$$\Rightarrow Z_n = \{[1], [2], ..., [n] = [0]\}$$

Let $f: G \to Z_n$ defined by $f(a^r) = [r]$ for all $a^r \in G$.

For all $[r] \in Z_n$, there exists a $a^r \in G$ such that $f(a^r) = [r]$

$\Rightarrow f$ is onto.

For $r \neq s$, $[r] \neq [s]$ and hence $f(a^r) \neq f(a^s)$

$\Rightarrow f$ is one-to-one.

For all $a^r, a^s \in G$, $f(a^r . a^s) = f(a^{r+s}) = [r+s] = [r] + [s]$

$$= f(a^r) +_n f(a^s)$$

$\Rightarrow f$ is a homomorphism. Hence $(G, \cdot)$ is isomorphic to $(Z_n, +_n)$

**Example 9. Prove that every finite group of order "n" is isomorphic to a permutation group of degree n.** **[A.U M/J 2013]**

**(OR)**

**State and prove Cayley's theorem on permutation groups.**

**[MCA, Nov, 93, May 95]**

**Proof :** Let G be the given group and A (G) be the group of all permutations of the set G.

For any $a \in$ G, define a map $f$ : G $\to$ G such that $f(x) = ax$.

$f_a$ **is well defined :**

Let $x = y \Rightarrow ax = ay \Rightarrow f_a(x) = f_a(y)$. Thus $f_a$ is well defined.

$f_a$ **is 1 – 1 :**

Again $f_a(x) = f_a(y) \Rightarrow ax \Rightarrow x = y$. Thus $f_a$ is 1 – 1.

$f_a$ **is onto :** For any $y \in$ G, $f_a(a^{-1}y) = a a^{-1} y$

$$= y \in G$$

Thus we find a preimage $a^{-1}y$ for any "$y$" in G. Thus $f_a$ is onto.

Hence $f_a$ is permutation. (i.e.,) $f_a \in A(G)$.

Let K be the set of all such permutations. We can show that K is a subgroup of A (G). Since $e \in G$, $f_a \in K$. Thus K is non-empty.

Let $f_a, f_b \in K$.

$$
\begin{aligned}
\text{Then } (f_a \circ f_a^{-1})(x) &= f_a(a^{-1}x) \\
&= aa^{-1}x \\
&= ex \\
&= f_e(x)
\end{aligned}
$$

Thus the inverse of $f_a$ is $f_a^{-1}$

$$
\begin{aligned}
(f_a \circ f_b)(x) &= f_a(f_b(x)) \\
&= f_b(bx) \\
&= abx \\
&= f_{ab}(x)
\end{aligned}
$$

$$\Rightarrow f_a \circ f_b = f_{ab} \in K.$$

Thus K is a subgroup of A (G).

Next we will show that G is isomorphic to K.

**Define a map :** $\chi : G \to K$ such that $\chi(a) = f_a$.

$\chi$ **is well defined :**

$$
\begin{aligned}
\text{For } a, b \in G,\ a = b &\Leftrightarrow ax = bx \\
&\Leftrightarrow f_a(x) = f_b(x) \\
&\Leftrightarrow f_a = f_b \\
&\Leftrightarrow \chi(a) = \chi(b)
\end{aligned}
$$

$\chi$ is one-one and onto.

$\chi$ is a homomorphism :

$\chi\ (ab) = f_{ab} = f_a \circ f_b = \chi\ (a) \cdot \chi\ (b)$

Thus $\chi$ is a homomorphism and hence an isomorphism which proves the theorem.

**Example 10. Show that every cyclic group of order n is isomorphic to $(Z_n, +_n)$**

**Solution :** Let $(G, o)$ be a cyclic group of order $n$.

The element of $G$ are $\{a, a^2, a^3, ..., a^n = e\}$.

The elements of $Z_n$ are $\{[0], [1], [2], ..., [n-1]\}$.

**Define**

$f : D \to Z_n$ by

$f(e) = [0]$ and $f(a^i) = [i]$ for $i < n$ where $f$ is one-one and onto.

$$\text{Then } f(a^i a^j) = f(a^{i+j}) = [i+j]$$

$$= [i] +_n [j]$$

$$= f(a^i) +_n f(a^j)$$

Hence $f$ is an isomorphism.

**Example 11. Define : Symmetric group, Dihedral group. Show that if (G, $*$) is a cyclic group, then every sub group of (G, $*$) must be cyclic.**

**(OR)** **[MCA, May 93, M.U]**

**Show that every subgroup of a cyclic group is cyclic.**

**Solution :** Let (G, $*$) be a cyclic group generated by "$a$", and let H be a subgroup of G. If H contains the identity element alone, then trivially H is cyclic and H $= (e)$. Suppose that H $\neq (e)$. Since H $\subseteq$ G, any element of H is of the form $a^k$ for some integer K. Let *(ii) Group homomorphism preserves inverse*

Since $a * a^{-1} = e_G = a^{-1} * a$ we have

$$g(a * a^{-1}) = g(e_G) = g(a^{-1} * a)$$

$$\Rightarrow g(a) \Delta g(a^{-1}) = e_H = g(a^{-1}) \Delta g(a)$$

$\Rightarrow g(a^{-1})$ is the inverse of $g(a)$

$$\therefore g(a^{-1}) = [g(a)]^{-1}$$

*(iii) Group homomorphism*

Let S be a subgroup of (G, *)

To show that $g(S) = \{x \in H / x = g(a) \text{ for some } a \in G\}$ is a subgroup of (H, Δ)

(i) As $e_G \in S$, $g(e_G) = e_H \in g(s)$

(ii) For each $x \in g(s)$, $\exists$ $a \in s$ such that $g(a) = x$

Since $s$ is a sub group of G,

for each $a \in s$, $a^{-1} \in s$

$$g(a^{-1}) = [g(a)]^{-1} \in g(s)$$

$$\Rightarrow x^{-1} \in g(s)$$

(iii) For $x, y \in g(s)$, $\exists$ $a, b \in s$

Such that $g(a) = x$ and $g(b) = y$

As $s$ is a subgroup, $a * b \in s$

$$\Rightarrow g(a * b) = g(a) \Delta g(b)$$
$$= x \Delta y \in g(s)$$

$\therefore g(s)$ is a subgroup of H.

## 4.3 NORMAL SUB-GROUP AND COSETS - LAGRANGE'S THEOREM :

**Definition 1 : Left coset of H in G.**

Let (H, $*$) be a subgroup of (G, $*$). For any $a \in$ G, the set $a$ H defined by

$a$ H $= \{a * h / h \in \text{H}\}$ is called the left coset of H in G determined by the element $a \in$ G.

The element $a$ is called the representative element of the left coset $a$ H.

**Note :** The left coset of H in G determined by $a \in$ G is the same as the equivalence class $[a]$ determined by the relation left coset modulo H.

**Definition 2 : Index of $H$ in $G$ $[i_G(H)]$**

Let $(H, *)$ be a subgroup of $(G, *)$, then the number of different left (or right) cosets of $H$ in $G$ is called the index of $H$ in $G$.

**Definition 3. Normal sub-group**

A subgroup (H, $*$) of (G, $*$) is called a normal sub-group if for any $a \in$ G, $a$ H = H $a$.

**Definition 4. Quotient group (or) factor group :**

Let N be a normal subgroup of a group (G, $*$).

The set of all right cosets of N in G be denoted by

$$G/N = \{Na \mid a \in G\}$$

Now, define $\otimes$ as binary operation on G/N as

$$N\,a \otimes N\,b = N\,(a * b)$$

Then (G/N $\otimes$} will form a group, called quotient group (or) factor group.

**Definition 5. Direct product**

Let (G, $*$) and (H, $\Delta$) be two groups. The direct product of these two groups is the algebraic structure (G $\times$ H, $\circ$) in which the binary operation $\circ$ on G $\times$ H is given by

$$(g_1, h_1) \circ (g_2, h_2) = (g_1 * g_2, h_1 \circ \Delta h_2)$$

for any $(g_1, h_1), (g_2, h_2) \in G \times H$.

**Definition 6. Group homomorphism :**

Let $(G, *)$ and $(G', \cdot)$ be two groups. A mapping $f : G \to G'$ is called a group homomorphism if

$$\forall\, a, b \in G,\ f(a * b) = f(a) . f(b)$$

**Definition 7. Kernel of group homomorphism :**

Let $(G, *)$ and $(G', \cdot)$ be two groups with $e'$ as the identity element of $G'$

Let $f : G \to G'$ be a homomorphism.

$ker f = \{a \in G \mid f(a) = e'\}$

**Statement 1 : [Lagrange's theorem] [A.U A/M 2004, 2005, N/D 2004]**

**The order of a subgroup of a finite group divides the order of the group. (OR) If G is a finite group, then 0(H) | 0(G), for all sub-group H of G.**

**Statement 2 :** Fundamental theorem on homomorphism of groups

If $f$ is a homomorphism of $G$ onto $G'$ with kernal $k$, then $G/K \approx G'$.

**Theorem 1 :**

Let (H, $*$) be a subgroup of (G, $*$). The set of left cosets of H in G form a partition of G. Every element of G belongs to one and only one left coset of H in G.

**Proof :** (i) *To prove :* Every element of G belongs to one and only one left coset of H in G.

Let H be a subgroup of a group G. Let $a \in G$. Then $a\,H = H$ if and only if $a \in H$.

**Proof :** Let $a \in G$

$$a\,H = H = ae \in H = H \Rightarrow a \in H$$

Conversely assume that $a \in H$

Then $ah \in H$, for all $h \in H$.

So $a\,H \subseteq H$ ... (1)

Given any $y \in H$, $a^{-1}y \in H$ and $y = a\,(a^{-1}y) \in H$.

So $y \in a\,H$ for all $y \in H$.

(i.e.,) $H \subseteq a\,H$ ... (2)

From (1) and (2) $H = a\,H$

Hence every element of G belongs to one and only one left coset of H in G.

(ii) *To prove :* The set of left cosets of H in G form a partition of G.

Let $a, b \in G$ and H be a sub group of G.

If $a\,H \cap H\,a \neq \phi$

Let $c \in a\,H \cap H\,a$

As $c \in a\,H$ we have $cH = a\,H$

[$\because$ Let H be a subgroup of a group G. Let $a, b \in G$ if $b \in a\,H$, then $b\,H = a\,H$]

As $c \in b\,H$, we have $cH = b\,H$

So $a\,H = c\,H = b\,H$

Thus if $a\,H \cap b\,H \neq \phi$, then $a\,H = b\,H$.

Therefore any two distinct left cosets are disjoint. Hence the set of all (distinct) left cosets of H in G forms a partition of G.

**Theorem 2 : [Lagrange's theorem]**

[A.U A/M 2004, 2005, N/D 2004, 2010]
[A.U A/M 2011, June 2011, M/J 2012, M/J 2013, M/J 2014]

**The order of a subgroup of a finite group divides the order of the group. (OR) If G is a finite group, then 0(H) | 0(G), for all sub-group H of G.**

**Solution : Statement :** If G is a finite group and H is a subgroup of G, then order of H is a divisor of order of G.

**Proof :**

Let $0(G) = n$, (Here $n$ is finite)

Let $G = \{a_1 = e, a_2, a_3, \ldots a_n\}$ and let H be a subgroup of H

Consider the left cosets as follows

$e * H = \{e * h \setminus \in H\}$

$a_2 * H = \{a_2 * H \setminus h \in H\}$

$a_n * H = \{a_n * h \setminus h \in H\}$

We know that any two left cosets are either identical or disjoint.

Also $\quad 0(e * H) = 0(H)$

$\therefore \quad 0(a_i * H) = 0(H), \ \forall\, a_i \in G.$

Otherwise if $a * h_i = a * h_j$ for $i \neq j$, by cancellation laws, we would have $h_i = h_j$, which is a contradiction.

Let there be $k$ – disjoint cosets of H in K. Clearly their union equals G (i.e.,) $G = (a_1 * H) \cup (a_2 * H) \cup \ldots \cup (a_k * H)$

$$\therefore 0(G) = 0\,(a_1 * H) + 0(a_2 * H) + \ldots + 0(a_k * H)$$

$$= \underbrace{0(H) + 0(H) + \ldots + 0(H)}_{K\text{ - times}}$$

$0(G) = K \cdot 0(H)$

This implies 0(H) is a divisor of 0(G).

**Theorem 3 : Let (G, $*$) and (H, $\Delta$) be groups and $g$ : G $\to$ H be a homomorphism. Then the Kernel of $g$ is a normal sub-group.**

**[A.U. N/D, 2004] [A.U A/M 2011, M/J 2012, M/J 2013]**

**Solution :** Let K be the Kernel of the homomorphism $g$ (i.e.,) K = {$x \in$ G\ $g(x) = e'$, where $e' \in$ H is the identity element of H}

To prove that K is a subgroup :

Let $x, y \in$ K, then $g(x) = e'$ and $g(y) = e'$.

Claim : $x * y^{-1} \in$ K

By definition of homomorphism,

$$g(x * y^{-1}) = g(x) \,\Delta\, g(y^{-1}) = g(x) \,\Delta\, [g(y)]^{-1}$$
$$= e' \,\Delta\, (e')^{-1}$$
$$= e' \,\Delta\, e' = e'.$$

Hence $x * y^{-1} \in$ K and this proves K is a sub-group of G by a criterion for sub-groups.

To prove that K is normal : Let $x \in$ K, $f \in$ G, then $g(x) = e'$

Claim : $f * x * f^{-1} \in$ K

$$g(f * x * f^{-1}) = g(f) * g(x) * g(f^{-1})$$
$$= g(f) \,.\, e^{-1} [g(f)]^{-1}$$
$$= g(f)\, [g(f)]^{-1}$$
$$= e'$$

$\therefore f * x * f^{-1} \in$ K.

Thus K is a normal subgroup of G.

**Theorem 4 : (Fundamental Thereom on homomorphism of groups)** If $f$ is a homomorphism of G onto G $'$ with kernal K, then G/K $\cong$ G $'$.

**[A.U June 2011, N/D 2013]**

**Proof :**

Let $f : G \rightarrow G'$ be a homomorphism from the group $(G, *)$ to the group $(G', \Delta)$.

$$\text{Then } K = \text{Ker}(f) = \{x \in G \mid f(x) = e'\}$$

is a normal sub-group of $(G, *)$

Also we know that the quotient set $(G/K, \otimes)$ is a group.

Define $\phi : G/K \rightarrow G'$ is mapping from the group $(G/K, \otimes)$ to the group $(G', \Delta)$, given by

$$\phi(K a) = f(a), \text{ for any } a \in G$$

Since, if $K a = K b$

$$\Rightarrow a * b^{-1} \in K$$

$$\Rightarrow f(a * b^{-1}) = e'$$

$$\therefore f(a) \, \Delta \, f(b^{-1}) = e'$$

$$f(a) \, \Delta \, [f(b)]^{-1} = e'$$

$$f(a) \, \Delta \, [f(b)]^{-1} \, \Delta \, [f(b)] = e' \, \Delta f(b)$$

$$\Rightarrow \quad f(a) \, \Delta \, e' = f(b)$$

$$\Rightarrow \quad f(a) = f(b)$$

$$\Rightarrow \quad \phi(Ka) = \phi(Kb)$$

$\therefore$ $\phi$ is well defined.

**Claim :** $\phi$ is a homomorphism.

Let $Ka$, $K b \in G/K$

Now $\phi$ (K $a \otimes$ K $b$) $= \phi$ [K $(a * b)$ ]

$= f[(a * b)]$

$= f(a) \Delta f(b)$

$= \phi$ (K$a$) $\Delta$ (K $b$)

$\therefore \phi$ is a homomorphism.

**Claim :** $\phi$ is one-to-one.

If $\phi$ (K$a$) $= \phi$ (K $b$)

then $f(a) = f(b)$

$f(a) \Delta f(b^{-1}) = f(b) \Delta f(b^{-1})$

$f(a * b^{-1}) = f(b * b^{-1}) = f(e) = e'$

$\therefore a * b^{-1} \in$ K $\Rightarrow$ K $a$ = K $b$

$\therefore \phi$ is one-to-one.

**Claim :** $\phi$ is onto.

Let $y$ be any element of G$'$.

Since $f$ : G $\rightarrow$ G$'$ is a homomorphism from G onto G$'$, therefore there exists an element $a \in$ G such that $f(a) = y$.

$\therefore$ For every $a \in$ G, K $a \in$ G/K

We get $\phi$ (K $a$) $= f(a)$, for all $f(a) = y \in$ G$'$

$\therefore$ $\phi$ is onto.

$\therefore$ $\phi$ : G/K $\rightarrow$ G$'$ is an isomorphism

G/K $\equiv$ G$'$.

**Theorem 5 : Prove that the intersection of two normal subgroups is a normal subgroup.** **[MCA May, 91, MU] [A.U M/J 2013]**

**Solution :** Let H and K be any two normal subgroups of a group G.

We have to prove that H $\cap$ K is normal in G.

Since H and K are subgroups of G, $e \in H$ and $e \in K$.

Hence $e \in H \cap K$. Thus $H \cap K$ is a non-empty set.

Let $a, b \in H \cap K$

**Claim :** $ab^{-1} \in H \cap K$

Since, $a, b \in H \cap K$, both $a, b$ being to H and K.

Since H and K are subgroups of G, $ab^{-1} \in H$ and $ab^{-1} \in K$ so that $ab^{-1} \in H \cap K$.

Hence $H \cap K$ is a subgroup of G, by a criterion for subgroup.

**To prove :** $H \cap K$ is normal :

Let $x \in H \cap K$, and let $g \in H$

Since $x \in H \cap K$ and $x \in H$ and $x \in K$.

Since $x \in H, g \in G, \Rightarrow gxg^{-1} \in K$ (as H is normal)

Likewise $x \in K, g \in G \in gxg^{-1} \in K$ (as K is normal)

Hence $x \in H \cap K$ and $g \in G \Rightarrow gxg^{-1} \in H \cap K$.

This $H \cap K$ is a normal subgroup of G.

**Theorem 6 : Every subgroup of an abelian group is a normal subgroup.**

**[A.U N/M 2013]**

**Proof :** Let $(G, *)$ be an abelian group and $(N, *)$ be a subgroup of G.

Let $g$ be any element in G and let $n \in N$.

Now, $g * n * g^{-1} = (n * g) * g^{-1}$ [$\because$ G is abelian]

$$= n * (g * g^{-1})$$

$$= n * e$$

$$= n \in N$$

$\therefore \forall$ A $g \in G$ and $n \in N$, $g * n * g^{-1} \in N$

$\therefore$ (N, $*$) is a normal subgroup.

**Theorem 7 : Let $< H, * >$ be a subgroup of $< G, * >$. Then show that $< H, * >$ is a normal subgroup iff $a * h * a^{-1} = H, \forall a \in G$.**

**[MCA, Nov., 93, May 92, MU]**

**Solution :** Let H be normal in G.

Then by definition $a * H = H * a$, for all $a \in G$.

$$\text{Then } a * H * a^{-1} = a * (a^{-1} * H)$$
$$= (a * a^{-1}) * H$$
$$= e * H$$
$$= H$$

Conversely let $a^{-1} * H * a = H$, for all $a \in G$.

(i.e.,) $a * (a^{-1} * H * a) = a * H)$

(i.e.,) $(a * a^{-1}) * (H * a) = a * H$

(i.e.,) $e * (H * a) = a * H$

(i.e.,) $H * a = a * H$

Thus H is a normal subgroup.

**Theorem 8 : Let $< A, * >$ be a group. Let $H = \{a/a \in G$ and $a * b = b * a \; \forall \; b \in G\}$. Show that H is a normal subgroup.**

**[MCA May, 1990, March, 96, MU]**

**Solution :** $H = \{a \in G \mid a * b = b * a, \forall \; b \in G\}$.

Since $e * a = a * e = a, \forall \; a \in G$, we have $e \in H$.

$\therefore$ H is non-empty

Let $x, y \in H$. Then

$a * x = x * a, \forall \; x \in G$ and $a * y = y * a, \forall \; y \in G$.

## 4.4 DEFINITIONS AND EXAMPLES OF RINGS AND FIELDS :

**Definition 1 : Ring** **[A.U M/J 2014]**

An algebraic system (S, +, .) is called a ring if the binary operations + and . on S satisfy the following three properties :

1. (S, +) is an abelian group
2. (S, .) is a semigroup
3. The operation . is distributive over + ; that is, for any $a, b, c \in S$,

$$a.(b+c) = a.b + a.c \quad \text{and} \quad (b+c).a = b.a + c.a$$

**Examples :**

1. The set of all integers Z, the set of all rational numbers $R^+$, the set of all real numbers R are rings under the usual addition and usual multiplication.

2. The set of all $n \times n$ matrices $M_n$ is a ring under the matrix addition and matrix multiplication.

3. If $n$ is a positive integer, then $Z_n = \{\bar{0}, \bar{1}, \dots \overline{n-1}\}$ is a ring under $+_n$, the addition modulo $n$ and $\times_n$, the multiplication modulo $n$.

4. Let (R, +, .) be a ring and X be a non-empty set. Let A be the set of all functions from X to R. (i.e.,) $A = \{f \mid f : X \to R \text{ is a function}\}$ we define $\oplus$ and . on A as follows :

(i) if $f, g \in A$, then $f \oplus g : X \to R$ is given by $(f \oplus g)(x) = f(x) + g(x)$ for all $x \in X$.

(ii) if $f, g \in X$ then $f.g : X \to R$ is given by $(f.g)(x) = f(x).g(x)$ for all $x \in X$.

**Definition 2 : Integral domain.**

A commutative ring $(S, +, \bullet)$ with identity and without divisors of zero is called can integral domain.

**Definition 3 : Field**

A commutative ring $(S, +, \bullet)$ which has more than one element such that every non-zero element of S has a multiplicative inverse in S is called a field.

**Definition 4 : Sub ring.**

A subset $R \subseteq S$ where $(S, +, \bullet)$ is a ring is called a subring if $(R, +, \bullet)$ is itself with the operations $+$ and $\bullet$ restricted to R.

**Examples :**

1. The ring of integers Z is a subring of the ring of all rational numbers Q.

2. In Z the ring of all integers the set of all even integers is a subring.

**Definition 5 : Ring homomorphism**

Let $(R, +, \bullet)$ and $(S, \oplus \odot)$ be rings. A mapping $g : R \rightarrow S$ is called a ring homomorphism from $(R, +, \bullet)$ to $(S, \oplus, \odot)$ if for any $a, b \in R$.

$$g(a+b) = g(a) \oplus g(b) \text{ and}$$

$$g(a.b) = g(a) \odot g(b)$$

**Examples :**

1. The ring $M_n$ of all non-matrices is not commutative and has non-zero zero divisors. For example : Let $n = 2$, then if $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ then $AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and $BA = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. So $AB \neq BA$ and A is non-zero zero divisor.

2. The ring Q of all rational numbers, and the ring R of real numbers are fields.

3. The ring $(Z_7, +_7, \times_7)$ is a field.

4. The ring $(Z_{10}, +_{10}, \times_{10})$ is not an integral domain. (as $5 \times_{10} 2 = 0$, yet $5 \neq 0$, $2 \neq 0$ in $Z_{10}$).

5. The ring Z of all integers is an integral domain but not a field.

**Definition 6. Commutative Ring :**

A ring $(R, +, codt)$ is said to be commutative if $a . b = b . a \ \forall \ a, b \in R$

**Theorem 1 : Every finite integral domain is a field.**

**Proof :** Let $(R, +, \bullet)$ be a finite integral domain.

To prove $(R - \{0\}, \bullet)$ is a group

i.e., to prove

(i) there exists an element $1 \in R$ such that $1 . a = a . 1 = a$, for all $a \in R$ ($1 \in R$ is an identity)

(ii) for every element of $0 \neq a \in R$, there exists an element $a^{-1} \in R$ such that

$$a . a^{-1} = a^{-1} . a = 1$$

Let $R - \{0\} = \{a_1, a_2, a_3, \dots a_n\}$

Let $a \in R - \{0\}$, then the elements $aa_1, aa_2, \dots aa_n$ are all in $R - \{0\}$ and they are all distinct.

(i.e.,) If $a . a_i = a . a_j$, $i \neq j$

then $a . (a_i - a_j) = 0$

Since R is an integral domain and $a \neq 0$, we must have $a_i - a_j = 0$,

(i.e.,) $a_i = a_j$ which is a contradiction.

$\therefore$ R - {0} has exactly $n$ elements, and R is a commutative ring with cancellation law

$\therefore$ we get $a = a \cdot a_{i_0}$, for some $i_0$ (since $a \in R - \{0\}$)

i.e., $a \cdot a_{i_0} = a_{i_0} \cdot a$ (Since R is commutative)

Thus, let $x = a \cdot a_i$ for same $a_i \in R - \{0\}$, and

$$y \cdot a_{i_0} = a \cdot a_{i_0} = (a_i \cdot a)\, a_{i_0} = a_i \cdot a = a \cdot a_j = y$$

$\therefore$ Hence $a_{i_0}$ is an unity R - {0}. We write it as 1.

Since $1 \in R - \{0\}$, therefore there exists an element $aa_k \in R\text{-}\{0\}$ such that

$$aa_k = 1$$

$\therefore$ $ba = ab = 1$ (let $a_k = b$)

$\therefore$ $b$ is the inverse of $a$, and conversely.

Hence $(R, +, \bullet)$ is a field.

**Thereom 2 : Every field is an integral domain, but the converse need not be true.**

**Proof :**

Let $(F, +, \bullet)$ is a field.

(i.e.,) F is a commutative ring with unity.

To prove F is an integral domain it is enough to show that it has non zero divisor.

Let $a, b \in F$, such that $a \cdot b = 0$

Let $a \neq 0$, then $a^{-1} \in F$

$$\therefore a \cdot b = 0$$

$$\Rightarrow a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0$$

# 5.1 PARTIAL ORDERING-POSETS - LATTICES AS POSETS

### Def. Partial order relation

A binary relation R in a set P is called a partial order relation or a partial ordering in P iff R is reflexive, antisymmetric, and transitive.

### Def. Poset

A set P together with a partial ordering R is called a partially ordered set or a poset.

**Note :** It is conventional to denote a partial ordering by the symbol $\leq$. This symbol does not necessarily mean "lessthan or equal to" as is used for real numbers.

### Def. Totally ordered set.

Let $(P, \leq)$ be a partially ordered set. If for every $x, y \in P$ we have either $x \leq y \vee y \leq x$, then $\leq$ is called **simple ordering** or **linear ordering** on P and $(P, \leq)$ is called a **totally ordered** or **simply ordered set** or a **Chain**

*Example* : The poset $(Z, \leq)$ is totally ordered, since $a \leq b$ or $b \leq a$ whenever $a$ and $b$ are integers.

**Def.** Let $(P, \leq)$ be a partially ordered set and let $A \subseteq P$. Any element $x \in P$ is an upper bound for A if for all $a \in A$, $a \leq x$.

Similarly, any element $x \in P$ is a lower bound for A if for all $a \in A$, $x \leq a$

**Def.** Let $(P, \leq)$ be a partially ordered set and let $A \subseteq P$. Any element $x \in P$ is a least upper bound or supremum, for A if $x$ is an upper bound for A and $x \leq y$ where $y$ is any upper bound for A. Similarly, then greatest lower bound, or infimum, for A is an element $x \in P$ such that $x$ is a lower bound and $y \leq x$ for all lower bounds $y$.

**Def. Well-ordered**

A partially ordered set is called well-ordered if every nonempty subset of it has a least member.

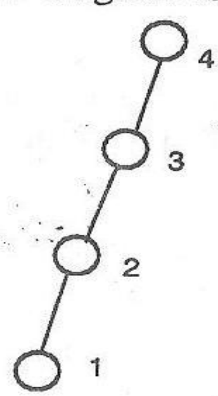
**Def. Hasse diagram or partially ordered set diagram.**

A partial ordering $\leq$ on a set P can be represented by means of a diagram known as a Hasse diagram or a partially ordered set diagram of $(P, \leq)$. In such a diagram, each element is represented by a small circle or a dot.

The circle for $x \in P$ is drawn below the circle for $y \in P$ if $x < y$, and a line is drawn between $x$ and $y$ if $y$ covers $x$.

If $x < y$ but $y$ does not cover $x$, then $x$ and $y$ are not connected directly by a single line. However, they are connected through one ore more elements of P. It is possible to obtain the set of ordered pairs in $\leq$ from such a diagram.

**Example :** Let $P = \{1, 2, 3, 4\}$ and $\leq$ be the relation "lessthan or equal to" then the Hasse diagram is



**Note :**

1. Hasse diagram, named after the twentieth - Century German mathematician Helmut Hasse.

2. In a digraph we apply the following rules then we get Hasse diagram.

(i) Each vertex of A must be related to itself. So the arrows from a vertex to itself are not necessary.

(ii) If $a$ vertex $b$ appears above vertex $a$ and if vertex $a$ is connected to vertex $b$ by an edge, then $aRb$, so direction arrows are not necessary.

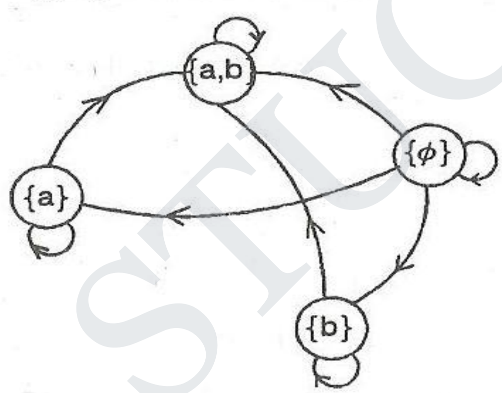
(iii) If vertex C is above $a$ and if $c$ is connected to a by a sequence of edges then arc.

(iv) The vertices are denoted by points rather than by circles.

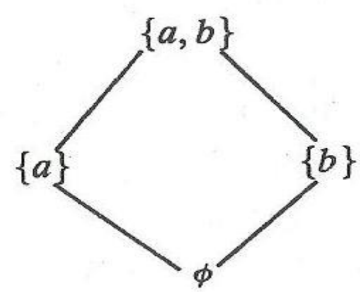
**Example.** Let A $= \{a, b\}$

B $=$ P(A) $= \{\{\phi\},\{a\},\{b\},\{a,b\}\}$

Then $\subseteq$ is a relation an a whose diagraph is as follows




Hasse diagram




**Example 1. Show that the "greater than or equal" relation ($\geq$) is a partial ordering on the set of integers.**

**Solution :** Since $a \geq a$ for every integer $a$, $\geq$ is reflexive. If $a \geq b$ and $b \geq a$, then $a = b$. Hence, $\geq$ is antisymmetric. Finally, $\geq$ is transitive since $a \geq b$ and $b \geq c$ imply that $a \geq c$. It follows that $\geq$ is a partial ordering on the set of integers and $(Z, \geq)$ is a poset.