FINITELY GENERATED MODULES OVER PRINCIPAL IDEAL DOMAINS

YUZE FU

Abstract. This essay explores the classification of finitely generated modules over Principal Ideal Domains (PIDs) and its profound implications for linear algebra. By establishing the Fundamental Theorem of Finitely Generated Modules in both its Invariant Factor and Elementary Divisor forms, we provide a unified framework for understanding the structure of abelian groups and linear transformations. Specifically, we demonstrate how the choice of decomposition leads to the construction of the Rational Canonical Form and the Jordan Canonical Form for a linear operator on a finite-dimensional vector space.

Theorem 0.1. *Let F be a field and let V be a n-dimensional F-vector space. Then, there is an isomorphism:*

$$V \cong F^n$$

This linear algebra theorem demonstrates the structure of every finite-dimensional vector space. However, this structure no longer holds if we generalize the scalar from a field F into a ring R. In this essay, our goal is to classify this new algebraic structure, **module**.

1. Introduction to Modules

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

Definition 1.1. 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
   (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 $r \in R$, $m, n \in M$, and
   (d) $1m = m$, for all $m \in M$

Remark 1.2. Specifically, this is the definition for left R-module where R contains 1 and is commutative over multiplication. The essay used this as the definition of R-modules.

Two fundamental examples of rings are $\mathbb{Z}$ and $F[X]$. We will construct the module action over each of them:

Date: April 3, 2026.

Example 1.3 ($\mathbb{Z}$-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,

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

Example 1.4 ($F[X]$-modules). Let V be a vector space over a field F, and let T be a linear transformation from V to V. We first clarify two conventions:

$$T^n = \begin{cases} I & \text{, if } n = 0 \\ \underbrace{T \circ \cdots \circ T}_{n \text{ times}} & \text{, if } n \in \mathbb{Z}^+ \end{cases}$$

We know that the composition of linear transformation is still linear transformation. So, T^n is a linear transformation for any nonnegative integer n. Also, for any two linear transformations A, B from V to V and elements $\alpha, \beta \in F$, we have

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

for any $v \in V$. Since $\alpha A + \beta B$ is a linear combination of linear transformation, it is also a linear transformation.

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 A. Then, by properties of linear transformation, the axioms of module are easy to prove.

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 $Xv = T(v)$. 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:

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

Recall Theorem 0.1, we are interested in finitely-generated algebraic structure. Similar to finite-dimensional vector space, the definition of finitely-generated modules is as following:

Definition 1.5. 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 $RA = \{r_1a_1 + r_2a_2 + \cdots + r_ma_m \mid r_1, \cdots, r_m \in R, a_1, \cdots, a_m \in A, m \in \mathbb{Z}^+\}$.

Other than "finitely-generated", we also restrict the ring R to be **Principal Ideal Domain (PID)**. Then, it is sufficient to show the fundamental theorem.

2. The Basic Theory

Theorem 2.1 (Fundamental Theorem: Invariant Factor Form)**.** *Let R be a PID and let M be a finitely generated R-module. Then M 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**.*

By Chinese Remainder Theorem, we can decompose the quotient rings more by prime factoring the invariant factors. Then, the following version is derived:

Theorem 2.2 (Fundamental Theorem: Elementary Divisor Form)**.** *Let R be a PID 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.*

Proof. First, by Theorem 2.1, we can get a unique isomorphic direct sum of M and the corresponding invariant factors. For each invariant factor a, we can write

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

where u is a unit, p_i's are distinct irreducible elements in R and α_i's are positive integers.

Since R is a Unique Factorization Domain (R is PID), the decomposition is unique up to units. Now, consider $(p_i^{\alpha_i})$. Since R is PID, $(p_i^{\alpha_i})$ are maximal ideals. Any two distinct maximal ideals in R are coprime. In particular, $(p_i^{\alpha_i}) + (p_j^{\alpha_j}) = R$. By Chinese Remainder Theorem,

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

By applying this on every term, we get the desired form. □

This version can be restricted into the context of groups, inducing the following classification:

Corollary 2.3 (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.

Proof. Let G be an arbitrary finitely generated abelian group. By Example 1.3, G is the same as a $\mathbb{Z}$-module M. Since G is finitely generated, so as M. Also, $\mathbb{Z}$ is a PID Then, by Theorem 2.2, we have

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

unique up to rearrangement. We can now take out the addition part from the quotient rings, and we can get $\mathbb{Z}_{p_i^{k_i}}$. Also, we can change direct sum and direct product with each other in finite cases (ie. $n + s < \infty$). Therefore, we can get

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

unique up to rearrangement. □

3. Canonical Forms

We have applied the fundamental theorem on $\mathbb{Z}$-modules (Example 1.3). We can now implement it with respect to $F[X]$-modules (Example 1.4).

Let V be a finite dimensional vector space over the field F and let T be a linear transformation of V. By Example 1.4, we know that V can be considered as a $F[X]$-module where $F[X]$ is a PID. Since V has finite dimension over F, it is finitely generated as an F-modules by definition. Furthermore, V is finitely generated as an $F[X]$-module as well since $F \subseteq F[X]$.

Before implementing the Fundamental Theorem on the $F[X]$-module, we claim that there is no $(F[X])^r$ form in the decomposition. Assume (for contradiction)

$$V \cong (F[X])^r \oplus Tor(V)$$

for some $r \in \mathbb{Z}^+$. Consider $F[X]$ to be a F-module. By definition of polynomial rings, $F[X]$ cannot be finitely generated over F, and $\dim_F(F[X]) = \aleph_0$. By the decomposition, $\dim_F(V) \geq \dim_F((F[X])^r) = r \cdot \dim(F[X]) = r \cdot \infty = \infty$. However, we have $\dim_F(V) < \infty$ by our assumption. Contradiction. Therefore, there is only torsion part in the decomposition.

Then, we have two choices: use the Invariant Factor Form to decompose or use the Elementary Divisor one. The former will induce the Rational Canonical Form while the latter will induce the Jordan Canonical Form.

3.1. **Rational Canonical Form.**

We first apply the Invariant Factor Form. By Theorem 2.1, we have an isomorphism

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

of $F[X]$-modules where $a_1(x), a_2(x), \cdots, a_m(x)$ are polynomials in $F[X]$ of degree at least one with the divisibility conditions

$$a_1(x) \mid a_2(x) \mid \cdots \mid a_m(x)$$

Though the invariant factors $a_i(x)$ are only unique up to unit multiplication, we can stipulate them to be monic which guarantees uniqueness.

We now consider each of $F[X]/a(x)$ form and choose a standard basis to find the corresponding matrix of T. For $F[X]/a(x)$, the standard basis is $\{1, x, x^2, \cdots, x^{k-1}\}$ where

$a(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_1x + b_0$. Recall from Example 1.4 that $T(v) = x \cdot v$, the way T acting on $F[X]/(a(x))$ is the same:

$$\begin{aligned} T : F[X]/(a(x)) &\to F[X]/(a(x)) \\ 1 &\mapsto x \\ x &\mapsto x^2 \\ &\vdots \\ x^{k-2} &\mapsto x^{k-1} \\ x^{k-1} &\mapsto x^k \equiv -b_0 - b_1x - \cdots - b_{k-1}x^{k-1} \mod a(x) \end{aligned}$$

With respect to the same basis for both sides of the transformation, the matrix for T is therefore

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

Such matrix is called **companion matrix** of $a(x)$, denoted as $\mathcal{C}_{a(x)}$.

Let $\mathcal{B}_i$ be the basis for vector space $F[X]/(a_i(x))$. Since all $F[X]/(a_i(x))$ are connected by direct sum, the union $\mathcal{B}$ of B_is gives a basis for the right hand side of the isomorphism. In other words, $\mathcal{B}$ is a basis for V. With respect to this basis, T has a matrix as direct sum of the companion matrices $\mathcal{C}_{a_i(x)}$:

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

Such matrix is called the **rational canonical form**. Notice that this matrix is uniquely determined from the invariant factors of the $F[X]$-module V which are also unique up to unit multiplication by the fundamental theorem. As we mentioned before, since $a_i(x) \in F[X]$, we can stipulate all of them into monic polynomials. This operation will make them unique without the condition of unit multiplication. The existence and uniqueness is stated as:

Theorem 3.1 (Rational Canonical Form for Linear Transformations)**.** *Let V be a finite dimensional vector space over the field F and let T be a linear transformation of V.*

(1) There is a basis for V with respect to which the matrix for T is in rational canonical form.
(2) The rational canonical form for T is unique.

Remark 3.2. Recall from linear algebra that any $n \times n$ matrix A with entries from the field F arises as the matrix for some linear transformation T of an n-dimensional vector space. It allows us to state the previous theorem in the language of matrices:

(1) The matrix A is similar to a matrix in rational canonical form.
(2) The rational canonical form for A is unique.

Again, recall from linear algebra that "similar" denoted as $\sim$ is an equivalence relation which is able to form equivalences classes for matrices.

Corollary 3.3. *Let A and B be $n \times n$ matrices over the field F. Then $A \sim B$ if and only if A and B have the same rational canonical form.*

Proof. $\Longrightarrow$: Suppose $A \sim B$. By the existence of Remark 3.2, $A \sim Q$ which is in rational canonical form. By transitivity, $B \sim Q$. By the uniqueness of Remark 3.2, A and B have the same rational canonical form Q. $\Longleftarrow$: Suppose A and B have the same rational canonical form Q. Then, both A and B is similar to Q. By transitivity, $A \sim B$. □

By this corollary, rational canonical forms can serve as representatives for equivalence classes. Furthermore, we have a universal property

$$\left\{ \begin{matrix} Q \in M_{n\times n}(F) \text{ a matrix} \\ \text{in rational canonical form} \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} [Q] \text{ an equivalence class} \\ \text{of } M_{n\times n}(F) \text{generated by } \sim \end{matrix} \right\}$$

The word *rational* indicates that this canonical form exists for vector spaces over any field F and any linear transformation T on it. For example, it works for any $\mathbb{Q}$-vector space V with a linear transformation T, and fixing V and T, the rational canonical form with $F = \mathbb{R}$ is same as the one with $F = \mathbb{Q}$. We can generalize this statement into any field extension $K \subseteq L$.

This is not the case for Jordan canonical form, which only exists if the field F contains the eigenvalues for T. Clearly, $\mathbb{Q}$ cannot always serve as the scalar for this form. Before moving to Jordan canonical form, we need to state one more proposition:

Proposition 3.4. *Let T be a linear transformation of an n-dimensional vector space over the field F. The characteristic polynomial of A is the product of all the invariant factors of T:*

$$c_T(x) = a_1(x)a_2(x)\cdots a_m(x)$$

Proof. The characteristic polynomial $c_T(x)$ is invariant regardless of the basis chosen to represent T as a matrix. Then, it is equivalent to show $c_A(x) = a_1(x)\cdots a_m(x)$ where A is the rational canonical form of T. First, we can prove that the characteristic polynomial for each of companion matrix $\mathcal{C}_{a(x)}$ is $a(x)$. Also, we have the lemma that for a block diagonal matrix, its characteristic polynomial is the product of those for its block matrices. By using the lemma, we get the equation we want. □

3.2. **Jordan Canonical Forms.**

For this canonical form, we aim to decompose each invariant factor $a(x)$ into powers of linear factors (i.e. $(x-a)^n(x-b)^m$). However, the Elementary Divisor Form of the fundamental theorem can only decompose $a(x)$ into powers of irreducible polynomials in $F[X]$, not necessarily into powers of linear factors. In general, we need to restrict the field F to be algebraically closed (i.e. F contains all roots of any $p(X) \in F[X]$).

Since the product of elementary divisors are same as the product of invariant factors, it is equal to the characteristic polynomial of T by Proposition 3.4. More specifically, F contains all roots is equivalent to F contains all eigenvalues of T. Under this assumption, by Theorem 2.2, we can get the following isomorphism:

$$V \cong F[X]/((x-\lambda_1)^{k_1}) \oplus F[X]/((x-\lambda_2)^{k_2}) \oplus \cdots \oplus F[X]/((x-\lambda_s)^{k_s})$$

where $\lambda_1, \lambda_2, \cdots, \lambda_s \in F$ are eigenvalues of T (possibly repeated), unique up to rearrangement.

For each of $F[X]/((x-\lambda)^k)$, we consider $\{1, x-\lambda, \cdots, (x-\lambda)^{k-2}, (x-\lambda)^{k-1}\}$ this time. It is a basis for the quotient ring since we can show it's equivalent to the standard basis

$\{1, x, \cdots, x^{k-2}, x^{k-1}\}$ by forward elimination. Recall that T acts on $F[X]/((x-\lambda)^k)$ as left multiplication by x:

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

With respect to this basis, the matrix for T is therefore

$$\begin{pmatrix} \lambda & 1 & & & \\ & \lambda & \ddots & & \\ & & \ddots & 1 & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix}$$

where the blank entries are all zero. Such matrix is called **Jordan block** of size k with eigenvalue λ, denoted as J_λ. Applying this to each $F[X]/((x-\lambda_i)^{k_i})$, we can get $\mathcal{B}_\rangle$ and J_{λ_i}. By the property of direct sum, the union $\mathcal{B} = \cup_{i=1}^{s} \mathcal{B}_\rangle$ is a basis for the right hand side of the isomorphism. Furthermore, $\mathcal{B}$ is a basis of V. With respect to this basis, T has a matrix as direct sum of the Jordan blocks J_{λ_i}:

$$\begin{pmatrix} J_{\lambda_1} & & & \\ & J_{\lambda_2} & & \\ & & \ddots & \\ & & & J_{\lambda_s} \end{pmatrix}$$

Such matrix is called **Jordan canonical form**. Notice that this matrix is uniquely determined up to rearrangement of the blocks along the diagonal by the elementary divisors of the $F[X]$-module V. Conversely, we can get the list of elementary divisors by checking the size (i.e. k) and diagonal entry (i.e. λ) of each Jordan block. Then, by Theorem 2.2, they uniquely determine the module V up to $F[X]$-module isomorphism. The existence and uniqueness is stated as:

Theorem 3.5 ((Jordan Canonical Form for Linear Transformation)). *Let V be a finite dimensional vector space over the field F and let T be a linear transformation of V. Assume F contains all the eigenvalues of T.*

(1) There is a basis for V with respect to which the matrix for T is in Jordan canonical form.
(2) The Jordan canonical form for T is unique up to a rearrangement of the Jordan blocks along the diagonal.

Remark 3.6. We have the same existence and uniqueness in the language of matrices.

By our design, Jordan canonical forms can demonstrate the structure of T (or matrix A representing T). It can answer a) How many distinct eigenvalues there are by diagonal entries, b) What their multiplicities are by sizes of block matrices. Clearly, the diagonal matrix is a

particular example of Jordan canonical form whose blocks are all size 1. Consequently, we obtain the following corollary:

Corollary 3.7.

(1) If a matrix A is similar to a diagonal matrix D (A is diagonalizable), then D is the Jordan canonical form of A.

(2) Two diagonal matrices are similar if and only if their diagonal entries are the same up to rearrangement.

Proof. Both of them can be deduced immediately from the uniqueness (up to rearrangement) of Jordan canonical forms. □

Table 1. Structural Comparison of Canonical Forms

Feature	**Rational Canonical (RCF)**	**Jordan Canonical (JCF)**
Field	Any field F	Contains all eigenvalues (algebraically closed)
Structure	Invariant Factors $a_i(x)$	Elementary Divisors $(x-\lambda_i)^{k_i}$
Blocks	Companion Matrices $C_{a_i(x)}$	Jordan Blocks J_{λ_i}
Decomposition	$V \cong \bigoplus F[X]/(a_i(x))$	$V \cong \bigoplus F[X]/(x-\lambda_i)^{k_i}$
Insight	Equivalence Classes (Similarity)	Eigenvalues/Multiplicity

A summary of the structural differences and field requirements for these two canonical forms is provided in Table 1.

4. Conclusion

This essay has demonstrated that the Fundamental Theorem of Finitely Generated Modules over a PID serves as the unifying bridge between abstract algebra and classical linear algebra. By establishing bijections between abelian groups and $\mathbb{Z}$-modules, we unify the study of finitely-generated groups under a single algebraic framework. Similarly, by identifying linear transformations with $F[X]$-modules, we have shown that the behavior of an operator T is an natural structural identity of the module V rather than a purely geometric property. This decomposition provides a definitive classification, proving that every finite-dimensional operator is equivalent to a unique arrangement of companion matrices or Jordan blocks.

Beyond the theoretical classification, the construction of these forms relies on algorithmic processes like the **Smith Normal Form**, which possesses a polynomial time complexity, typically $O(n^4)$ [3]. However, the numerical instability of the Jordan canonical form in floating-point arithmetic serves as a reminder of the delicate balance between algebraic exactness and computational reality. Ultimately, the theory of modules over PIDs reveals that the diverse landscapes of group theory and matrix analysis are, at their core, governed by the same fundamental algebraic laws.

References

[1] D. S. Dummit and R. M. Foote. *Abstract Algebra*. 3rd ed. John Wiley & Sons, 2004.
[2] K. Hoffman and R. Kunze. *Linear Algebra*. 2nd ed. Prentice-Hall, 1971.
[3] A. Storjohann. *Algorithms for Matrix Canonical Forms*. PhD Thesis, ETH Zurich, 2000.

Department of Computer and Mathematical Science, University of Toronto Scarborough, Toronto, ON, Canada
Email address: lucas.fu@mail.utoronto.ca