Lecture 2

1 Groups

A large number of sets endowed with a binary operation have properties like the set of integers with addition.
These systems are called groups defined as follows:

Groups:
A group is a set G, together with a binary operation $*$, satisfying the following properties:

1. G is closed under $*$, i.e for all $a, b \in G$, $a * b = c \in G$.

2. $*$ is associative, i.e for all $a, b, c \in G$, we have
   $(a * b) * c = a * (b * c)$

3. G has a $*$ identity element i.e $\exists e \in G$ such that for all $a \in G$
   $a * e = e * a = a$

4. Every element in G has its $*$ inverse i.e for all $a \in G, \exists b \in G$ such that $a * b = b * a = e$
   b is called the $*$ inverse of a, denoted as, a^{-1}.

Note: Often $a * b$ is written as ab. This should not be confused with ordinary multiplication in numbers.

Examples:

- *Eg.*1 $\langle \mathbb{Z}, + \rangle$
- *Eg.*2 $\langle \mathbb{Q}, + \rangle$
- *Eg.*3 $\langle \mathbb{Q}^*, \times \rangle$, where $\mathbb{Q}^* = \mathbb{Q} - \{0\}$
- *Eg.*4 $G = \{a + b\sqrt{2}, a, b \in \mathbb{Q}\}$

  $\langle G, + \rangle$ is a group.

  $\langle G^*, \times \rangle$ where $G^* = G - \{0\}$?

  Existence of $(a + b\sqrt{2})^{-1}$ if $a^2 = 2b^2$?
  Such elements are not in G.
  So it is a group.

- *Eg.*5$\langle \mathbb{C}, + \rangle$ and $\langle \mathbb{C}^*, \times \rangle$ are groups.

- *Eg.*6 Set of all $n \times n$ real invertible matrices forms a group under the operation of matrix multiplication.

  This group is called the general linear group of order n, denoted as $GL_n(\mathbb{R})$.
  Similarly $GL_n(\mathbb{C})$ is a group.

- *Eg. 7* Set of all permutations on the set of three elements: $\{1, 23\}$. Consider the permutations $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.
  e is the identity permutation.
  Verify that $\sigma^3 = \tau^2 = e$. The permutations can then be written as $S_3 = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$.
  We can check that $\sigma\tau = \tau\sigma^2$.

- *Eg.*8
  $\mathbb{Z}_4 = \{0, 1, 2, 3\}$.

  The binary operation is addition modulo 4.

  $a \oplus b = a + b(\text{mod}4)$.

  By definition, $\mathbb{Z}_4$ is closed under $\oplus$.

  $1 \oplus 2 = 3, \quad 1 \oplus 3 = 0, \quad 2 \oplus 3 = 1, \quad 3 \oplus 3 = 2, \quad 2 \oplus 2 = 0, \quad .....$

  0 is the identity. 1 and 3 are inverses of each other. 2 is its own inverse.

  For groups containing a small number of elements, a group table is a convenient way to specify the group completely.

  We construct the group table of $\mathbb{Z}_4$

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

- *Eg. 9*
  The Klein 4 group (K_4)

The group table of $K_4 = \{e, a, b, c\}$ is

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

The group table of any group with 4 elements either is similar to $\mathbb{Z}_4$ or to that of K_4 (exercise).

- Def:*Abellian Group*:
  If $ab = ba \ \ \forall \ \ a, \ b \ \in \ G$ then G is an abellian group.
  All the examples given above except *eg.*6, the group of matrices, and *eg.*7 are abellian groups.

  For e.g. in S_3, $\ \sigma\tau \neq \tau\sigma$

- *Lemma 1:*
  If $\langle G, * \rangle$ be a group. then we have the following

  (i) The identity element in $\langle G, * \rangle$ is unique.
  (ii) Every $a \in G$ has a unique inverse.
  (iii) $\forall \ a \in G, \ (a^{-1})^{-1} = a$.
  (iv) $\forall \ a, b \in G, \ (ab)^{-1} = b^{-1}a^{-1}$.
  Proof: (i) Let if possible e and e' be two distinct identities.

  Then $e * e' = e' * e = e'$, since e is an identity
  Also $e * e' = e' * e = e$, since e' is an identity
  $\implies \ e = e'$.

- *Lemma* 2:
  Let $a, b \in G$. Then there exist a unique solution to $a * x = b$ and $y * a = b$ in G.
  Also $\forall \ \ a, x, y \in G$

$$\begin{aligned} a * x &= a * y \implies x = y && \text{left cancelation law} \\ \text{and} \ \ x * a &= y * a \implies x = y && \text{right cancelation law} \end{aligned}$$

- Lemma 2 ensures that every row and every column of the group table contains each element of the group exactly once.

- Def.<u>*Order of a group*</u>:
  The number of elements in a finite group G is called the order of the group, denoted as $o(G)$.

- Notation: $a * a * .... * a(i \text{ times}) = a^i$

  $(a^i)^{-1} = (a^{-1} * a^{-1} * .... * a^{-1}) = (a^{-1})^i$ denoted as a^{-i}

  With this notation we can write $a^i * (a^j)^{-1} = a^{i-j}$

2 Subgroups

Def.*Subgroup:*
Let $\langle G, * \rangle$ be a group. A non-empty subset H of G is called a subgroup of G if $\langle H, * \rangle$ is a group.

- $2\mathbb{Z} = \{...., -6, -4, -2, 0, 2, 4, 6, ...\} = \{2k | k \in \mathbb{Z}\}$
  $\langle 2\mathbb{Z}, + \rangle$ is a subgroup of $\langle \mathbb{Z}, + \rangle$
- $\langle \mathbb{Z}, + \rangle$ is a subgroup of $\langle \mathbb{R}, + \rangle$ is a subgroup of $\langle \mathbb{C}, + \rangle$.
- Let $\mathcal{M}$ be the set of real 2×2 matrices with determinant =1. Then $\mathcal{M}$ is a subgroup of $GL_2(\mathbb{R})$.
- *Lemma* 3: A non-empty subset H of a group $\langle G, * \rangle$ is a subgroup of G if and only if
  (i) H is closed under $*$.
  (ii) $a \in H \implies a^{-1} \in H$.

  Eg: Let $n \in \mathbb{Z}$ and consider the set $n\mathbb{Z}$.

  Let $nk_1, nk_2 \in n\mathbb{Z}$ where $k_1, k_2 \in \mathbb{Z}$.

  Then $nk_1 + nk_2 = n(k_1 + k_2) \in n\mathbb{Z}$ since $\mathbb{Z}$ is closed under addition.

  So $n\mathbb{Z}$ is closed under addition.

  For any $nk \in n\mathbb{Z}$, $n(-k) \in n\mathbb{Z}$, which is its additive inverse.

  So by Lemma 3 $\langle n\mathbb{Z}, + \rangle$ is a subgroup of $\langle \mathbb{Z}, + \rangle$.
- *Lemma* 4: If H is a non-empty

  <u>finite</u> subset of a group $\langle G, * \rangle$, and H is closed under $*$ then H is a subgroup of G.

  Proof:

Since H is non-empty, $\exists a \in H$. Since H is closed under $*$, $a, a^2, ... \in H$.

But H is finite. So $\exists r, p \in \mathbb{Z}, p > r$ such that $a^p = a^r \implies a^{p-r} = e \in H$.

So $e \in H$.

Now $a^{(p-r)-1} * a = a * a^{(p-r)-1} = a^{p-r} = e$.

So $a^{(p-r)-1} = a^{-1}$.

Hence $\forall\ a \in H,\ \ a^{-1} \in H$. By Lemma 3, H is a subgroup of G.