Lecture 1 (Groups & Fields)

Definition: 1. Let G be a non empty set. A function $* : G \times G \longrightarrow G$ is called a **binary operation** on G.

Definition: 2. A non empty set G together with a binary operation $*$ is called a **group**, denoted as $(G, *)$, if it satisfies the following three properties:

1. $a * (b * c) = (a * b) * c \quad \forall \quad a, b, c \in G$ (Associativity);
2. there exists a unique element $e \in G$ such that $a * e = e * a = a \quad \forall a \in G$. The element e is called the identity element of G (Existence of identity);
3. for each $a \in G, \quad \exists \quad b \in G$ such that $a * b = b * a = e$. The element b is called the inverse of a and is denoted as a^{-1} (Existence of inverse).

In addition, if a group $(G, *)$ satisfies $a * b = b * a \quad \forall \quad a, b \in G$, then G is called a **commutative or an abelian group**.

Examples:

1. The set of real numbers $\mathbb{R}$, set of rational numbers $\mathbb{Q}$, set of integers $\mathbb{Z}$ form a group under usual addition.
2. The set of all $m \times n$ matrices with real entries $M_{m \times n}(\mathbb{R})$ forms a group under matrix addition.
3. Let $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$. Then $(Q^*, *)$ is a group under the usual multiplication. Similarly, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ and $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ are groups under usual multiplication.
4. **Permutation/Symmetric Groups:** Let $S_n = \{\sigma \mid \sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ is a bijection$\}$. Then, S_n has $n!$ elements and forms a group with respect to composition of functions.

   Let $\sigma \in S_n$. Then,

   (a) σ can be written as $\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$.

   (b) σ is one-one. Hence, $\{\sigma(1), \sigma(2), \ldots, \sigma(n)\} = \{1, 2, \ldots, n\}$ and thus, $\sigma(1)$ has n choices, $\sigma(2)$ has $n - 1$ and so on. Therefore, S_n has $n!$ elements.

   (c) $\sigma_1 \circ \sigma_2 \in S_n$ for any $\sigma_1, \sigma_2 \in S_n$. Thus, the operation $\circ$ on S_n is binary.

   (d) the associativity holds as $\sigma_1 \circ (\sigma_2 \circ \sigma_3) = (\sigma_1 \circ \sigma_2) \circ \sigma_3$ for all permutations $\sigma_1, \sigma_2, \sigma_3 \in S_n$. (Check yourself!)

   (e) the permutation $\sigma_0 \in S_n$ given by $\sigma_0(i) = i$ for $1 \leq i \leq n$ is the identity element of S_n.

   (f) for each $\sigma \in S_n$, σ^{-1} given by $\sigma^{-1}(m) = l$ if $\sigma(l) = m$ is the inverse element of σ in S_n. (Exercise: Show that σ^{-1} is well-defined and a bijection.)

Here, we discuss a few properties and results on permutation groups, which we will use later to define determinant function.

Proposition: 3. *Fix a positive integer n. Then, the group S_n satisfies the following:*

1. *Let $\tau \in S_n$. Then $\{\tau \circ \sigma : \sigma \in S_n\} = S_n$.*

2. *$S_n = \{\sigma^{-1} : \sigma \in S_n\}$.*

Proof. Part 1: Note that $\{\tau \circ \sigma : \sigma \in S_n\} \subseteq S_n$. Thus, $\{\tau \circ \sigma : \sigma \in S_n\} \neq S_n$ if and only if $\tau \circ \sigma_1 = \tau \circ \sigma_2$ for some $\sigma_1 \neq \sigma_2 \in S_n$, which is not possible. (Justify it!)

Part 2: Note that $\{\sigma^{-1} : \sigma \in S_n\} \subseteq S_n$ and equality does not hold only when $\sigma_1^{-1} = \sigma_2^{-1}$, where $\sigma_1 \neq \sigma_2 \in S_n$. But we know that $(\sigma^{-1})^{-1} = \sigma$ and get a contradiction.

Definition: 4 (Cyclic Notation)**.** *Let $\sigma \in S_n$. Suppose there exist r, $2 \leq r \leq n$ and $i_1, i_2, \ldots, i_r$ such that $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \ldots, \sigma(i_r) = i_1$ and $\sigma(j) = j$ for all $j \neq i_1, i_2, \ldots, i_r$. Then, we represent such a permutation by $\sigma = (i_1\, i_2\, \ldots\, i_r)$ and call it an r-cycle.*

For Example, $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 1 & 4 & 6 \end{pmatrix} = (1\,3\,5\,4)$ and $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix} = (2\,3)$.

Remark: 1. *1. Every permutation is either a cycle or product of disjoint cycles. For example,* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 6 & 3 & 5 & 7 & 1 & 4 & 9 & 8 \end{pmatrix} = (1\,2\,6)(4\,5\,7)(8\,9)$.

2. *A cycle of length 2 is called* **transposition**.

3. *For any cycle $(i_1\, i_2\, \ldots\, i_r)$, $(i_1\, i_2\, \ldots\, i_r) = (i_1\, i_r)(i_1\, i_{r-1}) \cdots (i_1\, i_2)$.*

4. *Every permutation is a product of transpositions. For example, $(1\,2\,3) = (1\,3)(1\,2)$ and* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 6 & 3 & 5 & 7 & 1 & 4 & 9 & 8 \end{pmatrix} = (1\,2\,6)(4\,5\,7)(8\,9) = (1\,6)(1\,2)(4\,7)(4\,5)(8\,9)$.

Definition: 5. *A permutation $\sigma \in S_n$ is called an* **even permutation** *if it can be written as product of even number of transpositions or it is the identity permutation and it is called an* **odd permutation** *if it can be written as a product of odd number of transpositions.*

Remark: 2. *1. A decomposition of a permutation into a product of transposition need not be unique. (Look for examples!)*

2. A permutation is either always even or always odd, that is, if a permutation can be expressed as a product of an even number of transpositions, then every decomposition of that permutation into transpositions must have an even number of transpositions.

Definition: 6. *A function sgn: $S_n \to \{1, -1\}$, called the* **signature of a permutation**, *by*

$$sgn(\sigma) = \begin{cases} 1 & \text{if } f \text{ is an even permutation} \\ -1 & \text{if } f \text{ is an odd permutation} \end{cases}$$

Remark: 3. *1. If σ and τ are both even or both odd permutations, then $\sigma \circ \tau$ and $\tau \circ \sigma$ are both even. Whereas, if one of them is odd and the other even then $\sigma \circ \tau$ and $\tau \circ \sigma$ are both odd.*

2. *The identity permutation* σ_0 *is an even permutation and hence* $sgn(\sigma_0) = 1$.

3. *A transposition is an odd permutation and hence its signature is -1.*

4. $sgn(\sigma \circ \tau) = sgn(\sigma)sgn(\tau)$.

Definition: 7. Let $\mathbb{F}$ be a non-empty set with two binary operations addition denoted as $+$ and multiplication denoted as $\cdot$. Then $\mathbb{F}$ is called a **field**, denoted as $(\mathbb{F}, +, \cdot)$, if

1. $\mathbb{F}$ is an abelian group under addition $+$;

2. $\mathbb{F}^* = \mathbb{F} \setminus \{e\}$ is an abelian group under multiplication ., where e denotes the additive identity of $\mathbb{F}$;

3. $a \cdot (b + c) = a \cdot b + a \cdot c \quad \forall \quad a, b, c \in \mathbb{F}$.

Definition: 8. Let $\mathbb{F}$ be a field and $\mathbb{F}_1 \subseteq \mathbb{F}$. Then $\mathbb{F}_1$ is said to be a **subfield** of $\mathbb{F}$ if $\mathbb{F}_1$ is itself a field under the same binary operations defined on $\mathbb{F}$.

Examples:

1. The set of complex numbers $\mathbb{C}$ forms a field under usual addition and multiplication of complex numbers.

2. The sets $\mathbb{R}$ and $\mathbb{Q}$ form a field under usual addition and multiplication.

3. The set of integers $\mathbb{Z}$ does not form a field under usual addition and multiplication.

4. $\mathbb{Q}$ is a subfield of $\mathbb{R}$ and $\mathbb{R}$ is a subfield of $\mathbb{C}$.

Note: The elements of a field are also called scalars.