

Lecture 10

Friday, 26/8/2022

Note Title

8/26/2022

Textbook: Contemporary Abstract Algebra by Joseph A. Gallian,
Publisher - Narada.

Let G be a non-empty set. A binary operation $*$ on G is a map $*$: $G \times G \rightarrow G$.

If $*$ is a binary operation on G , we also say that G is closed under $*$.

Algebraic Structures: Let $*$ be a binary operation on G .

1. (Semigroup): $(G, *)$ is called a semigroup if $*$ is associative, that is, $a * (b * c) = (a * b) * c \quad \forall a, b, c \in G$.

- An element $e \in G$ is called an identity element if

$$e * a = a = a * e \quad \forall a \in G.$$

(2) Monoid: A monoid is a semigroup $(G, *)$ with an identity element.

- Let $a \in G$, where $(G, *)$ is a monoid. An element $b \in G$ is said to be an inverse of a if $a * b = e = b * a$.

(3) Group: A group is a monoid $(G, *)$ where every element has an inverse.

Examples: Semigroups: $(\mathbb{N}, +)$, (\mathbb{N}, \cdot) , $(\mathbb{Z}, +)$, (\mathbb{Z}, \cdot) , $(\mathbb{Q}, +)$

(\mathbb{Q}, \cdot) , $(\mathbb{R}, +)$, (\mathbb{R}, \cdot) , $(\mathbb{C}, +)$, (\mathbb{C}, \cdot)

Monoid: (\mathbb{N}, \cdot) , $(\mathbb{Z}, +)$, (\mathbb{Z}, \cdot) , $(\mathbb{Q}, +)$, (\mathbb{Q}, \cdot) , $(\mathbb{R}, +)$, $(\mathbb{C}, +)$

Groups: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, (\mathbb{Q}^*, \cdot) , (\mathbb{C}^*, \cdot) .

(\mathbb{R}^*, \cdot) . Here $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, $\mathbb{C}^* = \mathbb{C} - \{0\}$, $\mathbb{R}^* = \mathbb{R} - \{0\}$.

$\mathbb{R}_{>0} = (0, \infty)$ is a group under multiplication.

- There is no finite subset of \mathbb{N} which is closed under $+$
- The only finite subset of \mathbb{Z} which is closed under $+$ is $\{0\}$

- The only finite subset of \mathbb{N} which is closed under multiplication is $\{1\}$.

- The only finite subsets of \mathbb{Z} closed under multiplication are $\{0\}$, $\{1\}$, $\{-1\}$, $\{-1, 0, 1\}$, $\{0, 1\}$.

Theorem 1: In a monoid $(G, *)$, identity element is unique.

Proof: Let e_1 and e_2 be two identity elements. Then,

$$e_1 * e_2 = e_1 = e_2 * e_1 \quad (\because e_2 \text{ is an identity element})$$

$$\text{and } e_1 * e_2 = e_2 = e_2 * e_1 \quad (\because e_1 \text{ is an identity element})$$

$$\therefore e_1 = e_2.$$

\neq

Theorem 2: In a monoid $(G, *)$, if $a \in G$ has an inverse, then the inverse is unique. Hence, in a group, inverse of every element is unique.

Proof: $a \in G$ has an inverse. Suppose that $b, c \in G$ are such that $a * b = e = b * a$ and $a * c = e = c * a$.

Now, $b = b * e = b * (a * c) = (b * a) * c = e * c = c$.

This completes the proof.

Notation: The inverse of a is denoted by a^{-1} .

- $a^0 = e$, if $n \geq 1$, then $a^n = a * a * \dots * a$ (n -times)
if $n \leq -1$, write $n = -m$ where $m \geq 1$. Then, $a^n = a^{-1} * \dots * a^{-1}$ (m -times)

- For $n \geq 1$, $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ is a group under addition modulo n .
- \mathbb{Z}_n is a **monoid** under multiplication modulo n .

$U(n)$ = the elements of \mathbb{Z}_n having inverse under multiplication modulo n .

$$= \{k \mid 1 \leq k \leq n, \gcd(k, n) = 1\}$$

$U(n)$ has $\varphi(n)$ number of elements.

$$g_n \quad U(4) = \{1, 3\}, \quad 1^{-1} = 1, \quad 3^{-1} = 3$$

$$U(5) = \{1, 2, 3, 4\}, \quad 1^{-1} = 1, \quad 2^{-1} = 3, \quad 3^{-1} = 2, \quad 4^{-1} = 4.$$

Definition: Let G be a group. If G is finite, then the order of G is defined to be the number of elements in G . If G is infinite, then the order of G is defined to be infinite. The order of G is denoted by $|G|$.

Ex: $|\mathbb{Z}_n| = n$, $|\cup(n)| = \varphi(n)$, order of $(\mathbb{Z}, +)$ is infinite.

Let $a \in G$. The smallest positive integer n satisfying $a^n = e$ is called the order of a , and is denoted by $O(a)$ or $|a|$. If no such n exists, then $O(a)$ is defined to be infinite.

Ex: • g_n any group, order of the identity element is 1.

• $g_n (\mathbb{Z}, +)$, if $n \neq 0$, then $O(n)$ is infinite.

• $g_n \mathbb{Z}_6$, $O(0)=1$, $O(1)=6$, $O(2)=3$, $O(3)=2$, $O(4)=3$, $O(5)=6$.

• $g_n U(6) = \{1, 5\}$, $O(1)=1$ and $O(5)=2$.

• $g_n U(12) = \{1, 5, 7, 11\}$, $O(1)=1$, $O(5)=2$, $O(7)=2$,

$O(11)=2$.

Let G be a group. For $a \in G$, we denote $\langle a \rangle$ the set $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$. #

Theorem: If $O(a) = n$ in a group G , then

$$\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}.$$

If $O(a)$ is infinite, then $a^i \neq a^j$ whenever $i \neq j$.

Proof. We have $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$.

We first prove that $e, a, a^2, \dots, a^{n-1}$ are all distinct elements. Suppose that $a^i = a^j$ for some $i < j$ and

$$\text{Then, } a^{-i} \cdot a^i = a^{j-i} \Rightarrow a^{j-i} = e \quad 0 \leq i, j < n-1.$$

Since $0 < j-i < n$, so this is a contradiction to the fact that $O(a) = n$. Hence, e, a, \dots, a^{n-1} are all distinct.

Now, let $a^k \in \langle a \rangle$. By division algorithm, we have $k = nq + r$, where $0 \leq r < n-1$.

$$\therefore a^k = a^{n \cdot q + r} = (a^n)^q \cdot a^r = e \cdot a^r = a^r.$$

$$\text{Hence, } \langle a \rangle = \{a^k \mid k \in \mathbb{Z}\} = \{e, a, a^2, \dots, a^{n-1}\}.$$

For the 2nd part, let $O(a) = \infty$ but $a^i = a^j$ for some $i < j$.
Then, we have $a^{j-i} = e$.

$\Rightarrow O(a) \leq j-i$, which is a contradiction as $O(a) = \infty$.
 \therefore If $O(a) = \infty$, then $a^i \neq a^j$ whenever $i \neq j$. \neq