22.5.24.

Module Fundamentals

Defn Let R be a ring (not necessarily commutative) a left R-module or a left module over R is a set M together with 2 operations

$+ : M \times M \longrightarrow M$ $\qquad$ $\cdot : R \times M \longrightarrow M$

$(m,n) \longmapsto m+n$ $\qquad$ $(r,m) \longrightarrow rm$

and a distinguished element $0 \in M$ so that

① $(M,+,0)$ is an abelian group

② $\forall r \in R, \forall m,n \in M : r(m+n) = rm + rn$

③ $\forall r,s \in R, \forall m \in M : (r+s)m = rm + sm$

④ $\forall r,s \in R, \forall m \in M : r(sm) = (rs)m$

⑤ $\forall m \in M : 1m = m$.

Rmk ① The maps $+, \cdot$ are called addition and scalar multiplication

The ring R acts on the set M via $\cdot : R \times M \to M$

This action respects the ring structure of R and the group operation $+$ in M.

② We have written the product rm with scalars r on the left

The axioms of a right R-module are similar with $(m+n)r = mr + nr$ etc.

③ If the ring R is commutative and M is a left R-module we can make M into a right R-module by defining $mr = rm$ $\forall m \in M$ $\forall r \in R$

If R is not commutative, axiom (4) will not hold with this definition. So not every left R module is also a Right R-module.

We'll assume from now on that R is a comm. ring, and drop the "left" from the left R-module

Examples (1) If R is a field F then the axioms of an R-module are exactly the axioms of a vector space over F

Hence modules over a field F and vector spaces over F are the same.

(2) Let R be any ring. Then $M = R$ is an R-module where $+, \cdot$ are the usual ring operations in R.

(3) If R is any ring, then $R^n = \{(a_1, \dots a_n) \mid a_i \in R \ \forall i\}$ the set of all n-tuples with components in R, is an R-module with usual defn of componentwise addition and scalar multiplication $r(a_1 \dots a_n) = (ra_1, ra_2, \dots ra_n)$

(4) $M = M_{m \times n}(R)$ set of all $m \times n$ matrices with entries in R. Then M is an R-module where addition is ordinary matrix addition and multiplication by r, of a matrix $A \in M$ means multiplication of each entry of A by r.

(5) Every abelian group A is a $\mathbb{Z}$-module where we write the operation of A as $+$
Make A into a $\mathbb{Z}$-module by defining for any $n \in \mathbb{Z}$, $a \in A$

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

Here 0 is the identity of the additive group A.

Defn A submodule N of an R-module M is a subset $N \subset M$ such that
(a) $N \neq \emptyset$
(b) N is a subgroup of M
(c) $\forall r \in R,\ n \in N : rn \in N$.

Submodules of M are subsets of M which are themselves modules under the restricted operations.

Ex (1) If $R = F$ a field, submodules are the same as vector subspaces.

(2) Every R-module M has 2 submodules M and 0 (unless it is the trivial module)

(3) Submodules of R as an R-module are exactly the ideals of R.

(4) $\bigcap_{i \in I} A_i$ is a submodule of M where A_i's are submodules of M.

Defn ① Given submodules $M_1, \ldots M_n$ of M

$$M_1 + \ldots + M_n := \{m_1 + \ldots + m_n \mid m_i \in M_i\}$$

is a submodule of M.

If the map $\pi : M_1 \times \ldots \times M_n \to M_1 + \ldots + M_n$

$$(m_1, \ldots, m_n) \longmapsto (m_1 + \ldots + m_n)$$

is bijective, then the sum is called the direct sum or internal direct sum of modules $M_1, \ldots, M_n$ and is denoted by

$$M_1 \oplus \ldots \oplus M_n = \bigoplus_{i=1} M_n$$

② Let $M_1, \ldots, M_n$ be a collection of R modules. The collection of n-tuples $(m_1, \ldots, m_n)$, $m_i \in M_i$ with addition and action of R defined component-wise is called the direct product or external direct sum of $M_1, \ldots, M_n$ is denoted by $M_1 \boxplus \ldots \boxplus M_n$ or sometimes also by $M_1 \oplus \ldots \oplus M_n$

③ If M_i, $i \in I$ is a collection of modules, (not nec. finite I). The direct product of the modules M_i is defined to be their direct product as abelian gps with componentwise addition, and action of R also defined componentwise.

The direct sum of modules M_i, ΣM_i is defined as the restricted direct product of abelian groups i.e. The direct sum of the M_i's is the subset of the direct product $\prod M_i$ which contains all elements $\prod_i m_i$ s.t only finitely many of the components are non-zero.

The action of R on the direct product or direct sum is given by $r \prod_i m_i = \prod_i r m_i$

(Recall $\prod_{i \in I} A_i$ for a collection of sets is the set of all functions $f : I \longrightarrow \bigcup_{i \in I} A_i$ s.t $f(i) \in A_i \ \forall i \in I$)

Rmk

The direct product and direct sum of an infinite number of modules are different in general. eg. $R = \mathbb{Z}$, $I = \mathbb{Z}^{\geq 2}$ M_i = cyclic gp of order i $= \mathbb{Z}/i\mathbb{Z}$

Then the direct sum of the M_i's is not isom to their direct product

The next proposition indicates when a module is isomorphic to the finite direct product of some of its submodules, and says that the interal direct sum of submodules $M_1, \dots, M_n$ is isomorphic to their external direct sum

As in the case of internal and external direct sum of groups one has.

Prop 9.1 Let $M_1 \dots M_n$ be submodules of R-module M. Then TFAE

① The map $\pi : M_1 \times \dots \times M_n \longmapsto M_1 + \dots + M_n$ defined by

$$\pi(m_1, \dots, m_n) = m_1 + \dots + m_n$$

is bijective (It is in fact an ison of R-modules).

② $M_j \cap (M_1 + \dots + M_{j-1} + M_j + \dots + M_n) = 0$

$\forall j \in \{1, \dots n\}$

③ Every $x \in M_1 + \dots + M_n$ can be written uniquely in the form $x = m_1 + \dots + m_n$ with $m_i \in M_i$

Defn ① A map between 2 R-modules $\varphi : M \to N$ is called R-linear or a (R-modul)-Homomorphism if it satisfies

① $\forall m, m' \in M, \quad \varphi(m + m') = \varphi(m) + \varphi(m')$

② $\forall m \in M, \ \forall r \in R, \quad \varphi(rm) = r\varphi(m)$.

The set of all homomorphism $M \to N$ is denoted by $Hom_R(M, N) = \{\varphi : M \to N \mid \varphi \text{ hom}\}$.

A homomorphism $M \to M$ is called an endomorphism, and we write $\mathrm{End}_R(M) := \mathrm{Hom}_R$

(3) An R-module hom is an isomorphism if it is bijective.
M, N are called isomorphic if there is some R-mod hom $\varphi : M \to N$

(4) An isomorphism $M \to M$ is called an automorphism of M.

(5) If $\varphi : M \to N$ is a R-module hom, then kernel of $\varphi := \ker\varphi := \{ m \in M \mid \varphi(m) = 0_N \}$
and
$\varphi(M) = \{ n \in N \mid n = \varphi(m) \text{ for some } m \in M \}$
is the image of φ.

It is easy to prove

Prop 9.2 For a hom of R-modules $\varphi : M \to N$ we have (a) $\ker\varphi$ is a submodule of M

(b) $\mathrm{Im}\,\varphi$ is a submodule of N
(c) φ is injective $\Leftrightarrow$ $\ker\varphi = \{0\}$
(d) φ is surjective $\Leftrightarrow$ $\mathrm{Im}\,\varphi = N$.

Prop 9.3

For an R-module M, and a submodule N the additive abelian quotient M/N can be made into an R-module by defining $r(x+N) := rx + N$

$\forall r \in R,\ x+N \in M/N$.

Then the natural projection $\pi : M \to M/N$, $x \mapsto x+N$ is an R-mod. hom with kernel N.

As in the case of group isom thms we have

Thm 9.4 Isom. Theorems

① Let M, N be R-modules, and $\varphi : M \to N$ an R-module homomorphism. Then φ induces an isomorphism $M/\ker\varphi \cong \varphi(M)$

$$m + \ker\varphi \longmapsto \varphi(m)$$

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, A and B submodules of M with $A \subseteq B$. Then $(M/A)/(B/A) \cong M/B$.

'In linear algebra, the concept of linear combination, spanning sets, basis make sense also when the coefficients come from a ring not just a field

Defn In an R-module M, an R-linear combination of elements $a_1, \ldots a_k \in M$ is an element of the form

$$m = r_1 a_1 + \ldots + r_k a_k, \text{ with } r_i \in R, i=1, \ldots k$$

If every element $m \in M$ is a linear combination of $a_1, \ldots a_k$ we say

$\{a_1, \ldots a_k\}$ is a spanning or generating set of M or a_i's generate M.

Defn An R-module M is called finitely generated when it has a finite spanning set.

Defn A spanning set A of an R-module M is a subset $\{a_i\}_{i \in I}$ of M such that

every $m \in M$ is a finite R-linear combination of the m_i's

$$m = \sum_{i \in I} r_i a_i \quad \text{where} \quad r_i \in R \ \forall i$$
$$r_i = 0 \quad \text{for almost all } i.$$

$RA = M = \{r_1 a_1 + \dots + r_k a_k \mid r_1 \dots r_k \in R, a_1 \dots a_k \in A, k \in \mathbb{Z}^+\}$

Rmk The definition of spanning set require that each lin combination is finite

Defn In an R-module M, a subset $\{a_i\}_{i \in I}$ is called linearly independent if the only relation $\sum r_i a_i = 0$ is the one where $r_i = 0 \ \forall i$!

ie $\sum_i r_i a_i = 0 \Rightarrow r_i = 0 \quad \forall i$

A subset of M is called a basis if it is a linearly independent spanning set.

A module that has a basis is called a free module

If the basis of a free module is finite then M is called finite-free module

If (the basis has n elements, M is said to be free of rank n.)*

Rmk An R-module M is free on the subset A of M if for every non-zero element $m \in M$, there is a unique non-zero elts $r_1, \dots, r_k \in R$ and unique $a_1 \dots a_k$ in A s.t

$$m = r_1 a_1 + \dots + r_k a_k \quad \text{for some } k \in \mathbb{Z}^+.$$

Rmk in a module every subset of a lin. indep. subset is lin. independent

and every set containing a lin. dependent set is linearly dependent just as the case in vector spaces.

BUT in a vector space linear independence of a subset can also be reformulated as no member of the subset is a lin. combination of the other members in the subset

in a module this condition (is valid for a lin. indep. subset but) is not equivalent to lin. independence

eg. $M = \mathbb{Z}$ as a $\mathbb{Z}$ module
we cannot write the elements $2, 3 \in \mathbb{Z}$ as a $\mathbb{Z}$-multiple of the other but the set $\{2, 3\}$ is lin dependent

$$2a + 3b = 0 \quad \text{with } a = 3,\ b = -2.$$