Lecture 2: Groups

Prof. Dr. Ali Bülent EKİN
Doç. Dr. Elif TAN

Ankara University

Definition

Let G be a nonempty set and the binary operation $*$ defined on G. $(G, *)$ is called a **group** if the following conditions are satisfied:

G_1) **Associative:** $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.

G_2) **Identity element:** $\exists\ e \in G$ such that $a * e = e * a = a$ for all $a \in G$.

G_3) **Inverse element:** For each $a \in G, \exists\ a' \in G$ such that $a * a' = a' * a = e$.

For simplicity we denote a group $(G, *)$ as G.

Remark:

- The identity element (zero element) of the group G is e.
- The inverse of an element a is a'.
- A group G is **abelian** if its binary operation is commutative, that is,

$$a * b = b * a \text{ for all } a, b \in G.$$

- For conventional notation, the inverse of an element a is a^{-1} for $(G, .)$ and the inverse of an element a is $-a$ for $(G, +)$.

Examples:

1. $(\mathbb{Z}^+, +)$ is not a group. (No identity element)

2. $(\mathbb{Z}_{\geq 0}, +)$ is not a group. (No inverse element)

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

4. $(\mathbb{Z}^+, \cdot)$ is not a group. (1 is identity element, but no inverse of 3)

5. $(\mathbb{Q}^+, \cdot), (\mathbb{R}^+, \cdot), (\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$ are commutative groups.

6. $(M_{m\times n}(\mathbb{R}), \oplus)$ is an abelian group.

7. $(M_n(\mathbb{R}), \odot)$ is not a group. (Zero matrix has no inverse)

8. $(GL(n, \mathbb{R}) = \{A_{n\times n} \mid \det A \neq 0\}, \odot)$ is a noncommutative group.

9. $(\mathbb{Z}_n, +_n)$ is a commutative group.

10. $(\mathbb{Z}_n, ._n)$ is not a group. $(\bar{0}$ has no inverse)

11. $(\mathbb{Z}_n^\star = \{\bar{a} \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}, ._n)$ is a group.

12. $\left(V_4 = \left\{e, a, b, c \mid a^2 = b^2 = e, ab = c\right\}, \cdot\right)$ is a group, called as Klein-4 group.

13. $(Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}, \cdot)$ is a noncommutative group, called as quaternion group, with multiplication defined as

$$i^2 = j^2 = k^2 = ijk = -1.$$

Let $(G, *)$ be a group. For $n \in \mathbb{Z}, a \in G$,

$$a^n = \begin{cases} \underbrace{a * a * \cdots * a}_{n}, & n > 0 \\ e, & n = 0 \\ \underbrace{a' * a' * \cdots * a'}_{|n|}, & n < 0. \end{cases}$$

Elementary properties of groups

Let $(G, *)$ be a group. Then we have the followings:

- The cancellation laws hold: For all $a, b, c \in G$,
  The left cancellation law: If $a * b = a * c$, then $b = c$.
  The right cancellation law: If $b * a = c * a$, then $b = c$.
- For $a, b \in G$, the linear equations $a * x = b$ and $y * a = b$ have unique solutions in G.
  Remark: By means of this result, one can say that every element of G appears exactly once in every column in the group table of G.
- G has a unique identity.
- Each element in G has a unique inverse.
- For all $a, b \in G$, $(a * b)' = b' * a'$.

Elementary properties of groups

Theorem

Let $\emptyset \neq G$ *and* $*$ *be a binary operation on* G*. If*
(i) $*$ *is associative*
(ii) *Left identity:* $\exists e \in G$ *such that* $e * x = x$ *for all* $x \in G$
(iii) *Left inverse: For each* $a \in G$, $\exists a' \in G$ *such that* $a' * a = e$,
then $(G, *)$ *is a group.*

Theorem

Let $\emptyset \neq G$ *and* $*$ *be a binary operation on* G*. If*
(i) $*$ *is associative*
(ii) $a * x = b$ *and* $y * a = b$ *have solutions in* G *for all* $a, b \in G$,
then $(G, *)$ *is a group.*

Theorem

Let $\emptyset \neq G$ is **finite** *and $*$ be a binary operation on G. If*
(i) $*$ is associative
(ii) the cancellation laws hold,
then $(G, *)$ is a group.

Remarks:

- Let $(G, *)$ be a group. If $x * x = x$ for $x \in G$, then x is called an **idempotent element.** Show that a group G has exactly one idempotent.
- Let $(G, *)$ be a group. If $x * x = e$ for all $x \in G$, then G is abelian.
- Let $(G, .)$ be a group. If $x^{-1} = x$ for all $x \in G$, then G is abelian.