Scientific Research Publishing

Advances in Pure Mathematics, 2020, 10, 699-705
https://www.scirp.org/journal/apm
ISSN Online: 2160-0384
ISSN Print: 2160-0368

A Note on Finitely Generated Modules over a *PID*

Xinru Ma[1], Heguo Liu[2], Honglian Zhang[1]

[1]Department of Mathematics, Shanghai University, Shanghai, China
[2]School of Mathematics and Statistics, Hubei University, Wuhan, China
Email: maxruu@163.com, ghliu@hubu.edu.cn, hlzhangmath@shu.edu.cn

How to cite this paper: Ma, X.R., Liu, H.G. and Zhang, H.L. (2020) A Note on Finitely Generated Modules over a *PID*. *Advances in Pure Mathematics*, **10**, 699-705.
https://doi.org/10.4236/apm.2020.1012043

Received: November 13, 2020
Accepted: December 18, 2020
Published: December 21, 2020

Abstract

In this note, we provide an effective proof of the fundamental structure theorem of finitely generated modules over a principal ideal domain, from which we find the minimality of decomposition for a finitely generated module over a principal ideal domain.

Keywords

Finitely Generated Module, Principal Ideal Domain, Cyclic Module

1. Introduction

In the late 1920s, influenced by the mathematics trend at that time, axiom of linear algebra has been formed. At the same time, German algebraist Emmy Noether was the first to realize the potential of the concept of module. Furthermore, the concept of module builds a bridge between the representation theory of finite groups and the theory of algebraic structures. The module concept communicates these two independent and parallel development theories in algebra, and gradually becomes a powerful and important tool in modern algebra. Module theory plays an important role in many algebraic research fields. The classification in algebra is often a topic, that is, portraying all possible different types of algebraic structures. As one kind of algebraic structure, the classification of finitely generated modules over R is the central issues of module theory or ring theory. Regarding the classification of R-module, the R-module is a linear space when R is a domain. It is know that the necessary and sufficient condition for linear space isomorphism is that the two spaces have the same dimension which has been completely classified. When it comes to a general ring R, the R-module is a linear space defined over the ring R macroscopically. However,

the specific classification work is difficult. For the case where R is the principal ideal domain (*PID* for short), the Main Fundamental Theorem for finitely generated modules has complete the classification of the finitely generated R-module. The proof of the Main Fundamental Theorem can be found with classic methods from [1] [2] [3].

This article is based on the concept of "natural generation", and pays full attention to the replacement of domain to ring. Based on the natural transfer of knowledge, the note will use the language of matrix to prove this basic theorem again. The purpose is to prove this classic theorem with more concise knowledge information. The language description and processing methods in this article are consistent with the linear transformation language in advanced mathematics. As a result, it is more conducive to learners to learn and use the Main Fundamental Theorem over the principal ideal domain D.

This note will provide a brief self-contained proof process. And this paper is mainly completed according to the following ideas. The basic concepts and symbols of the basic module and ring theory will be given for the further work at first. Then use properties of the ideal of D to introduce a special matrix A over D and give an important property of such matrix. Subsequently, combine the tool of D-matrix A with the minimum decomposition of D-modules M. Main Fundamental Theorem will be obtained by using contradiction. As a result of the proof, it is not difficult to conclude that there is a unique minimal one among all decompositions of a finitely generated module M over D.

2. Preliminaries

First of all, some basic definitions will be used in this paper. Throughout this note, let R be an arbitrary ring and denote D as a principal ideal domain (*PID*) especially. M is a (left) module over a ring R. And there are some foundations of module and ring theory needed.

1) M is said to be a direct sum of sub-R modules A and B if $M = A + B$ and $A \bigcap B = 0$. Then A and B are called direct summands, and denote that $M = A \oplus B$.

In the case $M = A \oplus B$, every $x \in M$ can be uniquely written as $x = a + b$ with $a \in A, b \in B$.

2) For a given element x in M, $ann(x)$ is the set $\{d \in R \mid dx = 0\} \in R$.

It is well known that $ann(x)$ is an ideal of R, and then call $ann(x)$ the annilator of x.

3) For non-negative integers $a, b\left(a^2 + b^2 \neq 0\right)$, $gcd(a,b)$ represent the greatest common divisor of a and b.

As is known, there exist an integer pair u, v, such that $gcd(a,b) = ua + vb$.

In the next discussion, M is a D-module. Let us recall the main fundamental theorem as mentioned in [1] [2].

Theorem 2.1. *If M is a finitely generated module over D, the following two results hold*:

i) M is a direct sum of cyclic modules: $M = Dx_1 \oplus Dx_2 \oplus \cdots \oplus Dx_s$ such that $annx_i$ satisfy

$$annx_s \subseteq \cdots \subseteq annx_2 \subseteq annx_1 \neq D. \tag{2.1}$$

ii) Let $M = Dx_1 \oplus Dx_2 \oplus \cdots \oplus Dx_s = Dy_1 \oplus Dy_2 \oplus \cdots \oplus Dy_t$, where

$$annx_s \subseteq \cdots \subseteq annx_2 \subseteq annx_1 \neq D \tag{2.2}$$

and

$$anny_t \subseteq \cdots \subseteq anny_2 \subseteq anny_1 \neq D. \tag{2.3}$$

Then $s = t$ and $annx_k = anny_k$ for $1 \le k \le s$.

Before giving our proof, we need some preparations.

Lemma 2.2. *There exists a unique decomposition* $d = up_1^{\alpha_1} p_2^{\alpha_2} \cdots p_l^{\alpha_l}$ *for any nonzero* $d \in D$, *where u is a unit,* p_i *are different prime elements of D and* $\alpha_i \in \mathbb{Z}$ *for* $i = 1, 2, \cdots, l$.

Compared to the definition of the set of lengths of elements in monoid in [4], the definition of length of $d \in D$ can be given certainly since Lemma 2.2.

Next give the length $l(d)$ of $d \in D$.

Definition 2.3. *For each element d in D, call*

$$l(d) = \begin{cases} 0, & d \text{ is a unit} \\ \sum_{i=1}^{l} \alpha_i, & d = up_1^{\alpha_1} p_2^{\alpha_2} \cdots p_l^{\alpha_l} \end{cases} \quad \textit{the length of d.}$$

In addition, let $l(0) = +\infty$ for convention.

Consequently, the length $l(d)$ of d is well-defined for any elements in D. And the following proposition is the key to re-prove the Theorem 2.1.

Proposition 2.4. *Suppose that* $a_1, a_2, \cdots, a_n$ *are coprime elements in D, then there exists an* $n \times n$ *-matrix* $A = \begin{pmatrix} a_1 & a_2 & \cdots & a_{n-1} & a_n \\ & & B & & \end{pmatrix}$ *such that* $\det A = 1$.

Proof. Now we use induction on n to verify this proposition.

Let $n = 2$, we have $(a_1, a_2) = 1, a_i \in D$. Consequently, there are two elements $b_1, b_2 \in D$ such that $a_1 b_1 - a_2 b_2 = 1$. Choose the matrix

$$A_1 = \begin{pmatrix} a_1 & a_2 \\ b_2 & b_1 \end{pmatrix}. \tag{2.4}$$

It is obvious that $\det A_1 = 1$.

Now suppose that the statement is right for the case $n-1$. In general case, firstly, let $(a_1, a_2, \cdots, a_{n-1}) = d$, it is clear that $d \neq 0$. By inductive hypothesis, there exists a $(n-1) \times (n-1)$-matrix

$$A_2 = \begin{pmatrix} \frac{a_1}{d} & \frac{a_2}{d} & \cdots & \frac{a_{n-1}}{d} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,n-1} \\ \vdots & \vdots & & \vdots \\ b_{n-1,1} & b_{n-1,2} & \cdots & b_{n-1,n-1} \end{pmatrix} \tag{2.5}$$

such that $\det A_2 = 1$.

Thanks to $(d, a_n) = 1$, we have $pd - qa_n = 1$, where $p, q \in D$. We construct

$$A=\begin{pmatrix} a_1 & a_2 & \cdots & a_{n-1} & a_n \\ b_{2,1} & b_{2,2} & \cdots & b_{2,n-1} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ b_{n-1,1} & b_{n-1,2} & \cdots & b_{n-1,n-1} & 0 \\ \dfrac{(-1)^n qa_1}{d} & \dfrac{(-1)^n qa_2}{d} & \cdots & \dfrac{(-1)^n qa_{n-1}}{d} & p \end{pmatrix}. \tag{2.6}$$

It is easy to see that $\det A=1$, which implies the statement is right in the case of n. Thus, this proposition has been verified.

Remark 2.5. *More generally, let* $P\in M_{m\times n}(D)$, $m\le n$ *such that the m-rank determinant factors of P are* 1, *then there exists a matrix* $\begin{pmatrix} P \\ * \end{pmatrix}$.

3. Proof of the Main Fundamental Theorem

Now we turn to give the self-contained proof of Theorem 2.1. The work will be achieved by contradiction on the consideration of the minimal decomposition of D-module M.

The proof of Theorem 2.1. Firstly, we check the existence. If $M=0$ is trivial, it is clear. For any nontrivial module

$$M=Dw_1+Dw_2+\cdots+Dw_n. \tag{3.1}$$

Since D is a *PID*, there exists $c_i\in D$ such that the ideals $annw_i=(c_i)$ for $i=1,2,\cdots,n$. Without loss of generality, we can assume that each c_i is not a unit. If not, then we have $Dw_i=0$. On the other hand, we also assume that $annw_i\neq D, i=1,2,\cdots,n$. Using the definition of length, we can assume $l(c_1)\le l(c_2)\le\cdots\le l(c_n)$ after reordering.

Using the above notations, corresponding to any decomposition of $M=Dw_1+Dw_2+\cdots+Dw_n$, there exists an $n+1$-tuple array $(n,l(c_1),l(c_2),\cdots,l(c_n))$. Let $\mathcal{S}$ be the set of all arrays, corresponding to all decompositions of M.

Clearly, $\mathcal{S}$ is a totally ordered set under the lexicographical order. There exists a minimal element in $\mathcal{S}$ with respect to the lexicographical order. We denote by $(s,l(d_1),l(d_2),\cdots,l(d_s))$ the minimal element of $\mathcal{S}$, corresponding to the decomposition of M as follows:

$$M=Dx_2+Dx_2+\cdots+Dx_s \tag{3.2}$$

such that $annx_i=(d_i)$ and $l(d_1)\le l(d_2)\le\cdots\le l(d_s)$.

Now we try to use the minimality to check the existence and the uniqueness of the fundamental structure theorem of M. In fact, for the above minimal decomposition, we have that

$$annx_{i+1}\subseteq annx_i \tag{3.3}$$

for $i=1,\cdots,s-1$.

If not, there exist some i such that $annx_{i+1}\nsubseteq annx_i$, namely, $d_i\nmid d_{i+1}$ for some $1\le i\le s-1$. Let i be the minimal index, then

$$gcd\left(d_i, d_{i+1}\right) = c \neq 0. \tag{3.4}$$

It is clear that $l(c) < l(d_i), l(c) < l(d_{i+1})$.

Using Lemma 2.2, there exists a matrix A_1 with $\det A_1 = 1$ as follows,

$$A_1 = \begin{pmatrix} d_i' & d_{i+1}' \\ * & * \end{pmatrix}. \tag{3.5}$$

Now we construct two elements x_i' and x_{i+1}' as follows:

$$\begin{pmatrix} x_i' \\ x_{i+1}' \end{pmatrix} = \begin{pmatrix} d_i' & d_{i+1}' \\ * & * \end{pmatrix} \begin{pmatrix} x_i \\ x_{i+1} \end{pmatrix}, \tag{3.6}$$

thanks to A_1 is invertible, hence we have

$$M = Dx_2 + Dx_2 + \cdots + Dx_{i-1} + Dx_i' + Dx_{i+1}' + Dx_{i+2} + \cdots + Dx_s. \tag{3.7}$$

Here we denote $annx_i' = (a)$. It is easy to see that $c \in (a)$, consequently,

$$l(a) \leq l(c) < l(d_{i+1}), \tag{3.8}$$

which is a contradiction to the minimality.

Next, we want to check that

$$M = Dx_1 \oplus Dx_2 \oplus \cdots \oplus Dx_s. \tag{3.9}$$

Otherwise, let us consider the following sequence of submodules:

$$\begin{cases} M_1 = Dx_1 \oplus Dx_2; \\ \quad \vdots \\ M_{m-1} = Dx_1 \oplus Dx_2 \oplus \cdots \oplus Dx_{m-1}. \end{cases} \tag{3.10}$$

Without loss of generality, we suppose that $Dx_1 \oplus Dx_2 \oplus \cdots \oplus Dx_m$ is not true for the least m. So we can find a nonzero element $a_m x_m \in M_{m-1} \bigcap Dx_m$, more precisely, there exist nonzero elements $a_1, \cdots, a_{m-1} \in D$ and $a_1 x_1 + \cdots + a_{m-1} x_{m-1} \in M_{m-1}$ such that

$$a_1 x_1 + \cdots + a_{m-1} x_{m-1} + a_m x_m = 0. \tag{3.11}$$

Let $d = gcd\left(a_1, \cdots, a_m\right)$, it is clear that $d \neq 0$. And

$$gcd\left(a_1', \cdots, a_m'\right) = 1, \tag{3.12}$$

where $a_i' = a_i d^{-1}$.

It is a consequence of Lemma 2.2 that there exists an $m \times m$-matrix B with $\det B = 1$,

$$B = \begin{pmatrix} a_1' & a_2' & \cdots & a_{m-1}' & a_m' \\ & & C & & \end{pmatrix}. \tag{3.13}$$

Similarly, since B is invertible, we can construct new generators $x_1', \cdots, x_m'$ of M, which can replace the original generators $x_1, \cdots, x_m$ as follows,

$$\begin{pmatrix} x_1' \\ \vdots \\ x_m' \end{pmatrix} = \begin{pmatrix} a_1' & a_2' & \cdots & a_{m-1}' & a_m' \\ & & C & & \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}. \tag{3.14}$$

Note that $x_1' = a_1' x_1 + \cdots + a_m' x_m$, suppose that $annx_1' = (d')$ for some $d' \in D$.

On the other hand, we have $dx_1' = 0$ for (3.11). Immediately, we have $d' \mid d$. If $d' = d$, then $a_m x_m = 0$, which is impossible. Hence $l(d') < l(d)$, which is a contradiction for the minimality of the decomposition of *M*.

So far we are left to check the uniqueness. If there exist two decompositions

$$M = Dx_1 \oplus Dx_2 \oplus \cdots \oplus Dx_s = Dy_1 \oplus Dy_2 \oplus \cdots \oplus Dy_t, \tag{3.15}$$

such that

$$annx_s \subseteq \cdots \subseteq annx_2 \subseteq annx_1 \neq D \tag{3.16}$$

and

$$anny_t \subseteq \cdots \subseteq anny_2 \subseteq anny_1 \neq D. \tag{3.17}$$

Let us denote that $annx_i = (d_i), anny_j = (e_j)$ for some $d_i, e_j \in D$. Since $\{x_1, x_2, \cdots, x_s\}$ and $\{y_1, y_2, \cdots, y_t\}$ are both generators sets of *M*, they can be *D*-represented by each other, *i.e.*, there exist $P \in M_{st}(D), Q \in M_{ts}(D)$ such that

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_s \end{pmatrix} = P_{st} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_t \end{pmatrix}, \quad \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_t \end{pmatrix} = Q_{ts} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_s \end{pmatrix}. \tag{3.18}$$

It can be immediately gotten that

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_s \end{pmatrix} = PQ \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_s \end{pmatrix}. \tag{3.19}$$

Hence, $PQ = I_s \pmod{d_1}$, which implies that $s \le t$. Similarly, we can get $t \le s$. That is $s = t$.

Thanks to $annx_i = (d_i)$, we have the following two decompositions of direct sum of modules,

$$d_i M = D(d_i x_1) \oplus \cdots \oplus D(d_i x_{i-1}) = D(d_i y_1) \oplus \cdots \oplus D(d_i y_s). \tag{3.20}$$

From the above process, the numbers of the direct summand of the two decompositions are the same, which forces $annx_i = anny_i$ for $1 \le i \le s$. So far, we have completed the proof of the fundamental structure theorem for a finitely generated module over *PID*.

□

It is easy to see that the minimality plays an important role in the above proof, which reveals the following remark.

Remark 3.1. *There exists an unique minimal decomposition for all finitely generated modules over PID.*

4. Conclusion

This brief investigated the Main Fundamental Theorem with a new proof method. The present research was based on the classic proofs of [2] and [1], and

improved readers' understanding of the Main Fundamental Theorem. Indeed, the property that any finitely generated module over *PID* has an unique minimal decomposition should be focused. It is hoped that our work can be extended to the study under the Dedeking domain (*DD* for short) that is similar to *PID* in some algebraic features, or more general king.

Founding

Supported by the National Natural Science Foundation of China (11771129 and 11871325).

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Hungerford, T.W. (1974) Algebra. Springer-Verlag, New York.

[2] Jacobson, N. (1985) Basic Algebra I. W. H. Freman and Company, New York.

[3] Jacobson, N. (1953) Lectures in Abstract Algebra II. Linear Algebra. Springer-Verlag, New York. https://doi.org/10.1007/978-1-4684-7053-6

[4] Geroldinger, A. and Schwab, E.D. (2017) Sets of Lengths in Atomic Unit-Cancellative Finitely Presented Monoids. *Colloquium Mathematicum*, **151**, 171-187. https://doi.org/10.4064/cm7242-6-2017