Dr. Rudra Narayan Padhan
Centre for Data Science

Notation:

1. Set of all natural numbers is denoted by $\mathbb{N} = \{1, 2, \ldots\}$.
2. Set of all integers is denoted by $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
3. Set of all rational numbers is denoted by $\mathbb{Q} = \{p/q \mid 0 \neq q, p \in \mathbb{Z}\}$.
4. Set of all real numbers is denoted by $\mathbb{R} = \mathbb{Q} \cup \overline{\mathbb{Q}}$, where $\overline{\mathbb{Q}} = \mathbb{R} - \mathbb{Q}$ is the set of all irrational numbers.
5. Set of all complex numbers is denoted by $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$.
6. Set of all non-zero integers, non-zero rational numbers, non-zero real numbers, non-zero complex numbers are denoted by $\mathbb{Z}^*$, $\mathbb{Q}^*$,$\mathbb{R}^*$, $\mathbb{C}^*$ respectively.

Properties of $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$:

1. For any $x, y \in \mathbb{Z}$, then there is a unique $x + y \in \mathbb{Z}$. Thus the addition define a function from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$.

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \quad \textbf{(Closure Properties)}$$

$$(2, 3) \mapsto 5$$

2. For any $x, y, z \in \mathbb{Z}$, then

$$x + (y + z) = (x + y) + z \qquad \textbf{(Associative Law)}$$

3. For any $x \in \mathbb{Z}$, there exist $0 \in \mathbb{Z}$ such that

$$x + 0 = x = x + 0 \qquad \textbf{(Existence of Identity)}$$

4. For any $x \in \mathbb{Z}$, there exist $-x \in \mathbb{Z}$ such that

$$x + (-x) = 0 = (-x) + x \qquad \textbf{(Existence of Inverse)}$$

5. For any $x, y \in \mathbb{Z}$, then

$$x + y = y + x \qquad \textbf{(Commutative Law)}$$

Now we will generalize the properties of $\mathbb{Z}$ w.r.t addition to any arbitrary set say G, for that we need to define a operation on that set, before that one need to define the meaning of operation. Throughout this topic we assume that G is a non-empty set.

Definition 0.0.1. *A binary operation $*$ on G is a function from $G \times G$ to G.*

$$* : G \times G \to G$$

Examples:

1. Addition '$+$' is a binary operation on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

2. Subtraction '$-$' is a binary operation on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, but not on $\mathbb{N}$.

3. Multiplication $\times$ is a binary operation on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, but not on $\mathbb{R} - \mathbb{Q}$.

Notation: We will denote a non-empty set G with a binary operation by $(G, *)$

Definition 0.0.2. *A non-empty set G with a binary operation $*$ is said to be group if the following holds:*

1. $a * (b * c) = (a * b) * c \quad \forall\ a, b, c \in G \quad (Associative\ Law)$.

2. *There exist an element $e \in G$ such that*

$$a * e = a = e * a \quad \forall \quad a \in G \quad (Existence\ of\ Identity).$$

3. *For each $a \in G$, there exist an element $b \in G$ such that*

$$a * b = e = b * a \qquad (Existence\ of\ Inverse).$$

Definition 0.0.3. *A group $(G, *)$ is said to abelian if commutative law holds, i.e,*

$$a * b = b * a \quad \forall a, b \in G.$$

Examples:

1. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ are abelian groups.

2. $(\mathbb{Q}^*, \times), (\mathbb{R}^*, \times), (\mathbb{C}^*, \times)$ are abelian groups.

3. $(\mathbb{N}, +), (\mathbb{Z}^*, \times)$ are not group.

Problem-1: Show that $(\mathbb{Z}, -), (\mathbb{Q}, -), (\mathbb{R}, -), (\mathbb{C}, -)$ are not groups.
Problem-2: Find the inverse of $a + ib$ in $(\mathbb{C}^*, \times)$.

Additive Group of Integers modulo n

Consider $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$. Let us fixed $n = 3$. We define an relation on $\mathbb{Z}$, two elements $a, b \in \mathbb{Z}$ are related $a \sim b$ if $3 \mid a - b$ (3 divides $a - b$) or $a \equiv b \ mod(n)$

Note: $a \equiv b \ mod(n)$ is read as "a is congruent to b modulo n".

Observation:

1. The above relation on $\mathbb{Z}$ reflexive, i.e., $a \sim a$ for all $a \in \mathbb{Z}$.

$$3 \mid a - a = 0$$

2. The above relation on $\mathbb{Z}$ symmetric, i.e., if $a \sim b$, then $b \sim a$ for all $a, b \in \mathbb{Z}$.

$$If \ 3 \mid a - b, \ then \ obviously \ 3 \mid \ -(a - b) = b - a$$

3. The above relation on $\mathbb{Z}$ transitive, i.e., if $a \sim b$ and $b \sim c$, then $a \sim c$ for all $a, b, c \in \mathbb{Z}$.

$$If \ 3 \mid a - b \ and \ 3 \mid b - c, \ then \ \exists \ q, s \in \mathbb{Z} \ such \ that \ a - b = 3q, \ b - c = 3s,$$

$$but \ a - c = (a - b) + (b - c) = 3q + 3s. \ Thus \ 3 \mid a - c.$$

4. Thus the above relation is an equivalence relation. Therefore

$$\mathbb{Z} = \bigsqcup_{a \in \mathbb{Z}} cl(a)$$

where

$$\begin{aligned} class(a) = cl(a) &= \{b \ : \ a \sim b\} \\ &= \{b \ : \ 3 \mid a - b\} \\ &= \{b \ : \ a - b = 3q \ for \ some \ q \in \mathbb{Z}\} \\ &= \{b \ : \ b = a + 3q \ for \ some \ q \in \mathbb{Z}\} \\ &= \{a + 3q \ : \ q \in \mathbb{Z}\} \end{aligned}$$

For example

$$\begin{aligned}
cl(0) &= \{b \ : \ b \sim 0\} \\
&= \{b \ : \ 3 \mid b - 0\} \\
&= \{b \ : \ b - 0 = 3q \ for \ some \ q \in \mathbb{Z}\} \\
&= \{b \ : \ b = 0 + 3q \ for \ some \ q \in \mathbb{Z}\} \\
&= \{3q \ : \ q \in \mathbb{Z}\} \\
&= \{0, \pm 3, \pm 6, \pm 9, \ldots\}
\end{aligned}$$

(When 3 divides remainder is zero)

$$\begin{aligned}
cl(1) &= \{b \ : \ b \sim 1\} \\
&= \{b \ : \ 3 \mid b - 1\} \\
&= \{b \ : \ b - 1 = 3q \ for \ some \ q \in \mathbb{Z}\} \\
&= \{b \ : \ b = 1 + 3q \ for \ some \ q \in \mathbb{Z}\} \\
&= \{1 + 3q \ : \ q \in \mathbb{Z}\} \\
&= \{\ldots, -5, -2, 1, 4, 7, 10, \ldots\}
\end{aligned}$$

(When 3 divides remainder is one)

$$\begin{aligned}
cl(2) &= \{b \ : \ b \sim 2\} \\
&= \{b \ : \ 3 \mid b - 2\} \\
&= \{b \ : \ b - 2 = 3q \ for \ some \ q \in \mathbb{Z}\} \\
&= \{b \ : \ b = 2 + 3q \ for \ some \ q \in \mathbb{Z}\} \\
&= \{2 + 3q \ : \ q \in \mathbb{Z}\} \\
&= \{\ldots, -4, -1, 2, 5, 8, 11, \ldots\}
\end{aligned}$$

(When 3 divides remainder is two)

$$\begin{aligned} cl(3) &= \{b \ : \ b \sim 3\} \\ &= \{b \ : \ 3 \mid b-3\} \\ &= \{b \ : \ b-3 = 3q \ for \ some \ q \in \mathbb{Z}\} \\ &= \{b \ : \ b = 3+3q \ for \ some \ q \in \mathbb{Z}\} \\ &= \{3(1+q) \ : \ q \in \mathbb{Z}\} \\ &= \{0, \pm 3, \pm 6, \pm 9, \ldots\} \end{aligned}$$

(class(3)=class(0))

Similarly, $cl(4) = cl(1), cl(5) = cl(2)$. The reason behind this can be observed from the division algorithm; if $a \in \mathbb{Z}$, then there exist an integer $q \in \mathbb{Z}$ such that

$$a = 3q + r \quad 0 \leq r \leq 2.$$

Therefore

$$\mathbb{Z} = cl(0) \cup cl(1) \cup cl(2)$$

$$= \{0, \pm 3, \pm 6, \ldots\} \cup \{0, \pm 4, \pm 7, \ldots\} \cup \{0, \pm 5, \pm 8, \ldots\}$$

5. We will denote $cl(a) = \overline{a}$, then $\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2}$.

6. Let $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$. We will define a binary operation '$\oplus_3'$ (addition modulo 3) on $\mathbb{Z}_3$. For $\overline{a}, \overline{b} \in \mathbb{Z}_3$, then define:

$$\overline{a} \oplus_3 \overline{b} := \overline{a+b}$$

Then

$$\overline{0} \oplus_3 \overline{0} = \overline{0}, \ \overline{0} \oplus_3 \overline{1} = \overline{1}, \ \overline{0} \oplus_3 \overline{2} = \overline{2}$$

$$\overline{1} \oplus_3 \overline{0} = \overline{1}, \ \overline{1} \oplus_3 \overline{1} = \overline{2}, \ \overline{1} \oplus_3 \overline{2} = \overline{3} = \overline{0}$$

$$\overline{2} \oplus_3 \overline{0} = \overline{2}, \ \overline{2} \oplus_3 \overline{1} = \overline{3} = \overline{0}, \ \overline{2} \oplus_3 \overline{2} = \overline{4} = \overline{1}$$

Observe that $\overline{0}$ is the identity element of $\mathbb{Z}_3$ and $\overline{1}$ is the inverse of $\overline{2}$. Thus $\mathbb{Z}_3$ forms a group under addition modulo 3. In fact $(\mathbb{Z}_3, \oplus_3)$ is an abelian group.

7. Let $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. Then $(\mathbb{Z}_n, \oplus_n)$ forms an abelian group, where $\overline{0}$ is

the identity element and inverse of $\bar{i}$ is $\overline{n-i}$, as

$$\bar{i} \oplus_n \overline{n-i} = \overline{i+n-i} = \overline{n} = \overline{0}.$$

Definition 0.0.4. *Let $(G, *)$ be a group. Then order of G, denoted by $o(G)$ or $|G|$, is the number of elements in G. If $o(G)$ is finite, then G is a finite group otherwise infinite group.*

Remarks:

1. $(\mathbb{Z}_n, \oplus_n)$ is a finite group, $o(\mathbb{Z}_n) = n$.

2. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)(\mathbb{Q}^*, \times), (\mathbb{R}^*, \times), (\mathbb{C}^*, \times)$ are infinite groups.

Definition 0.0.5. *Let $(G, *)$ be a group and $a \in G$. Then order a is the smallest positive integer n such that $a^n = e$, where e is the identity element of G.*

$$a^n = a * a * a \cdots * a = e.$$

Remarks:

1. In any group $(G, *)$, order of identity element is one.

2. Consider $(\mathbb{Z}_3, \oplus_3)$. Then observe that

$$\overline{1}^3 = \overline{1} \oplus_3 \overline{1} \oplus_3 \overline{1} = \overline{3} = \overline{0},$$

$$\overline{2}^3 = \overline{2} \oplus_3 \overline{2} \oplus_3 \overline{2} = \overline{6} = \overline{0}.$$

Thus $o(\overline{0}) = 1, o(\overline{1}) = 3, o(\overline{2}) = 3$.

Problem: Find order of each element in $(\mathbb{Z}_4, \oplus_4)$ and $(\mathbb{Z}_6, \oplus_6)$.

Now we will see some examples of Non-abelian Groups.

Quaternion Group

Let $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ be a set with a binary operation (Multiplication) on it, define by

$$1 \times (\pm i) = \pm i,\ 1 \times (\pm j) = \pm j,\ 1 \times (\pm k) = \pm k$$

$$i^2 = j^2 = k^2 = -1, (-1) \times (-1) = 1$$

$$i \times j = k,\ j \times k = i,\ k \times i = j$$

$$j \times i = -k, \ k \times j = -i, \ i \times k = -j$$

One may observe that the way we have defined the multiplication here is a binary operation on Q_8 and this multiplication is associative. Here 1 is the identity element of Q_8. Inverse of i is $-i$, inverse of j is $-j$, inverse of k is $-k$, and inverse of -1 is -1. Thus Q_8 forms a group know as quaternion Group.

Problem: Find the order of each element of Q_8.

Problem: Prove or disprove that $\mathbb{R}$ under the binary operation

$$a * b := a + b + ab$$

is a group.

Problem: Prove or disprove that $H = \{z \in \mathbb{C} \ : \ |z| = 1\}$ is a group under multiplication.

Problem: Prove or disprove that $\{2\mathbb{Z} = \{0, \pm 2, \pm 4, \ldots\}$ is group under addition.

Definition 0.0.6. *Let $(G, *)$ be a group. A subset H of G is said to be subgroup of G if H w.r.t the same binary operation $*$ is group.*

Examples:

1. $\mathbb{Z}$ is a subgroup $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ under addition.
2. $\mathbb{N}$ is not a subgroup $\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}$ under addition.

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Theorem 0.0.7. *H is a subgroup of $(G, *)$ if and only if for any $a, b \in H$, then $a * b^{-1} \in H$.*

Use above theorem and prove the following:
Problem: Prove that $\{2\mathbb{Z} = \{0, \pm 2, \pm 4, \ldots\}$ subgroup $(\mathbb{Z}, +)$.
Problem: Prove that $H = \{z \in \mathbb{C} \ : \ |z| = 1\}$ is a subgroup of $(\mathbb{C}^*, \times)$.