

3-2022

FINITELY GENERATED MODULES OVER A PRINCIPAL IDEAL DOMAIN

Mariam Mutawa Meshaab Shemal Al-Dhaheri

Follow this and additional works at: https://scholarworks.uaeu.ac.ae/all_theses

 Part of the [Mathematics Commons](#)



MASTER THESIS NO. 2022:65

College of Science

Department of Mathematical Sciences

**FINITELY GENERATED MODULES OVER A
PRINCIPAL IDEAL DOMAIN**

Mariam Mutawa Meshaab Shemal Al-Dhaheri

$$\begin{array}{cccc}
 36 = 2^2 \cdot 3^2, & 36 = 2 \cdot 2 \cdot 3^2, & 36 = 2^2 \cdot 3 \cdot 3, & 36 = 2 \cdot 2 \cdot 3 \cdot 3. \\
 G_1 = \mathbb{Z}_2 + \mathbb{Z}_3 & G_2 = \mathbb{Z}_2 + \mathbb{Z}_2 + \mathbb{Z}_3 & G_3 = \mathbb{Z}_2 + \mathbb{Z}_3 + \mathbb{Z}_3 & G_4 = \mathbb{Z}_2 + \mathbb{Z}_2 + \mathbb{Z}_3 + \mathbb{Z}_3
 \end{array}$$

United Arab Emirates University
College of Science
Department of Mathematical Sciences

FINITELY GENERATED MODULES OVER A PRINCIPAL IDEAL
DOMAIN

Mariam Mutawa Meshaab Shemal Al-Dhaheri

This thesis is submitted in partial fulfillment of the requirements for the degree of
Master of Science in Mathematics

Under the Supervision of Professor Viktor Bodi

March 2022

Declaration of Original Work

I, Mariam Mutawa Meshaab Shemal Al Dhaheri, the undersigned, a graduate student at the United Arab Emirates University (UAEU), and the author of this thesis entitled "*Finitely Generated Modules over a Principal Ideal Domain*", hereby, solemnly declare that this thesis is my own original research work that has been done and prepared by me under the supervision of Professor Viktor Bodi, in the College of Science at UAEU. This work has not previously been presented or published, or formed the basis for the award of any academic degree, diploma or a similar title at this or any other university. Any materials borrowed from other sources (whether published or unpublished) and relied upon or included in my thesis have been properly cited and acknowledged in accordance with appropriate academic conventions. I further declare that there is no potential conflict of interest with respect to the research, data collection, authorship, presentation and/or publication of this thesis.

Student's Signature _____



Date 11/07/2022

Copyright © 2022 Mariam Mutawa Meshaab Shemal Al Dhaheri
All Rights Reserved

Approval of the Master Thesis

This Master Thesis is approved by the following Examining Committee Members:

1) Advisor (Committee Chair): Professor Victor Bodi

Title: Professor

Department of Mathematical Sciences

College of Science

Signature _____



Date 24 November 2022 _____

2) Member: Dr. Adam Zsolt Balogh

Title: Assistant Professor

Department of Mathematical Sciences

College of Science

Signature _____



Date 24 November 2022 _____

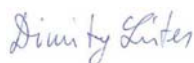
3) Member (External Examiner): Professor Dmitri Leites

Title: Professor, Research Scientist

Institution: NYUAD, Abu Dhabi, UAE

Institution: University of Stockholm, Sweden

Signature _____



Date 24 November 2022 _____

This Master Thesis is accepted by:

Dean of the College of Science: Professor Maamar Benkraouda

Signature Maamar Benkraouda Date Nov. 26, 2022

Dean of the College of Graduate Studies: Professor Ali Al-Marzouqi

Signature Ali Hassan Date Nov. 26, 2022

Copy ____ of ____

Abstract

This thesis covers the main theory of modules: modules, submodules, cosets, quotient modules, homomorphisms, ideals, direct sums, and some related topics. Using these notions, a theorem on the structure of finitely generated modules over domains of principal ideals is proved. As an application of this theorem, the theory of the structure of normal forms of matrices over various fields is presented.

Keywords: Module, finitely generated module, integral domain, ring, Euclidean ring, principle ideal domain, Jordan normal form, Frobenius normal form.

Title and Abstract(in Arabic)**مقاسات متتية التولد في نطاق مثالي رئيسي****المخلص**

تعتبر نظرية القياس أساسية في الجبر و الرياضيات الحديثة و تشمل الأمثلة نظرية التمثيل و تطبيقاتها في الفيزياء وميكانيكا الكم و نظرية الأوتار. حيث خصص بشكل أساسي عرض المفاهيم الأساسية لنظرية المقاس و منها المجموعات المشتركة و المقاسات محدودة التولد و تطبيقاتها في المصفوفات بصورة عادية. ستعرض هذه المواضيع بصورة مبسطة و متدرجة من السهولة الى الصعوبة. كما تطبق هذه النظريات على المصفوفات في مختلف الحقول الرياضية .

مفاهيم البحث الرئيسية المقاس بمقاس محدود التولد والنطاق المشترك الحلقة، الحلقة الاقليدية، نطاق مثالي أساسي و الصورة الاساسية جوردن

Acknowledgements

In the process of preparing and writing this thesis, I received a lot of support and help from my professors, my family and friends.

First of all, I would like to thank my supervisor, Professor Victor Bodi, who helped me in writing this thesis. He spent a lot of time discussing the topic and methods of the theory of Modules. Thank you for your constant help, hardworking and motivating words that inspired and supported me to complete this research work. I would like to express my special thanks to the internal expert Dr. Adam Zsolt Balogh and the external expert Professor Dmitri Leites for their constructive comments and review of my thesis. Finally, I express my gratitude to the members of the Department of Mathematics, especially the Head of the Department Dr. Adama Diene and the Coordinator of the Master Course, Professor Ahmed AlRawashedeh for their support.

To a faithful parent

Table of Contents

| | |
|--|------|
| Title | i |
| Declaration of Original Work | ii |
| Copyright | iii |
| Approval of the Master Thesis | iv |
| Abstract | vi |
| Title and Abstract (in Arabic) | vii |
| Acknowledgments | viii |
| Dedication | ix |
| Table of Contents | x |
| | |
| Chapter 1: Definition of Modules | 1 |
| 1.1 Introduction | 1 |
| 1.2 Notation | 2 |
| 1.3 Definition of Modules over Rings | 3 |
| 1.4 Submodules | 6 |
| 1.5 Direct Sums | 8 |
| 1.6 Cosets and the Quotient Module | 11 |
| 1.7 Homomorphisms of R -modules | 14 |
| | |
| Chapter 2: Euclidean Domain | 19 |
| 2.1 Ideals | 19 |
| 2.2 Ring Homomorphisms | 22 |
| 2.3 Euclidean Rings | 24 |
| 2.4 Ideals in Euclidean Rings | 28 |
| 2.5 Finitely Generated Modules | 29 |
| 2.6 Free Modules | 31 |
| 2.7 Matrices over Euclidean Rings | 33 |
| 2.8 The Main Theorem on Finitely Generated Modules | 38 |
| 2.9 Refinement of the Main Theorem | 42 |
| 2.10 Normal Form of Matrices over a Field | 47 |
| | |
| References | 56 |

Chapter 1: Definition of Modules

1.1 Introduction

The theory of modules is one of the main tools not only of algebra, but of all modern mathematics. Examples include representation theory and its applications in theoretical physics, quantum mechanics, and string theory. Therefore, familiarity with the foundations of the theory of modules over rings is equally necessary for all mathematicians, regardless of their future scientific specialization.

This master's thesis does not contain any deep results of the theory of modules. It is mainly devoted to the presentation of the basic concepts of the theory of modules — modules, submodules, cosets, quotient modules, homomorphisms, ideals, direct sums, and some related topics. Less elementary are the theorems on finitely generated modules and their applications to the theory of the normal form of matrices. Since my task is only to provide a simple introduction to a certain range of issues, I consider it necessary to note that the theorems presented do not pretend to be as general as possible. Those interested in generalizations may refer to the literature (see [1, 2, 3, 4, 5, 6, 7] listed at the end of the thesis).

The examples given in the thesis are mostly elementary, but they are chosen in such a way that it is easy to move on to more involved examples. For those who want to study the theory of modules and their applications in depth, I recommend not to skip these exercises in any case because solving them contributes to a more meaningful consumption of the theory.

1.2 Notation

\mathbb{Z} — the ring of integers;

\mathbb{Q} — the field of rational numbers;

\mathbb{R} — the field of real numbers;

\mathbb{C} — the the field of complex numbers;

\mathbb{Z}_m — the ring of residues modulo m ;

$P(x)$ — the ring of polynomials in x with coefficients in the field P ;

${}_R R$ — the ring R , which is considered as a module over R (the regular R -module);

$A \times B$ — the Cartesian product of the sets A and B ;

$f : A \rightarrow B$ — a mapping f of the set A to the set B ;

$f : a \mapsto b$ — a mapping f transfers element a to element b ;

\oplus — a direct sum of submodules;

$\dot{+}$ — the (external) direct sum of modules;

$\text{diag}(a_1, \dots, a_r)$ is a rectangular $n \times m$ matrix $A = (a_{i,j})$ with the elements

$a_{11} := a_1, \dots, a_{r,r} := a_r$, where $r = \min(n, m)$, and $a_{i,j} = 0$ for all $i \neq j$;

\implies — hence;

\iff — if and only if.

1.3 Definition of Modules over Rings

In the standard algebra course, we got acquainted with concepts such as a group, a ring, a field, and a linear space over a field. The concept of a module over a ring is a generalization of the concept of a linear space over a field. This generalization is obtained by replacing the field by a ring with unit in the definition of the linear space over the field. Indeed, each field is a commutative ring with unit, but a commutative ring with unit differs from the field in that in the field each nonzero element has an inverse, and in the ring this is not always the case (take, for example, the ring of integers \mathbb{Z} , where the equation $2x = 1$, has no solution). The impossibility of dividing by a nonzero element of the ring is the source of many difficulties arising in the theory of modules.

Let us first recall the definition of a linear space over a field: A *linear space over a field* P is an abelian with respect to addition group M , for which the operation $P \times M \rightarrow M$ of multiplying elements from M by “numbers” — the elements of the field P — is defined and the following conditions are met for all $\alpha, \beta \in P$ and $x, y \in M$:

- (i) $\alpha(x + y) = \alpha x + \alpha y$;
- (ii) $(\alpha + \beta)x = \alpha x + \beta x$;
- (iii) $(\alpha\beta)x = \alpha(\beta x)$;
- (iv) $1 \cdot x = x$.

Let us now agree that all rings considered in what follows contain a unit element, which is denote by the symbol 1.

Definition 1.3.1 A *module over the ring* R (or, in short, an *R-module*) is an abelian with to addition group M for which the operation $R \times M \rightarrow M$ of multiplying elements from M by elements from the ring R is defined, and the following conditions are met: for all $\alpha, \beta \in P$ and $x, y \in M$:

- (i) $\alpha(x + y) = \alpha x + \alpha y$;
- (ii) $(\alpha + \beta)x = \alpha x + \beta x$;
- (iii) $(\alpha\beta)x = \alpha(\beta x)$;
- (iv) $1 \cdot x = x$.

For the sake of terminological consistency, R -modules should be called “linear spaces over the ring R ”, but no one calls them that, and there are reasons for this.

The module defined above over the ring R is called the *left R-module*, since the elements of M are multiplied by elements of R on the left ($R \times M \rightarrow M$). In the *right R-module* M , the elements $x \in M$ are multiplied by the elements of the ring R on the

right. Since the theory of right R -modules develops in parallel with the theory of left R -modules, in what follows I restrict myself to considering only left R -modules and call them simply R -modules.

Examples 1.3.2. 1. Any linear space M over any field P is a P -module.

2. The ring $P[x]$ of polynomials over the field P naturally is a P -module, since $P[x]$ is an abelian group, and the operation of multiplying polynomials by numbers from the field P satisfies conditions (i)–(iv).

3. Let R be a subring of the ring K containing the unit of the ring K . Then, K is an R -module if we define the product αx as it is defined in the ring K itself. Indeed, K is an additive abelian group. Conditions (i)–(iv) also take place because this is a part of the ring axioms.

In the special case where $K = R$, we obtain the following result: the ring R can always be regarded as an R -module. This module is called a *regular R -module* and is denoted by ${}_R R$.

4. Let \mathfrak{A} be a linear transformation of the linear space M over the field P . We transform the linear space M into a $P[x]$ -module if we define the product of elements from M by polynomials $f(x) \in P[x]$ by the formula:

$$f(x) \cdot m = f(\mathfrak{A})m,$$

where $f(\mathfrak{A})$ denotes the linear transformation $f(\mathfrak{A}) = a_0\mathfrak{A}^n + \cdots + \mathfrak{A}_n$ of the space M obtained by replacing x with \mathfrak{A} in the polynomial $f(x) = a_0x^n + \cdots + a_n$. Indeed,

$$f(x)(m+n) = f(\mathfrak{A})(m+n) = f(\mathfrak{A})m + f(\mathfrak{A})n = f(x)m + f(x)n.$$

The first and third equalities are true by virtue of the definition of the operation of multiplying vectors by polynomials, and the second equality follows from the linearity of the transformation $f(\mathfrak{A})$.

To check condition (ii), we need to use the definition of the sum of linear transformations, for condition (iii) we use the definition of the product of linear transformations, for condition (iv) we use the definition of the identity transformation.

5. Any additive abelian group M is a module over the ring \mathbb{Z} if the product of elements $x \in M$ by integers, where the action of \mathbb{Z} is denoted by juxtaposition or \cdot , is defined as follows:

$$nx = x + \cdots + x(n \text{ times}), \quad 0 \cdot x = 0 \quad \text{and} \quad -nx = -x - \cdots - x(n \text{ times}),$$

where n is any positive integer (this is how multiples of x are defined in the group theory, where $2x$ is written instead of $x + x$, etc.). The fulfillment of conditions (i)–(iv) is easily verified.

In the same way as in the theory of linear spaces, the following statements can be derived from Axioms (i)–(iv):

1. $\alpha \cdot 0 = 0$ for all $\alpha \in R$;
2. $0 \cdot x = 0$ for all $x \in M$;
3. $(-\alpha)x = \alpha(-x) = -\alpha x$ for all $\alpha \in R$ and for all $x \in M$. In particular, $-1 \cdot x = -x$;
4. $\alpha(x - y) = \alpha x - \alpha y$ and $(\alpha - \beta)x = \alpha x - \beta x$ for all $\alpha, \beta \in R$ and for all $x, y \in M$.

However, the well-known statement of the theory of linear spaces: “If $\alpha x = 0$, then either $\alpha = 0$, or $x = 0$ ” is no longer true in the theory of R -modules (Example: take $M := \mathbb{Z}_6$, so $6x = 0$ for all $x \in M$).

To conclude this section, recall the notion of isomorphisms of R -modules. Two modules M and M' over the same ring R are called *isomorphic* if there exists a one-to-one mapping f of the module M onto the module M' , such that for for all $\alpha \in R$ and for all $x, y \in M$ hold:

- (i) $f(x + y) = f(x) + f(y)$;
- (ii) $f(\alpha x) = \alpha f(x)$.

In other words, condition (i) means that if $x \mapsto f(x)$ and $y \mapsto f(y)$, then the sum $x + y$ corresponds to the element $f(x + y) = f(x) + f(y)$. Condition (ii) means that if $x \mapsto f(x)$, then $\alpha x \mapsto \alpha f(x)$ for all $\alpha \in R$.

Isomorphic modules are “the same” from the algebraic point of view. They differ only in the nature of their elements, but not in their algebraic properties. Any statement of our theory that is true for M is also true for M' .

1.4 Submodules

Let M be an R -module. A subgroup N of a group M is called a *submodule* of the R -module M if it can withstand multiplication by elements of the ring R , that is, $\alpha x \in N$ for all $\alpha \in R$ and for all $x \in N$.

Note that N is also be an R -module because the fulfillment of conditions (i)–(iv) from the definition of a module is guaranteed by the fact that these conditions hold not only for all $x, y \in N$, but also for all $x, y \in M$.

Theorem 1.4.1 *A non-empty subset N of the R -module M is a submodule if and only if for all $\alpha \in R$ and $x, y \in N$ we have*

- (i) $x - y \in N$;
- (ii) $\alpha x \in N$.

The necessity of these conditions is obvious. Let us prove their sufficiency. Let x be any element of N . Then, from condition (ii) $0x = 0 \in N$ and $-1 \cdot x = -x \in N$. Together with condition (i) this shows that N is a subgroup of the group M . Condition (ii) shows that N can withstand multiplication by elements from R .

Any R -module M has submodules $\{0\}$ and M . Any other submodule of the R -module M it is called a *proper* submodule.

Examples 1.4.2. 1. If M is a linear space over the field P , that is, M is a P -module, then any subspace of the space M is a submodule of M .

2. If the ring \mathbb{Z} is regarded as a regular module (clearly, \mathbb{Z} is a group with respect to addition, and an operation of multiplication of \mathbb{Z} by elements of the ring \mathbb{Z} is defined), then the set $2\mathbb{Z}$ of all even numbers forms a submodule. In order to verify this, it is necessary to check the fulfillment of conditions (i) and (ii) from the previous theorem.

3. If an abelian group M is regarded as a \mathbb{Z} -module (see Example 1.4.2 .1), then any subgroup N of the group M is a submodule, since

$$kx = x + \cdots + x \in N \quad (\text{for all } k \in \mathbb{Z}, x \in N).$$

Let A and B be some subsets of the R -module M . The set

$$A + B := \{a + b \mid a \in A, b \in B\}$$

is called a *sum of the subsets A and B* . The intersection of the subsets A and B is called

their *set-theoretic intersection*.

The operation of addition of subsets is associative and commutative, since the operation of addition of elements is associative and commutative. As is known, the operation of intersection of subsets is also associative and commutative. All this allows us to talk about the sum and intersection of a finite number of subsets. For example,

$$A_1 + A_2 + A_3 := \{a_1 + a_2 + a_3 \mid a_i \in A_i, \quad i = 1, 2, 3\}.$$

Theorem 1.4.3 *The sum of two submodules of the R -module M is an R -submodule of M .*

Proof. Let A and B be two submodules of the R -module M . If $a_1 + b_1$ and $a_2 + b_2$ are two arbitrary elements from $A + B$, then their sum $(a_1 + a_2) + (b_1 + b_2)$ again lies in $A + B$ and

$$\alpha(a_1 + b_1) = \alpha a_1 + \alpha b_1 \in A + B, \quad (\alpha \in R).$$

The set $A + B$ is a submodule of the R -module M , by Theorem 1.4.1.

Theorem 1.4.4 *The intersection of submodules of the R -module M is a submodule of M .*

The proof is obvious.

1.5 Direct Sums

Let M_1, \dots, M_s be nonzero submodules of the R -module M . According to the definition, the submodule $M' = M_1 + \dots + M_s$ consists of all possible sums $x_1 + \dots + x_s$ when each x_i runs through M_i . In particular, if M' coincides with the module M , that is, $M = M_1 + \dots + M_s$, then we say that the module M is decomposed into the sum of submodules M_1, \dots, M_s . In this case, any element x from the module M can be represented as $x = x_1 + \dots + x_s$, where $x_i \in M_i$. It is possible that two different sums of this kind coincide, that is,

$$x_1 + \dots + x_s = y_1 + \dots + y_s, \quad (x_i, y_i \in M_i).$$

Definition 1.5.1 We say that the R -module M decomposes into a direct sum of submodules M_1, \dots, M_s , if each element x from M is uniquely represented in the form

$$x = x_1 + \dots + x_s, \quad (x_i \in M_i).$$

To distinguish the direct sum from the one which is not direct, the notation

$$M = M_1 \oplus \dots \oplus M_s$$

is used.

For example, if M is a set of vectors on the plane, considered as a module over the field of real numbers \mathbb{R} , and M_1 and M_2 are submodules of vectors lying on the axes OX and OY , respectively, then $M = M_1 \oplus M_2$, since each vector $a \in M$ is uniquely representable in the form $a = a_1 + a_2$, where $a_i \in M_i$.

Theorem 1.5.2 A given module M is a direct sum of its submodules M_1, \dots, M_s if and only if the following conditions are met:

- (i) $M = M_1 + \dots + M_s$;
- (ii) $M_i \cap (\sum_{j \neq i} M_j) = 0, \quad (1 \leq i \leq s).$

Proof. If the module M is the direct sum of its submodules, then the condition (i) is obvious. To prove condition (ii), assume that $x \in M_i \cap (\sum_{j \neq i} M_j)$. Then, the element x is written as

$$x = 0 + \dots + 0 + \underbrace{x}_i + 0 + \dots + 0,$$

because $x \in M_i$, and on the other hand, $x = x_1 + \dots + \underbrace{0}_i + \dots + x_s$ because $x \in$

$(\sum_{j \neq i} M_j)$. But since the decomposition of the elements of the M module into the sum of elements from the submodules M_1, \dots, M_s is unambiguous, then $x = 0$. Property (ii) is proved.

Sufficiency. Suppose that conditions (i) and (ii) are satisfied. From condition (i) we deduce that every element $x \in M$ can be represented as $x = x_1 + \dots + x_s$, where $x_i \in M_i$. If

$$x_1 + \dots + x_s = y_1 + \dots + y_s,$$

where, say $x_1 \neq y_1$, then

$$x_1 - y_1 = (y_2 - x_2) + \dots + (y_s - x_s).$$

This implies that the nonzero element $x_1 - y_1$ belongs to the intersection of M_1 with $M_2 + \dots + M_s$. This contradicts condition (ii).

The construction of the external direct sum presented below allows one to construct a new R -module from given R -modules. In a sense, this new module contains the given R -modules as submodules.

Given arbitrary R -modules M_1, \dots, M_s , we form the set M of s -dimensional "vectors" (x_1, \dots, x_s) , where $x_i \in M_i$. We introduce two operations in the set M : the addition and the multiplication of the elements of M by elements of the ring R . If $x = (x_1, \dots, x_s)$ and $y = (y_1, \dots, y_s)$ are arbitrary elements of M , then we set

$$x + y := (x_1 + y_1, \dots, x_s + y_s).$$

With respect to this operation, the elements of M form an additive abelian group. For any element $\alpha \in R$ and any element $x = (x_1, \dots, x_s) \in M$, put: $\alpha x := (\alpha x_1, \dots, \alpha x_s)$.

It is easy to check that the set M with the above operations of addition and multiplication by elements of R forms an R -module. This module is called the *external direct sum* of modules and is denoted:

$$M = M_1 \dot{+} \dots \dot{+} M_s.$$

This construction reminds us of constructing an s -dimensional vector space over a field, but here the components of the s -dimensional "vectors" (x_1, \dots, x_s) are elements of the modules M_1, \dots, M_s .

The subsets $\overline{M}_i = \{(0, \dots, 0, \underbrace{x_i}_i, 0, \dots, 0) \mid x_i \in M_i\}$ are submodules of the

R -module M , and $\overline{M}_i \cong M_i$. This isomorphism is given by the formula

$$(0, \dots, 0, \underbrace{x_i}_i, 0, \dots, 0) \mapsto x_i, \quad (\text{for all } x_i \in M_i).$$

Any element of the R -module M is uniquely represented as a sum of elements from the submodules \overline{M}_i :

$$(x_1, \dots, x_s) = (x_1, 0, \dots, 0) + (0, x_2, 0, \dots, 0) + \dots + (0, \dots, 0, x_s).$$

Therefore, the module $M = \overline{M}_1 \oplus \dots \oplus \overline{M}_s$ is the direct sum of its submodules \overline{M}_i . If the modules M_i are replaced with isomorphic modules \overline{M}_i , then the external direct sum becomes the direct sum of submodules

$$M_1 \dot{+} \dots \dot{+} M_s = \overline{M}_1 \oplus \dots \oplus \overline{M}_s.$$

Examples 1.5.3. 1. If the field P is regarded as a regular P -module, then the s -dimensional vector space V_s over the field P is the external direct sum of s copies of P , i.e., $V_s = P \dot{+} \dots \dot{+} P$. Indeed, any element of V_s (an s -dimensional vector) has the form (x_1, \dots, x_s) , where $x_i \in P$.

2. Let M_1 be a \mathbb{Z} -module consisting of all functions defined on the interval $(0, 1)$, and $M_2 = \mathbb{Z}$ be a regular \mathbb{Z} -module. Then,

$$M = M_1 \dot{+} M_2 = \{(f(x), k) \mid f(x) \in M_1, k \in \mathbb{Z}\},$$

so

$$(e^x, 12) + (2x^2, 15) = (e^x + 2x^2, 27),$$

$$6 \cdot (\cos x, 2) = (6 \cos x, 12).$$

1.6 Cosets and the Quotient Module

Let N be a fixed submodule of an R -module M . For any element $a \in M$, one can form the set $a + N = a + x$, where x runs over N . This set is called the *coset* of the module M modulo or by the submodule N , and the element a is called the *representative* of the coset. Note that $a \in a + N$, since $a = a + 0$, where $0 \in N$.

A given coset member does not stand out from the rest of the coset because any coset member can serve as a representative. More precisely, $b + N = a + N$ for all $b \in a + N$. Indeed, if $b \in a + N$, then $b = a + x$ for some $x_0 \in N$. Clearly, $b + x = a + (x_0 + x) \in a + N$ for every $x \in N$, that is, $b + N \subseteq a + N$. But at the same time, $a + x = b + (x - x_0) \in b + N$, that is, $a + N \subseteq b + N$. Therefore, $a + N = b + N$.

Lemma 1.6.1 *Two cosets $a + N$ and $b + N$ coincide if and only if $a - b \in N$.*

Proof. If $a + N = b + N$, then $a = b + x_0$ for some $x_0 \in N$, and $a - b = x_0 \in N$. If $a - b = x_0 \in N$, then

$a = b + x_0 \in b + N$, and hence one can choose a as a representative of the class $b + N$, that is, $a + N = b + N$.

Corollary 1.6.1.1 *The equality $a + N = N$ holds if and only if $a \in N$.*

If two cosets $a + N$ and $b + N$ have a common element c , then they coincide because

$$a + N = c + N = b + N.$$

Therefore, any two cosets either have no element in common or are the same. It follows that the module M can be represented as a set-theoretic sum of disjoint cosets modulo the submodule N . Choose a representative from each coset and denote the resulting set of representatives by T . Then,

$$M = \bigcup_{a \in T} (a + N).$$

The set of all cosets of the module M by the submodule N (we denote it by M/N) can be turned into an R -module if the operation of addition of cosets is defined by the formula

$$(a + N) + (b + N) = (a + b) + N,$$

and the operation of multiplication by elements of R is defined by the formula

$$\alpha(a + N) = \alpha a + N.$$

Verification of Axioms (i)–(iii) from the definition of the R -module is straightforward. Here we face another danger. The addition rule of cosets tells us: in order to add the coset $a + N$ with the coset $b + N$, we need to add their representatives a, b and take the coset with the representatives $a + b$, that is, the class $(a + b) + N$. However, the representative of a corresponding class is not chosen unambiguously.

Does the result of coset addition depend on the choice of representatives? It turns out not. If $a' \in a + N$ and $b' \in b + N$ are other representatives of cosets, then $(a' + b') + N = (a + b) + N$, since by Lemma 1.6.1 we have

$$(a' + b') - (a + b) = (a' - a) + (b' - b) \in N.$$

The case with the operation of multiplying cosets by elements $\alpha \in R$ is similar. If $a' \in a + N$, then $\alpha a' + N = \alpha a + N$, since $\alpha a' - \alpha a = \alpha(a' - a) \in N$.

In the R -module M/N , the role of the zero element is played by the coset $0 + N = N$, and the coset opposite to the coset $a + N$ is the coset $-a + N$, since $(a + N) + (-a + N) = N$.

The R -module M/N we have constructed is called the *quotient-module* of the module M by the module N .

Examples 1.6.2. 1. Consider the \mathbb{Z} -module $\mathbb{Z}_{12} = \{0, 1, 2, \dots, 11\}$ and its submodule $N = \{0, 3, 6, 9\}$. One of the cosets of \mathbb{Z}_{12} modulo N is the submodule N itself. Take any element of the module \mathbb{Z}_{12} that does not lie in N , for example, 5, and find its class $5 + N = \{5, 8, 11, 2\}$. Then, we select any element of the module \mathbb{Z}_{12} that does not lie in the union $N \cup (5 + N)$ of the previously found classes, for example, 7, and find the coset $7 + N = \{7, 10, 1, 4\}$. There are no other cosets of \mathbb{Z}_{12} by N , since

$$\mathbb{Z}_{12} = N \cup (5 + N) \cup (7 + N).$$

By direct verification, we make sure that $5 + N = 2 + N$, and $7 + N = 1 + N$. So, the quotient module \mathbb{Z}_{12}/N consists of three elements $N, 1 + N$ and $2 + N$. In this quotient module, we have

$$\begin{aligned} (1 + N) + (2 + N) &= (3 + N) = (N), \\ (2 + N) + (2 + N) &= 1 + N, \\ -5(2 + N) &= -10 + N = 2 + N, \end{aligned}$$

since in the module \mathbb{Z}_{12} , the element 10 is the additive inverse of 2.

2. The abelian group of Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is, clearly, a \mathbb{Z} -module, and $N = \{2a + 2bi \mid a, b \in \mathbb{Z}\}$ is its submodule. Let $a + bi$ be an element

of M . Dividing the integers a and b by 2 with remainders, we get $a = a' + 2k$ and $b = b' + 2t$, where $0 \leq a', b' \leq 1$. Then,

$$(a + bi) + N = a' + b'i + 2(k + ti) + N = a' + b'i + N$$

(see Corollary 1.6.1.1). Therefore, there are at most 4 cosets of $\mathbb{Z}[i]$ modulo N :

$$0 + N, 1 + N, i + N, 1 + i + N.$$

Direct verifications show that all these 4 classes are different. The quotient module $\mathbb{Z}[i]/N$ has 4 elements $N, 1 + N, i + N, 1 + i + N$. In this quotient module, we have

$$\begin{aligned} (1 + i + N) + (i + N) &= 1 + N, \\ 5(1 + i + N) &= 5 + 5i + N = 1 + i + N. \end{aligned}$$

1.7 Homomorphisms of R -modules

Definition 1.7.1 Let us be given R -modules M and M' . A mapping $f : M \rightarrow M'$ of the module M to the module M' is called an R -homomorphism if for all $\alpha \in R$ and for all $x, y \in M$ the following two conditions hold:

- (i) $f(x + y) = f(x) + f(y)$;
- (ii) $f(\alpha x) = \alpha f(x)$.

Condition (i) shows that the R -homomorphism is a homomorphism of the additive abelian group M into M' , and (ii) shows that the mapping f commutes with multiplication by elements $\alpha \in R$, that is, the elements of the ring can be moved outside the R -homomorphism sign.

We use the following terminology: If the image of f is the entire module M' , then f is said to be a homomorphism "on" (onto) or *surjection*. If f sends only 0 to $0 \in M'$, then we say that f is a homomorphism "in" (into) or *injection*.

If the homomorphism f is a one-to-one mapping of M onto M' , then it is called an *isomorphism*.

Examples 1.7.2. 1. Any linear transformation φ of the linear space M over the field P is a homomorphism of the P -module M to M , since for any $x, y \in M$ and $\alpha \in P$ by the definition of a linear transformation:

$$\varphi(x + y) = \varphi(x) + \varphi(y) \quad \text{and} \quad \varphi(\alpha x) = \alpha \varphi(x).$$

2. The differentiation operator $\frac{d}{dx}$ realizes a homomorphic mapping of the \mathbb{R} -module $\mathbb{R}[x]$ to itself, since for any polynomials $\varphi, \psi \in \mathbb{R}[x]$ and for any real number α we have

$$\frac{d}{dx}(\varphi + \psi) = \frac{d\varphi}{dx} + \frac{d\psi}{dx} \quad \text{and} \quad \frac{d}{dx}(\alpha\varphi) = \alpha \frac{d\varphi}{dx}.$$

Definition 1.7.3 Let $f : M \rightarrow M'$ is a homomorphic mapping of the R -module M to the R -module M' . The kernel of a homomorphism f is the collection of all the elements of M that are mapped to zero of M' . In other words, the kernel of the homomorphism f is the full preimage of the zero element of the module M' under the mapping f . The kernel of the homomorphism f is denoted by the symbol $\ker f$.

Theorem 1.7.4 *Let f be a homomorphism of the R -module M onto the R -module M' . Then,*

- (i) $f(0) \in M'$;
- (ii) $f(-x) = -f(x)$ for all $x \in M$;
- (iii) $\ker f$ is a submodule of the module M .

Proof. (i) $f(0) = f(0x) = 0f(x) = 0'$;

(ii) $f(-x) = f(-1 \cdot x) = -1 \cdot f(x) = -f(x)$ for all $x \in M$;

(iii) for any $x, y \in \ker f$, the element $x - y$ also belongs to $\ker f$, since

$$f(x - y) = f(x) - f(y) = 0' - 0' = 0'.$$

For any $\alpha \in R$, we have $f(\alpha x) = \alpha f(x) = \alpha \cdot 0' = 0'$, so $\ker f$ is a submodule of the module M by Theorem 1.4.1.

Let, as before, f be a homomorphism of the module M to the module M' . The image of the submodule $L \subseteq M$ under the homomorphism f is the set

$$f(L) = \{f(l) \mid l \in L\} \subseteq M'.$$

Let f^{-1} denote the full preimage, not the inverse of f . (Here we cannot talk about the inverse mapping at all, since, generally speaking, f is not a one-to-one mapping.) The full preimage of the submodule $L' \subseteq M'$ under the homomorphism f is the set

$$f^{-1}(L') = \{x \in M \mid f(x) \in L'\}.$$

Theorem 1.7.5 *Under the homomorphism of the module M to M' , the images of the submodules of the module M are submodules of the module M' , and the full inverse images of the submodules of the module M' are submodules of M .*

Proof. Let f be a homomorphism of M to M' and L a submodule of the module M . For any elements $f(l_1)$ and $f(l_2)$ of the set $f(L)$, their sum $f(l_1) + f(l_2) = f(l_1 + l_2)$ again lies in $f(L)$, since the submodule L contains the sum of any two of its elements l_1 and l_2 . For any $\alpha \in R$, we have $\alpha f(l) = f(\alpha l) \in f(L)$ because $\alpha l \in L$. Thus, $f(L)$ is a submodule of the module M' by Theorem 1.4.1.

Now, let L' be an arbitrary submodule of the module M' , and $L = f^{-1}(L')$. If x and y are any elements of L (this means that their images are $f(x), f(y) \in L'$), then $x + y \in L$, since $f(x + y) = f(x) + f(y) \in L'$. For any element $\alpha \in R$, the element αx also lies in L because $f(\alpha x) = \alpha f(x) \in L'$, so L is a submodule of the module M by Theorem 1.4.1.

Theorem 1.7.6 *Let N be a submodule of the R -module M . The mapping $\tau : x \mapsto x + N$, which assigns to each element x of the module M the containing this element coset M by N , is a homomorphism of the module M onto its quotient module M/N , and $\ker \tau = N$.*

Observe right away that the homomorphism τ is called the *natural homomorphism* of the module M onto its quotient module M/N .

Proof. For any $x, y \in M$, we have

$$\begin{aligned}\tau(x+y) &= x+y+N = (x+N) + (y+N) \quad (\text{coset addition rule}) \\ &= \tau(x) + \tau(y),\end{aligned}$$

and for any $\alpha \in R$, we get

$$\tau(\alpha x) = \alpha x + N = \alpha(x+N) = \alpha\tau(x).$$

Now, let us find $\ker \tau$. In the quotient module M/N , the role of zero is played by the coset $0+N$. According to Corollary 1.6.1.1, $x+N = 0+N$ if and only if $x \in N$. Hence, $\ker \tau = N$.

Theorem 1.7.7 [Main Theorem on homomorphisms] *Let $f : M \rightarrow M'$ be a homomorphism of the R -module M onto M' and $N = \ker f$. Then, the module M/N is isomorphic to the quotient module M'/N' .*

Proof. Take an arbitrary element $a' \in M'$ and prove that the full preimage of a' under the mapping f (that is, $f^{-1}(a')$ is the coset of M by N). Let a be a fixed preimage of a' (that is, $f(a) = a'$). Then, for any element $a+x$ of the coset $a+N$, we have

$$f(a+x) = f(a) + f(x) = a' + 0 = a' \implies (a+N) \subseteq f^{-1}(a').$$

Conversely, if some element $b \in M$ is mapped to a' , then

$$f(b-a) = f(b) - f(a) = a' - a' = 0 \implies b-a \in N \implies b \in a+N.$$

Therefore, $f^{-1}(a') = a+N$.

Since the inverse images of elements of M' are cosets of M by N , that is, elements of the quotient module M/N according to the following rule: $\varphi(a') \in M/N$ is the full preimage of a' under the homomorphism f , it follows that

$$\varphi(a') = a+N, \tag{1.1}$$

where a is the image of a' under the homomorphism f . The mapping φ is one-to-one.

Let $x', y' \in M'$ be such that x and y some of their preimages under the mapping f , that is, $f(x) = x'$ and $f(y) = y'$. In order to find $\varphi(x'+y')$ by formula (1.1), we need to know at least one preimage of the element $x'+y'$ when applying f . This preimage

is the element $x + y$, since

$$f(x + y) = f(x) + f(y) = x' + y'.$$

Then, by formula (1.1) we see that

$$\begin{aligned}\varphi(x' + y') &= x + y + N = (x + N) + (y + N) \\ &= \varphi(x') + \varphi(y').\end{aligned}$$

For any element $\alpha \in R$, we have $f(\alpha x) = \alpha f(x) = \alpha x'$, and therefore

$$\varphi(\alpha x') = \alpha x + N = \alpha \varphi(x').$$

Thus, we have shown that the mapping φ given by (1.1) is an isomorphism between the R -module M' and the R -module M/N .

Theorem 1.7.8*[About correspondence] Let f be a homomorphic mapping of the R -module M onto the R -module M' and $N = \ker f$. If we associate every submodule L' of the module M' with its full preimage under the homomorphism f , then we obtain a one-to-one correspondence φ between all submodules of the module M' and the submodules of the module M that contain N .*

If the submodules L' and L correspond to each other, then

$$L/N \cong L' \quad \text{and} \quad M/L \cong M'/L'.$$

Proof. According to Theorem 1.4.3, the complete preimages of submodules of the module M' are submodules of the module M . Obviously, different complete inverse images correspond to different submodules of the module M' .

Finally, any submodule L of the module M containing $N = \ker f$ is the full preimage of the submodule $f(L)$ of the module M' . Indeed, L is contained in the full preimage of $f(L)$. The opposite inclusion is somewhat more difficult to establish. We know from the proof of Theorem 1.7.7 on homomorphisms that the full preimage of an element $f(l)$ under the homomorphism f is a coset $l + N$, and $l + N \subset L$, since $l \in L$, and $N \subseteq L$.

Since the preimage of any element of the submodule $f(L)$ is contained in L , then the full preimage of the submodule $f(L)$ under the homomorphism f is contained in L . This proves the coincidence of the submodule L with the full preimage of the submodule $f(L)$, and at the same time that φ is one-to-one.

If we narrow the domain of definition of the homomorphism f from M to L , then we obtain a homomorphism of the module L onto $L' = f(L)$ with kernel N . By the main theorem on homomorphisms (Theorem 1.7.7) we have $L/N \cong L'$.

Let us prove that $M/L \cong M'/L'$. Consider the following sequence of homomorphisms:

$$M \xrightarrow{f} M' \xrightarrow{\tau} M'/L',$$

where τ is the natural homomorphism of the module M' to the quotient module. It is easy to see that the composition mapping ψ (the product $\tau \circ f$ or τf for short) is a homomorphism of M onto M'/L' .

Let us show that $\ker \psi = L$. The set $\ker \psi$ is the full preimage of the zero of the module M'/L' under the mapping $\psi = \tau f$. The full preimage of zero under the natural homomorphism $\tau : M' \rightarrow M'/L'$ is the submodule L' , and the full preimage of L' under the homomorphism $f : M \rightarrow M'$ is a submodule of L . So, $\ker \psi = L$. Applying now the main theorem on homomorphisms (Theorem 1.7.7) to the homomorphism ψ , we obtain $M/L \cong M'/L'$.

Theorem 1.7.9 *If L and N are submodules of R -module M , then*

$$(L + N)/N \cong L \cap N.$$

Proof. Consider the natural homomorphism τ of the module $L + N$ onto its quotient module $(L + N)/N$. The kernel of this homomorphism is N . We now restrict the domain of definition of the natural homomorphism τ to a submodule L and show that such a restricted homomorphism $\bar{\tau}$ maps L to the entire quotient module $(L + N)/N$.

An arbitrary element $(L + N)/N$ has the form $l + n + N$, where $l \in L$, $n \in N$, and is the image of l under the homomorphism τ , since $\tau(l) + l + N = l + n + N$.

We now apply the main theorem on homomorphisms (Theorem 1.7.7) to the following homomorphism

$$\bar{\tau} : L \rightarrow (L + N)/N.$$

Since the kernel of the homomorphism τ is equal to N , the kernel of the homomorphism $\bar{\tau}$ is equal to $L \cap N$ (after all, $\bar{\tau}$ is obtained from τ by restricting the domain). Therefore,

$$(L + N)/N \cong L \cap N.$$

Examples 1.7.10. 1. A linear transformation of the linear space M over the field P is a homomorphism of the P -module M into itself. We used to call the kernel of this homomorphism the kernel of a linear transformation.

2. Let \mathbb{R} be the field of real numbers, M the \mathbb{R} -module consisting of all continuous functions defined on the segment $[a, b]$, and ${}_{\mathbb{R}}\mathbb{R}$ the regular \mathbb{R} -module. The mapping $f : M \rightarrow \mathbb{R}$, which to each function $x(t)$ assigns its value at the point $t_0 \in [a, b]$, is a homomorphism of the \mathbb{R} -module M onto \mathbb{R} , since

$$f : x(t) + y(t) \mapsto x(t_0) + y(t_0), \quad \text{and} \quad f : \alpha x(t) \mapsto \alpha x(t_0), \quad \alpha \in \mathbb{R}.$$

The kernel N of the homomorphism f consists of all those functions of M that vanish at the point t_0 . The coset $x(t) + N$ consists of all those functions of M that take the value $x(t_0)$ at t_0 . By the main theorem, $M/N \cong \mathbb{R}$.

Chapter 2: Euclidean Domain

2.1 Ideals

Let R be a ring. A subset A of R is called a *left ideal* of R if for all $\rho \in R$ and for all $\alpha, \beta \in A$, we have:

- (i) $\alpha - \beta \in A$;
- (ii) $\rho\alpha \in A$.

Condition (i) says that the ideal A is a subgroup of the additive group of the ring R , and condition (ii) shows that the ideal A with every $\alpha \in A$ contains and all its left multiples $\rho\alpha$, where $\rho \in R$.

The subset A is called a *right ideal* if condition (ii) is replaced by the condition: $\alpha\rho \in A$.

If a left ideal of R is simultaneously a right ideal, then it is called a *two-sided ideal* of R . If the ring R is commutative, then there is no difference between left and right ideals.

In what follows, the word “ideal” will always mean “left ideal”.

Obviously, the ideal of the ring R is nothing but a submodule of the R -module ${}_R R$.

Examples 2.1.1. 1. In the ring $P[x]$, the subring $P[x^2]$ of polynomials in x^2 is not an ideal because $xx^2 = x^3 \notin P[x^2]$, although $x^2 \in P[x^2]$.

2. The set of even numbers $2\mathbb{Z}$ in the ring \mathbb{Z} of all integers is an ideal.

3. The set of all matrices of the form $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ is a left ideal in the ring of all second-order square matrices over the field P (and it is not a right ideal).

4. The set of all polynomials of the ring $P[x]$ that are divisible by the polynomial $x + 1$ is an ideal.

5. If α is a fixed element of the ring R , then the subset $R\alpha = \{\rho\alpha \mid \rho \in R\} \in R$ is a left ideal of the ring R . This ideal is called the *principal ideal generated by element α* . For example, in the ring of integers \mathbb{Z} , the principal ideal $5\mathbb{Z}$, consists of all integers that are multiples of 5.

Any ring R contains two ideals: the zero ideal (0) and the whole ring R . All other ideals of the ring R are called *proper*.

Definition 2.1.1 An element $\alpha \in R$ is called *invertible* if there is $\beta \in R$ such that $\alpha\beta = \beta\alpha = 1$. Invertible elements are simply called *units* of R and denoted as $U(R)$.

In the ring of integers \mathbb{Z} , the only invertible elements are ± 1 . In the ring of matrices over the field P , the invertible elements are invertible (nongenerate) matrices,

and in the ring of polynomials over the field P , the invertible elements are polynomials of degree zero, that is, nonzero numbers of the field P .

Lemma 2.1.3 *Let $\alpha \in A$ be an invertible element.*

Then, $(\rho\alpha^{-1})\alpha \in R$ for all $\rho \in R$, that is, $R = A$.

Proof. Let $\alpha \in A$ be a divisor of 1. Then, $(\rho\alpha^{-1})\alpha = \rho \in R$ for all $\rho \in R$, so $R = A$.

Corollary 2.1.3.1 *There are no nontrivial ideals in the field P .*

Proof. This follows from the fact that all nonzero elements of the field are divisors of the unit 1.

Theorem 2.1.4 *If there are no nontrivial ideals in the commutative ring R , then R is a field.*

Proof. If $\alpha \neq 0$, then the principal ideal $R\alpha \neq (0)$ because it contains the element $1 \cdot \alpha \neq 0$. Since there are no nontrivial ideals, $R\alpha = R$. Therefore, $\beta\alpha = 1$ for some $\beta \in R$. We have shown that every nonzero element $\alpha \in R$ has an inverse. It follows that R is a field.

Let us now define operations on ideals. Since the ideals of the ring R are submodules of the regular module ${}_R R$, we can assume that we already know what the sum and intersection of ideals are ideals, and that the sum and intersection of a finite number of ideals are again ideals of the ring R (Theorems 1.4.3 and 1.4.4).

The *product* of two ideals A and B is the following subset

$$AB = \left\{ \sum_{i=1}^t \alpha_i \beta_i \mid \alpha_i \in A, \beta_i \in B; \quad t < \infty \right\}$$

of all possible finite sums, each term of which is the product of an element by the ideal A by an element of the ideal B . It is easy to check that AB is an ideal of the ring R .

The multiplication of ideals is associative, which allows us to speak of the product of any finite number of ideals. For example,

$$ABC = \left\{ \sum_{i=1}^t \alpha_i \beta_i \gamma_i \mid \alpha_i \in A, \beta_i \in B, \gamma_i \in C; \quad t < \infty \right\}.$$

In the particular case where R is a commutative ring, if $A = R\alpha$ and $B = R\beta$ are principal ideals, then $R\alpha R\beta = R \cdot \alpha\beta$. Indeed, if $x \in R\alpha \cdot R\beta$, then

$$x = \sum_{i=1}^t \alpha_i \beta_i = \sum_{i=1}^t (\rho_i \alpha) (\delta_i \beta) = \left(\sum_{i=1}^t \rho_i \delta_i \right) \alpha \beta \in R\alpha\beta,$$

where $\alpha_i \in R\alpha$ and $\beta_i \in R\beta$.

Conversely, any element of the ideal $R\alpha\beta$ has the form $\rho\alpha\beta = (\rho\alpha)(1\cdot\beta)$ and belongs to the ideal $R\alpha \cdot R\beta$.

As a consequence, for any $\alpha, \beta, \dots, \gamma$ of a commutative ring R , we have

$$R\alpha \cdot R\beta \cdots R\gamma = R(\alpha\beta \cdots \gamma). \quad (2.1)$$

2.2 Ring Homomorphisms

A given mapping f of the ring R to the ring R' is a *homomorphism* if for all $x, y \in R$ the following two conditions are satisfied:

- (i) $f(x + y) = f(x) + f(y)$;
- (ii) $f(xy) = f(x) \cdot f(y)$.

The collection of all elements of the ring R that f maps to zero of the ring R' is called the *kernel of the homomorphism*.

Theorem 2.2.1 *The kernel $\ker f$ of the homomorphism $f : R \rightarrow R'$ is a two-sided ideal A .*

Proof. By definition, $A = \ker f = \{\alpha \in R \mid f(\alpha) = 0'\}$. Then, $\alpha - \beta \in A$ for all $\alpha, \beta \in A$, since

$$f(\alpha - \beta) = f(\alpha) - f(\beta) = 0' - 0' = 0'.$$

Further, $\rho\alpha \in A$ and $\alpha\rho \in A$ for all $\rho \in R$, for all $\alpha \in A$ because

$$f(\rho\alpha) = f(\rho) \cdot f(\alpha) = f(\rho)0' = 0' \text{ and } f(\alpha\rho) = f(\alpha)f(\rho) = 0'.$$

Therefore, A is a two-sided ideal.

The two-sided ideal A of the ring R is a subgroup of the additive group of the ring. The cosets of R by A form an additive group (the quotient group R/A), in which the addition operation is given by the formula

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

We now define the operation of coset multiplication by the formula

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

and show that the multiplication operation defined in this way does not depend on the choice of representatives of cosets. Indeed, if $\alpha' = \alpha + \mu$ and $\beta' = \beta + \nu$, where $\mu, \nu \in A$, then

$$\begin{aligned} (\alpha' + A)(\beta' + A) &= \alpha'\beta' + A \\ &= \alpha\beta + (\alpha\nu + \mu\beta + \mu\nu) + A \\ &= \alpha\beta + A = (\alpha + A)(\beta + A). \end{aligned}$$

In the penultimate equality, we used the fact that the two-sided ideal A contains, together with the elements μ and ν , also $\alpha\nu$ and $\mu\beta$, and $\mu\nu$, and their sum, and by

Corollary 1.6.1.1

$$\alpha\nu + \mu\beta + \mu\nu + A = A.$$

So, on the collection of all cosets of the ring R modulo A , we have defined the operations of addition and multiplication. With respect to these operations, the set of cosets forms a ring (the ring axioms are easy to be verified). This ring is called the *quotient ring* of the ring R by the two-sided ideal A and is denoted by R/A .

For example, all integers that are multiples of a fixed integer m form a two-sided ideal $m\mathbb{Z}$ in the ring \mathbb{Z} . Every element of the quotient ring $\mathbb{Z}/m\mathbb{Z}$ is a residue class modulo m :

$$0 + m\mathbb{Z}, 1 + m\mathbb{Z}, 2 + m\mathbb{Z}, \dots, (m-1) + m\mathbb{Z}.$$

For homomorphisms of rings, all theorems on homomorphisms of modules are valid with appropriate modifications: an ideal instead of a submodule, a quotient ring instead of a quotient module.

2.3 Euclidean Rings

A ring R is said to be a *ring without zero divisors* if the equality $\alpha\beta = 0$, where $\alpha, \beta \in R$ implies that either $\alpha = 0$, or $\beta = 0$. In a ring without zero divisors, one can cancel equalities of the form $\alpha\beta = \alpha\gamma$ by the element $\alpha \neq 0$. Indeed, if $\alpha\beta = \alpha\gamma$, then $\alpha(\beta - \gamma) = 0$. Since $\alpha \neq 0$, then $\beta - \gamma = 0$, that is, $\beta = \gamma$.

Definition 2.3.1 A commutative ring R with unit and without zero divisors is called a *Euclidean ring* if for every nonzero element $\alpha \in R$ there is a nonnegative integer $\varphi(\alpha)$ (called the *norm of α*) that satisfies the following conditions:

- (i) if $\alpha = \beta\gamma$, then $\varphi(\beta) \leq \varphi(\alpha)$;
- (ii) for all $\alpha, \beta \neq 0 \in R$ there exist $\xi, \rho \in R$ such that $\alpha = \beta\xi + \rho$, with either $\rho = 0$ or $\varphi(\rho) < \varphi(\beta)$.

Examples 2.3.2 1. The ring of integers \mathbb{Z} is a Euclidean ring in which the norm of any integer is defined by the formula $\varphi(\alpha) = |\alpha|$.

2. The ring $P[x]$ is a Euclidean ring in which the norm of the polynomial $f(x)$ is defined as

$$\varphi(f(x)) = 2^{\deg(f(x))}.$$

3. The field P is a Euclidean ring in which we assume that the norm of any nonzero element of the field P is 1. The fulfillment of condition (i) is obvious, and in condition (ii) one should always take ρ equal to 0.

A nonzero element $\beta \in R$ is said to be a *divisor* of an element α — this is denoted by $\beta|\alpha$ — if there is an element $\gamma \in R$ such that $\alpha = \beta\gamma$. Two nonzero elements $\alpha, \beta \in R$ are called *associated* if $\alpha = \beta\varepsilon$, where ε is a divisor of a unit of R . In this case, not only $\beta|\alpha$, but also $\alpha|\beta$, since $\beta = \alpha\varepsilon^{-1}$.

An invertible element $\varepsilon \in R$ is a divisor of any element $\alpha \in R$, since $\alpha = \varepsilon(\varepsilon^{-1}\alpha)$. All invertible elements of R and all elements associated with α are divisors of α . These divisors of α are called *trivial*.

For example, for $6 \in \mathbb{Z}$, the divisors are $\pm 1, \pm 6$, so 6 is trivial.

Definition 2.3.3 A nonzero element $\alpha \in R$ is called *prime (indecomposable)* if it is not a divisor of unit and if all its divisors are trivial.

Example 2.3.4 In the ring of integers \mathbb{Z} , the number 2 is prime, since all divisors of 2 are ± 1 (divisors of the unit 1) and ± 2 (associated with element 2), and the number 6 is not prime, since it has nontrivial divisors $\pm 2, \pm 3$.

In what follows, we will only talk about nonzero elements of the Euclidean ring R .

Definition 2.3.5 *Let α and β be elements of a ring R . The greatest common divisor (GCD) of α and β is their common divisor, which is divisible by any other common divisor.*

The proof of the existence of a GCD is carried out using the well-known Euclidean algorithm (the last nonzero remainder is the GCD of the elements α and β).

The GCD of the two elements α and β is denoted by (α, β) .

Let us show that the GCD of α and β is uniquely determined, up to divisors of unity. The proof is based on the following.

Lemma 2.3.6 *If α divides β and β divides α , then α and β are associated.*

Proof. Since $\alpha|\beta$, then $\beta = \alpha\gamma$, and since $\beta|\alpha$, then $\alpha = \beta\delta$. Therefore, $\alpha = \alpha\gamma\delta$. Dividing by α , we get $\gamma\delta = 1$, that is, γ is an invertible element. So, α and β are associated.

The uniqueness of the GCD immediately follows from this Lemma. If there are two GCDs δ and δ' of elements α and β , then by the definition of GCD $\delta|\delta'$ and $\delta'|\delta$. By Lemma 2.3.6 δ and δ' are associated.

Definition 2.3.7 *If $(\alpha, \beta) = 1$, then the elements α and β of the Euclidean ring R are called coprime or relatively prime.*

Lemma 2.3.8 *In any Euclidean ring, the following assertions on divisibility of elements hold:*

- (i) *If $\alpha|\beta$ and $\alpha|\gamma$, then $\alpha|(\beta \pm \gamma)$.*
- (ii) *If $\alpha|\beta$ and $\beta|\gamma$, then $\alpha|\gamma$.*
- (iii) *If $(\alpha, \beta) = \delta$, then there are $\mu, \nu \in R$ such that $\delta = \alpha\mu + \beta\nu$.*
- (iv) *If $(\alpha, \beta) = 1$ and $(\alpha, \gamma) = 1$, then $(\alpha, \beta\gamma) = 1$.*
- (v) *If $(\alpha, \beta) = 1$ and $\alpha|\beta\gamma$, then $\alpha|\gamma$.*
- (vi) *If $(\alpha, \beta) = 1$, then $(\alpha, \beta\gamma) = (\alpha, \gamma)$.*
- (vii) *If α is a prime element and $\alpha|\beta\gamma$, then $\alpha|\beta$ or $\alpha|\gamma$.*

In the next Lemma, we will deal with norms.

Lemma 2.3.9 *In any Euclidean ring the following assertions are valid:*

- (i) If the elements α and β are associated, then $\varphi(\alpha) = \varphi(\beta)$.
- (ii) If $\alpha|\beta$ and $\varphi(\alpha) = \varphi(\beta)$, then α and β are associated.
- (iii) If ε is an invertible element, then $\varphi(\varepsilon) = \varphi(1)$ and vice versa, if $\varphi(\varepsilon) = \varphi(1)$, then ε is an invertible element.
- (iv) If β is a nontrivial (proper) divisor of α , then $\varphi(\beta) < \varphi(\alpha)$.

Theorem 2.3.10 *In any Euclidean ring, every nonzero noninvertible element can be decomposed into a product of a finite number of indecomposable elements. This decomposition is unique up to factors that are units and up to the order of prime factors.*

Proof. Let $\alpha \neq 0$ be a non invertible element of R . If α is indecomposable, then there is nothing more to prove. Therefore, suppose that $\alpha = \beta\gamma$, where both β and γ are elements not associated with α . Then, $\varphi(\beta) < \varphi(\alpha)$ and $\varphi(\gamma) < \varphi(\alpha)$. If both β and γ are indecomposable, then the decomposition of $\alpha = \beta\gamma$ is the prime factorization required. If, for example, $\gamma = \delta\nu$, where δ and ν are not associated with γ , then $\alpha = \beta\gamma\nu$, and we get

$$\varphi(\nu) < \varphi(\gamma) < \varphi(\alpha) \quad \text{and} \quad \varphi(\delta) < \varphi(\gamma) < \varphi(\alpha).$$

This process cannot continue indefinitely due to the fact that the norms of the factors in the decomposition are decreasing all the time (recall that the norms of the elements of the ring R are non-negative integers). As a result, we get the decomposition of the element $\alpha = \pi_1 \cdot \pi_2 \dots \pi_s$ into a product of prime (indecomposable) elements of the ring R .

Let us prove the uniqueness of such an decomposition. For this, assume that there is another decomposition

$$\alpha = \pi_1 \cdot \pi_2 \cdots \pi_s = \omega_1 \omega_2 \cdots \omega_t \tag{2.2}$$

of α into the product of indecomposable elements. Let us show that $s = t$ and, after renumbering, $\omega_i = \pi_i \cdot \varepsilon_i$, where ε_i is a unit. Suppose, for definiteness, that $s \leq t$. Since the left-hand side of equality

$$\pi_1 \cdot \pi_2 \cdots \pi_s = \omega_1 \omega_2 \cdots \omega_t$$

is divisible by π_1 , the product $\omega_1 \cdot \omega_2 \cdots \omega_t$ is divisible by π_1 . The element π_1 divides one of the elements $\omega_1 \omega_2 \dots \omega_t$ by Lemma 2.3.8. We can assume that $\pi_1|\omega_1$ because the numbering of the factors ω_i is in our hands. Then, $\omega_1 = \pi_1 \cdot \varepsilon_1$, where ε_1 is a divisor of unit because ω_1 is an indecomposable element. We get

$$\pi_1 \cdots \pi_s = \pi_1 \cdot \varepsilon_1 \cdot \omega_2 \cdots \omega_t,$$

or $\pi_2 \cdots \pi_s = \varepsilon_1 \cdot \omega_2 \cdots \omega_t$, after dividing by π_1 . We apply the previous reasoning to

this equality and the element π_2 . As a result, we get:

$$1 = \omega_{s+1} \cdots \omega_t \cdot \varepsilon_1 \cdots \varepsilon_1.$$

If $s < t$, then it follows from the last equality that the elements of $\omega_{s+1} \cdots \omega_t$ are not prime because they are divisors of 1. This contradicts the assumption. Therefore, $s = t$ and $\omega_i = \pi_i \varepsilon_i$ for $i = 1, \dots, s$.

Let $\alpha = \pi_1 \cdots \pi_s$ be a prime factorization of α . Among the prime factors, there may be encountered equal. Combining them together, we get the *canonical* decomposition:

$$\alpha = \pi_1^{n_1} \cdots \pi_t^{n_t}, \text{ where } \pi_1, \dots, \pi_t \text{ are prime elements } R.$$

For example, $360 = 2^3 \cdot 3^2 \cdot 5$ is the canonical decomposition of $360 \in \mathbb{Z}$.

Examples 2.3.11. 1. The following are prime factorizations of $30 \in \mathbb{Z}$:

$$30 = 2 \cdot 3 \cdot 5 = 2(-3) \cdot (-5) = (-2) \cdot 3 \cdot (-5).$$

2. We know that any polynomial $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{C}[x]$ can be decomposed into a product of linear factors $f(x) = a_0(x - \alpha_1) \cdots (x - \alpha_n)$, where $\alpha_1, \dots, \alpha_n$ are the roots of the polynomial $f(x)$. Therefore, the first degree polynomials are prime (indecomposable) elements of the ring $\mathbb{C}[x]$.

3. In the ring $\mathbb{R}[x]$ polynomials and quadratic polynomials $x^2 + px + q$ with negative discriminant $p^2 - 4q$ are indecomposable. Any polynomial $f(x) \in \mathbb{R}[x]$ is decomposed into the product of linear factors corresponding to real roots of $f(x)$ and quadratic factors corresponding to complex pairwise conjugate roots of $f(x)$.

2.4 Ideals in Euclidean Rings

Theorem 2.4.1 *Every ideal of any Euclidean ring is principal.*

Proof. Let A be an arbitrary nonzero ideal of the Euclidean ring R and α an element of the ideal A with the least norm. Let us show that the ideal A is a principal ideal generated by the element α , that is, $A = R\alpha = \{\xi\alpha \mid \xi \in R\}$.

Let $\beta \in A$. According to the definition of a ring for elements α and β , there are elements $\xi, \rho \in R$ such that $\beta = \alpha\xi + \rho$, moreover, either $\rho = 0$, or $\varphi(\rho) < \varphi(\alpha)$. Since $\alpha, \beta \in A$, the element $\rho = \beta - \alpha\xi$ also belongs to the ideal A . If $\rho \neq 0$, then the inequality $\varphi(\rho) < \varphi(\alpha)$ contradicts the choice of the element α . Therefore, the remainder is $\rho = 0$ and $\beta = \xi\alpha \in R\alpha$. The opposite inclusion $R\alpha \subseteq A$ is obvious because $\alpha \in A$. So, $A = R\alpha$.

A given nontrivial ideal P is called *prime* if the quotient ring R/P is a ring without zero divisors. This means that from the membership $\alpha\beta \in P$ it follows that either $\alpha \in P$, or $\beta \in P$.

Theorem 2.4.2 *Any prime element π of any Euclidean ring R generates a prime principal ideal $R\pi$. Conversely, every prime ideal P of the Euclidean ring R has the form $P = R\pi$, where π is a prime element of the ring R .*

Proof. If π is a prime element of the ring R and $\alpha\beta \in R\pi$, then $\alpha\beta = \rho\pi$ for some element $\rho \in R$. By Lemma 2.3.8, either $\alpha \in R\pi$ or $\beta \in R\pi$.

Now, let P be a prime ideal of the ring R . Since every ideal of the ring R is principal, then $P = R\pi$ for some element $\pi \in R$. Suppose that π is decomposed into a product of nontrivial divisors $\alpha\beta = \pi \in P$. Then, by the definition of a prime ideal, α and π are associated elements. If $\beta \in P$, then β and π are associated elements. This contradicts the assumption that α and β are nontrivial divisors of π . Hence, π is a prime element of the ring R .

Theorem 2.4.2 implies that

$$R(\alpha \cdot \beta \cdots \gamma) = R\alpha \cdot R\beta \cdots R\gamma.$$

Theorem 2.4.3 *Every nontrivial ideal of any Euclidean ring can be uniquely, up to permutation of terms, decomposed into a product of prime ideals.*

Definition 2.4.4 *A commutative ring with unit and without zero divisors, in which every ideal is principal, is called the principal ideal domain.*

2.5 Finitely Generated Modules

Definition 2.5.1 An R -module M is called *finitely generated* if the module M contains elements u_1, \dots, u_n , where $n < \infty$, such that each element $x \in M$ can be represented as a linear combination of elements u_1, \dots, u_n with coefficients in the ring R :

$$x = \alpha_1 u_1 + \dots + \alpha_n u_n, \quad (u_i \in R).$$

If the elements u_1, \dots, u_n constitute a system of generators R -module M , they are called *generators* of the module M , and the notation $M = \langle u_1, \dots, u_n \rangle$ is used. An R -module M with one generator is called *cyclic*.

If u is a generator of a cyclic R -module M , then $M = \langle u \rangle = \{ \alpha u \mid \alpha \in R \}$.

Examples 2.5.2. 1. Any finite-dimensional vector space M over the field P is a finitely generated P -module. The system of generators here is a finite system of vectors containing a basis.

2. The polynomial ring $P[x]$ over the field P is not a finitely generated P -module.

3. In the linear space M over the field P , any 1-dimensional subspace is a cyclic submodule.

4. The regular module ${}_R R$ is also a cyclic module with generating element $1 \in R$.

5. Let M be a linear space over the field \mathbb{R} with the basis $\{e_1, e_2\}$ and let $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ be the matrix \tilde{A} of a linear transformation of the space M in this basis. Let us endow M with an $\mathbb{R}[x]$ -module structure by setting

$$f(x) \cdot m = f(A)m \quad (\text{for all } m \in M).$$

It is easy to see that M is a cyclic $\mathbb{R}[x]$ -module with generator e_1 . Indeed, if $N = \langle e_1 \rangle$, then $e_1 = 1 \cdot e_1 \in N$ and $x e_1 = \tilde{A}(e_1) = e_2 \in N$. Therefore, $M = N = \langle e_1 \rangle$.

Theorem 2.5.3 If R is a principal ideal domain, then every submodule of a finitely generated R -module is finitely generated and the number of generators of the submodule does not exceed the number of generators of the module.

Proof. Let us apply induction on the number of generators of the module. Suppose that the assertion of the theorem is true for all R -modules with less than n generators; let $M = \langle u_1, \dots, u_n \rangle$; let N be a submodule of the R -module M . Every element $x \in N$

can be represented as

$$x = \alpha_1 u_1 + \cdots + \alpha_n u_n.$$

If all the last coefficients α_n for all $x \in N$ are equal to zero, then N is contained in the submodule $\bar{M} = \langle u_1, \dots, u_{n-1} \rangle$ and the induction hypothesis can be applied to N . Therefore, we can assume that not all $\alpha_n = 0$. It is easy to check that all the coefficients α_n that occur in the decomposition of the elements x of the submodule N form a nonzero ideal A of the ring R . Since each ideal of the ring R is principal, then $A = R\alpha_0$, where α_0 occurs in the decomposition of some element $x_0 \in N$ as a coefficient of u_n :

$$x_0 = \beta_1 u_1 + \cdots + \beta_{n-1} u_{n-1} + \alpha_0 u_n.$$

If $x = \alpha_1 u_1 + \cdots + \alpha_n u_n \in N$, then $\alpha_n \in R\alpha_0$, and therefore $\alpha_n = \mu \alpha_0$. Note that the coefficient α_n , and hence the element μ , depends on the element $x \in N$, and if we need to emphasize this, then we will write $\mu(x)$ instead of μ .

For the element $x \in N$, we form the element

$$\tilde{x} = x - \mu x_0 = (\alpha_1 - \mu \beta_1) u_1 + \cdots + (\alpha_{n-1} - \mu \beta_{n-1}) u_{n-1}. \quad (2.3)$$

Clearly $x, x_0 \in N$, so $\tilde{x} \in N$. It is easy to see that the set

$$\tilde{M} = \{\tilde{x} := x - \mu(x)x_0 \mid x \in N\}$$

forms a submodule of the R -module N .

From the definition of the module \tilde{M} it follows that $N = \tilde{M} + \langle x_0 \rangle$, and from formula (2.3) we see that \tilde{M} is a submodule R -module $M = \langle u_1, \dots, u_{n-1} \rangle$. Since the number of generators of \tilde{M} is less than n , then by induction assumption $\tilde{M} = \langle v_1, \dots, v_{n-1} \rangle$. By virtue of the equality $N = \tilde{M} + \langle x_0 \rangle$, the elements v_1, \dots, v_{n-1}, x_0 are generators of the submodule N , that is,

$$N = \langle v_1, \dots, v_{n-1}, x_0 \rangle.$$

REMARK. The proof remains valid for $n = 1$ (the base of induction). In this case, $\tilde{M} = 0$ and $N = \langle x_0 \rangle$.

2.6 Free Modules

In the theory of linear spaces, the concept of linear dependence played an important role. This concept can be transferred to the module theory.

Elements u_1, \dots, u_n of an R -module M are called *linearly dependent* if there are nonzero elements $\alpha_1, \dots, \alpha_n \in R$, such that

$$\alpha_1 u_1 + \dots + \alpha_n u_n = 0.$$

If the equality $\alpha_1 u_1 + \dots + \alpha_n u_n = 0$ implies that all the coefficients $\alpha_i = 0$, then the elements u_1, \dots, u_n are called *linearly independent*. Any linearly independent system of generators of the R -module M is called an R -basis. It is proved in the usual way that any element of the R -module M can be uniquely expanded in terms of any basis.

Definition 2.6.1 *An R -module is called free, if it is a module that has an R -basis.*

Examples 2.6.2. 1. Any finite-dimensional vector space over any field P is a free P -module.

2. The additively written cyclic group $G = \mathbb{Z}_6$ of order 6 is not a free \mathbb{Z} -module, since $6x = 0$, for any $x \in G$ and $6 \neq 0$.

3. The additively written infinite cyclic group $G = \langle a \rangle$ is a free \mathbb{Z} -module with a as a basis element.

4. Let M be a linear vector space with basis $\{e_1, e_2\}$ over the field \mathbb{R} , let $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ be the matrix of a linear transformation of the space M . Let us endow M with a $\mathbb{R}[x]$ -module structure by setting $f(x)m = f(A)m$. Then, $M = \langle e_1 \rangle$ is a cyclic module generated by e_1 .

The vector e_1 is linearly dependent. Indeed, $f(x) = x^2 - 1 \neq 0$, and

$$f(x)e_1 = (A^2 - E)e_1 = 0, \quad \text{since} \quad A^2 = E.$$

Any other element of the module M has the form $g(x)e_1$, where $g(x) \in \mathbb{R}[x]$. Therefore, for the same $f(x)$ we have $f(g e_1) = g f(e_1) = 0$. Thus, there are no linearly independent elements in M . This is an example of a non-free $\mathbb{R}[x]$ -module.

For a given ring R , it is always possible to construct a free R -module with any given number of generators in advance. In order to construct such a module, consider

the symbols v_1, \dots, v_n and form the set \mathbb{V} of formal sums of the form

$$\alpha_1 v_1 + \dots + \alpha_n v_n, \text{ where } \alpha_i \in R.$$

We will assume that two such sums are equal if and only if all coefficients are equal, that is,

$$\sum_i \alpha_i v_i = \sum_i \beta_i v_i \iff \alpha_i = \beta_i \quad \text{for all } i.$$

The addition operation in \mathbb{V} is defined by the formula

$$\sum_i \alpha_i v_i + \sum_i \beta_i v_i = \sum_i (\alpha_i + \beta_i) v_i,$$

and the operation of multiplication by the elements of the ring by the formula

$$\alpha \cdot \sum_i \alpha_i v_i = \sum_i (\alpha \alpha_i) v_i.$$

With such a definition of operations, \mathbb{V} is an R -module with basis v_1, \dots, v_n .

Theorem 2.6.3 *Every finitely generated R -module is isomorphic to the quotient module of a free R -module with a finite basis.*

Proof. Let M be a finitely generated R -module with generators u_1, \dots, u_n , and \mathbb{V} the free R -module with generating elements v_1, \dots, v_n constructed above.

The mapping $f : \mathbb{V} \rightarrow M$ given by the formula

$$f(\alpha_1 v_1 + \dots + \alpha_n v_n) = \alpha_1 u_1 + \dots + \alpha_n u_n,$$

is a homomorphism of the module \mathbb{V} to the module M . If W is the kernel of this homomorphism, then by the main theorem on homomorphisms $M \cong \mathbb{V}/W$.

2.7 Matrices over Euclidean Rings

Let $A = \|\alpha_{ij}\|$ be a matrix of dimension $n \times m$ over the Euclidean ring R . The following transformations are said to be *elementary transformations* of this matrix:

- T1.** Transposition (interchange) of two rows or two columns;
- T2.** Adding to some row (column) to another row (column) multiplied by any element of R ;
- T3.** Multiplication of a row (column) by an invertible element of the ring R .

Definition 2.7.1 Two $n \times m$ matrices A and B over the ring R are called *equivalent* (notation: $A \sim B$) if the matrix A can be transformed into the matrix B using transformations **T1**, **T2** and **T3**.

It is easy to see that an equivalence relation is reflective, symmetric, and transitive. Therefore, the set of all R -matrices of size $n \times m$ splits into disjoint union of equivalence classes of matrices.

Our task is to show that each class contains a diagonal matrix

$$\text{diag}(\delta_1, \dots, \delta_t, 0, \dots, 0),$$

where δ_i divides δ_{i+1} for $i = 1, \dots, t-1$ and $t \leq \min\{m, n\}$. This matrix is called the *normal diagonal form* (NDF) of the given matrix, and the elements on the main diagonal are called *invariant factors* of the given matrix.

Theorem 2.7.2 Any matrix over any Euclidean ring R can be reduced to the normal diagonal form by elementary transformations **T1**, **T2** and **T3**.

Proof. Use induction on the size of the matrix. For 1×1 matrices, the theorem is obvious. Suppose that it is true for matrices of size $(n-1) \times (m-1)$. Let $A = (\alpha_{ij})$ be an arbitrary $n \times m$ matrix over the ring R . Let us denote by ϑ the class of $n \times m$ matrices equivalent to the matrix A . In this class, choose a matrix $B = \|\beta_{ij}\|$ which contains an element whose norm is not greater than the norm of any element of any matrix of the class ϑ . Without loss of generality, we can assume that this element is located in the upper left corner of the matrix B .

First, let us show that β_{11} divides all the elements of the first row and the first column of the matrix B . Indeed, if the element β_{11} does not completely divide β_{1i} , then we divide β_{1i} by β_{11} with remainder: $\beta_{1i} = \beta_{11}\xi + \rho$, where $\varphi(\rho) < \varphi(\beta_{11})$. Subtracting now from the i^{th} column of the matrix B the first column multiplied by ξ , we get a new matrix B' (equivalent to B), in which the i^{th} element on the first line is ρ . Since $\varphi(\rho) < \varphi(\beta_{11})$, we get a contradiction with the choice of the matrix B and the elements β_{11} . The contradiction proves that β_{11} divides all the elements of the first row. Similarly, we show that β_{11} divides all the elements of the first column. Applying

the second elementary transformation, we bring the matrix B to the form

$$C = \begin{pmatrix} \beta_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & & \\ 0 & & & \end{pmatrix}.$$

Then, by of the induction hypothesis, the matrix C' can be reduced to diagonal form by elementary transformations. Therefore, the matrix C can be reduced by elementary transformations to the form

$$D = \text{diag}(\delta_1, \dots, \delta_t, 0, \dots, 0),$$

where $\delta_1 = \beta_{11}$, and $\delta_i | \delta_{i+1}$ for $i = 2, \dots, t-1$ by the induction hypothesis. It remains to prove that $\delta_1 | \delta_2$. If it were not so, then we would add the second row to the first row of the matrix D and get a matrix of the form

$$\begin{pmatrix} \delta_1 & \delta_2 & 0 & \cdots & 0 \\ 0 & \delta_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Dividing δ_2 by $\delta_1 = \beta_{11}$ with the remainder, we would get

$$\delta_2 = \delta_1 \xi + \rho, \text{ where } \varphi(\rho) < \varphi(\delta_1) = \varphi(\beta_{11}).$$

Subtracting now from the second column of the resulting matrix, the first column multiplied by ξ , in the first row in the second place we get the element ρ whose norm is smaller than the norm of β_{11} . This contradicts to the choice of β_{11} . Hence, $\delta_1 | \delta_2$.

Remarks

1) If the first k invariant factors $\delta_1, \dots, \delta_k$ are invertible elements, then, applying the third elementary transformation T3, we can reduce our matrix to the following diagonal matrix

$$\text{diag}(1, \dots, 1, \delta_{k+1}, \dots, \delta_t, 0, \dots, 0).$$

Therefore, we always assume that if there are invertible elements among the invariant factors of δ_i , then they are simply equal to 1.

2) In the above proof, the element β_{11} is not constructively defined. In the practical reduction of the matrix A to the NDF, one should select the element of the least norm in the matrix A (for example, α_{11}). If it divides all the other elements of the matrix A , then this is the element denoted by β_{11} in the proof. If it does not divide some element of the matrix A , then it is possible to select the remainder ρ from dividing this

element by α_{11} . That is, by elementary transformations one can obtain from the matrix A the matrix B , one of whose elements is ρ and $\varphi(\rho) < \varphi(\alpha_{11})$. Repeat this process of lowering the norm until the next obtained remainder divides all the other elements of the matrix. This remainder will play the role of β_{11} . Then, proceed as in the proof of Theorem 2.7.2.

3) The proof of Theorem 2.7.2 carries over without significant changes to matrices over principal ideal domains. Indeed, if the ring R is a principal ideal domain, then each element of this ring can be uniquely decomposed into a product of prime elements: $a = \pi_1 \cdots \pi_s$. In the class \mathfrak{D} of all matrices equivalent to the matrix A , it is necessary to choose the matrix B , which contains a nonzero element β_{11} whose decomposition contains the smallest number of prime factors. To prove that β_{11} divides all other elements of the matrix B without remainder, we need to apply the following trick. For example, if β_{11} does not divide β_{12} , then $\delta = (\beta_{11}, \beta_{12})$ contains fewer prime factors than β_{11} . There are elements $\mu, \nu \in R$ such that $\delta = \beta_{11}\mu + \beta_{12}\nu$, and $(\mu, \nu) = 1$. Then, elementary transformations of the matrix B can produce the element δ , and this contradicts the choice of the element β_{11} .

We pass to the proof of uniqueness.

Theorem 2.7.3 *The invariant factors of a matrix A are determined uniquely, up to invertible factors.*

Proof. Let the matrix B be obtained from the matrix A using one elementary transformation.

Minors of the k^{th} order of the matrix B are linear combinations of the minors of the k^{th} order of the matrix A and vice versa. Indeed, if a transformation of type 2 or 3 was performed, then this is obvious. If the j -th row was added to the l -th row of the A matrix, then the minors of the resulting B matrix that do not contain the l -th row are equal to the corresponding minors of the A matrix, and the minors of the matrix B containing the i -th row, by the known property of the determinant, can be decomposed into the sum $M_1 + \lambda M_2$, where M_1 and M_2 are minors of the matrix A (or $M_2 = 0$ if the j -th row is included in the considered minor of the matrix B).

Since the minors of the k^{th} order of the matrix B are linear combinations of the minors of the k^{th} order of the matrix A , the greatest common divisor $d_k(A)$ of the minors of the k^{th} order of the matrix A coincides, up to an invertible factor, with the greatest common divisor $d_k(B)$ of the k -th order minors of the matrix B .

Suppose now that A is reduced by elementary transformations to the NDF

$$D = \text{diag}(\delta_1, \dots, \delta_r, 0, \dots, 0).$$

Then, $d_k(D) = \delta_1 \cdots \delta_k$ for $k = 1, \dots, t$, and therefore $\delta_1 = d_1(D)$, and

$$\delta_k = \frac{d_k(D)}{d_{k-1}(D)}, \quad (k = 2, \dots, t).$$

But, according to what was said above, $d_k(D) = d_k(A)\varepsilon_k$, where ε_k is an invertible element of the ring R . Therefore, $\delta_1 = d_1(A)\varepsilon_1$, and

$$\delta_k = \frac{d_k(A)\varepsilon_k}{d_{k-1}(A)\varepsilon_{k-1}}, \quad (k = 2, \dots, t).$$

The last formulas show that the invariant factors of the matrix A are uniquely (up to invertible factors) determined by the matrix A itself.

Let M be an R -module with generators u_1, \dots, u_m , and N a submodule of M with generators v_1, \dots, v_n ($n \leq m$). Since each element of the R -module M is a linear combination of the elements u_1, \dots, u_m , then $v_i = \alpha_{i1}u_1 + \cdots + \alpha_{im}u_m$ for $i = 1, \dots, n$. From the decomposition coefficients we form the following matrix

$$A = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1m} \\ \vdots & \vdots & \vdots \\ \alpha_{ni} & \cdots & \alpha_{nm} \end{pmatrix}, \quad (\alpha_{ij} \in R).$$

In what follows, this matrix is called *connecting matrix* for the system of generators of the module M and the submodule N . The following transformations of generators are called *elementary*:

- T1.** A transposition (interchange) of some generators.
- T2.** Adding to the generator $u_i(v_i)$ any other $u_j(v_i)$ multiplied by any element of the ring R .
- T3.** Multiplication of the generating element $u_i(v_i)$ by an invertible element of the ring R .

It is easy to see that elementary transformations transform any system of generators into a system of generators. The elementary transformations of generators generate elementary transformations of the connecting matrix. The transposition of v_i and v_j causes the transposition of the i -th and j -th rows of the matrix A (for the elements u_i and u_j should be the transposition columns). Adding the generating element v_j , where $i \neq j$, to v_i multiplied by $\lambda \in R$, causes adding the j -th row multiplied by λ to the i -th row (for the case $u_i + \lambda u_j$ we add to j -th column of i -th multiplied by $-\lambda$).

We perform such elementary transformations of the generators that bring the matrix A to the normal diagonal form. As a result, we get new generators u'_1, \dots, u'_m of the module M and new generators v'_1, \dots, v'_m of the submodule N for which the

connecting matrix is diagonal:

$$D = \text{diag}(\delta_1, \dots, \delta_n), \quad \text{where} \quad \delta_1 | \delta_2, \dots, \delta_{n-1} | \delta_n.$$

Then, $v'_i = \delta_i u'_i$, where $i = 1, \dots, n$. If the last few elementary divisors are equal to zero, then for the corresponding generators $v'_i = 0$ and $u'_i = 0$ and they can be removed from the system of generators. So, we have proved the following theorem for modules over principal ideal domains.

Theorem 2.7.4 *Let R be a principal ideal domain. Let N be a submodule of a finitely generated R -module M . Then, in the module M and in the submodule N , there exist systems of generators u_1, \dots, u_m and v_1, \dots, v_n , respectively, that $v_i = \delta_i u_i$ with all $\delta_i \neq 0$ and δ_i divides δ_{i+1} , where $i = 1, \dots, n$.*

As an application of this result we obtain the following.

Theorem 2.7.5 *If R is a principal ideal domain, then every submodule of a free R -module is free.*

Proof. Let M be a free module over the ring R with basis u_1, \dots, u_m , let N be its submodule. By Theorem 2.5.3, N is a finitely generated R -module.

Let v_1, \dots, v_n be generators of N . By Theorem 2.7.4, we can choose new generators u'_1, u'_2, \dots of M and new generators v'_1, v'_2, \dots , such that $v'_i = \delta_i u'_i$, where $\delta_i \neq 0$ and $i = 1, \dots, n$. Since elementary transformations transform a basis into a basis, the elements u'_i for $i = 1, \dots, m$ are linearly independent. The elements $\delta_1 u'_1, \dots, \delta_n u'_n$ are also linearly independent because any dependence between them entails the dependence of the elements u'_1, \dots, u'_m . Thus, the R -module N has a linearly independent system of generators, that is, it is a free R -module.

Example 2.7.6 Consider \mathbb{Z}_4 as a module over the ring \mathbb{Z}_4 . This is a free \mathbb{Z}_4 -module with generator 1. The submodule $N = \{0, 2\}$ of the module \mathbb{Z}_4 is not free, since both of its elements are linearly dependent (indeed: $2 \cdot 0 = 0$ and $2 \cdot 2 = 0$). The point is that \mathbb{Z}_4 is a zero-divisor ring. For this ring, the Theorem 2.7.5 is not applicable.

2.8 The Main Theorem on Finitely Generated Modules

Let M be an R -module, N a submodule of M . The annihilator of a submodule is the collection of all elements $\alpha \in R$ such that $\alpha x = 0$ for all $x \in N$:

$$\text{ann}N = \{\alpha \in R \mid \alpha x = 0 \text{ for all } x \in N\}.$$

It is easy to show that the annihilator of a submodule N is an ideal of the ring R .

Theorem 2.8.1 [The main theorem on finitely generated modules] Any *finitely generated module M over a principal ideal domain R decomposes into a direct sum of cyclic submodules whose annihilators are either zero ideals or the principal ideals:*

$$R\delta_1, R\delta_2, \dots, R\delta_t, \text{ where } \delta_1 \mid \delta_2 \mid \dots \mid \delta_t, \text{ for } i = 1, \dots, t.$$

Proof. By Theorem 2.6.3 there is a finitely generated free R -module \mathbb{V} and a submodule W in it such that $M \cong \mathbb{V}/W$. Choose a basis u_1, \dots, u_m of the module \mathbb{V} and a basis v_1, \dots, v_n of the submodule W by Theorem 2.7.4, so that

$$v_i = \delta_i u_i \quad \text{and} \quad \delta_i \mid \delta_{i+1} \quad (\text{for any } i = 1, \dots, n-1).$$

Any $x \in W$ can be decomposed (with respect to the basis of the module \mathbb{V}) in the following form $x = \alpha_1 u_1 + \dots + \alpha_m u_m$ and with respect to the basis of the submodule W in the following form

$$x = \beta_1 v_1 + \dots + \beta_n v_n = \beta_1 \delta_1 u_1 + \dots + \beta_n \delta_n u_n.$$

Due to the uniqueness of the decomposition in these bases:

$$\begin{cases} \alpha_i = \beta_i \delta_i, & \text{for } i = 1, \dots, n; \\ \alpha_j = 0, & \text{for } j = n+1, \dots, m. \end{cases} \quad (2.4)$$

Conversely, if equalities (2.4) hold for some element $x = \alpha_1 u_1 + \dots + \alpha_m u_m \in \mathbb{V}$, then $x \in W$.

As we know, $x + W = W$ if and only if $x \in W$. Clearly, for the element $x = \alpha_1 u_1 + \dots + \alpha_m u_m$, the equality $x + W = W$ holds if and only if the equalities (2.4) hold for its coefficients.

We denote by $\langle \bar{u}_i \rangle$ the cyclic submodule of the module \mathbb{V}/W generated by the element $\bar{u}_i = u_i + W$ for any $1 \leq i \leq m$, and show that

$$\mathbb{V}/W = \langle \bar{u}_1 \rangle \oplus \dots \oplus \langle \bar{u}_m \rangle. \quad (2.5)$$

For any element $x = \alpha_1 u_1 + \dots + \alpha_m u_m$ of the module \mathbb{V} , we have

$$\begin{aligned} x + W &= \alpha_1 (u_1 + W) + \dots + \alpha_m (u_m + W) \\ &= \alpha_1 \bar{u}_1 + \dots + \alpha_m \bar{u}_m, \end{aligned}$$

and therefore $\mathbb{V}/W = \langle \bar{u}_1 \rangle + \dots + \langle \bar{u}_m \rangle$. To prove that this sum is direct, it suffices to prove that the zero element $\bar{0}$ of the module \mathbb{V}/W can be represented only as the sum

of zero terms from the submodules $\langle \bar{u}_i \rangle$. Let $\bar{0} = \alpha_1 \bar{u}_1 + \cdots + \alpha_m \bar{u}_m$ be an arbitrary decomposition of the element $\bar{0}$ into the sum of elements of the cyclic submodules $\langle \bar{u}_i \rangle$. Then, we have

$$\begin{aligned} \bar{0} = W &= \alpha_1(u_1 + W) + \cdots + \alpha_m(u_m + W) \\ &= (\alpha_1 u_1 + \cdots + \alpha_m u_m) + W \\ &= x + W. \end{aligned}$$

Since $x + W = W$, formulas (2.4) hold for the coefficients α_i . Therefore, for $1 \leq i \leq n$, we have

$$\alpha_i \bar{u}_i = \alpha_i u_i + W = \beta_i \delta_i u_i + W = \beta_i v_i + W = W = \bar{0},$$

since $v_i \in W$. For $n \leq i \leq m$, we have $\alpha_i = 0$ and $\alpha_i \bar{u}_i = 0 \bar{u}_i = \bar{0}$. Thus,

$$\mathbb{V}/W = \langle \bar{u}_n \rangle + \cdots + \langle \bar{u}_m \rangle$$

is a direct sum of cyclic submodules.

Let us calculate the annihilators of the cyclic submodules $\langle \bar{u}_i \rangle$ of the module \mathbb{V}/W . Suppose first that $1 \leq i \leq n$ and let $\alpha \in \text{ann}\langle \bar{u}_i \rangle$. Then, $\alpha \bar{u}_i = \bar{0}$, or $\alpha u_i + W = W$. Applying formulas (2.4), we get $\alpha = \beta_i \delta_i \in R\delta_i$, whence $\text{ann}\langle \bar{u}_i \rangle \subseteq R\delta_i$. Conversely, for any element $\beta \delta_i$ of the ideal $R\delta_i$, we have

$$\beta_i \delta_i \bar{u}_i = \beta_i \delta_i u_i + W = \beta v_i + W = W = \bar{0},$$

and therefore $R\delta_i \subseteq \text{ann}\langle \bar{u}_i \rangle$. So, $\text{ann}\langle \bar{u}_i \rangle = R\delta_i$ for any $1 \leq i \leq n$.

Now, let $n \leq i \leq m$, and let $\alpha \in \text{ann}\langle \bar{u}_i \rangle$. Then, $\alpha \bar{u}_i = \bar{0}$, or $\alpha u_i + W = W$. Applying formulas (2.4), we see that $\alpha = 0$. In this case, $\text{ann}\langle \bar{u}_i \rangle = (0)$.

To complete the proof of the theorem, it remains to recall that $M \cong \mathbb{V}/W$.

Remark.

If $\delta_i = 1$ for some i , then $\bar{u}_i = u_i + W = v_i + W = W = \bar{0}$. Therefore, in decomposition (2.5), the corresponding direct summands $\langle \bar{u}_i \rangle$ should be omitted since they are zero.

So, we have shown that every finitely generated R -module M decomposes into a direct sum of cyclic submodules

$$M = \langle u_1 \rangle \oplus \cdots \oplus \langle u_n \rangle \oplus \cdots \oplus \langle u_m \rangle, \quad (2.6)$$

where $\text{ann}\langle u_i \rangle = R\delta_i \neq (0)$ for $1 \leq i \leq n$ and $\text{ann}\langle u_i \rangle = 0$ for $n \leq i \leq m$. Moreover, $\delta_i | \delta_{i+1}$ for all $i = 1, \dots, n-1$.

Theorem 2.8.2 [Uniqueness Theorem] *The decomposition (2.6) of the module M is uniquely determined, up to an isomorphism.*

This is a more subtle statement than Theorem 2.8.1, which establishes only the existence of decomposition (2.6). Let me give a sketch of the proof of this statement.

Obviously, two cyclic R -modules are isomorphic if and only if their annihilators coincide. Therefore, decomposition (2.6) is uniquely (up to an isomorphism of cyclic direct summands) determined by the following vector

$$(R\delta_1, R\delta_2, \dots, R\delta_n, 0, \dots, 0), \quad (2.7)$$

whose "components" are annihilators of cyclic submodules from decomposition (2.6). Let us show that vector (2.7), in its turn, is uniquely determined by the module M . Denoting by N the direct sum of the first n cyclic submodules from decomposition (2.6), and by T the sum of the remaining $m - n$ cyclic submodules, we obtain the decomposition $M = N \oplus T$.

The submodule N is absolutely uniquely determined by the module M because N contains those and only those elements $x \in M$ for which there is a nonzero element $\alpha \in R$ such that $\alpha x = 0$. Thus, $M/N \cong T$, and T is uniquely, up to an isomorphism, determined by the module M and T is a free R -module with basis u_{n+1}, \dots, u_m . It follows that the number of basis elements of the module T (i.e. the number of zero components of the vector (2.7)) is uniquely determined by the module T (and hence by the module M).

It remains to show that the nonzero components of the vector (2.7) are uniquely determined by the modulus N . Indeed, the nonzero components of vector (2.7) are annihilators of cyclic submodules from the decomposition

$$N = \langle u_1 \rangle \oplus \dots \oplus \langle u_n \rangle. \quad (2.8)$$

The last nonzero component of vector (2.7) is the ideal $R\delta_n$ and it is uniquely determined by the module N because $R\delta_n = \text{ann}N$, where it is essential that $\delta_i | \delta_{i+1}$. Since $\langle u_n \rangle \cong R/R\delta_n$, we see that the last cyclic submodule in decomposition (2.8) is uniquely, up to an isomorphism, determined with the submodule N . Therefore, the quotient module $N/\langle u_n \rangle \cong \langle u_1 \rangle \oplus \dots \oplus \langle u_{n-1} \rangle$ is defined uniquely, up to an isomorphism. To complete the proof, one should repeat the reasoning of the last paragraph applied to the quotient module $N/\langle u_n \rangle$, show that $R\delta_{n-1}$ is uniquely determined, etc.

Example 2.8.3 Let \mathbb{V} be a free \mathbb{Z} -module with basis e'_1 and e'_2 . Let W be a submodule of \mathbb{V} with basis $\omega'_1 = 14e'_1 + 12e'_2$ and $\omega'_2 = 6e'_1 + 6e'_2$. Let us describe the structure of the quotient module \mathbb{V}/W . To do this, we compose a connecting matrix

for the bases of the module and submodule $A = \begin{pmatrix} 14 & 12 \\ 6 & 6 \end{pmatrix}$ and convert it to NDF. In the first column of the matrix, the element of the least norm is 6 in the lower left corner of the matrix A . Since 6 does not divide 14, subtracting twice the second row from the first row, we get the matrix $A' = \begin{pmatrix} 2 & 0 \\ 6 & 6 \end{pmatrix}$ with an element of least norm 2. In the language of elementary transformations over bases, this means that we have passed from the basis (ω'_1, ω'_2) to the basis $(\omega'_1 - 2\omega'_2, \omega'_2)$. Indeed,

$$\begin{cases} \omega_1 = \omega'_1 - 2\omega'_2 = 2e'_1, \\ \omega_2 = \omega'_2 = 6e'_1 + 6e'_2. \end{cases}$$

Subtracting the second column from the first column of the matrix A' , we get the matrix $A = \begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix}$, which will be the NDF of A . This means that we have passed from the basis (e'_1, e'_2) to the basis $(e_1 = e'_1, e_2 = e'_1 + e'_2)$:

$$\begin{cases} \omega_1 = 2e'_1 = 2e_1, \\ \omega_2 = 6e'_1 + 6e'_2 = 6e_1, \end{cases} \quad \text{or} \quad \begin{cases} \omega_1 = 2e_1, \\ \omega_2 = 6e_2, \end{cases}$$

and the matrix D is connecting for the bases (e_1, e_2) and (ω_1, ω_2) .

Carrying out arguments similar to those in the proof of the main theorem, we obtain that $\mathbb{V}/W = \langle \bar{e}_1 \rangle \oplus \langle \bar{e}_2 \rangle$, where

$$\bar{e}_1 = e_1 + W, \quad \bar{e}_2 = e_2 + W \quad \text{and} \quad \text{ann}\langle \bar{e}_1 \rangle = 2\mathbb{Z}, \quad \text{ann}\langle \bar{e}_2 \rangle = 6\mathbb{Z}.$$

The cyclic submodule $\langle \bar{e}_1 \rangle$ contains 2 elements: $\bar{0}$ and \bar{e}_1 , where $2\bar{e}_1 = \bar{0}$, and the submodule $\langle \bar{e}_2 \rangle$ contains 6 elements: $\bar{0}, \bar{e}_2, 2\bar{e}_2, 3\bar{e}_2, 4\bar{e}_2, 5\bar{e}_2$, where $6\bar{e}_2 = \bar{0}$. The quotient module \mathbb{V}/W consists of 12 elements

$$\mathbb{V}/W = \{ \alpha\bar{e}_1 + \beta\bar{e}_2 \mid \alpha = 0, 1; \quad \beta = 0, \dots, 5 \}.$$

Clearly, $\langle \bar{e}_1 \rangle \cong \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2$ and $\langle \bar{e}_2 \rangle \cong \mathbb{Z}/6\mathbb{Z} = \mathbb{Z}_6$. Therefore, one can also say that

$$\mathbb{V}/W \cong \mathbb{Z}_2 + \mathbb{Z}_6.$$

Note that for description of \mathbb{V}/W there is no need to compute the explicit form of the new bases of the module and submodule. It is enough to know only the matrix D .

2.9 Refinement of the Main Theorem

Let R be a principal ideal domain. Let M be a module over R , and let A be an ideal in R . The product of the ideal A and the module M is the set

$$AM = \left\{ \sum_{i < \infty} \alpha_i m_i \mid \alpha_i \in A, \quad m_i \in M \right\},$$

which is a submodule of the R -module M .

The next result shows that any decomposition of $\text{ann}M$ into a product of coprime ideals causes a decomposition of the module M .

Lemma 2.9.1 *Let M be an R -module and let A be the annihilator of M . If the ideal A decomposes into a product of two coprime ideals B and C , then the module M decomposes into the direct sum of submodules BM and CM , and $\text{ann}(BM) = C$ and $\text{ann}(CM) = B$.*

Proof. Let $B = R\beta$ and $C = R\gamma$. Let us show that $\text{ann}(CM) = B$. Indeed, $B(CM) = A \cdot M = (0)$, therefore $B \cong \text{ann}(CM)$.

On the other hand, if $\lambda CM = 0$, for any non-zero $\lambda \in R$, then $\lambda C \in \text{ann}M = A = BC$. Then, $\lambda\gamma = \alpha\beta\gamma$ for some $\alpha \in R$. Dividing by γ , we get $\lambda = \alpha\beta \in R\beta = B$, that is, $\text{ann}(CM) \subseteq B$. Similarly, we see that $\text{ann}(BM) = C$.

Recall that ideals $B = R\beta$ and $C = R\gamma$ are called *coprime* if the elements β and γ generating them are coprime, that is, $(\beta, \gamma) = 1$. In this case, there are $\mu, \nu \in R$ such that $\beta\mu + \gamma\nu = 1$. Then, for any $m \in M$, we have

$$m = 1 \cdot m = (\beta\mu + \gamma\nu)m = \mu(\beta m) + \nu(\gamma m),$$

This means that $M = BM + CM$. For any $m \in BM \cap CM$, we have $\gamma m = 0$ and $\beta m = 0$. Therefore, $m = 1 \cdot m = \beta\mu m + \gamma\nu m = 0$. Hence, $M = BM \oplus CM$.

If the annihilator of a cyclic module M cannot be decomposed into a product of coprime ideals, then the module M itself cannot be decomposed into a direct sum of submodules.

Lemma 2.9.2 *A cyclic R -module $M = \langle v \rangle$ with the annihilator $R\pi^n$, where π is a prime element of the ring R , does not decompose into a direct sum of submodules.*

Proof. It is well known that any submodule N of a cyclic module M is also cyclic, i.e., $N = \langle \alpha v \rangle$, where $\alpha \in R$. Let $\alpha = \beta\pi^k$, where $(\beta, \pi) = 1$, and k is a non-negative integer. Let us show that the cyclic submodule $N = \langle \alpha v \rangle$ coincides with the submodule $\langle \pi^k v \rangle$. Since $(\beta, \pi^n) = (\beta, \pi) = 1$, there exist elements $\mu, \nu \in R$ such that $\beta\mu + \pi^n\nu =$

1. Then,

$$\pi^k v = \pi^k(\beta\mu + \pi^n v) = (\pi^k\beta)\mu v + 0 = \alpha\mu v \subseteq \langle \alpha v \rangle,$$

whence the inclusion $\langle \pi^k \rangle \subseteq \langle \alpha v \rangle$ follows. The opposite inclusion is obvious, since

$$\alpha v = \beta\pi^k v \subseteq \langle \pi^k v \rangle.$$

So, all nonzero submodules of the module $M = \langle v \rangle$ have the form

$$\langle \pi^k v \rangle, \text{ where } k = 0, 1, \dots, n-1:$$

recall that $\pi^n v = 0$. All these submodules have nontrivial intersections with each other, since they form the nested chain of submodules:

$$M = \langle v \rangle \supset \langle \pi v \rangle \supset \dots \supset \langle \pi^{n-1} v \rangle \supset (0).$$

Therefore, the R -module M cannot be represented as a direct sum of its submodules.

Theorem 2.9.3[Main theorem, final statement] *Any finitely generated module over the principal ideal domain R decomposes into a direct sum of indecomposable cyclic submodules whose annihilators either are of the form $R\pi^n$, where π is a prime element of the ring R , or are zero ideals.*

Proof. According to Theorem 2.8.1, we have

$$M = M_1 \oplus \dots \oplus M_s, \tag{2.9}$$

where $M_i = \langle v_i \rangle$, $\text{ann}M_i = R\delta_i$ for $i = 1, \dots, t$, and $\text{ann}M_i = (0)$ for $i = t+1, \dots, s$.

We expand the element δ_i for all $i = 1, \dots, t$, into a product of powers of different indecomposable (prime) elements $\delta_i = \pi_{i1}^{n_{i1}} \dots \pi_{ik}^{n_{ik}}$. By formula (2.1), the ideal $R\delta_i$ decomposes into a product of coprime ideals $R\pi_{ij}^{n_{ij}}$ for all $j = 1, \dots, k$. By Lemma 2.9.2, the cyclic submodule M_i is decomposed into a direct sum of k cyclic submodules

$$M_i = M_{i1} \oplus \dots \oplus M_{ik}, \text{ where } \text{ann}M_{ij} = R\pi_{ij}^{n_{ij}}, \tag{2.10}$$

in which each submodule M_{ij} is indecomposable by Lemma 2.9.2.

Theorem 2.9.4 [Krull-Schmidt] *If*

$$M = M_1 \oplus \dots \oplus M_s = M'_1 \oplus \dots \oplus M'_r \tag{2.11}$$

are two different decompositions of a finitely generated module M over a principal ideal domain R into a direct sum of indecomposable cyclic submodules, then $s = r$. In other words, decomposition (2.11) is unique, up to an isomorphism of direct summands.

Proof. In the decomposition of the module M into a direct sum of indecomposable cyclic submodules, we enumerate the terms so that the first m summands are submodules with nonzero annihilators

$$M = M_1 \oplus \cdots \oplus M_m \oplus M_{m+1} \oplus \cdots \oplus M_s, \quad (2.12)$$

where $\text{ann}M_i = R\pi_i^{n_i} \neq \langle 0 \rangle$ for $i = 1, \dots, m$ followed by $\text{ann}M_i = \langle 0 \rangle$ for $i = m+1, \dots, s$. Let

$$N = M_1 \oplus \cdots \oplus M_m; \quad T = M_{m+1} \oplus \cdots \oplus M_s.$$

The submodule N is uniquely determined by the module M and does not depend on the decomposition (4), since N consists of those and only those elements $x \in M$ for which there is a nonzero element $\alpha \in R$ — depending, of course, on x — such that $\alpha x = 0$. The submodule N is called the *periodic part* of the module M .

From the formula $M = N \oplus T$ we obtain $T \cong M/N$, whence we see that the submodule T is uniquely determined by the module M , up to an isomorphism. A free R -module T and its decomposition into a direct sum of indecomposable cyclic submodules is uniquely (up to an isomorphism) determined by the number of basis elements in T , since $T \cong R + \cdots + R$ with $s - m$ summands. It remains to prove the uniqueness of the decomposition

$$N = M_1 \oplus \cdots \oplus M_m. \quad (2.13)$$

Let $R\pi_1, \dots, R\pi_n$ be different prime ideals, the powers of which occur among the annihilators of the submodules M_i in decomposition (2.13). Let us collect into the submodule $M^{(j)}$ the cyclic submodules M_i from decomposition (2.13), whose annihilators are powers of the fixed prime ideal $R\pi_j$, where $1 \leq j \leq n$. As a result, we get $N = M^{(1)} \oplus \cdots \oplus M^{(n)}$, where the submodules $M^{(j)}$ are called *primary* (by π_j) submodules of the module N . Each primary submodule $M^{(j)}$ is uniquely determined by the module N and the ideal $R\pi_j$ because $M^{(j)}$ consist of those and only those elements $x \in N$ that are annihilated by some power of the element π_j .

Now, it remains to prove the uniqueness of the decomposition of the primary submodules $M^{(j)}$ into a direct sum of indecomposable submodules. This will be done in the next.

Lemma 2.9.5 *Let π be a prime element of the ring R , and M a finitely generated R -module, such that*

$$\begin{aligned} M &= \langle u_1 \rangle \oplus \cdots \oplus \langle u_k \rangle, \\ \text{ann}\langle v_1 \rangle &= R\pi^{n_1}, \dots, \text{ann}\langle v_k \rangle = R\pi^{n_k} \end{aligned} \quad (2.14)$$

be a decomposition of M into a direct sum of indecomposable cyclic submodules. This decomposition is uniquely determined, up to an isomorphism and the order of the direct summands.

Proof. First, let us show that the module M is uniquely determined by the number k ,

i.e., the number of direct summands. The module M uniquely defines the submodule

$$K = \{x \in M \mid \pi x = 0\}.$$

Let us endow K with the structure of a module over the ring $\bar{R} = R/R\pi$ by setting $\bar{\rho}x = \rho x$ for all $x \in M$, and for all $\bar{\rho} = \rho + R\pi \in \bar{R}$. This operation is well defined because the result does not depend on the choice of the coset element. Indeed, for all $\alpha \in R$, we get

$$(\rho + \alpha\pi)x = \rho x + \alpha(\pi x) = \rho x + 0 = \rho x.$$

The ideal $R\pi$ generated by the prime element π is a maximal ideal of the ring R . Indeed, if the ideal $R\pi$ belongs to a larger ideal $R\nu$, then the element ν would be a nontrivial divisor of the element π , which is impossible, since π is a prime element. Hence the quotient ring $\bar{R} = R/R\pi$ is a field. As a result, we see that K is a module over the field \bar{R} . It is easy to check that

$$K = \langle \pi^{n_1-1}u_1 \rangle \oplus \cdots \oplus \langle \pi^{n_k-1}u_k \rangle \cong \bar{R} \dot{+} \cdots \dot{+} \bar{R} \quad (k \text{ summands}).$$

Therefore, the number k is the dimension of the linear space K over the field \bar{R} . Since the submodule K is uniquely determined by the module M , the number k is also uniquely determined by the module M .

Let

$$\begin{aligned} M &= \langle v_1 \rangle \oplus \cdots \oplus \langle v_k \rangle, \\ \text{ann}\langle v_1 \rangle &= R\pi^{m_1}, \dots, \text{ann}\langle v_k \rangle = R\pi^{m_k} \end{aligned} \tag{2.15}$$

be a different decomposition of the module M into a sum of indecomposable cyclic submodules. Let us number the terms in (2.14) and (2.15) so that

$$n_1 \leq n_2 \leq \cdots \leq n_k \quad \text{and} \quad m_1 \leq m_2 \leq \cdots \leq m_k.$$

If $n_i = m_i$ not for all i , then let, for example, $n_1 = m_1, \dots, n_{r-1} = m_{r-1}$, but $n_r < m_r$. Then, from (2.14) we see that the number of indecomposable direct summands in the decomposition of the module $(R\pi^{n_r})M$ is less than $k - r$, and from (2.15) the same number is greater than or equal to $k - r$.

This contradiction shows that $n_i = m_i$ for all $i = 1, \dots, k$ and

$$\langle u_i \rangle \cong R/R\pi^{n_i} \cong \langle v_i \rangle \quad (\text{for all } i = 1, \dots, k).$$

This completes the proof of our Lemma.

This also completes the proof of the Krull-Schmidt theorem.

We now turn to applications of Theorems 2.9.3 and 2.9.4 to the theory of abelian groups. To this end, recall that the additively written abelian group G with a finite number of generators can be regarded as a finitely generated \mathbb{Z} -module. A cyclic submodule of the \mathbb{Z} -module G with annihilator $p^n\mathbb{Z}$, where p is a prime number, is a

cyclic subgroup of the group G of order p^n , and the cyclic submodule of \mathbb{Z} , the module G with zero annihilator, is an infinite cyclic subgroup of the group G . Theorems 2.9.3 and 2.9.4 immediately imply the following theorem.

Theorem 2.9.6 *Every abelian group with a finite number of generators uniquely (up to an isomorphism and an order of summands) decomposes into a direct sum of indecomposable cyclic subgroups which are either infinite cyclic groups or cyclic groups of order $p_i^{n_i}$, where each p_i is a prime number.*

Theorem 2.9.7 In order to obtain all non-isomorphic abelian groups of order n , one should decompose the integer n in all possible ways into the product of powers of prime numbers, not necessarily distinct, arranged in ascending order, and to each such decomposition $n = p_1^{n_1} \cdots p_t^{n_t}$ to associate a direct product of cyclic groups whose orders are $p_1^{n_1}, \dots, p_t^{n_t}$.

To prove this theorem, it suffices to recall that two cyclic groups are isomorphic if and only if their orders coincide, that the order of the direct sum of the two groups is equal to the product of the orders of the subgroups, and apply Theorem 2.9.4.

Examples 2.9.8. 1. Let us find all non-isomorphic abelian groups of order 36. To do this, expand the number 36 into the product of powers of prime numbers in ascending order:

$$36 = 2^2 \cdot 3^2, \quad 36 = 2 \cdot 2 \cdot 3^2, \quad 36 = 2^2 \cdot 3 \cdot 3, \quad 36 = 2 \cdot 2 \cdot 3 \cdot 3.$$

By Theorem 2.9.3, there are 4 non-isomorphic abelian groups of order 36:

$$\begin{aligned} G_1 &= \mathbb{Z}_{2^2} + \mathbb{Z}_{3^2}, & G_2 &= \mathbb{Z}_2 + \mathbb{Z}_2 + \mathbb{Z}_{3^2}, \\ G_3 &= \mathbb{Z}_{2^2} + \mathbb{Z}_3 + \mathbb{Z}_3, & G_4 &= \mathbb{Z}_2 + \mathbb{Z}_2 + \mathbb{Z}_3 + \mathbb{Z}_3, \end{aligned}$$

where by convention \mathbb{Z}_k denotes the cyclic group of order k .

2. In the decomposition of a finitely generated abelian group G into a direct sum of indecomposable cyclic subgroups, the orders of indecomposable cyclic subgroups is uniquely determined (up to an order). These orders are called *invariants* of the group G . An abelian group can be uniquely recovered from its invariants, up to an isomorphism and an order of the direct summands.

An abelian group with invariants $[2, 2^2, 3^3, 7, 11, 17]$ is the following group:

$$\mathbb{Z}_2 + \mathbb{Z}_{2^2} + \mathbb{Z}_{3^3} + \mathbb{Z}_7 + \mathbb{Z}_{11} + \mathbb{Z}_{17}$$

of order $2^3 \cdot 3^3 \cdot 7 \cdot 11 \cdot 17$.

2.10 Normal Form of Matrices over a Field

Let M be a finite-dimensional linear space over the field P with basis e_1, \dots, e_t . Let A be a fixed linear transformation of the space M which in the basis e_1, \dots, e_t is represented by the matrix which by abuse of notation will be also denoted by A . In this section, we show how to choose another basis e_1^*, \dots, e_t^* in which the matrix A of the linear transformation A has the most simple form.

Let us endow the linear space M with a $P[x]$ -module structure by setting:

$$f(x)m = f(A)m \quad \text{for all } f(x) \in P[x] \text{ and } m \in M.$$

The module M is a finitely generated $P[x]$ -module because the P -basis e_1, \dots, e_t is a finite system of generators for the module M . Since the ring $P[x]$ is a principal ideal domain, then, according to Theorem 2.8.1, the $P[x]$ -module M decomposes into a direct sum of cyclic submodules

$$M = M_1 \oplus \dots \oplus M_s,$$

where $M_i = \langle v_i \rangle$, $\text{ann}M_i = P[x]\delta_i(x)$ and $\delta_i | \delta_{i+1}$ for all $i = 1, \dots, s$.

According to Theorem 2.8.1, the last few invariant factors δ_i can be zero. However, in our case, all $\delta_i \neq 0$, that is, $\text{ann}M_i \neq (0)$.

Indeed, in the cyclic submodule $M_i = \langle v_i \rangle$ the elements $v_i, xv_i, x^2v_i, \dots, x^n v_i$, are linearly dependent over the field P . So, there is a finite number $n \in \mathbb{N}$ and simultaneously non-zero numbers $\alpha_0, \alpha_1, \dots, \alpha_n \in P$, such that

$$\alpha_0 v_i + \alpha_1 x v_i + \dots + \alpha_n x^n v_i = 0.$$

Simplifying we get $(\alpha_0 + \alpha_1 x + \dots + \alpha_n x^n)v_i = 0$, whence we see that the nonzero polynomial in parentheses belongs to the annihilator N_i . Hence, $\text{ann}M_i \neq (0)$.

Each submodule M_i is a subspace of the linear space M , invariant under the linear transformation A because $A(m) = xm \in M_i$ for all $m \in M_i$. Therefore, A can be regarded as a linear transformation of the space M_i . The space $M_i = \langle v_i \rangle$ is a cyclic $P[x]$ -module and $\text{ann}\langle v_i \rangle = P[x]\delta_i$, where $\delta_i \in P[x]$. Let us fix the index i , and set

$$\delta_i := x^n + \alpha_{n-1}x^{n-1} + \dots + \alpha_0.$$

In the submodule $M_i = \langle v_i \rangle$, consider the elements

$$\begin{cases} e_0^* & = v_i; \\ e_1^* & = xv_i; \\ e_2^* & = x^2v_i; \\ \vdots & \vdots \quad \vdots \quad \vdots \\ e_{n-1}^* & = x^{n-1}v_i. \end{cases} \quad (2.16)$$

Any element $m \in M_i$ is a P -linear combination of the elements $e_0^*, e_1^*, \dots, e_{n-1}^*$. Indeed, M_i is a cyclic submodule, so for any $m \in M_i$, we have $m = f(x)v_i$ for some $f(x) \in P[x]$. Dividing $f(x)$ by $\delta_i(x)$ with remainder, we get $f = \delta_i q + r$, where

$$r = \beta_0 + \beta_1 x + \dots + \beta_{n-1} x^{n-1}$$

is a polynomial of degree at most n . Obviously,

$$\begin{aligned} m = f(x)v_i &= (\delta_i q + r)v_i = q(\delta_i v_i) + rv_i = 0 + rv_i \\ &= \beta_0 v_i + \beta_1 x v_i + \dots + \beta_{n-1} x^{n-1} v_i \\ &= \beta_0 e_0^* + \beta_1 e_1^* + \dots + \beta_{n-1} e_{n-1}^*. \end{aligned}$$

Moreover, the elements e_0^*, \dots, e_{n-1}^* are linearly independent over the field P .

Indeed, assume that there are nonzero elements $\gamma_0, \dots, \gamma_{n-1} \in P$ such that

$$\gamma_0 e_0^* + \dots + \gamma_{n-1} e_{n-1}^* = 0.$$

Substituting the value e_j^* from the equations (2.16), we see that

$$\begin{aligned} \gamma_0 e_0^* + \dots + \gamma_{n-1} e_{n-1}^* &= \gamma_0 v_i + \gamma_1 x v_i + \dots + \gamma_{n-1} x^{n-1} v_i \\ &= (\gamma_0 + \gamma_1 x + \dots + \gamma_{n-1} x^{n-1}) v_i \\ &= 0, \end{aligned}$$

so

$$0 \neq \gamma_0 + \gamma_1 x + \dots + \gamma_{n-1} x^{n-1} \in \text{ann}\langle v_i \rangle = P[x]\gamma_i(x).$$

However, all nonzero polynomials of the ideal $P[x]\gamma_i(x)$ have degree not less than the degree of the polynomial $\delta_i(x) = x^n + \alpha_{n-1}x^{n-1} + \dots + \alpha_0$ which is n . The resulting contradiction shows that the elements e_0^*, \dots, e_{n-1}^* are linearly independent over the field P .

Summarizing the previous arguments, we can say that the elements e_0^*, \dots, e_{n-1}^*

form a basis of the linear space M_i over the field P , i.e., $M_i = \langle e_0^*, \dots, e_{n-1}^* \rangle_P$

In order to find the matrix A of a linear transformation of the linear space M_i in the basis e_0^*, \dots, e_{n-1}^* , we find the images of the basis vectors (note that $\tilde{A}(m) = xm$, for all $m \in M$):

$$\begin{aligned}
A(e_0^*) &= xe_0^* = xv_i = e_1^*, \\
A(e_1^*) &= xe_1^* = x^2v_i = e_2^*, \\
&\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\
A(e_{n-2}^*) &= xe_{n-2}^* = x^{n-1}v_i = e_{n-1}^*, \\
A(e_{n-1}^*) &= xe_{n-1}^* = x^n v_i = [x^n - \delta_i(x)]v_i \\
&= (-\alpha_0 - \alpha_1 x - \dots - \alpha_{n-1} x^{n-1})v_i \\
&= -\alpha_0 e_0^* - \alpha_1 e_1^* - \dots - \alpha_{n-1} e_{n-1}^*
\end{aligned} \tag{2.17}$$

(in the last equality of (2.17) we used the fact that $\delta_i \in \text{ann}\langle v_i \rangle$, and therefore $\delta_i v_i = 0$). The matrix A of the linear transformation of the space M_i in the basis e_0^*, \dots, e_{n-1}^* has the form

$$F_i = \begin{pmatrix} 0 & 0 & \dots & 0 & -\alpha_0 \\ 1 & 0 & \dots & 0 & -\alpha_1 \\ 0 & 1 & \dots & 0 & -\alpha_2 \\ \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -\alpha_{n-1} \end{pmatrix} \tag{2.18}$$

where $\alpha_0, \dots, \alpha_{n-1}$ are the coefficients of the polynomial $\delta_i(x)$, which generates the ideal $\text{ann}M_i$.

Note that from all polynomials that generate the ideal $\text{ann}M_i$ we have chosen the *normalized* polynomial $\delta_i(x)$ (the polynomial with the coefficient 1 on x^n). The polynomial $\delta_i(x)$ is uniquely determined by the ideal $\text{ann}M_i$.

The matrix F_i in (2.18) is called the *Frobenius cell* corresponding to the polynomial $\delta_i(x)$. It is uniquely determined by the polynomial $\delta_i(x)$: its size is equal to the degree of the polynomial $\delta_i(x)$; all columns, except for the last one, are filled with 0s and 1s so that the 1s are under the main diagonal, and, finally, the last column contains the coefficients of the polynomial $\delta_i(x)$ with opposite signs, starting with the free term.

Let us return now to the space $M = V_1 \oplus \dots \oplus M_s$. If in each subspace M_i we choose bases as described above and unite them, then we obtain a basis of the linear space M . Under the action of the linear transformation A , the basis vectors (2.16) of the subspace M_i are mapped into a linear combinations of same vectors (2.16).

Therefore, the matrix of the linear transformation A of the space M in such a basis has the following cell-diagonal form:

$$F = \begin{pmatrix} F_1 & & & 0 \\ & F_2 & & \\ & & \ddots & \\ 0 & & & F_s \end{pmatrix},$$

where F_i is the transformation matrix of the invariant subspace M_i for each $i = 1, \dots, s$. The matrix F is called the *preliminary normal form* (PNF) of the matrix A .

The original matrix A and the matrix F , being matrices of linear transformation in different bases, are related by the equality $F = C^{-1}AC$, where C is the transition matrix from the basis e_1, \dots, e_t to the basis e_1^*, \dots, e_t^* .

We turn to the practical search for the preliminary normal form F of the matrix A . It is easy to deduce that since $F = C^{-1}AC$, then

$$F - xE = C^{-1}(A - xE)C, \quad (x \in P[x])$$

where E is the unit matrix (of the identity operator). Hence, the matrices $F - xE$ and $A - xE$ with elements from the ring $P[x]$ are equivalent.

By direct verification, we make sure that for each Frobenius cell F_i from (2.18) the matrix $F_i - xE$ is reduced to the normal diagonal form $\text{diag}(1, \dots, 1, \delta_i)$, where

$$\delta_i = \alpha_0 + \alpha_1 x + \dots + \alpha_{n-1} x^{n-1} + x^n.$$

Therefore, the matrix $(F - xE) \sim \text{diag}(1, \dots, 1, \delta_1, \dots, \delta_s)$, where each δ_i is a normalized polynomial generating the ideal $\text{ann}M_i$ for $i = 1, \dots, s$. Moreover, according to Theorem 2.8.1, we see that $\delta_i | \delta_{i+1}$ for $i = 1, \dots, s$ and, consequently,

$$A - xE \sim F - xE \sim \text{diag}(1, \dots, 1, \delta_1, \dots, \delta_s).$$

Since $\delta_i | \delta_{i+1}$, the right-most of these matrices is the NDF of the matrix A .

Therefore, the following is a *rule for finding the preliminary normal form* of a given matrix A :

R1. Construct the characteristic matrix $A - xE$ and by elementary transformations bring it to the normal diagonal form

$$\text{diag}(1, \dots, 1, \delta_1, \dots, \delta_s),$$

where $\delta_i | \delta_{i+1}$ and δ_i is a normalized polynomial of nonzero degree for all $i = 1, \dots, s$.

R2. To each invariant factor δ_i different from 1 assign a Frobenius cell F_i (see (2.18)), the size of which is equal to the degree of the polynomial δ_i so that the last column of F_i contains the coefficients of the polynomial δ_i taken with opposite signs.

The invariant factors of the matrix $A - xE$ are uniquely determined by the matrix A , up to invertible factors (Theorem 2.7.3), which in this case are nonzero elements of the field P . However, if we require that in the normal diagonal form of the matrix $A - xE$, the invariant factors were normalized polynomials, then we see that the normalized invariant factors of the matrix $A - xE$ are uniquely determined by the matrix A . Thus, the PNF F of the matrix A is uniquely determined by the matrix A itself.

In order to obtain from the preliminary form F of the matrix A the *rational (Frobenius) normal form* Φ of the matrix A , we need each cyclic submodule M_i (with annihilators $P[x]\delta_i(x)$) decompose into the sum of indecomposable cyclic submodules in accordance with the decomposition of its annihilator $P[x]\delta_i(x)$ into the product of powers of different prime ideals.

However, such a decomposition of the ideal $P[x]\delta_i(x)$ is uniquely determined by the canonical decomposition of the normalized polynomial

$$\delta_i(x) = \pi_{i1}^{n_{i1}}(x) \cdots \pi_{ik}^{n_{ik}}(x), \quad (2.19)$$

which is unique (Theorem 2.3.10) if we additionally require that each prime polynomial $\pi_{ij}(x)$ be also normalized.

In accordance with decomposition (2.19), each module M_i is decomposed into a direct sum of indecomposable cyclic submodules M_{ij} :

$$M_i = \bigoplus_{j=1}^k M_{ij}, \quad \text{where} \quad \text{ann}M_{ij} = P[x]\pi_{ij}^{n_{ij}}(x).$$

This implies that the module M is represented in the form

$$M = \bigoplus_{j=1}^k M_{ij}. \quad (2.20)$$

If in each cyclic submodule M_{ij} , we choose a P -basis as described above and unite all these bases, then in this P -basis of the space M , the linear transformation A has the following matrix:

$$\Phi = \begin{pmatrix} \ddots & 0 & & \\ 0 & F_{ij} & 0 & \\ & 0 & \ddots & \end{pmatrix},$$

in which F_{ij} is a Frobenius cell corresponding to the polynomial $\pi_{ij}^{n_{ij}}$. The matrix Φ is called the *rational (Frobenius) normal form* of the matrix A .

We have shown above that the invariant factors $\delta_1, \dots, \delta_s$ are uniquely determined by the matrix A . By Theorem 2.3.10 the decomposition of the normalized polynomials δ_i into the product of powers of indecomposable normalized polynomials is uniquely determined. Therefore, the normal form Φ is uniquely determined by the matrix A , up to an order of the diagonal cells F_{ij} .

To actually construct Φ , apply the following rule:

R1. Reduce the matrix $A - xE$ by elementary transformations to the normal diagonal form

$$\text{diag}(1, \dots, 1, \delta_1, \dots, \delta_s),$$

in which each δ_i is a normalized polynomial and $\delta_i | \delta_{i+1}$ for all $i = 1, \dots, s$.

R2. Expand each invariant factor δ_i into a product of powers of indecomposable normalized polynomials (write down the canonical decomposition)

$$\delta_i(x) = \pi_{i1}^{n_{i1}}(x) \cdots \pi_{ik}^{n_{ik}}(x),$$

in which $\pi_{i1}^{n_{i1}}(x), \dots, \pi_{ik}^{n_{ik}}(x)$ are called *elementary divisors* of the matrix A .

R3. To each elementary divisor $\pi_{ij}^{n_{ij}}$, associate a Frobenius cell F_{ij} .

Note also that from the equation $A - xE \sim \text{diag}(1, \dots, 1, \delta_1, \dots, \delta_s)$ we see that the characteristic polynomial is $f(x) = |A - xE| = \delta_1 \cdots \delta_s$.

From the conditions $\delta_i | \delta_{i+1}$ for $i = 1, \dots, s$ we see that

$$M_i = P[x]\delta_i \supseteq \text{ann}M_s = P[x]\delta_s \text{ for each } i.$$

Therefore, the ideal $P[x]\delta_s$ annihilates the entire module $M = M_1 \oplus \cdots \oplus M_s$, that is,

$$P[x]\delta_s = \text{ann}M.$$

The uniquely defined normalized polynomial $\delta_s(x)$ generating the annihilator of the module M is called the *minimal polynomial* of the matrix A . From the equality

$$0 = \delta_s(x)m = \delta_s(A)m \text{ for all } m \in M,$$

it follows that $\delta_s(A)$ is a zero linear transformation. Therefore, $\delta_s(A)$ is a zero matrix.

If in the characteristic polynomial $f(x) = \delta_1(x) \cdots \delta_s(x)$ of the matrix A , instead of x the matrix A is substituted, then we see that

$$f(A) = \delta_1(A) \cdot \delta_2(A) \cdots \delta_s(A) = 0,$$

so, the matrix A is the root of its characteristic polynomial.

If all characteristic roots of the matrix A lie in the field P (it is always so if $P = \mathbb{C}$), then the elementary divisors of $\pi_{ij}^{n_{ij}}(x)$ have the form $(x - \lambda_{ij})^{n_{ij}}$, where $\lambda_{ij} \in P$. In this case, a more convenient basis can be chosen in the cyclic submodules M_{ij} . Fix i and j , and set

$$\pi_{ij}^{n_{ij}}(x) := (x - \lambda)^n, \quad M_{ij} := \langle v \rangle.$$

We choose the vectors

$$(x - \lambda_{ij})^{n-1}v, (x - \lambda_{ij})^{n-2}v, \dots, (x - \lambda)v, v$$

as a new P -basis of M_{ij} . In this basis, the transformation matrix A has the following form:

$$\begin{pmatrix} \lambda & 1 & & 0 \\ & \lambda & 1 & \\ & & \ddots & \ddots \\ & & & \ddots & 1 \\ 0 & & & & \lambda \end{pmatrix} \quad (n \text{ rows}).$$

Such a matrix is called a *Jordan cell* and it is uniquely determined by the polynomial $(x - \lambda)^n$ (the elementary divisor of $\pi_{ij}^{n_{ij}}$) because the size of this matrix is $n \times n$, and on the diagonal there is the root λ of the polynomial $(x - \lambda)^n$. Combining such P -basis of all subspaces M_{ij} , we obtain a new P -bases of the space M , in which the transformation A has the following cell-diagonal matrix:

$$J = \begin{pmatrix} \ddots & 0 & & \\ 0 & J_{ij} & 0 & \\ & 0 & \ddots & \end{pmatrix},$$

where J_{ij} is the Jordan cell corresponding to the elementary divisor of $\pi_{ij}^{n_{ij}}$. The matrix J is called the *Jordan normal form* of the matrix A . The Jordan normal form J of the matrix A is uniquely determined, up to an order of the cells along the diagonal.

The rule for finding the normal form of Jordan is obtained from the rule for

finding the normal form of Frobenius, if the “Frobenius cell F_{ij} ” is replaced by “the “Jordan cell J ”.

Examples 2.10.1. 1. Over the field \mathbb{R} , find the normal Frobenius form F of the following matrix:

$$A = \begin{pmatrix} 2 & -3 & 1 \\ 0 & -1 & 1 \\ 0 & -1 & 0 \end{pmatrix}.$$

We compose the characteristic matrix $A - xE$ and reduce it to the normal diagonal form

$$\text{diag}(1, 1, x^3 - x^2 - x - 2).$$

The factor

$$\delta_1(x) = x^3 - x^2 - x - 2 \in \mathbb{R}[x]$$

can be decomposed into a product of elementary divisors

$$\delta_1(x) = (x^2 + x + 1) \cdot (x - 2) = \pi_{11} \cdot \pi_{12}.$$

The elementary divisors $\pi_{11} = x^2 + x + 1$ and $\pi_{12} = x - 2$ correspond to Frobenius cells

$$F_{11} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}; \quad F_{12} = 2; \quad F = \begin{pmatrix} 0 & -1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

2. If for a matrix A over a field \mathbb{R} , we have

$$A - xE \sim \text{diag}(1, 1, 1, 1, x^2 + 1, x^4 - 1),$$

then

$$\delta_{11} = x^2 + 1 = \pi_{11},$$

$$\delta_{21} = (x^4 - 1) = (x^2 + 1) \cdot (x - 1) \cdot (x + 1) = \pi_{21} \cdot \pi_{22} \cdot \pi_{23}.$$

Frobenius cells have the form

$$F_{11} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad F_{21} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad F_{22} = 1, \quad F_{23} = -1.$$

3. Let A be a matrix over the field \mathbb{C} such that

$$A - xE \sim \text{diag}(1, \dots, 1, (x^4 - 1)^2(x - 1)^2).$$

Obviously,

$$\delta_1 = x^2 + 1 = (x + i)(x - i) = \pi_{11} \cdot \pi_{12},$$

$$\delta_2 = (x^4 - 1)^2(x - 1)^2$$

$$= (x + i)^2(x - i)^2(x + 1)^2(x - 1)^4 = \pi_{21}^2 \cdot \pi_{22}^2 \cdot \pi_{23}^2 \cdot \pi_{24}^4,$$

and in the Frobenius normal form, there are the following cells

$$F_{11} = -i, \quad F_{12} = i, \quad F_{21} = \begin{pmatrix} -i & 1 \\ 0 & -i \end{pmatrix}, \quad F_{22} = \begin{pmatrix} i & 1 \\ 0 & 1 \end{pmatrix},$$

$$F_{23} = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \quad F_{24} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

References

- [1] C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. I.* Wiley Classics Library. John Wiley & Sons, Inc., New York, 1990. With applications to finite groups and orders, Reprint of the 1981 original, A Wiley-Interscience Publication.
- [2] C. W. Curtis and I. Reiner. *Representation theory of finite groups and associative algebras.* AMS Chelsea Publishing, Providence, RI, 2006. Reprint of the 1962 original.
- [3] A. I. Kostrikin and Y. I. Manin. *Linear algebra and geometry*, volume 1 of *Algebra, Logic and Applications*. Gordon and Breach Science Publishers, Amsterdam, english edition, 1997. Translated from the second Russian (1986) edition by M. E. Alferieff.
- [4] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.
- [5] I. R. Shafarevich. Selected chapters from algebra. *Teach. Math.*, 2(1):1–30, 1999. Translated from the Russian.
- [6] I. R. Shafarevich. *Basic notions of algebra*, volume 11 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 2005. Translated from the 1986 Russian original by Miles Reid, Reprint of the 1997 English translation [MR1634541], Algebra, I.
- [7] B. L. van der Waerden. *A history of algebra*. Springer-Verlag, Berlin, 1985. From al-Khwārizmī to Emmy Noether.

UAEU

جامعة الإمارات العربية المتحدة
United Arab Emirates University



UAE UNIVERSITY MASTER THESIS NO. 2022:65

This thesis covers the main theory of modules, and some related topics. Using a theorem on the structure of finitely generated modules over domains of principal ideals is proved. The theory of the structure of normal forms of matrices over various fields is presented as application.

Mariam Mutawa received the Bachelor and Master of Science in Mathematical Sciences in United Arab Emirates University (UAEU).

www.uaeu.ac.ae