Contents

1 Introduction to Groups

1.1 Axioms of Groups

In this section, 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 1.1.1 ▸ Group

A **group** is a set G with an **associative** map $\star : G \times G \to G$ such that there exists some $e \in G$ with $a \star e = e \star a = a$ for all $a \in G$ and another map $(\quad)^{-1} : G \to G$ such that $a \star a^{-1} = a^{-1} \star a = e$.

In Definition 1.1.1, the map $\star$ is often called *multiplication* by convention, the element e is known as the *identity* element of G, and the map $(\quad)^{-1}$ is known as the *inversion* map.

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.

A group can be finite or infinite. A group defined over G is finite if and only if G is finite, where $|G|$ is known as the *order* of the group.

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 1.1.2 ▸ Abelian Group

A group G is called an **Abelian** or **commutative** group if $a \star b = b \star a$ for all $a, b \in G$.

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 1.1.1 perfectly!

We shall prove two trivial results directly from the definition.

Theorem 1.1.3 ▶ Uniqueness of Identity and Inverse of 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.

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 1.1.3 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.

We will now introduce some simple groups. First, it is easy to see that any singleton set $\{e\}$ is a group with e being the identity and the inverse of itself. One can check that the only valid multiplication map is the map $(e, e) \mapsto e$.

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ under $+$ are known as *additive groups*. $\mathbb{Q}^\times := \mathbb{Q} - \{0\}, \mathbb{R}^\times := \mathbb{R} - \{0\}, \mathbb{C}^\times := \mathbb{C} - \{0\}$ under $\times$ are known as *multiplicative groups*. Note that $\mathbb{Z} - \{0\}$ under $\times$ is not a group because there is no inverse for any $n \in \mathbb{Z}$ with $|n| > 1$. So we define $\mathbb{Z}^\times := \{-1, 1\}$ which under $\times$ is a multiplicative group.

Remark. In general, if A is a ring, then A under $+$ is an additive group and the set

$$A^\times \coloneqq \{a \in A : \exists b \in A \text{ such that } ab = ba = 1_A\}$$

under $\times$ is a multiplicative group.

As an extension, for any $n \in \mathbb{Z}^+$, the quotient set $\mathbb{Z}/n\mathbb{Z}$ under $+$ is an additive group and the set $(Z/n\mathbb{Z})^\times$ under $\times$ is a multiplicative group.

We can do a bit of nesting with the definitions. First, we shall prove a preliminary theorem.

Theorem 1.1.4 ▶ Bijectivity and Invertibility Are Equivalent

Let X, Y be any sets and let $\sigma \in \mathrm{Maps}(X, Y)$ 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

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

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

Conversely, suppose that σ is bijective. Define a map $\tau : Y \to X$ 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

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

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

Now for an arbitrary set Ω, we will consider the set

$$\mathrm{Perm}(\Omega) \coloneqq \{\sigma \in \mathrm{Maps}(\Omega, \Omega) : \sigma \text{ is bijective}\}.$$

$\mathrm{Perm}(\Omega)$ under $\circ$ is known as the *permutation group* of Ω. This group is intuitively named as such in a sense that each $\sigma \in \mathrm{Perm}(\Omega)$ defines a unique way to map an element of Ω to some element of Ω itself, forming a permutation of the set.

In particular, let $[n]$ denote the set of all natural numbers not greater than n, then the group of $\mathrm{Perm}([n] - \{0\})$ under $\circ$ is known as a *symmetric group* of degree n.

Definition 1.1.5 ▶ Cycle

Let $S_n = \{a_1, a_2, \cdots, a_n\}$ be a finite set. An *m*-cycle on S_n is the map

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

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.

Theorem 1.1.6 ▶ Cycle Decomposition

Let Ω be a finite set, then for all $\sigma \in \mathrm{Perm}(\Omega)$, σ is a product of finitely many cycles.

1.2 Multiplication

Proposition 1.2.1

Let G be a group. For any $a, b \in G$, there exists a unique $x \in G$ such that $ax = b$ and a unique $y \in G$ such that $ya = b$.

Proof. Observe that $x = a^{-1}b$ is such that $x \in G$ and $ax = b$. Suppose there is $x' \in G$ such that $ax' = b$, then

$$x' = a^{-1}ax' = a^{-1}b = a^{-1}ax = x.$$

Therefore, x is unique. One can check similarly that there exists a unique $y \in G$ such that $ya = b$. □

An important implication of Proposition 1.2.1 is that we can cancel "common factors" in multiplication between group elements.

Corollary 1.2.2 ▶ Cancellation Laws

Let G be a group. For any $a, u, v \in G$, if $au = av$, then $u = v$. Similarly, if $ua = va$, then $u = v$.

It is also easy to see that for any a in a group G, the maps $x \mapsto ax$ and $x \mapsto xa$ where $x \in G$ are always bijective.

Definition 1.2.3 ▸ Direct Product

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

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

where

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

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 $(a, b) \mapsto (a^{-1}, b^{-1})$.

Definition 1.2.4 ▸ Order

Let G be a group and $x \in G$. The **order** of x is the smallest $n \in \mathbb{Z}^+$ such that $x^n = 1$, denoted by $|x|$ or $\text{ord}(x)$. If $x^n \neq 1$ for all $n \in \mathbb{Z}^+$, we say that x is of **infinite order**.

1.3 Generators and Relations

Definition 1.3.1 ▸ 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 $G = (S)$.