# Group Theory

Buce-Ithon

10th August, 2024

# Contents

Figure 1: Beautiful Algebra To My Elma

# 0 What is Group?-Introduction to Group

Accoding to Chiniese Wikipeida:

In mathematics, the **Group** is a special set equiped a binary operation, (the operation) which has associativity, identity and inverse element. core of Group

Since lots of mathematical structure are all groups (for instance: the integer system equiped with addition forms a Group), therefore, common results can be succinctly summarized from different mathematical structures, which makes groups a core concept in contemporary mathematics.

The unilateral (left) definition of Group (weak definition) is below:

If a given set $G$, and it's equiped binary operation $\circ$: $G \times G \to G$ satisfying (the result of operation $\circ(a, b)$ is simplified as $a \circ b$): simplest definition of the Group

| | | |
|---|---|---|
| Associativity | $\forall g_1, g_2, g_3 \in G$, we have $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$ | |
| (L)Identity & (L)Inverse | $\exists e \in G, \forall g \in G$, we have | $e \circ g = g$ and exists $\gamma \in G$, s.t. $\gamma \circ g = e$ |

then we say $(G, \circ)$ is a **Group**. If $\circ$ is understood, $(G, \circ)$ is simplified as $G$.

The order of group operations is very important, i.e $a \cdot b = b \cdot a$(commutative) doesn't necessarily hold.
A group satisfies the commutative law is called Commutative Group (or Abelian Group named after Niels·Abel), those doesn't satisfy is called Non-commutative Group (Non-Abelian Group). (For instance: The Dihedra Group (appearing next chapter) is a Non-Abelian Group.)

Equivalance definition of Group: unilateral (right) definition of Group (strong definition) is below: The above definition part of identity and inverse can also be changed to: equivalance and full definition

| | | |
|---|---|---|
| Identity(R) & Inverse(R) | $\exists e \in G, \forall g \in G$, we have | $g \circ e = g$ and exists $\gamma \in G$, s.t. $g \circ \gamma = e$ |

Because no matter the original definition of lavender or the alternative definition of light-yellow, combined with the associativity, it's equivalent to the following definition:

| | | |
|---|---|---|
| Identity & Inverse | $\exists e \in G, \forall g \in G$, then we have | $e \circ g = g \circ e = g$ |
| | | and exists $\gamma \in G$, s.t. $\gamma \circ g = g \circ \gamma = e$ |

Ohh! Please remenber the definitions above, because this is the most concise definition of Group. And it will be very helpful for us to understand Group Theory!

# 1 Definition of Group and some Examples

**Definition 1.1.** *(Group) If a set $G$ of some elements (finite or infinite) equiped with a binary operation $\circ$ (or $\cdot$, or even can be omitted), satisfies:*

1. $\forall a, b \in G$, $a \circ b \in G$, *closure*
2. $\forall a, b, c \in G$, $(a \circ b) \circ c = a \circ (b \circ c)$, *associativity*
3. $\exists e \in G$, $\forall g \in G$, $e \circ g = g \circ e = g$, *identity (or neutral)*
4. $\forall g \in G$, $\exists g' \in G$, $g' \circ g = g \circ g' = e$, *inverse*
   *what's more, we denote* $g' = g^{-1}$.

*Then, we denote* $(G, \circ)$ *is a* ***Group***.

**Example.**

1. $(\mathbb{Z}, +)$ *is a group, identity* $e = 0$, *for some* $g \in G$, *its inverse* $g^{-1} = -g$
2. $(Q, +)$ *is a group, similiar with* $(\mathbb{Z}, +)$
   *Special,* $(Q^{\times}, \times)$ *is a group, with* $Q^{\times} = Q/\{0\}$ *and identity* $e = 1$
3. $(\mathbb{R}, +)$, $(\mathbb{R}^{\times}, \times)$ *with* $\mathbb{R}^{\times} = \mathbb{R}/\{0\}$ *both are groups*
4. $\mathbb{Z}_n = \{m | m = x \text{ mod } n, \ \forall x \in \mathbb{Z}\} = \{0, 1, \cdots, n-1\}$, $(\mathbb{Z}_n, +)$ *is a cyclic group*
5. *Dihedra group: a group of symetries of regular polygon, with elements of rotations* $(r_i)$ *and reflections* $(s_i)$, *often denoted by* $D_{2n}$ *(or* $(D_{2n}, \circ)$*) or* $D_n$ *for* $n$*-gon polygon with* $2n$ *elements.*

Cyclic group: a group can be generated by at least one element of the group.

Generate: Applying the binary operation of this group to the element, that is, all integer powers of the element.