

f 1 :- Let $(R, +, \cdot)$ be a ring. We say that M is a left R -module on R if :-

① $(M, +)$ abelian group.

② there exist a binary operation $\cdot : R \times M \rightarrow M$ such that :-

$$a - (r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m, \quad \forall r_1, r_2 \in R, \forall m \in M$$

$$b - (r_1 r_2) \cdot m = r_1 (r_2 \cdot m), \quad \forall r_1, r_2 \in R, \forall m \in M$$

$$c - r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2, \quad \forall r \in R, \forall m_1, m_2 \in M$$

M is called left Unitary R -module if

$$d - 1 \cdot m = m, \quad 1 \in R, \forall m \in M$$

Example 2 :- Every vector space V over field F is a left Unitary F -module.

let V be a vector space over field F , then

$$\textcircled{1} \quad \forall \vec{u}, \vec{v} \in V \Rightarrow \vec{u} + \vec{v} \in V$$

$$\textcircled{2} \quad \forall \vec{u}, \vec{v}, \vec{w} \in V \Rightarrow (\vec{u} + \vec{v}) + \vec{w} = \vec{u} + (\vec{v} + \vec{w})$$

$$\textcircled{3} \quad \forall \vec{u} \in V, \exists \vec{0} \in V \Rightarrow \vec{u} + \vec{0} = \vec{0} + \vec{u} = \vec{u}$$

$$\textcircled{4} \quad \forall \vec{u} \in V, \exists -\vec{u} \in V \Rightarrow \vec{u} + (-\vec{u}) = \vec{0}$$

$$\textcircled{5} \quad \forall \vec{u}, \vec{v} \in V \Rightarrow \vec{u} + \vec{v} = \vec{v} + \vec{u}$$

$\therefore (V, +)$ abelian group

there exist function $\cdot : F \times V \rightarrow V$ s.t

$$\textcircled{6} \quad \forall r_1, r_2 \in F, \vec{v} \in V \Rightarrow (r_1 + r_2) \cdot \vec{v} = r_1 \cdot \vec{v} + r_2 \cdot \vec{v}$$

$$\textcircled{7} \quad \forall r_1, r_2 \in F, \vec{v} \in V \Rightarrow (r_1 r_2) \cdot \vec{v} = r_1 (r_2 \cdot \vec{v})$$

$$\textcircled{8} \quad \forall r \in F, \vec{u}, \vec{v} \in V \Rightarrow r \cdot (\vec{u} + \vec{v}) = r \cdot \vec{u} + r \cdot \vec{v}$$

$$\textcircled{9} \quad \forall r \in F, \vec{v} \in V \Rightarrow 1 \cdot \vec{v} = \vec{v}$$

Example 3 :- Every $(I, +, \cdot)$ of a ring $(R, +, \cdot)$ is a left unitary R -module.

let $(I, +, \cdot)$ be ideal of the ring $(R, +, \cdot)$

① since $(I, +, \cdot)$ is ideal

$\therefore (I, +, \cdot)$ is subring

$\therefore (I, +)$ is abelian group.

② define $\cdot : R \times I \rightarrow I$ by $\cdot(r, a) = r \cdot a$, $\forall r \in R, \forall a \in I$

a- $\forall r_1, r_2 \in R, a \in I \Rightarrow (r_1 + r_2) \cdot a = r_1 \cdot a + r_2 \cdot a$
since $(R, +, \cdot)$ ring

b- $\forall r_1, r_2 \in R, a \in I \Rightarrow (r_1 r_2) \cdot a = r_1 (r_2 \cdot a)$
since $(R, +, \cdot)$ ring

c- $\forall r \in R, a_1, a_2 \in I \Rightarrow r(a_1 + a_2) = r \cdot a_1 + r \cdot a_2$
since $(R, +, \cdot)$ ring

d- $1 \in R, \forall a \in I \Rightarrow 1 \cdot a = a$

$\therefore I$ is a left R -module

Example 4 :- Every ring $(R, +, \cdot)$ is a left R -module.

since $(R, +, \cdot)$ is an ideal of $(R, +, \cdot)$

by example 3 $(R, +, \cdot)$ is a left R -module

$\forall a \in I, r \in R \Rightarrow r a \in I$ (as $(R, +, \cdot)$ is ideal of $(R, +, \cdot)$)
 \therefore \exists Z_p Algebra-Rings-and-module

Def 6:- Let $(R, +, \cdot)$ be a ring. we say that M is a Right R -module on R if :-

- ① $(M, +)$ is a abelian group
- ② there exist a binary operation $\circ : M \times R \rightarrow M$ such that :-

a- $M \cdot (r_1 + r_2) \circ M = r_1 \cdot M + r_2 \cdot M = M \cdot r_1 + M \cdot r_2, \forall r_1, r_2 \in R, \forall m \in M$

b- $M \cdot (nr) = (M \cdot n)r, \forall n \in R, \forall m \in M$

c- $(m_1 + m_2) \circ r = m_1 \circ r + m_2 \circ r, \forall m_1, m_2 \in M, \forall r \in R$

M is called Right Unitary R -module if

d- $m \cdot 1 = m, 1 \in R, m \in M$

Def 7:- Let M be left R -module on R and N be nonempty subset of M . N is called left submodule from the module M . denoted by $N \hookrightarrow M$ if N is left R -module on R

Remark :- Every left R -module M on R contains at least two submodules $M \hookrightarrow M, 0 \hookrightarrow M$ called trivial submodules.

Theorem 10.1 - let M be left R -module and N nonempty subset of M , then N is left submodule of M if and only if :-

- ① $a-b \in N, \forall a, b \in N$
- ② $ra \in N, \forall r \in R, \forall a \in N$

Proof :- (\Rightarrow) suppose $N \hookrightarrow M$

- $\therefore (N, +)$ abelian group
- $\therefore (N, +)$ subgroup of $(M, +)$
- $\therefore a-b \in N, \forall a, b \in N$
- $\therefore r \in R, a \in N \text{ and } N \hookrightarrow M$
- $\therefore N \text{ is an } R\text{-module}$
- $\therefore ra \in N \quad \forall r \in R, a \in N$

(\Leftarrow) $\because a-b \in N, \forall a, b \in N$

- $\therefore (N, +)$ is subgroup of $(M, +)$
- $\therefore (M, +)$ is abelian group
- $\therefore (N, +)$ is a belian subgroup
- $\therefore (M, +)$ an R -module
- \therefore there exist a binary operation $\circ : R \times M \rightarrow M$

define \circ on N by $r \circ a = ra$

$\therefore (I, +)$ is a subgroup of $(R, +)$

$$\therefore a-b \in I$$

③ $\forall r \in R, \forall a \in I \Rightarrow ra \in I$ since I is a submodule of R .

Def 12:- If M be an R -module and N_1, N_2 be two submodule of M , then

$$N_1 \cap N_2 = \{m \in M \mid m \in N_1 \wedge m \in N_2\}$$

$$N_1 + N_2 = \{a+b \in M \mid a \in N_1 \wedge b \in N_2\}$$

Theorem 13:- If M be an R -module and N_1, N_2 be two submodule of M , then $N_1 \cap N_2$ and $N_1 + N_2$ are submodule of M .

proof :- (a): (1): $\because N_1, N_2 \subseteq M \Rightarrow N_1 \cap N_2 \subseteq M$
 $\therefore o \in N_1, o \in N_2 \Rightarrow o \in N_1 \cap N_2 \neq \emptyset$
 $\therefore \emptyset \neq N_1 \cap N_2 \subseteq M$

(2): $\forall a, b \in N_1 \cap N_2 \Rightarrow a, b \in N_1 \wedge a, b \in N_2$

since $N_1 \hookrightarrow M \wedge N_2 \hookrightarrow M$

$\therefore a-b \in N_1 \wedge a-b \in N_2$

$\therefore a-b \in N_1 \cap N_2$

(3): $\forall r \in R \wedge a \in N_1 \cap N_2$

$\Rightarrow r \in R \wedge a \in N_1 \wedge a \in N_2$

since $N_1 \hookrightarrow M \wedge N_2 \hookrightarrow M$

Def (14) :- let M be left R -module and $X \subseteq M$, then :-

$$A = \begin{cases} \left\{ \sum_{i=1}^n r_i x_i \mid r_i \in R, x_i \in X, n \in \mathbb{Z}^+ \right\}; & \text{if } X \neq \emptyset \\ \{0\} & \text{if } X = \emptyset \end{cases}$$

A is a left submodule of M . A is called the submodule generated by X denoted by $\langle X \rangle$.

$$A = \langle X \rangle$$

Def (15) ① The module M on R is called finitely generated if X is finite set.

② If M be an R -module and N be submodule of M , then N is called cyclic submodule if X has only one element m ,

$$N = (m).$$

Example ① Every R -module M has a generated set M .

② Every ring R with identity is finitely generated R -module since $\langle X \rangle = \langle \{1\} \rangle = R$

$\Rightarrow \cancel{a+b} = c$ where $a \in A, b \in B, c \in C$
 $\Leftarrow B \hookrightarrow C \Rightarrow a, b \in A \cap C \Rightarrow a = c - b \in A \cap C$
 $\therefore a+b = c \in (A \cap C) + B \Rightarrow (A+B) \cap C \hookrightarrow (A \cap C) + B$
 Let $d \in A \cap C, b \in B$, then since $B \hookrightarrow C$ it follows

$$d+b \in (A+B) \cap C \quad [\text{as } d \in A \cap C \Rightarrow d \in A+B, b \in B \Rightarrow b \in C]$$

$$\therefore (A \cap C) + B \hookrightarrow (A+B) \cap C$$

Remark If $B \not\hookrightarrow C$, then

$$(A \cap C) + (B \cap C) \hookrightarrow (A+B) \cap C$$

Def (19) :- ① M is called internal direct sum of set $\{B_i | i \in I\}$ of submodules $B_i \hookrightarrow M$:-

$$M = \bigoplus_{i \in I} B_i = \begin{cases} (1) & M = \sum_{i \in I} B_i \\ (2) & \forall j \in I \left[B_j \cap \sum_{\substack{i \in I \\ i \neq j}} B_i = 0 \right] \end{cases}$$

$M = \bigoplus_{i \in I} B_i$ is also said to be direct decomposition of M . In case finite set I , then

$$M = B_1 \oplus B_2 \oplus \dots \oplus B_n$$

② A submodule $B \hookrightarrow M$ is called a direct summand of M if $\exists C \hookrightarrow M$ such that

Def (21) :- Let N, M be two left R -module
then $f: N \rightarrow M$ is called ^{left} left
homomorphism $\in R$ if:-

- ① $\forall a, b \in N \Rightarrow f(a+b) = f(a) + f(b)$
- ② $\forall r \in R, \forall a \in N \Rightarrow f(ra) = r f(a)$

Example (22) :-

Let N, M be two left R -module

and $\hat{o}: M \rightarrow N$ define by

$\hat{o}(a) = 0'$, $\forall a \in M$ is a left homomorphism

is called zero homomorphism. (0 -homomorphism)

$$\textcircled{1} \quad \forall a, b \in M \Rightarrow \hat{o}(a+b) = 0' = 0' + 0' = \hat{o}(a) + \hat{o}(b)$$

$$\textcircled{2} \quad \forall r \in R, \forall a \in M \Rightarrow \hat{o}(ra) = 0' = r \cdot 0' = r \hat{o}(a)$$

$\therefore \hat{o}$ is R -homomorphism

Let M be an R -module, $I_m: M \rightarrow M$

define by $I_m(a) = a$, $\forall a \in M$, then I_m is
an homomorphism is called identity homomorphism.

$$\textcircled{1} \quad \forall a, b \in M \Rightarrow I_m(a+b) = a+b = I_m(a) + I_m(b)$$

$$\textcircled{2} \quad \forall r \in R, \forall a \in M \Rightarrow I_m(ra) = ra = r I_m(a)$$

$\therefore I_m$ is an R -homomorphism

Def:- Let $\alpha: M \rightarrow N$ be R-homomorphism on R

then:

① Kernel α denoted by $\text{Ker}(\alpha)$ define:

$$\text{Ker}(\alpha) = \{a \in M \mid \alpha(a) = 0\}$$

② Image α denoted by $\text{Im}(\alpha)$ define:

$$\text{Im}(\alpha) = \{ \alpha(a) \mid a \in M \} = \alpha(M)$$

Theorem:- If $\alpha: M \rightarrow N$ R-homomorphism

then ① $\text{Ker}(\alpha) \hookrightarrow M$

② $\text{Im}(\alpha) \hookrightarrow N$

(a) $\alpha(0) = 0 \Rightarrow 0 \in \text{Ker}(\alpha) \neq \emptyset$

(b) $\forall a, b \in \text{Ker}(\alpha) \Rightarrow \alpha(a) = 0, \alpha(b) = 0$

$$\alpha(a-b) = \alpha(a) - \alpha(b) = 0 - 0 = 0$$

$$\therefore a-b \in \text{Ker}(\alpha)$$

(c) $\forall r \in R, \forall a \in \text{Ker}(\alpha) \Rightarrow \alpha(ra) = 0$

$$\alpha(ra) = r \alpha(a) = r \cdot 0 = 0$$

$$\therefore ra \in \text{Ker}(\alpha)$$

$$\therefore \text{Ker}(\alpha) \hookrightarrow N$$

Theorem :- Let $\alpha: M \rightarrow N$ and $\beta: N \rightarrow K$ be two R-homomorphism, then $\beta \circ \alpha: M \rightarrow K$ is R-homomorphism

Proof :- ① $\forall a, b \in M$

$$(\beta \circ \alpha)(a+b) = \beta(\alpha(a+b)) = \beta(\alpha(a) + \alpha(b)) \\ = \beta(\alpha(a)) + \beta(\alpha(b))$$

② $\forall r \in R, a \in M$

$$(\beta \circ \alpha)(ra) = \beta(\alpha(ra)) = \beta(r\alpha(a)) \\ = r\beta(\alpha(a)) = r(\beta \circ \alpha)(a)$$

Theorem (Homomorphism theorem) :- If R-homomorphism

$\alpha: M \rightarrow N$, there exist R-homomorphism

$\alpha': M/\text{Ker}(\alpha) \rightarrow N$ such that $\alpha = \alpha' \circ \pi$

where $\pi: M \rightarrow M/\text{Ker}(\alpha)$ is the
R-homomorphism.

Proof

