Finitely Generated Modules Over PID

Yuze Fu

March 26, 2026

Field Scalar v.s. Ring Scalar

Given a n-dimensional F-vector space V, we have the classification:

$$V \cong F^n$$

What about "R-vector space"? Are there similar classifications?

Modules

Modules are the general version of vector spaces whose scalars only need to be **rings** instead of fields.

Definition

Let R be a non-zero commutative ring. A **R-module** or a *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
   1. $(r+s)m = rm + sm$, for all $r, s \in R$, $m \in M$,
   2. $(rs)m = r(sm)$, for all $r, s \in R$, $m \in M$,
   3. $r(m+n) = rm + rn$, for all $r \in R$, $m, n \in M$, and
   4. $1m = m$, for all $m \in M$

$\mathbb{Z}$-modules

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

Let A be an abelian group and write the operation of A as $+$. Consider $R = \mathbb{Z}$, and define the action of $\mathbb{Z}$ on A: for all $n \in \mathbb{Z}, a \in A$

$$na = \begin{cases} a + a + \cdots + a \ (n \text{ times}) & \text{if } n \in \mathbb{Z}^+ \\ 0 \ (\text{the identity element of } A) & \text{if } n = 0 \\ -a - a - \cdots - a \ (-n \text{ times}) & \text{if } n \in \mathbb{Z}^- \end{cases}$$

This satisfies axiom (2), making A into a $\mathbb{Z}$-module. By axioms of modules, this action is the only possible one (which can proven by contradiction). So, there is a bijection between the set of abelian groups and the set of $\mathbb{Z}$-modules. More precisely,

$$\{A \text{ an } \mathbb{Z}\text{-module}\} \longleftrightarrow \{A \text{ an abelian group}\}$$

$F[X]$-modules

Example ($F[X]$-modules)

Given a finitely dimensional F-vector space V and a linear transformation T. Consider $R = F[X]$ the polynomial ring and define the action of $p(X) \in F[X]$ on V:

$$X \cdot v = T(v)$$

for any $v \in V$. In general, let $p(X) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ where $a_0, \cdots, a_n \in F$. For each $v \in V$, the action is

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

By this definition, we can consider $p(X)$ as a linear transformation. Then, by properties of linear transformation, the axioms of module are easy to prove.

→ Cont.

$F[X]$-modules

Example (Cont.)

Given an $F[X]$-module V, V is an F-module by restricting the polynomial into constants. Also, we can deduce the linear transformation T by the action of $X \in F[X]$ on V which is $T(v) = X \cdot v$. Clearly, given an F-vector space V and a linear transformation T, we can get a unique $F[X]$-module V. So, there exists a bijection:

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

Finitely Generated Modules and PID

Definition

Let M be an R-module. M is **finitely generated** if and only if there is some finite subset A of M such that $M = RA$, where $RA = \{r_1a_1 + r_2a_2 + \cdots + r_ma_m \mid r_1, \cdots, r_m \in R, a_1, \cdots, a_m \in A, m \in \mathbb{Z}^+\}$.

Goal

1. Classify finitely-generated modules over PID
2. Apply on $\mathbb{Z}$-modules
3. Apply on $F[X]$-modules

Classification

Theorem (Fundamental Theorem: Invariant Factor Form)

Let R be a P.I.D. and let M be a finitely generated R-module.

Then M is is isomorphic to the direct sum of finitely many cyclic modules. More precisely,

$$M \cong R^r \oplus \underbrace{R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)}_{Tor(M)}$$

for some integer $r \geq 0$ and nonzero elements $a_1, a_2, \cdots, a_m$ of R which are not units in R and which satisfy the divisibility relations

$$a_1 \mid a_2 \mid \cdots \mid a_m.$$

They are called the **invariant factors** *of M which is* **unique up to unit multiplication**.

Classification

For each $R/(a)$, by Chinese Remaindrer Theorem

$$R/(a) \cong R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_s^{\alpha_s})$$

where $a = up_1^{\alpha_1} \cdots p_s^{\alpha_s}$.

Theorem (Fundamental Theorem: Elementary Divisor Form)

Let R be a P.I.D. and let M be a finitely generated R-module. Then

$$M \cong R^r \oplus R/(p_1^{\alpha_1}) \oplus R/(p_2^{\alpha_2}) \oplus \cdots \oplus R/(p_t^{\alpha_t})$$

for a unique integer $r \geq 0$ and a (possibly empty) list of (possibly repeated) prime powers $p_1^{\alpha_1}, \cdots, p_t^{\alpha_t}$, **unique up to rearrangement**. *The list of prime powers is called the* **elementary divisors** *of M.*

Application on $\mathbb{Z}$-modules

Given a finitely-generated abelian group G, which is also an finitely-generated $\mathbb{Z}$-module ($\mathbb{Z}$ is a PID). By **Elementary Divisor Form**,

$$G \cong \mathbb{Z}^n \oplus \mathbb{Z}/(p_1^{k_1}) \oplus \mathbb{Z}/(p_2^{k_2}) \oplus \cdots \oplus \mathbb{Z}/(p_t^{k_s})$$

Only pick the addition part and the direct sum changes to direct product:

Corollary (Classification of Finitely Generated Abelian Group)

If G is a finitely generated abelian group, then

$$G \cong \mathbb{Z}^n \times \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_s^{k_s}}$$

for a unique integer $n \geq 0$ and a (possibly empty) list of (possibly repeated) prime powers $p_1^{k_1}, \cdots, p_t^{k_s}$, unique up to rearrangement.

Note: direct sum is only equivalent to direct product when there are finite many terms.

Applications on $F[X]$-modules (RCF)

Given a finitely dimensional F-vector space V and a linear transformation T on V. We know V is a $F[X]$-module and $F[X]$ is a PID. By **Invariant Factor Form**,

$$V \cong F[X]/(a_1(x)) \oplus F[X]/(a_2(x)) \oplus \cdots \oplus F[X]/(a_m(x))$$

where $a_1, \cdots, a_m$ is monic.
For each $F[X]/a(x)$ where $a(x)) = x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$, $\mathcal{B} = \{1, x, \cdots, x^{k-2}, x^{k-1}\}$ is a basis. With the action $T(v) = x \cdot v$,

$$\begin{aligned} T : F[X]/(a(x)) &\to F[X]/(a(x)) \\ 1 &\mapsto x \\ x &\mapsto x^2 \\ &\vdots \\ x^{k-2} &\mapsto x^{k-1} \\ x^{k-1} &\mapsto x^k \equiv -b_0 - b_1 x - \cdots - b_{k-1}x^{k-1} \mod a(x) \end{aligned}$$

→ Cont

Applications on $F[X]$-modules (RCF)

With respect to basis $\mathcal{B}$, the matrix for $T : F[X]/(a(x)) \to F[X]/(a(x))$ is

$$\begin{pmatrix} 0 & 0 & \cdots & \cdots & -b_0 \\ 1 & 0 & \cdots & \cdots & -b_1 \\ 0 & 1 & \cdots & \cdots & -b_2 \\ \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -b_{k-1} \end{pmatrix}$$

Such matrix is called **companion matrix**, denoted as $\mathcal{C}_{a(x)}$. Since each $F[X]/(a_i(x))$ is connected by direct sum, the matrix for $T : V \to V$ is

$$\begin{pmatrix} \mathcal{C}_{a_1(x)} & & & \\ & \mathcal{C}_{a_2(x)} & & \\ & & \ddots & \\ & & & \mathcal{C}_{a_m(x)} \end{pmatrix}$$

Such matrix is called the **rational canonical form**.

Applications on $F[X]$-modules (Comparison)

Feature	**Rational Canonical (RCF)**	**Jordan Canonical (JCF)**
Field	Any field F	Algebraically closed (e.g., $\mathbb{C}$)
Structure	Invariant Factors $a_i(x)$	Elementary Divisors $(x-\lambda_i)^k$
Blocks	Companion Matrices $C(a_i)$	Jordan Blocks $J_k(\lambda_i)$
Decomposition	$V \cong \bigoplus F[x]/(a_i(x))$	$V \cong \bigoplus F[x]/(x-\lambda_i)^k$
Insight	Minimal Polynomial	Eigenvalues/Multiplicity

References

Dummit, D. S., & Foote, R. M. (2004).
Abstract Algebra (3rd ed.).
John Wiley & Sons.
http://www.loc.gov/catdir/description/wiley039/2003057652.html