

ϵ is the only sign such function such that $\sigma(\Delta) = \epsilon(\sigma)\,\Delta$.

One can check that ϵ is surjective, so for any symmetric group, there exists at least one even permutation and at least one odd permutation. In general, we have the following result:

Corollary 1.3.5 ▸ Characterisation of the Sign of a Permutation

For any $\sigma \in S_n$, $\epsilon(\sigma) = 1$ if and only if σ is a product of an even number of transpositions.

Observe that every m-cycle has exactly $(m-1)$ reversals all with respect to the last index.

Let us examine two simple groups, S_2 and S_3, and try to list down all homomorphisms between them. Let $\varphi\colon S_2 \to S_3$ be a homomorphism, then by Proposition 1.3.2, we must have $\varphi\left(1_{S_2}\right) = 1_{S_3}$. Therefore, it suffices to fix $\varphi((12))$. Since $(12)^2 = 1$, we need to fix $b \in S_3$ with $b^2 = 1$, which means that $b = 1_{S_3}$ or (12) or (13) or (23). The other direction requires a bit more working.

Proposition 1.3.6 ▸ Homomorphisms from S_3 to S_2

Any group homomorphism from S_3 to S_2 is either the trivial identity map or the sign map $\operatorname{sgn}\colon S_3 \to S_2$ *such that*

$$\operatorname{sgn}(a) = \begin{cases} 1 & \text{if } a = 1 \text{ or } (123) \text{ or } (132) \\ (12) & \text{if } a = (12) \text{ or } (23) \text{ or } (13) \end{cases}.$$

Proof. Let $\psi\colon S_3 \to S_2$ be a homomorphism. We claim that

$$\psi((132)) = \psi((123)) = 1.$$

Notice that $(123)^3 = 1$, so $\psi((123))^3 = 1 \in S_2$, which implies that $\psi((123)) = 1$

because $(12)^3 = (12) \neq 1$. If $\operatorname{sgn} \neq \psi$, then there exists $a \in \{(12), (23), (13)\}$ such that $\psi(a) \neq (12)$. Without loss of generality, assume that $a = (12)$, then $\psi((12)) = 1$. Therefore,

$$\begin{aligned}\psi((13)) &= \psi((13)(12)) = \psi((123)) = 1, \\ \psi((23)) &= \psi((23)(12)) = \psi((123)) = 1.\end{aligned}$$

Therefore, ψ is the trivial map. Therefore, every homomorphism from S_3 to S_2 is either trivial or sgn. □

Like linear transformations, group homomorphisms come with the ideas of “kernels” and “images”.

Definition 1.3.7 ▸ Kernel and Image

Let $\varphi\colon G \to H$ be a group homomorphism, then the **kernel** of φ is

$$\ker(\varphi) := \{g \in G \colon \varphi(g) = 1_H\}$$

and the **image** of φ is

$$\operatorname{im}(\varphi) : \{\varphi(g) \in H \colon g \in G\}.$$

Intuitively, a homomorphism being bijective is equivalent to its image being the same as the co-domain. More specifically, we have the following characterisation:

Proposition 1.3.8 ▸ Kernel and Image Characterisation of Isomorphisms

Let $\varphi\colon G \to H$ be a group homomorphism, then

1. *φ is injective if and only if $\ker(\varphi) = \{1\}$;*
2. *φ is surjective if and only if $\operatorname{im}(\varphi) = H$.*

Proof. 2 is trivial so it suffices to prove 1. Suppose that φ is injective. Take $x \in G$ such that $\varphi(x) = 1$, then

$$\varphi(x) = 1 = \varphi(1),$$

which implies that $x = 1$ and so we have $\ker(\varphi) = \{1\}$. Suppose conversely that $\ker(\varphi) = \{1\}$, we show that φ is injective by considering the contrapositive statement. Suppose that φ is not injective, then there exists $x, y \in G$ with $x \neq y$ but $\varphi(x) = \varphi(y)$. Therefore,

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

Since $x \neq y$, we have $x^{-1} \neq y^{-1}$ and so $x^{-1}y \neq 1$. Therefore, $\ker(\varphi) \neq \{1\}$. □

Using the kernel, we can see that in S_n, the set of all permutations decomposed into an even number of transpositions is exactly $\ker(\epsilon)$.

Definition 1.3.9 ▸ Alternating Group

For every $n \in \mathbb{Z}^+$, the **alternating group** is defined by $A_n := \ker(\epsilon)$.

Intuitively, for every $n > 1$, exactly half of the permutations in S_n are even. Therefore, it is clear that $A_1 = S_1$ and $|A_n| = \frac{1}{2}n!$ for all $n > 1$.

Remark. There is no order-6 subgroup of A_4.

Fix $n \in \mathbb{Z}$, define the "multiplication by n" map by $m \mapsto nm$. One may check that this is a group homomorphism due to distributive law of multiplication. Clearly,

$$\ker(m \mapsto nm) = \begin{cases} 0 & \text{if } n \neq 0 \\ \mathbb{Z} & \text{otherwise} \end{cases}$$

and

$$\operatorname{im}(m \mapsto nm) = n\mathbb{Z} := \{nk \colon k \in \mathbb{Z}\}.$$

As a side note, such maps have covered all group homomorphisms over the addition group on $\mathbb{Z}$.

Proposition 1.3.10 ▸ Multiplication Is the Only Group Homomorphism over $(\mathbb{Z}, +)$

For every group homomorphism $\varphi\colon \mathbb{Z} \to \mathbb{Z}$, there exists some $n \in \mathbb{Z}$ such that

$$\varphi(m) = nm \qquad \textit{for all } m \in \mathbb{Z}.$$

Proof. Take $n := \varphi(1)$. For all $m \geq 0$, we have

$$\begin{aligned} \varphi(m) &= \varphi\left(\sum_{i=1}^{m} 1\right) \\ &= \sum_{i=1}^{m} \varphi(1) \\ &= \sum_{i=1}^{m} n \\ &= nm. \end{aligned}$$

For all $m < 0$, we have

$$\begin{aligned}\varphi(m) &= \varphi(-(-m)) \\ &= -\varphi(-m) \\ &= -n(-m) \\ &= nm.\end{aligned}$$

□

Since homomorphisms are mappings, it is natural to talk about their bijectivity. Intuitively, a "bijective homomorphism" establishes an equivalent relationship to transform between the groups.

Definition 1.3.11 ▸ Group Isomorphism

An **isomorphism** from G to H is a homomorphism $\varphi\colon G \to H$ such that there exists a homomorphism $\psi\colon H \to G$ such that $\psi \circ \varphi = \mathrm{id}_G$ and $\varphi \circ \psi = \mathrm{id}_H$. Groups G and H are said to be **isomorphic**, denoted by $G \cong H$.

Let us justify our intuition that an isomorphism is nothing but a bijective homomorphism.

Proposition 1.3.12 ▸ Characterisation of Group Isomorphism

A homomorphism $\varphi\colon G \to H$ is an isomorphism if and only if it is bijective.

Proof. By Proposition 1.2.1. □

Isomorphic groups are essentially the "different forms" of the "same group", so their binary operations are compatible with each other and underlying sets coincide. Naturally, being isomorphic is an equivalence relation.

Proposition 1.3.13 ▸ Properties of Isomorphic Groups

For any groups G, H and K,

- *$G \cong G$;*
- *if $G \cong H$, then $H \cong G$;*
- *if $G \cong H$ and $H \cong K$, then $G \cong K$.*

Proof. Trivial. □

Remark. It is worth noting that although $\cong$ is reflexive, symmetric and transitive, it is not an equivalence relation because there is no "set of all sets" and so there is no "set of all groups".

Recall that we have stated that S_n and S_Ω are essentially the same if $|\Omega| = n$. This is precisely because that $S_n \cong S_\Omega$. In fact, we can prove a more general result.

Proposition 1.3.14 ▸ Isomorphism between Symmetric Groups

Let Δ and Ω be sets and $\theta\colon \Delta \to \Omega$ be a bijection, then the map $\varphi_\theta\colon S_\Delta \to S_\Omega$ defined by

$$\varphi_\theta(\sigma) = \theta \circ \sigma \circ \theta^{-1}$$

is a group isomorphism.

Proof. For any $\tau, \sigma \in S_\Delta$, we have

$$\begin{aligned}\varphi_\theta(\tau \circ \sigma) &= \theta \circ (\tau \circ \sigma) \circ \theta^{-1} \\ &= \theta \circ \tau \circ \theta^{-1} \circ \theta \circ \sigma \circ \theta^{-1} \\ &= \varphi_\theta(\tau) \circ \varphi_\theta(\sigma).\end{aligned}$$

Therefore, φ_θ is a homomorphism. Similarly, $\varphi_{\theta^{-1}}\colon S_\Omega \to S_\Delta$ is a group homomorphism. Note that for each $\sigma \in S_\Omega$

$$\begin{aligned}\left(\varphi_\theta \circ \varphi_\theta^{-1}\right)(\sigma) &= \varphi_\theta(\varphi_{\theta^{-1}}(\sigma)) \\ &= \theta \circ \left(\theta^{-1} \circ \sigma \circ \theta\right) \circ \theta^{-1} \\ &= \sigma,\end{aligned}$$

so $\varphi_\theta \circ \varphi_{\theta^{-1}} = \mathrm{id}_{S_\Omega}$. Similarly, $\varphi_{\theta^{-1}} \circ \varphi_\theta = \mathrm{id}_{S_\Delta}$. Therefore, by Proposition 1.2.1, φ_θ is bijective and by Proposition 1.3.12, this means that φ_θ is a group isomorphism. □

Remark. In general, if Δ, Ω and Σ are sets and $\theta\colon \Delta \to \Omega$, $\eta\colon \Omega \to \Sigma$ are bijections, then $\varphi_{\theta \circ \eta} = \varphi_\theta \circ \varphi_\eta$. Furthermore, $\varphi_{\mathrm{id}_\Delta} = \mathrm{id}_{S_\Delta}$.

2 Universal Properties

2.1 Categories

A fundamental question in mathematics is **how one defines an mathematical object**. Conventionally, one uses a **constructive** approach by proposing an explicit structure of an object. However, certain objects are hard to be defined this way (an infamous example is the notion of a "set"). Therefore, we may opt for a different approach where we **describe the "behaviour"** of an object.

The Universal Properties is used to describe the interaction of an object with all other objects of choice. For example, Theorem 4.1.5 describes group homomorphisms $\mathbb{Z} \to G$ for any group G, which characterises $\mathbb{Z}$ (up to group isomorphisms).

To better understand this, let us introduce some preliminary definitions.

Definition 2.1.1 ▸ Category

A **category** $\mathcal{C}$ consists of a class of objects $\operatorname{ob}(\mathcal{C})$ and a class of morphisms between objects $\operatorname{mor}(\mathcal{C})$ such that:

- for any morphisms $f \colon A \to B$ and $g \colon B \to C$, there exists a morphism
$$h := g \circ f \colon A \to C;$$
- for every object $A \in \operatorname{ob}(\mathcal{C})$, there exists an **identity** morphism $\mathrm{id}_A \colon A \to A$ such that
$$\mathrm{id}_B \circ f = f \circ \mathrm{id}_A = f$$
for any morphism $f \colon A \to B$;
- for any morphisms $f \colon A \to B$, $g \colon B \to C$ and $h \colon C \to D$,
$$h \circ (g \circ f) = (h \circ g) \circ f.$$

We use the notation $\operatorname{Hom}(A, B)$ to denote the class of all morphisms from A to B in a category. It is clear that $\operatorname{Hom}(A, A) \neq \varnothing$ for every object A. In particular, the *category of group*, denoted as Grp, is constructed with

- $\operatorname{ob}(\mathrm{Grp})$: the class of all groups, and

- $\operatorname{Hom}(G, H)$: the class of all group homomorphisms from G to H,

where the composition, identities and associative law are defined in the intuitive way.

Categories are somewhat highly abstract collections of mathematical objects. Therefore, it is natural to think about how one would transform between different categories.

Definition 2.1.2 ▸ Functor

Let $\mathcal{C}$ and $\mathcal{D}$ be categories. A **functor** from $\mathcal{C}$ to $\mathcal{D}$ is a mapping F such that

- for each $X \in \operatorname{ob}(\mathcal{C})$, there exists some $Y \in \operatorname{ob}(\mathcal{D})$ with $Y = F(X)$;
- for each morphism $\varphi \colon X \to Y$ in $\mathcal{C}$, there exists a morphism

$$\phi := F(\varphi) : F(X) \to F(Y)$$

  in $\mathcal{D}$ such that
  - $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$;
  - $F(\psi \circ \varphi) = F(\psi) \circ F(\varphi)$ for any morphisms $\psi \colon Y \to Z$ and $\varphi \colon X \to Y$ in $\mathcal{C}$.

2.2 Universal Properties

Let Set be the category of set, then we can defined a *set-valued functor on the category of group* as $F \colon \mathrm{Grp} \to \mathrm{Set}$. Such a functor is not a map since there is no set of sets (and thus no set of groups). In particular, the following defines a functor to map each group to its underlying set:

Definition 2.2.1 ▸ Forgetful Functor

The **forgetful functor** is a functor $\mathrm{Forget} \colon \mathrm{Grp} \to \mathrm{Set}$ such that

$$\mathrm{Forget}(G) = G \quad \text{and} \quad \mathrm{Forget}(\varphi) = \varphi.$$

There is also a trivial functor $F \colon \mathrm{Grp} \to \mathrm{Set}$ defined by $F(G) = \varnothing$ and $F(\varphi) = \mathrm{id}_{\varnothing}$. The following proposition defines a more complex functor:

Proposition 2.2.2 ▸ Well-Defined-ness of the Hom-Functor

Fix a group K and define $F \colon \mathrm{Grp} \to \mathrm{Set}$ such that

$$F(G) = \operatorname{Hom}(K, G) \quad \textit{and} \quad F(\varphi) = \operatorname{Hom}(K, \varphi) := \tau \mapsto \varphi \circ \tau,$$

then F is a functor.

Proof. It suffices to prove that F preserves morphisms. Note that for any group G and any $\tau \in \operatorname{Hom}(K, G)$, we have

$$F(\mathrm{id}_G)(\tau) = \operatorname{Hom}(K, \mathrm{id}_G)(\tau) = \mathrm{id}_G \circ \tau = \tau,$$

so $F(\mathrm{id}_G) = \mathrm{id}_{\operatorname{Hom}(K,G)} = \mathrm{id}_{F(G)}$. Let $\varphi \in \operatorname{Hom}(G, H)$ and $\psi \in \operatorname{Hom}(H, K)$ be any group homomorphisms, then

$$\begin{aligned}
F(\psi \circ \varphi)(\tau) &= \operatorname{Hom}(K, \psi \circ \varphi)(\tau) \\
&= (\psi \circ \varphi) \circ \tau \\
&= F(\varphi) \circ F(\psi) \\
&= \psi \circ (\varphi \circ \tau) \\
&= \operatorname{Hom}(K, \psi)(\varphi \circ \tau) \\
&= \operatorname{Hom}(K, \psi)(\operatorname{Hom}(K, \varphi)(\tau)) \\
&= (\operatorname{Hom}(K, \psi) \circ \operatorname{Hom}(K, \varphi))(\tau) \\
&= (F(\psi) \circ F(\varphi))(\tau)
\end{aligned}$$

for any $\tau \in \operatorname{Hom}(K, G)$. Therefore, $F(\psi \circ \varphi) = F(\psi) \circ F(\varphi)$ and so F is a functor. □

Remark. The above functor is usually written as $\operatorname{Hom}(G, -)$.

Since there are numerous ways to define a functor between categories, it is natural to think about the question of whether the functors can be "transformed" into each other through composition as well.

Definition 2.2.3 ▸ Natural Transformation

Let F_1 and F_2 be functors from $\mathcal{C}$ to $\mathcal{D}$. A **natural transformation** $\eta \colon F_1 \Rightarrow F_2$ is a family of morphisms in $\mathcal{D}$ such that

- for every $X \in \operatorname{ob}(\mathcal{C})$, there exists some $\eta_X : F_1(X) \to F_2(X) \in \eta$, known as the **component** of η at X;
- for every morphism $\varphi \colon X \to Y$ in $\operatorname{mor}(\mathcal{C})$, we have $\eta_Y \circ F_1(\varphi) = F_2(\varphi) \circ \eta_X$.

Remark. With $\mathcal{C} := \mathsf{Grp}$ and $\mathcal{D} := \mathsf{Set}$, the natural transformation η is a collection of underlying maps for group homomorphisms.

We can think a natural transformation as a "projection" of a morphism in one category onto another category, such that the "shadow of the transformed object" is the same as the "transformed shadow of the original object".

Definition 2.2.4 ▸ Natural Isomorphism

A natural transformation $\eta\colon F_1 \Rightarrow F_2$ is an **natural isomorphism** if there exists a natural transformation $\zeta\colon F_2 \Rightarrow F_1$ such that $\zeta_X \circ \eta_X = \mathrm{id}_{F_1(X)}$ and $\eta_X \circ \zeta_X = \mathrm{id}_{F_2(X)}$ for every X. We say that F_1 and F_2 are **isomorphic**, denoted by $F_1 \cong F_2$.

In the case of groups, a natural isomorphism will contain group isomorphisms. Analogously speaking, a natural isomorphism between categories is not so different from bijective maps between sets.

Definition 2.2.5 ▸ Bijectivity of Natural Transformations

A natural transformation $\eta\colon F_1 \Rightarrow F_2$ is **bijective** if $\eta_X\colon F_1(X) \to F_2(X)$ is bijective for every X.

A natural conclusion here is that a natural isomorphism is nothing but a bijective natural transformation.

Proposition 2.2.6 ▸ Characterisation of Natural Isomorphisms

A natural transformation $\eta\colon F_1 \Rightarrow F_2$ is an isomorphism if and only if it is bijective.

Proof. Suppose that η is bijective. For any X, since η_X is bijective, there exists a unique morphism $\zeta_X\colon F_2(X) \to F_1(X)$ such that

$$\eta_X \circ \zeta_X = \mathrm{id}_{F_2(X)} \quad \text{and} \quad \zeta_X \circ \eta_X = \mathrm{id}_{F_1(X)}.$$

We claim that $\zeta := \{\zeta_X : \eta_X \in \eta\}$ is a natural transformation. □

Note that a natural isomorphism consists of morphisms which have a two-sided inverse. Using a weaker condition, we can consider morphisms with only one-sided inverses and in particular right inverses.

Definition 2.2.7 ▸ Epimorphism

A morphism $f\colon X \to Y$ is an **epimorphism** if $g_1 \circ f = g_2 \circ f$ implies $g_1 = g_2$ for all $g_1, g_2\colon Y \to Z$.

In other words, a morphism $f\colon X \to Y$ is an epimorphism if and only if there exists a morphism $h\colon Y \to X$ such that $f \circ h = \mathrm{id}_Y$.

In the category of group, **a group homomorphism is an epimorphism if and only if it is surjective**. An epimorphism might be said to be **canonical**, which implies that there is no other possibilities for this epimorphism.

Now we formally introduce the notion of a *universal property* of a group, which is a property that defines everything about the interaction between the group and any other group. In category-theoretic terms, this "universality" for $\mathbb{Z}$ is stated as follows:

Theorem 2.2.8 ▸ Universal Property of the Integers

Let $\operatorname{Hom}(\mathbb{Z}, -)$ *be a* Hom*-functor, then there is an isomorphism* $\operatorname{Hom}(\mathbb{Z}, -) \cong \text{Forget}$ *and for any group* K *such that* $\operatorname{Hom}(K, -) \cong \text{Forget}$, *there exists a canonical isomorphism* $\mathbb{Z} \cong K$.

Proof. For any group G, define $\eta_G \colon \operatorname{Hom}(\mathbb{Z}, G) \to \text{Forget}(G)$ by $\eta_G(\varphi) = \varphi(1)$. We claim that

$$\eta := \{\eta_G \colon G \text{ is a group}\}$$

is a natural transformation from $\operatorname{Hom}(\mathbb{Z}, -)$ to Forget. Let $\varphi \colon G \to H$ be any group homomorphism. Take any group G and $\tau \in \operatorname{Hom}(\mathbb{Z}, G)$, then

$$\begin{aligned}(\eta_H \circ \operatorname{Hom}(\mathbb{Z}, \varphi))(\tau) &= \eta_H(\varphi \circ \tau)\\ &= (\varphi \circ \tau)(1)\\ &= \varphi(\eta_G(\tau))\\ &= (\text{Forget}(\varphi) \circ \eta_G)(\tau).\end{aligned}$$

Therefore, $\eta_H \circ \operatorname{Hom}(\mathbb{Z}, \varphi) = \text{Forget}(\varphi) \circ \eta_G$ and so η is a natural transformation. For any group G, suppose that $\eta_G(\varphi) = \eta_G(\psi)$ for some $\varphi, \psi \in \operatorname{Hom}(\mathbb{Z}, G)$, then we have $\varphi(1) = \psi(1)$. By Theorem 4.1.5, there is a unique group homomorphism from $\mathbb{Z}$ to G which maps 1 to $\varphi(1)$, so $\varphi = \psi$ and so η_G is injective. For any $x \in G$, by Theorem 4.1.5, there exists some $\varphi \colon \mathbb{Z} \to G$ with $\varphi(1) = x$ and so $\eta_G(\varphi) = x$. Therefore, η_G is surjective and so η_G is a bijection. By Proposition 2.2.6, η is a natural isomorphism. Let $\zeta \colon \operatorname{Hom}(K, -) \Rightarrow \text{Forget}$ be a natural isomorphism. Define

$$\rho := \{\rho_G = \zeta_G^{-1} \circ \eta_G \colon G \text{ is a group}\},$$

which is clearly a natural isomorphism. Define

$$\alpha := \rho_{\mathbb{Z}}(\mathrm{id}_{\mathbb{Z}}) \in \operatorname{Hom}(K, \mathbb{Z}) \quad \text{and} \quad \beta := \rho_K^{-1}(\mathrm{id}_K) \in \operatorname{Hom}(\mathbb{Z}, K).$$

Consider

$$\begin{aligned}\beta \circ \alpha &= \operatorname{Hom}(K, \beta)(\alpha) \\ &= \left(\operatorname{Hom}(K, \beta) \circ \rho_{\mathbb{Z}}\right)(\mathrm{id}_{\mathbb{Z}}) \\ &= \left(\rho_K \circ \operatorname{Hom}(\mathbb{Z}, \beta)\right)(\mathrm{id}_{\mathbb{Z}}) \\ &= \rho_K\left(\operatorname{Hom}(\mathbb{Z}, \beta)(\mathrm{id}_{\mathbb{Z}})\right) \\ &= \rho_K(\beta \circ \mathrm{id}_{\mathbb{Z}}) \\ &= \rho_K\left(\rho_K^{-1}(\mathrm{id}_K)\right) \\ &= \mathrm{id}_K.\end{aligned}$$

Similarly, $\alpha \circ \beta = \mathrm{id}_{\mathbb{Z}}$ and so α and β are isomorphisms. □

3 Subgroups

3.1 Subgroups

Definition 3.1.1 ▸ Subgroup

A **subgroup** of a group G is a subset $H \subseteq G$, denoted by $H \leq G$, such that

- for all $x, y \in H$, we have $xy \in H$;
- $1_G \in H$;
- for all $x \in H$, we have $x^{-1} \in H$.

If $H \neq G$, then H is said to be a **proper subgroup** of G, denoted by $H < G$.

For every group G, the *trivial subgroup* is $\{1_G\}$ and every group is known to be its own *improper subgroup*.

Clearly, the binary operation on H must be compatible with that on G if $H \leq G$.

Proposition 3.1.2 ▸ Equivalent Definition of Subgroups

If $(G, \star)$ is a group and $H \subseteq G$, then $H \leq G$ if and only if $(H, \star)$ is a group.

Proof. Trivial. □

Since a subgroup lies entirely in a bigger group, there is a natural homomorphic structure between them.

Definition 3.1.3 ▸ Inclusion Homomorphism

Let G be a group and $H \leq G$ be a subgroup. The map $i \colon H \to G$ defined by $i(h) = h$ is called the **inclusion homomorphism**.

Clearly, the image of the inclusion map is the subgroup itself. This is a special case of the following more general result:

Proposition 3.1.4 ▸ Kernels and Images as Subgroups

Let $\varphi \colon G \to H$ be a group homomorphism, then $\ker(\varphi) \leq G$ *and* $\operatorname{im}(\varphi) \leq H$.

Proof. Trivial. □

Note that given any subgroup $H \leq G$, there is always a subgroup $H_0 \leq G$ such that $\operatorname{im}\left(i_{H_0}\right) \leq H$. More specifically, there are homomorphisms from G to both H and H_0, which motivates the universal property of subgroups.

Theorem 3.1.5 ▸ Universal Property of Subgroups

Let G be a group and $H \leq G$ be a subgroup. For every group homomorphism $\varphi \colon G \to H$, there exists a unique group homomorphism $\psi \colon G \to K$ where $\operatorname{im}(\varphi) \leq K \leq H$ such that $\varphi = i_K \circ \psi$.

Proof. Take $K = \operatorname{im}(\varphi)$ and define $\psi(g) = \varphi(g)$, then $\operatorname{im}(\varphi) \leq K \leq H$ and for every $g \in G$, we have

$$\varphi(g) = \psi(g) = i_K(\psi(g)) = (i_K \circ \psi)(g).$$

Therefore, $\varphi = i_K \circ \psi$. Let $\phi \colon G \to K$ be any group homomorphism where $K \leq G$ such that $\varphi = i_K \circ \phi$. Since $i_K \circ \phi$ is well-defined, we have $K = \operatorname{im}(\phi)$. For any $g \in G$, we have

$$\phi(g) = (i_K \circ \phi)(g) = \varphi(g)$$

and so $\phi = \varphi$, which implies that ϕ is unique. □

Subgroup relationship is obviously transitive.

Proposition 3.1.6 ▸ Transitivity of Subgroups

If $H \leq G$ and $K \leq H$, then $K \leq G$.

3.2 Subgroup Criteria

Now we study some conditions under which a subset becomes a subgroup.

Proposition 3.2.1 ▸ Subgroup Criterion

Let G be a group and $H \subseteq G$, then $H \leq G$ if and only if $H \neq \varnothing$ and $xy^{-1} \in H$ for all $x, y \in H$.

Proof. Suppose that $H \subseteq G$, then $1_G \in H$ and so $H \neq \varnothing$. For all $x, y \in H$, we have y^{-1} and so $xy^{-1} \in H$. Suppose conversely that $H \neq \varnothing$ and $xy^{-1} \in H$ for all $x, y \in H$. Take some $a \in H \subseteq G$, then $1_G = aa^{-1} \in H$. Therefore, $a^{-1} = a1_G^{-1} = a1_G = a \in H$. This means that for all $a, b \in H$, we have $b^{-1} \in H$ and so $ab = a\left(b^{-1}\right)^{-1} \in H$. Therefore, we have $H \leq G$. □

We examine the following structure with the criterion:

Proposition 3.2.2 ▸ Subgroups of Integers

For each $n \in \mathbb{Z}$, define

$$n\mathbb{Z} := \{nk \colon k \in \mathbb{Z}\} \subseteq \mathbb{Z},$$

then every subgroup $H \leq \mathbb{Z}$ is such that $H = n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

Proof. Let $H \leq \mathbb{Z}$ be a subgroup and take $n := \min\{h \in H \colon h > 0\}$. We claim that for all $m \in \{h \in H \colon h > 0\}$, we have $n \mid m$. Suppose on contrary that there exists some $m \in \{h \in H \colon h > 0\}$ such that $n \nmid m$, then $m > n$ and so we can write

$$m = nq + r \quad \text{for some } q, r \in \mathbb{Z}^+$$

where $0 < r < n$. Note that $-qn \in H$ and so

$$m + (-qn) = r \in [1, n-1]$$

is a smaller positive integer than n in H, which is a contradiction. Take any $h \in H$, then if $h \geq 0$, there exists some $k \in \mathbb{N}$ such that $h = nk$. Otherwise, $h < 0$ and so

$$h = -(-h) = nk'$$

for some $k' \in \mathbb{Z}^-$. Therefore, $H \subseteq n\mathbb{Z}$. Clearly, this implies that for all $k \in \mathbb{Z}^+$, we have $nk \in H$. Therefore, □

In finite subsets, it turns out that the existence of inverses becomes free.

Proposition 3.2.3 ▸ Finite Subgroup Criterion

Let G be a group. A finite subset $H \subseteq G$ is a subgroup of G if and only if $H \neq \varnothing$ and $xy \in H$ for all $x, y \in H$.

Proof. The forward direction is trivial. Take some $y \in H$, then clearly $y^a \in H$ for all $a \in \mathbb{Z}^+$. Let $\sigma_y \colon Z^+ \to H$ be defined by $\sigma_y(a) = y^a$, then since H is finite, σ_y is not injective. Therefore, without loss of generality, there exist $a, b \in Z^+$ with $a < b$ such that $\sigma_y(a) = \sigma_y(b)$. Therefore,

$$1_G = y^b y_a^{-1} = y^{b-a} \in H.$$

Notice that $b - a - 1 \in \mathbb{N}$, so $y^{b-a-1} \in H$. Notice that $yy^{b-a-1} = y^{b-a-1}y = y^{b-a} = 1_G$, so $y^{-1} = y^{b-a-1} \in H$. □

Intuitively, for any two subgroups of the same group, their intersection should still be a subgroup. This can be extended to the following general result:

Proposition 3.2.4 ▸ Preservation of Subgroups under Intersection

Let $\mathcal{S}$ be any non-empty family of subgroups of a group G, then

$$\bigcap_{H\in\mathcal{S}} H \leq G.$$

Proof. Left as an exercise to the reader. □

In a different perspective, the intersection of several subgroups can be seen as the "smallest common part" of the subgroups which still preserves the group structure. Therefore, this subgroup can be seen as "the minimal subgroup" that contains a small part of the original group.

Definition 3.2.5 ▸ Generated Subgroup

Let G be a group and $A \subseteq G$ be a subset, then the subgroup

$$\langle A\rangle := \bigcap_{A\subseteq H\leq G} H$$

is said to be **generated** by A.

In other words, a subgroup generated by a set A is the smallest subgroup containing A. It is curious how "small" this subgroup can get, but the intuition here is that in this subgroup, all elements should be expressible in terms of A and nothing else (otherwise it can be "reduced" by eliminating the extra elements).

Proposition 3.2.6 ▸ Generated Subgroup Criterion

Let G be a group and $A \subseteq G$ be a subset. Define

$$\overline{A} := \left\{\prod_{i=1}^{n} a_i^{e_i} : n\in\mathbb{N}, a_i\in A, e_i=\pm 1\right\},$$

then $\langle A\rangle = \overline{A}$.

Proof. Note that $1\in\overline{A}$ so $\overline{A}\neq\varnothing$. Take any $a,b\in\overline{A}$, then there exists some $m,n\in\mathbb{N}$ such that

$$a=\prod_{i=1}^{n} a_i^{e_i} \quad\text{and}\quad b=\prod_{i=1}^{m} b_i^{f_i},$$

where $a_1, a_2, \cdots, a_n, b_1, b_2, \cdots, b_m \in A$ and $e_i, f_i = \pm 1$. Note that

$$ab^{-1} = \prod_{i=1}^{m+n} c_i^{p_i}$$

where

$$c_i = \begin{cases} a_i & \text{if } i \leq n \\ b_i & \text{if } n < i \leq n+m \end{cases} \quad \text{and} \quad \begin{cases} p_i = e_i & \text{if } i \leq n \\ p_i = f_i & \text{if } n < i \leq n+m \end{cases}.$$

Therefore, $ab^{-1} \in \overline{A}$ and so by Proposition 3.2.1, $\overline{A}$ is a subgroup and so $\langle A \rangle \leq \overline{A}$. Let $H \leq G$ be any subgroup containing A, then the elements of A are closed under the binary operation in H and so $\overline{A} \leq H$. Therefore, $\overline{A} = \langle A \rangle$. □

3.3 Finite Groups

Trivially, the trivial group is the only group of cardinality 1 and it has a unique subgroup (which is itself). More interestingly, we can show that there exists a unique group of cardinality 2.

Proposition 3.3.1 ▸ Uniqueness of Group of Cardinality 2

There exists a unique group of cardinality 2 *up to isomorphism.*

Proof. Let $G := \{1, a\}$ with $a^2 = 1$, then G is clearly a group. Suppose on contrary that $G' := \{1, a'\}$ is a group with $G' \neq G$, then ${a'}^2 \neq 1$, which implies that ${a'}^2 = a'$ and so $a' = 1$. However, this means that $|G'| = 1$, which is a contradiction. □

Surprisingly this uniqueness extends to groups of cardinality 3.

Proposition 3.3.2 ▸ Uniqueness of Group of Cardinality 3

There exists a unique group of cardinality 3 *up to isomorphism.*

Proof. Sudoku. □

In particular, the group of cardinality 3 has the following multiplication table:

G	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

By observation, it is clear that any subset of cardinality 2 is not compatible with the binary operation on this group, which leads to the following conclusion:

Proposition 3.3.3 ▸ Subgroups of the Group of Cardinality 3

Let G be the group of cardinality 3. If $H \leq G$, then either $H = \{1\}$ or $H = G$.

Proof. Left as an exercise to the reader. □

We can continue our exploration onto groups of cardinality 4.

Proposition 3.3.4 ▸ Uniqueness of Groups of Cardinality 4

There exists exactly 2 distinct groups of cardinality 4 up to isomorphism.

Proof. Left as an exercise to the reader. □

With some effort, we can construct the following multiplication tables for the 2 groups of cardinality 4:

G_1	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

G_2	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

Based on this, we can list down all the possible subgroups of the groups of cardinality 4.

Proposition 3.3.5 ▸ Subgroups of the Groups of Cardinality 4

Let G_1 and G_2 be groups of cardinality 4 with multiplication tables:

G_1	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

G_2	1	a	b	c
1	1	a	b	c
a	a	b	c	1 ,
b	b	c	1	a
c	c	1	a	b

then the only subgroups of G_1 are $\{1\}$, $\{1, a\}$, $\{1, b\}$, $\{1, c\}$, G_1 and the only subgroups of G_2 are $\{1\}$, $\{1, b\}$ and G_2.

Proof. Left as an exercise to the reader. □

4 Cyclic Groups

4.1 Residue Classes

We start by considering an infinite arithmetic progression $\{a + kn \colon k \in \mathbb{Z}\}$ for some fixed $a \in \mathbb{Z}$. It is clear that the terms in this sequence are pairwise congruent modulo n with a remainder of a.

Definition 4.1.1 ▸ Residue Class

Let $n \in \mathbb{Z}$. For every $a \in \mathbb{Z}$, the set

$$\bar{a} := a + n\mathbb{Z} = \{a + kn \colon k \in \mathbb{Z}\}$$

is called a **residue class** of a modulo n. We denote

$$\mathbb{Z}/n\mathbb{Z} := \{\bar{a} \colon a \in \mathbb{Z}\}.$$

It is clear that for any $x, y \in \bar{a}$, we have $x \equiv y \mod n$. Therefore, $\mathbb{Z}/n\mathbb{Z}$ is intuitively the set of all equivalence classes of $\mathbb{Z}$ modulo n. This leads to the following result:

Proposition 4.1.2 ▸ Cardinality of Residue Class

For every $n \in \mathbb{N}$, we have $|\mathbb{Z}/n\mathbb{Z}| = n$.

Proof. Define $A := \{0, 1, 2, \cdots, n-1\}$ and $f \colon A \to \mathbb{Z}/n\mathbb{Z}$ by $f(a) = \bar{a}$. Let $a, b \in A$ be such that $f(a) = f(b)$, then $\bar{a} = \bar{b}$. This means that $a \in \bar{b}$ and so there exists some $k \in \mathbb{Z}$ such that $a = b + kn$. However, $0 \leq a, b < n$, so $k = 0$ and so $a = b$. Therefore, f is injective. Take any $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$. Note that there exists some $q \in \mathbb{Z}$ and $r \in \{0, 1, 2, \cdots, n-1\}$ such that $a = qn + r$. Take any $x \in \bar{a}$, then there exists some $k_1 \in \mathbb{Z}$ such that

$$x = a + kn = (q + k)\, n + r \in \bar{r}$$

and so $\bar{a} \subseteq \bar{r}$. Take any $y \in \bar{r}$, then there exists some $k_2 \in \mathbb{Z}$ such that

$$y = r + kn = a + (k - q)\, n \in \bar{a}$$

and so $\bar{r} \subseteq \bar{a}$. Therefore, $\bar{a} = \bar{r} = f(r)$ and so f is surjective. Therefore, f is a bijection and so $|\mathbb{Z}/n\mathbb{Z}| = |A| = n$. □

Remark. Combining Propositions 4.1.2 and 1.1.19, there exists a bijection $\mathbb{Z}/p\mathbb{Z} \to \mathbb{F}_p$ if $p \in \mathbb{Z}$ is a prime.

Note that there is a natural homomorphism from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ that maps each integer to its residue class.

Definition 4.1.3 ▸ Reduction-Modulo-n Map

For each $n \in \mathbb{Z}$, the **reduction-modulo-n map** $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is defined by $\pi(a) = \bar{a}$.

It is clear that such a map will send 1 to $\bar{1}$. However, surprisingly it is the only homomorphism with this property.

Proposition 4.1.4 ▸ Reduction-Modulo-n Map as the Canonical Epimorphism

The reduction-modulo-n map $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is the unique group homomorphism such that $\pi(1) = \bar{1}$.

Proof. Let $\varphi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be any group homomorphism such that $\varphi(1) = \bar{1}$, then for any $a \in \mathbb{Z}$,

$$\varphi(a) = \varphi\left(\sum_{i=1}^{a} 1\right) = \sum_{i=1}^{a} \varphi(1) = \sum_{i=1}^{a} \bar{1} = \bar{a}.$$

Therefore, $\varphi = \pi$ and so π is unique. □

A key observation by far is that $\mathbb{Z} = \langle 1 \rangle$, so the image of 1 under a group homomorphism in fact completely determines the image of any integer under the homomorphism. Therefore, given the image of 1, the group homomorphism is fully specified, which generalises Proposition 4.1.4 into the universal property for $\mathbb{Z}$.

Theorem 4.1.5 ▸ Universal Property of the Additive Group on the Integers

For any group G and any $x \in G$, there exists a unique group homomorphism $\varphi\colon \mathbb{Z} \to G$ such that $\varphi(1) = x$.

Proof. Define $\varphi\colon \mathbb{Z} \to G$ by $\varphi(n) = x^n$, then clearly $\varphi(1) = x$. One may check that φ is indeed a group homomorphism. Let $\psi\colon \mathbb{Z} \to G$ be any group homomorphism such that $\psi(1) = x$, then for any $a \in \mathbb{Z}$, we have

$$\psi(a) = \psi\left(\sum_{i=1}^{a} 1\right) = \sum_{i=1}^{a} \psi(1) = a \cdot x = a \cdot \varphi(1) = \varphi(a).$$

Therefore, $\psi = \varphi$ and so φ is unique. □

Based on the above theorem, once we fix the image of the unit element under a group homomorphism $\mathbb{Z} \to G$, we will then be able to express everything in $\langle x \rangle$ as an image of some integer. A direct consequence of this is that it justifies the notation for double exponentiation.

Corollary 4.1.6 ▸ Exponential Arithmetic in Groups

For any group G and any $x \in G$, we have $(x^a)^b = x^{ab}$ for all $a, b \in \mathbb{Z}$.

Proof. By Theorem 4.1.5, there exists a unique group homomorphism $\psi\colon \mathbb{Z} \to G$ such that $\psi(1) = x$. Define $\varphi_k\colon \mathbb{Z} \to \mathbb{Z}$ by $\varphi_k(n) = kn$, then φ is clearly a group homomorphism and so $\varphi_a \circ \varphi_b = \varphi_{ab}$. Note that

$$(\psi \circ \varphi_a) \circ \varphi_b = \psi \circ \varphi_{ab}\colon \mathbb{Z} \to G$$

is a group homomorphism. Observe that $\psi \circ \varphi_a\colon \mathbb{Z} \to G$ is the unique group homomorphism such that $(\psi \circ \varphi_a)(1) = x^a$, so

$$\begin{aligned}
(x^a)^b &= (\psi \circ \varphi_a)(b) \\
&= (\psi \circ \varphi_a)(\varphi_b(1)) \\
&= ((\psi \circ \varphi_a) \circ \varphi_b)(1) \\
&= (\psi \circ \varphi_{ab})(1) \\
&= \psi(\varphi_{ab}(1)) \\
&= \psi(ab) \\
&= \psi(1)^{ab} \\
&= x^{ab}.
\end{aligned}$$

□

4.2 Cyclic Groups

$\mathbb{Z}/n\mathbb{Z}$ is one example of a group that is generated by a single element of the group.

Definition 4.2.1 ▸ Cyclic Subgroup

Let G be a group. For any $x \in G$, the **cyclic subgroup** of G generated by x is the subset

$$\langle x \rangle := \{x^n : n \in \mathbb{Z}\}.$$

If there exists some $g \in G$ such that $\langle g \rangle = G$, then G is said to be **cyclic**.

Remark. In the above definition, the element $g \in G$ with $\langle g \rangle = G$ is not unique in general. For example, $\langle g \rangle = \langle g^{-1} \rangle$ for all $g \in G$.

Let us consider some simple examples. First, $(\mathbb{Z}, +)$ is clearly cyclic because $\mathbb{Z} = \langle 1 \rangle$. It is easy to see that all cyclic groups are Abelian, so groups like S_3 and D_8 are not cyclic.

Proposition 4.2.2 ▸ Cyclic Groups Are Abelian

Every cyclic group is Abelian.

Proof. Trivial. □

Note that it is possible that $x^a = x^b$ in a cyclic group for $a \neq b$. In such cases, a cyclic group could be finite. Now, an interesting question is whether we can construct cyclic groups of arbitrary order.

Theorem 4.2.3 ▸ Existence of Cyclic Groups of Arbitrary Order

For every $n \in \mathbb{N}$, there exists a cyclic group of order n.

Proof. Define

$$\bar{a} + \bar{b} = \overline{a + b}.$$

It is clear that $\overline{a + b} \in \mathbb{Z}/n\mathbb{Z}$ for any $a, b \in \mathbb{Z}$. Note that

$$\bar{a} + \bar{0} = \bar{0} + \bar{a} = \bar{a},$$

so $\bar{0}$ is the identity. Moreover, for each $a \in \mathbb{Z}$, we have

$$\bar{a} + \overline{-a} = \overline{-a} + \bar{a} = \bar{0},$$

so $\overline{-a} = \bar{a}^{-1}$ for all $a \in \mathbb{Z}$. Therefore, $(\mathbb{Z}/n\mathbb{Z}, +)$ is a group for all $n \in \mathbb{Z}$. For every $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ with $k \geq 0$, we have

$$\overline{k} = \sum_{i=1}^{k} \overline{1} = k \cdot \overline{1}.$$

For each $k \in \mathbb{Z}^-$, we have

$$\overline{k} = \overline{-k}^{-1} = -\left(-k \cdot \overline{1}\right) = k \cdot \overline{1}.$$

Therefore, $\mathbb{Z}/n\mathbb{Z} = \langle \overline{1} \rangle$ and is a cyclic group of order n. □

Beside knowing the existence of cyclic groups of arbitrarily large finite orders, the following result gives a concrete way to construct one cyclic group of any given finite order.

Proposition 4.2.4 ▸ Construction of Cyclic Groups

Let G be a group. Fix $x \in G$ and let $\varphi\colon \mathbb{Z} \to G$ be the unique group homomorphism with $\varphi(1) = x$, then

$$\operatorname{im}(\varphi) = \langle x \rangle \leq G$$

and

$$\ker(\varphi) = \begin{cases} n\mathbb{Z} & \text{if } |x| = n \in \mathbb{Z}^+ \\ \{0\} & \text{otherwise} \end{cases}.$$

Proof. It is clear that for each $g \in G$, we have $g \in \langle x \rangle$ if and only if $g = x^k = \varphi(k)$ for some $k \in \mathbb{Z}$. Conversely, $\varphi(k) = x^k \in \langle x \rangle$ for all $k \in \mathbb{Z}$, and so $\operatorname{im}(\varphi) = \langle x \rangle$. Consider

$$\varphi(0) = \varphi(1-1) = \varphi(1)\,\varphi(-1) = \varphi(1)\,\varphi(1)^{-1} = 1,$$

so $0 \in \ker(\varphi)$. If x has infinite order, then for any $n \in \mathbb{Z}^+$, we have $x^n \neq 1$ and so $x^{-n} = (x^n)^{-1} \neq 1$. Therefore, $\ker(\varphi) = \{0\}$. If there exists some $n \in \mathbb{Z}^+$ such that $|x| = n$, then $x^n = 1$. For any $z \in n\mathbb{Z}$, there exists some $k \in \mathbb{Z}$ such that $z = kn$, and so

$$\varphi(z) = \varphi(n)^k = (x^n)^k = 1^k = 1.$$

Therefore, $n\mathbb{Z} \subseteq \ker(\varphi)$. By the division algorithm, for any $z \in \ker(\varphi)$, there exists some $q \in \mathbb{Z}$ and $r \in \{0, 1, 2, \cdots, n-1\}$ such that $z = qn + r$. Note that

$$1 = \varphi(qn + r) = \varphi(n)^q + \varphi(1)^r = 1 + x^r.$$

Since for any $r \in \{1, 2, \cdots, n-1\}$, we have $x^r \neq 1$, so $r = 0$. Therefore, $z = qn \in n\mathbb{Z}$ and so $\ker(\varphi) \leq n\mathbb{Z}$. Hence, $\ker(\varphi) = n\mathbb{Z}$. □

Intuitively, for a group homomorphism φ with $n\mathbb{Z}$ as the kernel, we may view it to have a certain "periodic" behaviour such that it self-loops back to the identity over and over again. Clearly, this implies that there are only finitely many distinct choices for $\varphi(x)$, which can be formalised to the following result:

Corollary 4.2.5 ▸ Order of Cyclic Subgroup

Let G be a group. For any $x \in G$,

- *if x is of infinite order, then $\langle x \rangle$ is infinite;*
- *if $|x| = n \in \mathbb{Z}^+$, then $|\langle x \rangle| = n$.*

Proof. Let $\varphi\colon \mathbb{Z} \to G$ be the group homomorphism with $\varphi(1) = x$. Suppose on contrary that $x \in G$ is of infinite order but $\langle x \rangle$ is finite, then

$$N := \max\left\{n \in \mathbb{Z}^+ : x^n \in \langle x \rangle \text{ and } x^k \neq x^n \text{ for all } k \in \mathbb{Z}^+ \text{ and } k < n\right\}$$

exists. By the maximality of N, there is some $k \in \{1, 2, \cdots, N\}$ such that $x^{N+1} = x^k$, and so

$$\varphi(N + 1 - k) = x^{N+1-k} = 1_G.$$

This implies that $N + 1 - k \in \ker(\varphi)$. By Proposition 4.2.4, $\ker(\varphi) = \{0\}$ and so we have $N + 1 = k$, which is a contradiction. Therefore, $\langle x \rangle$ is infinite. If $|x| = n \in \mathbb{Z}^+$, by Proposition 4.2.4 we have

$$x^{nk} = \varphi(nk) = 1_G \qquad \text{for all } k \in \mathbb{Z}.$$

Therefore, for any $r \in \{0, 1, 2, \cdots, n-1\}$, we have $x^{nk+r} = x^r$ for all $k \in \mathbb{Z}$. We claim that for any $r_1, r_2 \in \{0, 1, 2, \cdots, n-1\}$ with $r_1 \neq r_2$, we have $x^{r_1} \neq x^{r_2}$. Suppose on contrary that $x^{r_1} = x^{r_2}$, then

$$\varphi(r_2 - r_1) = x^{r_2 - r_1} = 1_G.$$

This means that $r_2 - r_1 \in \ker(\varphi) = n\mathbb{Z}$, which is a contradiction since $|r_2 - r_1| < n$. Therefore,

$$\langle x \rangle = \left\{1_G, x, x^2, \cdots, x^{n-1}\right\}$$

and so $|\langle x \rangle| = n$. □

Intuitively, any cyclic group is at most countably infinite. Therefore, for any two infinite cyclic groups, we can "align" their "seeds" and so elements generated by the same power will be matched to each other perfectly.

Corollary 4.2.6 ▸ Infinite Cyclic Groups Are Isomorphic

The infinite cyclic group is unique up to isomorphism.

Proof. It suffices to prove that any infinite cyclic group $G := \langle x \rangle$ is such that $G \cong \mathbb{Z}$. Since G is infinite, by Corollary 4.2.5, x is of infinite order. By Theorem 4.1.5, there exists a unique homomorphism $\varphi \colon \mathbb{Z} \to G$ such that $\varphi(1) = x$. By Proposition 4.2.4, $\operatorname{im}(\varphi) = \langle x \rangle = G$ so φ is surjective. It is clear that φ is injective and so it is an isomorphism. Therefore, $G \cong \mathbb{Z}$. □

Intuitively, an infinite cyclic group has infinitely many cyclic subgroups because we can just pick any "step size" and generate the group. Formally, this is formulated as below:

Proposition 4.2.7 ▸ Cyclic Subgroups of Infinite Cyclic Groups

If $G := \langle x \rangle$ is an infinite cyclic group, then the map $\Phi \colon \mathbb{N} \to \{H \colon H \leq G\}$ defined by $\Phi(a) = \langle x^a \rangle$ is a bijection.

Proof. Let $\varphi \colon \mathbb{Z} \to G$ be the unique isomorphism such that $\varphi(1) = x$, then the map $\psi \colon \{K \colon K \leq \mathbb{Z}\} \to \{H \colon H \leq G\}$ defined by $\psi(K) = \varphi[K]$ is a bijection. Let K be any subgroup of $\mathbb{Z}$ and take $a \in K$ to be the smallest positive integer in K, then it is clear that $a\mathbb{Z} \leq K$. Suppose that there exists some $b \in K - a\mathbb{Z}$, then there exists $r, q \in \mathbb{Z}$ with $1 \leq r \leq a - 1$ such that $b = aq + r$. However, this means that $r \in K$ which is a contradiction to the minimality of a. Therefore, every subgroup of $\mathbb{Z}$ is of the form of $a\mathbb{Z}$ for some $a \in \mathbb{N}$. It is clear that the map $\eta \colon \mathbb{N} \to \{K \colon K \leq \mathbb{Z}\}$ defined by $\eta(a) = a\mathbb{Z}$ is a bijection, and so $\Phi = \psi \circ \eta$ is a bijection. □

Remark. The inverse map of Φ is

$$\Phi^{-1}(K) = \begin{cases} 0 & \text{if } K = \{1\} \\ \operatorname{argmin}_{a \in \mathbb{Z}^+} \{x^a \in K\} & \text{if } K \neq \{1\} \end{cases}.$$

We will study finite cyclic groups in more detail now. One such example is $\mathbb{Z}/n\mathbb{Z}$. By 4.1.5, there is a unique homomorphism $\pi \colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ such that $\pi(1) = \bar{1}$.

Remark. One can check that $\operatorname{im}(\pi) = \mathbb{Z}/n\mathbb{Z}$ and $\ker(\pi) = n\mathbb{Z}$.

It is clear that if a cyclic group is finite, the terms x^k will "cycle back and forth" and exhibits a periodic behaviour. In general, we have the following result:

Proposition 4.2.8 ▸ Periodicity in Groups

Let G be a group and $x \in G$. If there exist $a, b \in \mathbb{Z}$ such that $x^a = x^b = 1$, then we have $x^{\gcd(a,b)} = 1$.

Proof. By Bézout's Identity, there exists $r, s \in \mathbb{Z}$ such that $ar + bs = \gcd(a, b)$. Therefore,

$$x^{\gcd(a,b)} = x^{ar+bs} = (x^a)^r \left(x^b\right)^s = 1.$$

□

Intuitively, if it "takes d steps" for x to cycle back to 1, then any multiples of d is a valid step size to cycle from x back to 1.

Corollary 4.2.9 ▸ Order of Elements in Groups

Let G be a group and $x \in G$, then there exists some $n \in \mathbb{Z}$ such that $x^n = 1$ if and only if $|x| = d \in \mathbb{Z}$ such that $d \mid n$.

Proof. Suppose that there exists $n \in \mathbb{Z}$ such that $x^n = 1$, then $d := |x| \leq n$ is finite. By Proposition 4.2.8, we have

$$x^{\gcd(n,d)} = 1.$$

Note that $\gcd(n, d) \leq d$ but $|x| \leq \gcd(n, d)$, so $d = \gcd(n, d)$ and $d \mid n$. Suppose conversely that $|x| = d \mid n$, then there exists some $k \in \mathbb{Z}$ such that $n = kd$ and so

$$x^n = x^{kd} = \left(x^d\right)^k = 1.$$

□

Analogously to $\mathbb{Z}$, we can formulate the universal property for $\mathbb{Z}/n\mathbb{Z}$ as follows:

Theorem 4.2.10 ▸ Universal Property of $\mathbb{Z}/n\mathbb{Z}$

For any group G and any $x \in G$ with $x^n = 1$ for some $n \in \mathbb{Z}$, there exists a unique homomorphism $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to G$ such that $\varphi\left(\overline{1}\right) = x$.

Proof. Define φ by $\varphi(\xi) = x^a$ if and only if $\xi = \overline{a}$. We first show that φ is well-defined. Consider $a, a' \in \mathbb{Z}$ such that $\xi = \overline{a} = \overline{a'}$, then $a - a' \in \ker(\pi) = n\mathbb{Z}$ where π is the reduction-modulo-n map. This means that there exists some $k \in \mathbb{Z}$ such that $a - a' = nk$ and so

$$x^{a-a'} = (x^n)^k = 1.$$

Therefore, $x^a = x^{a'}$. It is clear that $\varphi\left(\overline{1}\right) = x$, so it suffices to prove that φ is a homomorphism. Take any $\xi, \eta \in \mathbb{Z}/n\mathbb{Z}$ such that $\xi = \bar{a}$ and $\eta = \bar{b}$, then $\xi + \eta = \overline{a+b}$ and so

$$\varphi(\xi + \eta) = x^{a+b} = x^a x^b = \varphi(\xi)\varphi(\eta),$$

which implies that φ is a homomorphism. Suppose that $\psi\colon \mathbb{Z}/n\mathbb{Z} \to G$ is any homomorphism such that $\psi(\bar{1}) = x$. We prove that $\psi(\bar{a}) = \varphi(\bar{a})$ for all $a \in \mathbb{N}$ by induction. For $a = 0$, clearly $\psi(\bar{0}) = 1 = \varphi(\bar{0})$. Assume that there exists some $k \in \mathbb{N}$ with $\psi(\bar{k}) = \varphi(\bar{k})$, then

$$\psi(\bar{k} + \bar{1}) = \psi(\bar{k})\psi(\bar{1}) = \varphi(\bar{k})\varphi(\bar{1}) = \varphi(\bar{k} + \bar{1}).$$

Therefore, $\varphi = \psi$ and so φ is unique. □

Fix $x \in G$. Notice that there is a unique homomorphism $\phi\colon \mathbb{Z} \to G$ with $\phi(1) = x$ and the reduction-modulo-n map $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is the unique homomorphism such that $\pi(1) = \bar{1}$. Therefore, by Theorem 4.2.10 it is clear that ϕ can be written as a composition $\phi = \varphi \circ \pi$.

Remark. In a way, this can be viewed as first "projecting" the infinite group $\mathbb{Z}$ onto a finite group $\mathbb{Z}/n\mathbb{Z}$ using residue classes.

Intuitively, $\mathbb{Z}/n\mathbb{Z}$ is a finite cyclic group, so by "embedding" it to G through the unique homomorphism, we expect the image to be a finite cyclic subgroup.

Proposition 4.2.11 ▸ Construction of Finite Cyclic Subgroups

Let G be a group with $x \in G$ such that $x^n = 1$ for some $n \in \mathbb{Z}$. Let $\varphi\colon \mathbb{Z}/n\mathbb{Z}$ be the unique homomorphism such that $\varphi(\bar{1}) = x$, then

1. $\operatorname{im}(\varphi) = \langle x \rangle \leq G$;
2. $\ker(\varphi) = \langle |x| \rangle \leq \mathbb{Z}/n\mathbb{Z}$.

Proof. It is clear that $\operatorname{im}(\varphi) \subseteq \langle x \rangle$. For any $x^a \in \langle x \rangle$, we have $\varphi(\bar{a}) = x^a$ and so $\langle x \rangle \subseteq \operatorname{im}(\varphi)$, which implies that $\operatorname{im}(\varphi) = \langle x \rangle$.

Let $\phi\colon \mathbb{Z} \to G$ be the unique homomorphism such that $\phi(1) = x$. By Proposition 4.2.4, $\ker(\phi) = |x|\mathbb{Z}$. Take any $\bar{a} \in \ker(\varphi)$, then

$$1 = \varphi(\bar{a}) = x^a = \phi(a),$$

so $a \in \ker(\phi)$. Therefore, there exists some $k \in \mathbb{Z}$ such that $a = k|x|$ and so $\bar{a} =$

$\overline{k|x|} \in \langle |x| \rangle$. Notice that for any $\overline{k|x|} \in \langle |x| \rangle$, we have

$$\varphi\left(\overline{k|x|}\right) = \varphi\left(|x|\right)^k = 1$$

because $x^{|x|} = 1$. Therefore, $\overline{k|x|} \in \ker(\varphi)$ and so $\ker(\varphi) = \langle |x| \rangle$. □

By taking the group used in the above proposition to be a finite cyclic group, we can prove that any finite cyclic group is equivalent to some residue group modulo n.

Theorem 4.2.12 ▸ Uniqueness of Finite Cyclic Groups

The finite cyclic group of order n is unique up to isomorphism.

Proof. Let $G := \langle x \rangle$ be any finite cyclic group of order n, then $|x| = n$ by Corollary 4.2.9. Let $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to G$ be the unique homomorphism with $\varphi\left(\bar{1}\right) = x$. By Proposition 4.2.11, we know that $\operatorname{im}(\varphi) = \langle x \rangle = G$ and $\ker(\varphi) = \langle \bar{n} \rangle = \left\{\bar{0}\right\}$, so φ is an isomorphism. Therefore, $G \cong \mathbb{Z}/n\mathbb{Z}$. □

Intuitively, each factor $d \mid n$ for a cyclic group of order n induces a "path" to cycle back to 1. This motivates the following result:

Proposition 4.2.13 ▸ Cyclic Subgroups of Finite Cyclic Groups

If $G := \langle x \rangle$ is a finite cyclic group, then the map $\Phi\colon \{a \in \mathbb{N} \colon a \mid n\} \to \{H \colon H \leq G\}$ defined by $\Phi(a) = \langle x^a \rangle$ is a bijection.

Proof. Let $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to G$ be the unique isomorphism such that $\varphi\left(\bar{1}\right) = x$, then the map $\psi\colon \{K \colon K \leq \mathbb{Z}/n\mathbb{Z}\} \to \{H \colon H \leq G\}$ defined by $\psi(K) = \varphi[K]$ is a bijection. Let K be any subgroup of $\mathbb{Z}/n\mathbb{Z}$ and take $a := \operatorname{argmin}_{a\in\mathbb{N}} \{\bar{a} \in K\}$, then it is clear that $\left\{\overline{ka} \colon k \in \mathbb{Z}\right\} \leq K$. Suppose that there exists some $\bar{b} \in K - \left\{\overline{ka} \colon k \in \mathbb{Z}\right\}$, then there exists $r, q \in \mathbb{Z}$ with $1 \leq r \leq a - 1$ such that $b = aq + r$. However, this means that $\bar{r} \in K$ which is a contradiction to the minimality of a. Therefore, every subgroup of $\mathbb{Z}$ is of the form of $\left\{\overline{ka} \colon k \in \mathbb{Z}\right\}$ for some $a \in \mathbb{N}$. It is clear that the map $\eta\colon \mathbb{N} \to \{K \colon K \leq \mathbb{Z}/n\mathbb{Z}\}$ defined by $\eta(a) = \left\{\overline{ka} \colon k \in \mathbb{Z}\right\}$ is a bijection, and so $\Phi = \psi \circ \eta$ is a bijection. □

Remark. The inverse map of Φ is

$$\Phi^{-1}(K) = \operatorname*{argmin}_{a\in\mathbb{N}} \{x^a \in K\}.$$

By observing $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$, an intuition is the the subgroups of a cyclic group seem to have to be cyclic as well. It is clear that this is a direct result based on Propositions 4.2.7 and 4.2.13.

Proposition 4.2.14 ▸ Subgroups of Cyclic Groups Are Cyclic

Every subgroup of a cyclic group is cyclic.

Note that the representation of a cyclic group might not be unique. However, there are certain conditions under which an element $x \in G$ is such that $G = \langle x \rangle$. Intuitively, when the binary operation on G is applied to (x, x), the "distance travelled" must be the "step size" between distinct elements in the cyclic group.

Proposition 4.2.15 ▸ Conditions of the Generators of Cyclic Groups

Let $G := \langle x \rangle$ be a cyclic group.

1. *If G is infinite, then $G = \langle x^a \rangle$ if and only if $a = \pm 1$.*
2. *If G is finite of order n, then $G = \langle x^a \rangle$ if and only if $\gcd(a, n) = 1$.*

5 Quotient Groups

5.1 Cosets

Given any subgroup H in a group G, we can fix an element g and map each element in H by applying left-multiplication by g. This structure is known as a *coset*.

Definition 5.1.1 ▸ Coset

Let G be a group and $H \leq G$. For any $g \in G$, the **left g-coset** of H in G is defined as

$$gH := \{gh \in G \colon h \in H\}$$

and the **right g-coset** of H in G is defined as

$$Hg := \{hg \in G \colon h \in H\} .$$

An element in a coset is called a **representative**.

It is clear that different element can, but not necessarily will, induce different cosets.

Definition 5.1.2 ▸ Set of Cosets

The **set of left cosets** of $H \leq G$ in a group G is defined as

$$G/H := \{gH \colon g \in G\}$$

and the **set of right cosets** denoted by $H \backslash G$ is defined analogously.

We list some common properties of cosets:

Proposition 5.1.3 ▸ Common Properties of Cosets

Let G be a group, $H \leq G$ be a subgroup and $g_1, g_2 \in G$ be any elements, then the followings are equivalent:

1. $g_1 H = g_2 H$;
2. $g_1 \in g_2 H$ *and* $g_2 \in g_1 H$;
3. $g_2^{-1} g_1, g_1^{-1} g_2 \in H$.

Remark. Note that $g_2^{-1}g_1 \in H$ if and only if $g_1^{-1}g_2 \in H$, so we can use $g_2^{-1}g_1 \in H$ as a characterisation for $g_1H = g_2H$.

In a sense, we can say that g_1 and g_2 are "equal" with respect to coset with H. This motivates us to consider some equivalence relation.

Proposition 5.1.4 ▸ Coset Partition of a Group

Let G be a group and $H \leq G$. Define $\sim$ to be a relation on G by $g_1 \sim g_2$ if and only if $g_1H = g_2H$, then $\sim$ is an equivalence relation, $G/H = G/\sim$ and the map $\pi\colon G \to G/H$ defined by $\pi(g) = gH$ is the quotient map.

Proof. Left to the reader as an exercise. □

Intuitively, $|G/H|$ is the number of distinct cosets H can have with respect to the elements of G.

Definition 5.1.5 ▸ Index

Let G be a group with $H \leq G$. The **index** of H is defined as $|G/H|$ and is denoted by $[G : H]$ or $|G\colon H|$.

Naturally, the index should stay consistent regardless of whether we use left- or right-cosets.

Proposition 5.1.6 ▸ Consistency of Index

For any group G and any $H \leq G$, we have $|H\backslash G| = |G/H|$.

Proof. Define $f\colon H\backslash G \to G/H$ by

$$f(X) = X^{-1} := \{x^{-1} \in G\colon x \in X\}.$$

For any $X \in H\backslash G$, there exists some $g \in G$ such that $X = gH$, then

$$\begin{aligned} f(X) &= \{x^{-1} \in G\colon x \in gH\} \\ &= \{h^{-1}g^{-1}\colon h \in H\} \\ &= \{h'g^{-1}\colon h' \in H\} \\ &= Hg^{-1}. \end{aligned}$$

Define $g\colon H/G \to H\backslash G$ by $g(X) = X^{-1}$, then by a similar argument, we can show that $f \circ g = \mathrm{id}_{H/G}$ and $g \circ f = \mathrm{id}_{H\backslash G}$. Therefore, f is a bijection and $|H\backslash G| =$

$|G/H|$. □

Clearly, for any $H \leq G$ and any $h_1, h_2 \in H$ with $h_1 \neq h_2$, we must have $gh_1 \neq gh_2$ by the cancellation laws. Therefore, H, gH and Hg should be equinumerous.

Proposition 5.1.7 ▸ Equinumerous Cosets

For any group G and any $g \in G$, we have $H \approx gH \approx Hg$ for any $H \leq G$.

Proof. Trivial. □

These above results combined give us a powerful way to determine the cardinality of a group.

Theorem 5.1.8 ▸ Lagrange's Theorem

For any group G and any $H \leq G$, we have $|G| = |G : H||H|$.

Proof. By Proposition 5.1.4, $H \backslash G$ is a partition of G, so

$$G = \bigsqcup_{X \in H \backslash G} X$$

and so

$$|G| = \sum_{X \in H \backslash G} |X|.$$

By Proposition 5.1.7, $|X| = |H|$ for any $X \in H \backslash G$ and so $|G| = |G : H||H|$. □

For finite groups, we have the following corollary:

Corollary 5.1.9 ▸ Lagrange's Theorem for Finite Groups

For any finite group G and any $H \leq G$, we have $|H| \mid |G|$.

Proof. Trivial. □

Remark. In particular, for any element $x \in G$, we have $|x| \mid |G|$ because $\langle x \rangle$ is a finite cyclic subgroup, and so $x^{|G|} = 1$.

By the above remark, it is easy to see that if G is finite and its order is prime, then we are left with no choice but to force $\langle x \rangle = \{1\}$ or G.

Corollary 5.1.10 ▸ Prime-Order Finite Groups Are Cyclic

If G is a finite group and $|G|$ is a prime, then G is cyclic.

Proof. Left to the reader as an exercise. □

Remark. A finite group with prime order is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

We can apply Lagrange's Theorem to the following context: consider the "multiplication" operation defined on $\mathbb{Z}/n\mathbb{Z}$ by

$$\bar{x}\cdot\bar{y}=\overline{xy}.$$

This is well-defined and associative over $\mathbb{Z}/n\mathbb{Z}$. However, $(\mathbb{Z}/n\mathbb{Z},\cdot)$ is not a group because some elements do not have an inverse.

Instead, we define $(\mathbb{Z}/n\mathbb{Z})^{\times}\subseteq\mathbb{Z}/n\mathbb{Z}$ to be the maximal subset such that $\left((\mathbb{Z}/n\mathbb{Z})^{\times},\cdot\right)$ is a group.

Proposition 5.1.11 ▸ The Multiplicative Group of $\mathbb{Z}/n\mathbb{Z}$

For any $n\in\mathbb{N}$, we have

$$(\mathbb{Z}/n\mathbb{Z})^{\times}=\{\bar{a}\in\mathbb{Z}/n\mathbb{Z}\colon a\leq n \textit{ and } \gcd(a,n)=1\}.$$

Proof. Take any integer $a\leq n$ coprime to n, then by Bézout's Identity, there exist $s,t\in\mathbb{Z}$ such that $sa+tn=1$. Therefore, $\overline{sa}=\overline{sa+tn}=\bar{1}$. Similarly, $\overline{as}=\bar{1}$. Take any $x\in(\mathbb{Z}/n\mathbb{Z})^{\times}$, then there exists some integer $a\in[0,n-1]$ such that $x=\bar{a}$. Notice that there exists $y:=\bar{b}\in(\mathbb{Z}/n\mathbb{Z})^{\times}$ such that $xy=1$. Therefore, $n\mid ab-1$ and so there exists some $k\in\mathbb{Z}$ such that $ab-kn=1$ and so $\gcd(a,n)=1$. □

Recall that the *Euler-φ function* counts the number of integers coprime to a fixed non-negative integer n, so

$$\varphi(n)=\left|(\mathbb{Z}/n\mathbb{Z})^{\times}\right|.$$

Combining with Lagrange's Theorem implies that for any $x\in(\mathbb{Z}/n\mathbb{Z})^{\times}$,

$$x^{\varphi(n)}=x^{\left|(\mathbb{Z}/n\mathbb{Z})^{\times}\right|}=\bar{1}.$$

In other words, for any integer a coprime to n, we have

$$a^{\varphi(n)}\equiv 1\mod n.$$

By taking $n=p$ to be a prime, we get *Fermat's Little Theorem*: for every $x\in(\mathbb{Z}/p\mathbb{Z})^{\times}$, we have $x^{p-1} = \bar{1}$ and that for any $a \in \mathbb{Z}$,

$$a^p \equiv a \mod p.$$

5.2 Conjugacy Classes

For each $g \in G$, we consider a mapping over itself. In particular, picking any element a, we first apply a left action by g, followed by a right action by g^{-1}. Such a mapping results in the notion of *conjugates*.

Definition 5.2.1 ▸ Conjugate

Let G be a group, then for each pair $(a, g) \in G \times G$, the **g-conjugate** of a is $gag^{-1} \in G$. The **conjugacy class** of a is defined as the set

$$\left\{gag^{-1} \in G \colon g \in G\right\}.$$

For each pair $(A, g) \in \mathcal{P}(G) \times G$, the **$g$-conjugate** of A is defined as

$$gAg^{-1} := \left\{gag^{-1} \in G \colon a \in A\right\}.$$

Things become interesting when this conjugate action happens to be an inclusion map.

Definition 5.2.2 ▸ Centraliser

Let G be a group, the element $g \in G$ is said to **centralise** $a \in G$ if $gag^{-1} = a$. The **centraliser** of $a \in G$ is defined as the set

$$C_G(a) := \left\{g \in G \colon gag^{-1} = a\right\}.$$

g is said to **centralise** $A \subseteq G$ if $gag^{-1} = a$ for all $a \in A$. The **centraliser** of $A \subseteq G$ is defined as the set

$$C_G(A) := \left\{g \in G \colon gag^{-1} = a \text{ for all } a \in A\right\}.$$

Remark. Clearly, $g \in G$ centralises $a \in G$ if and only if $ga = ag$.

It is possible that some $g \in G$ centralises the entire group.

Definition 5.2.3 ▸ Centre

The **centre** of a group G is defined as

$$Z(G) := \left\{g \in G \colon gag^{-1} = a \text{ for all } a \in G\right\}.$$

Similarly, we can consider the mapping $A \mapsto gAg^{-1}$ and focus on the case where this map is an inclusion map.

Definition 5.2.4 ▸ Normaliser

Let G be a group and $A \subseteq G$ be a subset. An element $g \in G$ is said to **normalise** A if $gAg^{-1} = A$. The **normaliser** of A is defined as the set

$$N_G(A) := \left\{g \in G \colon gAg^{-1} = A\right\}.$$

A normaliser of A might not be a centraliser for any $a \in A$ because the normalisation operation could be a permutation of A. However, if $g \in G$ centralises every $a \in A$, then g normalises A. Intuitively, this means that

$$\bigcap_{a \in A} C_G(a) \subseteq N_G(A).$$

However, the converse may not hold. Formally, we have the following properties:

Proposition 5.2.5 ▸ Relationship between Centraliser and Normaliser

For any group G,

1. $C_G(a) = N_G(\{a\})$ *for all* $a \in G$;
2. $C_G(A) = \bigcap_{a \in A} C_G(a) \subseteq N_G(A)$;
3. $Z(G) = C_G(G) = \bigcap_{a \in G} C_G(a)$;
4. $N_G(G) = G$;
5. $C_G(1) = G$.

Proof. Notice that

$$C_G(a) = \left\{g \in G \colon gag^{-1} = a\right\},$$
$$N_G(\{a\}) = \left\{g \in G \colon g\{a\}g^{-1} = \{a\}\right\}.$$

Observe that $g\{a\}g^{-1} = \{a\}$ if and only if $gag^{-1} = a$, so $C_G(a) = N_G(\{a\})$. Take any $g \in C_G(A)$, then $gag^{-1} = a$ for all $a \in A$, and so $g \in C_G(a)$ for every $a \in A$ and $g \in N_G(A)$, which means that $C_G(A) \subseteq \bigcap_{a \in A} C_G(a)$ and $C_G(A) \subseteq N_G(A)$. Take any $g \in \bigcap_{a \in A} C_G(a)$, then $gag^{-1} = a$ for each $a \in A$ and so $g \in C_G(A)$. Therefore, we have $\bigcap_{a \in A} C_G(a) \subseteq C_G(A)$ and so

$$C_G(A) = \bigcap_{a \in A} C_G(a) \subseteq N_G(A).$$

3 is trivial from the definitions. To show 4, it suffices to prove that $G \subseteq N_G(G)$. Take any $g \in G$. For any $x \in G$, define $a := g^{-1}xg \in G$, then clearly $x = gag^{-1}$ and so we have $x \in gGg^{-1}$. Therefore, $G \subseteq gGg^{-1}$ and so $gGg^{-1} = G$. Therefore, we have $g \in N_G(G)$. To show 5, it suffices to prove that $G \subseteq C_G(1)$. For any $g \in G$, it is clear that $g1g^{-1} = gg^{-1} = 1$, so $g \in C_G(1)$, which implies that $G \subseteq C_G(1)$. □

It is obvious that if G is an Abelian group, then every element of G centralises everything in G. This leads to a series of interesting and important properties.

Proposition 5.2.6 ▸ Centre Characterisation of Abelian Groups

For every group G, the followings are equivalent:

1. *G is Abelian;*
2. *$Z(G) = G$;*
3. *$C_G(a) = G$ for all $a \in G$;*
4. *$C_G(A) = N_G(A) = G$ for all $A \subseteq G$.*

Proof. Suppose that G is Abelian, to show that $Z(G) = G$, it suffices to prove that $G \subseteq Z(G)$. Take any $g \in G$, then for all $a \in G$, we have $ga = ag$ and so $gag^{-1} = a$, which means that $g \in Z(G)$. Therefore, $G \subseteq Z(G)$ and so $Z(G) = G$.

Suppose that $Z(G) = G$, for any $a \in G$, to show that $C_G(a) = G$, it suffices to prove that $G \subseteq C_G(a)$. Take any $g \in G \subseteq Z(G)$, then $gag^{-1} = a$ for all $a \in G$. Therefore, $g \in C_G(a)$ for all $a \in G$. Therefore, $G \subseteq C_G(a)$ and so $C_G(a) = G$ for all $a \in G$.

Suppose that $C_G(a) = G$ for all $a \in G$. Take any $A \subseteq G$. By Proposition 5.2.5, we already know that $C_G(A) \subseteq N_G(A)$. It is clear that $N_G(A) \subseteq G$. Fix some $a \in A$, then $G = C_G(a) \subseteq C_G(A)$, which means that

$$C_G(A) \subseteq N_G(A) \subseteq G \subseteq C_G(A),$$

and so $C_G(A) = N_G(A) = G$.

Suppose that $C_G(A) = N_G(A) = G$ for all $A \subseteq G$. Take $A = G$, then for any $g \in G$, since $g \in G = C_G(G)$, we have $gag^{-1} = a$ for all $a \in G$, and so $ga = ag$. Therefore, G is Abelian. □

The following proposition shows that every centraliser or normaliser is a subgroup.

Proposition 5.2.7 ▸ Centraliser and Normaliser as Subgroups

Let G be a group. For all $A \subseteq G$, we have $C_G(A), N_G(A) \leq G$.

Proof. For every $A \subseteq G$, we have $1a1^{-1} = a$ for all $a \in A$ and $1A1^{-1} = A$, so we have $1 \in C_G(A)$ and $1 \in N_G(A)$. This means that $C_G(A), N_G(A) \neq \varnothing$. Take any $g_1, g_2 \in C_G(A)$, then

$$g_1 a g_1^{-1} = a \quad \text{and} \quad g_2 a g_2^{-1} = a$$

for all $a \in A$. Consider

$$\left(g_1 g_2^{-1}\right) a \left(g_1 g_2^{-1}\right)^{-1} = g_1 g_2^{-1} a g_2 g_1^{-1} = a,$$

so $g_1 g_2^{-1} \in C_G(A)$. By Proposition 3.2.1, $C_G(A) \leq G$. Similarly, $N_G(A) \leq G$. □

5.3 Quotient Groups

Now we consider applying the conjugate action not on any set, but on a subgroup instead. Recall that every $g \in G$ normalises G, but G it not the only subgroup which is normalised by all elements. In particular, subgroups normalised by any element is called *normal*.

Definition 5.3.1 ▸ Normal Subgroup

Let G be a group. A subgroup $N \subseteq G$ is **normal** if $gNg^{-1} = N$ for all $g \in G$, denoted by $N \trianglelefteq G$.

In fact, it turns out that the equality can be implied by simply having a one-directional inclusion.

Proposition 5.3.2 ▸ Characterisation of Normal Subgroups

Let G be a group. A subgroup $N \leq G$ is normal if and only if $gNg^{-1} \subseteq N$ for all $g \in G$.

One can prove that the alternating group A_n is a proper normal subgroup of S_n.

Next, we introduce some preliminary notations:

Definition 5.3.3 ▸ Product and Inverse of Subgroups

Let G be a group and $X \leq G$ be a subgroup, then the **inverse** of X is defined by

$$X^{-1} := \left\{x^{-1} \colon x \in X\right\}.$$

If $Y \leq G$ is a subgroup, then the **product** of X and Y is defined by

$$XY := \{xy \in G \colon x \in X, y \in Y\}.$$

Here is a fact: for some normal subgroup $N \leq G$, consider the left-cosets G/N and take any $X_1, X_2 \in G/N$. Note that we can choose any $g_1 \in X_1$ and $X_1 = g_1N$. Similarly, $X_2 = g_2N$ for any $g_2 \in X_2$. One can check that $X_1X_2 = g_1g_2N \in G/N$.

> *Remark.* One can show that such a binary operation is well-defined if and only if N is a normal subgroup.

At the same time, the inverse of a coset $X \in G/N$ is simply $g^{-1}N \in G/N$ for any $g \in X$.

Clearly, the above defines a binary operation under which the left-cosets are closed and a way to define the inverse of a left-coset. By augmenting them into the set G/N, we should have a group.

Definition 5.3.4 ▸ Quotient Group

Let G be a group and $N \trianglelefteq G$ be a normal subgroup. The **quotient group of G modulo N** is the group $(G/N, \cdot)$.

> *Remark.* It is clear that the identity of a quotient group is N.

Observe that for each $g \in G$ and any quotient group G/N, we have $g \in gN$, so we can view each coset gN as a "labelling" of the element $g \in G$ representing the set it belongs to after the partitioning. Such a labelling is clearly a map.

Definition 5.3.5 ▸ Quotient Map

Let G be a group and $N \trianglelefteq G$ be a normal subgroup. The map $\pi \colon G \to G/N$ defined by $\pi(g) = gN$ is called the **quotient map**.

> *Remark.* It is obvious that every quotient map is surjective.

Clearly, the reduction-modulo-n map is a special case of the quotient map. One may check that not only the reduction-modulo-n map, but every quotient map is a group homomorphism.

Definition 5.3.6 ▸ Quotient $\mod N$ Homomorphism

Let G be a group and $N \trianglelefteq G$ be a normal subgroup. The quotient map $\pi\colon G \to G/N$ is called the **quotient $\mod N$ homomorphism**.

Next, we formulate the universal property of the quotient group.

Theorem 5.3.7 ▸ Universal Property of Quotient Groups

Let G be a group and $N \trianglelefteq G$ be a normal subgroup. For any group H and any group homomorphism $\varphi\colon G \to H$ with $N \leq \ker(\varphi)$, there exists a unique group homomorphism $\overline{\varphi}\colon G/N \to H$ such that $\varphi = \overline{\varphi} \circ \pi$.

Proof. Define $\overline{\varphi}(\xi) = \varphi(g)$ if and only if $\pi(g) = \xi$. We first prove that $\overline{\varphi}$ is well-defined. Take any $g_1, g_2 \in G$ with $g_1 \neq g_2$ and $\pi(g_1) = \pi(g_2)$, i.e., $g_1 N = g_2 N = \xi$. It suffices to prove that $\varphi(g_1) = \varphi(g_2)$. Notice that for any $n_1 \in N$, there exists some $n_2 \in N$ such that $g_1 n_1 = g_2 n_2$, so

$$\varphi(g_1)\varphi(n_1) = \varphi(g_2)\varphi(n_2).$$

Since $N \leq \ker(\varphi)$, we have $\varphi(n_1) = \varphi(n_2) = 1$, so $\varphi(g_1) = \varphi(g_2)$. For any $g \in G$, we have

$$(\overline{\varphi} \circ \pi)(g) = \overline{\varphi}(\pi(g)) = \varphi(g)$$

by definition. Let $\psi\colon G/N \to H$ be any group homomorphism such that $\varphi = \psi \circ \pi$, then for any $\xi \in G/N$, there exists some $g \in G$ with $\xi = \pi(g)$ and so

$$\psi(\xi) = \psi(\pi(g)) = \varphi(g) = \overline{\varphi}(\xi).$$

Therefore, $\psi = \overline{\varphi}$ and so $\overline{\varphi}$ is unique. □

Remark. Theorem 4.2.10 is a special case of Theorem 5.3.7.

Note that for any group homomorphism $\varphi\colon G \to H$, the image $\operatorname{im}(\varphi)$ is clearly a group. One can also check that $\ker(\varphi)$ is always a normal subgroup, so by applying Theorem 5.3.7 on $\operatorname{im}(\varphi)$ we can obtain a unique group homomorphism

$$\widetilde{\varphi}\colon G/\ker(\varphi) \to \operatorname{im}(\varphi) \qquad \text{such that } \widetilde{\varphi} \circ \pi = \varphi.$$

Notice also that $\operatorname{im}(\varphi) \leq H$, so by Theorem 3.1.5, φ is the unique homomorphism such that

$$\varphi = i_{\mathrm{im}(\varphi)} \circ \varphi = i_{\mathrm{im}(\varphi)} \circ \widetilde{\varphi} \circ \pi.$$

Using this approach, we have obtained a unique way to "decompose" any homomorphism using the quotient homomorphism.

Theorem 5.3.8 ▸ The First Isomorphism Theorem

Let G and H be groups. For any group homomorphism $\varphi\colon G \to H$, there exists a unique isomorphism $\widetilde{\varphi}\colon G/\ker(\varphi) \to \mathrm{im}(\varphi)$ such that $\varphi = i_{\mathrm{im}(\varphi)} \circ \widetilde{\varphi} \circ \pi$ is the canonical factorisation of φ.

Proof. By Theorem 5.3.7, there is a unique homomorphism $\widetilde{\varphi}\colon G/\ker(\varphi) \to \mathrm{im}(\varphi)$ such that $\varphi = \overline{\varphi} \circ \pi$. By Theorem 3.1.5, this means that

$$\varphi = i_{\mathrm{im}(\varphi)} \circ \varphi = i_{\mathrm{im}(\varphi)} \circ \widetilde{\varphi} \circ \pi$$

is the canonical factorisation of φ. It then suffices to prove that $\widetilde{\varphi}$ is an isomorphism. For any $h \in \mathrm{im}(\varphi)$, there exists some $g \in G$ such that

$$h = \varphi(g) = \left(i_{\mathrm{im}(\varphi)} \circ \widetilde{\varphi} \circ \pi\right)(g) = \widetilde{\varphi}(\pi(g)).$$

Since $\pi(g) \in G/\ker(\varphi)$, this means that $\widetilde{\varphi}$ is surjective. Let $\xi \in G/\ker(\varphi)$ be such that $\widetilde{\varphi}(\xi) = 1$. Note that there exists some $g \in G$ such that $\xi = \pi(g)$, so

$$1 = i_{\mathrm{im}(\varphi)}\left(\widetilde{\varphi}(\pi(g))\right) = \varphi(g).$$

Therefore, $g \in \ker(\varphi) = 1_{G/\ker(\varphi)}$ and so $\xi = \pi(g) = \ker(\varphi) = 1_{G/\ker(\varphi)}$. This implies that $\ker(\widetilde{\varphi}) = \{1\}$ and so by Proposition 1.3.8, $\widetilde{\varphi}$ is injective. Therefore, $\widetilde{\varphi}$ is an isomorphism. □

A side result of the above theorem is that the image of any group homomorphism is isomorphic to some quotient group of its domain over its kernel, which allows us to compute the cardinality of the image.

Corollary 5.3.9 ▸ Cardinality of the Images of Group Homomorphisms

Let $\varphi\colon G \to H$ be any group homomorphism, then

- $|\mathrm{im}(\varphi)| = |G\colon \ker(\varphi)|$;
- *if G is finite, then* $|\mathrm{im}(\varphi)| \mid |G|$;
- *if G and H are finite, then* $|\mathrm{im}(\varphi)| \mid |H|$.

Consider a group G with subgroups H and K. It is clear that $H \leq HK \leq G$. Suppose that K is normal and consider the quotient map $\pi\colon HK \to HK/K$ and the inclusion map $i_H\colon H \to HK$, then the composite map $\varphi = \pi \circ i_H$ is a group homomorphism from H to HK/K. Applying the First Isomorphism Theorem on φ yields the following result:

Theorem 5.3.10 ▸ The Second Isomorphism Theorem

Let G be a group and $H, K \leq G$ be subgroups such that $K \trianglelefteq G$ is a normal subgroup, then $H/(H \cap K) \cong HK/K$.

Proof. It is clear that K is a normal subgroup of HK, so HK/K is a quotient group. Define $\varphi\colon H \to HK/K$ by $\varphi = \pi_{HK} \circ i_H$ where $\pi_{HK}\colon HK \to HK/K$ is the quotient homomorphism and $i_H\colon H \to HK$ is the inclusion homomorphism. By Theorem 5.3.8, there exists a unique isomorphism $\widetilde{\varphi}\colon H/\ker(\varphi) \to \operatorname{im}(\varphi)$ such that

$$\varphi = i_{\operatorname{im}(\varphi)} \circ \widetilde{\varphi} \circ \pi_H$$

where $\pi_H\colon H \to H/\ker(\varphi)$ is the quotient homomorphism. Note that for any $k \in K$, we have $kK = K$. For any $\xi \in HK/K$, there exist some $h \in H$ and $k \in K$ such that $\xi = (hk)K = hK$, so φ is surjective and so $\operatorname{im}(\varphi) = HK/K$. Note that

$$\varphi(h) = \pi_{HK}(i_H(h)) = hK,$$

so $\ker(\varphi) = \{h \in H\colon hK = K\} = H \cap K$ because for any $h \in K - H$, it is clear that $hk \notin K$. Therefore, $\widetilde{\varphi}$ is an isomorphism between $H/(H \cap K)$ and HK/K, and so $H/(H \cap K) \cong HK/K$. □

Next, consider the case where there are two normal subgroups $N, K \trianglelefteq G$. Without loss of generality, we can assume that $N \leq K \leq G$, then $N \trianglelefteq K$. Notice that $K/N \leq G/N$. It can be proved that K/N is a normal subgroup of G/N, so there exists a composite quotient homomorphism $\varphi := \psi \circ \phi$ where $\psi\colon G \to G/N$ and $\phi\colon G/N \to (G/N)/(G/K)$ are quotient homomorphisms.

Theorem 5.3.11 ▸ The Third Isomorphism Theorem

Let G be any group with $N, K \trianglelefteq G$ such that $N \leq K \leq G$, then we have $K/N \trianglelefteq G/N$ and $G/K \cong (G/N)/(K/N)$.

Proof. Note that $N \trianglelefteq K$ and $K/N \leq G/N$. Take any $gN \in G/N$ and consider

$$(gN)(K/N)(gN)^{-1} = (gN)(K/N)(g^{-1}N).$$

Note that for any $k \in K$, we have $gkg^{-1} \in K$ and so

$$(gN)(kN)(g^{-1}N) = (gkg^{-1})N \in K/N.$$

Clearly, there exists some $k' \in K$ for every $k \in K$ such that $k = gk'g^{-1}$ because otherwise $gKg^{-1} \neq K$. Therefore,

$$kN = (gk'g^{-1})N = (gN)(k'N)(g^{-1}N) \in (gN)(K/N)(gN)^{-1},$$

which implies that $(gN)(K/N)(gN)^{-1} = K/N$ and so gN normalise K/N for any $g \in G$. Therefore, $K/N \trianglelefteq G/N$. Define $\varphi\colon G \to (G/N)/(K/N)$ by $\varphi = \psi \circ \phi$ where $\psi\colon G \to G/N$ and $\phi\colon G/N \to (G/N)/(K/N)$ are quotient homomorphisms. It is clear that φ is surjective and

$$\begin{aligned}
\ker(\varphi) &:= \{g \in G\colon \varphi(g) = K/N\} \\
&= \{g \in G\colon (gN)(K/N) = K/N\} \\
&= \{g \in G\colon (gk)N \in K/N \text{ for all } k \in K\} \\
&= \{g \in G\colon gk \in K \text{ for all } k \in K\} \\
&= K.
\end{aligned}$$

By Theorem 5.3.8, there exists a unique isomorphism $\widetilde{\varphi}\colon G/K \to (G/N)/(K/N)$ such that $\varphi = i_{(G/N)/(K/N)} \circ \widetilde{\varphi} \circ \pi$, and so $G/K \cong (G/N)/(K/N)$. □

Using the above results, we are able to prove the following:

Theorem 5.3.12 ▸ The Lattice Isomorphism Theorem

Let G be a group and $N \trianglelefteq G$ be a normal subgroup. Let $\pi\colon G \to G/N$ be the quotient homomorphism. Let $\mathcal{H}$ be the family of all subgroups of G containing N and $\mathcal{Q}$ be the family of all subgroups of G/N, then the map $\varphi\colon \mathcal{H} \to \mathcal{Q}$ defined by $\varphi(H) := \pi[H]$ is a bijection such that

1. *if $H \trianglelefteq G$, then $\varphi(H) \trianglelefteq G/N$;*
2. *if $X \trianglelefteq G/N$, then $\varphi^{-1}(X) \trianglelefteq G$.*

Proof. Define $\psi\colon \mathcal{Q} \to \mathcal{H}$ by $\psi(X) = \pi^{-1}[X]$. For every $H \in \mathcal{H}$, we have

$$H \subseteq \pi^{-1}[\pi[H]] = (\psi \circ \varphi)(H).$$

For any $g \in \pi^{-1}[\pi[H]]$, we have $\pi(g) \in \pi[H]$, so there exists some $h \in H$ such that

$\pi(g) = \pi(h)$. Clearly,

$$\pi\left(h^{-1}g\right) = \pi\left(h^{-1}\right)\pi(h) = N,$$

so $h^{-1}g \in \ker(\pi) = N \leq H$. Therefore, $g \in hH = H$ and so $\psi \circ \varphi = \mathrm{id}_{\mathcal{H}}$. For every $X \in \mathcal{Q}$, we have

$$(\varphi \circ \psi)(X) = \pi\left[\pi^{-1}[X]\right] = X.$$

Therefore, $\varphi \circ \psi = \mathrm{id}_{\mathcal{Q}}$ and so φ is bijective with $\varphi^{-1} = \psi$. For any $H \in \mathcal{H}$ with $H \trianglelefteq G$, by Theorem 5.3.11, $\varphi(H) = H/N \trianglelefteq G/N$. For any $X \trianglelefteq G/N$, we have

$$N = \ker(\pi) = \pi^{-1}\left[\left\{1_{G/N}\right\}\right] \leq \pi^{-1}[X] = \varphi^{-1}(X).$$

?????????????????? □

Group Actions

6.1 Group Actions

Definition 6.1.1 ▸ Group Action

A **left group action** of a group G on a set A is a map $\alpha\colon G \times A \to A$ such that

- $\alpha(1_G, a) = a$, and
- $\alpha(g_1, \alpha(g_2, a)) = \alpha(g_1 g_2, a)$ for any for all $g_1, g_2 \in G$ and all $a \in A$.

By convention, we denote $\alpha(g, a) = g \cdot a$ or ga.

Remark. A *right group action* is defined analogously. Clearly, for Abelian groups, the left and right actions are equivalent.

Let G be a group with a right group action $\cdot\colon A \times G \to A$. Define the "opposite" group of G to be $G^{\mathrm{op}} := (G, \star)$ such that

$$x \star y = yx \qquad \text{for all } x, y \in G.$$

Now it is clear that $g \diamond a := a \cdot g$ is a left group action. Therefore, in fact it suffices to study left group actions.

We can see the conjugation mapping $a \mapsto gag^{-1} \in G$ is a group action.

Proposition 6.1.2 ▸ Group Action over a Group

Let G be a group, then for each $g \in G$, the map $\alpha_g\colon G \to G$ defined by $\alpha_g(a) = gag^{-1}$ is a group action.

Since group action is essentially a mapping, it is natural to investigate its relationship with group homomorphisms.

Proposition 6.1.3 ▸ Group Actions Induce Group Homomorphisms

Let G be a group and A be a set with a left group action. For each $g \in G$, define the map $\sigma_g\colon A \to A$ such that $\sigma_g(a) = ga$, then

- *$\sigma_g \in S_A$ is bijective, and*

- *if $\varphi \colon G \to S_A$ is such that $\varphi(g) = \sigma_g$, then φ is a group homomorphism.*

Proof. Observe that for any $a \in A$, we have

$$\left(\sigma_g \circ \sigma_{g^{-1}}\right)(a) = g^{-1}(ga) = \left(g^{-1}g\right)a = 1_G a = a.$$

Similarly, $\left(\sigma_{g^{-1}} \circ \sigma_g\right)(a) = a$ for all $a \in A$, and so $\sigma_g \circ \sigma_{g^{-1}} = \sigma_{g^{-1}} \circ \sigma_g = \mathrm{id}_A$. Therefore, by Proposition 1.2.1, σ_g is bijective and so $\sigma_g \in S_A$.

Take any $g, h \in G$, then for any $a \in A$, we have

$$\varphi(gh)(a) = \sigma_{gh}(a) = (gh)a = g(ha) = \sigma_g(\sigma_h(a)) = (\varphi(g) \circ \varphi(h))(a).$$

Therefore, $\varphi(gh) = \varphi(g)\varphi(h)$ for any $g, h \in G$ and so φ is a group homomorphism. □

In the above result, σ_g is essentially an evaluation map that re-arranges the set A through a bijection by letting a particular element g in the group act on A. Therefore, each element g induces a permutation on A via a left group action.

Definition 6.1.4 ▸ Permutation Representation

Let G be a group and A be a set, then for each left group action $\alpha \colon (g, a) \mapsto ga$, the map $\varphi_\alpha \colon G \to S_A$ such that $\varphi_\alpha(g)(a) = \alpha(g, a)$ for all $(g, a) \in G \times A$ is called the **permutation representation** of or **action homomorphism** induced by the left group action.

Note that now, for each fixed group action of G on A, there is a correspondence between each element in G and the permutations of A, so every group action induces a homomorphism from G to S_A. Conversely, given a homomorphism from G to S_A, we can also construct a group action.

Proposition 6.1.5 ▸ Group Homomorphism Induces an Action Map

Let G be a group and A be a set. If $\varphi \colon G \to S_A$ is a group homomorphism, then the map $\alpha_\varphi \colon (G, A) \to A$ defined by $\alpha_\varphi(g, a) = \varphi(g)(a)$ is a left group action.

Proof. Note that $\alpha_\varphi(1_G, a) = \varphi(1_G)(a) = \mathrm{id}_A(a) = a$. For any $g_1, g_2 \in G$ and any $a \in A$, we have

$$\begin{aligned}\alpha_\varphi(g_1, \alpha(g_2, a)) &= \varphi(g_1)(\varphi(g_2)(a)) \\ &= (\varphi(g_1) \circ \varphi(g_2))(a) \\ &= \varphi(g_1 g_2)(a) \\ &= \alpha_\varphi(g_1 g_2, a).\end{aligned}$$

Therefore, α_φ is a left group action. □

This group action is said to be induced by the group homomorphism. In fact, if there are two groups H and G with a homomorphism $\psi\colon H \to G$, then by fixing a permutation representation $\varphi\colon G \to S_A$ for some set A acted upon by G, the composite map $\varphi \circ \psi$ is a permutation representation from H to S_A. In particular, for each $h \in H$, it is clear that $(\varphi \circ \psi)(h)(a) = \psi(h)\,a$ for each $a \in A$.

Definition 6.1.6 ▸ Induced Group Action from Group Homomorphism

Let G and H be groups with $\psi\colon H \to G$ as a group homomorphism. Let A be a set and $\varphi\colon G \to S_A$ be a permutation representation, then the map $\alpha_\psi\colon G \times A \to A$ defined by $\alpha_\psi(h, a) = \varphi(\psi(h))(a)$ is the **group action induced by ψ**.

Clearly, to induce an action from any group homomorphism $\varphi\colon G \to S_A$, we just need to substitute $H = G$ and $\psi = \mathrm{id}_G$ in the above definition.

For any subgroup $H \leq G$, we can substitute $\psi = i_H$ to induce a group action with the inclusion map. If G is a quotient subgroup of H, then we can substitute ψ with the quotient homomorphism and induce a group action.

Intuitively, if we pick an element from a group and let it act on all elements of a set to permute the set, different choices of the element should lead to different permutations.

Proposition 6.1.7 ▸ Injectivity of Permutation Representations

The permutation representation for every left group action is injective.

In particular, we can prove that the image of the injective permutation representation is a subgroup of some symmetric group, which leads to the following theorem:

Theorem 6.1.8 ▸ Cayley's Theorem

Every group is isomorphic to some subgroup of some symmetric group.

Observe that $(\varphi[G], \circ)$ is a group and $\varphi[G] \subseteq S_G$. Therefore, in fact every group G is isomorphic to a subgroup of S_G and every finite group G is isomorphic to some S_n for some $n \in \mathbb{Z}^+$. This implies that in theory, symmetric groups cover everything about group theory.

Consider the correspondence between each element in a group G and the permutations of a set A induced by a group action of G onto A. Intuitively, for different group actions, this correspondence should be different.

Proposition 6.1.9 ▸ Group Actions and Permutation Representations

Let G be a group and A be a set. Define $\mathcal{A}_{G,A}$ to be the set of all left group actions of G onto A and $\mathcal{H}_{G,A}$ to be the set of all action homomorphisms, then $\Phi\colon \mathcal{A}_{G,A} \to \mathcal{H}_{G,A}$ defined by $\Phi(\alpha) = \varphi_\alpha$ is bijective.

Proof. Define $\Psi : \mathcal{H}_{G,A} \to \mathcal{A}_{G,A}$ by $\Psi(\varphi) = \alpha_\varphi$, then it suffices to prove that Φ and Ψ are two-sided inverses of each other. Take any $\alpha \in \mathcal{A}_{G,A}$, consider

$$\alpha_{\varphi_\alpha} := (\Psi \circ \Phi)(\alpha) \in \mathcal{A}_{G,A}.$$

For any $(g, a) \in G \times A$, we have

$$\alpha_{\varphi_\alpha}(g, a) = \varphi_\alpha(g)(a) = \alpha(g, a),$$

so $\alpha_{\varphi_\alpha} = \alpha$ and so $\Psi \circ \Phi = \mathrm{id}_{\mathcal{A}_{G,A}}$. Similarly, one can check that $\Phi \circ \Psi = \mathrm{id}_{\mathcal{H}_{G,A}}$ by considering an arbitrary $\varphi \in \mathcal{H}_{G,A}$. Therefore, Φ is bijective. □

Remark. Basically, Φ takes in a group action and outputs a representation that maps each element in G to a permutation of A.

The permutation representation actually helps us to quickly construct some normal subgroups from a finite group.

Proposition 6.1.10 ▸ Normal Subgroups of Smallest Prime Index

Let G be a finite group and p the smallest prime factor of $|G|$, then every subgroup $H \leq G$ with $|G\colon H| = p$ is normal.

Proof. Let α be the left multiplication group action of G on G/H with permutation representation $\varphi_\alpha\colon G \to S_{G/H}$. By Theorem 5.3.8, there exists some $K \subseteq S_{G/H}$ such that $G/\ker(\varphi_\alpha) \cong K$. By Theorem 5.1.9,

$$|K| \,\Big|\, \left|S_{G/H}\right| = p!.$$

Therefore, we have $|G\colon \ker(\varphi_\alpha)| \mid p!$. Take any $k \in \ker(\varphi_\alpha)$, then $\varphi_\alpha(k) = \mathrm{id}_{G/H}$ and so $\varphi_\alpha(k)(H) = H$. This means that $kH = H$ and so $k \in H$. Therefore, we have $\ker(\varphi_\alpha) \leq H \leq G$, and so

$$|H\colon \ker(\varphi_\alpha)| = \frac{|G\colon \ker(\varphi_\alpha)|}{|G\colon H|} \,\Bigg|\, \frac{p!}{p} = (p-1)!.$$

By Theorem 5.1.8, $|H\colon \ker(\varphi_\alpha)| \mid |G|$, so if q is any prime factor of $|H\colon \ker(\varphi_\alpha)|$, we have $q \geq p \nmid (p-1)!$, so $|H\colon \ker(\varphi_\alpha)| = 1$. Therefore, $H = \ker(\varphi_\alpha)$ which is normal. □

Next, we study the group actions on $\mathcal{P}(A)$. Note that $S_{\mathcal{P}(A)}$ is the set of all bijections from $\mathcal{P}(A)$ to itself. Fix some bijection $\sigma\colon A \to A$. For each $B \subseteq A$, we can map it to $\sigma[B] \subseteq A$.

Proposition 6.1.11 ▸ Permutations on Power Set

Let A be any set. For each $\sigma \in S_A$, define $\mathcal{P}(\sigma) : \mathcal{P}(A) \to \mathcal{P}(A)$ by $\mathcal{P}(\sigma)(U) = \sigma[U]$, then the map $f\colon S_A \to S_{\mathcal{P}(A)}$ defined by $f(\sigma) = \mathcal{P}(\sigma)$ is a group homomorphism.

Proof. For every $\sigma \in S_A$, we claim that $\mathcal{P}(\sigma^{-1})$ is a two-sided inverse of $\mathcal{P}(\sigma)$. Take any $U \subseteq A$, then

$$(\mathcal{P}(\sigma^{-1}) \circ \mathcal{P}(\sigma))(U) = \sigma^{-1}[\sigma[U]] = U$$

because σ is a bijection. Therefore, $\mathcal{P}(\sigma^{-1}) \circ \mathcal{P}(\sigma) = \mathrm{id}_{\mathcal{P}(A)}$. Similarly, one can check that $\mathcal{P}(\sigma) \circ \mathcal{P}(\sigma^{-1}) = \mathrm{id}_{\mathcal{P}(A)}$. Therefore, $\mathcal{P}(\sigma) \in S_{\mathcal{P}(A)}$ for any $\sigma \in S_A$. Take any $\sigma_1, \sigma_2 \in S_A$, then for any $U \subseteq A$,

$$\begin{aligned} f(\sigma_1 \circ \sigma_2)(U) &= \mathcal{P}(\sigma_1 \circ \sigma_2)(U) \\ &= \sigma_1[\sigma_2[U]] \\ &= (\mathcal{P}(\sigma_1) \circ \mathcal{P}(\sigma_2))(U) \\ &= (f(\sigma_1) \circ f(\sigma_2))(U). \end{aligned}$$

Therefore, $f(\sigma_1 \circ \sigma_2) = f(\sigma_1) \circ f(\sigma_2)$ and so f is a group homomorphism. □

Take $f\colon S_A \to S_{\mathcal{P}(A)}$ as a permutation representation of group actions of S_A onto $\mathcal{P}(A)$. Since the permutation representation $\varphi_\alpha\colon G \to A$ is a homomorphism for any group action α of G onto A, by Definition 6.1.6, the composite homomorphism $f \circ \varphi_\alpha\colon G \to S_{\mathcal{P}(A)}$ defines a group action onto the power set of A with permutation representation $g \mapsto \mathcal{P}(\varphi_\alpha(g))$.

Consider a map $f \in \mathrm{Maps}(A, B)$. Pick some permutations $\sigma_A \in S_A$ and $\tau_B \in S_B$, we can replace A and B with $\sigma_A[A]$ and $\sigma_B[B]$ respectively while using the same correspondence defined by f. Informally, we "permute" the map using the transformation. This construction can be formalised as follows:

Proposition 6.1.12 ▸ Permutation of Maps

Let A, B be sets and $f \in \mathrm{Maps}\,(A, B)$ be a map, then the map

$$\alpha\colon\ (S_A \times S_B) \times \mathrm{Maps}\,(A, B) \to \mathrm{Maps}\,(A, B)$$

defined by $\alpha((\sigma_A, \sigma_B)\,, f) = \sigma_B \circ f \circ \sigma_A^{-1}$ is a group action of $S_A \times S_B$ on $\mathrm{Maps}\,(A, B)$.

Proof. Note that $(\mathrm{id}_A, \mathrm{id}_B)$ is the identity in $S_A \times S_B$ and $\mathrm{id}_B \circ f \circ \mathrm{id}_A^{-1} = f$ for all $f \in \mathrm{Maps}\,(A, B)$. For any $(\sigma_A, \sigma_B)\,, (\tau_A, \tau_B) \in S_A \times S_B$, consider

$$\begin{aligned}\alpha\Big((\sigma_A, \sigma_B)\,, \alpha((\tau_A, \tau_B)\,, f)\Big) &= \sigma_B \circ \alpha((\tau_A, \tau_B)\,, f) \circ \sigma_A^{-1}\\ &= \sigma_B \circ \tau_B \circ f \circ \tau_A^{-1} \circ \sigma_A^{-1}\\ &= (\sigma_B \circ \tau_B) \circ f \circ (\sigma_A \circ \tau_A)^{-1}\\ &= \alpha((\sigma_A, \sigma_B)\,(\tau_A, \tau_B)\,, f).\end{aligned}$$

Therefore, α is associative and so is a group action. □

Now, for any group G and any sets A and B, we can construct action homomorphisms $\varphi_A\colon G \to S_A$ and $\varphi_B\colon G \to S_B$. Since these homomorphisms are injective by Proposition 6.1.7, each $(g, f) \in G \times \mathrm{Maps}\,(A, B)$, is uniquely corresponded to $(\varphi_A\,(g)\,, \varphi_B\,(g)\,, f)$. Using the above construction, the map

$$(g, f) \mapsto \varphi_B\,(g) \circ f \circ \varphi_A^{-1}\,(g)$$

is a group action of G on $\mathrm{Maps}\,(A, B)$.

Consider a group action $\alpha\colon G \times A \to A$. Take some $A_0 \subseteq A$, then $\alpha\,[G \times A_0] \subseteq A$ but it is not necessarily overlapping with A_0. In a special case, the image of $G \times A_0$ under α will stay within A_0. In this case, we say that A_0 is *stable*.

Definition 6.1.13 ▸ Stability under Group Actions

Let G be a group and A be a set with a left group action $\alpha\colon G \times A \to A$. A subset $A_0 \subseteq A$ is said to be **stable** under α if $\alpha\,[G \times A_0] \subseteq A_0$.

Note that if we were to use the definition to check stability, we need to consider all possible pairings $(g, a_0) \in G \times A_0$, which can be tedious. Therefore, we can use the permutation representation to simplify the characterisation.

Proposition 6.1.14 ▸ Characterisation of Stable Subsets under Group Actions

Let G be a group and A be a set with a left group action $\alpha\colon G \times A \to A$ and a subset $A_0 \subseteq A$, then the followings are equivalent:

1. *A_0 is stable under α;*
2. *if $\varphi\colon G \to S_A$ is the permutation representation of α, then*

$$\varphi\left[G\right] = \operatorname{Perm}\left(A\right)_{A_0} := \left\{\sigma \in S_A : \sigma\left[A_0\right] = A_0\right\};$$

3. *$\sigma_g\left(a\right) \in A_0$ for any $g \in G$ and $a \in A_0$.*
4. *$\varphi|_{G\times A_0}$ is an action group homomorphism to A_0.*

6.2 Orbits

We propose a visualisation of group actions. Take some $g \in G$ and $a \in A$, then letting g act on a is to perform a “jump” from a to ga. Let $b := ga$, then we can re-use g to act on b to make it “jump” again. Clearly, by performing the “jump” repeatedly, the series of elements reached form a “chain”, which can be formalised as follows:

Proposition 6.2.1 ▸ Equivalence Relation Induced by Group Actions

Let $(g, a) \mapsto ga$ be a group action of a group G on a set A. Let $a \sim b$ in A if and only if there exists some $g \in G$ such that $b = ga$, then $\sim$ is an equivalence relation.

Proof. Left as an exercise to the reader. □

Now consider the equivalence classes of $\sim$ induced by a group action. Clearly, they form a partition. We give these classes a name.

Definition 6.2.2 ▸ Orbit

Let G be a group and A be a set. The **G-orbit** of any $a \in A$, denoted by $G \cdot a$, is the equivalence class of a under the equivalence relation induced by a group action of G on A.

It is possible that a set contains only one orbit under some group action. However, note the difference between this and cyclic groups: in this case, the elements in the single orbit are generated by repeatedly applying an action by some element g from the group onto a “seed”.

Definition 6.2.3 ▸ Transitive Group Action

A group action of G on A is **transitive** if A contains only one G-orbit induced by the action.

Clearly, this means that the only orbit in A is itself. It is also clear that for any $a, b \in A$, we can find some $g \in G$ such that $b = ga$, so everything in A can be produced by letting some element in A be acted upon by an element from the group.

Proposition 6.2.4 ▸ Characterisation of Transitive Group Actions

A group action of G on A is transitive if and only if for any $b \in A$, there exists some $a \in A$ and $g \in G$ such that $b = ga$.

Proof. Trivial. □

Notice that by fixing $a \in A$, to produce the G-orbit of a is simply to collect all element produced by letting each $g \in G$ act on a. In other words, $G \cdot a = f_a[G]$, where $f_a := g \to ga$. Recall that in functions we have the idea of invariant points. A similar notion can be constructed for group actions.

Definition 6.2.5 ▸ Stabiliser

Let G be a group acting of A, then the **stabiliser** of any $a \in A$ is the set

$$G_a := \{g \in G \colon ga = a\} \subseteq G.$$

We can view the stabiliser as all elements from the group G that make $a \in A$ “loop” around itself. We prove the following correspondence between the stabiliser and the orbits:

Proposition 6.2.6 ▸ Bijection between Stabiliser and Orbit

Let G be a group acting on a set A. Define $f \colon G/G_a \to G \cdot a$ by $f(gG_a) = ga$, then f is a bijection.

Proof. We first prove that f is well-defined. Let $g_1, g_2 \in G$ be such that $g_1G_a = g_2G_a$, then $g_2 \in g_1G_a$. Therefore, there exists some $h \in G_a$ such that $g_2 = g_1h$. Therefore,

$$g_2a = g_1ha = g_1(ha) = g_1a,$$

which means that $f(g_1G_a) = f(g_2G_a)$. Notice that f is clearly surjective, so it suffices to prove injectivity. For any $g_1, g_2 \in G$ such that $g_1 a = g_2 a$, we have

$$\left(g_2^{-1} g_1\right) a = g_2^{-1} \left(g_1 a\right) = g_2^{-1} \left(g_2 a\right) = a,$$

so $g_2^{-1} g_1 \in G_a$. This means that $g_2^{-1} g_1 G_a = G_a$ and so $g_1 G_a = g_2 G_a$. Therefore, this means that $f\left(g_1 G_a\right) = f\left(g_2 G_a\right)$ implies that $g_1 G_a = g_2 G_a$, and so f is injective. □

Remark. The above implies that $|G \colon G_a| = |G \cdot a|$.

Note that a set can be decomposed into a partition using orbits, so the above gives rise to the following result:

Corollary 6.2.7 ▸ Orbit Decomposition

Let G be a group acting on a finite set A. Let $\{G \cdot a_i\}_{i \in I}$ be the collection of all distinct G-orbits in A, where I is an index set, then there exists a bijection between $\bigsqcup_{i \in I} G / G_{a_i}$ and $\bigsqcup_{i \in I} G \cdot a_i$.

It is possible that the stabiliser of some element is the entire group. In this case, the element is intuitively "fixed" to a position forever.

Definition 6.2.8 ▸ Fixed Point

Let G be a group acting on a set A. An element $a \in A$ is said to be a **fixed point** if $ga = a$ for all $g \in G$. The set of all fixed points of A is denoted by A^G.

Remark. Equivalently, if a is a fixed point, then $G_a = G$ and $G \cdot a = \{a\}$.

The following result is trivial:

Proposition 6.2.9 ▸ Cardinality of a Set Acted upon by a Group

Let G be a group acting on a finite set A. If $\{G \cdot a_i\}_{i \in I}$ are all distinct non-trivial orbits in A for some index set I, then

$$|A| = \left|A^G\right| + \sum_{i \in I} \left|G \colon G_{a_i}\right|.$$

Recall the conjugacy action of a group G on itself. The G-orbits of the action are simply the conjugacy classes in G, the stabilisers are the centralisers in G, and the fixed points are the centre of G.

Theorem 6.2.10 ▸ The Class Equation

Let G be a finite group such that $\{G \cdot g_i\}_{i \in I}$ are all distinct non-trivial conjugacy classes of G for some index set I, then

$$|G| = |Z(G)| + \sum_{i \in I} |G \colon C_G(g_i)|.$$

6.3 Sylow p-Subgroups

In this section, we introduce a special class of groups known as the *p-groups*.

Definition 6.3.1 ▸ p-Group

Let p be a prime. A **p-group** is a finite group G with $|G| = p^\alpha$ for some $\alpha \geq 1$. A **p-subgroup** is a subgroup which is a p-group.

A *Sylow p-subgroup* is a p-subgroup with additional restrictions.

Definition 6.3.2 ▸ Sylow p-Subgroup

A **Sylow p-subgroup** of a group G is a maximal p-subgroup of G. We denote the collection of all Sylow p-subgroups of G by $\mathrm{Syl}_p(G)$ and define $n_p := |\mathrm{Syl}_p(G)|$.

Equivalently, a Sylow p-subgroup can be characterised as follows:

Proposition 6.3.3 ▸ Characterisation of Sylow p-Subgroups

Let G be a finite group with order $p^\alpha m$ where p is a prime, $\alpha \geq 1$ and $p \nmid m$, then a subgroup $H \leq G$ is a Sylow p-subgroup if and only if $|H| = p^\alpha$ or $\gcd(|G \colon H|, p) = 1$.

The Sylow p-subgroups give rise to a series of interesting results collectively known as Sylow's Theorems. We first state a preliminary lemma:

Lemma 6.3.4 ▸ The Basic Lemma

If H is a p-group acting on a finite set A, then $|A^H| \equiv |A| \mod p$.

Proof. Left as an exercise to the reader. □

We can extend the lemma to p-subgroups:

Corollary 6.3.5 ▸ The Basic Lemma on Subgroups

If H is a p-subgroup of a finite group G, then $\left|N_G(H) : H\right| \equiv |G\colon H| \mod p$.

Proof. With respect to the left multiplication action of H on G/H, we have

$$\begin{aligned}(G/H)^H &= \{\xi \in G/H\colon h\xi = \xi \text{ for all } h \in H\}\\ &= \left\{xH \in G/H\colon x^{-1}hx \in H \text{ for all } h \in H\right\}\\ &= \left\{xH \in G/H\colon x^{-1}Hx \subseteq H\right\}\\ &= \left\{xH \in G/H\colon x^{-1}Hx = H\right\}\\ &= \left\{xH \in G/H\colon x \in N_G(H)\right\}\\ &= N_G(H)/H.\end{aligned}$$

By Lemma 6.3.4,

$$\left|N_G(H) : H\right| = \left|N_G(H)/H\right| = \left|(G/H)^H\right| \equiv |G/H| = |G\colon H| \mod p.$$

□

We first use the lemma to prove some simple result of p-groups.

Proposition 6.3.6 ▸ Centre of p-Groups

For every p-group P, we have $Z(P) \neq \{1_P\}$.

Proof. Consider the conjugation action of P on itself, then $P^P = Z(P)$. By Lemma 6.3.4,

$$|Z(P)| = \left|P^P\right| \equiv \{P\} \mod p.$$

Since $p \mid |P|$, this means that $p \mid |Z(P)|$. Note that $Z(P) \neq \varnothing$, so it is non-trivial. □

The first question of Sylow p-subgroups is their existence. A weaker version on the existence of Sylow p-subgroups is as follows:

Theorem 6.3.7 ▸ Cauchy's Theorem

For every finite group G and any prime $p \mid |G|$, there exists some $g \in G$ such that $|g| = p$.

Proof. Define $\alpha\colon S_p \times G^p \to G^p$ by

$$\alpha\left(\sigma, (g_i)_{i=1}^p\right) = \left(g_{\sigma^{-1}(i)}\right)_{i=1}^p.$$

One may check that α is a group action of S_p on G^p. Take $\sigma_0 := (1, 2, \cdots, p)$ and consider the cyclic group $\langle\sigma_0\rangle \leq S_p$. It is clear that $|\langle\sigma_0\rangle| = p$ by Corollary 4.2.5 and so $\langle\sigma_0\rangle \cong \mathbb{Z}/p\mathbb{Z}$ by Corollary 5.1.10. Note that $\alpha|_{\langle\sigma_0\rangle}$ is a group action of $\langle\sigma_0\rangle$ on G^p. Observe that for any $(g_i)_{i=1}^p \in G^p$ with $\prod_{i=1}^p g_i = 1_G$, we have

$$\alpha\left(\sigma_0, (g_i)_{i=1}^p\right) = \left(g_2, g_3, \cdots, g_p, g_1\right),$$

where

$$\left(\prod_{i=2}^p g_i\right) g_1 = g_1^{-1} 1_G g_1 = 1_G.$$

Therefore, $A := \left\{(g_i)_{i=1}^p \in G^p : \prod_{i=1}^p g_i = 1_G\right\}$ is stable under $\alpha|_{\langle\sigma_0\rangle}$ by Proposition 6.1.14. Let $\{\langle\sigma_0\rangle \cdot a_i\}_{i\in I}$ be all distinct non-trivial $\langle\sigma_0\rangle$-orbits in A in the orbit decomposition for some index set I, then by Proposition 6.2.9,

$$|A| = \left|A^{\langle\sigma_0\rangle}\right| + \sum_{i\in I} \left|\langle\sigma_0\rangle : \langle\sigma_0\rangle_{a_i}\right|.$$

By Corollary 5.1.9, each $\left|\langle\sigma_0\rangle : \langle\sigma_0\rangle_{a_i}\right|$ is a factor of p and is strictly greater than 1, so $\left|\langle\sigma_0\rangle : \langle\sigma_0\rangle_{a_i}\right| = p$ for all $i \in I$. Therefore,

$$|A| \equiv \left|A^{\langle\sigma_0\rangle}\right| \mod p.$$

By the multiplication rule, $p \mid |A| = |G|^{p-1}$, so $p \mid \left|A^{\langle\sigma_0\rangle}\right|$. Since $A^{\langle\sigma_0\rangle} \neq \varnothing$, this means that $\left|A^{\langle\sigma_0\rangle}\right| \geq p > 1$. Therefore, there exists some $a \in A^{\langle\sigma_0\rangle} \subseteq G$ with $a \neq 1_G$. By Corollary 4.2.9, $|a| = p$. □

We can use the above result to extend the statement into a stronger version:

Theorem 6.3.8 ▸ Sylow's First Theorem

For every finite group G and any prime factor p with multiplicity α of $|G|$, there exists a Sylow p-subgroup of G of order p^α.

Proof. We shall prove a stronger statement: for any $k \in \mathbb{Z}$ with $0 \leq k \leq \alpha$, there exists a p-subgroup of G of order p^k. We proceed by induction on k. The case where $k = 0$ is trivial by taking $\{1_G\} \leq G$. Suppose that there exists some $k \in \{0, 1, \cdots, \alpha - 1\}$ such that there exists a p-subgroup $H \leq G$ of order p^k. By Theorem 5.1.8,

$$|G : H| = \frac{|G|}{|H|} = \frac{p^\alpha m}{p^k}$$

for some $m \geq 1$. Since $\alpha > k$, this means that $p \mid |G \colon H|$. Notice that $H \trianglelefteq N_G(H)$ is always a normal subgroup. By Corollary 6.3.5, we have

$$|N_G(H) : H| \equiv |G \colon H| \equiv 0 \mod p.$$

Let $\pi \colon N_G(H) \to N_G(H)/H$ be the quotient homomorphism, then by Theorem 6.3.7, there exists some $\xi \in N_G(H)$ such that $K := \langle \xi \rangle \leq N_G(H)$ is a subgroup of order p. For each coset $\kappa \in K$, we have $|\kappa| = |H| = p^k$, so the p distinct cosets in K imply that $\left|\pi^{-1}(K)\right| = p^{k+1}$. Note that $\pi^{-1}(K) \leq N_G(H) \leq G$, so there exists a p-subgroup of order p^k of G for every $k \in \{0, 1, 2, \cdots, \alpha\}$. By Proposition 6.3.3, the p-subgroup among them with order α is a Sylow p-subgroup. □

Next, we investigate the relationship between Sylow p-subgroups.

Theorem 6.3.9 ▸ Sylow's Second Theorem

Let G be a finite group. For any $P, Q \in \operatorname{Syl}_p(G)$, there exists some $g \in G$ such that $Q = gPg^{-1}$.

Proof. With respect to the left multiplication action of Q on G/P, we have

$$\begin{aligned}(G/P)^Q &= \{gP \in G/P \colon qgP = gP \text{ for all } q \in Q\} \\ &= \{gP \in G/P \colon g^{-1}qg \in P \text{ for all } q \in Q\} \\ &= \left\{gP \in G/P \colon g^{-1}Qg \subseteq P\right\}.\end{aligned}$$

Since Q is a Sylow p-subgroup, it is maximal and so

$$(G/P)^Q = \left\{gP \in G/P \colon g^{-1}Qg = P\right\}.$$

By Lemma 6.3.4, $\left|(G/P)^Q\right| \equiv |G \colon P| \mod p$. Note that $(G/P)^Q \neq \varnothing$, so there exists some $g \in G$ such that $gPg^{-1} = Q$. □

Based on this conjugacy relationship, we can derive the following result:

Corollary 6.3.10 ▸ Sylow p-Subgroups Contain all p-Subgroups

Let G be a finite group, then every p-subgroup is contained in some Sylow p-subgroup.

Proof. Let H be a p-subgroup of G and $P \in \operatorname{Syl}_p(G)$. One may check that

$$(G/P)^H = \left\{gP \in G/P \colon H \subseteq gPg^{-1}\right\}.$$

By Lemma 6.3.4, this means that there exists some $g \in G$ such that $H \subseteq gPg^{-1}$. By Theorem 6.3.9, $gPg^{-1} \in \operatorname{Syl}_p(G)$. □

Lastly, we investigate the number of Sylow p-subgroups in a group.

Theorem 6.3.11 ▸ Sylow's Third Theorem

Let G be a finite group with $|G| = p^\alpha m$ where p is a prime, $\alpha \geq 1$, and $p \nmid m \geq 1$, then

- $n_p(G) \mid m$;
- $n_p \equiv 1 \mod p$;
- $n_p = |G : N_G(P)|$ *where P is any Sylow p-subgroup.*

Proof. By Theorem 6.3.8, $\operatorname{Syl}_p(G) \neq \varnothing$. Note that Theorem 6.3.9 implies that $\operatorname{Syl}_p(G)$ is transitive under conjugation. Therefore, by Proposition 6.2.6, we have

$$n_p(G) = \left|\operatorname{Syl}_p(G)\right| = |G \cdot P| = |G/G_P| = |G : G_P|$$

for any $P \in \operatorname{Syl}_p(G)$. By definition, $G_P = N_G(P)$. Let α be the conjugation action restricted to $P \leq G$, then

$$\begin{aligned} \operatorname{Syl}_p(G)^P &= \left\{Q \in \operatorname{Syl}_p(G) : gQg^{-1} = Q \text{ for all } g \in P\right\} \\ &= \left\{Q \in \operatorname{Syl}_p(G) : P \subseteq N_G(Q)\right\}. \end{aligned}$$

By maximality of P, for any $Q \in \operatorname{Syl}_p(G)^P$, both P and Q are Sylow p-subgroups of $N_G(Q)$. By Theorem 6.3.11, there exists some $\nu \in N_G(Q)$ such that

$$Q = \nu Q \nu^{-1} = P.$$

This means that $\operatorname{Syl}_p(G)^P = \{P\}$. By Lemma 6.3.4,

$$n_p(G) = \left|\operatorname{Syl}_p(G)\right| \equiv \left|\operatorname{Syl}_p(G)^P\right| = 1 \mod p.$$

By Theorem 5.1.8, $|G : N_G(P)| \mid |G|$, so

$$n_p(G) = \left|\operatorname{Syl}_p(G)\right| = |G : N_G(P)| \mid |G| = p^\alpha m.$$

Note that $n_p(G) \nmid p$, so $n_p(G) \mid m$. □

6.4 Simple Groups

Most applications of Sylow's Theorems involve a special type of groups known as *simple groups*.

Definition 6.4.1 ▸ Simple Group

A group G is **simple** if $|G| > 1$ and the only normal subgroups of G are $|1_G|$ and G.

We first state a result without proof on the properties of finite simple groups.

Theorem 6.4.2 ▸ Classification of Finite Simple Groups

There exists exactly 18 *unique families of finite simple groups and* 26 *unique sporadic finite simple groups up to isomorphism.*

We list down some facts:

- $\{\mathbb{Z}/p\mathbb{Z}\}$ is one of these families.
- $\{A_n : n \geq 5\}$ consisting of non-Abelian finite simple groups is one of the families.
- The smallest non-Abelian finite simple group is A_5 of order 60.

By some very tedious enumeration and computation, we have the following result:

Theorem 6.4.3 ▸ Lower Bound of Order of Non-abelian Simple Groups

Every non-Abelian simple finite group has order at least 60.

Remark. Equivalently, every group of order smaller than 60 is either Abelian simple and is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ of prime order p, or not simple.

Recall in Proposition 6.3.6, every p-group has a non-trivial centre which is normal, so it is easy to derive the following corollary:

Corollary 6.4.4 ▸ Necessary Condition of Simple p-Groups

Every p-group with order greater than p is not simple.

Proof. Left as an exercise to the reader. □

Using Sylow's Theorems, we can further generalise this necessary condition.

Proposition 6.4.5 ▸ Necessary Condition of Finite Simple Groups

Any finite group of order pq where p and q are primes is not simple.

Proof. If $p = q$, the statement is trivial by Corollary 6.4.4. Otherwise, without loss of generality, assume that $p < q$. By Theorem 6.3.11, $n_q \mid p$ and $n_q \equiv 1 \mod q$. This means that $n_q = 1$. Let S be the unique Sylow q-subgroup. By Theorem 6.3.9, for any element g in the group, $gSg^{-1} = S$, so S is normal. Therefore, the group is not simple. □

We can generalise this even more:

Proposition 6.4.6 ▸ Generalised Necessary Condition of Finite Simple Groups

ny finite group of order $p^\alpha q^\beta$ where p and q are primes, $\alpha, \beta \geq 1$, and $p^k \not\equiv 1 \mod q$ for any $k = 1, 2, \cdots, \alpha$ is not simple.

Proof. If $p = q$, the statement is trivial by Proposition 6.4.4. Otherwise, by Theorem 6.3.11, $n_q \mid p^\alpha$ and $n_q \equiv 1 \mod q$. Therefore, $n_q = 1$. By the same reasoning with Theorem 6.3.9, this means that the unique Sylow q-subgroup is normal. □