

Lecture 17 (Group and its properties)

Definition 1 Let G be a set. A function $*$: $G \times G \rightarrow G$ is called a binary operation.

Examples: Let \mathbb{C} , \mathbb{R} , \mathbb{Q} , \mathbb{Z} , \mathbb{N} denote the set of complex numbers, the set of real numbers, the set of rational numbers, the set of integers, the set of natural numbers respectively. Let $M_{m \times n}(G)$ denote the set of $m \times n$ matrices whose entries are from the set G .

1. The operation $+$ in \mathbb{C} , \mathbb{R} , \mathbb{Q} , \mathbb{Z} , \mathbb{N} is binary. The operation $-$ is a binary operation on \mathbb{R} , \mathbb{C} , \mathbb{Q} , and \mathbb{Z} but not in \mathbb{N} .
2. The usual matrix addition is a binary operation in $M_{m \times n}(G)$, where $G \in \{\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}\}$.

Definition 2 A group is a pair $(G, *)$, where G is a set and $*$ is a binary operation on G , such that the following axioms hold:

1. (Associative law) $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.
2. (Existence of an identity) There exists an element $e \in G$ with the property that $e * a = a$ and $a * e = a$ for all $a \in G$.
3. (Existence of an inverse) For each $a \in G$ there exists an element $b \in G$ such that $a * b = b * a = e$.

Definition 3 A group $(G, *)$ is called an abelian or commutative group if $a * b = b * a$ for all $a, b \in G$.

Proposition 1 • **(Uniqueness of the Identity:)** The identity e is the unique element in G : To see this suppose we have another identity f . Using the fact that both of these are identities we see that

$$f = f * e = e.$$

We will usually denote this element by 1 (or by 0 if the group operation is commutative).

- **(Uniqueness of Inverses:)** The inverse $b \in G$ of $a \in G$ is unique. To see this suppose that c is another inverse to a . Then

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

We call this unique element b , the inverse of a . It is often denoted a^{-1} (or $-a$ when the group operation is commutative). For simplicity, we write ab for $a * b$.

- **(Cancellation:)** In a group G , the right and left cancellation laws hold; that is, $ba = ca$ implies $b = c$, and $ab = ac$ implies $b = c$.

Proof: Suppose $ba = ca$. Let a^{-1} be an inverse of a . Then, multiplying on the right by a^{-1} yields $(ba)a^{-1} = (ca)a^{-1}$. Associativity yields $b(aa^{-1}) = c(aa^{-1})$. Then, $be = ce$ and, therefore, $b = c$ as desired. Similarly, one can prove that $ab = ac$ implies $b = c$ by multiplying by a^{-1} on the left.

- **(Socks-Shoes Property:)** For group elements a and b , $(ab)^{-1} = b^{-1}a^{-1}$.

Proof: Since $(ab)(ab)^{-1} = e$ and $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$, we have by uniqueness of inverses that $(ab)^{-1} = b^{-1}a^{-1}$.

Examples:

1. The group of integers $(\mathbb{Z}, +)$ and $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ with respect to addition are abelian groups.
2. The set \mathbb{R}^* of nonzero real numbers is a group under ordinary multiplication. The identity is 1. The inverse of a is $1/a$.
3. The set $\mathbb{Z}_n = \{0, 1, \dots, n - 1\}$ for $n \geq 1$ is a group under addition modulo n . For any $j \in \mathbb{Z}_n$, the inverse of j is $n - j$. This group is usually referred to as the group of integers modulo n .
4. The set $\{1, 2, \dots, n - 1\}$ is a group under multiplication modulo n if and only if n is prime.
5. The subset $\{1, -1, i, -i\}$ of the complex numbers is a group under complex multiplication. Note that -1 is its own inverse, whereas the inverse of i is $-i$, and vice versa.
6. Let X be a set and let $Sym(X)$ be the set of all bijective maps from X to itself. Then $Sym(X)$ is a group with respect to composition, \circ , of maps. This group is called the symmetric group on X and we often refer to the elements of $Sym(X)$ as permutations of X . When $X = \{1, 2, 3, \dots, n\}$ the group is often denoted S_n and called the symmetric group on n letters.

7. The set of all $n \times n$ matrices with determinant 1 with entries from \mathbb{Q} , \mathbb{R} , \mathbb{C} , or \mathbb{Z}_p (p a prime) is a non-Abelian group under matrix multiplication. This group is called the special linear group of $n \times n$ matrices over \mathbb{Q} , \mathbb{R} , \mathbb{C} , or \mathbb{Z}_p , respectively.
8. The set of all 2×2 matrices with real number entries is not a group under the matrix multiplication operation. Inverses do not exist when the determinant is 0.
9. The set $\{0, 1, 2, 3\}$ is not a group under multiplication modulo 4. Although 1 and 3 have inverses, the elements 0 and 2 do not.
10. The set of integers under subtraction is not a group, since the operation is not associative.

Definition 4 A subset H of a group G with the binary operation $*$ is called a subgroup if H is itself a group under the operation $*$.

Subgroup Test. Let $(G, *)$ be a group and H be a non-empty subset of G . Then H is a subgroup of G if the following conditions holds:

1. If $a, b \in H$ then $ab \in H$.
2. If $a \in H$ then $a^{-1} \in H$.

Note: One can replace the above two conditions in one as: a non-empty subset H of G is a subgroup if $a, b \in H$ then $a^{-1}b \in H$.

Definition 5 The number of elements of a group (finite or infinite) is called the order of the group. We will use $|G|$ to denote the order of a group G .

Example: The group \mathbb{Z} of integers under addition has infinite order, whereas the group $U(10) = \{1, 3, 7, 9\}$ under multiplication modulo 10 has order 4.

Definition 6 The order of an element g in a group G is the smallest positive integer n such that $g^n = e$. In additive notation, this would be $ng = 0$. If no such integer exists, we say that g has infinite order. The order of an element g is denoted by $|g|$.

Example: Consider \mathbb{Z}_{10} under addition modulo 10. Since $2 + 2 = 4, 2 + 2 + 2 = 6, 2 + 2 + 2 + 2 = 8, 2 + 2 + 2 + 2 + 2 = 0$, we know that $|2| = 5$. Similar computations show that $|0| = 1, |7| = 10, |5| = 2, |6| = 5$.

Definition 7 A group G is called cyclic if there is an element a in G such that $G = \{a^n : n \in \mathbb{Z}\}$. Such an element a is called a generator of G .

Definition 8 Let G be a group and H a subgroup of G . For any $a \in G$, the set $aH = \{ah : h \in H\}$ is called the left coset of H in G , similarly Ha is called the right coset of H in G .

Properties of Cosets: Let H be a subgroup of G , and let a and b belong to G . Then,

1. $a \in aH$,

Proof: $a = ae$, where e is the identity element of H .

2. $aH = H$ if and only if $a \in H$,

Proof: Let $aH = H$. Then $a = ae \in aH = H$. So $a \in H$.

Let $a \in H$. Then $aH \subseteq H$ by closure property of H . Now, to show that $H \subseteq aH$, let $h \in H$. Then $a^{-1}h \in H$. Thus $h = eh = a(a^{-1}h) \in aH$. Hence $H \subseteq aH$.

3. $aH = bH$ if and only if $a \in bH$.

Proof. Let $aH = bH$. Then $a = ae \in aH = bH$. So $a \in bH$.

Let $a \in bH$. Then $a = bh$ for some $h \in H$ and then $aH = bhH = bH$ (by Property 2).

4. $aH = bH$ or $aH \cap bH = \emptyset$.

Proof. Suppose $x \in aH \cap bH$. Then $x \in aH$ and $x \in bH$. Then by Property 3, $xH = aH$ and $xH = bH$. Thus $aH = bH$.

5. $aH = bH$ if and only if $a^{-1}b \in H$.

Proof. By Property 2, $a^{-1}b \in H$ if and only if $a^{-1}bH = H \Leftrightarrow bH = aH$.

6. $|aH| = |bH|$.

Proof. Define a map $f : aH \rightarrow bH$ by $f(ah) = bh$. Then the map f is bijective.

7. $aH = Ha$ if and only if $H = aHa^{-1}$.

Proof. $aH = Ha \Leftrightarrow aHa^{-1} = Haa^{-1} = H$.

8. aH is a subgroup of G if and only if $a \in H$.

Proof. Let $a \in H$ then $aH = H$. So aH is a subgroup. On the other hand if aH is a subgroup of then $e \in aH$ and so $eH \cap aH \neq \emptyset$. So $aH = eH = H$.

9. $x^{-1}y \in H$ if and only if $y \in xH$.

Remark. Suppose G is a group with a subgroup H . Define a relation \mathcal{R} on G as follows:

$$x\mathcal{R}y \text{ iff } x^{-1}y \in H.$$

This relation is an equivalence relation. Note that $x\mathcal{R}y$ iff $x^{-1}y \in H$ iff (by Property 9) $y \in xH$. Hence the equivalence class of x is $[x] = xH$, the left coset of H in G .

Theorem 1 (Lagrange's Theorem:) Let G be a finite group with a subgroup H , with $|H| = r$. Then $|H|$ divides $|G|$.

Proof: Let a_1H, a_2H, \dots, a_rH be the distinct left cosets of H in G . By the above remark

$$G = a_1H \cup a_2H \cup \dots \cup a_rH \Rightarrow |G| = |a_1H| + |a_2H| + \dots + |a_rH|.$$

By Property 6,

$$|a_1H| = |a_2H| = \dots = |a_rH| = |H|.$$

Thus $|G| = r|H|$. Thus the proof. □

Corollary: If G is a group of finite order m , then the order of any $a \in G$ divides the order of G and in particular $a^m = e$.

Remark. The converse of Lagrange's theorem is not always true. Consider A_4 (Alternating group of four elements), which consists of even permutations. Note that $|A_4| = 12$ and 6 divides 12, but A_4 has no subgroup of order 6 (Check it !).

Definition: (Normal Subgroup) A subgroup H of a group G is called a normal subgroup if $aH = Ha$ for all $a \in G$. We denote this as $H \triangleleft G$.

Normal Subgroup Test. A subgroup H of G is said to be a normal subgroup if

$$g^{-1}Hg \subseteq H \quad \forall g \in G.$$

Definition: Let G be a group with a subgroup H . The number of left cosets of H in G is called the index of H in G and is denoted by $[G : H]$.

Note:

- Every subgroup N of an abelian group G is normal.
- The trivial subgroup $\{e\}$ and G itself are always normal subgroups of G .
- If H is a subgroup of G such that $[G : H] = 2$ then H is normal subgroup of G .

Definition: Let $(G, *)$, (H, \circ) be groups. A map $\Phi : G \rightarrow H$ is a homomorphism if

$$\Phi(a * b) = \Phi(a) \circ \Phi(b)$$

for all $a, b \in G$. Furthermore Φ is an isomorphism if it is bijective.

Example: Let \mathbb{R}^+ be the set of all the positive real numbers. There is a (well-known) isomorphism $\Phi : (\mathbb{R}, +) \rightarrow (\mathbb{R}^+, \cdot)$ given by $\Phi(x) = e^x$.

Properties of Homomorphism. Let $(G, *)$ and (H, \circ) be groups and $\Phi : G \rightarrow H$ a homomorphism. Then

1. $\Phi(e_G) = e_H$.
2. $\Phi(a^{-1}) = (\Phi(a))^{-1}$ for all $a \in G$.
3. If K is a subgroup of G , then $\Phi(K)$ is a subgroup of H .
4. If S is a subgroup of H , then $\Phi^{-1}(S)$ is a subgroup of G .
5. The order of $\Phi(a)$ divides the order of a in G .