Lectures in Group Theory

MOHAMMED ALABBOOD

University of Basrah-College of Science
Department of Mathematics

May 18, 2020

Group of integers modulo n

Let $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. Define an operation on $\mathbb{Z}_6$ as follows: For $a, b \in \mathbb{Z}_6 : a + b = r$, where r is the remainder when we divide $a + b$ by 6. For example, to find $5 + 5$, we divide 10 by 6. Then we get the reminder $r = 4$. Thus, $5 + 5 = r = 4 \in \mathbb{Z}_6$. Similarly, we have the following table

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Note from the above table, our operation + is a binary operation on $\mathbb{Z}_6$. Moreover, for all $a, b, c \in \mathbb{Z}_6$, we have $a + (b + c) = (a + b) + c$. The identity element of $\mathbb{Z}_6$ is 0. Every element in $\mathbb{Z}_6$ is invertible, namely

$$0^{-1} = 0, 1^{-1} = 5, 2^{-1} = 4, 3^{-1} = 3, 4^{-1} = 2, 5^{-1} = 1.$$

Group of integers modulo n

Thus, $\mathbb{Z}_6$ with our operation forms a group, it is called the group of integer modulo 6.

Remark: In the same argument above, we can define the group of integer modulo n for any positive integer n.

Remark: The table above is called the group table of $\mathbb{Z}_6$.

Homework:

1. Define an operation on $\mathbb{Z}_6$ as follows:
   For $a, b \in \mathbb{Z}_6 : a \cdot b = r$, where r is the remainder when we divide $a \cdot b$ by 6. Prove that $\mathbb{Z}_6$ is a monoid under the above operation. Is $\mathbb{Z}_6$ a group under the same operation?
2. Find the group table of $(\mathbb{Z}_5, +)$. Determine inverse of each element in this group.

Abelian group and Finite group

Definition: A group $(G, *)$ is called abelian if $\forall\, a, b \in G : a * b = b * a$.
Definition: A group $(G, *)$ is called finite if the number of element in group is finite. If G has n element, we say that G has finite order, and we write $|G| = n$.
Example1: $(\mathbb{Z}_n, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$, $(\mathbb{Q}\backslash\{0\}, \cdot)$, $(\mathbb{R}\backslash\{0\}, \cdot)$, $(\mathbb{C}\backslash\{0\}, \cdot)$ and $(\mathfrak{S}_2, \circ)$ are abelian groups.
Example2: $(\mathfrak{S}_3, \circ)$ is a group with $|\mathfrak{S}_3| = 6 = 3!$, but it is not abelian. Recall the symmetric group $(\mathfrak{S}_3, \circ)$ in the previous lecture,. Note that,

$$f_3 \circ f_2 = f_6 \neq f_5 = f_2 \circ f_3.$$

that is, $(\mathfrak{S}_3, \circ)$ is not abelian group.
Homework:

1. Is $GL_2(\mathbb{R})$ abelian group under usual multiplication of matrices? Is $GL_2(\mathbb{R})$ has finite order?
2. Find the order of the groups, $(\mathbb{Z}_4, +)$ and $(\mathfrak{S}_4, \circ)$.