# COUNCILE OF SCIENTIFIC & INDUSTRIAL RESEARCH

# Unit – 4 : ABSTRACT ALGEBRA

## 4. Abstract Algebra

### 4.1 Set:

**4.1.1 Set:** A well defined collection of distinct objects is called a set.

**Well-defined:** Either an object belongs to a set or it does not belongs to a set i.e. there should be no ambiguity what so ever regarding the membership of such collection of a set.

**Example (4.1) :** Collection of all positive integers is a set but a collection of some positive integers is not a set, as is not clear whether a particular positive integer, say 5, is a member of this collection or not.

**4.1.2. Power Set:** $P(X) = \{A : A \text{ is a subset of } X\}$

$$|P(X)| = 2^k \text{ where } |X| = k$$

**Null Set**$(\emptyset)$ **:** $\emptyset = \{x \in 2 : x^2 + 1 = 0\}$

**4.1.3. Ordered Pair :** Let $x \in X$ and $y \in Y$. The ordered pair of elements x and y denoted by $(x, y)$, is the set $\{\{x\}, \{x, y\}\}$.

Clearly, $(x, y) = \{\{x\}, \{x, y\}\} \neq \{\{y\}, \{x, y\}\} = (x, y), \text{where } x \neq y$

$$(x, y) = (z, w) \Leftrightarrow x = z, y = w.$$

### 4.2. Cartesian Product :

**4.2.1. Cartesian Product:** $X \times Y = \{(x, y) : x \in X, \ y \in Y\}$

(i) Assume $X \times \emptyset = \emptyset = \emptyset \times X \text{ for any set } X.$

(ii) If $|X| = m, |Y| = n, \text{then } |X \times Y| = mn.$

(iii) $X \times Y$ is called diagonal of $X$ and it is denoted by $\Delta_x$.

### 4.3. Relations:

**4.3.1. Relations:** A binary relation or simply a relation$\rho$ from a set $A$ into a set $B$ is a subset of $A \times B$.

**Domain of:** $D(\rho) = \{a \in A : \exists\, b \in B \text{ such that } (a, b) \in \rho\}$

**Range or Image of :** $R(\rho) = \{b \in B : \exists\, a \in A \text{ such that } (a, b) \in \rho\}$

**Inverse relation**$(\boldsymbol{\rho^{-1}})$**:**$(\rho^{-1}) = \{(b, a) : (a, b) \in \rho\}, \ (\rho^{-1})^{-1} = \rho$

**4.3.2.Composition :** Let $\rho_1$ be a relation from A into B and $\rho_1$ be a relation from B to C then the composition of $\rho_1$ and $\rho_2$ is denoted by $\rho_2 \circ \rho_1$is a relation from A to C.

**4.3.3. Definition :** Let A be a set and $\rho$ be a relation of A. Then $\rho$

i. reflexive if for all $a \in A, (a,a) \in \rho$

ii. symmetric, if for all $a, b \in A, whenever\ (a,b) \in \rho \ \Rightarrow (b,a) \in \rho$

iii. transitive, if for all $a, b, c \in A, whenever\ (a,b) \in \rho\ wher\ (b,c) \in \rho \ \Rightarrow (a,c) \in \rho$

**4.3.4. Definition (Equivalence relation):** A relation $\rho$ on a set A is called an equivalence of $\rho$ in reflexive, symmetric and transitive.

**4.3.5. Definition (Anti symmetric):**$\rho$ is said to be anti symmetric if $\forall\ a, b \in A\ where\ (a,b) \in \rho\ and\ (b,a) \in \ \rho \ \Rightarrow a = b.$

**Examples (4.2):**

$\forall\ x, y, \in\ \mathbb{R}$therefore the following reasons

| | | Reflexive | Symmetric | Transitive | Antisymmetric |
|---|---|---|---|---|---|
| 1 | $y = 2x$ | $\times$ | $\times$ | $\times$ | |
| 2 | $x < y$ | $\times$ | √ | $\times$ | √ |
| 3 | $x \neq y$ | $\times$ | √ | $\times$ | |
| 4 | $xy > 0$ | $\times$ (0,0) | √ | √ | |
| 5 | $y\ \neq x + 2$ | √ | $\times$ (3,5) | $\times$ | |
| 6 | $x \leq y$ | √ | $\times$ | √ | √ |
| 7 | $xy \geq 0$ | √ | √ | $\times$ (5,0), (0, −2) | $\times$ |
| 8 | $x = y$ | √ | √ | √ | √ |

**4.3.6. Definition (Partially order set or poset):** A relation $\rho$ on a set A is said to be a partial order on A if $\rho$ is reflexive, anti symmetric and transitive. The set A with the partial order defined on it is called a partially order set or poset and it is denoted by $(A, \rho)$.

**Example (4.3):**$(\mathbb{R}, \leq), (P(X),\ \subseteq)$.

**4.3.7. Definition (Linearly ordered set or chain)**: A poset$(A, \rho)$ is called a linearly ordered set or chain if $\forall\ a, b \in A\ either\ a, b \in \rho\ or\ (b,a) \in\ \rho$ must hold.

**Example (4.4):** $(\mathbb{R}, \leq)$ but not $(P(X), \subseteq)$, since for some $a, b \in X\ \{a\},\{b\} \in P(X)\ such\ that\ \{a\} \nsubseteq \{b\}\ and\ \{b\} \nsubseteq \{a\}$.

**Examples (4.5):** Let S be a finite set and $|S| = n$. Then

i. The number of reflexive relation defined on S is $2^{n^2-n}$

ii. The number of symmetric relation defined on S is $2^{\frac{n^2+n}{2}}$

iii. The number of relation that are both reflexive and symmetric is $2^{\frac{n^2-n}{2}}$

## 4.4. Functions:

**Definition:** For two nonempty sets A and B, a relation $f$ from A into B is called a function from A into B if

i. $D(f) = A$

ii. $f$is well defined (or, single valued) in the series that $\forall\ (a,b),(a',b') \in f, a = a' \Rightarrow b = b'\ i.e,\ a = a' \Rightarrow f(a) = f(a')$.

**Identity mapping:**$f: A \to A, f(x) = x\ \forall\ x \in A$.

**Constant mapping:** $f: A \to B, f(x) = c\ \ \forall\ x \in A,\ some\ c \in B$.

**Examples (4.6):** Let A and B be two finite sets and $|A| = n\ and\ |B| = m\ (n \geq m)$. Then

(i). The number of distinct functions defined from $A$ to $B$ is $m^n$.

(ii). The number of onto functions defined from $A$ to $B$ is $\emptyset(n,m) \times m!$, where $\emptyset(n,m)$ is the number of partitions of a set A with n elements into m subsets (1$\leq m \leq n$) , $\emptyset(n,m)$ is known as stirlling number of 2nd kind and it can be calculated from the formula:

$$\emptyset(n,m) = \begin{cases} 1 & if\ m = 1\ or\ n \\ \emptyset(n-1,m-1) + m\emptyset(n-1,m) & otherwise \end{cases}$$

(iii). The number of injective function defined from$A(|A| = n)\ to\ B(|B| = m, n \leq m)$ is ${}^mP_n$ and bijective is $n!$(if $m\ =\ n$) otherwise 0.

**4.4.1. Definition:** Let us consider a function $f: A \to B$. Then

a) $f$is called injective (one-one) where $\forall\ a_1, a_2 \in A\ if\ a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_{d2})$.

b) $f$is called subjective if $Im\ (f) = B$.

c) $f$ is called bijective if $f$ is both injective and subjective

**4.4.2. (Theorem):** Composition of functions is associative, provided the requisite composition make sense.

**4.4.3. (Theorem):** Suppose that $f: A\ \to B\ and\ g: B \to C$. Then

(i). if $f$ and g are both injective then $g \circ f$ is also so,

(ii). if $f$ and g are both surjective then $g \circ f$ is also so,
(iii). if $f$ and g are both bijective then $g \circ f$ also so,
(iv). if $g \circ f$ is injective then f is injective.
(v). if $g \circ f$ is surjective then g is surjective.
(vi). if $g \circ f$ is bijective, then f is injective and g is surjective.

**4.4.4. (Theorem):** Let $A$ be any set and $f: A \to A$ be an identity injective function. Then $f: A \to A$ is an injective $\forall\, n \geq 1$.

**4.4.5. (Theorem):** For any finite set $A$ if $f: A \to A$ *is injective*, then $f$ is bijective.

If $A$ is infinite this is not true. Example $f: [1,2] \to [1,2]$by $(x) = \frac{x}{2}$. Then $f$ is one – one but there in number of $x \in [1,2]$ *such that* $2 = f(x)$, *i.e.* $f$ is not onto and hence not bijective $(f: \mathbb{R} \to \mathbb{R}, f(x) = e^x$.

**4.4.6.Definition :** Consider a function $f: A \to B$ then $f$ is called

(i). Left invertible, if $\exists\, g: B \to A$ *such that* $g \circ f = i_A$ *and* $g$ is called left inverse of $f$.
(ii). Right invertible if $\exists\, h: B \to A$ such that $f \circ h = i_B$and then h is called right inverse of $f$.
(iii). Invertible if $f$ is both left and right invertible.

**Example (4.7):** $f : \mathbb{N} \to \mathbb{N}, f(n) = n + 1 \;\forall\, n \in \mathbb{N}$ and $g: \mathbb{N} \to \mathbb{N}, g(1) = 1$ and $g(n) = n - 1, n > 1$. Now $(g \circ f)(n) = g\big(f(n)\big) = g(n+1) = n \Rightarrow$ g is left inverse of $f$.

But $f \circ g(1) = f\big(g(1)\big) = f(1) = 2 \Rightarrow g$ *is not right inverse of* $f$.

**4.4.7. (Theorem):** Let $f: A \to B$ be a function. Then –

(i). $f$ is left invertible $\Leftrightarrow f$ is injective.

(ii). $f$ is right invertible $\Leftrightarrow f$ is surjective.

(iii). $f$ is invertible $\Leftrightarrow f$ is bijective.

**4.5 Definition ( Binary Operation) :** Let $A$ be a nonempty set. A binary operation $*$ *on* $A$ is a function from $A \times A \to A$.

**Example (4.8):**$(\mathbb{Z}, +), (\mathbb{N}, +), (\mathbb{R}, \cdot), (\mathbb{R}, +)$ not binary operation $(\mathbb{N}, -)$ since 1 – 2 = –1$\not\subset \mathbb{N}$.

**4.5.1. (Multiplication Table):** $A = \{1, \omega, \omega^2\}$, $*: A \times A \to A$ is complex multiplication.

$$M \equiv \begin{array}{c|ccc} * & 1 & \omega & \omega^2 \\ \hline 1 & 1 & \omega & \omega^2 \\ \omega & \omega & \omega^2 & 1 \\ \omega^2 & \omega^2 & 1 & \omega \end{array}$$

Note: $*$ is commutative (-) M is symmetry.

**4.5.2. (Theorem):** An identity of a mathematical system $(A,*)$, if it exists unique.

**Example (4.9):**

(i). (No identity): $(\mathbb{Z},*)$, where $a \times b = |a+b| \quad \forall\, a,b \in \mathbb{Z}\ and\ a \times b = a$.
(ii). Right identity but no left identity $(\mathbb{Z},*), a * b = a - b \quad \forall\, a,b \in \mathbb{Z}$. Here 0 is such element.
(iii). (No identity) $(\mathbb{Z},*), a * b = a$.
(iv). (No identity): $(\mathbb{N},+)$.
(v). (Not cancellation) $(\mathbb{Z},*), with\ a * b = a$.

**4.5.3. (Semi group):** Let $S$ be a non-empty set and $*: S \times S \to S$ be a binary operation on $S$ and $*$ is associative. Then $(S,*)$ is called semi group.

**Example (4.10):** $(\mathbb{Z},-)$.

**4.5.4. (Monoid):** Semi group with identity.

**Example (4.11):** $(\mathbb{N},+)$ is a semi group but not monoid and $(\mathbb{N} \cup \{0\},+)$ is monoid.

**4.5.5. (Quasi group):** A mathematical system $(G,*)$ i.e, $G$ is used under $*$ is called a quasi group, if $\forall\, a,b, \in G$ each of the equations $a \times x = b\ and\ y - a = b$ has a unique solution in $G$.

**Example (4.12):**

(i). $(\mathbb{Z},-), a - x = b\ and\ y - a = b\ have\ solution\ x = a - b, y = a + b$.
(ii). $(\mathbb{Z},*),\ a * b = |a+b|$. Not a quasi group. Since $a * b = b \Rightarrow |a+x| = b > 0$ has two solution $x = -a + b\ and\ x = -a - b$

**Example (4.13):** Let $|S| = n$. How many different binary operations can be defined on S?

Answer: Total number of binary operations $= n^{n^2}$

Number of commutative binary operations $= 2^{\frac{n^2+n}{2}} = number\ of\ symmetric\ realtion.$

## 4.6. Groups :

**Definition (Group):** A group is an ordered pair $(G,*)$, where $G$ is a non-empty set and $*$ is a binary operation on $G$ such that following properties hold :

(i). $\forall\, a,b,c \in G, a * (b * c) = (a * b) * c\ (\ associative\ law)$.
(ii). $\exists\, e \in G\ such\ that\ \forall\, a \in G, a * e = a = e * a\ (\ existence\ of\ identity)$.
(iii). for each $a \in G\ \exists\, b \in G\ such\ that\ a * b = e = b * a\ (\ existence\ of\ an\ inverse)$.

**4.6.1. (Theorem):** Let $(G,*)$ be a group. Then identity and inverse are unique.

**4.6.2. Abelian (Commutative):** $\forall\, a, b \in G, a * b = b * a \quad i.e. (\mathbb{Z},+)$.

**4.6.3. (Non commutative) :** $(S_3, 0),\ (GL(2,\mathbb{R}),\ \cdot)$.

**Example (4.14):**

(i). $(\mathbb{Z}_n,+) = \{\bar{0},\bar{1},\ldots\ldots\ldots,\overline{n-1},+\}, \forall\, \bar{a},b \in \mathbb{Z}_n,\ a+\ = a+b$ is a commutative group and $n \in \mathbb{Z}^+$.

(ii). $V_w,\ \cdot) = \{\bar{a} \in \mathbb{Z}_n|\{\bar{0}\} : \gcd(a,n) = 1\}\ and\ \bar{a}.\bar{b} = \overline{ab}$ is also a commutative group.

(iii). $\mathbb{Q}[\sqrt{2}] = \{a+\sqrt{2}\,b : a\,.\ b \in \mathbb{Q}\}\ Then\big(\mathbb{Q}[\sqrt{2}],+\big)\ and\ (\ \mathbb{Q}[\sqrt{2}]|\{\bar{0}\},\ \cdot)$ are commutative groups.

(iv). $(P(X),\Delta)$ where $X$ be a set and $P(X)$ is the power set of $X$ and for all $A,B \in P(X), A\Delta B = (A\backslash B) \cup (B\backslash A)$ is a commutative group and $\Delta(A) = 2\ \forall\ A \in P(X)$.

Note : If $X$ is infinite then $(P(X),\Delta)$ is an infinite group but order of every element is finite, namely 1 and $A^{-1} = A$.

(v). $(S_n,0)$ is non-commutative for $n > 2$ where $\delta_n$ is the collection of all bijeciton mapping (permutation) from $X\ to\ X$ where $|X| = x$.

(vi). $GL(2,\mathbb{R}) = (G,*)$where $G = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{R}, ad-bc\ \neq 0\}$ and $*$ is the matrix multiplication. Then $GL(2,\mathbb{R})$ is a $SL(2,\mathbb{R}) = \ \left(\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad-bc = 1\right\},*\right)$

**4.6.4. (Theorem):** Let $(G,*)$ be a group, then

(i). $\forall\ a \in G, (a^{-1})^{-1} = a$

(ii). $\forall\ a,b \in G, (a*b)^{-1} = \ b^{-1}*a^{-1}$

(iii). $[cancellation\ law]\ \forall\ a,b,c \in G\ if\ either\ a*c = b*c\ or\ c*a = c*b,$ $then\ a = b.$

(iv). $\forall\ a,b\ \in G, the\ equation\ a*x = b\ and\ y*a = b$ have unique solution in $G$ for $x\ and\ y.$

**4.6.5. (Corollary):** Let $(G,*)$ be a group and $a \in G.$ If $a*a = a,$ then $a = e$ and $a$ is idempotent element and in a group $e$ is the only idempotent element.

**4.6.6.(Theorem):** A semi group $(S,*)$ is a group if only if

(i). $\exists\ e \in S\ such\ that\ e*a = a\ \forall\ a \in S\ \ (left\ identity)$

(ii). $\forall\ a \in S, \exists\ b \in S\ such\ that\ b*a = e(left\ identity)$

**4.6.7. (Theorem):** A semi group $(S,*)$ in a group $\Leftrightarrow\ \forall\ \ a,b \in S,$ the equation $a*x = b$ and $y*a = b$ have solutions in $S\ for\ x\ and\ y.$

**4.6.8. (Theorem):** A finite semi group $(S,*)$ is a group $\Leftrightarrow$ $(S,*)$ satisfies the cancellation laws.

$*$ Finite is necessary. Example (4.15) $(\mathbb{Z}\{0\},\ \cdot)$ is a semi group and satisfies cancellation laws but inverse of an element $1 \neq a \in \mathbb{Z}\{0\}$ does not exist.

**4.6.9. Definition(Order):** Let $(G,*)$ be a group and $a \in G$. If $\exists$ a positive integer $n$ such that $a^n = e$, then the smallest such positive integer is called the order of $a$.

**4.6.10. (Theorem):** Let $(G,*)$ be a group and $a \in G$ such that $O(a) = n$

(i). If $a^m = e$ for some positive integer m, then n divides m.
(ii). For any positive integer $t$,

$$O(a^t) = \frac{O(a)}{\gcd(t,n)} = \frac{n}{\gcd(t,n)}$$

**Example (4.16):** Give a counter example to justify that in a semi group with, left identity, if every element has a right inverse with respect to the left identity, it need not be a group.

Solution: Consider $\mathbb{Z} \times \mathbb{Z}$ endowed with the operation $(a,b) * (c,d) = (c, b * d) \forall (a,b),(c,d) \in \mathbb{Z} \times \mathbb{Z}$.Then $\mathbb{Z} \times \mathbb{Z},*)$ is a semi group.

Now, $(0,0) * (a,b) = (a,b) \forall (a,b) \in \mathbb{Z} \times \mathbb{Z}$ where $(0,0)$ is a left identity and $(0,-b) \in \mathbb{Z} \times \mathbb{Z}$ *and* $(a,b) * (0,-b) = (0,0) \Leftrightarrow (0,-b)$ is a right $(0,0)$ – inverse of $(a,b) \in \mathbb{Z} \times \mathbb{Z}$.But( $\mathbb{Z} \times \mathbb{Z},*)$ has no identity and hence $(\mathbb{Z} \times \mathbb{Z},*)$ is not a group.

**4.6.11.** If $(G,*)$ is an even order group, then there must exist at least one non-identity element $a \in G$ *such that* $a^2 = e$.

**4.6.12.** A group $G$ is commutative $\Leftrightarrow$ $(a * b)^n = a^n * b^n$ for any three commutative integer $n$ and for all $a, b \in G$.

**4.6.13. Definition(Permutation):** Let A be a set (non-empty). A permutation of $A$ is a bijective mapping of $A$ onto itself.

**4.6.14. Definition:** A group $(G,*)$ is called a permutation group, on a non-empty set $A$ if the elements of $G$ are some permutations of $A$ and the operation $*$ is the composition of two mapping.

**Example (4.17):**$S_3, 0)$, $S_n$ symmetric group and $|S_n| = n!$

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad p = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \; Then\ \alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 3 & 1 \end{pmatrix}$$

**4.6.15. (Theorem):** If $n$ is positive integer such that $n \geq 3$, then the symmetric group $S_n$ is a non-commutative group.

**4.6.16. Definition:** Cycle of length 2 is called transposition.

**4.6.17. Definition:** A permutation is called even permutation is called even permutation if it can be expressed as a product of even number of transpositions.

**4.6.18. (Theorem):** If $\alpha$ *and* $\beta$ be the disjoint cycles in $S_n$ *i.e.* $\alpha \cap \beta = \{i_1, i_2, \ldots \ldots \ldots, i_k\} \cap \{j_1, j_2, \ldots \ldots \ldots, j_p\} = \phi$, *then* $\alpha \circ \beta = \beta \circ \alpha$.

**4.6.19. (Theorem):** Any non-identity permutation $\alpha \in S_n$ $(n \geq 2)$ can be expressed as a product of disjoint cycles where cycle is of *length* $\geq 2$.

**4.6.20. (Theorem):** Any cycle of $length \geq 2$ is either a transposition or can be expressed as a product of transpositions.

**Example (4.18):**

$$\alpha = \begin{pmatrix} 1 & 2 & 34 & 5 & 67 & 8 \\ 8 & 5 & 63 & 7 & 42 & 1 \end{pmatrix} = (1 \quad 8)(2 \quad \overset{*}{5} \quad \overset{\leftarrow}{7})(3 \quad 6 \quad 4)$$

$$= (1 \quad 8)(2 \quad 7)(2 \quad 5)(3 \quad 4)(3 \quad 6)$$

**4.6.21. (Theorem: Order and length):** Let $n \geq 2$ and $\sigma \in S_n$ be a cycle. Then $\sigma$ is a

$$k - cycle \Leftrightarrow order\ of\ \sigma\ is\ k.$$

**4.6.22. (Theorem):** Let $\sigma \in S_n,\ n \geq 2\ and\ \sigma = \sigma_1 \circ \sigma_2 \circ \ldots \ldots \circ \sigma_k$ be a product of disjoint cycles and suppose $O(\sigma_i) = n_i, i = 1,2, \ldots \ldots, k.\ Then\ O(\sigma) = (n_1, n_1 \ldots \ldots, n_k)$

**Example (4.19):**

(i). $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, Then $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

(ii). The number of even permutations in $S_n (n \geq 2)$is the same as that of the odd permutations.

## 4.7. Subgroups :

**Definition :** Let $(G,*)$ be a group and $H$ be a non-empty sub-set of $G$. Then $H$ called a subgroup of $(G,*)$, if $H$ is closed under the binary operation $*$ and $(H,*)$ is a group.

Note: $\{e\}$ and $G$ are two trivial subgroup of $G$.

**Example(4.20):** $(E,+) of\ (\mathbb{Z},+) where\ E = \{2x : x \in \mathbb{Z}\}$.

**4.7.1. (Theorem):** All subgroups of $(G,*)$ have the same identity.

**4.7.2. (Theorem):** Let $G$ be a group and $H$ be a non-empty subset of $G$. Then $H$ is a subgroup of $G \Leftrightarrow \forall\ a, b \in H, ab^{-1} \in H$.

**4.7.3. (Corollary):** Let $G$ be a group and $H$ be a non-empty finite subset of $G$. Then $H$ is a subgroup $\Leftrightarrow \forall\ a, b \in H, ab \in H$.

**4.7.4. (Theorem):** The intersection of any collection of subgroups of a group $G$ is a subgroup of $G$.

- Union of two subgroups of a group $G$ may not be a subgroup of$G$.

**Example (4.21):** Consider $G = S_3\ and\ H = \{e, (2,3)\}\ and\ K = \{e, (1,2)\}$

Then $H, K$ are two subgroup of$S_3$. Now, $H \cup K = \{e, (1 \quad 2), (2 \quad 3)\}$ is not a group. Since

$$(1 \quad 2) \circ (2 \quad 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \quad 2 \quad 3) \notin H \cup K$$

**4.7.5. (Theorem):** Let $n \geq 3$. Then $A_n$ is generated by the set of all $\exists\ cycle$. Number of cycle length $r$ in $S_n$ is $\frac{n!}{r \times (n-r)!}$

**4.7.6. Definition:** Let $H$ and $K$ be two non-empty subsets of a group$G$. Then the product of $H$ and $K$ is defined to be the set

$$H_k = \{hk: h \in H, x \in K\}$$

Product of two subgroups may not be a subgroup. Let $H = \{e, (1 \quad 2)\} \quad K = \{e, (1 \quad 3)\}$.

Now, $H_k = \{e, (1 \quad 2), (1 \quad 3), (1 \quad 3 \quad 2)\}$ $but$ $(1 \quad 3)(1 \quad 2) = (1 \quad 2 \quad 3) \in H_k$

**4.7.7. (Theorem)** Let $H$ $and$ $K$ be two subgroup of a group$G$. Then the following are equivalent:

(i). $H_k$ $is\ a\ subgroup\ of\ G.$
(ii). $HK = KH$
(iii). $KH$ is a subgroup of$G$

**4.7.8. (Corollary):** If $H$ $and$ $K$ are two subgroup of a commutative group $G$, then $HK$ is a subgroup of $G$.

**4.7.9. (Centre of G):**$Z(G) = \{x \in G : gx = xg \ \forall\ g \in G\}$

(i). $Z(G) is\ a\ subgroup\ of\ G.$
(ii). $If\ G\ is\ commutative, then\ Z(G) = G.$

- Let $H$ be a subgroup of $G$. Then for any $g \in G, K = gHg^{-1} = \{gHg^{-1} : h \in H\}$ in a subgroup of G and $|H| = |K|$.
- All subgroups of the group $(\mathbb{Z}, +)$ are $T_n = \{r_n : r \in \mathbb{Z}\}, n \in \mathbb{N}_0$



## 4.8. (Cyclic Groups):

**Definition:** A group $G$ is called cyclic group if $\exists$ an element $a \in G$ such that

$G = < a \geq \{a^n : n \in \mathbb{Z}\}$. Such an element a is called a generator of $G$.

**Example (4.22):**

(i). $G = \{1, -1, i, -i\}, G = < i > = < -i >$
(ii). $(\mathbb{Z}, +) = (< 1 >, +)$
(iii). $(\{2n : n \in \mathbb{Z}\}, +) = (< 2 >, +)$
(iv). $(\mathbb{Z}, +) = \{[1], +\}$

**4.8.1. (Theorem):** Every cyclic group $G$ is commutative.

**4.8.2. (Theorem):** A finite group g is cyclic $\Leftrightarrow$ $\exists\ a \in G\ such\ that\ O(a) = |G|$

**4.8. 3.(Corollary):** Let $< a >$ be a finite cyclic group. Then $O(a) = |G|$

**4.8.4. (Theorem):** Let $G =< a >$ be a cyclic group of order $n$. Then for any integer $k$ where $1 \leq k < n, a^k$ *is a generator of* $G \Leftrightarrow \gcd(n, k) = 1$

**4.8.5. (Theorem):** Every subgroup of a cyclic group is cyclic.

**4.8.6. (Theorem):** Let $G =< a >$ be a cyclic group of order $n$

(i). If $H$ is a subgroup of $G$, then $|H|$ divides $|G|$.(For any group).

(ii). If $m$ is a positive integer such that $m$ *divides* $n$, the $\exists$ a unique subgroup of $G$ of order $n$.(True for also any commutative group).

(iii). If $G =< a >$ is an infinite cyclic group, then any subgroup $H \neq \{e\}$ of $G$ is also infinite order.

(iv). Let $G =< a >$ be an infinite cyclic group. Then
(a) $a^r = a^t \Leftrightarrow r = t, r, t \in \mathbb{Z}$
(b) $G$has only two generators.

## 4.9. Co-sets and Lagrange's Theorem :

**Definition:** Let $H$ be a subgroup of $G$. If $a \in G$, the subset $aH = \{ah : h \in H\}$ is called a left co-sets of $H$in $G$. Similarly, $Ha = \{ha : h \in H\}$ is called a right co-set of $H$ *in* $G$.

Note: $eH = H = He \Rightarrow H$ is a left and right co-set of itself in $G$

- $aH \neq Ha$always example(4.23) $H = \{e, (1 \quad 2)\}$ in $S_3$. Then
  $(2 \quad 3)H = \{(2 \quad 3), (1 \quad 3 \quad 2)$ *and* $Ha = \{(2 \quad 3), (1 \quad 2 \quad 3)$
  i.e.$(2 \quad 3)H \neq H(2 \quad 3)$



**4.9.1. (Theorem):** Let $H$ be a subgroup of a group $G$ and let $a, b \in G$

(i). $aH = H \Leftrightarrow a \in H\ (i*) Ha = H \Leftrightarrow a \in H$

(ii). $aH = bH \Leftrightarrow a^{-1}b \in H (ii*)\ Ha = Hb \Leftrightarrow ba^{-1} \in H$

(iii). Either $aH \cap bH = \phi$ *or* $aH = bH$ $(iii*) Either\ Ha \cap Hb = \phi\ or\ Ha = Hb$

$\Rightarrow$ Left co-set or right co-sets gives a partition of $G$ is $\{aH : a \in G$ forms a partition of $G$.

**4.9.2. (Theorem):**$|aH| = |H| = |Ha|\ \forall\ a \in G$ *and any subgorup* $H$ *of* $G$.

**4.9.3. (Theorem):** Let H be a subgroup of G. Then $|L| = |R|$, *where* $L$(*represent* $R$) denotes the set of all left (represents right) co-sets of $H$in $G$.

**4.9.4.** Index of subgroup: Let $H$ be a subgroup of $G$. Then the number of distinct left (or right) co-sets of $H$in $G$, written $[G, H]$ is called the index o f a $H$ in $G$.

**4.9.5. (Lagrange's Theorem):** Let $H$ be a subgroup of a finite group $G$. Then $|H|$divides $|G|$. In particular, $|G| = |H|[G, H]$.

**4.9.10. (Corollary):** (i) Every group of prime order is cyclic and hence commutative.

(ii) Let $|G| = n$ and $a \in G$.Then $\phi(a)$ divides $n = |G|$ *and* $a^n = e$.