Let R be a ring.

A (left) R**-module** is an abelian group $(M, +)$ with an R-action

$$R \times M \longrightarrow M,$$
$$(r, m) \longmapsto r \cdot m$$

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

(1) a binary operation $+$, under which M is an abelian group, and
(2) an R-action on M (i.e., a map $R \times M \to M$) denoted by rm for all $r \in R$ and $m \in M$ which satisfies
   (i) $(r + s)m = rm + sm$,
   (ii) $(rs)m = r(sm)$,
   (iii) $r(m + n) = rm + rn$,
   (iv) if $1 \in R$, then $1m = m$.

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

Ring	Group	Module	Submodules	Homomorphisms
R	$(R, +)$	mul. in R	Ideals of R	-
$\mathbb{Z}$	G Abelian	group operation	Subgroups of G	Group Homs
F Field	V an F-v.s.	scalar mul.	lin. subspaces of	lin. trans.
$F[x]$	V an F-v.s.	via $\theta \in \mathrm{End}_F(V)$	θ-invariant subspaces	-

---

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

A map $\varphi : M \to N$ is an R**-module homomorphism** if it respects the R-module structure of M and N, i.e., for all $x, y \in M$ and $r \in R$ the map satisfies

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

If φ is also a bijection, it is called an **isomorphism** (of R-modules), and the R-modules M and N are said to be **isomorphic**, denoted $M \cong N$.

The **kernel** of φ is the set

$$\ker \varphi = \{m \in M \mid \varphi(m) = 0\}.$$

The **image** of φ is the set

$$\varphi(M) = \{\varphi(m) \mid m \in M\}.$$

Define $\mathrm{Hom}_R(M,N)$ to be the set of all R-module homomorphisms from M to N.

For $\varphi, \psi \in \mathrm{Hom}_R(M,N)$, define $\varphi + \psi$ by

$$(\varphi+\psi)(m) = \varphi(m) + \psi(m), \qquad \text{for all } m \in M.$$

Then $\varphi + \psi \in \mathrm{Hom}_R(M,N)$ and under this operation, $\mathrm{Hom}_R(M,N)$ is an abelian group.

If R is commutative, then for $r \in R$ define $r\varphi$ by

$$(r\varphi)(m) = r(\varphi(m)), \qquad \text{for all } m \in M.$$

Then $r\varphi \in \mathrm{Hom}_R(M,N)$ and under this action, $\mathrm{Hom}_R(M,N)$ is an R-module.

With addition as above and taking composition as multiplication, $\mathrm{Hom}_R(M,M)$ is a ring with identity. We call this ring the **endomorphism ring** of M and denote it by $\mathrm{End}_R(M)$; its elements are called **endomorphisms**.

Let M be an R-module and N be an R-submodule of M. Then the quotient group

$$M/N = \{\overline{x} = x + N \mid x \in M\}$$

can be made into an R-module with the R-action defined by $r\overline{x} = \overline{rx}$, where rx is determined by the R-action on M. This is called the **quotient R-module of M by N** and the natural projection $\pi : M \to M/N$ is an R-module homomorphism, with $\ker \pi = N$.

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

The **sum** of $N_1, \ldots, N_n$ is the set of all finite sums of elements from the sets, denoted by

$$N_1 + \cdots + N_n = \{a_1 + \cdots + a_n \mid a_j \in N_j\}.$$

For any $A \subseteq M$ define the **R-submodule of M generated by A** to be

$$RA = \{r_1a_1 + \cdots + r_ka_k \mid r_j \in R,\ a_j \in A,\ k \in \mathbb{Z}^+\}.$$

If A is the finite set $\{a_1, \ldots, a_n\}$, write $Ra_1 + \cdots + Ra_n$ for RA. If $A = \varnothing$, take $RA = \{0\}$.

If N is an R-submodule of M and $N = RA$ for some $A \subseteq M$, we call A a **generating set** for N, and say N is **generated** by A.

We say N is **finitely generated** if it is generated by a finite subset of M, i.e., if $N = RA$ for some finite subset A of M.

An R-submodule N of M is **cyclic** if it is generated by a single element of M, i.e., if

$$N = Ra = \{ra \mid r \in R\}$$

for some $a \in M$.

If $N_1, \ldots, N_n$ are R-submodules of M which are generated by the subsets $A_1, \ldots, A_n$ of M, then the sum $N_1 + \cdots + N_n$ is generated by $A_1 \cup \cdots \cup A_n$.

If $M = Rx_1 + \cdots + Rx_n$, i.e., M is generated by the set $\{x_1, \ldots, x_n\}$, and N is an R-submodule of M, then $M/N = R\overline{x_1} + \cdots + R\overline{x_n}$.

Let $M_1, \ldots M_n$ be a collection of R-modules. The **direct product** of $M_1, \ldots, M_n$ is the R-module

$$M_1 \times \cdots \times M_n = \{(x_1, \ldots, x_n) \mid x_j \in M_j\},$$

with addition defined by

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

and R-action defined by

$$r(x_1, \ldots, x_n) = (rx_1, \ldots, rx_n).$$

Also referred to as the (external) **direct sum** and denoted $M_1 \oplus \cdots \oplus M_n$.

Let R be a ring with identity.

And R-module M is said to the **free** on the subset $A \subseteq M$ if, for every nonzero element $x \in M$, there exist unique nonzero elements $r_1, \ldots, r_n \in R$ and unique $a_1, \ldots, a_n \in A$ such that $x = r_1a_1 + \cdots + r_na_n$, for some $n \in \mathbb{Z}^+$. Equivalently, M is free on A if

(i) every $x \in M$ can be written as a finite sum $x = r_1a_1 + \cdots + r_na_n$ for some $a_1, \ldots, a_n \in A$ and $r_1, \ldots, r_n \in R$, and
(ii) for all $r_1, \ldots, r_n \in R$ and distinct $a_1, \ldots, a_n \in A$,

$$r_1a_1 + \cdots + r_na_n = 0 \implies r_1 = \cdots = r_n = 0.$$

In this case, we say A is a **basis** or a set of **free generators** for M. And if R is commutative, then the cardinality of A is called the **rank** of M.

Let M be an R-module.

Define

$$\mathrm{Tor}_R(M) = \{x \in M \mid rx = 0 \text{ for some nonzero } r \in R\}.$$

When R is an integral domain, $\mathrm{Tor}_R(M)$ is called the **torsion R-submodule** of M.

If $\mathrm{Tor}_R(M) = 0$, then M is said to be **torsion free**.

For any R-submodule N of M, the **annihilator** of N is the ideal of R defined by

$$\mathrm{Ann}_R(N) = \{r \in R \mid rx = 0 \text{ for all } x \in N\}.$$

If N is not a torsion R-submodule of M then $\mathrm{Ann}_R(N) = (0)$

Proposition 1. (Submodule Criterion) Let R be a ring with identity. A subset N of an R-module M is an R-submodule of M if and only if

(i) $N \neq \varnothing$,
(ii) $x + ry \in N$ for all $r \in R$ and $x, y \in N$.

Proposition 2. Let R be a ring with identity and let M and N be R-modules. A map $\varphi : M \to N$ is an R-module homomorphism if and only if

$$\varphi(rx + y) = r\varphi(x) + \varphi(y), \qquad \text{for all } x, y \in M,\ r \in R.$$

Theorem 1. (Isomorphism Theorems)

(1) Let M and 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) Let A and B be R-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 R-submodules of M with $A \subseteq B$. Then $(M/A)/(B/A) \cong M/B$.
(4) Let N be an R-submodule of the R-module M and $\pi : M \to M/N$ be the natural projection. Then the map

$$\begin{aligned} \{R\text{-submodules of } M \text{ containing } N\} &\to \{R\text{-submodules of } M/N\} \\ A &\mapsto \overline{A} = A/N \end{aligned}$$

is a bijection and its inverse map is

$$\begin{aligned} \{R\text{-submodules of } M/N\} &\to \{R\text{-submodules of } M \text{ containing } N\} \\ \overline{A} &\mapsto \pi^{-1}(\overline{A}) = \{x \in M \mid \overline{x} \in \overline{A}\}. \end{aligned}$$

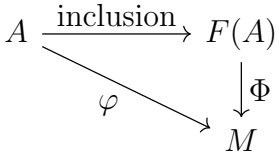
Proposition 3. Let $N_1, \ldots, N_k$ be R-submodules of the R-module N. Then the following are equivalent:

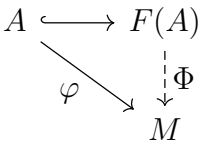
(1) The map

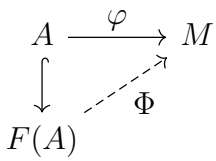
$$\begin{aligned} \pi : N_1 \times \cdots \times N_k &\to M \\ (a_1, \ldots, a_k) &\mapsto a_1 + \cdots + a_k \end{aligned}$$

is an isomorphism of R-modules.
(2) $N_1 + \cdots + N_k = M$ and $N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = 0$.
(3) Every $x \in M$ can be written uniquely in the form $x = a_1 + \cdots + a_k$ with $a_j \in N_j$.

Theorem 2. For any set A there exists a free R-module $F(A)$ on A, satisfying 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:







When A is the finite set $\{a_1, \ldots, a_n\}$, $F(A) = Ra_1 \oplus \cdots \oplus Ra_n \cong R^n$.

Corollary 1. If M_1 and M_2 are free modules on the same set A, there is a unique isomorphism between M_1 and M_2 which is the identity on A.

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

Theorem 3. (Fundamental Theorem of Finitely Generated Modules over PID's) Let R be a PID and let M be a finitely generated R-module.

(1) (Invariant Factor Form)

$$M \cong R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$$

for some $r \in \mathbb{Z}_{\geq 0}$ and nonzero non-unit $a_1, \ldots, a_m \in R$ satisfying $a_j \mid a_{j+1}$. The integer r is uniquely determined by M and the elements $a_1, \ldots, a_m$ are uniquely determined up to units by M.

(2) (Elementary Divisor Form)

$$M \cong R^r \oplus R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_k^{\alpha_k})$$

for some $r \in \mathbb{Z}_{\geq 0}$ (same as in (1)) and nonzero prime $p_1, \ldots, p_k \in R$ (not necessarily distinct) and $\alpha_1, \ldots, \alpha_k \in \mathbb{Z}^+$. The integer r is uniquely determined by M and the elements $p_1, \ldots, p_k$ are uniquely determined up to units by M.

We call r the **free rank** of M, the elements $a_1, \ldots, a_m$ the **invariant factors** of M, and the elements $p_1, \ldots, p_k$ the **elementary divisors** of M.

Examples

1. Any ring R is naturally an R-module under the action of multiplication . If R is commutative, any subset is an R-submodule if and only if it is an ideal.
2. Let M be an R-module and I be an ideal of R. Then the set

$$IM = \{a_1m_1 + \cdots + a_nm_n \mid a_j \in I,\ m_j \in M,\ n \in \mathbb{Z}^+\}$$

   is an R-submodule of M.
3. If $\varphi : R \to S$ is a ring homomorphism and M is an S-module, then M is also an R-module with the R-action $rm = \varphi(r)m$, where $\varphi(r)$ acts on m under the S-action. In particular, if I is an ideal of R, then any (R/I)-module is an R-module, where the R-action is obtained from the (R/I)-action using the natural projection.
4. An abelian group $(A, +)$ is naturally a $\mathbb{Z}$-module with the action defined inductively for $n \in \mathbb{Z}$ and $a \in A$ by

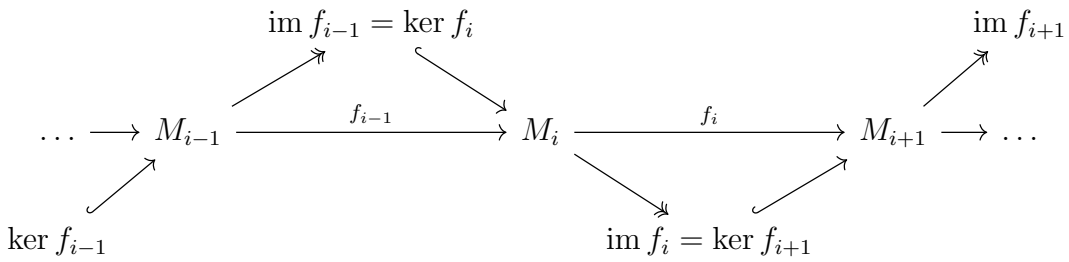
$$\begin{aligned} 0a &= 0 \\ (n+1)a &= na + a, \quad n \geq 0 \\ -1a &= -a. \end{aligned}$$

   In other words, the action of an integer on an element of the group is repeated addition, with negative integers giving the additive inverse in the group. If the binary operation of the group is written multiplicatively, then the $\mathbb{Z}$-action can be written as a^n, and follows the usual laws of exponents. In fact, this is the only $\mathbb{Z}$-module structure than can be put on A, and any $\mathbb{Z}$-module admits an abelian group. So $\mathbb{Z}$-module are the same as abelian groups, with submodules being the subgroups.
5. For a field F, the axioms of an F-module are precisely the axiom of a vector space over F, i.e., F-modules and vector spaces over F are the same. Let V be a vector space over F and let $T : V \to V$ be a linear transformation. Then V can be viewed as an $F[x]$-module under the $F[x]$-action

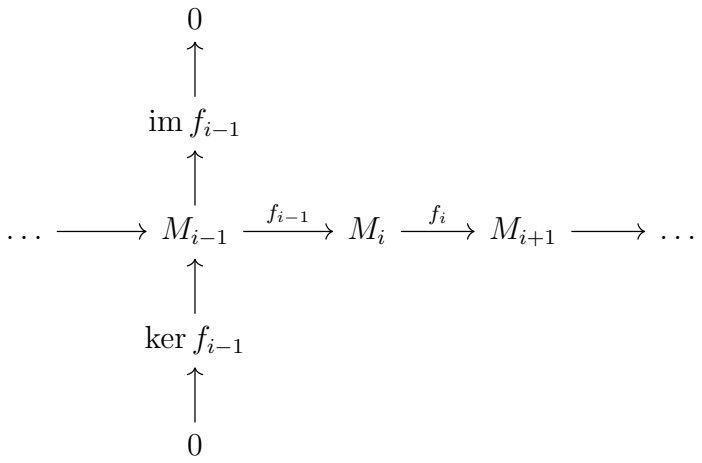
$$(a_nx^n + \cdots a_1x + a_0)v = (a_nT^n + \cdots a_1T + a_0)v = a_nT^n(v) + \cdots a_1T(v) + a_0v.$$

   This $F[x]$ action agrees with the natural F-action for elements of F. In fact there is a bijective correspondence between $F[x]$-modules and linear operators on vectors spaces over F. The $F[x]$-submodules are the subspaces of the vector space which are stable under the linear operator.

exact sequences



sploogl



Let F be a field and denote by $\mathrm{M}_{n\times n}(F)$ the set of $n \times n$ matrices with entries in F.

Define the **general linear group** of degree n over F to be the set

$$\mathrm{GL}_n(F) = \{A \in \mathrm{M}_{n\times n}(F) \mid \det A \neq 0\},$$

which is a group under the usual matrix multiplication.

Let $A \in \mathrm{M}_{n\times n}(F)$.

The **characteristic polynomial** of a A is

$$c_A(x) = \det(xI - A).$$

Note that $c_{P^{-1}AP}(x) = c_A(x)$ for all $P \in \mathrm{GL}_n(F)$.

A monic polynomial $m_A(x) \in F[x]$ is called the **minimal polynomial** of A if

(i) $m_A(A) = 0$,
(ii) $p(A) = 0$ implies $m_A(x) \mid p(x)$, for all $p(x) \in F[x]$.

Let V be a vector space of dimension n over the field F. Let $T : V \to V$ be a linear transformation and fix a basis $\beta = \{e_1, \ldots, e_n\}$ of V.

Then T corresponds to a matrix $A_T \in \mathrm{M}_{n\times n}(F)$ such that $T(v) = A_T[v]_\beta$ for all $v \in V$, where $[v]_\beta$ is the $n \times 1$ vector of the coordinates of v in the basis β.

The characteristic polynomial of T is defined as $c_T(x) = c_{A_T}(x)$.

The minimal polynomial of T is defined as $m_T(x) = m_{A_T}(x)$.

Both $c_T(x)$ and $m_T(x)$ are independent of the choice of basis β.

Let F be a field and $A \in \mathrm{M}_{n\times n}(F)$. Let $V = F^n$ be equipped with the $F[x]$-module structure induced by the linear transformation

$$\begin{aligned} T_A : V &\to V \\ v &\mapsto Av. \end{aligned}$$

Since $F[x]$ is a PID, then the fundamental theorem of finitely generated modules over PID's implies (after checking that free rank of V is zero) that

$$V \cong F[x]/(a_1(x)) \oplus \cdots \oplus F[x]/(a_m(x)),$$

where each $a_j(x)$ is a monic polynomial in $F[x]$ with $\deg a_j(x) \geq 1$ and $a_j(x) \mid a_{j+1}(x)$. And

$$V \cong F[x]/(p_1(x)^{\alpha_1}) \oplus \cdots \oplus F[x]/(p_k(x)^{\alpha_k}),$$

where each $p_j(x)$ is a monic, irreducible polynomial in $F[x]$ and $\alpha_j \in \mathbb{Z}_{\geq 0}$.

We call $a_1(x), \ldots, a_m(x)$ the invariant factors of A and $p_1(x), \ldots, p_k(x)$ the elementary divisors of A.

Let F be a field. Let $k \in \mathbb{Z}^+$ and $\lambda \in F$.

The $k \times k$ **elementary Jordan matrix** with eigenvalue λ, or the **Jordan block** of size k with eigenvalue λ, is the matrix

$$\begin{bmatrix} \lambda & 1 & & 0 \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{bmatrix} \in \mathrm{M}_{k\times k}(F).$$

A matrix is said to be in **Jordan canonical form** if is has the shape

$$\begin{bmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_t \end{bmatrix}$$

where each J_i is a Jordan block.

Proposition 4. Let F be a field, $A \in \mathrm{M}_{n\times n}(F)$, and $a_1(x), \ldots, a_m(x)$ be the invariant factors of A.

(1) $m_A(x) = a_m(x)$
(2) $c_A(x) = a_1(x) \cdots a_m(x)$
(3) (Cayley-Hamilton) $c_A(A) = 0$

Theorem 4. Let F be a field and $A \in \mathrm{M}_{n\times n}(F)$. Suppose that $c_A(x)$ factorizes into a product of degree one polynomials in $F[x]$ (not necessarily distinct). (If $F = \mathbb{C}$, then this condition is always satisfied.)

(1) A is similar to a matrix in Jordan canonical form, i.e., there exists $P \in \mathrm{GL}_n(F)$ such that

$$P^{-1}AP = \begin{bmatrix} J_1 & & \\ & \ddots & \\ & & J_t \end{bmatrix}$$

where each J_i is a Jordan block.

(2) The Jordan block form of A is unique up to a permutation of the Jordan blocks. More precisely, under the assumption on $c_A(x)$, the elementary divisors of A are

$$(x-\lambda_1)^{\alpha_1}, \ldots, (x-\lambda_k)^{\alpha_k},$$

where $\lambda_1, \ldots, \lambda_k \in F$ (not necessarily distinct). The Jordan canonical form of A has k Jordan blocks, which are of sizes $\alpha_1, \ldots, \alpha_k$ and eigenvalues $\lambda_1, \ldots, \lambda_k$.