Abstract Algebra II

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 342

Subsection 1

Basic Definitions and Examples

Modules

Definition (Module)

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

(1) a binary operation $+$ on M under which M is an abelian group, and

(2) an action of R on M (that is, a map $R \times M \to M$) denoted by rm, for all $r \in R$ and for all $m \in M$, which satisfies:

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

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

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

  If the ring R has a 1, we impose the additional axiom:

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

- The descriptor "left" in the above definition indicates that the ring elements appear on the left.
- **Right R-modules** can be defined analogously.

Remarks on the Definition

- If the ring R is commutative and M is a left R-module, we can make M into a right R-module by defining $mr = rm$, for $m \in M$ and $r \in R$.
- If R is not commutative, Axiom 2(b),

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

  in general will not hold with this definition.

  So not every left R-module is also a right R-module.
- Unless explicitly mentioned otherwise the term "module" will always mean "left module."
- Modules satisfying Axiom 2(d),

$$1m = m, \text{ for all } m \in M,$$

  are called **unital modules**.
- All our modules will be unital.

Submodules

- When R is a field F, the axioms for an R-module are precisely the same as those for a vector space over F.

  Modules over a field F and vector spaces over F are the same.

Definition (Submodule)

Let R be a ring and let M be an R-module. An R-**submodule of** M is a subgroup N of M which is closed under the action of ring elements, i.e., $rn \in N$, for all $r \in R, n \in N$.

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

  In particular, if $R = F$ is a field, submodules are the same as subspaces.
- Every R-module M has the two submodules M and 0 (the latter is called the **trivial submodule**).

View of a Ring as a Module

(1) Let R be any ring. Then $M = R$ is a left R-module, where the action of a ring element on a module element is just the usual multiplication in the ring R (similarly, R is a right module over itself).

In particular, every field can be considered as a (1-dimensional) vector space over itself.

When R is considered as a left module over itself in this fashion, the submodules of R are precisely the left ideals of R (and if R is considered as a right R-module over itself, its submodules are the right ideals).

Thus, if R is not commutative, it has a left and right module structure over itself and these structures may be different (e.g., the submodules may be different).

Affine n-Space of a Field

(2) Let $R = F$ be a field.

Every vector space over F is an F-module and vice versa.

Let $n \in \mathbb{Z}^+$ and let

$$F^n = \{(a_1, a_2, \ldots, a_n) : a_i \in F, \text{ for all } i\}$$

(called **affine n-space over F**).

Make F^n into a vector space by defining addition and scalar multiplication componentwise:

$$\begin{aligned}(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) &= (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) \\ \alpha(a_1, \ldots, a_n) &= (\alpha a_1, \ldots, \alpha a_n), \quad \alpha \in F.\end{aligned}$$

As in the case of Euclidean n-space (i.e., when $F = \mathbb{R}$), affine n-space is a vector space of dimension n over F (we shall discuss the notion of dimension more formally later).

Free Modules of Rank n

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

Define
$$R^n = \{(a_1, a_2, \ldots, a_n) : a_i \in R, \text{ for all } i\}.$$

Make R^n into an R-module by componentwise addition and multiplication by elements of R in the same manner as when R was a field.

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

An obvious submodule of R^n is given by the i-th component, namely the set of n-tuples with arbitrary ring elements in the i-th component and zeros in the j-th component for all $j \neq i$.

Multiple Module Structures

(4) The same abelian group may have the structure of an R-module for a number of different rings R and each of these module structures may carry useful information.

Specifically, if M is an R-module and S is a subring of R with $1_S = 1_R$, then M is automatically an S-module as well.

For instance the field $\mathbb{R}$ is:

- an $\mathbb{R}$-module;
- a $\mathbb{Q}$-module;
- a $\mathbb{Z}$-module.

Annihilating Ideals

(5) If M is an R-module and for some (2-sided) ideal I of R,

$$am = 0, \text{ for all } a \in I \text{ and all } m \in M,$$

we say M is **annihilated by** I.

In this situation we can make M into an (R/I)-module by defining an action of the quotient ring R/I on M as follows:

$$(r + I)m = rm, \text{ for all } m \in M \text{ and coset } r + I \text{ in } R/I.$$

Since $am = 0$, for all $a \in I$ and all $m \in M$, this is well defined.

One easily checks that it makes M into an (R/I)-module.

In particular, when I is a maximal ideal in the commutative ring R and $IM = 0$, then M is a vector space over the field R/I.

$\mathbb{Z}$-Modules

- Let $R = \mathbb{Z}$, let A be any abelian group (finite or infinite) 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
  $$na = \begin{cases} a + a + \cdots + a \text{ (n times)}, & \text{if } n > 0 \\ 0, & \text{if } n = 0 \\ -a - a - \cdots - a \text{ } (-n \text{ times}), & \text{if } n < 0 \end{cases}$$
  (here 0 is the identity of the additive group A).
  This definition of an action of $\mathbb{Z}$ on A makes A into a $\mathbb{Z}$-module.
  The module axioms show that this is the only possible action of $\mathbb{Z}$ on A making it a (unital) $\mathbb{Z}$-module.
  Thus every abelian group is a $\mathbb{Z}$-module.
  Conversely, if M is any $\mathbb{Z}$-module, a fortiori M is an abelian group.
  Hence, $\mathbb{Z}$-modules are the same as abelian groups.
- Furthermore, it is immediate from the definition that $\mathbb{Z}$-submodules are the same as subgroups.

$\mathbb{Z}$-Modules (Cont'd)

- For the cyclic group $\langle a \rangle$ written multiplicatively, the additive notation na becomes a^n, that is, we have all along been using the fact that $\langle a \rangle$ is a right $\mathbb{Z}$-module (the laws of exponents are the $\mathbb{Z}$-module axioms).
- Since $\mathbb{Z}$ is commutative these definitions of left and right actions by ring elements give the same module structure.
- If A is an abelian group containing an element x of finite order n, then $nx = 0$. Thus, in contrast to vector spaces, a $\mathbb{Z}$-module may have nonzero elements x, such that $nx = 0$, for some nonzero ring element n.

  In particular, if A has order m, then by Lagrange's Theorem $mx = 0$, for all $x \in A$. In that case, A is a module over $\mathbb{Z}/m\mathbb{Z}$.

  In particular, if p is a prime and A is an abelian group (written additively) such that $px = 0$, for all $x \in A$, then A is a $\mathbb{Z}/p\mathbb{Z}$-module, i.e., can be considered as a vector space over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

$F[x]$-modules

- Let F be a field, let x be an indeterminate and let R be the polynomial ring $F[x]$.

  Let V be a vector space over F (i.e., an F-module) and let T be a linear transformation from V to V.

  The linear map T enables us to make V into an $F[x]$-module:
  - For the nonnegative integer n, define

  $$\begin{array}{rcl} T^0 & = & I, \text{ the identity map from } V \text{ to } V, \\ T^n & = & T \circ T \circ \cdots \circ T \ (n \text{ times}), \circ \text{ is function composition.} \end{array}$$

  - Also, for any two linear transformations A, B from V to V and elements $\alpha, \beta \in F$, let $\alpha A + \beta B$ be defined (pointwise) by

  $$(\alpha A + \beta B)(v) = \alpha(A(v)) + \beta(B(v)).$$

  Then $\alpha A + \beta B$ is seen to be a linear transformation from V to V.

  I.e., linear combinations of linear transformations are again linear transformations.

$F[x]$-modules (Cont'd)

- Define the action of any polynomial in x on V: Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where $a_0, \ldots, a_n \in F$.
  For each $v \in V$, define an action of $p(x)$ on the module element v by

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

  i.e., $p(x)$ acts by:
  - substituting the linear transformation T for x in $p(x)$;
  - applying the resulting linear transformation to v.

  Put another way:
  - Let x act on V as the linear transformation T;
  - Extend this to an action of all of $F[x]$ on V in a natural way.

$F[x]$-modules (Verification)

- It is easy to check that this definition of an action of $F[x]$ on V satisfies all the module axioms,

  i.e., for all $f(x), g(x) \in F[x]$ and all $v, u \in V$,
  - $(f(x) + g(x))v = f(v)v + g(x)v$;
  - $(f(x)g(x))v = f(x)(g(x)v)$;
  - $f(x)(v + u) = f(x)v + f(x)u$;
  - $1v = v$.

  So it makes V into an $F[x]$-module.
- The field F is naturally a subring of $F[x]$ and the action of these field elements is by definition the same as their action when viewed as constant polynomials.
- So the definition of the $F[x]$ action on V is consistent with the given action of the field F on the vector space V.

$F[x]$-modules (Special Cases)

- The way $F[x]$ acts on V depends on the choice of T.
- Thus, there are in general many different $F[x]$-module structures on the same vector space V.
  - If $T = 0$, and $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$, $v \in V$, then
  $$p(x)v = a_0 v,$$
  i.e., the polynomial $p(x)$ acts on v simply by multiplying by the constant term of $p(x)$.
  In this case, the $F[x]$-module structure is just the F-module structure.
  - If T is the identity transformation,
  $$T^n(v) = v \text{ for all } n \text{ and } v.$$
  We now get
  $$\begin{array}{rcl} p(x)v & = & a_n v + a_{n-1} v + \ldots + a_0 v \\ & = & (a_n + \cdots + a_0)v. \end{array}$$
  So $p(x)$ multiplies v by the sum of the coefficients of $p(x)$.

$F[x]$-modules (Another Special Case)

- For another example, let V be affine n-space F^n and let T be the "shift operator" $T(x_1, x_2, \ldots, x_n) = (x_2, x_3, \ldots, x_n, 0)$.

  Let e_i be the usual i-th basis vector $(0, 0, \ldots, 0, 1, 0, \ldots, 0)$, where the 1 is in position i. Then:

$$T^k(e_i) = \begin{cases} e_{i-k}, & \text{if } i > k \\ 0, & \text{if } i \leq k \end{cases}$$

  So for example, if $m < n$,

$$(a_m x^m + a_{m-1} x^{m-1} + \cdots + a_0) e_n = (0, \ldots, 0, a_m, a_{m-1}, \ldots, a_0).$$

  From this we can determine the action of any polynomial on any vector.

Characterization of $F[x]$-modules

- The construction of an $F[x]$-module from a vector space V over F and a linear transformation T from V to V in fact describes all $F[x]$-modules:

  An $F[x]$-module is a vector space together with a linear transformation which specifies the action of x, since then:
  - V is an F-module;
  - the action of the ring element x on V is a linear transformation from V to V.
  - The axioms for a module ensure that the actions of F and x on V uniquely determine the action of any element of $F[x]$ on V.
- There is a bijection between the collection of $F[x]$-modules and the collection of pairs V, T

$$V \text{ an } F[x]\text{-module} \leftrightarrow \left\{ \begin{array}{c} V \text{ a vector space over } F \\ T : V \to V \text{ a linear transformation} \end{array} \right\}$$

given by: "the element x acts on V as the linear transformation T".

$F[x]$-Submodules

- Consider $F[x]$-submodules of V where
  - V is any $F[x]$-module;
  - T is the linear transformation from V to V given by the action of x.
- If W is an $F[x]$-submodule of V:
  - It must first be an F-submodule, i.e., a vector subspace of V.
  - Second, it must be sent to itself under the action of the ring element x, i.e., we must have $T(w) \in W$, for all $w \in W$.
- Any vector subspace U of V, such that $T(U) \subseteq U$ is called T-**stable** or T-**invariant**.
- If U is any T-stable subspace of V, it follows that $T^n(U) \subseteq U$, for all $n \in \mathbb{Z}^+$ (e.g., $T(U) \subseteq U$ implies $T^2(U) = T(T(U)) \subseteq T(U) \subseteq U$).

  Moreover any linear combination of powers of T then sends U into U.

  So U is also stable by the action of any polynomial in T.

  Thus U is an $F[x]$-submodule of V.

$F[x]$-Submodules (Cont'd)

- The preceding reasoning shows that the $F[x]$-submodules of V are precisely the T-stable subspaces of V.
- In terms of the bijection above,

$$W \text{ an } F[x]\text{-submodule} \leftrightarrow \left\{ \begin{array}{l} W \text{ a subspace of } V \\ W \text{ is } T\text{-stable} \end{array} \right\}$$

which gives a complete dictionary between $F[x]$-modules V and vector spaces V together with a given linear transformation T from V to V.

Example: Suppose T is the shift operator defined on affine n-space above and k is any integer in the range $0 \leq k \leq n$. The subspace

$$U_k = \{(x_1, x_2, \ldots, x_k, 0, \ldots, 0) : x_i \in F\}$$

is T-stable. So U_k is an $F[x]$-submodule of V.

A Submodule Criterion

Proposition (The Submodule Criterion)

Let R be a ring and let M be an R-module. A subset N of M is a submodule of M if and only if:

(1) $N \neq \emptyset$, and

(2) $x + ry \in N$, for all $r \in R$ and for all $x, y \in N$.

- If N is a submodule, then $0 \in N$ so $N \neq \emptyset$. Also N is closed under addition and is sent to itself under the action of elements of R.

  Conversely, suppose (1) and (2) hold. Let $r = -1$ and apply the subgroup criterion (in additive form) to see that N is a subgroup of M. In particular, $0 \in N$. Now let $x = 0$ and apply hypothesis (2) to see that N is sent to itself under the action of R.

  This establishes the proposition.

Subsection 2

Quotient Modules and Module Homomorphisms

Homomorphisms, Kernels and Images

Definition (R-Module Homomorphism)

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 it respects the R-module structures of M and N:

(a) $\varphi(x+y) = \varphi(x) + \varphi(y)$, for all $x, y \in M$;

(b) $\varphi(rx) = r\varphi(x)$, for all $r \in R, x \in M$.

(2) An R-module homomorphism is an **isomorphism** (**of** R-**modules**) if it is both injective and surjective. The modules M and N are said to be **isomorphic**, denoted $M \cong N$, if there is some R-module isomorphism $\varphi : M \to N$.

(3) If $\varphi : M \to N$ is an R-module homomorphism, let $\ker\varphi = \{m \in M : \varphi(m) = 0\}$ (the **kernel** of φ) and let $\varphi(M) = \{n \in N : n = \varphi(m),$ for some $m \in M\}$ (the **image** of φ, as usual).

(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.

Remarks

- Any R-module homomorphism is also a homomorphism of the additive groups; However, not every group homomorphism need be a module homomorphism.
- It is an easy exercise using the submodule criterion to show that kernels and images of R-module homomorphisms are submodules.
- If R is a ring and $M = R$ is a module over itself, then:
  (a) R-module homomorphisms (even from R to itself) need not be ring homomorphisms;
  Example: When $R = \mathbb{Z}$, the $\mathbb{Z}$-module homomorphism $x \mapsto 2x$ is not a ring homomorphism (1 does not map to 1).
  (b) Ring homomorphisms need not be R-module homomorphisms.
  Example: When $R = F[x]$ the ring homomorphism $\varphi : f(x) \mapsto f(x^2)$ is not an $F[x]$-module homomorphism: If it were, we would have $x^2 = \varphi(x) = \varphi(x \cdot 1) = x\varphi(1) = x$.

Examples

(2) Let R be a ring, let $n \in \mathbb{Z}^+$ and let $M = R^n$. For each $i \in \{1, \ldots, n\}$, the projection map $\pi_i : R^n \to R$; $\pi_i(x_1, \ldots, x_n) = x_i$, is a surjective R-module homomorphism with kernel equal to the submodule of n-tuples which have a zero in position i.

(3) If R is a field, R-module homomorphisms are called **linear transformations**.

(4) For the ring $R = \mathbb{Z}$ the action of ring elements (integers) on any $\mathbb{Z}$-module amounts to just adding and subtracting within the (additive) abelian group structure of the module. So in this case condition (b) of a homomorphism is implied by condition (a).

E.g., $\varphi(2x) = \varphi(x + x) = \varphi(x) + \varphi(x) = 2\varphi(x)$.

Thus, $\mathbb{Z}$-module homomorphisms are the same as abelian group homomorphisms.

Examples (Cont'd)

(5) Let R be a ring, let I be a 2-sided ideal of R and suppose M and N are R-modules annihilated by I:

$$\begin{array}{rcll} am & = & 0, & a \in I, m \in M, \\ an & = & 0, & a \in I, n \in N. \end{array}$$

Any R-module homomorphism from N to M is then automatically a homomorphism of (R/I)-modules.

- In particular, if A is an additive abelian group such that for some prime p, $px = 0$, for all $x \in A$, then any group homomorphism from A to itself is a $\mathbb{Z}/p\mathbb{Z}$-module homomorphism, i.e., is a linear transformation over the field $\mathbb{F}_p$.

  In particular, the group of all (group) automorphisms of A is the group of invertible linear transformations from A to itself: $\mathrm{GL}(A)$.

Properties of Homomorphisms

Proposition

Let M, N and L be R-modules.

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

(2) Let $\varphi, \psi \in \mathrm{Hom}_R(M, N)$.
- Define $\varphi + \psi$ by $(\varphi + \psi)(m) = \varphi(m) + \psi(m)$, for all $m \in M$. 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 $r\varphi$ by $(r\varphi)(m) = r(\varphi(m))$, for all $m \in M$. Then $r\varphi \in \mathrm{Hom}_R(M, N)$ and with this action of the commutative ring R the abelian group $\mathrm{Hom}_R(M, N)$ is an R-module.

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

(4) With addition as above and multiplication defined as function composition, $\mathrm{Hom}_R(M, M)$ is a ring with 1.

Proof of Properties

(1) If φ is an R-module homomorphism, $\varphi(rx+y) = r\varphi(x)+\varphi(y)$. Suppose, conversely, $\varphi(rx+y) = r\varphi(x)+\varphi(y)$.

- Take $r=1$ to see that φ is additive;
- Take $y=0$ to see that φ commutes with the action of R on M (i.e., is **homogeneous**).

(2) It is straightforward to check that all the abelian group and R-module axioms hold with these definitions. The commutativity of R is used to show that $r\varphi$ satisfies the second axiom for $r\varphi$:

$$\begin{array}{rcl}(r_1\varphi)(r_2m) & = & r_1\varphi(r_2m) \quad \text{(definition of } r_1\varphi) \\ & = & r_1r_2(\varphi(m)) \quad (\varphi \text{ homomorphism}) \\ & = & r_2r_1\varphi(m) \quad (R \text{ commutative}) \\ & = & r_2(r_1\varphi)(m). \quad \text{(definition of } r_1\varphi)\end{array}$$

Verification of the axioms relies ultimately on the hypothesis that N is an R-module. The domain M could in fact be any set - it does not have to be an R-module nor an abelian group.

Proof of Properties (Cont'd)

(3) Let φ and ψ be as given and let $r \in R$, $x, y \in L$. Then

$$\begin{array}{rcl}(\psi \circ \varphi)(rx + y) & = & \psi(\varphi(rx + y)) \\ & = & \psi(r\varphi(x) + \varphi(y)) \\ & = & r\psi(\varphi(x)) + \psi(\varphi(y)) \\ & = & r(\psi \circ \varphi)(x) + (\psi \circ \varphi)(y).\end{array}$$

So, by (1), $\psi \circ \varphi$ is an R-module homomorphism.

(4) Note that since the domain and codomain of the elements of $\text{Hom}_R(M, M)$ are the same, function composition is defined. By (3), it is a binary operation on $\text{Hom}_R(M, M)$. As usual, function composition is associative. The remaining ring axioms are straightforward to check. The identity function, I ($I(x) = x$, for all $x \in M$), is seen to be the multiplicative identity of $\text{Hom}_R(M, M)$.

The Ring of Endomorphisms

Definition (Endomorphism Ring)

The ring $\mathrm{Hom}_R(M, M)$ is called the **endomorphism ring** of M and will often be denoted by $\mathrm{End}_R(M)$, or just $\mathrm{End}(M)$ when the ring R is clear from context. Elements of $\mathrm{End}(M)$ are called **endomorphisms**.

- When R is commutative there is a natural map from R into $\mathrm{End}(M)$ given by
$$r \mapsto rI,$$
where the latter endomorphism of M is just multiplication by r on M.
- The ring homomorphism from R to $\mathrm{End}_R(M)$ may not be injective, since for some r we may have $rm = 0$, for all $m \in M$, take, e.g., $R = \mathbb{Z}, M = \mathbb{Z}/2\mathbb{Z}$, and $r = 2$.
- When R is a field, however, this map is injective (in general, no unit is in the kernel of this map) and the copy of R in $\mathrm{End}_R(M)$ is called the (subring of) **scalar transformations**.

Quotient Modules and Natural Projections

Proposition

Let R be a ring, let M be an R-module and let N be a submodule of M. The (additive, abelian) quotient group M/N can be made into an R-module by defining an action of elements of R by

$$r(x+N) = (rx) + N \text{ for all } r \in R,\ x+N \in M/N.$$

The natural projection map $\pi : M \to M/N$ defined by $\pi(x) = x + N$ is an R-module homomorphism with kernel N.

- Since M is an abelian group under $+$ the quotient group M/N is defined and is an abelian group.
  We show, next, that the action of the ring element r on the coset $x+N$ is well defined:

  Suppose $x+N = y+N$. Then $x-y \in N$. Since N is an R-submodule, $r(x-y) \in N$. Thus $rx - ry \in N$. Hence, $rx + N = ry + N$.

Quotient Modules and Natural Projections (Cont'd)

- Since the operations in M/N are "compatible" with those of M, the axioms for an R-module are easily checked in the same way as was done for quotient groups.

  For example, for axiom 2(b), if $r_1, r_2 \in R$ and $x + N \in M/N$,

$$\begin{array}{rcl}(r_1 r_2)(x + N) & = & (r_1 r_2 x) + N \\ & = & r_1(r_2 x + N) \\ & = & r_1(r_2(x + N)).\end{array}$$

  The other axioms are similarly checked.

Quotient Modules and Natural Projections (Cont'd)

- Finally, the natural projection map π described above is, in particular, the natural projection of the abelian group M onto the abelian group M/N, hence is a group homomorphism with kernel N.

  The kernel of any module homomorphism is the same as its kernel when viewed as a homomorphism of the abelian group structures.

  It remains only to show π is a module homomorphism, i.e., $\pi(rm) = r\pi(m)$:

$$\pi(rm) = rm + N = r(m + N) = r\pi(m).$$

The Sum of Two Submodules

Definition (Sum of Submodules)

Let A, B be submodules of the R-module M. The **sum** of A and B is the set $A + B = \{a + b : a \in A, b \in B\}$.

- The sum of two submodules A and B is a submodule:
  - Clearly, $0 = 0 + 0 \in A + B$. So $A + B \neq \emptyset$.
  - Let $a_1 + b_1, a_2 + b_2 \in A + B$ and $r \in R$. We have

$$\begin{array}{rcl} (a_1 + b_1) + r(a_2 + b_2) & = & (a_1 + b_1) + (ra_2 + rb_2) \\ & = & (a_1 + ra_2) + (b_1 + rb_2) \in A + B. \end{array}$$

  By the Submodule Criterion, $A + B$ is a submodule of M.
- $A + B$ is the smallest submodule which contains both A and B.
  - Since $0 \in A$ and $0 \in B$, $A \subseteq A + B$ and $B \subseteq A + B$;
  - Suppose N is a submodule of M containing A and B. Since N is closed under addition, $A + B \subseteq N$. Thus, $A + B$ is the smallest submodule of M containing A and B.

The Module Isomorphism Theorems

Theorem (Isomorphism Theorems)

(1) (The First Isomorphism Theorem for Modules) Let M, N be R-modules and let $\varphi : M \to N$ be an R-module homomorphism. Then $\ker\varphi$ is a submodule of M and $M/\ker\varphi \cong \varphi(M)$.

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

(3) (The Third Isomorphism Theorem) Let M be an R-module, and let A, B be submodules of M with $A \subseteq B$. Then $(M/A)/(B/A) \cong M/B$.

(4) (The Fourth or Lattice Isomorphism Theorem) Let N be a submodule of the R-module M. There is a bijection between the submodules of M which contain N and the submodules of M/N, given by $A \leftrightarrow A/N$, for all $A \supseteq N$. This correspondence commutes with sums and intersections (i.e., is a lattice isomorphism between the lattices of submodules of M/N and of submodules of M which contain N).

Subsection 3

Generation, Direct Sums and Free Modules

Sum and Generation

Definition (Sum and Generation of Submodules)

Let M be an R-module and let $N_1, \ldots, N_n$ be submodules of M.

(1) The **sum** of $N_1, \ldots, N_n$ is the set of all finite sums of elements from the sets N_i: $\{a_1 + a_2 + \cdots + a_n : a_i \in N_i, \text{ for all } i\}$. Denote this sum by $N_1 + \cdots + N_n$.

(2) For any subset A of M let

$$\begin{aligned} RA \quad = \quad & \{r_1a_1 + r_2a_2 + \cdots + r_ma_m : \\ & r_1, \ldots, r_m \in R, a_1, \ldots, a_m \in A, m \in \mathbb{Z}^+\} \end{aligned}$$

(where by convention $RA = \{0\}$, if $A = \emptyset$). If A is the finite set $\{a_1, a_2, \ldots, a_n\}$, we shall write $Ra_1 + Ra_2 + \cdots + Ra_n$, for RA. Call RA the **submodule of** M **generated by** A.
If N is a submodule of M (possibly $N = M$) and $N = RA$, for some subset A of M, we call A a **set of generators** or **generating set** for N, and we say N is **generated by** A.

Finite Generation and Cyclic Modules

Definition (Finite Generation and Cyclic Modules)

Let M be an R-module.

(3) A submodule N of M (possibly $N = M$) is **finitely generated** if there is some finite subset A of M such that $N = RA$, that is, if N is generated by some finite subset.

(4) A submodule N of M (possibly $N = M$) is **cyclic** if there exists an element $a \in M$ such that $N = Ra$, that is, if N is generated by one element: $N = Ra = \{ra : r \in R\}$.

- These definitions do not require that the ring R contain a 1; however this condition ensures that A is contained in RA.
- Using the Submodule Criterion, we see that for any subset A of M, RA is indeed a submodule of M.
- RA is the smallest submodule of M which contains A (i.e., any submodule of M which contains A also contains RA).

Finite Generation and Minimal Generating Sets

- For submodules $N_1, \ldots, N_n$ of M, $N_1 + \cdots + N_n$ is the submodule generated by the set $N_1 \cup \cdots \cup N_n$.

  It is the smallest submodule of M containing N_i, for all i.
- If $N_1, \ldots, N_n$ are generated by sets $A_1, \ldots, A_n$, respectively, then $N_1 + \cdots + N_n$ is generated by $A_1 \cup \cdots \cup A_n$.
- A submodule N of an R-module M may have many different generating sets.
- If N is finitely generated, then there is a smallest nonnegative integer d, such that N is generated by d elements (and no fewer).

  Any generating set consisting of d elements will be called a **minimal set of generators** for N (it is not unique in general).
- If N is not finitely generated, it need not have a minimal generating set.

The Case of $\mathbb{Z}$-Modules (Abelian Groups)

(1) Let $R = \mathbb{Z}$ and let M be any R-module, i.e., any abelian group.

If $a \in M$, then $\mathbb{Z}a$ is just the cyclic subgroup of M generated by a: (a).

More generally, M is generated as a $\mathbb{Z}$-module by a set A if and only if M is generated as a group by A (the action of ring elements in this instance produces no elements that cannot already be obtained from A by addition and subtraction).

- The definition of "finitely generated" for $\mathbb{Z}$-modules is identical to that for abelian groups.

A Ring R Viewed as an R-Module

(2) Let R be a ring with 1 and let M be the (left) R-module R itself.

R is a finitely generated, in fact cyclic, R-module because $R = R1$.

The submodules of R are precisely the left ideals of R.

- Saying I is a cyclic R-submodule of the left R-module R is the same as saying I is a principal ideal of R.
- Saying I is a finitely generated R-submodule of R is the same as saying I is a finitely generated ideal.

When R is a commutative ring we often write AR or aR for the submodule (ideal) generated by A or a respectively (e.g., $n\mathbb{Z}$).

In this situation $AR = RA$ and $aR = Ra$ (element-wise as well).

According to this view, a Principal Ideal Domain is a (commutative) integral domain R with identity in which every R-submodule of R is cyclic.

Remark on Finite Generation

- Submodules of a finitely generated module need not be finitely generated.

  Example: Take M to be the cyclic R-module R itself, where R is the polynomial ring in infinitely many variables $x_1, x_2, x_3, \ldots$ with coefficients in some field F.

  The submodule (i.e., 2-sided ideal) generated by $\{x_1, x_2, \ldots\}$ cannot be generated by any finite set.

Free Module of Rank n Over R

(3) Let R be a ring with 1 and let M be the free module of rank n over R. For each $i \in \{1, 2, \ldots, n\}$, let $e_i = (0, 0, \ldots, 0, 1, 0, \ldots, 0)$, where the 1 appears in position i. Since

$$(s_1, s_2, \ldots, s_n) = \sum_{i=1}^{n} s_i e_i$$

it is clear that M is generated by $\{e_1, \ldots, e_n\}$. If R is commutative, then this is a minimal generating set.

$F[x]$-Modules

(4) Let F be a field, let x be an indeterminate, let V be a vector space over F and let T be a linear transformation from V to V.

Make V into an $F[x]$-module via T.

Then V is a cyclic $F[x]$-module (with generator v) if and only if

$$V = \{p(x)v : p(x) \in F[x]\},$$

that is, if and only if every element of V can be written as an F-linear combination of elements of the set $\{T^n(v) : n \geq 0\}$.

This in turn is equivalent to saying $\{v, T(v), T^2(v), \ldots\}$ span V as a vector space over F.

$F[x]$-Modules (Cont'd)

(4)

- Suppose T is the identity linear transformation from V to V or the zero linear transformation.
  Then for every $v \in V$ and every $p(x) \in F[x]$, we have $p(x)v = \alpha v,$ for some $\alpha \in F$.
  Thus, if V has dimension > 1, V cannot be a cyclic $F[x]$-module.
- Suppose V is affine n-space and T is the "shift operator".
  Let e_i be the i-th basis vector numbered so that T is defined by

  $$T^k(e_n) = e_{n-k}, \text{ for } 1 \leq k < n.$$

  Thus, V is spanned by the elements $e_n, T(e_n), \ldots, T^{n-1}(e_n)$.
  Hence, V is a cyclic $F[x]$-module with generator e_n.
  For $n > 1$, V is not a cyclic F-module.

Direct Product of Modules

Definition (Direct Product of Modules)

Let $M_1, \ldots, M_k$ be a collection of R-modules. The collection of k-tuples $(m_1, m_2, \ldots, m_k)$, where $m_i \in M_i$, with addition and action of R defined componentwise is called the **direct product** of $M_1, \ldots, M_k$, denoted $M_1 \times \cdots \times M_k$.

- The direct product of a collection of R-modules is again an R-module.
- The direct product of $M_1, \ldots, M_k$ is also referred to as the (**external**) **direct sum** of $M_1, \ldots, M_k$ and denoted $M_1 \oplus \cdots \oplus M_k$.

Properties of Direct Product

Proposition

Let $N_1, N_2, \ldots, N_k$ be submodules of the R-module M. Then the following are equivalent:

(1) The map $\pi : N_1 \times N_2 \times \cdots \times N_k \to N_1 + N_2 + \cdots + N_k$ defined by $\pi(a_1, a_2, \ldots, a_k) = a_1 + a_2 + \cdots + a_k$ is an isomorphism (of R-modules): $N_1 + N_2 + \cdots + N_k \cong N_1 \times N_2 \times \cdots \times N_k$.

(2) $N_j \cap (N_1 + N_2 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = 0$, for all $j \in \{1, 2, \ldots, k\}$.

(3) Every $x \in N_1 + \cdots + N_k$ can be written uniquely in the form $a_1 + a_2 + \cdots + a_k$, with $a_i \in N_i$.

(1)$\Rightarrow$(2): Suppose for some j that (2) fails to hold. Let $a_j \in (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) \cap N_j$ with $a_j \neq 0$. Then $a_j = a_1 + \cdots + a_{j-1} + a_{j+1} + \cdots + a_k$, for some $a_j \in N_j$. Hence, $(a_1, \ldots, a_{j-1}, -a_j, a_{j+1}, \ldots, a_k)$ is a nonzero element of $\ker \pi$, a contradiction.

Properties of Direct Product (Cont'd)

(2)⇒(3): Assume that (2) holds. Suppose for some module elements $a_i, b_i \in N_i$,

$$a_1 + a_2 + \cdots + a_k = b_1 + b_2 + \cdots + b_k.$$

Then, for each j,

$$a_j - b_j = (b_1 - a_1) + \cdots + (b_{j-1} - a_{j-1}) + (b_{j+1} - a_{j+1}) + \cdots + (b_k - a_k).$$

The left hand side is in N_j. The right side belongs to $N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k$. Thus,

$$a_j - b_j \in N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = 0.$$

This shows $a_j = b_j$, for all j. So (2) implies (3).

(3)⇒(1): Observe first that the map π is clearly a surjective R-module homomorphism. (3) implies π is injective. Hence it is an isomorphism.

Internal Direct Sum

- If an R-module $M = N_1 + N_2 + \cdots + N_k$ is the sum of submodules $N_1, N_2, \ldots, N_k$ of M satisfying the equivalent conditions of the proposition above, then M is said to be the (**internal**) **direct sum** of $N_1, N_2, \ldots, N_k$, written $M = N_1 \oplus N_2 \oplus \cdots \oplus N_k$.
- By the proposition, this is equivalent to the assertion that every element m of M can be written uniquely as a sum of elements $m = n_1 + n_2 + \cdots + n_k$, with $n_i \in N_i$.
- Part (1) of the proposition says that the internal direct sum of $N_1, N_2, \ldots, N_k$ is isomorphic to their external direct sum.

Free Modules and Bases

Definition (Free Module, Bases, Rank)

An R-module F is said to be **free** on the subset A of F if, for every nonzero element x of F, there exist unique nonzero elements $r_1, r_2, \ldots, r_n$ of R and unique $a_1, a_2, \ldots, a_n$ in A, such that

$$x = r_1 a_1 + r_2 a_2 + \cdots + r_n a_n,$$

for some $n \in \mathbb{Z}^+$. In this situation we say A is a **basis** or **set of free generators** for F. If R is a commutative ring the cardinality of A is called the **rank** of F.

- One should be careful to note the difference between the uniqueness property of direct sums and the uniqueness property of free modules:
  - In the direct sum of two modules, say $N_1 \oplus N_2$, each element can be written uniquely as $n_1 + n_2$; the uniqueness refers to the module elements n_1 and n_2.
  - In the case of free modules, the uniqueness is on the ring elements as well as the module elements.

Examples on Free Modules

- Suppose $R = \mathbb{Z}$ and let $N_1 = N_2 = \mathbb{Z}/2\mathbb{Z}$.

  Each element of $N_1 \oplus N_2$ has a unique representation in the form $n_1 + n_2$, where each $n_i \in N_i$.

  However, n_1 (for instance) can be expressed as n_1 or $3n_1$ or $5n_1$, etc.

  So each element does not have a unique representation in the form $r_1 a_1 + r_2 a_2$, where $r_1, r_2 \in R$, $a_1 \in N_1$ and $a_2 \in N_2$.

  Thus, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is not a free $\mathbb{Z}$-module on the set $\{(1,0),(0,1)\}$.

  Similarly, it is not free on any set.

Universal Property of Free Modules

Theorem

For any set A, there is a free R-module $F(A)$ on the set A and $F(A)$ satisfies the following universal property:
If M is any R-module and $\varphi : A \to M$ is any map of sets, then there is a unique R-module homomorphism $\Phi : F(A) \to M$, such that $\Phi(a) = \varphi(a)$, for all $a \in A$, i.e., the following diagram commutes:

$$\begin{tikzcd} A \arrow[r, "\text{inclusion}"] \arrow[dr, "\varphi"'] & F(A) \arrow[d, "\Phi"] \\ & M \end{tikzcd}$$

When $A = \{a_1, a_2, \ldots, a_n\}$, $F(A) = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n \cong R^n$.

- Let $F(A) = \{0\}$ if $A = \emptyset$. If A is nonempty, let $F(A)$ be the collection of all set functions $f : A \to R$, such that $f(a) = 0$, for all but finitely many $a \in A$. Make $F(A)$ into an R-module by pointwise operations:

$$\begin{array}{rcl} (f+g)(a) & = & f(a) + g(a), \quad f, g \in F(A), a \in A; \\ (rf)(a) & = & r(f(a)), \quad f \in F(A), r \in R, a \in A. \end{array}$$

All the R-module axioms hold.

Universal Property of Free Modules (Inclusion)

- Identify A as a subset of $F(A)$ by

$$a \mapsto f_a,$$

where $f_a(x) = \begin{cases} 1, & \text{if } x = a \\ 0, & \text{if } x \neq a \end{cases}$, for all $x \in A$.

We can, in this way, think of $F(A)$ as all finite R-linear combinations of elements of A: Let $f \in F(A)$, such that

$$f(a_i) = r_i,\ i = 1, \ldots, n, \quad \text{and} \quad f(a) = 0,\ a \neq a_i, i = 1, \ldots, n.$$

Then

$$f = r_1 f_{a_1} + r_2 f_{a_2} + \cdots + r_n f_{a_n}.$$

Moreover, each element of $F(A)$ has a unique expression as such a formal sum.

Universal Property of Free Modules (From φ to Φ)

- To establish the universal property of $F(A)$, suppose $\varphi : A \to M$ is a map of the set A into the R-module M.

$$\begin{tikzcd} A \arrow[r, "\text{inclusion}"] \arrow[dr, "\varphi"'] & F(A) \arrow[d, "\Phi"] \\ & M \end{tikzcd}$$

  Define $\Phi : F(A) \to M$ by $\Phi : \sum_{i=1}^{n} r_i f_{a_i} \mapsto \sum_{i=1}^{n} r_i \varphi(a_i)$.
  - By the uniqueness of the expression for the elements of $F(A)$ as linear combinations of the f_{a_i} we see that Φ is a well defined R-module homomorphism.
  - By definition, the restriction of Φ to $\{f_a : a \in A\}$ equals φ.
  - $F(A)$ is generated by $\{f_a : a \in A\}$. Hence, once we know the values of an R-module homomorphism on $\{f_a : a \in A\}$, its values on every element of $F(A)$ are uniquely determined.

  So $\Phi : F(A) \to M$ is the unique R-module homomorphism, such that $\Phi(f_a) = \varphi(a)$. for all $a \in A$.

Finitely Generated Free Modules

- When A is the finite set $\{a_1, a_2, \ldots, a_n\}$, the proposition shows that $F(A) = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n$. Since $R \cong Ra_i$, for all i (under the map $r \mapsto ra_i$) the direct sum is isomorphic to R^n.

Corollary

(1) If F_1 and F_2 are free modules on the same set A, there is a unique isomorphism between F_1 and F_2 which is the identity map on A.

(2) If F is any free R-module with basis A, then $F \cong F(A)$. In particular, F enjoys the same universal property with respect to A as $F(A)$ does.

- If F is a free R-module with basis A, we often define R-module homomorphisms from F into other R-modules by specifying their values on the elements of A and then saying "extend by linearity".
- When $R = \mathbb{Z}$, the free module on a set A is called the **free abelian group** on A. If $|A| = n$, $F(A)$ is called the free abelian group of **rank** n and is isomorphic to $\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ (n times).