# Group Theory Notes

Lance Remigio

June 7, 2024

# Contents

# List of Theorems

# Chapter 1

# Introduction to Groups

## 1.1 Basic Axioms and Examples

**Definition 1.1.1** (Binary Operation). (1) A **binary operation** $\cdot$ on a set $G$ is a function $\cdot : G \times G \to G$. For any $a, b \in G$, we shall write $a \cdot b$ for $\cdot(a, b)$.

(2) A binary operation $\cdot$ on a set $G$ is **associative** if for all $a, b, c \in G$, we have

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

(3) If $\cdot$ is a binary operation on a set $G$ we say elements $a$ and $b$ of $G$ **commute** if $a \cdot b = b \cdot a$. We say $\cdot$ (or $G$) is **commutative** if for all $a, b \in G$, $a \cdot b = b \cdot a$.

Suppose we have a binary operation $\cdot$ defined on a set $G$ and $H$ is a subset of $G$. Then the operations described in the definition above are preserved in $H$.

**Example 1.1.1.** (1) $+$ (usual addition) is a commutative binary operation on $\mathbb{Z}, \mathbb{R}$, or $\mathbb{C}$.

(2) $\times$ (usual multiplication) is a commutative binary operation on $\mathbb{Z}$ (or on $\mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$).

(3) $-$ (usual subtraction) is a noncommutative binary operation on $\mathbb{Z}$, where $-(a, b) = a - b$. The map $a \to -a$ is not a binary operation.

(4) $-$ is not a binary operation on $\mathbb{Z}^+$ (nor $\mathbb{Q}^+, \mathbb{R}^+$) because $a, b \in \mathbb{Z}^+$ with $a < b$, $a - b \notin \mathbb{Z}^+$ that is, $-$ does not map $\mathbb{Z}^+ \times \mathbb{Z}^+$ into $\mathbb{Z}^+$.

(5) The vector cross product in $\mathbb{R}^3$ is a binary operation that is neither commutative nor associative.

**Definition 1.1.2** (Groups). A **group** is an ordered pair $(G, \cdot)$ where $G$ is a set and $\cdot$ is a binary operation on $G$ satisfying the following axioms:

(i) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$.

(ii) There exists an element $e$ in $G$, called an **identity** of $G$, such that for all $a \in G$, we have $a \cdot e = e \cdot a = a$.

(iii) For each $a \in G$, there is an element $a^{-1}$ of $G$, called an **inverse** of a, such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

**Definition 1.1.3** (Abelian). A group $(G, \cdot)$ is called **abelian** (or **commutative**) if $a \cdot b = b \cdot a$ for all $a, b \in G$.

**Definition 1.1.4** (Finite Group). If $G$ is a group, then we call $G$ **finite** if $G$ is a finite set.

**Example 1.1.2.** (1) Under the binary operation $+$, the sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are groups with $e = 0$ and $a^{-1} = -a$ for all $a$.

**Proposition 1.1.1.** If $G$ is a group under the operation $\cdot$, then

(1) The identity of $G$ is unique.

(2) For each $a \in G$, $a^{-1}$ is uniquely determined.

(3) $(a^{-1})^{-1} = a$ for all $a \in G$.

(4) $(a \cdot b)^{-1} = (b^{-1}) \cdot (a^{-1})$

(5) For any $a_1, a_2, \ldots, a_n \in G$ the value of $a_1 \cdot a_2 \cdot \cdots a_n$ is independent of how the expression is bracketed (this is called the **generalized associative law**).

**Proof.** (1) Suppose $f$ and $g$ are both identities. Since $G$ is a group under the operation $\cdot$ and $g$ is an identity of $G$, we have $f \cdot g = f$. Using the same axiom, $f$ is an identity of $G$. Thus, $g \cdot f = g$. So, $f = f \cdot g = g \cdot f = g$, and the

(2) Suppose $b$ and $c$ are both inverses of $a$ and let $e$ be the identity of $G$. Since $b$ is an inverse of $a$, we must have $b \cdot a = a \cdot b = e$. Likewise, $c \cdot a = a \cdot c = e$ since c also an inverse of $a$. We need to show that $b = c$. Since associativity holds in $G$, we must have

$$\begin{aligned} a \cdot b = e &\Rightarrow c \cdot (a \cdot b) = c \cdot e \\ &\Rightarrow (c \cdot a) \cdot b = c \cdot e \\ &\Rightarrow e \cdot b = c \cdot e \\ &\Rightarrow b = c. \end{aligned}$$

Thus, $b = c$ and we conclude that the multiplicative identity of $a$ is uniquely determined.

(3) Since $aa^{-1} = a^{-1}a = e$. We can view $a^{-1}$ as the element in question, and state that $a$ is the inverse of $a^{-1}$. Thus, we can write that $a = (a^{-1})^{-1}$.

(4) Let $c = (a \cdot b)^{-1}$. Since every element in $G$ contains an inverse, we have

$$(a \cdot b) \cdot c = e. \tag{1}$$

. Since $a$ and $b$ also contain inverses, we must have $a^{-1}a = e$ and $b^{-1}b = e$. Using associativity, we get that

$$a \cdot (b \cdot c) = e$$

and applying the binary operation $\cdot$ to the left-side, we must have

$$b \cdot c = a^{-1}e.$$

Then applying $b^{-1}$ on both sides, we have

$$c = b^{-1}a^{-1}.$$

So, we conclude that $(a \cdot b)^{-1} = b^{-1}a^{-1}$.

(5) *Left as an exercise.*

■

**Proposition 1.1.2.** Let $G$ be a group and let $a, b \in G$. The equation $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$. In particular, the left and right cancellation laws hold in $G$, i.e,

(1) If $au = av$, then $u = v$, and

(2) If $ub = vb$, then $u = v$.

**Proof.** ■