Modules

KYB

Thrn, it's a Fact

mathrnfact@gmail.com

January 13, 2021

Overview

Definition

Let R be a ring (not necessarily commutative nor with 1). A *left* R-module is a set M together with

(1) $(M, +)$ is an abelian group

(2) $\cdot : R \times M \to M$ is a function denoted by rm for all $r \in R$ and $m \in M$ satisfying

  (a) $(r+s)m = rm + sm$ for all $r, s \in R$, $m \in M$

  (b) $(rs)m = r(sm)$ for all $r, s \in R$, $m \in M$

  (c) $r(m+n) = rm + rn$ for all $r \in R$, $m, n \in M$

 If R has a 1,

  (d) $1m = m$ for all $m \in M$.

- Similarly if $M \times R \to M$ by $(m, r) \mapsto mr$, M is a right module.
- If M is both a left R module and a right S module, we say M is a R, S-bimoudle.
- If R is commutative and M is a left R-module, we can define a right R-module structure by $mr = rm$. In this case, we say M is a R-module.
- Unless explicitly mentioned otherwise, “module” means “left module”.

Definition

Let R be a ring and let M be an R-module. A R-submodule of M is a subgroup N of M such that

$$rn \in N \text{ for all } r \in R, n \in N.$$

Definition

If R is a field, a R-module is called a vector space.

Example

- Let R be any ring. Then R is itself R-module. In this case, a submodule is an ideal of R. If R is not commutative, R as a left module and R as a right module may be different.
- For $n > 1$, let $R = M_n(F)$ where F is a field. Let $M \subset R$ be such that

  $$A \in M \iff A_i = 0 \text{ for all } i > 1.$$

  Then M is a submodule of R when R is considered as a left module over itself, but M is not a submodule of R when R is considered as a right R-module.

  $$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \notin M.$$

Example

Let R be a ring with 1 and let $n \in \mathbb{Z}^+$.

$$R^n = \{(a_1, \cdots, a_n) : a_i \in R, \text{ for all } i\}$$

is an R-module. R^n is called *the free module of rank n over R*.

Example ($\mathbb{Z}$-modules)

Let $R = \mathbb{Z}$ and let A be any abelian group and write the operation of A as $+$. Make A into a $\mathbb{Z}$-module as follows: for any $n \in \mathbb{Z}$ and $a \in A$ define

$$na = \begin{cases} a + a + \cdots + a \text{ (n times)} & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ -a - a - \cdots - a \text{ ($-n$ times)} & \text{if } n < 0 \end{cases}$$

Thus every abelian groups ia a $\mathbb{Z}$-module in this sense. Conversely every $\mathbb{Z}$-module is an abelian group.

Example

Let F be a field, let x be an indeterminate and let $R = F[x]$. Let V be a vector space over F and let T be a linear transformation from V to V. Using T, we can make V into an $F[x]$-module as follows: For $n \geq 0$, define

$$T^0 = I, T^1 = T, \cdots, T^n = T \circ T \circ \cdots \circ T \text{ (n times)}.$$

Let $p(x) \in F[x]$ where $p(x) = a_n x^n + \cdots + a_1 x + a_0$ and $v \in V$. Define

$$\begin{aligned} p(x) \cdot v &= (a_n T^n + a_{n-1} T^{n-1} + \cdots + a_1 T + a_0)(v) \\ &= a_n T^n(v) + a_{n-1} T^{n-1}(v) + \cdots + a_1 T(v) + a_0 v. \end{aligned}$$

Then V is an $F[x]$-module. Note that $F \subset F[x]$ as constant polynomial.

Definition

Let R be a commutative ring with identity. An R-algebra is a ring A with identity together with a ring homomorphism $f : R \to A$ mapping $1_R \to 1_A$ such that the subring $f(R)$ of A is contained in the center of A.
Recall that the center of A is the set $C(A)$ such that $a \in C(A)$ iff $ar = ra$ for all $r \in R$.

Remark

If A is an R-algebra, then A has a natural left and right R-module structure defined by $r \cdot a = a \cdot r = f(r)a$. Since R is commutative and $f(R) \subset C(A)$, this is well-defined R-module.

Definition

If A and B are two R-algebras, an R-algebra homomorphism is a ring homomorphism $\varphi : A \to b$ mapping $1_A \to 1_B$ such that $\varphi(r \cdot a) = r \cdot \varphi(a)$ for all $r \in R$ and $a \in A$. If φ is a bijective R-algebra, we call it an R-algebra isomorphism.

Example

Suppose that A is a ring with identity 1_A that is a left R-module satisfying $r \cdot (ab) = (r \cdot a)b = a(r \cdot b)$ for all $r \in R$ and $a, b \in A$.

- Then the map $f : R \to A$ defined by $f(r) = r \cdot 1_A$ is a ring homomorphism mapping $1_R \to 1_A$ and $f(R)$ is contained in the center of A.
- So A is an R-algebra and that the R-module structure on A induced by its algebra structure is precisely the original R-module structure.

Definition

Let R be a ring and let M and N be R-modules.

(1) A map $\varphi : M \to N$ is an R-module homomorphism if
  (a) $\varphi(x + y) = \varphi(x) + \varphi(y)$ for all $x, y \in M$;
  (b) $\varphi(rx) = r\varphi(x)$ for all $r \in R$ and $x \in M$.

(2) An R-homomorphism is an isomorphism if it is bijective.

(3) If $\varphi : M \to N$ is an R-module homomorphism, ler
  - $\mathrm{Ker}\varphi = \{m \in M : \varphi(m) = 0\}$
  - $\mathrm{Im}\,\varphi = \{\varphi(m) : m \in M\}$

(4) Let M and N be R-modules and define $\mathrm{Hom}_R(M, N)$ to be the set of all R-module homomorphisms from M into N.

Example

Let R be a ring and $M = R$. Then R-module homomorphism need not be ring homomorphism and vise versa. For instance,

- when $R = \mathbb{Z}$, $\varphi(x) = 2x$ is a $\mathbb{Z}$-homomorphism but not a ring homomorphism.
- when $R = F[x]$, $\varphi(f(x)) = f(x^2)$ is not an $F[x]$-module homomorphism but it is a ring homomorphism.

Example

Let R be a ring and let $n \in \mathbb{Z}^+$ and let $M = R^n$. For $i = 1, \cdots, n$, the projection map

$$\pi_i(x_1, \cdots, x_n) = x_i$$

is a surjective R-module homomorphism with kernel equal to the submodule of n-tuples which have a zero in position i.

Example

Every abelian group is a $\mathbb{Z}$-module. Moreover a map φ between two groups is an abelian group homomorphism iff $\mathbb{Z}$-module homomorphism.

Proposition

Let M and N and L be R-modules.

(1) A map $\varphi : M \to N$ is an R-module homomorphism iff

$$\varphi(rx + y) = r\varphi(x) + \varphi(y).$$

(2) Let $\varphi, \psi \in \mathrm{Hom}_R(M, N)$.
- Define $\varphi + \psi$ by $(\varphi + \psi)(m) = \varphi(m) + \psi(m)$. Then $\varphi + \psi \in \mathrm{Hom}_R(M, N)$ and with this operation $\mathrm{Hom}_R(M, N)$ is an abelian group.
- If R is a commutative ring, then for $r \in R$, define $r\phi$ by $(r\varphi)(m) = r\varphi(m)$. Then $r\varphi \in \mathrm{Hom}_R(M, N)$ and with this operation $\mathrm{Hom}_R(M, N)$ is an R-module.

(3) If $\varphi \in \mathrm{Hom}_R(L, M)$ and $\psi \in \mathrm{Hom}_R(M, N)$, then $\psi \circ \varphi \in \mathrm{Hom}_R(M, N)$.

(4)
- With addition as above and multiplication defied as function composition, $\mathrm{Hom}_R(M, M)$ is a ring with 1.
- When R is commutative, $\mathrm{Hom}_R(M, M)$ is an R-algebra.

Definition

The ring $\mathrm{Hom}_R(M, M)$ is called the endomorphism ring of M and will often be denoted by $\mathrm{End}_R(M)$. Elements of $\mathrm{End}_R(M)$ are called endomorphisms.

Remark

Suppose R is commutative. Then there is a natural map $R \to \mathrm{End}_R(M)$ given by $r \mapsto rI$. Since the image of this map is contained in the center of $\mathrm{End}_R(m)$, $\mathrm{End}_R(M)$ is an R-algebra. So this map is a ring homomorphism. Note that if $R = \mathbb{Z}$ and $M = \mathbb{Z}/2\mathbb{Z}$ and $r = 2$, $2 \mapsto 2I = 0$. Thus this map is not injective.

Observe

Since every R-module M is an abelian group, for any submodule N of M, M/N forms an additive group structure in the natural way. So if we can define a scalar product on M/N, M/N is a R-module, say the quotient module of M by N.

Proposition

Let R be a ring, let M be an R-module and let N be a submodule of M. Define $r \cdot (x + N) = rx + N$. This map is well-defined, and thus M/N is again R-module. The natural projection map $\pi : M \to M/N$ by $\pi(x) = x + N$ is an R-module homomorphism with kernel N.

Definition

Let A, B be submodules of the R-module M. The sum of A and B is the set

$$A + B = \{a + b : a \in A, b \in B\}.$$

Theorem (Isomorphism Theorems)

(1) *Let* M, N *be* R*-modules and let* $\varphi : M \to N$ *be an* R*-module homomorphism. Then* $\mathrm{Ker}\varphi$ *is a submodule of* M *and* $M \cong \mathrm{Im}\,\varphi$*.*

(2) *Let* A, B *be submodules of the* R*-module* M*. Then* $(A+B)/B \cong A/(A \cap B)$*.*

(3) *Let* M *be an* R*-module, and let* A *and* B *be submodules of* M *with* $A \subset B$*. Then* $(M/A)/(B/A) \cong M/B$*.*

(4) *Let* N *be a submodule of the* R*-module* M*. There is a bijective between the submodules of* M *which contain* N *and the submodules of* M/N*. The correspondence is given by* $A \leftrightarrow A/N$ *for all* $A \supset N$*.*

Exercise

$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/\gcd(m,n)\mathbb{Z}.$

Exercise

Let R be a commutative ring.

- $\mathrm{Hom}_R(R, M) \cong M$ as left R-modules M.
- $\mathrm{Hom}_R(R, R) \cong R$ as rings.

The End