16. Groups

Group. Definition Let G be a non-empty set equipped with a binary operation denoted by $\circ$ i.e., $a \circ b$ or more conveniently ab represents the elements of G obtained by applying the said binary operation between the elements a and b of G taken in that order. Then this algebric structure $(G, \circ)$ is a group, if the binary operation $\circ$ satisfies the following postulates:

1. Closure property: $a \circ b \in G \quad \forall\, a, b \in G$.
2. Associativity: $(a \circ b) \circ c = a \circ (b \circ c) \quad \forall\, a, b, c \in G$.
3. Existence of Identity: There exists an element $e \in G$ such that $a \circ e = e \circ a = a \quad \forall\, a \in G$. The element e is called the identity.
4. Existence of inverse: Each element of G possesses inverse. In other words $a \in G \Rightarrow$ there exists an element $b \in G$ such that $a \circ b = e = b \circ a$. The element b is then called the inverse of a and we write $b = a^{-1}$. Thus a^{-1} is an element such that $a^{-1} \circ a = e = a \circ a^{-1}$.

Abelian group or Commutative group. Definition A group G is said to be abelian if in addition to the above four postulates the following postulate is also satisfied.

Abelian group or Commutative group. **Definition** A group G is said to be abelian if in addition to the above four postulates the following postulate is also satisfied.

5. **Commutativity:** $a \circ b = b \circ a \quad \forall\, a, b \in G.$

Abelian group $\Rightarrow$ group

Note 1. A group is not simply a set but it is an algebric structure.

Note 2. If we use additive notation '+' to denote the composition in G, then the inverse of an element $a \in G$ is denoted by the symbol $-a$, i.e.,

$$a + (-a) = e = (-a) + a.$$

Note 3. The smallest group for a given composition is the set $\{e\}$ consisting of the identity element e alone.

Example 1 Show that the set Z of all integers

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

is an abelian group under ordinary addition.

Solution: 1. **Closure property.** We know that the sum of two integers is also an integer i.e., $a + b \in Z \quad \forall\, a, b \in Z$. Thus Z is closed under ordinary addition.

2. **Associativity.** We know that addition of integers is an associative composition. Therefore,

$$(a+b)+c = a+(b+c) \quad \forall \; a,b,c \in \mathbb{Z}.$$

3. Existence of Identity. The number $0 \in \mathbb{Z}$. Also we have $a+0 = a = 0+a \quad \forall \; a \in \mathbb{Z}$. Therefore the integer 0 is the identity.

4. Existence of Inverse. If $a \in \mathbb{Z}$, then $-a \in \mathbb{Z}$. Also we have $a+(-a) = 0 = (-a)+a$. Thus every element possesses additive inverse.

Therefore $\mathbb{Z}$ is a group under ordinary addition.

5. Commutativity. $a+b = b+a \quad \forall \; a,b \in \mathbb{Z}$.

Therefore $(\mathbb{Z},+)$ is an abelian group.

Similarly, we can show that $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ are all abelian groups under ordinary addition.

- $(\mathbb{Z},\cdot)$ is not a group as 0 has no multiplicative inverse.
  $\cdot$ ↳ ordinary multiplication

  Infact, none of $(\mathbb{Z},\cdot)$, $(\mathbb{R},\cdot)$, $(\mathbb{Q},\cdot)$, and $(\mathbb{C},\cdot)$ is a group.

- Define $\mathbb{Z}^* = \mathbb{Z} - \{0\} = \{\ldots,-2,-1,1,2,\ldots\}$, $\mathbb{R}^* = \mathbb{R} - \{0\}$, $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, and $\mathbb{C}^* = \mathbb{C} - \{0\}$.

  Then $\mathbb{R}^*$, $\mathbb{Q}^*$, and $\mathbb{C}^*$ are all abelian group under ordinary multiplication.

the set of residue classes modulo n

- For $n > 1$, define $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$, where

$$[0] = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$$
$$[1] = \{\ldots, -2n+1, -n+1, 1, n+1, 2n+1, \ldots\}$$
$$\vdots$$
$$[n-1] = \{\ldots, -2n+(n-1), -n+(n-1), (n-1), n+(n-1), 2n+(n-1), \ldots\}.$$

Equivalence classes

For example, $\mathbb{Z}_3 = \{[0], [1], [2]\}$, where

$0 + 3 \times 2$

$$[0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\} = \{0 + 3k \mid k \in \mathbb{Z}\}$$
$$[1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\} = \{1 + 3k \mid k \in \mathbb{Z}\}$$
$$[\boxed{2}] = \{\ldots, -4, -1, 2, 5, 8, \ldots\} \quad \{2 + 3k \mid k \in \mathbb{Z}\}$$

is the least non-negative remainder when each integer in this class is divided by 3.

$1 + 3 \times (-2)$

Note that $[0], [1]$, and $[2]$ are pairwise disjoint, and $[0] \cup [1] \cup [2] = \mathbb{Z}$.

Also, we define $\mathbb{Z}_n^* = \{[1], [2], \ldots, [n-1]\} = \mathbb{Z}_n - \{[0]\}$.

In $\mathbb{Z}_n$ we often write a for $[a] = \{a + nk \mid k \in \mathbb{Z}\}$.

- For $n \in \mathbb{Z}^+$, $n > 1$, $(\mathbb{Z}/n, +)$ is an abelian group.
- When p is prime, $(\mathbb{Z}/^*_p, \cdot)$ is also an abelian group.

Example 2(a) Prove that $(\mathbb{Z}/_6, +)$ is an abelian group.

Solution: $\mathbb{Z}/_6 = \{[0], [1], [2], [3], [4], [5]\}$.

Composition table (dropping the square brackets)

+	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	0	1	2	3	4	5

$[4] + [3] = [4+3]$
$= [7]$
$= [1]$

7 when divided by 6 leaves remainder 1.

1. Closure property. We see that all the entries in the composition table are elements of the set $\mathbb{Z}/_6$. Therefore $\mathbb{Z}/_6$ is closed under addition.

2. Associativity: $(a+b)+c = a+(b+c) \ \forall \ a, b, c \in \mathbb{Z}/_6$.

2. Associativity: $(a+b)+c = a+(b+c) \ \forall \ a, b, c \in \mathbb{Z}/_6$.

Therefore the composition '+' is associative.

3. Existence of Identity. We have $[0] \in \mathbb{Z}/_6$. If a is any element of $\mathbb{Z}/_6$, then from the composition table we see that

$$a + [0] = a = [0] + a.$$

Therefore, 0 is an identity element.

4. Existence of Inverse. From the table we see that the inverse of $[0], [1], [2], [3], [4], 5$ are $[0], [5], [4], [3], [2], [1]$ respectively.

For example, $[2]+[4] = [2+4] = [6] = [2] = [4]+[2]$ implies $[4]$ is the inverse of $[2]$.

5. Commutativity. $a+b = b+a \ \forall \ a, b \in \mathbb{Z}/_6$.

Therefore, $(\mathbb{Z}/_6, +)$ is an abelian group.

Example 2(b) Prove that $(\mathbb{Z}_5^*, \cdot)$ is an abelian group.

Solution: $\mathbb{Z}_5^* = \{[1], [2], [3], [4]\}$

$\hookrightarrow$ prime

Composition table

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	2	4	2
4	4	3	2	1

$$[3]\cdot[4] = [3\cdot 4]$$
$$= [12]$$
$$= [2]$$
$$12 \equiv 2 \pmod 5$$

1. closure property. All the entries in the composition table are elements of $\mathbb{Z}/_5^*$. Therefore $\mathbb{Z}/_5^*$ is closed with respect to addition.

2. Associativity. $(a+b)+c = a+(b+c) \quad \forall a, b, c \in \mathbb{Z}/_5^*$.

3. Existence of Identity. We have $[1] \in \mathbb{Z}/_5^*$. If a is an element of $\mathbb{Z}/_5^*$, then from the composition table we see that

$$a + [1] = a = [1] + a.$$

$\therefore$ $[1]$ is the identity element.

4. Existence of Inverse. From the table we see that the inverse of $[1], [2], [3], [4]$ are $[1], [3], [2], [4]$ respectively.

For example, $[2]\cdot[3] = [2\cdot 3] = [6] = [1] = [3]\cdot[2]$ implies

[3] is the inverse of [2].

5. Commutativity. $a+b = b+a \quad \forall\, a,b \in \mathbb{Z}_5^*$.

Therefore, $(\mathbb{Z}_5^*, \cdot)$ is an abelian group.

Order of a group

- For every group G the number of elements in G is called its order.
  We denote it by $|G|$.
- If $|G| < \infty$, G is called finite group. Otherwise, it is called non finite group.
- For each $n \in \mathbb{Z}^+$, $|(\mathbb{Z}_n, +)| = n$, while $|(\mathbb{Z}_p^*, \cdot)| = p-1$ for each prime p.
  - $|(\mathbb{Z}_6, +)| = 6$.
  - $|(\mathbb{Z}_5^*, \cdot)| = 5-1 = 4$.
  - $|(\mathbb{Z}, +)| = \infty$.
  - $|(\mathbb{Z}^*, \cdot)| = \infty$.

Theorem 1 → Optional

For every group G,

a) the identity of G is unique.

b) the inverse of each element of G is unique.

c) if $a,b,c \in G$ and $ab = ac$, then $b = c$. [left-cancellation property]

d) if $a, b, c \in G$ and $ba = ca$, then $b = c$. [Right cancellation property]

Subgroup Let G be a group and H be a non-empty subset of G. If H is a group under the binary operation of G, then we call H a subgroup of G.

For example, $(2\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$.

Example 3 Let $G = (\mathbb{Z}_6, +)$. If $H = \{0, 2, 4\}$, then H is non-empty subset of G.
Show that $(H, +)$ is a subgroup of G.

Solution: $H = \{0, 2, 4\}$

Composition table

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

- $a + b \in H \quad \forall\, a, b \in H$. ✓
- $(a+b)+c = a+(b+c) \quad \forall\, a, b, c \in H$. ✓

- $a + 0 = a = 0 + a \ \forall a \in H$.

  Therefore, 0 is the identity element. ✓

- The inverse of $0, 2, 4$ are $0, 4, 2$ respectively. ✓

Thus $(H, +)$ is a group.

$\phi \neq H \subseteq G$ and $(H, +)$ is a group $\Rightarrow (H, +)$ is a subgroup of G.

Theorem 2 If H is a non empty subset of a group G, then H is a subgroup of G if and only if

(a) $ab \in H \quad \forall a, b \in H$

(b) $a^{-1} \in H \quad \forall a \in H$.

Theorem 3 If G is a group and $\phi \neq H \subseteq G$, with H finite, then H is a subgroup of G if and only if H is closed under the binary operation of G.

Exercises

Q.3 Why is the set $\mathbb{Z}$ not a group under subtraction?

Solution: $1, 2, 3 \in \mathbb{Z}$, but $1 - (2 - 3) \neq (1 - 2) - 3$. [Associativity]

Therefore, $(\mathbb{Z}, -)$ is not a group.

Q.15 If G is a group, let $H = \{a \in G \mid ag = ga \text{ for all } g \in G\}$. Prove that H is a subgroup of G.

Solution: Let e be the identity element of the group G.

By definition: $eg = g = ge \quad \forall g \in G$.

Therefore H contains e i.e., $e \in H$.

- If a and b are in H, then so is ab; by associativity:

$$(ab)g = a(bg) = a(gb) = (ag)b = g(ab) \quad \forall g \in G$$

Therefore H is closed.

- If $a \in H$, then so does a^{-1} as, for all $g \in G$,

$$(ag = ga) \Rightarrow (a^{-1}aga^{-1} = a^{-1}gaa^{-1})$$
$$\Rightarrow \quad ga^{-1} = a^{-1}g.$$

Therefore, by theorem 2, H is a subgroup of G.

Q.1 For each of the following sets, determine whether or not the set is a group under the stated bynary operation. If so, determine its identity and inverse of each of its element. If it is not a group, state the condition(s) of the definition that it violets.

(a) $\{-1, 1\}$ under multiplication.

Ans. YES

My Notebook - OneNote for Windows 10

- $a \cdot b \in \{-1, 1\} \quad \forall \; a, b \in \{-1, 1\}$.
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall \; a, b, c \in \{-1, 1\}$.
- $1 \in \{-1, 1\}$ and $1 \cdot a = a = a \cdot 1 \quad \forall \; a \in \{-1, 1\}$.

  Therefore 1 is the identity element.
- $\left. \begin{array}{l} 1 \cdot 1 = 1 = 1 \cdot 1 \\ (-1) \cdot (-1) = 1 = (-1)(-1) \end{array} \right\}$ Inverse of 1 is 1 and the inverse of -1 is -1.

(b) $\{-1, 1\}$ under addition.

Ans. NO!

$-1, 1 \in \{-1, 1\}$, but $-1 + (1) = 0 \notin \{-1, 1\}$.

$\{-1, 1\}$ is not closed under addition.

(c) $\{-1, 0, 1\}$ under addition.

Ans. NO!

$1, 1 \in \{-1, 0, 1\}$ but $1 + 1 = 2 \notin \{-1, 0, 1\}$.

$\{-1, 0, 1\}$ is not closed under addition.

(d) $\{10n \mid n \in \mathbb{Z}\}$ under addition.

Ans. YES

$10\mathbb{Z} = \{10n \mid n \in \mathbb{Z}\} = \{\ldots, -20, -10, 0, 10, 20, \ldots\}$.

- $a + b \in 10\mathbb{Z} \quad \forall \; a, b \in 10\mathbb{Z}$.

- $a+(b+c) = (a+b)+c \quad \forall\, a,b,c \in 10\mathbb{Z}$.
- $0 \in 10\mathbb{Z}$ and

  $a+0 = a = 0+a \quad \forall\, a \in 10\mathbb{Z}$.

  Therefore 0 is the identity element.
- For $a \in 10\mathbb{Z}$, $-a \in 10\mathbb{Z}$ s.t.

  $a+(-a) = (-a)+a = 0$.

  Therefore the inverse of a is $-a$.

(e) The set of all one to one functions $g: A \to A$, where $A = \{1,2,3,4\}$, under function composition.

Ans. YES

- closure property. Let f and g be two one to one function in the set. We need to show that $g \circ f$ is a one-to-one function.

  Since f and g are one-to-one, for any distinct elements x and y in A, $f(x) \neq f(y)$ and $g(f(x)) \neq g(f(y))$. This implies that $g \circ f$ is also one-to-one.
- Associativity. For any three functions $f, g,$ and h in the set, we have to show that $(h \circ g) \circ f = h \circ (g \circ f)$.

  For any $x \in A$:

  $$(h \circ g) \circ f(x) = (h \circ g)(f(x)) = h(g(f(x)))$$
  $$h \circ (g \circ f)(x) = h(g \circ f(x)) = h(g(f(x))).$$

Therefore, $(h \circ g) \circ f = h \circ (g \circ f)$, and associativity holds.

- **Existence of Identity.** Define $e(x) = x$ for all $x \in A = \{1, 2, 3, 4\}$.

  Note that for any function f in the set:

  $$(e \circ f)(x) = e(f(x)) = f(x).$$

  $$(f \circ e)(x) = f(e(x)) = f(x).$$

  So, e is the identity element.

- Let f be any one-to-one function in the set.

  Then for any $x \in A$:

  $$f \circ f^{-1}(x) = f(f^{-1}(x)) = x = e(x).$$

  $$f^{-1} \circ f(x) = f^{-1}(f(x)) = x = e(x).$$

  Thus, f^{-1} is the inverse of f.

H.W. Q.8, Q.10 [Exercises 16.1]