Mathematics and Its Applications

Michiel Hazewinkel,
Nadiya Gubareni
and V.V. Kirichenko

Algebras, Rings and Modules

Volume 1

Kluwer Academic Publishers

Algebras, Rings and Modules

Mathematics and Its Applications

Managing Editor:

M. HAZEWINKEL

Centre for Mathematics and Computer Science, Amsterdam, The Netherlands

Volume 575

Algebras, Rings and Modules

Volume 1

by

Michiel Hazewinkel
CWI,
Amsterdam, The Netherlands

Nadiya Gubareni
Technical University of Częstochowa,
Poland

and

V.V. Kirichenko
Kiev Taras Shevchenko University,
Kiev, Ukraine

KLUWER ACADEMIC PUBLISHERS
NEW YORK, BOSTON, DORDRECHT, LONDON, MOSCOW

eBook ISBN: 1-4020-2691-9
Print ISBN: 1-4020-2690-0

Created in the United States of America

Visit Springer's eBookstore at: http://ebooks.springerlink.com
and the Springer Global Website Online at: http://www.springeronline.com

Table of Contents

Preface

Accosiative rings and algebras are very interesting algebraic structures. In a strict sense, the theory of algebras (in particular, noncommutative algebras) originated from a single example, namely the quaternions, created by Sir William R. Hamilton in 1843. This was the first example of a noncommutative "number system". During the next forty years mathematicians introduced other examples of noncommutative algebras, began to bring some order into them and to single out certain types of algebras for special attention. Thus, low-dimensional algebras, division algebras, and commutative algebras, were classified and characterized. The first complete results in the structure theory of associative algebras over the real and complex fields were obtained by T.Molien, E.Cartan and G.Frobenius.

Modern ring theory began when J.H.Wedderburn proved his celebrated classification theorem for finite dimensional semisimple algebras over arbitrary fields. Twenty years later, E.Artin proved a structure theorem for rings satisfying both the ascending and descending chain condition which generalized Wedderburn structure theorem. The Wedderburn-Artin theorem has since become a cornerstone of noncommutative ring theory.

The purpose of this book is to introduce the subject of the structure theory of associative rings. This book is addressed to a reader who wishes to learn this topic from the beginning to research level. We have tried to write a self-contained book which is intended to be a modern textbook on the structure theory of associative rings and related structures and will be accessible for independent study.

The basic tools of investigation are methods from the theory of modules, which, in our opinion, give a very simple and clear approach to both classical and new results. Other interesting tools which we use for studying rings in this book are techniques from the theory of quivers. We define different kinds of quivers of rings and discuss various relations between the properties of rings and their quivers. This is unusual and became possibly only recently, as the theory of quivers is a quite new arrival in algebra.

Some of the topics of the book have been included because of their fundamental importance, others because of personal preference.

All rings considered in this book are associative with a nonzero identity.

The content of the book is divided into two volumes. The first volume is devoted to both the standard classical theory of associative rings and to more modern results of the theory of rings.

A large portion of the first volume of this book is based on the standard university course in abstract and linear algebra and is fully accessible to students in their second and third years. In particular, we do not assume knowledge of any preliminary information on the theory of rings and modules.

A number of notes, some of them of a bibliographical others of a historical nature, are collected at the end of each chapter.

In chapter 1 the fundamental tools for studying rings are introduced. In this chapter we give a number of basic definitions, state several fundamental properties and give a number of different examples. Some important concepts that play a central role in the theory of rings are introduced.

The main objects of chapter 2 are decomposition theorems for rings. In particular, much attention is given to the two-sided Peirce decomposition of rings. In section 2.2. we study semisimple modules which form one of the most important classes of modules and play a distinguished role in the theory of modules. For semisimple rings we prove the fundamental Wedderburn-Artin theorem, which gives the complete classification of such rings. In this chapter there is also provided a brief introduction to the theory of lattices and Boolean algebras. In section 2.4 we introduce finitely decomposable rings and finitely decomposable identity rings and study their main properties. For these rings we prove the decomposition theorems using the general theory of Boolean algebras and the theory of idempotents.

Chapter 3 is devoted to studying Noetherian and Artinian rings and modules. In particular, we prove the famous Jordan-Hölder theorem and the Hilbert basis theorem. The most important part of this chapter is the study of the Jacobson radical and its properties. In this chapter we also prove Nakayama's lemma which is a simple result with powerful applications. Section 3.6 presents a criterion of rings to be Noetherian or Artinian. In section 3.7 we consider semiprimary rings and prove a famous theorem, due to Hopkins and Levitzki, which shows that any Artinian ring is also Noetherian.

Chapter 4 presents the fundamental notions of the theory of homological algebra, such as categories and functors. In particular, we introduce the functor Hom and the tensor product functor and discuss the most important properties of them. In this chapter we also study tensor product of modules and direct and inverse limits.

Chapter 5 gives a brief study of special classes of modules, such as free, projective, injective, and flat modules. We also study hereditary and semihereditary rings. Finally we consider the Herstein-Small rings, which provide an example of rings which are right hereditary but not left hereditary.

Homological dimensions of rings and modules are discussed in chapter 6. In this chapter derived functors and the functors Ext and Tor are introduced and studied. This chapter presents the notions of projective and injective dimensions of modules. We also define global dimensions of rings and give some principal results of the theory of homological dimensions of rings.

In chapter 7 we consider different classes of commutative domains, such as principal ideal domains, factorial rings and Euclidean domains. We study their main properties and prove the fundamental structure theorem for finitely generated modules over principal ideal domains. We also give the main applications of this theorem to the study of finitely generated Abelian groups and canonical forms of

matrices.

Chapter 8 is devoted to studying Dedekind domains and finitely generated modules over them. Besides that, we characterize commutative integral domains that are hereditary and show that they are necessarily Dedekind rings. Finally in this chapter some properties of Prüfer rings are studied.

In chapter 9 we briefly study the main problems of the theory of rings of fractions. We start this chapter with the classical Ore condition and study necessary and sufficient conditions for the existence of a classical ring of fractions. In section 9.2 we introduce prime and semiprime ideals and rings, and consider the main properties of them. Section 9.3 introduces the important notion of Goldie rings and presents the proof of the famous Goldie theorem, which gives necessary and sufficient conditions when a ring has a classical ring of quotients which is a semisimple ring.

We start chapter 10 with introducing some important classes of rings, namely, local and semilocal rings. As a special class of local rings we study discrete valuation rings (not necessarily commutative). Section 10.3 is devoted to the study of semiperfect rings which were first introduced by H.Bass. In this section we consider the main properties of these rings using methods from the theory of idempotents. The next section introduces the notion of a projective cover which makes it possible to study the homological characterization of semiperfect rings. In section 10.4 we introduce the notion of an equivalence of categories and study the properties of it. Of fundamental importance in the study of rings is the famous Morita theorem, which is proved in this chapter.

The last four chapters of this volume are devoted to more recent results: the quivers of semiperfect rings, the structure theory of special classes of rings, such as uniserial, hereditary, serial, and semidistributive rings. Some of the results of these chapters until now have been available only in journal articles.

In chapter 11 we introduce and study different types of quivers for rings. The notion of a quiver for finite dimensional algebra and its representations was introduced by P.Gabriel in connection with a description of finite dimensional algebras over an algebraically closed field with zero square radical. In Gabriel's terminology a quiver means the usual directed graph with multiple arrows and loops permitted. In section 11.1 we introduce the notion of a quiver for a semiperfect right Noetherian ring which coincides with the Gabriel definition of the quiver in the case of finite dimensional algebras. The prime radical and their properties are studied in section 11.2. We define the prime quiver of a right Noetherian ring and prove that a right Noetherian ring A is indecomposable if and only if its prime quiver $PQ(A)$ is connected. In this chapter we prove the annihilation lemma and the Q-Lemma which play the main role in the calculation of a quiver of a right Noetherian semiperfect ring.

A ring is called decomposable if it is a direct sum of two rings, otherwise a ring A is indecomposable. In the theory of finite dimensional algebras an algebra is indecomposable if and only if its quiver is connected. This assertion still

holds for Noetherian semiperfect rings, but it is not true for only right Noetherian semiperfect rings. A serial Herstein-Small ring is a counterexample in this case.

Chapter 12 presents the most basic results for a specific class of rings, namely, two-sided Noetherian serial rings. Serial rings provide the best illustration of the relationship between the structure of a ring and its categories of modules. They were introduced by T.Nakayama inspired by work of K.Asano and G.Köthe. These rings were one of the earliest example of rings of finite representation type; their introduction was fundamental to what has become known as the representation theory of Artinian rings and finite dimensional algebras. In particular, in section 12.2 we prove a decomposition theorem which describes the structure of semiperfect principal ideal rings and which can be considered as a generalization of the classical theorem about the structure of Artinian principal ideal rings. Using the technique of quivers we prove the decomposition theorem which gives the structure of Noetherian serial rings. We also prove the famous Michler theorem about the structure of Noetherian hereditary semiperfect prime rings.

The most basic properties of right Noetherian serial rings are given in chapter 13. In particular, using the technique of matrix problems, we prove the Drozd-Warfield theorem characterizing serial rings in terms of finitely presented modules. Besides, in this section there is proved an implementation of the Ore condition for serial rings. Using the technique of quivers we prove the structure theorem for right Noetherian serial rings. We end this chapter by studying serial right hereditary rings and the structure of Noetherian hereditary semiperfect semiprime rings.

In chapter 14 we study semidistributive rings and tiled orders. For tiled orders over a discrete valuation ring, i.e., for prime Noetherian semiperfect and semidistributive rings, we give a formula for adjacency matrices of their quivers, using exponent matrices.

There is no complete list of references on the theory of rings and modules. We point out only some textbooks and monographs in which the reader can get acquainted with other aspects of the theory of rings and algebras.

We apologize to the many authors whose works we have used but not specifically cited. Virtually all the results in this book have appeared in some form elsewhere in the literature, and they can be found either in the books that are listed in our bibliography at the end of the book, or in those listed in the bibliographies in the notes at the end of each chapter.

In closing, we would like to express our cordial thanks to a number of friends and colleagues for reading preliminary version of this text and offering valuable suggestions which were taken into account in preparing the final version. We are especially greatly indebted to Z.Marciniak, W.I.Suszczanski, M.A.Dokuchaev, V.M.Futorny, A.N.Zubkov and A.P.Petravchuk, who made a large number of valuable comments, suggestions and corrections which have considerably improved the book. Of course, any remaining errors are the sole responsibility of the authors.

Finally, we are most grateful to Marina Khibina for help in preparing the manuscript. Her assistance has been extremely valuable for us.

1. Preliminaries

1.1 BASIC CONCEPTS AND EXAMPLES

We assume the reader is familiar with basic concepts of abstract algebra such as semigroup, group, Abelian group. Let us recall the definition of a ring.

Definition. A **ring** is a nonempty set A together with two binary algebraic operations, that we shall denote by $+$ and $\cdot$ and call addition and multiplication, respectively, such that, for all $a, b, c \in A$ the following axioms are satisfied:

(1) $a + (b + c) = (a + b) + c$ (associativity of addition);

(2) $a + b = b + a$ (commutativity of addition);

(3) there exists an element $0 \in A$, such that $a + 0 = 0 + a = a$ (existence of a zero element);

(4) there exists an element $x \in A$, such that $a + x = 0$ (existence of "inverses" for addition);

(5) $(a + b) \cdot c = a \cdot c + b \cdot c$ (right distributivity);

(6) $a \cdot (b + c) = a \cdot b + a \cdot c$ (left distributivity).

We shall usually write simply ab rather than $a \cdot b$ for $a, b \in A$. One can show that an element $x \in A$ satisfying property (4) is unique. Indeed, if $a + x = 0$ and $a + y = 0$, then $x = 0 + x = (y + a) + x = y + (a + x) = y + 0 = y$. The element x with this property we denote by $-a$.

The group, formed by all elements of a ring A under addition, is called the **additive group of** A. The additive group of a ring is always Abelian.

A trivial example of a ring is the ring having only one element 0. This ring is called the **trivial ring** or **nullring**. Since the trivial ring is not interesting in its internal structure, we shall mostly consider rings having more than one element and therefore having at least one nonzero element. Such a ring is called a **nonzero ring**.

A ring A is called **associative** if the multiplication satisfies the associative law, that is, $(a_1a_2)a_3 = a_1(a_2a_3)$ for all $a_1, a_2, a_3 \in A$.

A ring A is called **commutative** if the multiplication is commutative in A, that is, $a_1a_2 = a_2a_1$ for any elements $a_1, a_2 \in A$; otherwise it is **noncommutative**.

By a multiplicative **identity** of a ring A we mean an element $e \in A$, which is neutral with respect to multiplication, that is, $ae = ea = a$ for all $a \in A$. Notice, that if a nonzero ring has an identity element, then it is uniquely determined. It is usually denoted by 1. In general, a ring need not have an identity. A ring with the multiplicative identity is usually called a **ring with identity** or, for short, a **ring with** 1.

A nonempty subset S of a ring A is said to be a **subring** of A if S itself is a ring under the same operations of addition and multiplication in A. For a ring with 1 a subring is required to have the same identity.

In order to determine whether a set S is a subring of a ring A with 1 it is sufficient to verify the following conditions:

a) the elements 0 and 1 are in S;

b) if $x, y \in S$, then $x - y \in S$ and $xy \in S$.

From now on, if not stated otherwise, by a ring we shall always mean an associative ring with identity $1 \neq 0$.

Let A be a ring. A nonzero element $a \in A$ is said to be a **right zero divisor** if there exists a nonzero element $b \in A$ such that $ba = 0$. Left zero divisors are defined similarly. In the commutative case the notions of right and left zero divisors coincide and we may just talk about zero divisors. A ring A is called a **domain** if $ab \neq 0$ for any nonzero elements $a, b \in A$. In such a ring there are no left (or right) zero divisors.

An element $a \in A$ is said to be **right invertible** if there exists an element $b \in A$ such that $ab = 1$. Such an element b is called a **right inverse** for a. Left invertible elements and their left inverses are defined analogously. If an element a has both a right inverse b and a left inverse c, then $c = c(ab) = (ca)b = b$. In this case we shall say that a is **invertible** or that a is a **unit** and the element $b = c$ is the **inverse** of a. It is easy to see that for any invertible element a its inverse is uniquely determined and it is usually denoted by a^{-1}. If a and b are units in a ring A, then $a^{-1} \cdot a = a \cdot a^{-1} = 1$ and $a \cdot b \cdot (b^{-1} \cdot a^{-1}) = (b^{-1} \cdot a^{-1}) \cdot a \cdot b = 1$, that is, a^{-1} and ab are also units. Therefore in a ring A the units form a group with respect to multiplication, which is called the **multiplicative group** of A and usually denoted by A^* or $U(A)$.

An element e of a ring A is said to be an **idempotent** if $e^2 = e$. Two idempotents e and f are called **orthogonal** if $ef = fe = 0$. It is obvious that the zero and the identity of any ring are idempotents. However, there may exist many other idempotents.

A **division ring** (or a **skew field**) D is a nonzero ring for which all nonzero elements form a group under multiplication; i.e., every nonzero element is invertible. A commutative division ring is called a **field**.

Let a field L contain a field k. In this case we say that the field L is an **extension** of k and that the field k is a **subfield** of L. Evidently, L is a vector space over k. An element $\alpha \in L$ is called **algebraic over the field** k if α is a root of some polynomial $f(x) \in k[x]$.

A field L is called an **algebraic extension** of a field k if every element of L is algebraic over k. An extension L of a field k is called **finite** if L is a finite dimensional vector space over k. The dimension L over k is called the **degree of an extension** and denoted by $[L : k]$. If $[L : k] = n$ then for any element $\alpha \in L$ the elements $1, \alpha, ..., \alpha^n$ are linearly dependent over k, and therefore α is a root of

some polynomial $f(x) \in k[x]$. Thus, any finite extension is algebraic.

Proposition 1.1.1. *Let $L \supset K \supset k$ be a chain of extensions, where K is a finite extension of a field k with a basis $w_1, ..., w_n$, and L is a finite extension of the field K with a basis $\theta_1, ..., \theta_m$. Then $w_i\theta_j$ $(i = 1, ..., n; j = 1, ..., m)$ is a basis of the field L over k. In particular,*

$$[L : k] = [L : K][K : k].$$

The proof consists of a directly checking the fact that the elements $w_i\theta_j$ form a basis of the space L over k and is left to the reader.

An **algebra** over a field k (or k-algebra) is a set A which is both a ring and a vector space over k in such a manner that the additive group structures are the same and the axiom

$$(\lambda a)b = a(\lambda b) = \lambda(ab)$$

is satisfied for all $\lambda \in k$ and $a, b \in A$.

A k-algebra A is said to be **finite dimensional** if the vector space A is finite dimensional over k. The dimension of the vector space A over k is called the **dimension of the algebra** A and denoted by $[A : k]$.

If a field L contains a field k, then L is an algebra over k.

Just like for groups we can introduce the notions of a quotient ring, a homomorphism and an isomorphism of rings.

Definition. A map φ of a ring A into a ring A' is called a **ring morphism**, or simply a **homomorphism**, if φ satisfies the following conditions:
(1) $\varphi(a + b) = \varphi(a) + \varphi(b)$
(2) $\varphi(ab) = \varphi(a)\varphi(b)$
(3) $\varphi(1) = 1$
for any $a, b \in A$.

If a homomorphism $\varphi : A \to A'$ is injective, i.e., $a_1 \neq a_2$ implies $\varphi(a_1) \neq \varphi(a_2)$, then it is called a **monomorphism** of rings. If a homomorphism $\varphi : A \to A'$ is surjective, i.e., for any element $a' \in A'$ there is $a \in A$ such that $a' = \varphi(a)$, then φ is called an **epimorphism** of rings.

If a homomorphism $\varphi : A \to A'$ is a bijection, i.e., it is both a monomorphism and an epimorphism, then it is called an **isomorphism** of rings. If there exists an isomorphism $\varphi : A \to A'$, the rings A and A' are said to be **isomorphic**, and we shall write $A \simeq A'$. Note that then $\varphi^{-1} : A' \to A$ is also a morphism of rings, so that φ is an isomorphism in the category of rings (see Chapter 4) in the categorial sense. In case $A = A'$, φ is called an **automorphism**.

By the **kernel** of a homomorphism φ of a ring A into a ring A' we mean the set of elements $a \in A$ such that $\varphi(a) = 0$. We denote this set $Ker\varphi$. The subset of A' consisting the elements of the form $\varphi(a)$, where $a \in A$, is called the **homomorphic**

image of A under a homomorphism $\varphi : A \to A'$ and denoted $Im\varphi$. It is easy to verify that $Ker\varphi$ and $Im\varphi$ are both closed under the operations of addition and multiplication. The kernel plays an important role in the theory of rings. It is actually an ideal in A according to the following definition.

A subgroup $\mathcal{I}$ of the additive group of a ring A is called a **right** (resp. **left**) **ideal** of A if $ia \in \mathcal{I}$ (resp. $ai \in \mathcal{I}$) for each $i \in \mathcal{I}$ and every $a \in A$. A subgroup $\mathcal{I}$, which is both a right and left ideal, is called a **two-sided ideal** of A, or simply an **ideal**. Of course, if A is commutative, every right or left ideal is an ideal.

Every ring A has at least two trivial ideals, the entire ring A and the zero ideal, consisting of 0 alone. Any other right (resp. left, two-sided) ideal is called a **proper** right (resp. left, two-sided) ideal.

For any family of right ideals $\{\mathcal{I}_i \ : \ i \in I\}$ of a ring A we can define its sum $\sum\limits_{i\in I} \mathcal{I}_i$ as a set of elements of the form $\sum\limits_{i\in I} x_i$, where $x_i \in \mathcal{I}_i$ and all x_i except a finite number are equal to zero for $i \in I$.

We can also define the product of two right ideals $\mathcal{I}$, $\mathcal{J}$ of A as the set of elements of the form $\sum\limits_{i} x_i y_i$, where $x_i \in \mathcal{I}$, $y_i \in \mathcal{J}$ and only a finite number of $x_i y_i$ are not equal to zero.

It is easy to verify that a sum and a product of right ideals are right ideals as well. Similar statements hold of course for left ideals and ideals. In the usual way, we denote $\mathcal{I}\mathcal{I}$ by $\mathcal{I}^2$; and in general for each positive integer $n > 1$ we write $\mathcal{I}^n = \mathcal{I}^{n-1}\mathcal{I}$ for any right ideal $\mathcal{I}$.

For any family of right ideals $\{\mathcal{I}_i \ : \ i \in I\}$ of a ring A we can consider its intersection $\bigcap\limits_{i\in I} \mathcal{I}_i$ as a set of elements $\{x \in A\}$ such that $x \in \mathcal{I}_i$ for any $i \in I$. Obviously, it is a right ideal of A as well. Note that if $\mathcal{I}$ and $\mathcal{J}$ are two-sided ideals, then $\mathcal{I}\mathcal{J} \subseteq \mathcal{I} \cap \mathcal{J}$. If $\mathcal{I}$ and $\mathcal{J}$ are right ideals, then $\mathcal{I}\mathcal{J} \subset \mathcal{I}$, but it is not necessarily true that $\mathcal{I}\mathcal{J} \subset \mathcal{J}$.

The union of two ideals is not necessarily an ideal. However this is true for some particular cases.

Proposition 1.1.2. *Suppose $\{\mathcal{I}_i \ : \ i \in \mathbf{N}\}$ is a family of proper right ideals of a ring A with the property that $\mathcal{I}_n \subseteq \mathcal{I}_{n+1}$ for all $n \in \mathbf{N}$. Then $\mathcal{I} = \bigcup\limits_{n\in\mathbf{N}} \mathcal{I}_n$ is a proper right ideal of A.*

Proof. Suppose $x \in \mathcal{I}$, then there exists $n \in \mathbf{N}$ such that $x \in \mathcal{I}_n$. Therefore for any $a \in A$ we have $xa \in \mathcal{I}_n$ and so $xa \in \mathcal{I}$. If $y \in \mathcal{I}$, then there exists $m \in \mathbf{N}$ such that $y \in \mathcal{I}_m$. Suppose $k = max(n, m)$, then $\mathcal{I}_n \subseteq \mathcal{I}_k$ and $\mathcal{I}_m \subseteq \mathcal{I}_k$. Therefore $x, y \in \mathcal{I}_k$ and $x + y \in \mathcal{I}_k$. Hence, $x + y \in \mathcal{I}$. Thus, $\mathcal{I}$ is an ideal of A. If $\mathcal{I}$ is not proper, then $\mathcal{I} = A$. In particular, $1 \in \mathcal{I}$. But then $1 \in \mathcal{I}_n$ for some $n \in \mathbf{N}$. Since $\mathcal{I}_n$ is proper, this is impossible. We conclude that $\mathcal{I}$ is a proper right ideal of A.

Any proper ideal of a ring A is contained in a larger ideal, namely A itself. If an ideal is so large that it is properly contained only in the ring A, then we call

it **maximal**. More exactly, a right ideal $\mathcal{M}$ of a ring A is called **maximal** in A if there is no right ideal $\mathcal{I}$, different from $\mathcal{M}$ and A, such that $\mathcal{M} \subset \mathcal{I} \subset A$. Maximal ideals are very important in the theory of rings, but unfortunately we do not have any constructive method of obtaining the maximal ideals of a given ring. Only Zorn's lemma shows that, under reasonable conditions, maximal ideals exist.

Definition. A set S is called **partially ordered** or, for short, a **poset** if there is a relation $\leq$ between its elements such that:
P1. $a \leq a$ for any $a \in S$ (reflexivity);
P2. $a \leq b$, $b \leq c$ implies $a \leq c$ for any $a, b, c \in S$ (transitivity);
P3. $a \leq b$, $b \leq a$ implies $a = b$ for any $a, b \in S$ (antisymmetry).
Such a relation $\leq$ is called a **partial order**.

Example 1.1.1.
The usual relation $\leq$ is a partial order on the set of all positive integers.

Example 1.1.2.
Let S be a set. The **power set** $\mathcal{P}(S)$ is the collection of all subsets of S. Then $\mathcal{P}(S)$ is a partially ordered set with respect to the relation of set inclusion.

Example 1.1.3.
Let A be a ring and let S be the set of all its right ideals. Obviously, S is a partially ordered set with respect to the relation of ideal inclusion. Analogously, one may consider the partially ordered sets of left and two-sided ideals.

Let S be a poset and let A be a subset of S. An element $c \in S$ is called an **upper bound** of A if $a \leq c$ for all $a \in A$. Of course, there may be several upper bounds for a particular subset A, or there may be none at all. An element $m \in S$ is called **maximal** if from $m \leq a$ it follows that $m = a$ for all $a \in S$ having this property. In general, not every poset S has maximal elements.

Definition. A partially ordered set S is **linearly ordered** (or a **chain**) if for any two elements $a, b \in S$ it follows that either $a \leq b$ or $b \leq a$.

We can now state Zorn's lemma. Zorn's lemma gives a convenient sufficient condition for the existence of maximal elements.

Zorn's Lemma. *If every chain contained in a partially ordered set S has an upper bound, then the set S has at least one maximal element.*

Zorn's lemma is equivalent, as is well known, to the axiom of choice.

Axiom of choice. *Let I be an indexing set and let $\mathcal{P}_i$ be a nonempty set for all $i \in I$. Then there exists a map f from I to $\bigcup_{I \in I} \mathcal{P}_i$ such that $f(i) \in \mathcal{P}_i$ for all $i \in I$. (This map is called a* **choice function**.*) In other words, the Cartesian product of any nonempty collection of nonempty sets is nonempty.*

We use Zorn's lemma to prove the following statement.

Proposition 1.1.3. *Any proper right ideal $\mathcal{I}$ of a ring A with identity is contained in a maximal proper right ideal.*

Proof. Consider the poset S of all proper right ideals containing $\mathcal{I}$. Since the ring A has an identity, by proposition 1.1.2, the union of any chain of right proper ideals is again a proper right ideal which is an upper bound of this chain. The statement now immediately follows from Zorn's lemma.

Note that all arguments above for right ideals have analogies for left and two-sided ideals.

A right ideal $\mathcal{I}$ of a ring A is **nilpotent** if $\mathcal{I}^n = 0$ for some positive integer $n > 1$. In this case $x_1x_2...x_n = 0$ for any elements x_1, x_2,...,x_n of $\mathcal{I}$.

If A is a ring and $a \in A$, then $\mathcal{I} = aA$ (resp. $\mathcal{I} = Aa$) is a right (resp. left) ideal which is called the **right** (resp. **left**) **principal ideal**, determined by a. A ring, all of whose right (resp. left) ideals are principal, is called a **principal right** (resp. **left**) **ideal ring**. Analogously, $\mathcal{I} = AaA$ is called the **two-sided principal ideal** determined by a and it is denoted by (a). Each element of this ideal has the form $\sum x_iay_i$, where $x_i, y_i \in A$. A ring, all of whose right and left ideals are principal, is called a **principal ideal ring**. A domain, all of whose right and left ideals are principal, is called a **principal ideal domain** or a PID for short.

Proposition 1.1.4. *Let A be a principal ideal ring. Then any family of right (left) ideals $\{\mathcal{I}_i \ : \ i \in \mathbf{N}\}$ of the ring A with the property that $\mathcal{I}_n \subset \mathcal{I}_{n+1}$ for all $n \in \mathbf{N}$ contains only a finite number of ideals, i.e., there is a number $k \in \mathbf{N}$ such that $\mathcal{I}_k = \mathcal{I}_n$ for all $n \geq k$.*

Proof. Let A be a principal ideal ring and suppose we have a family of right ideals $\{\mathcal{I}_i \ : \ i \in \mathbf{N}\}$ of the ring A such that $\mathcal{I}_n \subset \mathcal{I}_{n+1}$ for all $n \in \mathbf{N}$. By proposition 1.1.2, $\mathcal{I} = \bigcup\limits_{i \in \mathbf{N}} \mathcal{I}_i$ is a right ideal of A. Since A is a principal ideal ring, $\mathcal{I}$ is a principal right ideal that has a generator $a \in \mathcal{I}$. Now since $a \in \bigcup\limits_{i \in \mathbf{N}} \mathcal{I}_i$, there exists a number $k \in \mathbf{N}$ such that $a \in \mathcal{I}_k$. We claim that $\mathcal{I}_k = \mathcal{I}_n$ for all $n \geq k$. For if this were not true, then there exists $n > k$ such that $\mathcal{I}_k \subset \mathcal{I}_n$ and $\mathcal{I}_k \neq \mathcal{I}_n$, i.e., the set $X = \mathcal{I}_n \backslash \mathcal{I}_k$ is nonempty. Let $x \in X$. Since $x \in \mathcal{I}_n$, then $x \in \mathcal{I}$, so that $x = ab$ for some $b \in A$. Also, since $\mathcal{I}_k$ is a right ideal and $a \in \mathcal{I}_k$, we have $ab \in \mathcal{I}_k$. Since $x = ab$, $x \in \mathcal{I}_k$. A contradiction.

Let $\mathcal{I}$ be a two-sided ideal of a ring A. Then we can construct a **quotient ring** $A/\mathcal{I}$ by defining it as the set of all cosets of the form $a + \mathcal{I}$ for any $a \in A$ with the following operations of addition and multiplication

$$(a + \mathcal{I}) + (b + \mathcal{I}) = (a + b) + \mathcal{I},$$

$$(a+\mathcal{I})(b+\mathcal{I}) = (ab)+\mathcal{I}.$$

The zero of this ring is the coset $0+\mathcal{I}$, and the identity is the coset $1+\mathcal{I}$.

The map $\pi : A \to A/\mathcal{I}$ defined by $\pi(a) = a+\mathcal{I}$, is an epimorphism of A onto $A/\mathcal{I}$ and called the **natural projection** of A onto $A/\mathcal{I}$.

Example 1.1.4.

The set of all integers $\mathbf{Z}$ forms a commutative ring under the usual operations of addition and multiplication. We shall show that any ideal in $\mathbf{Z}$ is principal. Let $\mathcal{I}$ be an ideal in $\mathbf{Z}$. If $\mathcal{I}$ is the zero ideal, then $\mathcal{I} = (0)$ is the principal ideal generated by 0. If $\mathcal{I} \neq 0$, then $\mathcal{I}$ contains nonzero positive integers. Let n be the smallest positive integer which belongs to the ideal $\mathcal{I}$. Obviously, $(n) \subseteq \mathcal{I}$.

We shall show that $\mathcal{I} \subseteq (n)$ as well. Let $m \in \mathcal{I}$. By the division algorithm there exist integers q and r such that $m = qn + r$ and $0 \leq r < n$. Since $m, n \in \mathcal{I}$ and $r = m - qn$, it follows that $r \in \mathcal{I}$. If $r \neq 0$, then we have a positive integer in $\mathcal{I}$ which is less than n. This contradiction shows that $r = 0$ and $m = qn$. From this equality it follows that $m \in (n)$, so $\mathcal{I} \subseteq (n)$. Therefore $\mathcal{I} = (n)$ is a principal ideal generated by n. So the ring $\mathbf{Z}$ is a commutative principal ideal domain.

Example 1.1.5.

The sets $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ of rational, real and complex numbers are fields.

Example 1.1.6.

Let A be a ring. Then the set

$$Cen(A) = \{x \in A : xa = ax \quad \text{for any } a \in A\}$$

is called the **center** of the ring A. It is easy to verify that $Cen(A)$ is a subring of A. Obviously, $Cen(A)$ is a commutative ring.

Example 1.1.7.

The polynomials in one variable x over a field K form a commutative ring $K[x]$. The field K may be naturally considered as a subring of $K[x]$. We shall show that any ideal in $K[x]$ is also principal. Let $\mathcal{I} \neq 0$ be an ideal in $K[x]$. We choose in $\mathcal{I}$ a polynomial $p(x) = a_0x^n + a_1x^{n-1} + ... + a_n$ $(a_0 \neq 0)$ with the smallest degree $deg(p(x)) = n$. Obviously, $(p(x)) \subseteq \mathcal{I}$. We shall show that $\mathcal{I} \subseteq (p(x))$ as well. Let $f(x)$ be an arbitrary element in $\mathcal{I}$. Then by the division algorithm there exist polynomials $q(x), r(x) \in K[x]$ such that $f(x) = q(x)p(x) + r(x)$ and $0 \leq deg(r(x)) < n$. Since $p(x), f(x) \in \mathcal{I}$ and $r(x) = f(x) - q(x)p(x)$, it follows that $r(x) \in \mathcal{I}$. If $r(x) \neq 0$, then we have the element in $\mathcal{I}$ whose degree is less than n. This contradiction shows that $r(x) = 0$ and $f(x) = q(x)p(x)$. Therefore $f(x) \in (p(x)))$ and $\mathcal{I} \subseteq (p(x))$. Thus, $\mathcal{I} = (p(x))$ is the principal ideal and $K[x]$ is a commutative principal ideal domain.

We can generalize this example. Let A be an arbitrary ring. We can consider $A[x]$, the set of all polynomials in one variable x over A (that is, with coefficients

in A). If the ring A is commutative, then $A[x]$ is also commutative. The identity of A is also the identity of $A[x]$. However, there exist rings A such that not all ideals in $A[x]$ are principal. For example, let $A = \mathbf{Z}$ be the ring of integers and $\mathcal{I}$ be the set of all polynomials with even constant terms. It is easy to see that $\mathcal{I}$ is an ideal in $\mathbf{Z}[x]$ but it is not a principal ideal.

Analogously we can consider the ring $A[x, y]$ of polynomials in two variables x and y with coefficients in a ring A and so on.

Example 1.1.8.

Consider one more generalization of the previous example. Let K be a field and let x be an indeterminate. Denote by $K[[x]]$ the set of all expressions of the form

$$f = \sum_{n=0}^{\infty} a_n x^n, \quad a_n \in K; \quad n = 0, 1, 2, ...$$

If

$$g = \sum_{n=0}^{\infty} b_n x^n, \quad b_n \in K; \quad n = 0, 1, 2, ...$$

is also an element of $K[[x]]$ define addition and multiplication in $K[[x]]$ as follows:

$$f + g = \sum_{n=0}^{\infty} (a_n + b_n) x^n,$$

and

$$fg = \sum_{n=0}^{\infty} d_n x^n,$$

where

$$d_n = \sum_{i+j=n} a_i b_j, \quad n = 0, 1, 2, ...$$

As is natural $f = g$ if and only if $a_n = b_n$ for all n. It is easy to verify that the set $K[[x]]$ forms a commutative ring under the operations of addition and multiplication as specified above, and it is called the **ring of formal power series** over the field K. The elements of K and $K[x]$ themselves can be considered as elements of $K[[x]]$. So, the field K and the polynomial ring $K[x]$ may naturally be considered as subrings of $K[[x]]$. In particular, the identity of K is the identity of $K[[x]]$.

We shall now show that an element $f \in K[[x]]$ is invertible in $K[[x]]$ if and only if $a_0 \neq 0$. Let $f \in K[[x]]$ be invertible, then there exists an element $g \in K[[x]]$ such that $fg = gf = 1$. From the definition of multiplication it follows that $a_0 b_0 = b_0 a_0 = 1$, i.e., $a_0 \neq 0$.

Conversely, suppose that $f \in K[[x]]$ and $a_0 \neq 0$. We are going to show that there exists an element $g \in K[[x]]$ such that $fg = gf = 1$. Consider the following system of equations:

$$\begin{cases} a_0b_0 = 1 \\ a_0b_1 + a_1b_0 = 0 \\ a_0b_2 + a_1b_1 + a_2b_0 = 0 \\ \vdots \\ a_0b_n + a_1b_{n-1} + ... + a_nb_0 = 0 \\ a_0b_{n+1} + a_1b_n + ... + a_nb_1 + a_{n+1}b_0 = 0 \\ \vdots \end{cases}$$

for unknowns $b_0, b_1, ..., b_n, ...$

Since K is a field and $a_0 \neq 0$, from the first equation we have $b_0 = a_0^{-1} \in K$. The second of these equations determines b_1 as follows: $b_1 = -a_0^{-1}a_1b_0$. By induction, if $b_0, b_1, ..., b_n$ have been determined, then b_{n+1} is determined by the last displayed equation. Therefore the element $g = \sum\limits_{n=0}^{\infty} b_n x^n$ is the inverse for f.

We shall show now that any ideal $\mathcal{I}$ in $K[[x]]$ is principal. Let $\mathcal{I} \neq 0$ and $f = \sum\limits_{n=k}^{\infty} a_n x^n$ be an element in $\mathcal{I}$ with the least integer k for which $a_k \neq 0$. Then this element can be written in the form $f = x^k\varepsilon$, where $\varepsilon = \sum\limits_{n=k}^{\infty} a_n x^{n-k}$. From the above it follows that the element ε is invertible. Therefore $x^k \in \mathcal{I}$ and $(x^k) \subseteq \mathcal{I}$. We shall show that $\mathcal{I} \subset (x^k)$. Let $g = \sum\limits_{n=m}^{\infty} b_n x^n \in \mathcal{I}$ and $b_m \neq 0$. Then $g = x^m\xi$, where ξ is invertible and $m \geq k$, therefore $g = x^k x^{m-k}\xi \in (x^k)$, i.e., $\mathcal{I} \subseteq (x^k)$. Thus, every nonzero ideal $\mathcal{I}$ is principal and has the form (x^k) for some nonnegative integer k. Therefore $K[[x]]$ is a principal ideal ring and all ideals in $K[[x]]$ form such a descending chain

$$K[[x]] \supset (x) \supset (x^2) \supset (x^3) \supset ... \supset (x^n) \supset ....$$

Write $M_n = (x^n)$ and $N = \bigcap\limits_{n=0}^{\infty} M_n$. We shall show that $N = 0$. Suppose that $N \neq 0$. Since N is an ideal in $K[[x]]$ and any nonzero ideal in $K[[x]]$ has the form M_n, there exists a positive integer $k > 0$ such that $N = M_k$. Hence $N = M_k \subset M_n$ for any n and, in particular, for $n > k$. A contradiction. Therefore $N = 0$.

Example 1.1.9.

Denote by $\mathbf{Z}_{(p)}$ (p is a prime integer) the set of irreducible fractions $\frac{m}{n}$ in $\mathbf{Q}$ such that $(n, p) = 1$. The set $\mathbf{Z}_{(p)}$ forms the ring under the usual operations of addition and multiplication and it is called the **ring of p-integral numbers**. We shall show that an element $a = \frac{m}{n} \in \mathbf{Z}_{(p)}$ is invertible if and only if $(m, p) = 1$. Obviously, if $(m, p) = 1$ then $b = \frac{n}{m} \in \mathbf{Z}_{(p)}$ and $ab = ba = 1$, i.e., a is invertible and b is an inverse for a. Conversely, let $a = \frac{m}{n}$ be an invertible element in $\mathbf{Z}_{(p)}$, then there exists an element $b = \frac{m_1}{n_1}$ such that $ab = ba = 1$. Hence, $mm_1 = nn_1$.

Since $(n,p)=1$ and $(n_1,p)=1$, we have $(mm_1,p)=1$. Thus, $(m,p)=1$ and $(m_1,p)=1$.

We are going to show that any ideal $\mathcal{I}$ in $\mathbf{Z}_{(p)}$ is principal. Let $\mathcal{I}\neq 0$ and $a=\frac{p^k m}{n}$ be an element in $\mathcal{I}$ with the least integer k for which $(m,p)=1$. Then this element can be written as $a=p^k\varepsilon$, where $\varepsilon=\frac{m}{n}$ and $(m,p)=1$. From above assertions it follows that the element ε is invertible. Therefore $p^k\in\mathcal{I}$ and $(p^k)\subseteq\mathcal{I}$. We shall show that $\mathcal{I}\subseteq(p^k)$.

Let $b=\frac{p^s m}{n}\in\mathcal{I}$ and $(m,p)=1$, $s\geq 0$. Then $b=p^s\xi$, where ξ is invertible and $s\geq k$, therefore $g=p^k p^{s-k}\xi\in(p^k)$, i.e., $I\subseteq(p^k)$. Thus, every nonzero ideal $\mathcal{I}$ is principal and has the form (p^k) for some positive integer k. So, $\mathbf{Z}_{(p)}$ is a principal ideal domain and all its ideals form such a descending chain

$$\mathbf{Z}_{(p)}\supset(p)\supset(p^2)\supset(p^3)\supset\ldots\supset(p^n)\supset\ldots.$$

As in the case of the previous example it is easy to show that $\bigcap\limits_{n=0}^{\infty}(p^n)=0$.[1])

Example 1.1.10.

The set of all square matrices of order n over a division ring D forms the noncommutative ring $M_n(D)$ with respect to the ordinary operations of addition and multiplication of matrices. This ring is usually called the **full matrix ring**. An element of $M_n(D)$ has the form

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix}$$

where all $a_{ij}\in D$. The elements of $M_n(D)$ can also be written in another form. For $i,j=1,2,\ldots,n$ we denote by e_{ij} the matrix with 1 in the (i,j) position and zeroes elsewhere. These n^2 matrices e_{ij} are called the **matrix units** and form a basis of $M_n(D)$ over D, so that an element of $M_n(D)$ can be uniquely written as a linear combination

$$\sum_{i,j=1}^{n} a_{ij}e_{ij}.$$

The elements e_{ij} multiply according to the rule

$$e_{ij}e_{mn}=\delta_{jm}e_{in} \tag{1.1.1}$$

where

$$\delta_{jm}=\begin{cases} 1 & \text{if } j=m \\ 0 & \text{if } j\neq m \end{cases}$$

[1]) $\mathbf{Z}_{(p)}$ is what is called a localization of $\mathbf{Z}$. Quite generally a localization of a PID is a PID. This is just an instance. The proof in general is not more difficult.

is the **Kronecker delta**. The matrix $E_n = e_{11} + e_{22} + ... + e_{nn}$, which has 1 along the principal diagonal and zeroes elsewhere, is the **identity matrix** of $M_n(D)$ and we shall often denote it simply by E if we know the dimension n. Obviously, the elements e_{ii} $(i = 1, 2, ..., n)$ are orthogonal idempotents.

Let $\alpha \in D$, then a matrix of the form αE is often called a **scalar matrix**. Taking into account (1.1.1) it is easy to verify that $e_{ij}\alpha = \alpha e_{ij}$ for any $\alpha \in D$ and $i, j = 1, 2, ..., n$.

In a similar way we may consider the matrix ring $M_n(A)$ with entries in an arbitrary ring A.

Example 1.1.11.

Let K be any associative ring and let G be a multiplicative group. Consider the set KG of all formal finite sums $\sum\limits_{g \in G} a_g g$ with $a_g \in K$. The operations in KG are defined by the formulas:

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g,$$

$$(\sum_{g \in G} a_g g)(\sum_{g \in G} b_g g) = \sum_{h \in G} c_h h,$$

where $c_h = \sum a_x b_y$ with summation over all $(x, y) \in G \times G$ such that $xy = h$. It is easy to verify that KG is indeed an associative ring. This ring is called the **group ring** of the group G over the ring K. Clearly, KG is commutative if and only if both K and G are commutative. Furthermore, if K is a field, then KG is a K-algebra called the **group algebra** of the group G over the field K. If K is a commutative ring with 1, the group ring KG is often called the **group algebra** of the group G over the ring K as well.

Example 1.1.12.

Consider a vector space $\mathbf{H}$ of dimension four over the field $\mathbf{R}$ of real numbers with the basis $\{1, i, j, k\}$. Define the multiplication in $\mathbf{H}$ by means of the following multiplication table:

	1	i	j	k
1	1	i	j	k
i	i	- 1	k	-j
j	j	-k	- 1	i
k	k	j	-i	- 1

It is to be understood that the product of any element in the left column by any element in the top row is to be found at the intersection of the respective row and column. This product can be extended by linearity to all elements of $\mathbf{H}$. An element of $\mathbf{H}$ can be written as $a_0 + a_1 i + a_2 j + a_3 k$, where $a_s \in \mathbf{R}$ for $s = 0, 1, 2, 3$.

Then the associative product law for any elements of $\mathbf{H}$ is given by

$$\begin{aligned}(a_0 + a_1 i + a_2 j + a_3 k)(b_0 + b_1 i + b_2 j + b_3 k) = \\ = (a_0 b_0 - a_1 b_1 - a_2 b_2 - a_3 b_3) \cdot 1 + \\ + (a_0 b_1 + a_1 b_0 + a_2 b_3 - a_3 b_2) i + \\ + (a_0 b_2 - a_1 b_3 + a_2 b_0 + a_3 b_1) j + \\ + (a_0 b_3 + a_1 b_2 - a_2 b_1 + a_3 b_0) k.\end{aligned}$$

It is easy to verify that the set of elements $\mathbf{H}$ forms a noncommutative ring under addition and multiplication defined as above. The identity of this ring is the element $1 + 0i + 0j + 0k$. If $\alpha = a + bi + cj + dk \in \mathbf{H}$, where $a, b, c, d \in \mathbf{R}$, then we define $\overline{\alpha} = a - bi - cj - dk$. It is easy to verify that

$$\alpha\overline{\alpha} = \overline{\alpha}\alpha = a^2 + b^2 + c^2 + d^2 \in \mathbf{R}.$$

If $\alpha \neq 0$ then $\alpha\overline{\alpha}$ is a nonzero real number. Therefore, if $\alpha \neq 0$ then α has an inverse element

$$\alpha^{-1} = (a^2 + b^2 + c^2 + d^2)^{-1}\overline{\alpha} \in \mathbf{H}.$$

Hence, $\mathbf{H}$ is a division ring (more exactly, this is a division algebra over the field $\mathbf{R}$) and it is called the **algebra of real quaternions**. Historically, this algebra was introduced in 1843 by Sir William Rowan Hamilton as the first example of a noncommutative number system. As said before (in the introduction), this example can be with justice considered the origin of noncommutative algebra. However, Hamilton invented it for different reasons. Those came from mechanics. And from that point of view the quaternions are a beautiful container of 3-dimensional vector calculus including scalar and vector product.

Example 1.1.13.

The Cayley algebra (the algebra of octaves or octonions) $\mathbf{O}$ is an 8-dimensional (non-associative) division algebra over the field of real numbers. The Cayley algebra consists of all formal sums $\alpha + \beta e$, where α, β are quaternions and e is a new symbol with $e^2 = -1$, with obvious addition and multiplication by real numbers.

In other words, it is an 8-dimensional vector space over $\mathbf{R}$ with basis $\{1, i, j, k, e, ie, je, ke\}$ and the following multiplication table:

	1	*i*	*j*	*k*	*e*	*ie*	*je*	*ke*
1	*1*	*i*	*j*	*k*	*e*	*ie*	*je*	*ke*
i	*i*	*-1*	*k*	*-j*	*ie*	*-e*	*-ke*	*je*
j	*j*	*-k*	*-1*	*i*	*je*	*ke*	*-e*	*-ie*
k	*k*	*j*	*-i*	*-1*	*ke*	*-je*	*ie*	*-e*
e	*e*	*-ie*	*-je*	*-ke*	*-1*	*i*	*j*	*k*
ie	*ie*	*e*	*-ke*	*je*	*-i*	*-1*	*-k*	*j*
je	*je*	*ke*	*e*	*-ie*	*-j*	*k*	*-1*	*-i*
ke	*ke*	*-je*	*ie*	*e*	*-k*	*-j*	*i*	*-1*

Example 1.1.14.

Division algebras and orthogonal permutations

Let $\mathbf{R}^n$ be the n-dimensional real vector space, and let $\mathbf{e_i} = (0, \dots, 1, \dots, 0)$, $i = 1, \dots, n$, be its standard basis. A linear transformation P: $\mathbf{R}^n \to \mathbf{R}^n$ is called a (signed) **linear permutation** (or simply **permutation**) if for any $\mathbf{a} = (a_1, \dots, a_n) \in \mathbf{R}^n$, $P\mathbf{a} = (\varepsilon_1(P)\alpha_{\pi_{P(1)}}, \dots, \varepsilon_n(P)\alpha_{\pi_{P(n)}})$, where $\pi_P \in \mathbf{S}_n$ is a permutation and $\varepsilon_i(P) \in \{+1, -1\}$. Two linear permutations P and P' are called **orthogonal** if $(P\mathbf{a}, P'\mathbf{a}) = 0$ for every $\mathbf{a} \in \mathbf{R}^n$; $(\mathbf{a}, \mathbf{b})$ being the standard scalar product of $\mathbf{a}, \mathbf{b} \in \mathbf{R}^n$. A set $\mathcal{P} = (P_1, \dots, P_m)$ of (linear) permutations is called an **orthogonal system of permutations** if P_i and P_j are orthogonal for any two distinct $i, j \in \{1, \dots, m\}$. Obviously, $m \leq n$. If $m = n$, then this orthogonal system of permutations is said to be **complete**.

It is clear that, given any orthogonal system of permutations $\mathcal{P} = (P_1, \dots, P_m)$ and any permutation P, one can construct a new orthogonal system $P\mathcal{P} = (PP_1, \dots, PP_m)$. That is why we shall only consider the systems such that $P_1 = E$ (the identity mapping).

Given an orthogonal system of permutations $\mathcal{P} = (P_1, \dots, P_m)$, put $\varepsilon_{ij} = \varepsilon_i(P_j)$ and $p_i = \sum_{j=1}^{n} P_i\mathbf{e}_j$. Then $p_i = (p_{i_1}, \dots, p_{i_m})$ with $p_{i_j} = \varepsilon_{ij}p_{\pi_{ij}}$, where $\varepsilon_{ij} = \varepsilon_j(P_i)$ and $\pi_i = \pi_{P_i}$. Obviously, the system $(p_1, \dots, p_n)$ determines the orthogonal system of permutations $\mathcal{P}$. Note that π_1 is the identity permutation since $P_1 = E$.

To each complete system of orthogonal permutations $\mathcal{P} = (P_1, \dots, P_m)$ we associate an $\mathbf{R}$-algebra (not necessarily associative) $A_\mathcal{P}$ with a basis $\mathbf{e_i}\,(i = 1, \dots, n)$ and the multiplication given by the rule: $\mathbf{e_i a} = P_i\mathbf{a}$. Note that if $P_1 = E$, the vector $\mathbf{e_1}$ is a left unit of this algebra.

Theorem 1.1.5. *For every complete system of orthogonal permutations $\mathcal{P}$, the algebra $A_\mathcal{P}$ is a division algebra i.e., for any $\mathbf{a}, \mathbf{b} \in A_\mathcal{P}$, $\mathbf{a} \neq 0$, each of the equations* (1) $\mathbf{xa} = \mathbf{b}$ *and* (2) $\mathbf{ay} = \mathbf{b}$ *has a unique solution*).

Proof. Since $A_\mathcal{P}$ is finite dimensional, it is enough to prove that one of the equations (1) or (2) has a solution for every $\mathbf{a} \neq 0$ or, what is the same, that the vectors $\mathbf{e_i a}\,(i = 1, \dots, n)$ form a basis of $A_\mathcal{P}$. But in our case the vectors $\mathbf{e_i a} = P_i\mathbf{a}$ are nonzero and pairwise orthogonal. Hence, they form an orthogonal basis of $A_\mathcal{P}$.

A division algebra A is called **alternative** if all its subalgebras generated by two elements are associative. The following finite dimensional algebras over the field of real numbers $\mathbf{R}$ are well-known:

0) the field of real numbers $\mathbf{R}$;

1) the field of complex numbers $\mathbf{C}$;

2) the division ring of quaternions $\mathbf{H}$.

Here is the structure of orthogonal permutations which corresponds to the field of complex numbers $\mathbf{C}$, the division ring of quaternions $\mathbf{H}$ and the Cayley algebra $\mathbf{O}$:

1) the complex numbers $\mathbf{C}$.

Multiplying the complex number $a_1 + a_2 i$ corresponding to the vector $\mathbf{a} = (a_1, a_2)$ by the basic elements 1 and i, we obtain:

$P_1\mathbf{a} = (a_1, a_2)$

$P_2\mathbf{a} = (-a_2, a_1)$.

2) the quaternions $\mathbf{H}$.

Again, multiplying the quaternion $a_1 + a_2 i + a_3 j + a_4 k$ corresponding to the vector $\mathbf{a} = (a_1, a_2, a_3, a_4) \in \mathbf{R}^4$ by the basic elements $1, i, j, k$, we obtain the following permutations in $\mathbf{R}^4$:

$P_1\mathbf{a} = (a_1, a_2, a_3, a_4)$,

$P_2\mathbf{a} = (-a_2, a_1, -a_4, a_3)$,

$P_3\mathbf{a} = (-a_3, a_4, a_1, -a_2)$,

$P_4\mathbf{a} = (-a_4, -a_3, a_2, a_1)$

3) the Cayley algebra $\mathbf{O}$.

Just in the same way one can obtain the following permutations in $\mathbf{R}^8$ (for $\mathbf{a} = (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$):

$P_1\mathbf{a} = (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$,

$P_2\mathbf{a} = (-a_2, a_1, -a_4, a_3, -a_6 a_5, a_8, a_7)$,

$P_3\mathbf{a} = (-a_3, a_4, a_1, -a_2, -a_7, -a_8, a_5, a_6)$,

$P_4\mathbf{a} = (-a_4, -a_3, a_2, a_1, -a_8, a_7, -a_6, a_5)$,

$P_5\mathbf{a} = (-a_5, a_6, a_7, a_8, a_1, -a_2, -a_3, -a_4)$,

$P_6\mathbf{a} = (-a_6, -a_5, a_8, -a_7, a_2, a_1, a_4, -a_3)$,

$P_7\mathbf{a} = (-a_7, -a_8, -a_5, a_6, a_3, -a_4, a_1, a_2)$,

$P_8\mathbf{a} = (-a_8, a_7, -a_6, -a_5, a_4, a_3, -a_2, a_1)$.

Theorem 1.1.6. (J.F.Adams (1960)) *If A is a finite dimensional division algebra over $\mathbf{R}$, then $dim_{\mathbf{R}} A = 2^n$ for $n = 0, 1, 2, 3$.*

Remark. The result of John Frank Adams should not be confused with one of the famous results of A.Ostrowski (around 1917). In its usual formulation this Ostrowski theorem says: If φ is an Archimedean norm on an associative (but not necessarily commutative) field K then there exists an isomorphism of K onto an everywhere dense subfield of $\mathbf{R}$, $\mathbf{C}$, or $\mathbf{H}$ such that φ is equivalent to the norm induced by that of $\mathbf{R}$, $\mathbf{C}$, or $\mathbf{H}$. (See *V.I.Danilov, Norm on a field K, In: M.Hazewinkel(ed.), Encyclopaedia of Mathematics, Vol.6, 461-462, KAP, 1990.*)

In particular if K is complete it is isomorphic to $\mathbf{R}$, $\mathbf{C}$, or $\mathbf{H}$. There is an extension to not necessarily associative fields and then the Cayley numbers turn up as the fourth and last possibility.

As a corollary we obtain the following statement:

Corollary 1.1.7. *There exists no complete system of orthogonal permutations of n-dimensional vectors if $n \neq 1, 2, 4, 8$.*

1.2 MODULES AND HOMOMORPHISMS

One of the most important notions of modern algebra is the notion of a module, which can be considered as a natural generalization of a vector space.

Definition. A **right module over a ring** A (or **right** A**-module**) is an additive Abelian group M together with a map $M \times A \to M$ such that to every pair (m, a), where $m \in M$, $a \in A$, there corresponds a uniquely determined element $ma \in M$ and the following conditions are satisfied:

1. $m(a_1 + a_2) = ma_1 + ma_2$
2. $(m_1 + m_2)a = m_1a + m_2a$
3. $m(a_1a_2) = (ma_1)a_2$
4. $m \cdot 1 = m$

for any $m, m_1, m_2 \in M$ and any $a, a_1, a_2 \in A$.

In a similar way one can define the notion of a **left** A**-module**. We shall sometimes write $M = M_A$ to emphasize the right action of A. If A is a commutative ring and $M = M_A$ then we can make M into a left A-module by defining $am = ma$ for $m \in M$ and $a \in A$. Thus for commutative rings we can write the ring elements on either side. If A is not commutative, in general not every right A-module is also a left A-module. In what follows, by saying an A-module we shall mean a right A-module.

Note that if A is a field, then a right A-module is precisely a right vector space. Formally, the notion of a module is a generalization of the idea of a vector space. In general, the properties of modules can be quite different from the properties of vector spaces.

Example 1.2.1.

Let $M = A$ and as the map $\varphi : M \times A \to M$ we take the usual multiplication, i.e., $\varphi(m, a) = ma \in M$. Then we obtain a right module A_A which is called the **right regular module**. Analogously, we can construct the left regular module ${}_AA$. Therefore any ring A may be considered as a module over itself and any right (left) ideal in A is clearly a right (left) A-module.

Example 1.2.2.

Let $A = \mathbf{Z}$ be the ring of integers. Then any Abelian group G is a $\mathbf{Z}$-module, if we define the map $\varphi : G \times \mathbf{Z} \to G$ as the usual multiplex addition $\varphi(g, n) = gn = g + ... + g \in G$.

Example 1.2.3.

Let G be a primary Abelian group, i.e., every element $g \in G$ has order p^k for some fixed prime integer p and an integer k. Let $\frac{m}{n}$ be an element of $\mathbf{Z}_{(p)}$. Since

$(n,p)=1$, we have $(n,p^k)=1$ as well. Therefore there exist integers x,y such that $nx+p^ky=1$. Thus, for any element $g\in G$ we have $g\cdot 1=g\cdot nx+g\cdot p^ky=g\cdot nx$. So, $g=g\cdot nx=(gx)n$, i.e., the operation $g\cdot\frac{1}{n}=gx$ is well defined in G. Therefore we can define a map $G\times \mathbf{Z}_{(p)}\to G$ by the following rule:

$$g\cdot\frac{m}{n}=(gm)x$$

and the primary Abelian group G can be considered as a $\mathbf{Z}_{(p)}$-module.

Now we introduce the concepts of homomorphisms and isomorphisms for modules.

Definition. A **homomorphism** of a right A-module M into a right A-module N is a map $f:M\to N$ satisfying the following conditions

1. $f(m_1+m_2)=f(m_1)+f(m_2)$ for all $m_1,m_2\in M$;
2. $f(ma)=f(m)a$ for all $m\in M$, $a\in A$.

The set of all such homomorphisms f is denoted by $Hom_A(M,N)$.

If $f,g\in Hom_A(M,N)$ then $f+g:M\to N$ is defined by $(f+g)(m)=f(m)+g(m)$ for all $m\in M$. One can verify that $f+g$ is also a homomorphism and the set $Hom_A(M,N)$ forms an additive Abelian group.

If a homomorphism $f:M\to N$ is injective, i.e., $m_1\neq m_2$ implies $f(m_1)\neq f(m_2)$, then it is called a **monomorphism**. In order to verify that f is a monomorphism of A-modules it is sufficient to show that $f(m)=0$ implies $m=0$. If a homomorphism $f:M\to N$ is surjective, i.e., every element of N is of the form $f(m)$, then f is called an **epimorphism**.

If a homomorphism $f:M\to N$ is bijective, i.e., injective and surjective, then it is called an **isomorphism** of modules. In this case we say that M and N are **isomorphic** and we shall write $M\simeq N$. Isomorphic modules have the same properties and they can be identified. It is easy to check that then $f^{-1}:N\to M$, defined by $f^{-1}(n)=m$ if and only if $f(m)=n$ is also a homomorphism of modules, so that a bijective homomorphism is an isomorphism in the categorical sense.

A nonempty subset N of an A-module M is called an A-**submodule** if N is a subgroup of the additive group of M which is closed under multiplication by elements of A. Note that since A itself is a right A-module, submodules of the regular module A_A are precisely the right ideals of A.

Let N be a submodule of an A-module M. We say that two elements $x,y\in M$ are equivalent if $x-y\in N$. Consider the set M/N of equivalence classes $m+N$, where $m\in M$. We can introduce a module structure on M/N if we define the operations of addition and multiplication by an element $a\in A$ by setting

$$(m+N)+(m_1+N)=(m+m_1)+N,$$

$$(m+N)a=ma+N$$

for all $m, m_1 \in M$.

The A-module M/N is called the **quotient module** of M by N.

Note that the quotient module has a natural map $\pi : M \to M/N$ assigning to each element $m \in M$ the class $m + N \in M/N$. Moreover, it is easy to see that π is an epimorphism of A-modules. This epimorphism is called the **natural projection** of M onto the quotient module M/N.

Let $f : M \to N$ be a homomorphism of A-modules. The set

$$Ker(f) = \{m \in M \ : \ f(m) = 0\}$$

is a submodule of M. It is called the **kernel** of the homomorphism f. Obviously, $f(m_1) = f(m_2)$ holds if and only if $m_1 - m_2 \in Ker(f)$. It is easy to prove that for the natural projection $\pi : M \to M/N$ we have $Ker(\pi) = N$.

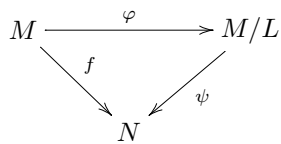
The **image** of a homomorphism f is the set $Im(f)$ of all elements of N of the form $f(m)$. It is easy to verify that $Im(f)$ is a submodule in N. The set

$$Coker(f) = N/Im(f)$$

is called the **cokernel** of the homomorphism f and it is the quotient module of N by $Im(f)$.

Proposition 1.2.1. *Let $f : M \to N$ be a homomorphism of A-modules.*

1. Suppose L is submodule of M contained in $Ker f$. Then there exists a unique homomorphism $\psi : M/L \to N$ such that the diagram



(1.2.1)

is commutative, i.e., $\psi\varphi = f$, where φ is the natural projection.

2. Suppose $g : N_1 \to N$ is a monomorphism with $Im f \subset Im g$, then there exists a unique homomorphism $h : M \to N_1$ such that $f = gh$.

Proof.

1. Let $m + L$ be an arbitrary element of M/L. Since $L \subseteq Ker f$, we can define the map $\psi : M/L \to N$ setting $\psi(m + L) = f(m)$. It is easy to see that ψ is an A-module homomorphism. In fact, $\psi(m + L + m_1 + L) = \psi(m + m_1 + L) = f(m + m_1) = f(m) + f(m_1) = \psi(m + L) + \psi(m_1 + L)$ and $\psi(ma + L) = f(ma) = f(m)a = \psi(m + L)a$. Furthermore, if φ is a natural projection, then $\psi\varphi(m) = \psi(m + L) = f(m)$ for any $m \in M$. So $\psi\varphi = f$ and ψ is the unique such homomorphism.

2. For each $m \in M$, $f(m) \in Im f \subseteq Im g$. Since g is a monomorphism, there exists a unique $n \in N_1$ such that $g(n) = f(m)$. Therefore there is a function defined by $h(m) = n$ such that $f = gh$.

We shall often use the following simple but very useful statement:

Proposition 1.2.2. *Let M and N be A-modules and $f : M \to N$ be a homomorphism of A-modules. Then*
(1) *f is an epimorphism if and only if $Imf = N$;*
(2) *f is a monomorphism if and only if $Kerf = 0$.*

Suppose M is an A-module, I is an index set, and for each $i \in I$, N_i is a submodule of M. Denote by $\sum\limits_{i\in I} N_i$ the set of all finite sums of the form $x_1 + x_2 + ... + x_m$, where each x_k belongs to some N_i. Then $\sum\limits_{i\in I} N_i$ is a submodule of M, and it is called the **sum of the family of submodules** $\{N_i \ : \ i \in I\}$. In particular, if $I = \{1, 2, ..., n\}$ then the sum of submodules may be written as

$$N_1 + N_2 + ... + N_n = \{x_1 + x_2 + ... + x_n \ : \ \ n_i \in N_i \text{ for each } i \in I\}.$$

It is easy to verify, that

$$\bigcap_{i\in I} N_i = \{m \in M \ : \ m \in N_i \text{ for each } i \in I\}$$

is also a submodule of M and it is called the **intersection of the family of submodules** $\{N_i \ : \ i \in I\}$. Note that, if $I = \emptyset$ then $\bigcap\limits_{i\in\emptyset} N_i = M$.

Let $X \subset M$ be a subset, then the set

$$N = \{x_1a_1 + x_2a_2 + ... + x_ka_k \ : \ x_i \in X, a_i \in A \text{ for each } \ i\}$$

is a submodule of M and it is called the **submodule generated by the set** X. If $M = N$, then X is called the **set of generators** of M. If an A-module M has a finite set of generators then it is called **finitely generated**. In this case there exists a set of elements $X = \{m_1, m_2, ..., m_n\} \subset M$ such that every element $m \in M$ can be written as $m = \sum\limits_{i=1}^{n} m_ia_i$ for some $a_i \in A$.

An A-module M is said to be **cyclic** if it generated by one element, i.e., it has an element m_0 such that every element of M is of the form m_0a, where $a \in A$. So in this case $M = m_0A$. The element m_0 is called a **generator** of the module M. Clearly, this notion is analogous to the notion of a principal ideal.

1.3 CLASSICAL ISOMORPHISM THEOREMS

In this section we shall prove the fundamental Noether isomorphism theorems.

Theorem 1.3.1 (Homomorphism theorem). *If M and N are A-modules and $f : M \to N$ is an A-homomorphism, then*

$$M/Ker(f) \simeq Im(f).$$

Proof. Let $m+Ker(f)$ be an element of $M/Ker(f)$. By proposition 1.2.1, there exists a unique A-homomorphism $g : M/Ker(f) \to Imf$, where $g(m+Ker(f)) = f(m)$. We need only show that g is an isomorphism. Since every element of $Im(f)$ has a form $f(m) = g(m + Ker(f))$, g is an epimorphism. Assume that $g(m + Ker(f)) = 0$, then $f(m) = 0$, i.e., $m \in Ker(f)$. Therefore $m + Ker(f) = 0 + Ker(f)$ is the zero class of $M/Ker(f)$. Thus, g is a monomorphism. Hence, g is an isomorphism.

Denote $r.ann(m) = \{a \in A \ : \ ma = 0\}$. It is a right ideal in A and it is called the **right annihilator** of the element m. If $r.ann(m) \neq 0$, then the element m is called a **torsion element**, otherwise it is called a **torsion-free element**. If all elements of an A-module M are torsion, M is called a **torsion module**.

From theorem 1.3.1 it is easy to obtain the following statement.

Corollary 1.3.2. *Every cyclic module is isomorphic to a quotient module of the regular module by some right ideal.*

Proof. Let M be a cyclic A-module with a generator m_0, i.e., $M = m_0A$. We define a map $f : A \to M$ by setting $f(a) = m_0a$. From the module axioms it follows that f is a module homomorphism and, since m_0 is the generator of M, we have $Im(f) = M$. Now theorem 1.3.1 yields $M \simeq A/\mathcal{I}$, where $\mathcal{I} = Ker(f)$ is a right ideal in A. It is easy to see that $Ker(f) = r.ann(m_0)$ and so $m_0A \simeq A/r.ann(m_0)$.

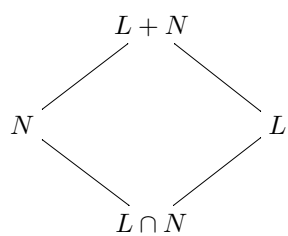
Theorem 1.3.3 (First isomorphism theorem). *If L and N are submodules of an A-module M, then*

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

Proof. Consider the natural projection $\pi : L + N \to (L + N)/N$, then $(L + N)/N = \pi(L+N) = \pi(L)$. So we can consider the restriction $\pi' : L \to (L+N)/N$ which is an epimorphism. Furthermore, the kernel of this map is the set of those elements of L that both map to 0 and belong to L, thus $Ker(\pi') = L \cap N$. By the homomorphism theorem, we have

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

This theorem has a simple illustration in the form of "parallelogram":



where the quotient modules $(L+N)/N$ and $L/(L\cap N)$ are the "opposite sides of the parallelogram". Therefore this theorem is sometimes referred to in the literature as the **"parallelogram law"**.

Consider the natural homomorphism $\pi : M \to M/L$ with the kernel $Ker(\pi) = L$. For a submodule N of M we set $\pi(N) = \{\pi(x) : x \in N\}$. Since N is a submodule and π is a homomorphism, $\pi(x_1) + \pi(x_2) = \pi(x_1 + x_2) \in \pi(N)$ and $\pi(x)a = \pi(xa) \in N$ for all $x_1, x_2 \in N$, $a \in A$. Therefore $\pi(N)$ is a submodule of M/L. If N' is a submodule of M/L we define $\pi^{-1}(N') = \{m \in M : \pi(m) \in N'\}$. Since $\pi(y) = 0 \in N'$ for any $y \in L$, we have $L \subset N'$. Let $m_1, m_2 \in \pi^{-1}(N')$ and $a \in A$, then $\pi(m_1 + m_2) = \pi(m_1) + \pi(m_2) \in N'$ and $\pi(m_1 a) = \pi(m_1)a \in N'$. Hence $\pi^{-1}(N')$ is a submodule of M containing L. Furthermore, every element $\overline{m} \in N'$ is of the form $\pi(m)$, where $m \in M$, and also $m \in \pi^{-1}(N')$ because $\pi(m) = \overline{m} \in N'$. Hence we obtain the formula $N' = \pi(\pi^{-1}(N'))$. Let $L \subset N$. Consider the restriction of π to N. We obtain a homomorphism $\overline{\pi} : L \to M/L$ with the kernel $Ker(\overline{\pi}) = L$ and the image $Im(\overline{\pi}) = \pi(N)$. Obviously, $N \subset \pi^{-1}(\pi(N))$. We now prove the converse inclusion. Let $m \in \pi^{-1}(\pi(N))$, then $\pi(m) = \pi(x)$, where $x \in N$. Therefore $\pi(m - x) = 0$, i.e., $m - x = y \in Ker(\pi) = L$. Since $L \subset N$, we have $m = x + y \in N$. As a result, $\pi^{-1}(\pi(N)) = N$ and, by theorem 1.3.1, $\pi(N) = Im(\overline{\pi}) \simeq N/Ker(\overline{\pi}) = N/L$. So we have proved the following lemma.

Lemma 1.3.4. *Let L be a submodule of M and $\pi : M \to M/L$ be the natural projection. For any submodule $N \subset M$ and any submodule $N' \subset M/L$ we have*
1) *$\pi(N)$ is a submodule of M/L;*
2) *$\pi^{-1}(N')$ is a submodule of M;*
3) *$\pi(\pi^{-1}(N')) = N'$;*
4) *if $L \subset N$ then $\pi^{-1}(\pi(N)) = N$.*

As a corollary of this lemma we have the following theorem.

Theorem 1.3.5 (Second isomorphism theorem). *Let L be a submodule of an A-module M. Then any submodule of the A-module M/L has the form N/L, where $L \subset N \subset M$, and*

$$(M/L)/(N/L) \simeq M/N.$$

Proof. Let $\pi : M \to M/L$ be the natural projection. Then $\pi(M) = M/L$. Consider a submodule N' of $\pi(M)$ and write $N = \pi^{-1}(N')$, which is a submodule of M. Then by the previous lemma $N' = \pi(N) = N/L$. Let $\tau : M/L \to (M/L)/(N/L)$ be the natural projection, then we can consider the homomorphism $\tau\pi : M \to (M/L)/(N/L)$. Since τ and π are epimorphisms, $\tau\pi$ is also an epimorphism. The kernel of the epimorphism $\tau\pi$ is equal to $\pi^{-1}(\pi(N)) = N$ by lemma 1.3.4. Now the homomorphism theorem 1.3.1 yields $(M/L)/(N/L) \simeq M/N$.

Theorem 1.3.6 (Modular law). *Let A, B and C be submodules of M with*

$B \subseteq A$. Then:

$$A \cap (B + C) = B + (A \cap C).$$

Proof. It is clear that $B + (A \cap C) \subseteq A \cap (B + C)$. We shall now show the converse inclusion. Let $x \in A \cap (B + C)$, so that $x = a = b + c$ for suitable $a \in A$, $b \in B$, $c \in C$. Since $B \subseteq A$, we have $c = a - b \in A$, so $c \in A \cap C$ and $x = b + c \in B + (A \cap C)$.

1.4 DIRECT SUMS AND PRODUCTS

Let $M_1, M_2, ..., M_n$ be modules over a ring A. Consider the set M of the n-tuples $(m_1, m_2, ..., m_n)$, where $m_i \in M_i$, and define the operations componentwise:

$$(m_1, m_2, ..., m_n) + (m_1', m_2', ..., m_n') = (m_1 + m_1', m_2 + m_2', ..., m_n + m_n'),$$

$$(m_1, m_2, ..., m_n)a = (m_1 a, m_2 a, ..., m_n a), \quad a \in A.$$

Obviously, M is an A-module under these operations and it is called the **external direct sum** of the modules $M_1, M_2, ..., M_n$ and denoted by $M_1 \oplus M_2 \oplus ... \oplus M_n$, or $\bigoplus_{i=1}^{n} M_i$.

In a similar manner, if $(M_i)_{i \in I}$ is a set of A-modules, then we can introduce the **external direct sum** $\bigoplus_{i \in I} M_i$ as the set of infinite tuples $(m_i)_{i \in I}$ with $m_i \in M_i$ for all $i \in I$ and for almost all $i \in I$ m_i is equal to zero (i.e., only a finite number of m_i are not equal to zero). Furthermore, the operations on this set are defined componentwise, so that $(\oplus_i m_i) + (\oplus_i m_i') = \oplus_i (m_i + m_i')$ and $(\oplus_i m_i)a = \oplus_i (m_i a)$ for all $i \in I$ and any $a \in A$. If there is no assumption on the number of nonzero components then we obtain the **external strong direct sum**. This one is denoted $\prod_{i \in I} M_i$ and is called the **direct product** of the modules M_i. The external direct sum coincides with the direct product of modules M_i, $i \in I$, if the set I is finite, but in general there is not the case. For the finite case we may use either the product or sum notation, i.e., $M_1 \oplus M_2 \oplus ... \oplus M_n = M_1 \times M_2 \times ... \times M_n$.

External direct sums may be described in terms of sets of homomorphisms. Let $M = \bigoplus_{i \in I} M_i$ be the external direct sum of a family of submodules M_i $(i \in I)$. Then for every $i \in I$ there exists the natural embedding $\sigma_i : M_i \to M$ given by $\sigma_i(m_i) = (..., 0, m_i, 0, ...)$ and the natural projection $\pi_i : M \to M_i$ given by $\pi_i(..., m_j, ..., m_i, ...) = m_i$. Clearly, $\pi_i \sigma_i = 1_{M_i}$ and $\pi_i \sigma_j = 0$ for $i \neq j$. Here 1_{M_i} is the identity map of a module M_i. Moreover, if the set I is finite, $I = \{1, 2, ..., n\}$, and $M = M_1 \oplus M_2 \oplus ... \oplus M_n$ then $\sigma_1 \pi_1 + \sigma_2 \pi_2 + ... + \sigma_n \pi_n = 1_M$. If the set I is infinite, then for any $m \in M$ we have $m = \sigma_{i_1} \pi_{i_1} m + \sigma_{i_2} \pi_{i_2} m + ... + \sigma_{i_n} \pi_{i_n} m$.

If $M = \prod_{i \in I} M_i$ is a direct product of modules, then the analogous set of homomorphisms $\{\sigma_i\}$ and $\{\pi_i\}$ defines it. But in this case we have the following conditions:

1) $\pi_i\sigma_i = 1_{X_i}$ and $\pi_i\sigma_j = 0$ for $i \neq j$;

2) if we have a set of elements $\{m_i\}$, where there is only one element $m_i \in M_i$ for each $i \in I$, then there exists a unique element $m \in \prod_{i\in I} M_i$ such that $\pi_i m = m_i$ for each $i \in I$.

Let $A_1, A_2, ..., A_n$ be rings. Consider the set A of elements $a = (a_1, a_2, ..., a_n)$, where $a_i \in A_i$, $i = 1, 2, ..., n$. Let $b = (b_1, b_2, ..., b_n) \in A$. Define the operations of addition and multiplication in A as follows

$$a + b = (a_1 + b_1, a_2 + b_2, ..., a_n + b_n),$$

$$ab = (a_1b_1, a_2b_2, ..., a_nb_n).$$

We shall consider that $a = b$ if and only if $a_i = b_i$ for $i = 1, 2, ..., n$. It is easy to verify that the set A forms a ring under the above operations of addition and multiplication and with identity element $(1, 1, ..., 1)$, where the identity of the ring A_i is at the i-th position. This ring is said to be the **direct product** of the finite number of rings $A_1, A_2, ..., A_n$ and denoted by $A_1 \times A_2 \times ... \times A_n$.

Put $e_i = (0, ..., 1, ..., 0)$, where the identity of the ring A_i is at the i-th position and zeroes elsewhere. Obviously, the elements $e_1, e_2, ..., e_n$ are pairwise orthogonal idempotents and $e_1 + e_2 + ... + e_n$ is the identity of A. But in this particular case the idempotents e_i have an additional property: $e_ia = (0, ..., a_i, ..., 0) = ae_i$ for any $a = (a_1, a_2, ..., a_n) \in A$, i.e., the idempotents e_i are in the center of the ring A. Such idempotents are said to be **central**.

If $A_i = A$ for all $i = 1, 2, ..., n$, then we denote the direct product by $A^n = A \times A \times ... \times A$.

Suppose a ring A is a direct product of rings A_i $(i = 1, 2, ..., n)$ $A = \prod_{i=1}^{n} A_i$. Then the set of elements $(0, ..., 0, a_i, 0, ..., 0) \in A$, where $a_i \in A_i$, forms an ideal $\mathcal{I}_i$ in A. Then the ring A, considered as the regular module, is a direct sum of the ideals $\mathcal{I}_i$. Conversely, let $A = \mathcal{I}_1 \oplus ... \oplus \mathcal{I}_n$ be a decomposition of a ring A into a direct sum of ideals, then $A \simeq \prod_{i=1}^{n} (A/\mathcal{J}_i)$, where $\mathcal{J}_i = \bigoplus_{j\neq i} \mathcal{I}_j$. Furthermore, every ideal $\mathcal{I}_i$ is a ring which is isomorphic to $A/\mathcal{J}_i$.

Definition. A module, which is isomorphic to a direct sum $M_1 \oplus M_2$, where M_1 and M_2 are nonzero modules, is said to be **decomposable**, otherwise it is called **indecomposable**.

Here is an internal characterization of a decomposable module.

Proposition 1.4.1. *Let M_1 and M_2 be submodules of a module M and let $f : M_1 \oplus M_2 \to M$ be the homomorphism defined by $f(m_1, m_2) = m_1 + m_2$. Then the following conditions are equivalent:*

1) *f is an isomorphism;*

2) $M = M_1 + M_2$ *and* $M_1 \cap M_2 = 0$.

Proof.

1) $\Rightarrow$ 2). Let the homomorphism $f : M_1 \oplus M_2 \to M$ defined by $f(m_1, m_2) = m_1 + m_2$ be an isomorphism. Since $M \simeq Imf$, any element $m \in M$ can be written as $m = m_1 + m_2$. Let $x \in M_1 \cap M_2$, then $f(x, -x) = x - x = 0$, i.e., $(x, -x) \in Ker(f)$. Since $Ker(f) = 0$, we have $x = 0$. Therefore $M_1 \cap M_2 = 0$.

2) $\Rightarrow$ 1). Conversely, let $M = M_1 + M_2$ and $M_1 \cap M_2 = 0$, then obviously f is an epimorphism. If $(x, y) \in Ker(f)$, then $x + y = 0$, i.e., $x = -y$. Therefore $x \in M_1 \cap M_2 = 0$, i.e., $Ker(f) = 0$. Hence, f is both an epimorphism and a monomorphism, i.e., f is an isomorphism.

Inspired by this proposition we may introduce the following definition. A module M is said to be the **internal direct sum** of submodules M_1 and M_2 if the equivalent conditions of proposition 1.4.1 are satisfied. The submodules M_1 and M_2 are called **direct summands** of the module M.

The internal direct sum of several modules can be defined in a similar way. For this purpose we shall prove the following statement.

Theorem 1.4.2. *Let M_i $(i \in I)$ be a family of submodules of a module M, and $f : \bigoplus\limits_{i \in I} M_i \to M$ be the homomorphism defined by the formula $f(\oplus_i m_i) = \sum_i m_i$. Then the following conditions are equivalent*:

1) *f is an isomorphism;*

2) $\sum\limits_{i \in I} M_i = M$ *and* $M_i \cap (\sum\limits_{j \neq i} M_j) = 0$ *for any i;*

3) $\sum\limits_{i \in I} M_i = M$ *and* $M_i \cap (\sum\limits_{j < i} M_j) = 0$ *for any $i > 1$.*

Proof.

1) $\Rightarrow$ 2). Since f is an epimorphism, we immediately have $M = M_1 + M_2 + ... + M_n$. Let $x \in M_i \cap (\sum\limits_{j \neq i} M_j)$, then $x = -m_i = \sum\limits_{j \neq i} m_j$, where $m_i \in M_i$. Hence $f(\oplus_i m_i) = \sum_i m_i = 0$. Since f is a monomorphism, $m_i = 0$ for all i, i.e., $M_i \cap (\sum\limits_{j \neq i} M_j) = 0$ for any i.

2) $\Rightarrow$ 3). Trivial.

3) $\Rightarrow$ 1). From the condition $M = \sum\limits_{i \in I} M_i$ we obtain that f is an epimorphism. Let $f(\oplus_i m_i) = 0$ and i be the last position for which $m_i \neq 0$, then $m_i = -\sum\limits_{j < i} m_j \in M_i \cap (\sum\limits_{j < i} M_j)$, and hence $m_i = 0$. This contradiction shows that $m_i = 0$ for all i. Therefore f is a monomorphism and therefore it is an isomorphism.

We say that a module M is the **internal direct sum** of a family of submodules M_i $(i \in I)$ if the equivalent conditions of theorem 1.4.2 are satisfied.

We have introduced two definitions of a direct sum. In fact, there is a close

connection between these notions. The external and internal definitions of a direct sum are equivalent. Let $M = \underset{i\in I}{\oplus} M_i$ be an external direct sum. Then the set of the elements $(..., 0, ..., 0, m_i, 0, ..., 0, ...)$ (all components but the i-th one are 0) forms a submodule M_i' in M and $M_i' \simeq M_i$. Therefore the decomposition $M = \underset{i\in I}{\oplus} M_i'$ gives an internal direct sum. In what follows we shall simply say the **direct sum**, meaning the notion of the external direct sum if we deal with modules, and meaning the notion of the internal direct sum if we deal with submodules.

The following proposition gives the description of modules over a direct product of rings.

Proposition 1.4.3. *Let $A = A_1 \times ... \times A_t$ be a direct product of a finite number of rings. Then any right A-module can be decomposed into a direct sum of A-modules such that each of them is a right A_i-module for some $i = 1, .., t$.*

Proof. Let $1 = e_1 + ... + e_t$ be a decomposition of the identity of a ring A into a sum of mutually orthogonal central idempotents such that $A_i = e_iA = Ae_i$ $(i = 1, ..., t)$.

Let M be a right A-module. We shall show that M decomposes into the direct sum of A_i-modules Me_i $(i = 1, .., t)$. Since e_i is a central idempotent, we have that Me_i is an A-module and $Me_iA_j = 0$ for $i \neq j$. Therefore, indeed, Me_i is an A_i-module.

On the other hand, any element $m \in M$ can be written as $m = m \cdot 1 = me_1 + ... + me_t$. Moreover, if $m = m_1 + m_2 + ... + m_t$, where $m_i \in Me_i$, then $me_i = m_i$. Therefore such a decomposition gives a representation of the module M in the form of a direct sum of modules Me_i $(i = 1, ..., t)$. The proposition is proved.

1.5 FINITELY GENERATED AND FREE MODULES

We have already met with finitely generated modules in section 1.2.1.

We recall that an A-module M is **finitely generated** if there is a finite number of elements $m_1, m_2, ..., m_n$ of M such that every element $m \in M$ can be written as $m = \sum_{i=1}^{n} m_i a_i$, where $a_i \in A$.

The following lemma gives some simple but useful properties of finitely generated modules.

Proposition 1.5.1. *If M is an A-module then:*

(i) *If M is a sum of the finite number of finitely generated modules, then M is a finitely generated module.*

(ii) *If M can be generated by n elements and N is a submodule of M, then M/N can be generated by n elements.*

(iii) *If $M = M_1 \oplus M_2$ and M can be generated by n elements, then M_1 can be generated by n elements.*

Proof.

(i) is obvious.

(ii) By assumption there exist n elements $m_1, ..., m_n \in M$ such that any element $m \in M$ has the form $m = \sum_{i=1}^{n} m_i a_i$ with $a_i \in A$. Then $m + N = \sum_{i=1}^{n} (m_i + N)a_i$, which shows that the n elements $m_1 + N, ..., m_n + N$ generate M/N.

(iii) By theorem 1.3.3, we have $M/M_2 = (M_1 \oplus M_2)/M_2 \simeq M_1/(M_1 \cup M_2 = M_1/0 \simeq M_1$. Now by (ii) M/M_2 can be generated by n elements. Hence, M_1 can be generated by n elements.

Now we introduce a special class of modules that can be considered as the most natural generalization of vector spaces and that play a very important role in the theory of modules.

Definition. An A-module M is called **free** if it is isomorphic to a direct sum of regular modules, i.e., $M \simeq \underset{i \in I}{\oplus} M_i$. where $M_i \simeq A_A$ for all $i \in I$.

Thus, if $A = k$ is a field, every module over A is free, i.e., a vector space.

Free modules play an important role in the theory of modules. It is easy to prove the following proposition.

Proposition 1.5.2. *If an A-module M is finitely generated with n generators, then it is isomorphic to a quotient module of the free module A^n.*

Proof. Let $\{m_1, m_2, ..., m_n\}$ be a set of generators of an A-module M. Define the map $\varphi : A^n \to M$ setting $\varphi(a_1, a_2, ..., a_n) = \sum_{i=1}^{n} m_i a_i$. It is easy to see that φ is an epimorphism and by the homomorphism theorem $M \simeq A^n/Ker(\varphi)$.

Let F be a free A-module and $\alpha : F \to \underset{i \in I}{\oplus} A_A$ be an isomorphism of A-modules. Consider the elements f_i for which $\alpha(f_i) = e_i$ are elements of $\underset{i \in I}{\oplus} A_A$ having the identity of A at the i-th position and zeroes elsewhere. Then any element $f \in F$ can be written as $f = \sum_{i \in I} f_i a_i$, where $a_i \in A$ and only a finite number of a_i are not equal to zero. Suppose $f = 0$. Since $\alpha(f) = \sum_{i \in I} e_i a_i = 0$, all $a_i = 0$. Therefore $f = \sum_{i \in I} f_i a_i = 0$ if and only if all $a_i = 0$. Hence, any element $f \in F$ can be uniquely written as a finite sum $\sum_{i \in I} f_i a_i$ with $a_i \in A$. Such a set of elements $\{ f_i \in F \ : \ i \in I\}$ is called a **free basis** for F.

Conversely, let a module F have a free basis $\{ f_i \in F \ : \ i \in I\}$. Then

$f = \sum_{i\in I} f_i a_i = 0$ if and only if all $a_i = 0$. Therefore a map $\bigoplus_{i\in I} A \to F$ given by $\sum_i a_i \to \sum_i f_i a_i$ is an isomorphism.

Hence, we obtain the following result.

Proposition 1.5.3. *A module F is free if and only if it has a free basis. In particular, F has a finite free basis of n elements if and only if F is isomorphic to A^n.*

The following statement is a generalization of proposition 1.5.2 and shows the importance of free modules.

Proposition 1.5.4. *Any module is isomorphic to a quotient module of a free module.*

Proof. Let M be a right A-module and $\{ m_i \in M \ : \ i \in I \}$ be a set of generators of the module M, i.e., we can write $M = \sum_{i\in I} m_i A$. Let $\varphi_i(a) = m_i a$ be an epimorphism of the module A onto the module $m_i A$. Then there is a homomorphism $\varphi : \bigoplus_{i\in I} A \to M$, which coincides with φ_i on the direct summand with index i. Obviously, φ is an epimorphism. The proposition follows now from the homomorphism theorem.

As one can note the notion of a free basis for a free module is a generalization of a vector space basis. But though for a finite dimensional vector space all bases have the same number of elements, this is not always true for finitely generated free modules over an arbitrary ring. There are rings A for which $A^n \simeq A^m$ and $n \neq m$. But if A is a commutative ring, then any two free bases of a finitely generated free A-module have the same number of elements. This number of elements is called the **rank** of a free module.

Proposition 1.5.5. *If A is a commutative ring, and F is a free A-module, then any two free bases of F have the same cardinal number.*

Proof. By Zorn's lemma, A has a maximal ideal M. Let $\{ f_i \in F \ : \ i \in I\}$ be a free basis of F and denote by F_i an A/M-module $f_i A/f_i AM \simeq A/M$. If $\pi_i : f_i A \to F_i$ is a natural projection, then we denote $\pi_i(f_i) = \bar{f}_i$. Define the homomorphism $\sigma_i : F_i \to F/FM$ by $\sigma_i(\bar{f}_i) = f_i + FM$ and the projection $\tau_i : \sum_{i\in I} F_i \to F_i$. Then it is easy to show that the homomorphism $\sigma = \sum_{i\in I} \sigma_i\tau_i$ gives an isomorphism of A/M-modules $\sum_{i\in I} F_i$ and F/FM. Since M is maximal in A, A/M is a field, and so F/FM is a vector space over A/M. Hence, the isomorphism $F/FM \simeq \sum_{i\in I} F_i$ shows that any free basis of F has cardinal number equal to the dimension of F/FM over the field A/M, and therefore any two free bases of F have the same cardinality.

1.6 NOTES AND REFERENCES

In fact, the term "ring" was introduced by Richard Dedekind and David Hilbert in the end of the 19-th century and only in the concrete setting of rings of algebraic integers, which are commutative rings.

The first abstract definition of a ring was given by A.Fraenkel in 1914 in the paper *Über die Teiler der Null und die Zerlegung von Ringen // J. de Crelle, 145 (1914), 139-176.* Among the main concepts introduced in this paper were "zero divisors" and "regular elements".

What we now call "ring theory" was known in 19th century and in the first decades of the 20th century as the theory of "complex number systems" or "hypercomplex number systems" or as the theory of "linear associative algebras".

The first example of a noncommutative algebra, namely the quaternions, was given by Sir William Hamilton in 1843 (see *W.R.Hamilton, Lecture on quaternions, Dublin, 1853*). Some years later H.Grassmann introduced his algebra, which is now known as Grassmann's algebra, (see *H.Grassmann, Die Ausdehnungslehre von 1862, t.I, Leipzig, 1896* and *Sur les différents genres de multiplication // J. de Grelle, 59 (1855)*). In 1855, in a paper entitled *Remarques sur la notation des functions algebriques*, Sir Arthur Cayley introduced matrices, defined the inverse of a matrix and the product of two matrices, exhibited the relation of matrices to quadratic and bilinear forms. In the paper entitled *A memoir on the theory of matrices // Phil. Trans., 1858*) he also defined the sum of matrices and the product of a matrix by a scalar, and showed that $n \times n$ matrices form an associative algebra. During the next forty years mathematicians introduced other examples of noncommutative algebras.

B.Peirce's paper *Linear Associative Algebra // Amer. J. Math., 1881, V.4, pp.97-229* was of fundamental importance. In this paper Benjamin Peirce classified algebras of dimension ≤ 5 over the field of complex numbers by giving their multiplication tables. What is important in this paper, though, is not the classification but the means used to obtain it. For here B.Peirce introduced concepts and derived results, which were fundamental for subsequent development. Among the conceptual advances in Peirce's work were: an "abstract" definition of a finite dimensional associative algebra, the use of complex coefficients, introduction of nilpotent and idempotent elements, and the " two-sided Peirce decomposition".

The first complete results in the structure theory of associative algebras over the real and complex fields were obtained by T.Molien, E.Cartan and G.Frobenius.

A new departure was provided by Wedderburn's ground breaking paper of 1908 entitled *On hypercomplex numbers// Proc. London Math. Soc., V.6, N.2 (1908), p.77-118.* In this paper previous results were summarized and unified, placing them in a new perspective and providing new directions for subsequent work in the field. The major result in Wedderburn's paper, namely the structure theorem for finite dimensional algebras, was essentially the same as that given by E.Cartan.

There was "merely" an extension of the field of scalars of the algebra of real numbers **R** and complex numbers **C** to an arbitrary field. This extension, however, necessitated a new approach to the subject - a rethinking and reformulation of the major concepts and results of the theory of hypercomplex number systems.

Group algebras were introduced by Sir Arthur Cayley in the paper entitled *On the theory of groups, as depending on the symbolic equation* $\theta^n = 1$*, Phil. Mag., 1854*, in which he defined a finite abstract group. At the end of this paper he gave the definition of a group algebra over the real or complex numbers. The theory of group rings is a specious and very interesting part of algebra which has a number of its own problems. Is was and still stays an area of active study. (For an up-to-date survey see, *S.K.Sehgal, Group rings. In: M.Hasewinkel (ed.), Handbook of Algebra, Vol.3, Elsevier, 2003.*) The most famous results in the theory of group rings and algebras were obtained by G.Frobenius, I.Schur, T.Molien, H.Maschke, C.Rickart, D.S.Passman, E.Zelmanov, K.W.Roggenkamp, A.E.Zalesskij, S.K.Sehgal, Z.Marciniak, J.Krempa, C.Polcino Milies, J.Z.Gonsalves, A.Bovdi, G.Karpilovsky and others. As a current account of the theory of group rings we can recommend the books *D.S.Passman, The algebraic structure of group rings, Wiley, 1977*; *S.K.Sehgal, Topics in group rings, M.Dekker, 1978*; *K.W.Roggenkamp, M.Taylor, Group Rings and Class Groups, Birkhäuser Verlag, Basel, 1992*; *G.Karpilovsky, Unit groups of group rings, Longman, Essex, 1989* and *C.Polcino Milies, S.K.Sehgal, An introduction to group rings. Algebra and Applications, Kluwer Academic Publishers, Dordrecht, 2002.*

The proof of theorem 1.1.6 was given by J.F.Adams in the paper *On the nonexistence of elements of Hopf invariant one// Math. Ann., v.72, 1960.* More information about nonassociative algebras and rings may be found in the book: *K.A.Zhevlakov, A.M.Slin'ko, I.P.Shestakov, A.I.Shirshov, Rings that are nearly associative. Translated from the Russian by Harry F.Smith. Pure and Applied Mathematics, 104. Academic Press, New York-London, 1982.*

The basic notions of the modern theory of rings were formed in the 1920-ies basically in the works of Emmy Noether and Emil Artin.

The concept of a module seems to have made its first appearance in algebra in algebraic number theory. Modules first became an important tool in algebra in the late 1920's largely due to the insights of Emmy Noether, who was the first to realize the potential of the module concept. In particular, she observed that this concept could be used to bridge the gap between two important developments of algebra that had been going on side by side and independently: the theory of representations (=homomorphisms) of finite groups by matrices due to G.Frobenius, W.Burnside, and I.Schur, and the structure theory of algebras due to T.Molien, E.Cartan and J.H.M.Wedderburn.

In 1929 E.Noether in her fundamental paper *Hyperkomplexe Grössen und Darstellungstheorie// Math. Zeitschr. XXX (1929), p.641-692* established a close connection between the theory of algebras and the theory of representations and

in this paper she introduced in general form the notion of homomorphisms of groups with operators and proved for groups with operators the famous "Isomorphism Theorems", which generalized many theoretic-group theorems of W.Krull and O.Yu.Schmidt.

Although the concept of an ideal first appeared in Cartan's work (and, to some extent, also in the Molien and Frobenius papers), but only in the papers of J.H.Wedderburn, E.Noether and E.Artin this notion obtained an essential application in the theory of rings and algebras (see *J.H.N.Wedderburn, On hypercomplex numbers// Proc. London Math. Soc., V.6, N.2 (1908), p.77-118*; *E.Noether, Idealtheorie in Ringenbereichen // Math. Ann, v.83 (1921), p.24-66* and *E.Noether, Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern// Math. Ann., v.96 (1927), p.26-61*).

Among the first monographs in which the ideas of E.Artin, E.Noether, R.Brauer and others were developed one should note the influential book of van der Warden: *Moderne Algebra. I, II, Springer, Berlin, 1931; and the 2d edition, Moderne Algebra, I, 1937; Moderne Algebra, II, 1940* and one of the first monographs of N.Jacobson *The Theory of Rings. American Mathematical Society Surveys, Vol. 2, American Mathematical Society, Providence, 1943.*

2. Decompositions of rings

In many cases the description of modules over a ring is reduced to the description of indecomposable modules and conditions when a given module can be decomposed into a direct sum of indecomposable ones.

Any decomposition of a module into a direct sum of submodules has a close connection with idempotents of the ring. This connection will be considered in the case of the example of the two-sided Peirce decomposition of a ring in section 2.1.

The first example of the decomposition of a module into a direct sum of indecomposable modules was obtained for semisimple modules and their complete description is given by the famous Wedderburn-Artin theorem. Section 2.2 is devoted to the proof of this remarkable theorem.

In section 2.3 we consider one more important class of rings which are called Boolean algebras and their connection with lattices of a special type. Our main goal of this section is to prove Stone's theorem on decomposition for finite Boolean algebras.

In section 2.4 we introduce a class of rings which we call finitely decomposable rings (or, simply FD-rings) and finitely decomposable identity rings (or simply, FDI-rings) and prove decomposition theorems for such rings. To this end we use the results for Boolean algebras taking into account that the set of all central idempotents of a ring forms a Boolean algebra.

2.1 TWO-SIDED PEIRCE DECOMPOSITION OF A RING

In the previous chapter we have already had occasions to use idempotents in rings. Here we present results establishing a close connection between idempotents and decompositions of rings. These results will play a main role in the following chapters of the book.

Definition. Let A be a ring. We recall that an element $e \in A$ is called an **idempotent** if $e^2 = e$. Two idempotents e and f are called **orthogonal** if $ef = fe = 0$. An equality $1 = e_1 + e_2 + ... + e_n$, where e_1, e_2,...,e_n are pairwise orthogonal idempotents, will be called a **decomposition of the identity** of the ring A.

Proposition 2.1.1. *There is a bijective correspondence between decompositions of a ring* $A = \overset{n}{\underset{i=1}{\oplus}} e_iA$ ($A = \overset{n}{\underset{i=1}{\oplus}} Ae_i$) *into a direct sum of right (left) ideals and decompositions* $1 = e_1 + e_2 + ... + e_n$ *of the identity of the ring* A.

Proof. Let $A = \mathcal{I}_1 \oplus ... \oplus \mathcal{I}_m \oplus ...$ be a decomposition of a ring A into a direct sum of nonzero right ideals (the number of summands is not necessarily finite). Suppose $1 = e_{j_1} + ... + e_{j_n}$, where $e_{j_t} \in \mathcal{I}_{j_t}$ and the e_{j_t} are not equal to zero $(t = 1, ..., n)$. Assume there exists $\mathcal{I}_k$ such that $\mathcal{I}_k \neq \mathcal{I}_{j_t}$ for $t = 1, ..., n$. Let $a_k \in \mathcal{I}_k$. Then $a_k = 1 \cdot a_k = \sum\limits_{t=1}^{n} e_{j_t} a_k \in \sum\limits_{t=1}^{n} \mathcal{I}_{j_t}$. Since the sum of ideals $\mathcal{I}_s$ $(s = 1, 2, ..., m, ...)$ is direct, $\mathcal{I}_k = 0$. We obtain a contradiction. Therefore $A = \mathcal{I}_{j_1} \oplus ....\oplus \mathcal{I}_{j_n}$. Renumbering these ideals one may assume that $A = \mathcal{I}_1 \oplus ....\oplus \mathcal{I}_n$ and $1 = e_1 + ... + e_n$. Since the sum is direct, $a_k = e_k a_k$ for every $a_k \in \mathcal{I}_k$. Therefore $e_k = e_k^2$ and $e_i e_j = 0$ for $i \neq j$.

Conversely, let $1 = e_1 + ... + e_n$ be a decomposition of the identity of a ring A. The equality $a = 1 \cdot a = e_1 a + ... + e_n a$ gives a decomposition of the ring A into a sum of ideals $e_1 A, ..., e_n A$. We shall show that this sum is direct. If $a \in e_i A \cap \sum\limits_{j \neq i} e_j A$, then $a = e_i a_i = \sum\limits_{j \neq i} e_j a_j$. Multiplying the last equality on the left side by e_i we obtain $a = e_i a = e_i^2 a_i = \sum\limits_{j \neq i} e_i e_j a_j = 0$, i.e., $a = 0$. From theorem 1.4.2 it follows that we have a decomposition of the ring A into a direct sum of ideals $e_i A$.

The proposition is proved.

We shall denote by $Hom_A(M, N)$ the set of all homomorphisms from an A-module M to an A-module N. If $M = N$, then this set is denoted by $End_A(M)$ and the elements of $End_A(M)$ are called **endomorphisms** of the module M. In this case we can define operations of addition and multiplication in the usual way:

$$(\alpha + \beta)m = \alpha m + \beta m,$$

$$(\alpha\beta)m = \alpha(\beta m)$$

for any $\alpha, \beta \in End_A(M)$ and $m \in M$.

The set of all endomorphisms of the module M forms a ring with respect to these operations. This ring is called the **endomorphism ring** of the module M. The invertible elements of this ring are the **automorphisms** of M.

An important role in the structural theory of rings is played by the circumstance that a ring may be considered as a module over itself and the fact that $A \simeq End_A(A)$, as will be proved below.

Theorem 2.1.2. *Let e and f be idempotents of a ring A. Then there is an isomorphism between the additive groups $Hom_A(eA, fA)$ and fAe. If $f = e$, then $End_A(eA)$ is a ring which isomorphic to eAe. In particular, $A \simeq End_A(A)$.*

Proof. If $\psi \in Hom_A(eA, fA)$, then for some $a \in A$ we have $\psi(e) = fa$. Since ψ is a homomorphism of modules, $\psi(e) = \psi(e^2) = \psi(e)e = fae \in fAe$. Therefore we can define the map $\theta : Hom_A(eA, fA) \to fAe$ by the formula $\theta(\psi) = \psi(e)$. From the above it follows that $\theta(\psi) = fae \in fAe$. It is easy to verify that θ

is a homomorphism of groups. We shall show that it is an isomorphism. Let $\theta(\psi) = 0$. Then $\psi(ea_1) = \psi(e)a_1 = 0$ for any $a_1 \in A$. Hence $\psi = 0$, i.e., θ is a monomorphism. For any $fae \in fAe$ we can construct a homomorphism $\psi \in Hom_A(eA, fA)$ by setting $\psi(e) = fa$ and a homomorphism θ by setting $\theta(\psi) = fae$. So θ is an epimorphism and therefore θ is an isomorphism.

Taking $f = e$ we have a group isomorphism $\theta : End_A(eA) \to eAe$. We are going to show that θ preserves multiplication. Let $\psi, \psi_1 \in End_A(eA)$ and $\psi(e) = ea$, $\psi_1(e) = ea_1$. Then $\theta(\psi) = ea$ and $\theta(\psi_1) = ea_1$. Since $\psi\psi_1(e) = \psi(ea_1) = \psi(e)a_1 = \psi(e^2)a_1 = \psi(e)ea_1 = eaea_1$, we have $\theta(\psi\psi_1) = \psi\psi_1(e) = eaea_1 = \theta(\psi)\theta(\psi_1)$, as desired.

Taking $e = 1$ we obtain $End_A(A) \simeq A$.

Let $1 = e_1 + ... + e_n$ be a decomposition of the identity of a ring A and let $A = e_1A \oplus ... \oplus e_nA$ be a corresponding decomposition of the ring A into a direct sum of right ideals. For any element $a \in A$ we get $a = 1 \cdot a \cdot 1 = (e_1 + ... + e_n)a(e_1 + ... + e_n) = \sum\limits_{i,j=1}^{n} e_iae_j$. It is not difficult to verify that such a decomposition defines a decomposition of the ring A into a direct sum of Abelian groups e_iAe_j $(i, j = 1, 2, ..., n)$:

$$A = \bigoplus_{i,j=1}^{n} e_iAe_j.$$

Elements of $A_{ij} = e_iAe_j$ will be denoted by a_{ij}. It is convenient to write any element $a \in A$ as a matrix

$$a = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix},$$

where $a_{ij} = e_iae_j \in A_{ij}$. So the ring A can be represented as a matrix ring

$$A = \begin{pmatrix} A_{11} & A_{12} & \dots & A_{1n} \\ A_{21} & A_{22} & \dots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n2} & \dots & A_{nn} \end{pmatrix}$$

with the usual operations of addition and multiplication. This decomposition is called the **two-sided Peirce decomposition**, or simply the **Peirce decomposition** of the ring A. Note that, in view of theorem 2.1.2, the elements of e_iAe_j are naturally identified with homomorphisms from e_jA to e_iA.

Proposition 2.1.3. *Let $M = M_1 \oplus ... \oplus M_n$ be a decomposition of an A-module M into a direct sum of mutually isomorphic submodules $M_1 \simeq M_2 \simeq ... \simeq$*

M_n. Then the ring of endomorphisms of the module M is isomorphic to the ring $M_n(End_A(M_1))$ of all square matrices of order n with entries in $End_A(M_1)$.

Proof. The projection π_i of the module M onto the i-th direct summand M_i is, obviously, an idempotent of the ring $End_A(M)$, and moreover for $1 \in End_A(M)$ we have the decomposition $1 = \pi_1 + ... + \pi_n$. Consider the corresponding two-sided Peirce decomposition of the ring $End_A(M)$:

$$End_A(M) = \bigoplus_{i,j=1}^{n} \pi_i End_A(M) \pi_j.$$

In accordance with this decomposition any element $\varphi \in End_A(M)$ has the form

$$\varphi = \begin{pmatrix} \varphi_{11} & \varphi_{12} & \cdots & \varphi_{1n} \\ \varphi_{21} & \varphi_{22} & \cdots & \varphi_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_{n1} & \varphi_{n2} & \cdots & \varphi_{nn} \end{pmatrix},$$

where $\varphi_{ij} = \pi_i \varphi \pi_j$. The elements φ_{ij} are naturally considered as homomorphisms of the module M_j to the module M_i. Let us fix isomorphisms $\mu_i : M_1 \longrightarrow M_i$ and assign to the matrix $\varphi = (\varphi_{ij})$ the matrix $\hat{\varphi} = (\mu_i^{-1} \varphi_{ij} \mu_i) \in M_n(End_A(M_1))$. Clearly, this map yields an isomorphism between the rings $End_A(M)$ and $M_n(End_A(M_1))$.

2.2 THE WEDDERBURN-ARTIN THEOREM

In this section we shall study a most important class of rings which are called semisimple. Historically the first full classification of rings was obtained for semisimple rings. We shall prove the fundamental Wedderburn-Artin theorem which gives the complete description of these rings and which is one of the earliest classification theorems in noncommutative ring theory.

The following two definitions are fundamental in the theory of modules.

Definition. A nonzero module M is called **simple** (or **irreducible**) if it has exactly two submodules (the two trivial submodules M and the zero module). A module M is called **semisimple** (or **completely reducible**) if it can be decomposed into a direct sum of simple modules.

A ring A is called a **right** (resp. **left**) **semisimple** if it is semisimple as a right (resp. left) module over itself. Since A has an identity and any right submodule of A is just a right ideal, A is right semisimple if A is a direct sum of a finite number of simple right ideals.

The proof of the Wedderburn-Artin theorem is based on the following fundamental result which is known as Schur's lemma.

Proposition 2.2.1 (Schur's lemma). *Any nonzero homomorphism between simple modules is an isomorphism. In particular, the endomorphism ring of a simple module is a division ring.*

Proof. Let $f : U \to V$ be a homomorphism from a simple module U to a simple module V. Since $Kerf$ and Imf are submodules of U and V, respectively, $f \neq 0$ implies $Kerf \neq U$ and $Imf \neq 0$. Since U and V are simple modules, $Kerf = 0$ and $Imf = V$, i.e., f is both a monomorphism and an epimorphism, hence f is an isomorphism.

Theorem 2.2.2 (Wedderburn-Artin). *The following conditions are equivalent for a ring A:*

(a) *A is right semisimple;*

(b) *A is isomorphic to a direct sum of a finite number of full matrix rings over division rings;*

(c) *A is left semisimple.*

Proof.

$(a) \Rightarrow (b)$. By definition, a ring A as the regular right A-module decomposes into a finite direct sum of simple right modules. Grouping isomorphic modules together we can consider that the decomposition has the form $A = P_1^{n_1} \oplus ... \oplus P_s^{n_s}$, where the modules $P_1, ..., P_s$ are mutually nonisomorphic simple right A-modules. Let $1 = f_1 + ... + f_s$ be a decomposition of the identity of the ring A such that $f_iA = P_i^{n_i}$ $(i = 1, 2, ..., s)$. By Schur's lemma (taking into account theorem 2.1.2) $f_iAf_j = 0$ for $i \neq j$ and f_iAf_i are rings for $i, j = 1, 2, ..., s$. Therefore the ring A decomposes into a direct sum of rings $f_iAf_i \simeq P_i^{n_i}$ $(i = 1, .., s)$. In view of theorem 2.1.2 and proposition 2.1.3, $f_iAf_i \simeq M_{n_i}(End_A(P_i))$. Since by Schur's lemma $End_A(P_i)$ is a division ring, implication $(a) \Rightarrow (b)$ is proved.

In a similar way implication $(c) \Rightarrow (b)$ can be proved.

$(b) \Rightarrow (a)$. To prove this implication it suffices to show that $A = M_n(D)$, where D is a division ring, is a right semisimple ring. Denote by e_{ij} the matrix units of the full matrix ring $M_n(D)$ (see example 1.1.10). Obviously, $A = \oplus_{i=1}^{n} e_{ii}A$. We shall show that the right ideal $e_{ii}A$ is a simple A-module. Denote, for short, $e_{ii}A = V$. Let U be a nonzero A-submodule of V, $a \in U$ and $a \neq 0$,

$$a = \begin{pmatrix} 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix} = \sum_{k=1}^{n} e_{ik}\alpha_k, \quad \text{where} \quad \alpha_k \in D.$$

Since $a \neq 0$, there exists an index m such that $\alpha_m \neq 0$.

Then $a\alpha_m^{-1}e_{mm} = e_{im}$ and any element $b = \sum\limits_{k=1}^{n} e_{ik}\beta_k \in V$, where $\beta_k \in D$, can

be written in the form $b = \sum_{k=1}^{n} e_{ik}\beta_k = \sum_{k=1}^{n} e_{im}e_{mk}\beta_k = a\alpha_m^{-1}e_{mm}\sum_{k=1}^{n} e_{mk}\beta_k$, i.e., b belongs to the ideal generated by the element $a \in U$. Therefore $V \subset U$, and hence we obtain that $V = U$, i.e., V is a simple A-module and the ring $M_n(D)$ is semisimple.

We can also note that all modules $e_{ii}A$ $(i = 1, ..., n)$ are mutually isomorphic. Indeed, the multiplication on the left by the element e_{ij} of the elements of the module $e_{jj}A$ gives a nonzero homomorphism of the module $e_{jj}A$ to the module $e_{ii}A$, which is an isomorphism by Schur's lemma.

$(b) \Rightarrow (c)$. The ring $A = M_n(D)$ decomposes into a direct sum of left ideals $Ae_{ii} : A = \bigoplus_{i=1}^{n} Ae_{ii}$. Just in the same way as in the proof of the implication $(b) \Rightarrow (a)$ it can be shown that all left modules Ae_{ii} $(i = 1, ..., n)$ are simple and mutually isomorphic.

The theorem is proved.

In view of this theorem, we shall say that A is a **semisimple ring** if the equivalent conditions of theorem 2.2.2 are satisfied.

Definition. A ring is called **simple** if it has no two-sided ideals different from zero and the ring itself.

Proposition 2.2.3. *The ring $M_n(D)$, where D is a division ring, is simple.*

Proof. Let $\mathcal{I}$ be a nonzero two-sided ideal of A and let $m = (m_{ij})$ be a nonzero element of $\mathcal{I}$. Suppose that $m_{kl} \neq 0$, then for every $i = 1, 2, ..., n$ we have $e_{ik}m_{kl}e_{kl} = e_{ik}e_{kl}m_{kl} = e_{il}m_{kl} \neq 0$. Therefore $e_{ik}m \neq 0$. Since $e_{ik}m \in \mathcal{I} \cap e_{ii}A$, we have $\mathcal{I} \cap e_{ii}A \neq 0$ for any i. Taking into account that $e_{ii}A$ is simple and $\mathcal{I} \cap e_{ii}A \subset e_{ii}A$, $\mathcal{I} \cap e_{ii}A \subset \mathcal{I}$ we obtain $\mathcal{I} \cap e_{ii}A = e_{ii}A \subset \mathcal{I}$ for any i. Therefore $A = \sum_{i=1}^{n} e_{ii}A \subset \mathcal{I}$, i.e., $A = \mathcal{I}$, as required.

Proposition 2.2.4. *The following conditions are equivalent for an A-module M:*

(a) *M is a sum of some family of simple submodules*;

(b) *M is a semisimple module;*

(c) *any submodule N of M is a direct summand in M, i.e., there exists a submodule $N' \subset M$ such that $M = N \oplus N'$.*

Moreover, any submodule and any quotient module of a semisimple module is semisimple.

Proof.

$(a) \Rightarrow (b)$. Let $M = \sum_{i \in I} M_i$ be a sum of simple submodules. Then there exists an index subset $J \subset I$ such that $M = \sum_{j \in J} M_j$ is a direct sum of submodules.

Indeed, let J be a maximal subset in I such that $\sum\limits_{j\in J} M_j$ is a direct sum. Since M_i is a simple module, the intersection of $\sum\limits_{j\in J} M_j$ with M_i is either equal to zero or coincides with M_i. Hence, we may conclude that either $M_i \subset \sum\limits_{j\in J} M_j$ or the sum $\sum\limits_{j\in J} M_j + M_i$ is a direct one, and the last contradicts the maximality of the set J.

$(b) \Rightarrow (c)$. Suppose N is a submodule of a module M and J is a maximal index subset in I such that the sum $N + \sum\limits_{j\in J} M_j$ is direct. The same arguments as above show that $N + \sum\limits_{j\in J} M_j = M$.

$(c) \Rightarrow (a)$. We shall show that any nonzero submodule N of an A-module M contains a simple submodule. Let $n \in N$ and $n \neq 0$. The kernel of the homomorphism $A \to nA$, for which $a \mapsto na$, is a right ideal X in the ring A. Since $X \neq A$, by proposition 1.1.3, there exists a maximal right ideal Y of A such that $X \subset Y$. Then Y/X is a maximal submodule in A/X. Therefore nY is a maximal submodule in nA. Then, by assumption, there exists a submodule M' of M such that $M = nY \oplus M'$. Let $na \in nA$, then $na = ny + m'$, where $m' \in M'$. This gives a direct decomposition $nA = nY \oplus (M' \cap nA)$ because $m' \in nA$. Since nY is a maximal submodule in nA, $M' \cap nA$ is a simple submodule in N.

Let M_0 be the sum of all simple submodules of the module M. If $M_0 \neq M$, then, by assumption, $M = M_0 \oplus M_1$ where $M_1 \neq 0$. As we have shown above the submodule M_1 contains a simple submodule, that contradicts the definition of M_0. So M is a sum of simple submodules.

Let N be a submodule of M and let N_0 be the sum of all simple submodules of N. By assumption $M = N_0 \oplus M_1$. Any element $n \in N$ can be unique written as $n = n_0 + m_1$, where $n_0 \in N_0$ and $m_1 \in M_1$. Since $m_1 \in N$, we obtain $N = N_0 \oplus (N \cap M_1)$. The submodule $N \cap M_1 = 0$; otherwise it contains a simple submodule, that contradicts the definition of the module N_0. Therefore $N = N_0$.

The quotient module M/N is, obviously, isomorphic to a semisimple submodule N' of the decomposition $M = N \oplus N'$. The proposition is proved.

Definition. A nonzero right ideal $\mathcal{I}$ of a ring A is called **minimal** if $\mathcal{I}$ contains no other nonzero right ideal. In particular, $\mathcal{I}$ is minimal if and only if $\mathcal{I}_A$ is a simple right A-module.

Theorem 2.2.5. *The following conditions are equivalent for a ring A:*
(a) *A is right semisimple;*
(b) *A is left semisimple;*
(c) *any right A-module M is semisimple;*
(d) *any left A-module M is semisimple.*

Proof.
$(a) \Rightarrow (c)$. Let $M = M_A$ be a right A-module. Since A_A is a semisimple right

A-module, A is a direct sum of minimal right ideals A_i $(i \in I)$. The module M can be written as the following sum: $M = \sum\limits_{m \in M} mA = \sum\limits_{m \in M} \sum\limits_{i \in I} mA_i$. For every submodule mA_i consider the homomorphism $\varphi : A_i \to mA_i$ given by the formula $\varphi(a_i) = ma_i$. Since A_i is a minimal ideal, we conclude that either $Im(\varphi) = mA_i = 0$ or $Ker(\varphi) = 0$. Hence $mA_i \simeq A_i$ is a simple right module. Therefore M is a sum of simple modules and from proposition 2.2.4 it follows that M is a semisimple right A-module.

Analogously one can prove $(b) \Rightarrow (d)$.

$(c) \Rightarrow (a)$ and $(d) \Rightarrow (b)$ are trivial.

$(a) \Leftrightarrow (b)$ follows from the Wedderburn-Artin theorem.

Proposition 2.2.6. *If A is a semisimple ring, then the full matrix ring $M_n(A)$ is semisimple as well.*

Proof. We leave the proof of this statement as an exercise.

2.3 LATTICES. BOOLEAN ALGEBRAS AND RINGS

In this section we shall study certain partially ordered sets and their connection with Boolean algebras and rings. Our main goal is to prove the fundamental Stone theorem for finite Boolean algebras which yields their full description.

Recall the definition of a partially ordered set.

Definition. A set S is called **partially ordered** or, for short, a **poset** if it is equipped with a relation $\leq$, which satisfies the following conditions:

P1. $a \leq a$ for any $a \in S$ (reflexivity);

P2. $a \leq b$, $b \leq c$ implies $a \leq c$ for any $a, b, c \in S$ (transitivity);

P3. $a \leq b$, $b \leq a$ implies $a = b$ for any $a, b \in S$ (antisymmetry).

The relation $\leq$ is called a **partial order**.

Let $b \geq a$ mean $a \leq b$. Then $\geq$ is also a partial order relation. In the theory of partially ordered sets there exists a useful result which is known as the "duality principle":

If in any theorem about partially ordered sets we replace the relation $\leq$ by the relation $\geq$ we obtain a theorem which is true as well.

Let S be a poset and let T be a subset of S. An element $a \in S$ is called an **upper bound** (resp. **lower bound**) of T if $t \leq a$ (resp. $a \leq t$) for all $t \in T$. In general a set can have several upper bounds or it can have none at all.

An element $a \in T$ is a **greatest** (resp. **least**) element of T if $t \leq a$ (resp. $a \leq t$) for all $t \in T$. Not every subset T of a poset S has a greatest (or least) element. But if T has such an element then it is unique. Indeed, let x and y be greatest elements of T. Then $x \leq y$ and $y \leq x$. Hence from property P3 it follows

that $x = y$. The uniqueness of a least element of T can be proved analogously. So the greatest (resp. least) element, if it does exist, is unique and is an upper (resp. lower) bound for T. If the set of upper bounds of T has a least element, then it is called the **least upper bound** (or **supremum**) of T and denoted by $\sup(T)$. If the set of lower bounds has a greatest element, it is called the **greatest lower bound** (or **infimum**) of T and denoted by $\inf(T)$. It is obvious that if a subset T has a supremum (resp. infimum), then it is uniquely determined.

Definition. A poset S, whose every pair of elements has both a supremum and an infimum in S, is said to be a **lattice**.

Example 2.3.1.
If X and Y are subsets in S, then their supremum in $\mathcal{P}(S)$ is equal to the union $X \cup Y$ and their infimum in $\mathcal{P}(X)$ is the intersection $X \cap Y$. Therefore $\mathcal{P}(X)$ is a lattice.

Example 2.3.2.
Let A be a ring and X be the set of all ideals of the ring A ordered by inclusion. Let $\mathcal{I}$ and $\mathcal{J}$ be ideals in A. Then their supremum in X is the sum $\mathcal{I} + \mathcal{J}$ and their infimum in X is the intersection $\mathcal{I} \cap \mathcal{J}$. Therefore X is a lattice.

The operations **sup** and **inf** are not really binary operations for arbitrary posets. But this is true for a lattice.

Let S be a lattice. Then each pair $a, b \in S$ has both a supremum and an infimum. Let us denote

$$a \vee b = \sup\{a, b\} \quad \text{and} \quad a \wedge b = \inf\{a, b\} \tag{2.3.1}$$

Then the maps $\vee$ and $\wedge$ from $S \times S$ to S defined by

$$(a, b) \mapsto a \vee b \quad \text{and} \quad (a, b) \mapsto a \wedge b$$

are binary operations on S.

The following proposition gives several interesting properties of these operations.

Proposition 2.3.1. *Let S be a lattice with operations $\vee$ and $\wedge$ defined by* (2.3.1). *Then for all $a, b, c \in S$ the following properties hold:*

1) *commutative laws:* $a \vee b = b \vee a$; $\quad a \wedge b = b \wedge a$;
2) *associative laws:* $a \vee (b \vee c) = (a \vee b) \vee c$; $\quad a \wedge (b \wedge c) = (a \wedge b) \wedge c$;
3) *idempotent laws:* $a \vee a = a$; $\quad a \wedge a = a$;
4) *absorption laws:* $a \vee (a \wedge b) = a$; $\quad a \wedge (a \vee b) = a$.

Proof. We shall prove the last of these laws; the proofs of the others are left as exercises.

Proof that $a \vee (a \wedge b) = a$: Since the partial ordering relation is reflexive, we must have $a \leq a$. Also, since $a \wedge b$ is one of the lower bounds for $\{a, b\}$, we have

$a \wedge b \leq a$. These two relations show that the element a is one of the upper bounds of the set $\{a, a \wedge b\}$. Evidently, if c is any upper bounds of $\{a, a \wedge b\}$ then $a \leq c$. Thus, by definition, $\sup\{a, a \wedge b\} = a$.

The following proposition shows that these properties actually characterize a lattice.

Proposition 2.3.2. *If we have a set S with two binary operations $\vee$ and $\wedge$ such that for all elements $a, b, c \in S$ there hold*
(i) $a \vee b = b \vee a; \quad a \wedge b = b \wedge a;$
(ii) $a \vee (b \vee c) = (a \vee b) \vee c; \quad a \wedge (b \wedge c) = (a \wedge b) \wedge c;$
(iii) $a \vee a = a; \quad a \wedge a = a;$
(iv) $a \vee (a \wedge b) = a; \quad a \wedge (a \vee b) = a$
then there is a unique partial ordering in S that makes S a lattice and such that the given operations "$\vee$" and "$\wedge$" are, respectively, the supremum and the infumum in the lattice.

Proof. For proof it suffices to show that the relation " $\leq$ " defined by

$$a \leq b \Longleftrightarrow a \vee b = b$$

is a partial ordering relation. We leave this to the reader as a simple exercise.

So far, in this section we have considered only conditions, which are satisfied by all lattices. There are several interesting conditions which are satisfied by some lattices, but not by others.

Definition. A lattice S is **distributive** if it satisfies the following property:

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

for all $a, b, c \in S$.

Using the "duality principle" it is easy to obtain a symmetric definition:

Proposition 2.3.3. *A lattice S is distributive if and only if for all $a, b, c \in S$ it satisfies the following property:*

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

The lattices of examples 2.3.1 and 2.3.2 are distributive.

A partially ordered set can or can not have greatest and least elements. The same is true for a lattice. The real numbers with the usual ordering form a lattice with neither a greatest nor a least element; the real numbers between zero and one inclusive form a lattice with both a greatest and a least element. If a lattice has a greatest and/or a least element we shall denote them as 1 and/or 0, respectively.

As we have seen, the power set $\mathcal{P}(S)$ of subsets of a given set S forms a lattice under inclusion as the ordering relation. The greatest element 1 of this lattice is S itself, and the least element 0 is the empty set $\emptyset$. The familiar set operations of union and intersection are the operations sup and inf on the power set. But there is another set operation, complementation, which we have not yet had occasion to use. The complement $\overline{X}$ of a subset X in S is defined to be the collection of all elements of S that are not elements of X. It is easy to see that $X \cup \overline{X} = S$ and $X \cap \overline{X} = \emptyset$. This familiar set operation of complementation suggests the following definition.

Let S be a lattice with the greatest element 1 and the least element 0. An element $b \in S$ is a **complement** of the element $a \in S$ if $a \vee b = 1$ and $a \wedge b = 0$.

Definition. A lattice is said to be **complemented** if it has a greatest element and a least element and each its element has at least one complement.

We have defined a lattice as a special type of a poset. A Boolean algebra is a special type of a lattice.

Definition. A **Boolean algebra** is a complemented distributive lattice.

It is easy to show that each element of a Boolean algebra has precisely one complement. Indeed, let b and c be complements of an element a. Then

$$b = b \wedge 1 = b \wedge (a \vee c) = (b \wedge a) \vee (b \wedge c) = 0 \vee (b \wedge c) =$$

$$(a \wedge c) \vee (b \wedge c) = (a \vee b) \wedge c = 1 \wedge c = c.$$

We shall use $\overline{a}$ to denote the complement of an element a in a Boolean algebra.

Example 2.3.3.
The power set $\mathcal{P}(S)$ is a Boolean algebra.

Example 2.3.4.
Consider the set $\mathbf{B} = \{0, 1\}$ with the ordinary logical operations of disjunction $\vee$ and conjunction $\wedge$ and operation of complementation $\overline{0} = 1$ and $\overline{1} = 0$. Obviously, in this case we can write $a \vee b = \max\{a, b\}$, $a \wedge b = \min\{a, b\}$ and $\overline{a} = 1 - a$ for any $a, b \in \mathbf{B}$. Then $\mathbf{B}$ with these operations is a Boolean algebra.

Example 2.3.5.
Consider a finite direct product $\mathbf{B}^n = \mathbf{B} \times ... \times \mathbf{B}$ which is the set of n-tuples $(b_1, b_2, ..., b_n)$, where $b_i \in \mathbf{B}$. Let $(a_1, a_2, ..., a_n)$ and $(b_1, b_2, ..., b_n)$ be elements in $\mathbf{B}^n$. Introduce the following "coordinate wise" operations in $\mathbf{B}^n$:

$$(a_1, a_2, ..., a_n) \vee (b_1, b_2, ..., b_n) = (a_1 \vee b_1, a_2 \vee b_2, ..., a_n \vee b_n)$$

$$(a_1, a_2, ..., a_n) \wedge (b_1, b_2, ..., b_n) = (a_1 \wedge b_1, a_2 \wedge b_2, ..., a_n \wedge b_n)$$

$$\overline{(a_1, a_2, ..., a_n)} = (\overline{a}_1, \overline{a}_2, ..., \overline{a}_n).$$

Then $\mathbf{B}^n$ is a Boolean algebra with greatest element $1 = (1, 1, ..., 1)$ and least element $0 = (0, ..., 0)$. The number of all elements in $\mathbf{B}^n$ is equal to 2^n.

The following proposition shows that the operations in a lattice have properties analogous to set operations.

Proposition 2.3.4. *In any Boolean algebra the operation of complementation satisfies the following properties:*[1])

(a) $\overline{\overline{a}} = a$
(b) $\overline{a \vee b} = \overline{a} \wedge \overline{b}$
(c) $\overline{a \wedge b} = \overline{a} \vee \overline{b}$
(d) $a \vee b = \overline{\overline{a} \wedge \overline{b}}$
(c) $a \wedge b = \overline{\overline{a} \vee \overline{b}}$
(d) $\overline{1} = 0$
(e) $\overline{0} = 1$

We shall prove only property (b); the remainder of the proof is left to the reader as an exercise. Since complements are unique in a Boolean algebra, any element x which satisfies the properties $(a \vee b) \vee x = 1$ and $(a \vee b) \wedge x = 0$ must be the complement of $a \vee b$. It remains only to verify this for the element $x = \overline{a} \wedge \overline{b}$. We have

$$(a \vee b) \vee (\overline{a} \wedge \overline{b}) = [(a \vee b) \vee \overline{a}] \wedge [(a \vee b) \vee \overline{b}] = 1 \wedge 1 = 1$$

and

$$(a \vee b) \wedge (\overline{a} \wedge \overline{b}) = [(a \wedge b) \wedge \overline{a}] \vee [(a \wedge b) \wedge \overline{b}] = 0 \vee 0 = 0.$$

In proposition 2.3.2 a characterization of a lattice was given in terms of two binary operations. It is not difficult to prove the following proposition that gives a similar characterization of a Boolean algebra.

Proposition 2.3.5. *If we have a set S containing two special elements 1 and 0 with two binary operations $\vee$ and $\wedge$ such that for all elements $a, b, c \in S$ there hold:*

(i) $a \vee b = b \vee a$; $\quad a \wedge b = b \wedge a$;
(ii) $a \vee (b \vee c) = (a \vee b) \vee c$; $\quad a \wedge (b \wedge c) = (a \wedge b) \wedge c$;
(iii) $a \vee a = a$; $\quad a \wedge a = a$;
(iv) $a \vee (a \wedge b) = a$; $\quad a \wedge (a \vee b) = a$;
(v) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$;
(vi) *for any element $a \in S$ there exists an element $\overline{a} \in S$ such that $a \vee \overline{a} = 1$ and $a \wedge \overline{a} = 0$,*

[1]) In the case of the Boolean algebra $\mathcal{P}(S)$ of subsets of a set (and also more generally) these rules (properties) are known as the "de Morgan laws". (More strictly (b) and (c) are the de Morgan laws.)

then there is a unique partial ordering relation in S which makes S a Boolean algebra and such that the given operations $\vee$ and $\wedge$ are the supremum and the infimum, respectively, in the Boolean algebra. Moreover, 1 and 0 are the greatest and the least elements of S, respectively, and $\overline{a}$ is the complement of a.

Proof. By proposition 2.3.2, the conditions (i) through (iv) in proposition 2.3.5 imply that there is a unique partial ordering relation in S which makes S a lattice. Conditions (v) states that this lattice is distributive.

For any element a of S we have

$$a \vee 1 = a \vee (a \vee \overline{a}) = (a \vee a) \vee \overline{a} = a \vee \overline{a} = 1$$

and

$$a \wedge 0 = a \wedge (a \wedge \overline{a}) = (a \wedge a) \wedge \overline{a} = a \wedge \overline{a} = 0,$$

thus 1 and 0 are, respectively, the greatest and the least elements of the lattice. Condition (vi) now states that the lattice is complemented and that $\overline{a}$ is the complement of a.

Lemma 2.3.6. *In any Boolean algebra $\mathcal{B}$ the condition $a \vee b = a$ holds if and only if $a \wedge b = b$.*

Proof. If $a \vee b = b$ then $a = (a \vee b) \wedge a = b \wedge a = a \wedge b$. The inverse statement follows from the "duality principle".

From this lemma it follows that in any Boolean algebra we have

$$a \leq b \quad \Leftrightarrow \quad a \vee b = b \quad \Leftrightarrow \quad a \wedge b = a \tag{2.3.2}$$

Lemma 2.3.7. *In any Boolean algebra $\mathcal{B}$ there hold:*
1. $a \wedge b \leq a \leq a \vee b$
2. $0 \leq a \leq 1$

for any $a, b \in \mathcal{B}$.

Proof.
1. By the absorption law we have $(a \wedge b) \vee a = a$. Hence, $a \wedge b \leq a$. Analogously, we obtain $(a \vee b) \wedge a = a$ and from lemma 2.3.6 it follows that $a \leq a \vee b$.
2. This follows from the facts that $a \vee 0 = a$ and $a \wedge 1 = a$.

We have seen that the power set $\mathcal{P}(S)$ for a given finite set S forms a finite Boolean algebra. Actually, every finite Boolean algebra is isomorphic to a Boolean algebra of sets with the partial ordering relation being set inclusion, and it can always be arranged that each of these sets is a subset of some particular finite set S. We are going to prove this result.

Definition. An element $a \neq 0$ of a Boolean algebra is called an **atom** if it cannot be expressed in the form $a = b \vee c$ with $a \neq b$ and $a \neq c$.

It is well known that any natural number can be factorized into a product of prime numbers and this factorization is unique. We shall show that a similar fact holds in any Boolean algebra, that is, any nonzero element of a finite Boolean algebra can be expressed as a sum of different atoms.

Example 2.3.6.
An atom in the algebra $\mathcal{P}(S)$ is any one-element set $\{s\}$, where $s \in S$. Any set $A = \{a_1, a_2, ..., a_m\} \in \mathcal{P}(S)$ can be written as $A = \{a_1\} \cup \{a_2\} \cup ... \cup \{a_m\}$.

Example 2.3.7.
The Boolean algebra $\mathbf{B}$ has a unique atom which is equal to 1.

Example 2.3.8.
The Boolean algebra $\mathbf{B}^n$ has n atoms. They are of the form

$$e_i = (0, ..., 0, 1, 0, ...0)$$

with 1 at the i-th position and 0 elsewhere. Any nonzero element $b = (b_1, b_2, ..., b_n) \in \mathbf{B}^n$ can be written as $b = e_{i_1} \vee e_{i_2} \vee ... \vee e_{i_k}$ where $b_{i_j} = 1$ for $j = 1, ..., k$ and $b_{i_j} = 0$ for other i_j.

Lemma 2.3.8. *A nonzero element a of a Boolean algebra $\mathcal{B}$ is an atom if and only if the inequality $x \leq a$ has exactly two solutions $x = a$ and $x = 0$.*

Proof. Let a nonzero element $a \in \mathcal{B}$ be an atom, and suppose $x \leq a$, where $a \neq 0$. Assume $x \neq 0$ and $x \neq a$. Then we have $a = a \wedge 1 = (x \vee a) \wedge (x \vee \overline{x}) = x \vee (a \wedge \overline{x})$. Since a is an atom, it follows that either x or $(a \wedge \overline{x})$ must be equal to a. But by hypothesis $x \neq a$, therefore $a \wedge \overline{x} = a$. In this case, by lemma 2.3.6, $x = a \wedge x = (a \wedge \overline{x}) \wedge x = a \wedge (\overline{x} \wedge x) = a \wedge 0 = 0$.

Conversely, if a is not an atom then $a = x \vee y$ for some $x, y \in \mathcal{B}$ and $x \neq a$, $y \neq a$. Since, by lemma 2.3.6, $x \leq x \vee y = a$, it follows that $x \leq a$ and $x \neq a$. At the same time $x \neq 0$. Otherwise we have $a = 0 \vee y = y \neq a$.

Lemma 2.3.9. *For any nonzero element b of a finite Boolean algebra $\mathcal{B}$ there exists at least one atom $a \in \mathcal{B}$ such that $a \leq b$.*

Proof. Let b be an element of a Boolean algebra $\mathcal{B}$ and $b \neq 0$. If b is an atom, the proposition is proved. If b is not an atom, By lemma 2.3.8, there are at least three solutions for $x \leq b$. Let c be any solution of this inequality different from 0 and b. If c is an atom, the result is evident; if not, let d be a solution of $x \leq c$ which different from 0 and c. Since $\mathcal{B}$ is finite, continuing this process in such a way we must arrive at an atom after a finite number of steps.

Let $\mathcal{B}$ be a finite Boolean algebra with set of atoms $A = \{a_1, ..., a_n\}$. For any element $x \in \mathcal{B}$ we denote by $T(x)$ the set of all atoms $a \in A$ such that $a \leq x$.

Proposition 2.3.10. *Any nonzero element $x \in \mathcal{B}$ can be written as a finite sum of distinct atoms:*

$$x = a_{i_1} \vee a_{i_2} \vee ... \vee a_{i_k} \tag{2.3.3}$$

where $a_{i_j} \in T(x)$ for $j = 1, ..., k$. Moreover, this factorization is unique up to the order of its elements and $T(x) = \{a_{i_1}, a_{i_2}, ..., a_{i_k}\}$.

Proof. First we shall show that any nonzero element $x \in \mathcal{B}$ can be written in the form (2.3.3). Suppose that this is not true and let S be the set of all nonzero elements of $\mathcal{B}$ which cannot be written as a finite sum of atoms. Let $x \in S$. Since x is not an atom, it can be written as $x = y \vee z$, where $y \leq x$, $z \leq x$ and $y, z \neq x$, $y, z \neq 0$. Moreover, at least one element either y or z belongs to S. So, for any element $x \in S$ there exists at least one element $y \in S$ such that $y \leq x$ and $y \neq x$, $y \neq 0$. Then it follows that for any $x \in S$ there exists an infinite chain of nonzero elements $x = x_0 \geq x_1 \geq x_2 \geq ...$ and $x_i \neq x_{i+1}$ for any i. But this contradicts the finiteness of the Boolean algebra $\mathcal{B}$. So any element $x \in \mathcal{B}$ can be written in the form (2.3.3).

We shall now show that any element x can be written in the form (2.3.3), where all atoms $a_{ij} \in T(x)$.

Since $1 \in \mathcal{B}$, it follows that 1 can be written in form (2.3.3). Since $1 \vee a = 1$ for any element $a \in \mathcal{B}$, we may consider that in the decomposition of 1 into a finite sum of atoms there appear all atoms of A, i.e.,

$$1 = a_1 \vee a_2 \vee ... \vee a_n.$$

Then for any element $x \in \mathcal{B}$ we have

$$x = x \wedge 1 = x \wedge (a_1 \vee a_2 \vee ... \vee a_n) = (x \wedge a_1) \vee ... \vee (x \wedge a_n).$$

Since $x \wedge a_i \leq a_i$ and a_i is an atom, from lemma 2.3.8 it follows that either $x \wedge a_i = a_i$ if $a_i \in T(x)$ or $x \wedge a_i = 0$ otherwise. So we obtain the required decomposition.

We are going to prove the uniqueness of this form. Let $x = b_1 \vee ... \vee b_k$, where $b_i \in A$ are atoms, $i = 1, ..., k$. Then $b_i \leq x$ for all i and therefore $\{b_1, b_2, ..., b_k\} \subseteq T(x)$. On the other hand, if $a \in T(x)$ and $a \neq 0$ then

$$a = a \wedge x = a \wedge (b_1 \vee ... \vee b_k) = (a \wedge b_1) \vee ... \vee (a \wedge b_k).$$

Since $a \neq 0$, there exists an index i such that $a \wedge b_i \neq 0$. Since a and b_i are atoms, $a = a \wedge b_i = b_i$, that is, $T(x) \subseteq \{b_1, b_2, ..., b_k\}$. Therefore $T(x) = \{b_1, b_2, ..., b_k\}$, as required.

Lemma 2.3.11. *For any Boolean algebra $\mathcal{B}$ and any elements $x, y \in \mathcal{B}$ there hold:*

(i) $T(x \vee y) = T(x) \cup T(y)$
(ii) $T(x \wedge y) = T(x) \cap T(y)$

(iii) $T(\overline{x}) = \overline{T(X)}$

Proof.
(i) Let $a \in T(x \vee y)$, i.e., $a \leq x \vee y$. Then from (2.3.2) it follows that

$$a = a \wedge (x \vee y) = (a \wedge x) \vee (a \wedge y).$$

Since a is an atom, $a \wedge x = a$ or $a \wedge y = a$, and hence $a \leq x$ or $a \leq y$, that is, $a \in T(x)$ or $a \in T(y)$. From the definition of set addition it follows that $a \in T(x) \cup T(y)$. Therefore, $T(x \vee y) \subseteq T(x) \cup T(y)$.

Conversely, let $a \in T(x) \cup T(y)$, then $a \in T(x)$ or $a \in T(y)$, which implies $a \leq x$ or $a \leq y$. From (2.3.2) we have $a \wedge x = a$ or $a \wedge y = a$. By the absorption law we obtain

$$a = (a \wedge x) \vee (a \wedge y) = a \wedge (x \vee y).$$

Hence, $a \leq x \vee y$, i.e., $a \in T(x \vee y)$. Therefore, $T(x) \cup T(y) \subseteq T(x \vee y)$.

So, $T(x \vee y) = T(x) \cup T(y)$.

(ii) Let $a \in T(x \wedge y)$, i.e., $a \leq x \wedge y$. Then from (2.3.2) it follows that

$$a = a \wedge (x \wedge y) = (a \wedge x) \wedge y = (a \wedge y) \wedge x.$$

Hence, $a \leq y$ and $a \leq x$, that is, $a \in T(x) \cap T(y)$. Therefore $T(x \wedge y) \subseteq T(x) \cap T(y)$.

Let $a \in T(x) \cap T(y)$, then $a \leq y$ and $a \leq x$. Hence, $a = a \wedge x$ and $a = a \wedge y$. Therefore $a = (a \wedge x) \wedge y = a \wedge (x \wedge y)$, that is, $a \leq x \wedge y$. Therefore $a \in T(x \wedge y)$. So, $T(x \wedge y) = T(x) \cap T(y)$.

(iii) Finally, $S = T(1) = T(x \vee \overline{x}) = T(x) \cup T(\overline{x})$ and $\emptyset = T(0) = T(x \wedge \overline{x}) = T(x) \cap T(\overline{x})$ and owing to the uniqueness of the complement we have $T(\overline{x}) = \overline{T(x)}$.

Lemma 2.3.12. *For any element $x \in \mathcal{B}$,* $\sup T(x) = x$.

Proof. If $x = 0$, then the statement is obvious. If $x \neq 0$, then, by lemma 2.3.10, $T(x) \neq \emptyset$ and because it is a finite subset in $\mathcal{B}$, it has a supremum. Let $\sup T(x) = y$ and assume $y \neq x$. Since x is one of the upper bounds of $T(x)$, we have $y \leq x$. Since $y \neq x$, we have $x \not\leq y$. Hence, by (2.3.2), it follows that $x \neq x \wedge y$. Let $\overline{y}$ be a complement of y, then we have

$$x = x \wedge 1 = x \wedge (y \vee \overline{y}) = (x \wedge y) \vee (x \wedge \overline{y})$$

Since $x \neq x \wedge y$, we obtain that $x \wedge \overline{y} \neq 0$. Then, by lemma 2.3.7, $x \wedge \overline{y} \leq (x \wedge y) \vee (x \wedge \overline{y}) = x$. Since $x \wedge \overline{y} \neq 0$, by lemma 2.3.9, there exists an atom $a \in A$ such that $a \leq x \wedge \overline{y}$. Therefore $a \leq x$ and $a \leq \overline{y}$. Hence, $a \in T(x)$ and by the definition of supremum $a \leq y$. Thus, $a \leq y$ and at the same time $a \leq \overline{y}$. Then we have $a = a \wedge y$ and $a = a \wedge \overline{y}$. Hence, $a = (a \wedge y) \wedge \overline{y} = 0$. This contradiction shows that $y = x$.

From the uniqueness of the supremum for any set we obtain the following result.

Corollary 2.3.13. *$T(x) = T(y)$ if and only if $x = y$.*

To prove the main theorem of this section we introduce the notion of an isomorphism of Boolean algebras.

Definition. For two Boolean algebras $\mathcal{B}_1$ and $\mathcal{B}_2$ a bijective mapping φ of $\mathcal{B}_1$ onto $\mathcal{B}_2$ is called an **isomorphism of Boolean algebras** if it satisfies the following conditions:

(1) $\varphi(x \vee y) = \varphi(x) \vee \varphi(y)$
(2) $\varphi(x \wedge y) = \varphi(x) \wedge \varphi(y)$
(3) $\varphi(\overline{x}) = \overline{\varphi(x)}$

for all $x, y \in \mathcal{B}_1$.

Theorem 2.3.14. *Any finite Boolean algebra $\mathcal{B}$ with set of atoms $A = \{a_1, a_2, ..., a_n\}$ of size n is isomorphic to the Boolean algebra $\mathcal{P}(A)$ of all subsets of the given set A. In particular, $\mathcal{B}$ has 2^n elements and the element 1 of $\mathcal{B}$ has a unique decomposition into a sum of all distinct atoms*

$$1 = a_1 \vee a_2 \vee ... \vee a_n. \tag{2.3.4}$$

Proof. Consider the map $\varphi : \mathcal{B} \to \mathcal{P}(A)$, where $\varphi(x) = T(x)$ for any element $x \in \mathcal{B}$. By corollary 2.3.13 and proposition 2.3.10, this map is one-to-one and onto. By lemma 2.3.11, it follows that φ is an isomorphism of Boolean algebras. The uniqueness of decomposition $1 \in \mathcal{B}$ in the form (2.3.4) follows from proposition 2.3.10.

Since the number of all subsets of the set A is equal to 2^n, we have proved the theorem.

Theorem 2.3.14 is a particular case of the famous Stone theorem of which the proof can also be found in the book *R.Sikorsky, Boolean algebras, Springer, 1964*:

Theorem 2.3.15 (Stone's theorem). *Any Boolean algebra is isomorphic to the Boolean algebra of some (not necessarily all) subsets of a given set.*

The following example gives a Boolean algebra which is not isomorphic to a Boolean algebra formed by collection of all subsets of any set with inclusion as the ordering relation.

Example 2.3.9.

Let S be an infinite set, and let H be a set of all finite or cofinite subsets of S. (Here a cofinite subset means a subset with finite complement.) Clearly, the set H is a Boolean algebra with inclusion as the ordering relation. The cardinality of H is strictly less than the cardinality of the power set $\mathcal{P}(S)$, so H cannot be isomorphic to a Boolean algebra formed by collection of all subsets of any set.

As a corollary of theorem 2.3.14 we have the following result which says that any finite Boolean algebra is completely determined by the number of its atoms.

Theorem 2.3.16. *If $\mathcal{B}_1$ and $\mathcal{B}_2$ are two finite Boolean algebras with the sets of their atoms equal to $A_1 = \{a_1, ..., a_n\}$ and $A_2 = \{b_1, ..., b_n\}$, respectively, then there exists an isomorphism of Boolean algebras $\varphi : \mathcal{B}_1 \to \mathcal{B}_2$ such that $\varphi(a_i) = b_i$ for $i = 1, ..., n$.*

Consider the Boolean algebra $\mathbf{B}^n$. It also has exactly n atoms and has 2^n elements. On the other hand, $\mathbf{B}^n$ is a finite direct product of n copies of the simple Boolean algebra $\mathbf{B}$. So we have also the following corollary.

Corollary 2.3.17. *Any finite Boolean algebra $\mathcal{B}$, having n atoms, is isomorphic to the Boolean algebra $\mathbf{B}^n$, which is a finite product of n copies of the simple Boolean algebra $\mathbf{B}$.*

Definition. An associative ring $\mathcal{R}$ (maybe without identity) is called a **Boolean ring** if each its element $a \in \mathcal{R}$ is an idempotent, i.e., $a^2 = a$.

Proposition 2.3.18.

1. *Every Boolean ring $\mathcal{R}$ is commutative and $a + a = 0$ for any $a \in \mathcal{R}$.*
2. *If $\mathcal{R}$ is a Boolean ring then the direct sum $\mathcal{T} = \bigoplus_{i \in I} \mathcal{R}$ of copies of $\mathcal{R}$ is a Boolean ring as well.*

Proof.

1. First, for any element $a \in \mathcal{R}$ we have

$$a + a = (a + a)^2 = a^2 + a^2 + a^2 + a^2 = a + a + a + a$$

and hence $a + a = 0$.

On the other hand,

$$a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + b + ab + ba$$

and hence $ab + ba = 0$. Then

$$ab = ab + (ba + ba) = (ab + ba) + ba = ba$$

2. Let $a = (a_1, a_2, ..., a_k) \in \mathcal{T}$. Then $a^2 = aa = (a_1^2, a_2^2, ..., a_k^2) = (a_1, a_2, ..., a_k) = a$.

We shall prove that in any Boolean ring $\mathcal{R}$ with identity it is possible to define a partial ordering relation so that $\mathcal{R}$ becomes a Boolean algebra. Conversely, in any Boolean algebra $\mathcal{B}$ it is possible to define two binary operations so that $\mathcal{B}$ becomes a Boolean ring with identity.

Proposition 2.3.19. *Let $\mathcal{B}$ be a Boolean algebra. Then $\mathcal{B}$ becomes a Boolean ring with identity if the binary operations of addition and multiplication are defined on $\mathcal{B}$ by follows*

$$a + b = (a \wedge \overline{b}) \vee (\overline{a} \wedge b)$$

and

$$a \cdot b = a \wedge b.$$

Proof. The proof of this proposition consists of simply checking all axioms of a ring and we leave this to the reader as an exercise.

Proposition 2.3.20. *Let $\mathcal{R}$ be a Boolean ring with identity. Then $\mathcal{R}$ becomes a Boolean algebra if we set*

$$a \vee b = a + b + ab$$

$$a \wedge b = ab$$

and the ordering relation " $\leq$ " is defined in $\mathcal{R}$ by

$$a \leq b \Longleftrightarrow ab = a.$$

Proof. It is evident that " $\leq$ " is a relation on $\mathcal{R}$. To prove that " $\leq$ " is an ordering relation, note that $aa = a$ for any $a \in \mathcal{R}$, that is, $a \leq a$ and thus " $\leq$ " is reflexive. If $a \leq b$ and $b \leq a$, then $a = ab = ba = b$, so " $\leq$ " is antisymmetric. If $a \leq b$ and $b \leq c$, then $ac = (ab)c = a(bc) = ab = a$. Thus, " $\leq$ " is transitive. Therefore $\mathcal{R}$ is a partially ordered set.

To show that $\mathcal{R}$ is a lattice it suffices to prove that $\sup\{a, b\} = a + b + ab$ and $\inf\{a, b\} = ab$. Since $aa = a$, $bb = b$ and $ab + ab = 0$, we have $a(a + b + ab) = a$. Similarly, $b(a + b + ab) = b$. Hence, $a \leq a + b + ab$ and $b \leq a + b + ab$; that is, $a + b + ab$ is an upper bound for $\{a, b\}$. If c is another upper bound for $\{a, b\}$, then $ac = a$ and $bc = b$, thus $(a + b + ab)c = ac + bc + abc = a + b + ab$ so that $a + b + ab \leq c$, proving that $a + b + ab = \sup\{a, b\}$. The proof that $\inf\{a, b\} = ab$ is similar.

It is easy to see that 1 and 0 are, respectively, the greatest and least element in $\mathcal{R}$. Moreover, $1 + a$ is a complement of a since $a \wedge (1 + a) = a(1 + a) = 0$ and $a \vee (1 + a) = a + (1 + a) + a(1 + a) = 1$.

The proof of distributivity of this lattice is left to the reader. Since $\mathcal{R}$ is a complemented, distributive lattice, it is a Boolean algebra.

Since the Boolean algebra $\mathbf{B}$ is a simple ring, from corollary 2.3.17 we obtain the following statement.

Theorem 2.3.21. *Any finite Boolean ring $\mathcal{R}$ with identity is isomorphic to a direct sum of simple Boolean rings.*

We conclude this section by considering other important types of posets and their properties.

Definition. A poset S, in which every subset of S has both supremum and infimum in S, is said to be a **complete lattice**.

Proposition 2.3.22. *A partially ordered set S is a complete lattice if and only if S has a supremum and every nonempty subset of S has an infimum in S.*

Proof. It will suffice to prove that if $X \subseteq S$ then X has a supremum in S. Let $a \in S$ be the greatest element of S. Then $x \leq a$ for all $x \in S$. In particular, the set of upper bounds of X is not empty, so it has the infimum. It is clear that this infimum is an upper bound of X and, hence, the supremum of X.

Definition. A lattice S is said to be **modular** if it satisfies the modularity condition:

$$\text{if} \quad b \leq a \quad \text{then} \quad a \wedge (b \vee c) = b \vee (a \wedge c) \tag{2.3.5}$$

for all $a, b, c \in S$.

Example 2.3.10.
If $\mathcal{A}$ is a subset in $\mathcal{P}(X)$ (that is, a set of subsets in X), then its supremum in $\mathcal{P}(X)$ is the union $\bigcup\limits_{Y \subset X} Y$ and its infimum in $\mathcal{P}(X)$ is the intersection $\bigcap\limits_{Y \subset X} Y$. Therefore $\mathcal{P}(X)$ is a complete lattice. Moreover, it is modular.

Example 2.3.11.
Let A be a ring and X be a set of all ideals of a ring A. Let $Y = \{\mathcal{I}_i \ : \ i \in I\}$ be a subset of X. We define supremum in X as the sum $\sum\limits_{i \in I} \mathcal{I}_i$ and infimum in X as the intersection $\bigcap\limits_{i \in I} \mathcal{I}_i$. Then X is a complete lattice. Moreover, by theorem 1.3.6, it is modular. Thus, we obtain the following result.

Proposition 2.3.23. *The ideals in a ring form a complete modular lattice with respect to ideal inclusion.*

For ideals in a semisimple ring we can say much more. Actually, the following theorem is a corollary of the Wedderburn-Artin theorem and theorem 2.3.14.

Theorem 2.3.24. *The ideals in a semisimple ring A form a finite Boolean algebra consisting of 2^s elements.*

Proof. From the Wedderburn-Artin theorem it follows that a semisimple ring A is isomorphic to a direct sum of s full matrix rings over some division rings:

$$A = M_{n_1}(D_1) \times M_{n_2}(D_2) \times ... \times M_{n_s}(D_s). \tag{2.3.6}$$

Then any two-sided ideal $\mathcal{I}$ in A can be decomposed into a direct sum of ideals

$$\mathcal{I} = \mathcal{I}_1 \times \mathcal{I}_2 \times ... \times \mathcal{I}_s \tag{2.3.7}$$

where every ideal $\mathcal{I}_k$ is a two-sided ideal in $M_{n_k}(D_k)$. Since $M_{n_k}(D_k)$ is a simple ring, it follows that either $\mathcal{I}_k = 0$ or $\mathcal{I}_k = M_{n_k}(D_k)$. Denote by S the set of all two-sided ideals in the ring A. Then, by proposition 2.3.23, S is a complete lattice. Consider the map φ of the set S to the Boolean algebra $\mathbf{B}^s$ by setting $\varphi(\mathcal{I}) = (\alpha_1, \alpha_2, ..., \alpha_s)$, where $\alpha_k = 1$ if $\mathcal{I}_k = M_{n_k}(D_k)$ and $\alpha_k = 0$ if $\mathcal{I}_k = 0$ in decomposition (2.3.7) of the ideal $\mathcal{I}$. Then it is easy to verify that this map is an isomorphism of Boolean algebras.

2.4 FINITELY DECOMPOSABLE RINGS

We shall begin this section with a more careful study of the general properties of idempotents which play such a central role in the structural theory of rings and modules. Recall that an element e of a ring A is called an **idempotent** if $e^2 = e$. Any ring has always the two idempotents 0 and 1 which are called **trivial idempotents**. Two idempotents $e^2 = e$ and $f^2 = f$ are called **orthogonal** if $ef = fe = 0$. Let $1 = e_1 + e_2 + ... + e_n$ be a decomposition of the identity of a ring A, i.e., $e_1, ..., e_n$ are pairwise orthogonal idempotents. The following theorem establishes a connection between decompositions of an A-module M into a direct sum of submodules and decompositions of the identity of the endomorphism ring $End_A(M)$ of M.

Theorem 2.4.1. *There is a bijective correspondence between decompositions of an A-module M into a direct sum of submodules and decompositions of the identity of the ring $E = End_A(M)$.*

Proof. Let $M = M_1 \oplus M_2 \oplus ... \oplus M_n$ be a decomposition of an A-module M into a direct sum of submodules. This means that every element $m \in M$ can be uniquely written in the form $m = m_1 + m_2 + ... + m_n$, where $m_i \in M_i$ for $i = 1, ..., n$. Let $e_i \in E$ be the natural projection from M to M_i, i.e., $e_i m = m_i$ for $i = 1, ..., n$. Then $m = e_1 m + e_2 m + ... + e_n m = (e_1 + e_2 + ... + e_n)m$ for every $m \in M$. Hence, $e_1 + e_2 + ... + e_n = 1_E$ is the identity of the ring E. Since $e_i m = m_i$, we have $e_i^2 m = e_i(e_i m) = e_i m_i = m_i = e_i m$ for any $m \in M$, i.e., $e_i^2 = e_i$. On the other hand, if $i \neq j$ then $e_j m_i = 0$. Hence, for any $m \in M$ we have $0 = e_j m_i = e_j e_i m$, i.e., $e_j e_i = 0$ for $i \neq j$. Therefore the $e_1, ..., e_n$ are pairwise orthogonal idempotents of the ring E and $1 = e_1 + e_2 + ... + e_n$ is a decomposition of the identity of the ring E.

Conversely, let $1 = e_1 + e_2 + ... + e_n$ be a decomposition of the identity of the ring E. Put $M_i = e_i M$. We shall show that $M = M_1 \oplus M_2 \oplus ... \oplus M_n$. Indeed, for any element $m \in M$ we have $m = (e_1 + e_2 + ... + e_n)m = e_1 m + e_2 m + ... + e_n m = m_1 + m_2 + ... + m_n$, where $m_i \in M_i$, that is, $M = M_1 + M_2 + ... + M_n$. Let $m \in M_i \cap M_j$ for $i \neq j$. Then $m = e_i x$ and $m = e_j y$. Since $e_i^2 = e_i$,

$e_j^2 = e_j$ and $e_i e_j = 0$, we have $e_i m = e_i^2 x = e_i x = m$ and analogously $e_j m = m$. Therefore $m = e_i m = e_i e_j m = 0$, i.e., $M_i \cap M_j = 0$. From 1.4.3 it follows that $M = M_1 \oplus M_2 \oplus ... \oplus M_n$.

The following statement is immediate from theorems 2.1.2 and 2.4.1.

Corollary 2.4.2. *There is a bijective correspondence between decompositions of an A-module M and decompositions of the regular module over the ring $End_A(M)$.*

Definition. An idempotent $e \in A$ is said to be **primitive** if e has no decomposition into a sum of nonzero orthogonal idempotents $e = e_1 + e_2$ in A.

Lemma 2.4.3. *Let M be a nonzero A-module. Then the following statements are equivalent:*

1. *M is indecomposable.*
2. *$End_A(M)$ has no nontrivial idempotents.*
3. *1 is a primitive idempotent in $End_A(M)$.*

Proof. This lemma is immediate from theorem 2.4.1 taking into account that if e is a nontrivial idempotent in $End_A(M)$, then e and $f = 1 - e$ are orthogonal idempotents, and $1 = e + (1 - e)$ is a decomposition of the identity of the ring $End_A(M)$.

The following proposition gives another characterization of a primitive idempotent.

Proposition 2.4.4. *For any nonzero idempotent $e \in A$ the following conditions are equivalent:*

1. *eA is indecomposable as a right A-module.*
2. *Ae is indecomposable as a left A-module.*
3. *The ring eAe has no nontrivial idempotents.*
4. *The idempotent e is primitive.*

Proof.

The equivalences $1 \Longleftrightarrow 3$ and $2 \Longleftrightarrow 3$ follow from the previous lemma taking into account theorem 2.1.2.

$3 \Longleftrightarrow 4$. Assume $e = e_1 + e_2$, where e_1, e_2 are nonzero orthogonal idempotents in A. Then $e = e_1 + (e - e_1)$ is a decomposition of the identity of the ring eAe. Applying lemma 2.4.3 we end the proof of the statement.

Recall that an idempotent e of a ring A is called **central** if $ea = ae$ for any element $a \in A$, i.e., $e \in Cen(A)$.

Lemma 2.4.5. *An idempotent $e \in A$ is central if and only if $eAf = fAe = 0$, where $f = 1 - e \in A$.*

Proof. Let $a \in A$ and $eaf = fae = 0$, then $ea = ea(e+f) = eae = (e+f)ae = ae$, i.e., $e \in Cen(A)$. Conversely, from $ef = fe = 0$ it follows that $eaf = efa = fea = fae = 0$ for any $a \in A$.

Let S be the set of all central idempotents of a ring A. Define an addition $\oplus$ on S by $e \oplus f = e + f - ef$ and define a multiplication $\times$ on S by the operation of multiplication in A: $e \times f = ef$. One can show that $\mathcal{B} = (S, \oplus, \times)$ is a Boolean algebra.

Proposition 2.4.6. *The set of all central idempotents of a ring A forms a Boolean algebra $\mathcal{B}(A)$.*

Proof.

1. Obviously, $e \oplus f = f \oplus e$.

2. $e \oplus (f \oplus g) = e \oplus (f + g - fg) = e + f + g - fg - ef - eg + efg$ and $(e \oplus f) \oplus g = (e + f - ef) \oplus g = e + f - ef + g - eg - fg + efg$.

3. $e \oplus e = e + e - e^2 = e$

The operation $\times$ satisfies analogous conditions because it is the operation of multiplication in the ring A.

4. $e \oplus (e \times f) = e \oplus ef = e + ef - e^2 f = e$ and $e \times (e \oplus f) = e \times (e + f - ef) = e^2 + ef - e^2 f = e$.

5. $e \times (f \oplus g) = e(f + g - fg) = ef + eg - efg$ and $(e \times f) \oplus (e \times g) = ef + eg - efg$.

So the operations $\oplus$ and $\times$ satisfy the conditions (i)-(v) of proposition 2.3.5. Since $e \oplus (1 - e) = e + 1 - e - e + e^2 = 1$ and $e \times (1 - e) = e - e^2 = 0$, for any element $e \in S$ there exists a complement $1 - e$. Moreover, 0 and 1 are two special elements in $\mathcal{B}(A)$. Thus, by proposition 2.3.5, $\mathcal{B}(A)$ is a Boolean algebra.

In the Boolean algebra $\mathcal{B}(A)$ there is an ordering relation $\leq$ defined by

$$e \leq f \iff e \oplus f = f \iff e \times f = e.$$

Definition. A central idempotent $e \in A$ is called **centrally primitive** if it cannot be written as a sum of two nonzero orthogonal central idempotents.

Lemma 2.4.7. *A central idempotent $e \in A$ is centrally primitive if and only if e is an atom of the Boolean algebra $\mathcal{B}(A)$.*

Proof. Suppose a central idempotent $e \in A$ is not centrally primitive, i.e., there exists a decomposition $e = f_1 + f_2$, where f_1, f_2 are nonzero orthogonal central idempotents. Then $f_1 e = f_1^2 + f_1 f_2 = f_1$, that is, $f_1 \leq e$ and $f_1 \neq 0$, $f_1 \neq e$. But this means that e is not an atom.

Conversely, suppose, $e \in \mathcal{B}(A)$ is not an atom, then there exists a nonzero element $f \in \mathcal{B}$ such that $f \leq e$ and $f \neq e$. Consider the decomposition $e = f + (e - f)$. Since $f^2 = f$ and $f \leq e$ implies $fe = f$, we have $(e - f)^2 = e^2 - fe - ef + f^2 = e - f$ and $f(e - f) = fe - f^2 = f - f = 0$, therefore both

f and $e - f$ are nonzero orthogonal central idempotents in A. Consequently, e is not a centrally primitive idempotent. The lemma is proved.

Suppose the set of all central idempotents of a ring A is finite. Then the Boolean algebra $\mathcal{B}(A)$ is finite and, by theorem 2.3.14, the identity of $\mathcal{B}(A)$ can be uniquely decomposed into a sum of all its different atoms

$$1 = e_1 \oplus e_2 \oplus ... \oplus e_n.$$

Since e_i, e_j are atoms and, by lemma 2.3.7, $e_i e_j \leq e_i$ we obtain that $e_i e_j = 0$ for $i \neq j$. Therefore $e_i \oplus e_j = e_i + e_j$. So, by the previous lemma the identity of A can be decomposed into a sum of all different centrally primitive orthogonal idempotents

$$1 = e_1 + e_2 + ... + e_n.$$

Since, by proposition 2.3.10, any element of the Boolean algebra $\mathcal{B}(A)$ is uniquely expressible as a finite sum of different atoms, any central idempotent of the ring A is a sum of different centrally primitive idempotents. So, from the discussion above we obtain the following result.

Proposition 2.4.8. *Suppose a ring A has a finite number of central idempotents. Then*

1. *The identity of A can be written as a sum of all different centrally primitive orthogonal idempotents*

$$1 = e_1 + e_2 + ... + e_n.$$

2. *This decomposition is unique up to a permutation of the summands, i.e., if we have another decomposition of the identity into a sum of centrally primitive orthogonal idempotents*

$$1 = f_1 + f_2 + ... + f_k$$

then $n = k$ and there is a permutation σ of numbers $\{1, 2, ..., n\}$ such that $f_i = e_{\sigma(i)}$ for $i = 1, 2, ..., n$.

3. *Any centrally primitive idempotent $e \in A$ belongs to the set $\{e_1, e_2, ..., e_n\}$. In particular, any two distinct centrally primitive idempotents in A are orthogonal.*

4. *Any central idempotent $e \in A$ can be uniquely written as a sum of distinct centrally primitive idempotents*

$$e = e_{1_k} + e_{2_k} + ... + e_{s_k}$$

where $e_{i_k} \in \{e_1, e_2, ..., e_n\}$ for $i = 1, ..., s$.

Definition. A ring A is said to be **indecomposable** if $A \neq 0$ and A cannot be decomposed into a direct product of two nonzero rings.

Lemma 2.4.9. *A ring A is indecomposable if and only if it has no nontrivial central idempotents.*

Proof. Let A be an indecomposable ring. Suppose $e \in A$ is a central idempotent, i.e., $e \neq 0$, $e \neq 1$ and $ea = ae$ for any $a \in A$. Then $f = 1 - e$ is also an idempotent in A. Since $ef = e(1-e) = 0$ and $fa = (1-e)a = a - ea = a - ae = a(1-e) = af$, we obtain that e, f are both nontrivial orthogonal central idempotents and $1 = e + f$. Hence $eA = Ae = eAe$, $fA = Af = fAf$ and, by lemma 2.4.5, $eAf = fAe = 0$. Therefore eAe, fAf are both rings with identities e and f, respectively. So the two-sided Peirce decomposition has the form

$$A = \begin{pmatrix} eAe & 0 \\ 0 & fAf \end{pmatrix},$$

and so A can be decomposed into a direct product of two nonzero rings. This leads to contradiction.

Conversely, let $A = A_1 \times A_2$, where A_1, A_2 are nonzero rings. Put $e_1 = (1, 0)$ and $e_2 = (0, 1)$. Then $1 = e_1 + e_2$ and e_1, e_2 are orthogonal idempotents. Moreover, they are both central, because $e_1 a = (a_1, 0) = ae_1$ and $e_2 a = (0, a_2) = ae_2$ for any $a \in A$. So in this case A has at least two nontrivial central idempotents.

Definition. A ring A is called a **finitely decomposable ring** (or, for short, **FD-ring**) if it can be expressed as a direct product of a finite number of indecomposable rings.

Suppose the identity of a ring A can be written as a sum of a finite number of orthogonal centrally primitive idempotents $1 = e_1 + e_2 + ... + e_n$. Then, by proposition 2.1.1, we obtain a decomposition of the ring A into a direct sum of right ideals $A = \overset{n}{\underset{i=1}{\oplus}} A_i$, where $A_i = e_i A$. Since e_i is a central idempotent, $A_i = e_i A = Ae_i = e_i A e_i$ is a ring with the identity e_i and $e_i A e_j = e_i e_j A = 0$. Since every idempotent e_i is centrally primitive, in view of proposition 2.4.9, all the rings A_i are indecomposable. Then the two-sided Peirce decomposition of A has the form

$$A = \begin{pmatrix} A_1 & 0 & \dots & 0 \\ 0 & A_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & A_n \end{pmatrix}.$$

But then $A \simeq A_1 \times A_2 \times ... \times A_n$ and so A is an FD-ring.

Conversely, let A be an FD-ring, i.e., $A = A_1 \times A_2 \times ... \times A_n$, where A_i is an indecomposable ring, $i = 1, ..., n$. Put $e_i = (0, ..., 1, ..., 0)$, where the identity of the ring A_i is at the i-th position and zeroes elsewhere. Obviously, $e_i^2 = e_i$ and $e_i e_j = 0$, i.e., $e_1, e_2, ..., e_n$ are pairwise orthogonal idempotents and $1 = e_1 + e_2 + ... + e_n$. Since $e_i a = (0, ..., a_i, ..., 0) = ae_i$, each idempotent e_i is central and therefore $A = \mathcal{I}_1 \oplus \mathcal{I}_2 \oplus ... \oplus \mathcal{I}_n$, where $\mathcal{I}_i = e_i A = Ae_i = e_i A e_i$ is a two-sided ideal in A. Moreover, since A_i is an indecomposable ring, due to lemma 2.4.9, e_i is a centrally primitive idempotent. So we have the following proposition.

Proposition 2.4.10. *A ring A is an FD-ring if and only if the identity of A can be written as a sum of a finite number of orthogonal centrally primitive idempotents.*

As a corollary of propositions 2.4.8 and 2.4.10 we obtain the following main result.

Theorem 2.4.11. *Any FD-ring A can be uniquely decomposed into a direct product of a finite number of indecomposable rings, that is, if $A = B_1 \times B_2 \times ... \times B_s = C_1 \times C_2 \times ... \times C_t$ are two of such decompositions, then $s = t$ and there exists a permutation σ of $\{1, 2, ..., t\}$ such that $B_i = C_{\sigma(i)}$ for $i = 1, 2, ..., t$.*

In view of the Wedderburn-Artin theorem, all semisimple rings are FD-rings. Therefore theorem 2.4.11 is similar to the Krull-Schmidt theorem for semisimple rings. An important class of FD-rings are all right Noetherian (and right Artinian) rings which we shall consider in the next chapter. All semiperfect rings (which may be neither Noetherian nor Artinian rings) are also examples of FD-rings. These rings will be considered in chapter 10.

Now we consider another important class of FD-rings, namely, those rings whose right regular modules can be decomposed into a direct sum of indecomposable right ideals. We are going to show that these rings are really FD-rings.

Suppose a ring A can be decomposed into a direct sum of indecomposable modules. Then from propositions 2.1.1 and 2.4.4 it follows that there is a decomposition of the identity of A into a sum of pairwise orthogonal primitive idempotents:

$$1 = e_1 + e_2 + ... + e_n.$$

Thus, in this case we have a finite set of pairwise orthogonal primitive idempotents $S = \{e_1, e_2, ..., e_n\}$. We shall introduce a binary relation on this set. We define the relation $e \sim f$ for any $e, f \in S$ to mean that there exists $g \in S$ such that $eAg \neq 0$ and $fAg \neq 0$. This relation is obviously symmetric and reflexive. Then it generates some equivalence relation $e \approx f$ such that $e \sim e_{i1} \sim e_{i2} \sim ... \sim e_{ik} \sim f$ for a sequence of idempotents $e_{i1}, ..., e_{ik} \in S$.[2])

Let $E_1, E_2, ..., E_k$ be the equivalence classes of S. Then $S = \bigcup_{i=1}^{k} E_i$ and $E_i \cap E_j = 0$ for $i \neq j$. Denote by u_i the sum of all idempotents from the equivalence class E_i, i.e., $u_i = \sum_{e_{is} \in E_i} e_{is}$. Then each u_i is an idempotent in A and all idempotents $u_1, u_2, ..., u_k$ are pairwise orthogonal with $1 = u_1 + u_2 + ... + u_k$. By the definition of the relations $\sim$ and $\approx$, it follows that $eAf = fAe = 0$ if e and f belong to different equivalence classes. So $u_i A u_j = u_j A u_i = 0$ for $i \neq j$ and $u_i A u_i$ is a ring with the identity u_i for $i = 1, ..., k$. Thus, we have the following two-sided Peirce decomposition of the ring A:

[2]) This relation $\approx$ is the socalled transitive closure of $\sim$.

$$A = \begin{pmatrix} u_1Au_1 & 0 & \dots & 0 \\ 0 & u_2Au_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & u_kAu_k \end{pmatrix}. \tag{2.4.1}$$

The idempotents $u_1, u_2, ..., u_k$ are called the **block idempotents** of A and the rings $u_1Au_1, u_2Au_2, ..., u_kAu_k$ are called the **blocks** of A determined by the set S.

To prove the main theorem about block decompositions we shall need the following lemmas.

Lemma 2.4.12. *For any primitive idempotent $e \in S$ and a central idempotent $c \in A$ we have either $e = ce \in cA$ or $e = (1-c)e \in (1-c)A$.*

Proof. Let c be a nonzero central idempotent of a ring A. If $e \in S$, then $e = ce+(1-c)e$ and $ce, (1-c)e$ are two orthogonal idempotents. Since e is primitive, we obtain that either $ce = 0$ or $(1-c)e = 0$. In the first case $e = (1-c)e \in (1-c)A$ and otherwise $e = ce \in cA$.

Lemma 2.4.13. *Let $e_i, e_j \in S$ and $e_i \approx e_j$. Then for any central idempotent $c \in A$ one has $e_i \in cA$ if and only if $e_j \in cA$.*

Proof. Let $e_i, e_j \in S$ and $e_i \sim e_j$, i.e., there exists an idempotent $f \in S$ such that $e_iAf \neq 0$ and $e_jAf \neq 0$. Suppose $e_i \in cA$, then $e_iAf = e_icAf = e_iA(cf)$. Since $e_iAf \neq 0$, this implies that $cf \neq 0$ and by lemma 2.4.12 $f = cf \in cA$. But then $e_jAf = e_jA(cf) = (ce_j)Af \neq 0$. Hence $ce_j \neq 0$ And, by lemma 2.4.12, $e_j = ce_j \in cA$.

Definition. A ring A is called a **finitely decomposable identity ring** (or for short, a **FDI-ring**) if there exists a decomposition of the identity $1 \in A$ into a finite sum

$$1 = e_1 + e_2 + ... + e_n$$

of pairwise orthogonal primitive idempotents e_i.

Theorem 2.4.14. *Let A be an FDI-ring. If $u_1, u_2, ..., u_k$ are the block idempotents of A determined by the set $S = \{e_1, e_2, ..., e_n\}$, then $u_1, u_2, ..., u_k$ are pairwise orthogonal centrally primitive idempotents with*

$$1 = u_1 + u_2 + ... + u_k.$$

Moreover, each block u_iAu_i $(i = 1, 2, ..., k)$ is an indecomposable ring and we have a decomposition of A in form (2.4.1). This decomposition into a direct product of rings is unique up to a permutation of blocks.

Proof. Taking into account the discussion above it suffices to show that each idempotent u_i is centrally primitive and that the decomposition (2.4.1) is unique.

Let $a \in A$, then since $u_i A u_j = 0$ for $i \neq j$, we have: $u_i a = u_i a(u_1 + u_2 + ... + u_k) = u_i a u_i = (u_1 + u_2 + ... + u_k) a u_i = a u_i$, i.e., each u_i is a central idempotent.

We shall show that u_i is the unique central idempotent in $u_i A u_i$.

Let c be a nonzero central idempotent in $u_i A u_i$. Then $c = c u_i = c \sum_{e_{is} \in E_i} e_{is}$. Since $c \neq 0$, there exists $e_{is} \in E_s$ such that $c e_{is} \neq 0$. From lemma 2.4.12 it follows that $e_{is} \in cA$ and from lemma 2.4.13 this means that $e_{ij} \in cA$ for all $e_{ij} \in E_i$. Thus

$$c = c u_i = c \sum_{e_{is} \in E_i} e_{is} c u_i = \sum_{e_{is} \in E_i} e_{is} = u_i$$

i.e., u_i is the only central idempotent in $u_i A u_i$ and so, by lemma 2.4.9, it is centrally primitive and the ring $u_i A u_i$ is indecomposable.

Corollary 2.4.15. *Any FDI-ring is an FD-ring.*

Remark. Note that the inverse statement to corollary 2.4.15 is not true. There are FD-rings which are not FDI-rings. Here is an example of such a ring. Let A be the set of all countably-dimensional square matrices with entries from an arbitrary field k, so that any matrix of A has only a finite number of nonzero entries. This is a countably-dimensional algebra over k without identity. We adjoin the identity to A in the following way. Consider the algebra $\bar{A}$ consisting of pairs (a, α), where $a \in A$ and $\alpha \in k$, with the componentwise addition and multiplication by scalar, and ring multiplication defined by

$$(a, \alpha)(b, \beta) = (ab + \alpha b + a\beta, \alpha\beta).$$

It is easy to verify that $\bar{A}$ is a countably-dimensional algebra over the field k and that the element $(0, 1)$ is its identity. Obviously, $\bar{A}$ is an indecomposable ring which is not an FDI-ring.

2.5 NOTES AND REFERENCES

The Peirce decomposition was proposed by B.Peirce in his paper *Linear Associative Algebra // Amer. J. Math., 1881, V.4, p.97-229*, were he also introduced and used the notions of idempotent and nilpotent element.

Modern ring theory began when J.H.Wedderburn proved his celebrated classification theorem for finite dimensional semisimple algebras over fields (see *J.H.N.Wedderburn, On hypercomplex numbers// Proc. London Math. Soc., V.6, N.2 (1908), p.77-118*). Twenty years later, E.Noether and E.Artin introduced the ascending chain condition and descending chain condition as substitutes for finite dimensionality, and E.Artin proved the analogue of Wedderburn's theorem for general semisimple rings (see *E.Artin, Zur Theorie der hyperkomplexen Zahlen // Abh. Math. Sem. Univ. Hamburg, 5 (1927), p.251-260*). This theorem, regarded by many as the first major result in the abstract structure theory of rings, has

remained as important today as it was in the early days of the twentieth century when it was first discovered.

There are several different ways to define semisimplicity. J.H.Wedderburn, being interested mainly in finite dimensional algebras over fields, defined the radical of such an algebra A to be the largest nilpotent ideal of A, and defined A to be semisimple if this radical is zero, i.e., if there is no nonzero nilpotent ideal in A. Since we are interested in rings in general, and not just finite dimensional algebras, we have followed a somewhat more modern approach, using the convenient language of modules. Our definition of right semisimple rings is somewhat different from the one Wedderburn originally used.

Searching for the algebraic underpinnings of two-valued logic lead in the XIX-th century to the definition of a Boolean algebra (see *G.Boole, The Mathematical Analysis of Logic // Cambridge and London, 1847* and *G.Boole, An investigation of the Laws of Thought // London, 1854*).

The theory of Boolean algebras is important both from the historical and modern practical points of view. On the one hand, the theory of Boolean algebras is comparatively simple, and on the other hand, it has a very rich structure. This theory, along the theory of mathematical logic and set theory, is related to the foundations of mathematics[3]) and at the same time it found wide applications, in particular, in computer science. Recently the name of G.Boole (1815-1864) has become known even to people far from mathematics and logic. The notions of a Boolean algebra and Boolean variables are now known by all programmers and specialists in computer science.[4])

The general study of Boolean lattices was carried out in 1936 by M.H.Stone in his famous large paper *The theory of representations for Boolean algebras // Trans. Amer. Math. Soc., v.40 (1936), p.37-111.* In this paper M.H.Stone for the first time introduced the notion of a Boolean ring and its connection with Boolean lattices, and he proved his general theorem on representations of a Boolean lattice.

The theory of Boolean algebras has also been perfectly described by R.Sikorski in his book *Boolean algebras, Springer-Verlag, Berlin-Heidelberg-New York, 1964.*

Finite decomposable rings and finite decomposable identity rings arise very naturally though in fact only in this book these notions are first emphasized and their connection with Stone's theorem is made clear.

The proof of theorem 2.4.14 in many points follows the well-known book *T.Y. Lam, A First Course in Noncommutative Rings. Graduate Texts in Mathematics, Vol. 131, Springer-Verlag, Berlin-Heidelberg-New York, 1991.*

---

[3]) In particular Boolean valued models play a major role in set theory and foundatinal mathematics, especially in independence of axioms investigations. (See e.g. *Yu.I.Manin, A course in mathematical logic // Springer, 1977*; *J.Barkley Rosser, Simplified independence proofs. Boolean valued models of set theory // Acad. Pr., 1969*; *Thomas Jech, Set theory // Acad. Pr., 1978.*)

[4]) For an up to date survey of Boolean algebras, see *J.Donald Monk, Robert Bonnet (eds.), Handbook of Boolean algebras (3 volumes)// Elsevier, 1989.*

3. Artinian and Noetherian rings

3.1 ARTINIAN AND NOETHERIAN MODULES AND RINGS

An important role in the theory of rings and modules is played by various finiteness conditions, in particular, chain conditions on submodules and one-sided ideals.

We say that a module M satisfies the **descending chain condition** (or **d.c.c.**) if there does not exist an infinite strictly descending chain

$$M_1 \supset M_2 \supset M_3 \supset ...$$

of submodules of M.

Sometimes the following equivalent formulation of this condition is useful:

A module M satisfies the **descending chain condition** (or **d.c.c.**) if every descending chain of submodules of M

$$M_1 \supseteq M_2 \supseteq M_3 \supseteq ...$$

contains only a finite number of elements, i.e., there exists an integer n such that $M_n = M_{n+1} = M_{n+2} = ...$

Recall that a submodule N of a module M is said to be **minimal** if $N \neq 0$ and there is no submodule L, different from 0 and N, such that $L \subset N \subset M$. We say that a module M satisfies the **minimum condition** if every nonempty family of submodules of M has a minimal element with respect to inclusion.

Proposition 3.1.1. *For a module M the following conditions are equivalent:*

1) *the family of all submodules of M satisfies d.c.c.*;

2) *any nonempty family of submodules of M has a minimal element*[1]) (*with respect to inclusion*).

Proof.

2) $\Rightarrow$ 1). Let $M_1 \supseteq M_2 \supseteq ...$ be a descending chain of submodules of a module M. Because the set of submodules of this sequence has a minimal element M_n, then $M_n = M_{n+1} = ...$

1) $\Rightarrow$ 2). Suppose S is a nonempty set of submodules of a module M without minimal element. Let M_1 be an arbitrary element of this set S. Since M_1 is not minimal, there exists $M_2 \in S$ such that $M_1 \supset M_2$. Since M_2 is not minimal, it contains a submodule M_3 and so on. Continuing this process we obtain a strictly descending infinite chain $M_1 \supset M_2 \supset M_3 \supset ...$ of submodules of M, contradicting to d.c.c.

The proposition is proved.

[1]) Not necessarily an element that is a minimal submodule.

Definition. A module M is called **Artinian** if the equivalent conditions of proposition 3.1.1 are satisfied.

Analogously, in a dual way, we say that a module M satisfies the **ascending chain condition** (or **a.c.c.**) if there does not exist an infinite strictly ascending chain

$$M_1 \subset M_2 \subset M_3 \subset ...$$

of submodules of M.

The equivalent formulation of this condition is follows:

A module M satisfies the **ascending chain condition** (or **a.c.c.**) if every ascending chain of submodules of M

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq ...$$

contains only a finite number of elements, i.e., there exists an integer n such that $M_n = M_{n+1} = M_{n+2} = ...$

Recall that a submodule N of a module M is said to be **maximal** if $N \neq M$ and there is no submodule L, different from M and N, such that $N \subset L \subset M$. We say that a module M satisfies the **maximum condition** if every nonempty family of submodules of M has a maximal element.

The following proposition is dual to proposition 3.1.1 and therefore its proof will be omitted.

Proposition 3.1.2. *For a module M the following conditions are equivalent:*

1) *the family of all submodules of M satisfies a.c.c.;*

2) *any nonempty family of submodules of M has a maximal element (with respect to inclusion).*

Definition. A module M is called **Noetherian** if the equivalent conditions of proposition 3.1.2 are satisfied.

Proposition 3.1.3. *Let N be a submodule of a module M. Then M is Artinian (Noetherian) if and only if M/N and N are both Artinian (Noetherian).*

Proof. First we shall prove the proposition in the Artinian case.

Let M be an Artinian module. Since any descending chain of submodules of N is also a chain of submodules of M, it is immediate that N is Artinian.

Let $\pi : N \to M/N$ be the natural projection and $L_1 \supseteq L_2 \supseteq ...$ be a descending chain of submodules of M/N. Then using lemma 1.3.4 we can form the descending chain of submodules of M, $L'_1 \supseteq L'_2 \supseteq ...$ where $L'_i = \pi^{-1}(L_i)$. Since M is Artinian there exists some n such that $L'_i = L'_n$ for all $i \geq n$. Taking into account that $L_i = \pi(L'_i)$ we also have that $L_i = L_n$ for all $i \geq n$. Thus, M/N is Artinian.

Conversely, assume that modules M/N and N are Artinian. Let $M_1 \supset M_2 \supset ...$ be a descending chain of submodules of the module M. Consider the following

two descending chains of submodules

$$M_1 \cap N \supset M_2 \cap N \supset ...$$

$$(M_1 + N)/N \supset (M_2 + N)/N \supset ...$$

in N and M/N. Then there exists some n such that $M_i \cap N = M_n \cap N$ and $(M_i + N)/N = (M_n + N)/N$ for all $i \geq n$. Hence, $M_i + N = M_n + N$ for all $i \geq n$. Since $M_i \subseteq M_n$ for $i \geq n$, the modular law implies $M_n \cap (M_i + N) = M_i + (M_n \cap N)$. Then $M_n = M_n \cap (M_n + N) = M_n \cap (M_i + N) = M_i + (M_n \cap N) = M_i + (M_i \cap N) = M_i$, i.e., $M_n = M_i$ for all $i \geq n$. Therefore, M is Artinian.

Analogous arguments prove the Noetherian case.

Corollary 3.1.4. *A direct sum of a finite number of modules is an Artinian (resp. Noetherian) module if and only if any summand is Artinian (resp. Noetherian).*

Proposition 3.1.5. *A module is Noetherian if and only if each of its submodules is finitely generated.*

Proof. Assume that every submodule of a module M is finitely generated. We shall show that the module M is Noetherian. Consider an ascending chain $M_1 \subseteq M_2 \subseteq ...$ of submodules of the module M. Denote by T the union of all modules of this chain. The module T is finitely generated, i.e., there exists a finite set of generators $\{x_1, ..., x_s\}$ such that $T = \{x_1, ..., x_s\}$. Obviously then there exists a submodule M_n such that all elements $x_1, ..., x_s$ belong to M_n. Then $M_n = T$ and thus $M_i = M_n$ for all $i \geq n$, establishing a.c.c. for submodules of M. Therefore M is Noetherian.

Conversely, assume that the module M is Noetherian but that there exists a submodule N of M which is not finitely generated. Let $x_1 \in N$ and $x_1 \neq 0$. Then $\{x_1\} \neq N$ and there exists an element $x_2 \in N$ such that $x_2 \notin \{x_1\}$. Continuing this process we obtain an infinite strictly ascending chain of submodules $\{x_1\} \subset \{x_1, x_2\} \subset ....$ This contradicts the a.c.c for M.

This statement has some sort of analog for the Artinian case. For this we need to introduce some definition which is dual to the notion of a finitely generated module. A module M is finitely generated if M is generated by a finite subset of M. This statement is equivalent to the statement:

If $M = \sum_{i \in I} M_i$ is a sum of submodules M_i, then there exists a finite subset $J \subset I$ such that $M = \sum_{i \in J} M_i$.

Definition. An A-module M is said to be **finitely cogenerated** if for any family M_i, $i \in I$, of submodules of M, $\bigcap_{i \in I} M_i = 0$ implies $\bigcap_{i \in J} M_i = 0$ for some

finite subset J of I.[2])

Example 3.1.1.
Any finite dimensional vector space V over a field k is finitely cogenerated.

Example 3.1.2.
The regular module $\mathbf{Z}_{\mathbf{Z}}$ is not a finitely cogenerated, since $\bigcap p\mathbf{Z} = 0$, where p runs over all primes, but for any finite subset of prime numbers p_1, p_2,..., p_m we have $\bigcap_{i=1}^{m} p_i\mathbf{Z} \neq 0$.

The following proposition is dual to proposition 3.1.5 and therefore its proof will be omitted.

Proposition 3.1.6. *A module is Artinian if and only if each of its quotient modules is finitely cogenerated.*

We are going to consider properties of endomorphisms of Artinian and Noetherian modules.

Proposition 3.1.7. *An endomorphism φ of an Artinian (resp. Noetherian) module is an automorphism if and only if φ is a monomorphism (resp. epimorphism).*

Proof. Let φ be an endomorphism of a Noetherian module M which is an epimorphism. We shall show that $Ker\varphi = 0$. There is the ascending chain of submodules: $0 \subset Ker\varphi \subset Ker\varphi^2 \subset ...$ which must stabilize, i.e., $Ker\varphi^n = Ker\varphi^{n+1}$. Let $m \in Ker\varphi$. From the fact that φ^n is an epimorphism we obtain that $m = \varphi^n m_1$. But then $m_1 \in Ker\varphi^{n+1} = Ker\varphi^n$, i.e., $m = 0$.

Now, let's show that a monomorphism φ of an Artinian module M is an epimorphism. There is the descending chain of submodules $M \supset Im\varphi \supset Im\varphi^2 \supset ...$ which must stabilize, i.e., $Im\varphi^n = Im\varphi^{n+1}$. Therefore, for an arbitrary $m \in M$ there is an equality $\varphi^n m = \varphi^{n+1} m_1$, $m_1 \in M$. Since φ^n is a monomorphism, $m = \varphi m_1$, i.e., φ is an epimorphism.

The following proposition is known as Fitting's lemma.[3])

Proposition 3.1.8 (Fitting's lemma). *For any endomorphism φ of an Artinian and Noetherian module M there exists an integer n such that $M = Im\varphi^n \oplus Ker\varphi^n$.*

[2]) This is essentially a compactness notion. More precisely such modules are linearly compact with respect to the discrete topology. (See *V.I.Arnautov, Linearly-compact module, In: M.Hazewinkel (ed.), Encyclopaedia of Mathematics. Vol.5, p.526, KAP, 1990*, and *N.Bourbaki, Algébre commutative, Chapt.3, Hermann, 1961.*)

[3]) Usually the Fitting lemma is just stated for endomorphisms of finite dimensional vector spaces. Even Fitting's original paper went deeper than that.

Proof. Since M is both an Artinian and Noetherian module, for any endomorphism φ of M both chains of submodules

$$M \supseteq Im\varphi \supseteq Im\varphi^2 \supseteq ... \supseteq Im\varphi^n \supseteq Im\varphi^{n+1} \supseteq ...$$

and

$$0 \subseteq Ker\varphi \subseteq Ker\varphi^2 \subseteq ... \subseteq Ker\varphi^n \subseteq Ker\varphi^{n+1} \subseteq ...$$

must stabilize. Therefore there exists an n such that $Im\varphi^n = Im\varphi^m$ and $Ker\varphi^n = Ker\varphi^m$ for all $m \geq n$. Let $x \in Im\varphi^n \cap Ker\varphi^n$, then $\varphi^n(x) = 0$ and $x = \varphi^n(y)$ for some $y \in M$. Therefore $0 = \varphi^n(x) = \varphi^{2n}(y) = \varphi^n(y) = x$, i.e., $Im\varphi^n \cap Ker\varphi^n = 0$.

On the other hand, for every element $m \in M$ there holds the equality $\varphi^n(m) = \varphi^{2n}(m_1)$, i.e., $\varphi^n(m - \varphi^n m_1) = 0$ and $m = \varphi^n m_1 + (m - \varphi^n m_1)$. This yields the decomposition of the module M into the direct sum of $Im\varphi^n$ and $Ker\varphi^n$.

Corollary 3.1.9. *If M is indecomposable and both an Artinian and a Noetherian module, then any endomorphism of M is either an automorphism or nilpotent.*

Proposition 3.1.10. *The following conditions are equivalent for a semisimple module M:*

(a) *M is Artinian;*

(b) *M is Noetherian;*

(c) *M is a direct sum of a finite number of simple modules.*

Proof. Since a simple module is both Noetherian and Artinian, implications $(c) \Rightarrow (a)$ and $(c) \Rightarrow (b)$ are true by corollary 3.1.4.

Conversely, suppose a module M is decomposed into an infinite direct sum of simple modules: $M = U_1 \oplus U_2 \oplus U_3 \oplus .....$ Then in the module M there are two chains of submodules: $U_1 \subset U_1 \oplus U_2 \subset ...$ and $M \supset U_2 \oplus U_3 \oplus ... \supset U_3 \oplus U_4 \oplus ....$ From the existence of these chains there follow the remaining statements of the proposition.

Definition. A ring A is called a **right** (**left**) **Artinian** (resp. **Noetherian**) if the right regular module A_A (left regular module ${}_AA$) is Artinian (resp. Noetherian). A ring A is called **Artinian** (resp. **Noetherian**), if it is right and left Artinian (resp. Noetherian).

From corollary 3.1.4, proposition 3.1.10 and the Wedderburn-Artin theorem we immediately obtain the following corollary:

Corollary 3.1.11. *A semisimple ring is both Artinian and Noetherian.*

Example 3.1.3.

Let V be an n-dimensional vector space over a field k. Then V is both Noetherian and Artinian. For, if W is a proper subspace of V, then $dimW < dimV = n$. Thus any proper ascending (or descending) chain of subspaces cannot have more than $n + 1$ terms.

Example 3.1.4.
Any principal ideal domain A is a Noetherian ring, because every ideal is principal (see proposition 1.1.4).

Example 3.1.5.
The ring of integers $\mathbf{Z}$ is a Noetherian ring, since it is a PID. But it is not Artinian. For example, we may form the infinite properly descending chain of ideals:

$$(n) \supset (n^2) \supset (n^3) \supset ...$$

Example 3.1.6.
Now we present an example of a ring which is right Artinian and right Noetherian but it is neither left Artinian nor left Noetherian.

Let $A = \begin{pmatrix} \mathbf{Q} & \mathbf{R} \\ 0 & \mathbf{R} \end{pmatrix} = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} \ : \ \alpha \in \mathbf{Q}; \beta, \gamma \in \mathbf{R} \right\}$, i.e., A is a subring of the algebra of upper triangle matrices $T_2(\mathbf{R})$ of order two over the field of real numbers such that the entry at position (1,1) is rational.

It is not difficult to verify that the right ideals in the ring A are A, $e_{11}A$, $e_{22}A$ and the various $\mathbf{R}$-subspaces of the two-dimensional space $\begin{pmatrix} 0 & \mathbf{R} \\ 0 & \mathbf{R} \end{pmatrix}$. Hence, it easily follows that the ring A is right Artinian and right Noetherian. At the same time $\mathbf{Q}$-subspaces in $\begin{pmatrix} 0 & \mathbf{R} \\ 0 & 0 \end{pmatrix}$ are left ideals of the ring A. Since $\mathbf{R}$ is an infinite space over $\mathbf{Q}$, it is not difficult to build an infinite strictly ascending (or descending) chain of left ideals. This shows that the ring A is neither left Artinian nor left Noetherian.

Proposition 3.1.12. *If A is a right Noetherian (resp. Artinian) ring, then any finitely generated right A-module M is Noetherian (resp. Artinian).*

Proof. If M is a finitely generated A-module, then it is isomorphic to a quotient module F/K, where F is a finitely generated free A-module and K is a submodule of F. Since F is isomorphic to a direct sum of a finite number of copies of the Noetherian (resp. Artinian) module A_A, it is Noetherian (resp. Artinian), by corollary 3.1.4. Then, by proposition 3.1.3, M must be Noetherian (resp. Artinian).

Corollary 3.1.13. *If A is a right Noetherian ring, then any submodule of finitely generated right A-module M is finitely generated.*

Proof. This follows from proposition 3.1.12 and proposition 3.1.5.

3.2 THE JORDAN-HÖLDER THEOREM

Definition. A finite chain of submodules of a module M: $0 = M_0 \subset M_1 \subset ... \subset M_n = M$ is called a **composition series** for the module M if all quotient

modules M_{i+1}/M_i are simple ($i = 0, 1, ..., n-1$). The quotient modules M_{i+1}/M_i are called the **factors** of this series and the number n is the **length of the series**. By convention, the zero module is considered to have a composition series of length zero with no composition factors.

Evidently, not every module has a composition series (for example, the ring $\mathbf{Z}$ considered as a module over itself).

We shall say that a finite chain $0 \subset M_1 \subset ... \subset M_t = M$ of submodules of a module M can be included into a chain of submodules: $0 \subset L_1 \subset ... \subset L_s = M$ if each M_i ($i = 1, 2, ..., t$) is some L_j ($j = 1, 2, ..., s$). The number t is called the **length of the chain** $0 \subset M_1 \subset ... \subset M_t = M$.

Theorem 3.2.1 (Jordan-Hölder). *If a module M has a composition series, then any finite chain of submodules of M can be included in a composition series. The lengths of any two composition series of the module M are equal and between the factors of these series one can establish a bijection in such a way that the corresponding factors are isomorphic.*

Proof. Let $0 = M_0 \subset M_1 \subset .... \subset M_n = M$ be a composition series of the module M. We shall prove the theorem by induction on n. If $n = 1$, then the module M is simple and everything is proved. Let $0 = N_0 \subset N_1 \subset ... \subset N_t = M$ be an arbitrary finite chain of submodules of M. If $N_{t-1} = M_{n-1}$, then in $M_{n-1} = N_{t-1}$ there exists a composition series of the length $n-1$ and M/N_{t-1} is a simple module. Therefore by the induction hypothesis the chain $0 = N_0 \subset N_1 \subset ... \subset N_t = M$ can be included in a composition series of length $n-1$ with factors that are isomorphic to factors of the composition series $0 = M_0 \subset M_1 \subset ... \subset M_{n-1}$. In this case the theorem is proved.

Let $N_{t-1} \neq M_{n-1}$. Since the quotient module M/M_{n-1} is simple, $M_{n-1} + N_{t-1} = M$. In view of theorem 1.3.3, $M/N_{t-1} = (M_{n-1} + N_{t-1})/N_{t-1} \simeq M_{n-1}/(M_{n-1} \cap N_{t-1})$. From the induction hypothesis for the module M/N_{t-1} there exists a composition series. Since $M/M_{n-1} = (M_{n-1} + N_{t-1})/M_{n-1} \simeq N_{t-1}/(M_{n-1} \cap N_{t-1})$ is a simple module and, by the induction hypothesis, the length of the composition series of the module $M_{n-1} \cap N_{t-1}$ does not exceed $n-2$, we obtain that in the module N_{t-1} the lengths of all composition series are not more than $n-1$. Therefore the chain of submodules $N_{t-1} \supset N_{t-2} \supset .... \supset N_0 = 0$ can be included in a composition series. But then the entire chain $0 = N_0 \subset N_1 \subset ... \subset N_t = M$ can be included in a composition series.

Let $0 \subset M_1 \subset ... \subset M_n = M$ and $0 \subset K_1 \subset ... \subset K_t = M$ be two composition series for the module M. We shall show that their lengths are equal and that their factors are isomorphic. One may assume that $M_{n-1} \neq K_{t-1}$. Then $M_{n-1} + K_{t-1} = M$, moreover, the quotient modules $M/M_{n-1} \simeq K_{t-1}/(M_{n-1} \cap K_{t-1})$ and $M/K_{t-1} \simeq M_{n-1}/(M_{n-1} \cap K_{t-1})$ are simple. We now construct a composition series for the module $M_{n-1} \cap K_{t-1}$. By the induction hypothesis its length is equal to $n-2$. But then the module K_{t-1} has a composition series of length $n-1$.

Therefore all composition series of K_{t-1} have length equal to $n-1$. Thus $n=t$. By the induction hypothesis the factors of the composition series $M_{n-1} \supset M_{n-2} \supset ... \supset M_0 = 0$ and $M_{n-1} \supset M_{n-1} \cap K_{n-1} \supset ... \supset 0$ are isomorphic. In a similar way the factors of $K_{n-1} \supset K_{n-2} \supset ... \supset K_0 = 0$ and $K_{n-1} \supset M_{n-1} \cap K_{n-1} \supset ... \supset 0$ are isomorphic. Taking into account the isomorphisms mentioned above we obtain that the factors of the initial series for some bijective correspondence are pairwise isomorphic. The theorem is proved.

Proposition 3.2.2. *A module M has a composition series if and only if M is both Artinian and Noetherian.*

Proof. Let M be both a Noetherian and Artinian module. Then there exists a nonzero minimal submodule M_1 of M. In the set of modules, which strictly contain M_1, we choose the minimal element M_2. Obviously, the quotient module M_2/M_1 is simple. Continuing this process we obtain an ascending chain of submodules $0 = M_0 \subset M_1 \subset M_2 \subset ...$ with simple factors that must stabilize because the module M is Noetherian.

Conversely, let the module M have a composition series of length n. Suppose that M is not Artinian. Then there is a strictly descending chain of submodules of M with respect to inclusion, whose length is equal to $n+1$. Clearly, it cannot be included in a composition series of length n. This contradicts the Jordan-Hölder theorem. Analogously, it can be proved that the module M is Noetherian. The proposition is proved.

Definition. A module M is called a **module of finite length** if M is both Artinian and Noetherian. The length of its composition series is called the **length** of the module M and denoted by $l(M)$. The factors of the composition series are called the **simple factors** of M.

In view of the Jordan-Hölder theorem, the definitions of length and simple factors do not depend on the choice of the composition series.

The next two propositions immediately follow from the Jordan-Hölder theorem.

Proposition 3.2.3. *Let a module M have a composition series and let N be a submodule of M. Then $l(M) = l(N) + l(M/N)$.*

Proposition 3.2.4. *Let K and L be submodules of a module M and let the module $K+L$ have a composition series. Then*

$$l(K+L) + l(K \cap L) = l(K) + l(L).$$

Proposition 3.2.5 (The Krull-Schmidt theorem for semisimple modules). *If $M = U_1 \oplus ... \oplus U_n = V_1 \oplus ... \oplus V_m$ are two decompositions of a semisimple module M into a direct sum of simple modules, then $m = n$ and, after a suitable permutation, $U_i \simeq V_i$ for $i = 1, ..., n$.*

Proof. Obviously, $0 \subset U_1 \subset U_1 \oplus U_2 \subset ... \subset U_1 \oplus ... \oplus U_n = M$ and $0 \subset V_1 \subset V_1 \oplus V_2 \subset ... \subset V_1 \oplus ... \oplus V_m = M$ are two composition series of the module M with simple factors $U_1, ..., U_n$ and $V_1, ..., V_m$, respectively. Therefore the statement immediately follows from the Jordan-Hölder theorem.

3.3 THE HILBERT BASIS THEOREM

Let A be a ring. Along with the ring A we can consider the polynomial ring in one variable x with coefficients in the ring A. This ring is denoted by $A[x]$. The aim of this section is to prove the following theorem:

Theorem 3.3.1 (Hilbert basis theorem). *Let A be a right Noetherian ring. Then the ring $A[x]$ is right Noetherian as well.*[4])

Proof. Let the ring A be right Noetherian and let $\mathcal{I}$ be an arbitrary right ideal in the ring $A[x]$. Clearly, the set

$$\hat{\mathcal{I}} = \{a_n \in A \quad : \quad a_0 + a_1 x + ... + a_n x^n \in \mathcal{I},\ a_n \neq 0\} \cup \{0\}$$

forms a right ideal in A. By proposition 3.1.5, the ideal $\hat{\mathcal{I}}$ is finitely generated. Therefore there is a finite set of generators $b_1, ..., b_s$ such that $\hat{\mathcal{I}} = \{b_1, ..., b_s\}$. Denote by $f_i(x)$ a polynomial of $\mathcal{I}$ with the leading coefficient b_i: $f_i(x) = b_i x^{n_i} + ...$ $(i = 1, ..., s)$ and denote by n the largest number among all such numbers n_i.

Let $f(x)$ be an arbitrary polynomial of $\mathcal{I}$. We shall show that $f(x)$ can be expressed in the form:

$$f(x) = f_1(x)g_1(x) + ... + f_s(x)g_s(x) + h(x),$$

where the degree of the polynomial $h(x)$ does not exceed $n-1$. Let m be the degree of $f(x)$ and let a be its leading coefficient. If $m < n$, then everything is proved. Let $m \geq n$. We have $a = \sum\limits_{i=1}^{s} b_i c_i$, where $c_1, ..., c_s \in A$. Consider the polynomial

$$t_1(x) = f(x) - \sum_{i=1}^{s} c_i f_i(x) x^{m-n_i}.$$

Evidently, $t_1(x) \in \mathcal{I}$ and the degree of $t_1(x)$ is strictly less than m. If the degree of the polynomial $t_1(x)$ exceeds $n-1$, then applying to it the construction mentioned above we obtain a polynomial $t_2(x)$, whose degree is strictly less than the degree of $t_1(x)$. Continuing this process we obtain the needed form.

The coefficients at x^{n-i} in the polynomials of the ideal $\mathcal{I}$, whose degrees are not more than $n-i$ $(i = 1, ..., n)$, form an ideal L_i in the ring A. Denote by $d_1^i, ..., d_{s_i}^i$

[4]) Hilbert originally proved his basis theorem (1890) with a view towards invariant theory (finiteness of a system of generating invariants), which, at the time, was very calculatory. It was a revolution. A contemporary wrote "this is not mathematics, this is theology".

systems of generators of the ideal L_i and by $f_j^i(x)$ a polynomial of degree $n-i$ of $\mathcal{I}$ with the leading coefficient d_j^i $(i=1,...,n; j=1,...,s_i)$. It is easy to verify that the polynomials $h(x) \in \mathcal{I}$, whose degrees do not exceed $n-1$, can be expressed by the polynomials $f_j^i(x)$. Therefore a system of generators of the ideal $\mathcal{I}$ is formed by the polynomials $f_1(x),...,f_s(x)$ and $f_j^i(x)$ $(i=1,...,n; j=1,...,s_i)$. The theorem is proved.

Corollary 3.3.2. *If A is a right Noetherian ring, then the polynomial ring $A[x_1,...,x_n]$ is right Noetherian.*

Proof. The proof is immediate from the previous theorem by induction on the number of variables n.

3.4 THE RADICAL OF A MODULE AND A RING

Let M be an arbitrary A-module. Denote by $radM$ the intersection of all its maximal submodules. By convention, if M does not have maximal submodules we define $radM = M$. This submodule is called the **radical of the module** M.

For any nonzero homomorphism $\varphi : M \to U$, where U is a simple A-module, we have $Im\varphi = U$. Therefore, by the homomorphism theorem, $M/Ker\varphi \simeq U$ is a simple module. Therefore $Ker\varphi$ is a maximal submodule of M. Conversely, for any maximal submodule $M_1 \subset M$ we can build the projection $\pi : M \to M/M_1$ for which $Ker\varphi = M_1$ and M/M_1 is a simple module. Thus, we can give an equivalent definition of the radical of the module M:

Proposition 3.4.1. $radM = \{ \cap Ker\varphi \ : \ \varphi$ *runs through all homomorphisms of M to all simple modules* $\}$.

Remark. The inclusion $radM \subset M$ is not always strict. For example, denote by $\mathbf{Z}_{(p)}$ the ring of p-integral numbers (where p is a prime integer), i.e., $\mathbf{Z}_{(p)} = \{\frac{m}{n} \in \mathbf{Q} \ : \ (n,p)=1\}$. Clearly, $\mathbf{Q}$ may be considered as a $\mathbf{Z}_{(p)}$-module and, so considered, $rad\mathbf{Q} = \mathbf{Q}$.

Proposition 3.4.2. *Let $f : M \to N$ be a homomorphism of A-modules. Then $f(radM) \subset radN$.*

Proof. Let $m \in radM$. We need to show that for any homomorphism $\varphi : N \to U$, where U is a simple module, $\varphi(f(m)) = 0$. Obviously, φf is a homomorphism of the module M to the simple module U. Since $m \in radM$, we conclude that $\varphi f(m) = 0$, as required.

Proposition 3.4.3. $rad\ (\underset{\alpha\in I}{\oplus} M_\alpha) = \underset{\alpha\in I}{\oplus} radM_\alpha$.

Proof. Let $\psi : M = \underset{\alpha\in I}{\oplus} M_\alpha \to U$ be a homomorphism of the module M to a simple module U. Let $\pi_\alpha : M \to M_\alpha$ be the projection of M onto M_α and

$i_\alpha : M_\alpha \to M$ be the natural inclusion of M_α into M. Then the homomorphism ψ satisfies the formula $\psi(m) = \sum\limits_{\alpha\in I} \psi i_\alpha \pi_\alpha(m) = \sum\limits_{\alpha\in I} \psi_\alpha(m_\alpha)$, where $\psi_\alpha = \psi i_\alpha$ is a homomorphism of M_α to the simple module U. Hence, if $m_\alpha \in radM_\alpha$, then $\psi_\alpha(m_\alpha) = 0$ for all $\alpha \in I$. Therefore $m = \sum_{\alpha\in I} m_\alpha \in radM$ as well.

Let $m = \sum_{\alpha\in I} m_\alpha \in radM$ and let ψ_α be the family of homomorphisms of M_α to a simple module U ($\alpha \in I$). Consider a homomorphism φ_α from M to U defined as $\varphi_\alpha(m) = \psi_\alpha\pi_\alpha(m) = \psi_\alpha(m_\alpha)$. Since $m \in radM$, we have $\varphi_\alpha(m) = 0$, and hence $\psi_\alpha(m_\alpha) = 0$, i.e., $m_\alpha \in radM_\alpha$, for all $\alpha \in I$.

Recall that a right (resp. left, two-sided) ideal $\mathcal{M}$ in a ring A is called **maximal** in A if there is no right (resp. left, two-sided) ideal $\mathcal{I}$, different from $\mathcal{M}$ and A, such that $\mathcal{M} \subset \mathcal{I} \subset A$.

By proposition 1.1.3, in any nonzero ring with identity always there exist maximal proper right (left) ideals.

An important role in the theory of rings is played by the notion of the Jacobson radical.

Definition. The intersection of all maximal right ideals in a ring A is called the **Jacobson radical** of A.

Denote by $R = radA$ the Jacobson radical of a ring A. We shall call the Jacobson radical of A simply the **radical**.

In the definition of the radical of a ring we have used maximal right ideals. So it should really be called the right radical of a ring and in a similar way we should introduce the notion of the left radical of a ring. Fortunately, the definitions of the right and left radical coincide. The next thing to show is that $radA$ coincides with the intersection of all maximal left ideals of the ring A.

In view of proposition 3.4.1, the radical of a ring A coincides with the intersection of all $Ker\psi$, where ψ runs over all homomorphisms from A, as a right A-module, to all simple A-modules.

Proposition 3.4.4. *The radical R of a ring A is a two-sided ideal.*

Proof. Evidently, R is a right ideal. Consider an endomorphism $\varphi : A \to A$ (as a right module over itself) given by the formula $\varphi(a) = a_0 a$, where $a_0, a \in A$. By proposition 3.4.2, $a_0 r \in R$ for any $r \in R$, $a_0 \in A$.

Proposition 3.4.5. *The radical R of a ring A coincides with the set of all elements $r \in A$ such that the element $1 - ra$ is right invertible for all $a \in A$.*

Proof. Let $r \in R$, $a \in A$. Consider the right ideal $(1 - ra)A$. If $(1 - ra)A = A$, then the element $1 - ra$ is right invertible. If $(1 - ra)A \neq A$, then $(1 - ra)A$ is contained in a proper maximal right ideal $\mathcal{I}$. Then $1 - ra \in \mathcal{I}$. Since $ra \in R \subset \mathcal{I}$, we obtain that $1 \in \mathcal{I}$. A contradiction.

Let now $1-ra$ be right invertible for all a. If $r \notin R$, then there exists a proper maximal right ideal $\mathcal{J}$ such that $r \notin \mathcal{J}$. Hence, $rA + \mathcal{J} = A$, i.e., $1 = ra + j$ and the element $j = 1 - ra$ is not right invertible. A contradiction.

Proposition 3.4.6. *The radical of a ring is the largest (with respect to inclusion) two-sided ideal R among all two-sided ideals $\mathcal{I}$ such that $1 - i$ is two-sided invertible for all $i \in \mathcal{I}$.*

Proof. By the previous proposition, R contains any such ideal $\mathcal{I}$. We are going to show the invertibility of $1-r$ for any $r \in R$. We know that $1-r$ is right invertible, i.e., $(1 - r)x = 1$. It follows that $1 - x = -rx \in R$ and so $1 - (1 - x) = 1 + rx$ is right invertible, i.e., $xy = 1$ for some y. But $(1 - r)xy = ((1 - r)x)y = y$, i.e., $y = 1 - r$ and so the element $1 - r$ is left invertible.

In view of symmetry of proposition 3.4.6, there is the following consequence:

Proposition 3.4.7. *The radical of a ring coincides with the intersection of all maximal left ideals.*

An important fact, which in many cases helps to calculate the radical of a ring, is given by the following proposition.

Proposition 3.4.8. *Let $e^2 = e \in A$. Then $rad(eAe) = eRe$, where R is the radical of A.*

Proof. Assume $r \in eRe$. We shall show that for any $a = ebe \in eAe$ the element $e - ra$ is right invertible in the ring eAe. By proposition 3.4.5, the element $1 - ra$ is right invertible in A. From $a \in eAe$ it follows that there exists an element y such that $(1 - ra)y = 1$. Multiplying this equality on the right and on the left by e we obtain $(e - ra)eye = e$, i.e., $e - ra$ is right invertible in eAe. By proposition 3.4.5, $r \in rad(eAe)$.

Assume $r = ere \in rad(eAe)$. Then for any $a \in A$ the element $e - rae$ is right invertible in the ring eAe, i.e., $(e - rae)y = e$, where $y = eye$. Set $e = e_1$ and $e_2 = 1-e_1$. Then $e_1e_2 = e_2e_1 = 0$ and $e_2^2 = e_2$. Write for the element $1-ra$ its two-sided Peirce decomposition with respect to the decomposition $1 = e_1 + e_2$ in the form of a matrix of the order two: $1 - ra = \begin{pmatrix} e_1 - rae_1 & -rae_2 \\ 0 & e_2 \end{pmatrix}$. Multiplying $1 - ra$ on the right by the matrix $Y_1 = \begin{pmatrix} y & 0 \\ 0 & e_2 \end{pmatrix}$ we obtain $(1-ra)Y_1 = \begin{pmatrix} e_1 & -rae_2 \\ 0 & e_2 \end{pmatrix}$. Multiplying $(1 - ra)Y_1$ on the right by the matrix $\begin{pmatrix} e_1 & rae_2 \\ 0 & e_2 \end{pmatrix}$ we obtain the identity of the ring A. Hence, the element $1 - ra$ is invertible in R. Therefore we have that $rad(eAe) \subset R$. Hence, $rad(eAe) = eRe$. The proposition is proved.

The following proposition is often useful.

Proposition 3.4.9. *Let M be a right A-module, and let R be the radical of the ring A. Then $MR \subset radM$.*

For any $m \in M$ we define the homomorphism $\psi : A \to M$ by the formula $\psi(1) = m$. Then $\psi(R) = mR$ is a submodule of M and by proposition 3.4.2 it belongs to $radM$ for any $m \in M$, as required.

Proposition 3.4.10. *Let $B = M_n(A)$ be the ring of all square matrices of order n over a ring A with radical R. Then $rad(M_n(A)) = M_n(R)$.*

Proof. We shall prove this proposition by induction on the order n. For $n = 2$ let e_{ij} be the matrix units[5]) of the ring B and $X = rad(M_2(B))$. By proposition 3.4.8, we have $e_{11}Xe_{11} = R$ and $e_{22}Xe_{22} = R$. Suppose, $\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \in X$. Then $\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in X$, which implies $a \in R$. So, $e_{11}Xe_{22} = R$. Analogously, $e_{22}Xe_{11} = R$. Thus, $rad(M_2(A)) = M_2(R)$. Let $n \geq 3$ and $X = rad(M_n(A))$. Write $f_1 = e_{11} + ... + e_{n-1,n-1}$, $f_2 = e_{22} + ... + e_{nn}$, $f_3 = e_{11} + e_{nn}$. Then by the induction hypothesis $f_1Xf_1 = M_{n-1}(R)$, $f_2Xf_2 = M_{n-1}(R)$ and by the above $f_3Xf_3 = M_2(R)$. The proposition is proved.

The following Nakayama lemma plays an important role in many circumstances.

Lemma 3.4.11 (Nakayama's Lemma). *Let M be a finitely generated A-module and $MR = M$. Then $M = 0$.*

Proof. Let $m_1, ..., m_s$ be a minimal system of generators of a nonzero module M. Since $M = MR$, any $m \in M$ can be written in the form $m = \sum_{i=1}^{s} m_i r_i$, where $r_1, ..., r_s \in R$. In particular, $m_1 = m_1 r_1 + ... + m_s r_s$. Consequently, $m_1(1 - r_1) = m_2 r_2 + ... + m_s r_s$. Since the element $1 - r_1$ is invertible, we obtain $m_1 = m_2 a_2 + ... + m_s a_s$ which contradicts the minimality property of s.

Nakayama's lemma is often used in the following form:

Lemma 3.4.12 (Nakayama's Lemma, version 2). *Let N be a submodule of a finitely generated module M and $N + MR = M$. Then $N = M$.*

To prove this statement it suffices to apply Nakayama's lemma to the quotient module M/N.

3.5 THE RADICAL OF ARTINIAN RINGS

Historically, the notion of the radical was first introduced by E.Cartan for finite

[5]) I.e., the matrices with a 1 at position (i, j) and zeros everywhere else.

dimensional nonassociative algebras and later was developed by T.Molien and J.H.M.Wedderburn for studying the structure of finite dimensional associative algebras over fields. Some years later E.Artin considered a new class of rings which satisfied descending chain conditions (these rings are now called Artinian rings) and extended Wedderburn's theory and the notion of the radical to these rings. I.M.Gel'fand introduced the notion of the radical for a normed ring as the intersection of all its maximal ideals. Finally, N.Jacobson introduced a generalization of the notion of the radical to arbitrary rings, which now is known as the Jacobson radical. For Artinian rings the Jacobson radical coincides with the classical Wedderburn radical. Therefore it is interesting to study the properties of the radical for an Artinian ring.

Definition. An ideal $\mathcal{I}$ is called **nilpotent** if there exists a natural number n such that $\mathcal{I}^n = 0$.

Note that $\mathcal{I}^n = 0$ means that $a_1 a_2 ... a_n = 0$ for any n elements $a_1, a_2, ..., a_n \in \mathcal{I}$.

Proposition 3.5.1 (C.Hopkins). *The radical R of a right Artinian ring A is nilpotent.*

Proof. Let R be the radical of the ring A. Consider the set of all natural powers R^n of the radical R. In this set there exists a minimal element $X = R^n$. Obviously, $X^2 = X$. Suppose $X \neq 0$ and let Y be a minimal element in the set of all right ideals Z of A such that $Z \subset X$ and $ZX \neq 0$. Evidently, $yX \neq 0$ for some $y \in Y$ and $(yX)X = yX^2 = yX \neq 0$. Therefore $yX = Y$ and, hence, $yx = y$ for some $x \in X$. We have $y(1 - x) = 0$. Since $x \in X \subset R$, by proposition 3.4.6 the element $1 - x$ is invertible. Therefore $y = 0$. A contradiction.

Definition. An element a is called **nilpotent** if there exists a positive integer n such that $a^n = 0$. An ideal is called a **nil-ideal** if all its elements are nilpotent.

Remark. There exist nil-ideals which are not nilpotent, as can be seen from the following example.

Example 3.5.1.

Let $A = k[x_1, ..., x_n, ...]$ be the polynomial ring over a field k in a countable number of variables x_1, x_2, ..., x_n,... and let J be the ideal generated by the set of polynomials $\{x_1^2, x_2^3, ..., x_n^{n+1}, ...\}$. Then in the quotient ring $\overline{A} = A/J$ the ideal generated by images (under the natural projection $A \to \overline{A}$) of polynomials without constant terms is, obviously, a nil-ideal but it is not a nilpotent ideal.

Proposition 3.5.2. *The radical of a ring A contains all one-sided nil-ideals.*

Here is a proof of this proposition for a right nil-ideal $\mathcal{J}$ taking into account that by proposition 3.4.6 for left ideals one may use the left variant of proposition 3.4.5.

Let r be a nilpotent element and $r^n = 0$. Then $(1-r)(1+r+r^2+...+r^{n-1}) = 1$

and so $1 - r$ is an invertible element. Therefore for any $i \in \mathcal{J}$ and all $a \in A$ the element $1 - ia$ is invertible in A and by proposition 3.4.5 $\mathcal{J} \subset R$.

Corollary 3.5.3. *The Jacobson radical of a right Artinian ring is the largest nilpotent ideal containing all one-sided nilpotent ideals.*

Definition. A ring A is called **semiprimitive** if its Jacobson radical is equal to zero.

The ring of integers $\mathbf{Z}$ and the ring of all square matrices over a division ring are semiprimitive. At the same time the ring of p-integral numbers $\mathbf{Z}_{(p)}$ is not semiprimitive though its structure (in a way) is simpler than that of $\mathbf{Z}$.

Proposition 3.5.4. *If R is the radical of a ring A, then the quotient ring A/R is semiprimitive.*

The proof is left to the reader as an exercise.

Theorem 3.5.5. *The following statements are equivalent for a ring A:*
(a) A is semisimple;
(b) A is right Artinian and semiprimitive.

Proof.
$(a) \Rightarrow (b)$. Obviously, the radical of a simple module is equal to zero. Therefore this implication follows from proposition 3.4.3.

$(b) \Rightarrow (a)$. Let $R = 0$. Then $\cap \mathcal{I}_\alpha = 0$, where $\mathcal{I}_\alpha$ runs through all maximal right ideals of the ring A. Because the ring A is right Artinian, we can choose a finite number of maximal right ideals $\mathcal{I}_1, ..., \mathcal{I}_n$ such that $\bigcap_{k=1}^{n} \mathcal{I}_k = 0$. Denote by ψ_i the natural projection of the ring A onto $A/\mathcal{I}_k$ $(k = 1, ..., n)$. We set $\psi(a) = (\psi_1(a), ..., \psi_n(a))$. Evidently, ψ is a monomorphism of the right module A into a semisimple module $\bigoplus_{k=1}^{n} A/\mathcal{I}_k$. By proposition 2.2.4 the module A_A is semisimple.

Theorem 3.5.6. *A right Artinian ring A is right Noetherian.*

Proof. Consider in the ring A a strictly descending chain of powers of the radical R: $A \supset R \supset R^2 \supset ... \supset R^{n-1} \supset R^n = 0$. All quotient modules A/R, R/R^2,..., R^{n-1}/R^n are Artinian. At the same time, they are modules over the ring A/R which is semisimple by theorem 3.5.5. Then by theorem 2.2.5 and proposition 3.1.10 each of these modules can be decomposed into a direct sum of a finite number of indecomposable modules. Therefore they are Noetherian. Thus, the modules $R^{n-1}/R^n = R^{n-1}$ and R^{n-2}/R^{n-1} are Noetherian. Hence, by proposition 3.1.3, the module R^{n-2} is Noetherian. Continuing this process in a similar way we obtain that all modules R^{n-1}, R^{n-2},...,R, A are Noetherian, as required.

Remark. Note that the example of the ring of integers shows that the inverse statement is not true.

Recall that a ring A is called **simple** if it has no proper two-sided ideals.

Proposition 3.5.7. *A right Artinian ring A is simple if and only if it is isomorphic to the ring of square matrices over a division ring.*

Proof. From proposition 2.2.3 it follows that if $A \simeq M_n(D)$, where D is a division ring, then it is simple.

Conversely, let a ring A be right Artinian and simple. Since the radical of the ring A is a two-sided ideal and A is simple, $radA = 0$, i.e., A is semiprimitive. By theorem 3.5.5 it is semisimple. Therefore, by the Wedderburn-Artin theorem, A is isomorphic to a direct sum of a finite number of full matrix rings over division rings. Obviously, each direct summand is a two-sided ideal. Therefore $A \simeq M_n(D)$, where D is a division ring.

Note that because the radical of a right Artinian ring is nilpotent, we have a lemma similar to Nakayama's lemma for any module over such a ring. Namely, the following statement is true, which we shall call Nakayama's lemma for Artinian rings.

Lemma 3.5.8 (Nakayama's lemma for Artinian rings). *Let A be a right Artinian ring, M be a right A-module and $N + MR = M$. Then $N = M$.*

3.6 A CRITERION FOR A RING TO BE ARTINIAN OR NOETHERIAN

In this section we give a useful criterion which helps us to decide whether a ring is Artinian (or Noetherian).

Theorem 3.6.1. *Let A be an arbitrary ring with an idempotent $e^2 = e \in A$. Set $f = 1 - e$, $eAf = X$, $fAe = Y$, and let*

$$A = \begin{pmatrix} eAe & X \\ Y & fAf \end{pmatrix}$$

be the corresponding two-sided Peirce decomposition of the ring A. Then the ring A is right Noetherian (Artinian) if and only if the rings eAe and fAf are right Noetherian (Artinian), X is a finitely generated fAf-module and Y is a finitely generated eAe-module.

Proof. Let A be a right Noetherian ring and $\mathcal{I}$ be a right ideal in eAe. Set $\overline{\mathcal{I}} = (\mathcal{I}, \mathcal{I}X)$. Obviously, $\overline{\mathcal{I}}$ is a right ideal in the ring A. Consider an ascending chain $\mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq ...$ of right ideals in the ring eAe and the associated chain $\overline{\mathcal{I}_1} \subseteq \overline{\mathcal{I}_2} \subseteq ...$ of ideals in A. Since the ring A is right Noetherian, this chain stabilizes, i.e., $\overline{\mathcal{I}}_n = \overline{\mathcal{I}}_{n+1} = ...$, and thus $\mathcal{I}_n = \mathcal{I}_{n+1} = ...$ Therefore, the ring eAe is right Noetherian.

Let $L \subseteq X$ be a fAf-submodule of the module X. Clearly, $\overline{L} = (LY, L)$ is a right ideal in the ring A. Suppose that fAf-module X is not finitely generated. Then one can construct a strictly ascending chain of submodules in $X : L_1 \subseteq L_2 \subseteq ...$, which implies the existence of a strictly ascending chain of right ideals $\overline{L_1} \subseteq \overline{L_2} \subseteq ...$ in the ring A. But this contradicts the fact that A is right Noetherian.

Analogously, one can prove that fAf is a right Noetherian ring and Y is a finitely generated right eAe-module.

Conversely, suppose now that the rings eAe and fAf are right Noetherian and the modules X and Y are finitely generated. Let $\overline{\mathcal{I}}$ be a right ideal of the ring A lying in eA. Consider the Peirce decomposition of the right ideal $\overline{\mathcal{I}} = \overline{\mathcal{I}}e \oplus \overline{\mathcal{I}}f$. Obviously, $\overline{\mathcal{I}}e = \mathcal{I}$ is a right ideal in the ring eAe while $\overline{\mathcal{I}}f = L$ is an fAf-submodule in X.

Consider an ascending chain of right ideals in the ring A lying in eA: $\overline{\mathcal{I}_1} \subseteq \overline{\mathcal{I}_2} \subseteq ....$ Using this chain we can construct two ascending chains $\mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq ...$ and $L_1 \subseteq L_2 \subseteq ....$ They must stabilize, which implies that the right ideal eA is Noetherian.

Similarly, one can prove that the ideal fA is Noetherian. Therefore, A is a right Noetherian ring as a direct sum of Noetherian modules.

Since a right Artinian ring is also right Noetherian, by proposition 3.1.10, any finitely generated module over this ring is both Artinian and Noetherian. Using this fact one can prove analogously the theorem in the Artinian case. The theorem is proved.

Corollary 3.6.2. *Let $K \subset L$ be fields such that $dim_K L = \infty$. Then the ring*

$$A = \begin{pmatrix} K & L \\ 0 & L \end{pmatrix}$$

is right Noetherian and right Artinian, but neither left Noetherian nor left Artinian.

Example 3.6.1

Let $\mathbf{Z}$ be the ring of all integers and $\mathbf{Q}$ be the field of all real numbers. Consider the following ring

$$H(\mathbf{Z}, 1, 1) = \begin{pmatrix} \mathbf{Z} & \mathbf{Q} \\ 0 & \mathbf{Q} \end{pmatrix}.$$

Since $\mathbf{Z}$ and $\mathbf{Q}$ are Noetherian rings and $\mathbf{Q}$ is a finitely generated $\mathbf{Q}$-module, $H(\mathbf{Z}, 1, 1)$ is a right Noetherian ring.

However, $H(\mathbf{Z}, 1, 1)$ is not a left Noetherian ring because $\mathbf{Q}$ is an infinitely generated $\mathbf{Z}$-module. Since $\mathbf{Z}$ is not an Artinian ring, the ring $H(\mathbf{Z}, 1, 1)$ is neither right nor left Artinian.

Example 3.6.2
Consider the following ring:

$$H(\mathbf{Q},1,1)=\begin{pmatrix}\mathbf{Q} & \mathbf{R}\\ 0 & \mathbf{R}\end{pmatrix}.$$

This ring, by corollary 3.6.2, is right Artinian (and therefore right Noetherian) but not left Artinian.

3.7 SEMIPRIMARY RINGS

In this section we consider an important class of rings.

Definition. A ring A with radical R is called **semiprimary** if A/R is semisimple and R is nilpotent.

Semiprimary rings form a class of rings that contains both left and right Artinian rings. However, there are semiprimary rings which are neither left Artinian nor right Artinian. Consider the ring of 2×2 upper triangular real matrices with all diagonal entries rational:

$$A=\begin{pmatrix}\mathbf{Q} & \mathbf{R}\\ 0 & \mathbf{Q}\end{pmatrix}.$$

The radical of this ring

$$radA=\begin{pmatrix}0 & \mathbf{R}\\ 0 & 0\end{pmatrix}$$

and so $(radA)^2=0$ and A/R is semisimple. Thus, A is a semiprimary ring. However, since $\mathbf{R}$ is an infinite dimensional vector space over the field $\mathbf{Q}$, by theorem 3.6.1, this ring is neither left nor right Artinian.

Theorem 3.7.1 (Hopkins-Levitzki). *Let A be a semiprimary ring. Then for any right A-module M the following statements are equivalent:*
(1) *M is Artinian.*
(2) *M is Noetherian.*
(3) *M has a composition series.*

Proof.
(3) $\Rightarrow$ (1) and (3) $\Rightarrow$ (2) follows from proposition 3.2.2.
(1) $\Rightarrow$ (3). Let A be a semiprimary ring with nilpotent radical R so that $R^n=0$ and $\overline{A}=A/R$. Suppose M is a right Artinian module and consider a chain of submodules:

$$M\supseteq MR\supseteq MR^2\supseteq ...\supseteq MR^n=0.$$

To complete the proof it suffices to show that any factor $M_k = MR^k/MR^{k+1}$ has a composition series. But M_k is a module over $\overline{A}$. Since $\overline{A}$ is a semisimple ring, by theorem 2.2.5, M_k is a semisimple module and therefore it is a direct sum of simple $\overline{A}$-modules. Since M_k is an Artinian module, this sum is finite, so M_k has a composition series as $\overline{A}$-module.

(1) $\Rightarrow$ (2) is proved analogously.

Corollary 3.7.2 (Hopkins-Levitzki). *A ring A is right Artinian if and only if A is right Noetherian and semiprimary.*

Proof. By proposition 3.5.1 and theorem 3.5.6, a right Artinian ring is right Noetherian and semiprimary.

Due to the equivalence (1) $\Longleftrightarrow$ (2) from the previous theorem applied to the right regular module A_A, it follows that a right Noetherian and semiprimary ring is right Artinian.

Proposition 3.7.3. *If $e^2 = e$ is an idempotent of a semiprimary ring A, then eAe is semiprimary as well.*

Proof. Denote by $\mathcal{J}$ the Jacobson radical of the ring eAe. Then, by proposition 3.4.8, $\mathcal{J} = eRe$, where R is the Jacobson radical of the ring A. Since R is nilpotent, $\mathcal{J}$ is also nilpotent. Since the ring A/R is Artinian, by theorem 3.6.1, $eAe/\mathcal{J}$ is also Artinian. Then by theorem 3.5.5 the ring $eAe/\mathcal{J}$ is semisimple, and so eAe is a semiprimary ring.

3.8 NOTES AND REFERENCES

The ascending chain condition was introduced by R.Dedekind in connection with his study of ideals in algebraic number fields. J.H.M.Wedderburn in his paper on the structure of algebras uses "descending chain condition" arguments without employing that term. It was W.Krull and E.Noether who began to use these notions systematically in their investigations. W.Krull used them for the study of Abelian groups with operators and E.Noether used them for the characterization of Dedekind rings.

In 1921 E.Noether extended the Dedekind theory of ideals and the representation theory of integral domains (and rings of algebraic numbers) to the case of arbitrary commutative rings satisfying a.c.c. These rings are called now Noetherian rings.

In two great papers *Idealtheorie in Ringenbereichen // Math. Ann, v.83 (1921), p.24-66* and *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern // Math. Ann., v.96 (1927), p.26-61* on ideal theory Emmy Noether founded the abstract study of rings with chain conditions. In the first paper she gave an abstract treatment of the decomposition theories of D.Hilbert, E.Lasker and F.S.Macaulay for polynomial rings, and in the second one an ax-

iomatic treatment of theories of R.Dedekind and L.Kronecker for algebraic numbers and function fields. (E.Lasker (1868-1941) was a famous German mathematician and chess master. In particular, he introduced the notion of a primary ideal and developed the theory of primary decomposition. He was the chess world champion for 27 years. In 1921 E.Lasker lost the world championship match to the Cuban chess master X.P.Capablanca.)

J.Levitzki in the paper: *On rings which satisfy the minimum condition for right-hand ideals // Compositto Math., v.7 (1939), p.214-222* and C.Hopkins in the paper: *Rings with minimal condition for left ideals // Ann. of Math., v.40 (1939), p.712-730* proved independently that a ring satisfying d.c.c. on left ideals also satisfies a.c.c. on them. They proved that the radical of an Artinian ring is nilpotent and so it was proved that the Wedderburn-Artin theorem is true for rings with only d.c.c.

Artinian modules and Artinian rings were first systematically studied in the book: *E.Artin, C.Nesbitt, R.Thrall, Rings with Minimum condition, Michigan, 1944.*

Fitting's lemma was proved by H.Fitting in his paper: *Die Theorie der Automorphismenringe Abelscher Gruppen und ihr Analogon bei nicht kommutativen Gruppen // Math. Ann., v.107 (1933), p.514-542.*

The Jordan-Hölder theorem was first proved for composition series of a finite group. C.Jordan proved that for any two composition series of a finite group G, the list of the orders of the composition factors in one series is a permutation of the corresponding list for the other series (see *C.Jordan, Théorèmes sur les équations algébriques // J. Math. Pures Appl. (2) 14 (1869), p.139-146.* and *C.Jordan, Commentaires sur Galois // Math. Annalen, v.1 (1869), p.141-160*). The fact that any two composition series for G are isomorphic was proved by O.Hölder in his paper *Zurückführung einer beliebigen algebraischen Gleichung auf eine Kette von Gleichungen // Math. Ann., v.34 (1889), p.26-56.*

The Krull-Schmidt theorem (one also finds the name Krull-Remak-Schmidt theorem) was first proved for finite Abelian groups by R.Remak in his paper *Über die Zerlegung der endlichen Gruppen in direkte unzerlegbare Faktoren // J. Reine Angew. Math., v.139 (1911), p.293-308* and by W.Krull in the paper *Über verallgemeinerte endliche Abelsche Gruppen // Math. Z., 23, 1925, pp.161-196* and for infinite Abelian groups with finiteness conditions by O.Yu.Schmidt in the paper *Über unendliche Gruppen mit endlicher Kette // Math. Z., 29, 1928, 34-41.* This result for rings has been proved by W.Krull in the paper *Algebraische Theorie der Ringe II // Math. Ann., 91 (1924), p.1-46.*

The Hilbert basis theorem for commutative rings was proved by D.Hilbert in his paper *Über die Theorie der algebraischen Formen // Math. Ann., 1890, Bd. 36, S.473-534.*

Historically, the notion of a radical was directly connected with the notion of semisimplicity. It is interesting to remark that the radical was studied first in the context of nonassociative rings. Namely, the notion of a radical appeared

during the investigation of finite dimensional Lie algebras, first in a particular case in a paper of G.Scheffers: *Zurückführung complexer Zahlensysteme auf typische Formen // Math. Ann. XXXIX (1891), p.293-390* and then in the papers of T.Molien: *Über Systeme höherer complexer Zahlen // Math. Ann. XLI (1893), p.83-156* and E.Cartan : *Les groupes bilinéaires et systémes de nombres complexes // Ann. Fac. Sc. Toulouse, 1898.* The term "radical" is due to G.Frobenius.

Studying finite dimensional algebras over a field J.H.M.Wedderburn defined for every such algebra A an ideal, $radA$, which is the largest nilpotent ideal in A, i.e., the sum of all the nilpotent ideals in A. In parallel with Cartan's theory of finite dimensional Lie algebras, he called a finite dimensional associative algebra A semisimple if and only if its radical is zero. E.Artin extended Wedderburn's theory of semisimple algebras to rings with minimum condition. For such a ring A the sum of all its nilpotent ideals is nilpotent, so A has a largest nilpotent ideal $radA$, called the Wedderburn radical of A.

For a ring A, which does not satisfy Artin's descending chain condition, the sum of all nilpotent ideals need no longer be nilpotent; thus, A may not possess a largest nilpotent ideal, and so we no longer have the notion of a Wedderburn radical. The problem of finding an appropriate generalization of Wedderburn's radical for an arbitrary ring was solved by N.Jacobson in his fundamental paper *The radical and semisimplicity for arbitrary rings //Amer. J. Math., 1945, v.67, pp.300-320*, where he introduced the general notion of a radical for an arbitrary ring. In the introduction of this paper he wrote: "The radical of an algebra with a finite basis, or, more generally, of a ring A that satisfies the descending chain condition is defined to be the join of the nil right (left) ideals of A. The importance of the radical for the structure theory of these rings is due to the facts that 1) the radical R is two-sided ideal whose difference ring $A - R$ is semisimple in the sense that its radical is 0, and 2) the structure of semisimple rings satisfying the descending chain condition can be subjected to a thorough analysis that leads in many important cases to a complete classification. Several investigations of nil ideals in arbitrary rings have been made recently but none of these has led to a structure theory for general semisimple rings (see *R.Baer, Radical ideals // American Journal of mathematics, vol. LXV (1943), pp.537-568*). This is one of a number of indications that in order to develop a satisfactory structure theory for arbitrary rings it is necessary to abandon the concept of a nil ideal in defining the radical.

Other possibilities for defining a radical are afforded by two important characterizations of the radical R of an algebra A with a finite basis. One of these, due to Perlis, makes use of the notion of quasi-regularity (see *S.Perlis, A characterization of the radical of an algebra // Bulletin of the American Mathematical Society, vol. 48 (1942), pp.128-132*). An element z of A is right quasi-regular if there exists a z' in A such that $z + z' + zz' = 0$. Perlis has shown that $z \in R$ if and only if $u + z$ is right quasi-regular for all right quasi-regular u. A second characterization of R for algebras with an identity is that R is the intersection of the maximal right (left)

ideals of A (see *N.Jacobson, The theory of Rings // Mathematical Surveys, vol. 2 (New York, 1943)*, cf. also *G.Birkhoff, The radical of a group with operators, Bulletin of the American Mathematical Society, vol. 49 (1943), pp.751-753*). A start in the investigation of the first characterization as a possibility for defining a radical for an arbitrary ring A was made by Baer, who showed that the totality R of elements z that generated right ideals containing only right quasi-regular elements is a right ideal (see *R.Baer, Radical ideals, p.562*). This definition of the radical has been independently proposed by Hille and Zorn who proved that R is two-sided ideal and that if A has an identity, R is the intersection of the maximal right (left) ideals of A. These results were announced by Hille in his Colloquium Lectures in August 1944)".

For a ring satisfying a one-sided minimum condition, the Jacobson radical coincides with the classical Wedderburn radical, so, in general, the former provides a good substitute for the latter.

Earlier, in 1941, studying the special class of normed rings I.M.Gel'fand introduced the notion of the radical of such rings in the form of the intersection of all maximal ideals (see *I.M.Gel'fand, Normierte Ringe// Mat. sb., new series, 1941, v.9, p.3-23* and *I.M.Gel'fand, Ideale und primare ideale in normierten Ringen // Mat. sb., new series, 1941, v.9, p.41-48*).

Also, there are several other radicals which can be defined for arbitrary rings, and which provide alternate generalizations of the Wedderburn radical. These other radicals may not be as fundamental as the Jacobson radical, but in one way or another, they reflect more accurately the structure of the nil (and nilpotent) ideals of the ring, so one might say that these other radicals resemble the Wedderburn radical more than does the Jacobson radical. The general theory of radicals was systematically studied in the books *V.A.Andrunakievich, Yu.M.Ryabukhin, Radicals of Algebras and Structural theory, Nauka, Moscow, 1979*; *N.J.Divinsky, Rings and Radicals, Univ. of Toronto Press, Toronto, 1965*. It should be noted that there are also papers of other mathematicians studying properties of radicals in different types of rings (see, for example, *N.J.Divinsky, J.Krempa, A.Sulinsky, Strong radical properties of alternative and associative rings // J.Algebra, v.17, 1971, p.369-388*; *E.Jespers, J.Krempa, E.R.Puczylowski, On radicals of graded rings // Comm. Algebra, v.10, 1982, N17, pp.1849-1854*).

The idea of Nakayama's lemma originated from the work of more than one mathematician. In the commutative case and when M itself is an ideal of R, (1) $\Rightarrow$ (2) was discovered and used effectively by W.Krull. N.Jacobson proved this lemma in the case when M is a right ideal contained in the radical (see *N.Jacobson, The radical and semi-simplicity for arbitrary rings // Amer. J. Math. v.67 (1945), p.300-320*). G.Azumaya carried over Jacobson's proof to the module case (see *G.Azumaya, On maximally central algebras, Nagoya Math. J. v.2 (1951), p.119-150*). An alternative proof derived from a generalized result was presented by T.Nakayama (see *T.Nakayama, A remark on finitely generated modules // Nagoya Math. J., v.3 (1951), p.139-140*).

A criterion for a ring to be Noetherian or Artinian first was proved in the papers *V.V.Kirichenko, Generalized uniserial rings // Mat. sb. v.99(141), N4 (1976), p.559-581* and *V.V.Kirichenko, Rings and Modules, Kiev, 1981.*

Semiprimary rings naturally arise as endomorphism rings of modules of finite length. The structure and properties of semiprimary rings was considered by G.Hopkins, *Rings with minimal condition for left ideals // Ann. of Math., v.40 (1939), p.712-730)*; J. Levitzki, *A characteristic condition for semiprimary rings", Duke Math. J., 1944, v.11, p.267-368*, and *On rings which satisfy the minimum condition for right-hand ideals // Compositto Math., v.7 (1939), p.214-222*; K.Asano, *Über Hauptidealringe mit Kettensatz // Osaka Math. J., v.1(1949), p.52-61*; *Über die Quotientenbildung von Schiefringen // J. Math. Japan, v.1(1949), p.73-79*; S.U.Chase *Direct product of modules // Trans. Amer. Math. Soc., v.97 (1960), p.457-473* and others.

4. Categories and functors

4.1 CATEGORIES, DIAGRAMS AND FUNCTORS

In this section we introduce some of the basic language of category theory involving the notions of category and functor, which include the concept of a class. This concept is intended to generalize the concept of a set and we use the Gödel-Bernay axioms of the set theory, whose objects are classes. We assume the reader is more or less familiar with notions of a set and a class. For our purposes all we need to know is that the class concept is like the set concept, only some what broader. Besides in set theory it is not possible to carry out the operations over classes which can lead to problems such as Russell's paradox. All sets are classes and all the elementary set operations, like union, intersection, formation of function, etc., can be carried out for classes as well.

Definition. We shall say that we have a **category** C if there are defined:

1) a class ObC, whose elements are called the **objects** of the category C;

2) a set $MorC$, whose elements are called the **morphisms** of the category C;

3) for any morphism $f \in MorC$ there is an ordered pair of objects (X, Y) of the category C (we shall say that f is a morphism from an object X to an object Y and write $f : X \to Y$). The set of all morphisms from X to Y will be denoted by $Hom_C(X, Y)$, or shortly $Hom(X, Y)$;

4) for any ordered triple $X, Y, Z \in ObC$ and any pair of morphisms $f : X \to Y$ and $g : Y \to Z$ there is a uniquely defined morphism $gf : X \to Z$, which is called the **composition** or **product** of morphisms f and g.

These objects, morphisms and compositions are required to satisfy the following conditions:

5) composition of morphisms is associative, i.e., for any triple of morphisms f, g, h one has $h(gf) = (hg)f$ whenever these products are defined;

6) if $X \neq X'$ or $Y \neq Y'$, then $Hom(X, Y)$ and $Hom(X', Y')$ are disjoint sets;

7) for any object $X \in ObC$ there exists a morphism $1_X \in Hom(X, X)$ such that $f \cdot 1_X = f$ and $1_X \cdot g = g$ for any morphisms $f : X \to Y$ and $g : Z \to X$.

It is easy to see that a morphism 1_X with the above properties is unique. It is called the **identity morphism** of the object X.

If in a category C the class ObC is actually a set, then that category is called **small**.

Example 4.1.1.

Sets - category of sets. Ob**Sets** is the class of all sets. $Hom(A, B)$ is the set of all maps from A to B.

Example 4.1.2.
Gr - category of groups. $Ob\mathbf{Gr}$ is the class of all groups. $Hom(A, B)$ is the set of all group homomorphisms from A to B.

Example 4.1.3.
Ab - category of Abelian groups. $Ob\mathbf{Ab}$ is the class of all Abelian groups. $Hom(A, B)$ is a set of all Abelian group homomorphisms from A to B.

Example 4.1.4.
Ring - category of rings. $Ob\mathbf{Ring}$ is the class of all nonzero rings with 1. $Hom(A, B)$ is a set of all (1-preserving) ring homomorphisms from A to B.

Example 4.1.5.
The main example of a category, which we shall consider in this book, is the category C of right (resp. left) modules over a ring A. ObC is the class of all right (resp. left) A-modules. $Hom(X, Y)$ is a set of all module homomorphisms from X to Y. The category of right (resp. left) A-modules is often denoted by mod-A (resp. A-mod) or $\mathbf{M}_A$ (resp. ${}_A\mathbf{M}$). If the ring A is commutative we make no distinction between $\mathbf{M}_A$ and ${}_A\mathbf{M}$.

Example 4.1.6.
Given a category C, form the opposite category C^{op}: $ObC^{op} = ObC$, while $Hom_{C^{op}}(X, Y) = Hom_C(Y, X)$. Composition of morphisms in C^{op} is defined reversed, i.e., if $*$ denotes composition in C^{op} then $f * g = g \cdot f$.

We shall often use diagrams to illustrate the compositions of morphisms. Let C be a category and $X, Y \in ObC$. Any morphism $\varphi \in Hom(X, Y)$ can be illustrated by an arrow:

$$X \xrightarrow{\varphi} Y$$

Let $M_i, N_i \in ObC$ and $\varphi_i \in Hom(M_i, N_i)$ $(i = 1, 2)$, $\alpha \in Hom(M_1, M_2)$, $\beta \in Hom(N_1, N_2)$. Consider a **diagram** of morphisms of the form

$$\begin{array}{ccc} M_1 & \xrightarrow{\alpha} & M_2 \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} \\ N_1 & \xrightarrow{\beta} & N_2 \end{array} \tag{4.1.1}$$

If $\varphi_2\alpha = \beta\varphi_1$, then diagram (4.1.1) is said to be **commutative**.

Analogously, a triangular diagram of morphisms

$$\begin{array}{ccc} M_1 & \xrightarrow{\alpha} & M_2 \\ & {\scriptstyle \varphi_1}\searrow \quad \swarrow{\scriptstyle \varphi_2} & \\ & N & \end{array} \tag{4.1.2}$$

is called **commutative** if $\varphi_2\alpha = \varphi_1$.

In general, a diagram is called **commutative** if all its square and triangular and other subdiagrams are commutative. In other words, if in this diagram all compositions of morphisms taken along each path that start from the same point and finish at the same point are equal.

Note that a diagram is not a mathematical object but only a picture which helps reading complicated expressions.

One of the most important concepts in category theory is the notion of a functor.

Definition. A **covariant functor** F from a category C to a category D is a pair of maps $F_{ob} : ObC \to ObD$ and $F_{mor} : MorC \to MorD$ satisfying the following conditions:

1) if $X, Y \in ObC$, then to each morphism $f : X \to Y$ in $MorC$ there corresponds a morphism $F_{mor}(f) : F_{ob}(X) \to F_{ob}(Y)$ in $MorD$;

2) $F_{mor}(1_X) = 1_{F_{ob}(X)}$ for all $X \in ObC$;

3) if the product of morphisms gf is defined in C, then

$$F_{mor}(gf) = F_{mor}(g)F_{mor}(f).$$

Usually, instead of $F_{mor}(f)$ and $F_{ob}(X)$ one simply writes $F(f)$ and $F(X)$.

A **contravariant functor** from a category C to a category D is literally a covariant functor from C to D^{op}. That is, we have the following definition.

A **contravariant functor** F from a category C to a category D is a pair of maps $F_{ob} : ObC \to ObD$ and $F_{mor} : MorC \to MorD$ satisfying the following conditions:

1) if $X, Y \in ObC$, then to each morphism $f : X \to Y$ in $MorC$ there corresponds a morphism $F_{mor}(f) : F_{ob}(Y) \to F_{ob}(X)$ in $MorD$;

2) $F_{mor}(1_X) = 1_{F_{ob}(X)}$ for all $X \in ObC$;

3) if the product of morphisms gf is defined in C, then

$$F_{mor}(gf) = F_{mor}(f)F_{mor}(g).$$

A **functor** is defined as either a covariant functor or a contravariant functor.

A functor F is called **additive** if for any pair of morphisms $f_1 : X \to Y$ and $f_2 : X \to Y$ we have $F(f_1 + f_2) = F(f_1) + F(f_2)$. [1])

Besides functors in one variable, one may also consider functors in many variables. Such a functor may be covariant in some of its variables and covariant in others. A functor in two variables is often called a **bifunctor**.

[1]) Here it is assumed that here is a sensible way to add morphisms in the categories C and D, as is e.g. the case for categories of modules. (But not e.g. for the categories of sets or noncommutative groups.)

Definition. Let F and G be two functors from a category C to a category D. A **morphism** (or a **natural transformation**) from the functor F to the functor G is a map φ which assigns to each object $X \in ObC$ a morphism $\varphi(X) : F(X) \to G(X)$ of the category D with the following property: for any pair of objects $X, Y \in ObC$ and any any morphism $f : X \to Y$ of the category C we have $G(f)\varphi(X) = \varphi(Y)F(f)$, i.e., the following diagram commutes:

$$\begin{array}{ccc} F(X) & \xrightarrow{\varphi(X)} & G(X) \\ \Big\downarrow{\scriptstyle F(f)} & & \Big\downarrow{\scriptstyle G(f)} \\ F(Y) & \xrightarrow{\varphi(Y)} & G(Y) \end{array}$$

A morphism of functors will be simply denoted by $\varphi : F \to G$. If for every $X \in ObC$ the morphism $\varphi(X)$ is an isomorphism, then φ is an **natural isomorphism of functors** which is written $\varphi : F \simeq G$.

Suppose we have another functor $H : C \to D$ and a morphism of functors $\psi : G \to H$. In this situation one can define the composition $\psi\varphi : F \to H$ by setting $(\psi\varphi)(X) = \psi(X)\varphi(X)$. It is not difficult to verify that with this definition the set of functors from the category C to the category D with the set of their morphisms forms a category, which is called the **functor category** $Func(C, D)$.

4.2 EXACT SEQUENCES. DIRECT SUMS AND DIRECT PRODUCTS

Consider the category of right A-modules over a fixed given ring A. A sequence of A-modules and homomorphisms

$$... \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow ... \tag{4.2.1}$$

is said to be **exact at** M_i if $Imf_i = Kerf_{i+1}$. If the sequence (4.2.1.) is exact at every M_i, then it is called **exact**.

In particular, a sequence

$$0 \longrightarrow N \xrightarrow{f} M$$

is exact if and only if $Kerf = 0$, i.e., f is injective. Analogously, a sequence

$$N \xrightarrow{f} M \longrightarrow 0$$

is exact if and only if $Imf = M$, i.e., f is surjective.

An exact sequence of the form

$$0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} L \longrightarrow 0 \tag{4.2.2}$$

is called a **short exact sequence**. Since this sequence is exact at N, f is injective and we can consider Imf as a submodule of M and identify it with N. Similarly,

since the sequence is exact at L, we conclude that g is surjective and L can be identified with the factor module $M/Kerg$. Since the sequence is exact at M, we have $Imf = Kerg$. Thus, the exact sequence (4.2.2) may be expressed in the equivalent form

$$0 \longrightarrow Imf \xrightarrow{f} M \xrightarrow{g} M/Imf \longrightarrow 0 \tag{4.2.3}$$

where f is the canonical embedding and g is the natural projection.

A short exact sequence (4.2.2) is said to be **split** if there exist homomorphisms $\overline{f} : M \to N$ and $\overline{g} : L \to M$ such that $\overline{f}f = 1_N$ and $g\overline{g} = 1_L$.[2])

Let $X \oplus Y$ be the external direct sum of modules X and Y. Then there exist the following canonical embeddings

$i_X : X \to X \oplus Y$ given by $x \mapsto (x, 0)$

$i_Y : Y \to X \oplus Y$ given by $y \mapsto (0, y)$

and canonical projections

$\pi_X : X \oplus Y \to X$ given by $(x, y) \mapsto x$

$\pi_Y : X \oplus Y \to Y$ given by $(x, y) \mapsto y$.

Clearly, $\pi_X i_X(x) = \pi(x, 0) = x$, i.e., $\pi_X i_X = 1_X$ is the identity map on X, and analogously, $\pi_Y i_Y = 1_Y$ is the identity on Y. Furthermore, $i_X \pi_X(x, y) = i_X(x) = (x, 0)$ and $i_Y \pi_Y(x, y) = i_Y(y) = (0, y)$. Therefore $i_X \pi_X + i_Y \pi_Y = 1_{X \oplus Y}$ is the identity map on $X \oplus Y$.

Consider an exact sequence of the form:

$$0 \longrightarrow X \xrightarrow{i_X} X \oplus Y \xrightarrow{\pi_Y} Y \longrightarrow 0 \tag{4.2.4}$$

where i_X and π_Y are the canonical maps defined above. Then there is the following commutative diagram

$$0 \rightleftarrows X \underset{\pi_X}{\overset{i_X}{\rightleftarrows}} X \oplus Y \underset{i_Y}{\overset{\pi_Y}{\rightleftarrows}} Y \rightleftarrows 0, \tag{4.2.5}$$

i.e., $\pi_X i_X = 1_X$ and $\pi_Y i_Y = 1_Y$. Thus, the sequence (4.2.4) is split.

We are going to prove the inverse statement. Suppose

$$0 \longrightarrow X \xrightarrow{f} M \xrightarrow{g} Y \longrightarrow 0 \tag{4.2.6}$$

is an exact sequence and there exists a homomorphism $\overline{g} : Y \to M$ such that $g\overline{g} = 1_Y$. We construct a homomorphism $\varphi : X \oplus Y \to M$ by setting $\varphi(x, y) = f(x) + \overline{g}(y)$ and show that it is an isomorphism. Let $\varphi(x, y) = 0$. Since $X \oplus Y$ is a direct sum, we can write down the canonical maps i_X, i_Y, π_X and π_Y defined above. Because $i_X \pi_X = 1_X$ and $i_Y \pi_Y = 1_Y$, we have $0 = \varphi(x, y) = f\pi_X(x, y) = f(x)$. Since f is a monomorphism, this implies $x = 0$. On the other hand, $0 = \varphi(x, y) = \overline{g}\pi_Y(x, y) = \overline{g}(y)$. Since $g\overline{g} = 1_Y$, from the last equality it follows that $0 = g\overline{g}(y) = y$. Therefore φ is a monomorphism.

[2]) In fact if either $\overline{f}$ or $\overline{g}$ exists (such that $\overline{f}f = 1_N$, resp. $g\overline{g} = 1_M$), so does the other. See below.

Let m be any element in M. Consider the element $m_1 = m - \overline{g}g(m) \in M$. Since $g\overline{g} = 1_Y$, we have $g(m_1) = g(m - \overline{g}g(m)) = g(m) - g\overline{g}g(m) = g(m) - g(m) = 0$, i.e., $m_1 \in Kerg$. Since $Kerg = Imf$ there exists $x \in X$ such that $m_1 = f(x)$. If we write $y = g(m) \in Y$, then we obtain $m = f(x) + \overline{g}(y)$. Therefore, φ is an epimorphism and, consequently, is an isomorphism.

Suppose that we have an exact sequence (4.2.6) and a homomorphism $\overline{f} : M \to X$ such that $\overline{f}f = 1_X$. Then we can define a homomorphism $\psi : M \to X \oplus Y$ as follows $\psi(m) = (\overline{f}(m), g(m))$. Assume $\psi(m) = 0$, then $\overline{f}(m) = 0$ and $g(m) = 0$, i.e., $m \in Kerg$. Since $Kerg = Imf$, there exists $x \in X$ such that $m = f(x)$. Taking into account that $\overline{f}f = 1_X$ we have $0 = \overline{f}(m) = \overline{f}f(x) = x$. Hence, $x = 0$ and $m = f(x) = 0$. Therefore ψ is a monomorphism.

Let's now show that ψ is an epimorphism. Consider an element $(x, y) \in X \oplus Y$. Since g is an epimorphism, there exists an element $m_1 \in M$ such that $g(m_1) = y$. Denote it by $m_1 = g^{-1}(y)$ and consider the element $m = f(x - \overline{f}g^{-1}(y)) + g^{-1}(y)$. Since $\overline{f}f = 1_X$, we have $\overline{f}(m) = \overline{f}f(x - \overline{f}g^{-1}(y)) + \overline{f}g^{-1}(y) = x - \overline{f}g^{-1}(y) + \overline{f}g^{-1}(y) = x$. Taking into account that $gf = 0$ we have $g(m) = gf(x - \overline{f}g^{-1}(y)) + gg^{-1}(y) = y$. Therefore any element $(x, y) \in X \oplus Y$ can be written in the form $(x, y) = (\overline{f}(m), g(m))$, where m is defined as above. Therefore ψ is an epimorphism and, consequently, an isomorphism.

Thus, we have proved the following proposition.

Proposition 4.2.1. *The following statements for an exact sequence*

$$0 \longrightarrow X \xrightarrow{f} M \xrightarrow{g} Y \longrightarrow 0$$

are equivalent:

1) *the sequence is split*;
2) *there exists a homomorphism* $\overline{g} : Y \to M$ *such that* $g\overline{g} = 1_Y$;
3) *there exists a homomorphism* $\overline{f} : M \to X$ *such that* $\overline{f}f = 1_X$;
4) $M \simeq X \oplus Y$.

In section 1.5 the notions of direct sum and direct product of modules were introduced. External direct sums and direct products of modules can be also described in terms of set of homomorphisms as has been done above for two modules. In general, a direct sum (resp. direct product) of modules X_i $(i \in I)$ defines for each $i \in I$ a canonical injection σ_i and a canonical projection π_i

$$X_i \xrightarrow{\sigma_i} \bigoplus_{i \in I} X_i \xrightarrow{\pi_i} X_i$$

(resp. $X_i \xrightarrow{\sigma_i} \prod_{i \in I} X_i \xrightarrow{\pi_i} X_i$), where $\sigma_i x_i = (..., 0, x_i, 0, ...)$, $\pi_i(..., x_j, ..., x_i, ...) = x_i$, satisfying the following conditions:

1) $\pi_i\sigma_i = 1_{X_i}$ and $\pi_i\sigma_j = 0$ for $i \neq j$;

2) if the set I is finite, i.e., $I = \{1, 2, ..., n\}$, and $X = X_1 \oplus ... \oplus X_n$, then $\sigma_1\pi_1 + ... + \sigma_n\pi_n = 1_X$;

if the set I is infinite, then instead of 2) for a direct sum we have:

$2'$) each element $x \in X$ can be written in the form of a finite sum $x = \sigma_{i_1}\pi_{i_1}x + ... + \sigma_{i_n}\pi_{i_n}x$;

and for a direct product we have:

$2''$) if we have a set of elements $\{x_i\}$, with only one element $x_i \in X_i$ for each $i \in I$, then there exists a unique element $x \in \prod\limits_{i\in I} X_i$ such that $\pi_i x = x_i$ for each $i \in I$.

The following statements are very useful and they are known as the universal properties of direct sums and direct products.

Proposition 4.2.2. *Let $\varphi_i : X_i \to Y$ be a set of homomorphisms of A-modules, $i \in I$. Then there exists a unique homomorphism ψ such that the diagrams*

$$\begin{array}{ccc} X_i & \xrightarrow{\sigma_i} & \bigoplus\limits_{i\in I} X_i \\ & \searrow^{\varphi_i} & \downarrow{\scriptstyle \psi} \\ & & Y \end{array} \tag{4.2.7}$$

are commutative for each $i \in I$.

Proof. Let $x \in \bigoplus\limits_{i\in I} X_i$. It can be written in the form $x = \sigma_1\pi_1 x + ... + \sigma_n\pi_n x$, where the π_k are the canonical projections. Let $\psi x = \varphi_1\pi_1 x + ... + \varphi_n\pi_n x$. It is easy to see that ψ is a A-homomorphism and $\psi\sigma_i x_i = \varphi_i\pi_i\sigma_i x_i = \varphi_i x_i$. If ψ' is another homomorphism from $\bigoplus\limits_{i\in I} X_i$ to Y, which makes the diagrams (4.2.7) commutative, then $(\psi - \psi')(\sigma_i x_i) = 0$ for all $i \in I$ and so $(\psi - \psi')x = 0$ for all $x \in \bigoplus\limits_{i\in I} X_i$. Thus $\psi = \psi'$.

Proposition 4.2.3. *Let $\varphi_i : Y \to X_i$ be a set of homomorphisms of A-modules, $i \in I$. Then there exists a unique homomorphism ψ such that the diagrams*

$$\begin{array}{ccc} Y & & \\ \downarrow{\scriptstyle \psi} & \searrow^{\varphi_i} & \\ \prod\limits_{i\in I} X_i & \xrightarrow{\pi_i} & X_i \end{array} \tag{4.2.8}$$

are commutative for each $i \in I$.

Proof. Let $y \in Y$ and $\varphi_i y = x_i \in X_i$. By the properties of the direct product, there exists a unique element $x \in \prod\limits_{i\in I} X_i$ such that $\pi_i x = x_i$. Then we set $\psi y = x \in X$. Obviously, ψ is an A-homomorphism and $\pi_i\psi = \varphi_i$ for each $i \in I$. If ψ' is another homomorphism from Y to $\prod\limits_{i\in I} X_i$, which makes the diagrams (4.2.8)

commutative, then $\pi_i(\psi - \psi')y = 0$ for all $i \in I$ and so all components of the element $(\psi - \psi')y \in \prod_{i\in I} X_i$ are equal to zero. This means that $(\psi - \psi')y = 0$ for all $y \in Y$, i.e., $\psi - \psi' = 0$.

Lemma 4.2.4 (Five Lemma). *Let*

$$\begin{array}{ccccccccc} M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \xrightarrow{f_3} & M_4 & \xrightarrow{f_4} & M_5 \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} & & \downarrow{\scriptstyle \varphi_4} & & \downarrow{\scriptstyle \varphi_5} \\ N_1 & \xrightarrow{g_1} & N_2 & \xrightarrow{g_2} & N_3 & \xrightarrow{g_3} & N_4 & \xrightarrow{g_4} & N_5 \end{array} \tag{4.2.9}$$

be a commutative diagram with exact rows and isomorphisms φ_i, $i = 1, 2, 4, 5$. Then φ_3 is also an isomorphism.

Proof. Let $x \in M_3$ be in the kernel of φ_3, i.e., $\varphi_3 x = 0$. Then $\varphi_4 f_3 x = g_3\varphi_3 x = 0$ and thus, since φ_4 is an isomorphism, $f_3 x = 0$, i.e., $x \in Ker f_3$. Now, in view of the exactness at M_3, $Ker f_3 = Im f_2$. This means that there is an element $y \in M_2$ such that $x = f_2 y$. In addition, $g_2\varphi_2 y = \varphi_3 f_2 y = \varphi_3 x = 0$. Thus, $\varphi_2 y \in Ker g_2 = Im g_1$, i.e., $\varphi_2 y = g_1 z$ for some $z \in N_1$. However, φ_1 is also an isomorphism and therefore $z = \varphi_1 u$ with $u \in M_1$ and $\varphi_2 f_1 u = g_1\varphi_1 u = g_1 z = \varphi_2 y$. Hence $f_1 u = y$ and $x = f_2 y = f_2 f_1 u = 0$. Consequently, $Ker\varphi_3 = 0$ and so φ_3 is a monomorphism.

Now, choose an element $a \in N_3$. Since φ_4 is an isomorphism, there is $b \in M_4$ such that $\varphi_4 b = g_3 a$. Moreover, $\varphi_5 f_4 b = g_4\varphi_4 b = g_4 g_3 a = 0$ and thus $f_4 b = 0$ and $b \in Ker f_4 = Im f_3$. Hence $b = f_3 c$, where $c \in M_3$. Put $e = a - \varphi_3 c$. Since $g_3\varphi_3 c = \varphi_4 f_3 c = \varphi_4 b = g_3 a$, $g_3 e = 0$ and $e \in Ker g_3 = Im g_2$. Thus, $e = g_2 d$ for some $d \in N_2$. Furthermore, $d = \varphi_2 h$ for $h \in M_2$. Then $\varphi_3 f_2 h = g_2\varphi_2 h = g_2 d = e$ and we obtain $a = e + \varphi_3 c = \varphi_3(f_2 h + c) \in Im\varphi_3$. It follows that φ_3 is an epimorphism, and thus an isomorphism.[3])

Corollary 4.2.5. *Let*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} & & \\ 0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & 0 \end{array} \tag{4.2.10}$$

be a commutative diagram with exact rows and isomorphisms φ_1 and φ_3. Then φ_2 is also an isomorphism.

Proof. This follows immediately from lemma 4.2.4 if we complete diagram (4.2.10) by the zero homomorphisms of the zero modules to the form of diagram (4.2.9).

[3]) This type of argument is called "diagram chasing". It is an elegant, rewarding and powerful technique.

Corollary 4.2.6. *Let*

$$\begin{array}{ccccccc} M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} & & \\ N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & 0 \end{array} \tag{4.2.11}$$

be a commutative diagram with exact rows and isomorphisms φ_1 and φ_2. Then φ_3 is also an isomorphism.

Proof. This follows immediately from lemma 4.2.4 if we complete diagram (4.2.11) to the diagram

$$\begin{array}{ccccccccc} M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 & \longrightarrow & 0 \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} & & \downarrow & & \downarrow \\ N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & 0 & \longrightarrow & 0 \end{array}$$

by the zero homomorphism.

Similarly we have the following statement:

Corollary 4.2.7. *Let*

$$\begin{array}{ccccccc} 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 \\ & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} \\ 0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 \end{array} \tag{4.2.12}$$

be a commutative diagram with exact rows and isomorphisms φ_2 and φ_3. Then φ_1 is also an isomorphism.

4.3 THE HOM FUNCTORS

Let M and N be right A-modules, then the set $Hom_A(M,N)$ of all A-homomorphisms from M to N forms an additive Abelian group. We shall show that for each fixed right A-module M $Hom_A(M,*)$ is a covariant functor from the category $\mathbf{M}_A$ of right A-modules to the category **Ab** of Abelian groups and $Hom_A(*,M)$ is a contravariant functor from $\mathbf{M}_A$ to **Ab**.

Suppose M, B, C and D are right A-modules. If $\varphi : B \to C$ is an A-homomorphism, then φ determines an additive group homomorphism $\varphi_* : Hom_A(M,B) \to Hom_A(M,C)$ given by $\varphi_*(f) = \varphi f$ for any $f \in Hom_A(M,B)$. If $\psi \in Hom_A(C,D)$, then $(\varphi\psi)_*(f) = (\varphi\psi)(f) = \varphi(\psi f) = \varphi_*(\psi f) = \varphi_*\psi_* f$ if the product $\varphi\psi$ is defined. Hence, $(\varphi\psi)_* = \varphi_*\psi_*$. Moreover, $(1_B)_* = 1_{Hom(M,B)}$. Thus, $Hom(M,*)$ is a covariant functor.

In a similar way one can show that for a fixed right A-module M $Hom(*,M)$ is a contravariant functor from $\mathbf{M}_A$ to **Ab**. In this case for each $\varphi \in Hom_A(B,C)$

and $f \in Hom_A(C,M)$ we define $\varphi^* : Hom_A(C,M) \to Hom_A(B,M)$ as $\varphi^*(f) = f\varphi$. If $\psi \in Hom_A(C,D)$, then $(\varphi\psi)^*(f) = f\varphi\psi = (\varphi^* f)\psi = \psi^*(\varphi^* f) = (\psi^*\varphi^*)(f)$. Hence, $(\varphi\psi)^* = \psi^*\varphi^*$.

So $Hom_A(M,N)$ is a bifunctor, which is covariant in the second variable and contravariant in the first.

Note that if $f_i : M' \to M$ and $\varphi : N \to N'$ for $i = 1, 2$, then

$$Hom_A(f_1 + f_2, N) = Hom_A(f_1, N) + Hom_A(f_2, N)$$

and

$$Hom_A(M, \varphi_1 + \varphi_2) = Hom_A(M, \varphi_1) + Hom_A(M, \varphi_2).$$

Thus, the Hom functor is additive.

Proposition 4.3.1. *A sequence of right A-modules B_1, B, B_2*

$$0 \longrightarrow B_1 \xrightarrow{\varphi} B \xrightarrow{\psi} B_2 \tag{4.3.1}$$

is exact if and only if for any right A-module M the sequence

$$0 \longrightarrow Hom_A(M, B_1) \xrightarrow{\overline{\varphi}} Hom_A(M, B) \xrightarrow{\overline{\psi}} Hom_A(M, B_2) \tag{4.3.2}$$

is exact.

Proof.

1. Assume that sequence (4.3.1) is exact. Suppose that $f_1, f_2 \in Hom_A(M, B_1)$ and $\overline{\varphi}(f_1) = \overline{\varphi}(f_2)$. Then $\varphi f_1 = \varphi f_2$. But by hypothesis φ is a monomorphism, so $f_1 = f_2$. Hence, $\overline{\varphi}$ is a monomorphism with the image

$$Im\overline{\varphi} = \{\ \alpha \in Hom_A(M, B) \mid Im\alpha \subseteq Im\varphi\ \}.$$

Since $Im\varphi = Ker\psi$, we obtain that $\psi\alpha = \psi\varphi f = 0$. But $\overline{\psi} = \psi\overline{\varphi}$, therefore $Im\overline{\varphi} \subseteq Ker\overline{\psi}$. On the other hand, let $\beta : M \to B$ and $\beta \in Ker\overline{\psi}$, i.e., $\psi\beta = 0$. Then $Im\beta \subseteq Ker\psi = Im\varphi$ and hence we obtain $Ker\overline{\psi} \subseteq Im\overline{\varphi}$. So we conclude that $Ker\overline{\psi} = Im\overline{\varphi}$, and we have shown that the sequence (4.3.2) is exact.

2. Conversely, let the sequence (4.3.2) be exact for any M. Taking $M = Ker\varphi$ we see that the map $Hom_A(Ker\varphi, B_1) \longrightarrow Hom_A(Ker\varphi, B_2)$ is a monomorphism. Thus, if i is the embedding of $Ker\varphi$ into B_1, then $\varphi i = 0$ and $i = 0$. Therefore $Ker\varphi = 0$ and φ is a monomorphism.

Now, let $N = B_1$. Then $\varphi 1_M = \bar{\varphi}(1_M) \in Im\bar{\varphi} = Ker\bar{\psi}$. Thus, $\psi\varphi = \bar{\psi}(\varphi) = 0$ and $Im\varphi \subset Ker\varphi$. Finally, taking $M = Ker\psi$ and denoting by σ the embedding of M in B_2 , we obtain $\bar{\psi}(\sigma) = \psi\sigma = 0$ Thus, $\sigma \in Ker\bar{\psi} = Im\bar{\varphi}$. Therefore $\sigma = \varphi\theta$, $Ker\psi = Im\sigma \subset Im\varphi$, and the sequence (4.3.1) is exact.

In a similar way one can prove the following statement:

Proposition 4.3.2. *A sequence of right A-modules* B_1, B, B_2

$$B_1 \xrightarrow{\varphi} B \xrightarrow{\psi} B_2 \longrightarrow 0 \tag{4.3.3}$$

is exact if and only if for any right A-module M *the sequence*

$$0 \longrightarrow Hom_A(B_2, M) \xrightarrow{\overline{\varphi}} Hom_A(B, M) \xrightarrow{\overline{\psi}} Hom_A(B_1, M) \tag{4.3.4}$$

is exact.

Let A and A' be rings and let $F : \mathbf{M}_A \to \mathbf{M}_{A'}$ be a covariant functor. Suppose $0 \longrightarrow B_1 \xrightarrow{\varphi} B \xrightarrow{\psi} B_2$ is an arbitrary exact sequence in $\mathbf{M}_A$, then we say that F is **left exact** if the sequence

$$0 \longrightarrow F(B_1) \xrightarrow{\varphi} F(B) \xrightarrow{\psi} F(B_2)$$

is exact in $\mathbf{M}_{A'}$. Analogously, we say that F is **right exact** if from the exactness of an arbitrary sequence of right A-modules $B_1 \xrightarrow{\varphi} B \xrightarrow{\psi} B_2 \longrightarrow 0$ there follows the exactness of the sequence

$$F(B_1) \xrightarrow{\varphi} F(B) \xrightarrow{\psi} F(B_2) \longrightarrow 0$$

in $\mathbf{M}_{A'}$. If F both left and right exact, i.e., if exactness of a sequence

$$0 \longrightarrow B_1 \xrightarrow{\varphi} B \xrightarrow{\psi} B_2 \longrightarrow 0$$

always implies exactness of a sequence

$$0 \longrightarrow F(B_1) \xrightarrow{\varphi} F(B) \xrightarrow{\psi} F(B_2) \longrightarrow 0$$

then F is said to be an **exact functor**.

In accordance with these definitions we can reformulate propositions 4.3.1 and 4.3.2 in the following form:

Proposition 4.3.3. *The Hom functor is left exact in each variable.*

The following statements show the behavior of the Hom functor with regards to direct sums and direct products.

Proposition 4.3.4. *Let* A *be a ring and* Y, X_i, $(i \in I)$ *be A-modules. Then there exists a natural* [4]) *isomorphism*

$$Hom_A(\bigoplus_{i\in I} X_i, Y) \simeq \prod_{i\in I} Hom_A(X_i, Y).$$

[4]) The technical meaning of "natural" is "functorial", see the definition of "natural transformation" in section 4.1 above. It was precisely to distinguish "natural" (iso)morphisms from accidental ones that category theory was invented.

Proof. Let $\bigoplus_{i\in I} X_i = X$ and $\sigma_i : X_i \to X$ be the canonical injection for the direct sum. If now $f \in Hom_A(X,Y)$, then $(..., f\sigma_i, ...) \in \prod_{i\in I} Hom_A(X_i, Y)$. The map $\varphi : Hom(\bigoplus_{i\in I} X_i, Y) \to \prod_{i\in I} Hom_A(X_i, Y)$ such that $\varphi(f) = (..., f\sigma_i, ...)$ yields the required isomorphism.

Proposition 4.3.5. *Let A be a ring and X, Y_i, $(i \in I)$ be A-modules. Then there exists a natural isomorphism*

$$Hom_A(X, \prod_{i\in I} Y_i) \simeq \prod_{i\in I} Hom_A(X, Y_i).$$

Proof. Let $\prod_{i\in I} Y_i = Y$ and $\pi_i : X \to X_i$ be the canonical projection for the direct product. Then each A-homomorphism $f \in Hom_A(X, \prod_{i\in I} Y_i)$ defines homomorphisms $\pi_i f \in Hom_A(X, Y_i)$. Then the map

$$\varphi : Hom(X, \prod_{i\in I} Y_i) \to \prod_{i\in I} Hom_A(X, Y_i)$$

such that $\varphi(f) = (..., \pi_i f, ...)$ yields the required isomorphism.

4.4 BIMODULES

In general, the Abelian group $Hom_A(M,N)$ is not a right A-module. However there are some cases when this is true (in a natural way). For example, this is true if A is a commutative ring. In this section we consider another important case when $Hom_A(M,N)$ is a module.

Definition. Let A and B be two rings. An Abelian group M is called an (A,B)-**bimodule**, which is denoted by ${}_AM_B$, if M is both a left A-module and a right B-module such that $(am)b = a(mb)$ for all $a \in A$, $m \in M$, and $b \in B$.

If M and N are both (A,B)-bimodules, then a map $f : M \to N$, which is simultaneously A-linear and B-linear, is called a **homomorphism of bimodules**. Analogously for bimodules one can introduce all other concepts which were introduced for modules: isomorphism, subbimodule, quotient bimodule, direct sum, etc.

Example 4.4.1.
Every ring A may be considered as a bimodule over itself. This bimodule is called the regular bimodule and denoted by ${}_AA_A$.

Example 4.4.2.
Every right A-module M is a $(\mathbf{Z}, A)$-bimodule, i.e., $M = {}_{\mathbf{Z}}M_A$.

Example 4.4.3.
If $C = Cen(A)$ is the center of a ring A, then every A-module is a (C, A)-bimodule.

If $M = {}_BM_A$ is a bimodule, then $Hom_A({}_BM_A, N_A)$ may be considered as a right B-module by setting $(fb)(m) = f(bm)$ for any $f \in Hom_A({}_BM_A, N_A)$, $b \in B$, and $m \in M$. Analogously, if $N = {}_BN_A$ is a bimodule, then $Hom_A(M_A, {}_BN_A)$ may be considered as a left B-module by setting $(bf)(m) = bf(m)$ for any $f \in Hom_A(M_A, {}_BN_A)$, $b \in B$, and $m \in M$.

Example 4.4.4.
If M is an Abelian group, then it is both a left and a right $\mathbf{Z}$-module. Since A is an $(A, \mathbf{Z})$-bimodule, then $Hom_{\mathbf{Z}}(A, M) = Hom_{\mathbf{Z}}({}_AA_{\mathbf{Z}}, M_{\mathbf{Z}})$ is a right A-module. Analogously, $Hom_{\mathbf{Z}}(M, A) = Hom_{\mathbf{Z}}(M_{\mathbf{Z}}, {}_AA_{\mathbf{Z}},)$ is a left A-module.

4.5 TENSOR PRODUCTS OF MODULES

Let A be any ring, and let $X \in \mathbf{M}_A$ be a right A-module and $Y \in {}_A\mathbf{M}$ be a left A-module.

Definition. Let A be a ring and G be an additive Abelian group. Suppose $X \in \mathbf{M}_A$ and $Y \in {}_A\mathbf{M}$. An A-**balanced map** from $X \times Y$ to G is a map $\varphi : X \times Y \to G$ satisfying the following identities:
1) $\varphi(x, y + y') = \varphi(x, y) + \varphi(x, y')$,
2) $\varphi(x + x', y) = \varphi(x, y) + \varphi(x', y)$,
3) $\varphi(xa, y) = \varphi(x, ay)$
for all $x, x' \in X$, $y, y' \in Y$, and $a \in A$.[5])

Consider the free Abelian group F, whose free generators are the elements of $X \times Y$. In other words, each element of this group can be uniquely written as a formal finite sum $\sum_{i,j} c_{ij}(x_i, y_j)$, where $x_i \in X; y_j \in Y$, and $c_{ij} \in \mathbf{Z}$, but only a finite number of the integers c_{ij} are allowed to be nonzero. Then we have a natural monomorphism $i : X \times Y \to F$ such that $i(x, y) = i(x', y')$ if and only if $x = x'$ and $y = y'$.

Let H be the subgroup of F generated by all elements of the form:

$$(x + x', y) - (x, y) - (x', y)$$

$$(x, y + y') - (x, y) - (x, y')$$

$$(xa, y) - (x, ay)$$

Then there is the canonical projection $\pi : F \to F/H$. Write $\varphi = \pi i$, then

$$\varphi((x + x', y) - (x, y) - (x', y)) = 0$$

[5]) Conditions 1) and 2) say that φ is a bilinear map of Abelian groups.

$$\varphi((x, y + y') - (x, y) - (x, y')) = 0$$

$$\varphi((xa, y) - (x, ay)) = 0$$

i.e., the map φ is A-balanced from $X \times Y$ to F/H.

We write $\varphi(x, y) = x \otimes y$ and write $X \otimes Y$ (or $X \otimes_A Y$ if A is to be emphasized) for the Abelian quotient group F/H. With these notations we have that $X \otimes Y$ is an Abelian group, whose generators $x \otimes y$ satisfy the following identities:

$$(x_1 + x_2) \otimes y = (x_1 \otimes y) + (x_2 \otimes y)$$

$$x \otimes (y_1 + y_2) = (x \otimes y_1) + (x \otimes y_2)$$

$$x\alpha \otimes y = x \otimes \alpha y$$

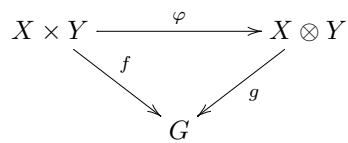
Note that these properties imply

$$(x \otimes y)k = xk \otimes y = x \otimes ky$$

for all $x \in X$, $y \in Y$ and $k \in \mathbf{Z}$. In particular, $0 \otimes y = x \otimes 0 = 0$ for all $x \in X$, $y \in Y$. From these properties it follows that each element of $X \otimes Y$ can be written as a finite sum of the form $\sum(x \otimes y)$, where $x \in X$ and $y \in Y$, but this representation is not unique in the general case. If a set $\{x_i | i \in I\}$ generates X and $\{y_j | j \in J\}$ generates Y, then the set $\{x_i \otimes y_j | i \in I, j \in J\}$ generates $X \otimes Y$.

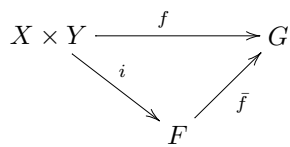
We shall show that the Abelian group $X \otimes Y$ has a **universal property**, which we formulate as the following proposition:

Proposition 4.5.1. *Let A be a ring and G be an Abelian group. Let $X \in \mathbf{M}_A$ and $Y \in {}_A\mathbf{M}$. For any A-balanced map $f : X \times Y \to G$ there exists a unique morphism of Abelian groups $g : X \otimes Y \to G$ such that the diagram*



is commutative.

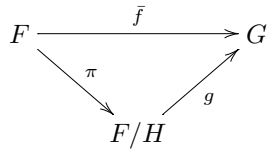
Proof. Suppose f is an A-balanced map from $X \times Y$ to an Abelian group G. Since F is a free Abelian group, there exists a unique homomorphism $\bar{f} : F \to G$ such that the diagram



is commutative, i.e., $\bar{f}i = f$, where i is the natural embedding. Since f is an A-balanced map from $X \times Y$ to G, this is also true for $\bar{f}$, i.e.,

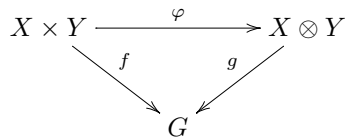
$$\bar{f}(x + x', y) = \bar{f}(x, y) + \bar{f}(x', y)$$
$$\bar{f}(x, y + y') = \bar{f}(x, y) + \bar{f}(x, y')$$
$$\bar{f}(xa, y) = \bar{f}(x, ay)$$

So $H \subseteq Ker\bar{f}$ and, by proposition 1.2.1, there exists a unique homomorphism $g : F/H \to G$ such that the diagram



is commutative.

Let $\varphi = \pi i$, then $g\varphi = g\pi i = \bar{f}i = f$ and so the diagram

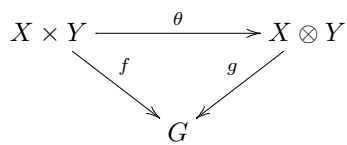


is commutative.

Now, let's show that g is unique in making this diagram commutative. If g' is another homomorphism from F/H to G, which makes this diagram commutative, i.e., $g'\varphi = f$, then $g'\pi i = g'\varphi = f = g\pi i = \bar{f}i$. Hence, by uniqueness of $\bar{f}$, we have $g'\pi = \bar{f}$. So $g'\pi = \bar{f} = g\pi$ and since π is surjective, we have $g = g'$. Hence, g is unique.

As we have seen $X \otimes_A Y$ is more that just an Abelian group. It comes equipped with a unique canonical map $X \times Y \to X \otimes_A Y$ having the universal property described above. These observations give us the basis to introduce the following formal definition:

Definition. Let X_A and ${}_AY$ be modules over a ring A. A pair (T, θ) is a **tensor product** of modules X and Y over A if T is an Abelian group and for any Abelian group G and all A-balanced maps $f : T \to G$ there exists a unique group homomorphism $g : T \to G$ such that the diagram



is commutative.

Then we obtain the following proposition:

Proposition 4.5.2. *Let A be a ring and $X \in \mathbf{M}_A$ and $Y \in {}_A\mathbf{M}$. Suppose that $(X \otimes_A Y, \varphi)$ is as before, then:*

1. *$(X \otimes_A Y, \varphi)$ is a tensor product of X and Y;*

2. *If (T, θ) is any other tensor product of X and Y, then there exists an Abelian group isomorphism $\sigma : X \otimes_A Y \to T$ such that $\sigma\varphi = \theta$, i.e., the diagram*

$$\begin{array}{ccc} X \times Y & \xrightarrow{\varphi} & X \otimes_A Y \\ & {\scriptstyle\theta}\searrow \quad \swarrow{\scriptstyle\sigma} & \\ & T & \end{array}$$

is commutative.

Proof.

1. This follows immediately from proposition 4.5.1.

2. Let (T, θ) be any other tensor product of X and Y. Since θ is an A-balanced map, by the universal property for $X \otimes_A Y$, there exists $\sigma : X \otimes_A Y \to T$ such that $\sigma\varphi = \theta$. Similarly, since $\varphi : X \times Y \to X \otimes_A Y$ is an A-balanced map, by the definition of a tensor product, there exists $\tau : T \to X \otimes Y$ such that $\tau\theta\varphi$. Thus, $\tau\sigma\varphi = \varphi$ and $\sigma\tau\theta = \theta$. Then uniqueness of θ and φ implies that $\tau\sigma$ and $\sigma\tau$ are both identity maps on appropriate groups. In particular, σ is an isomorphism.[6])

Example 4.5.1.

Let $A = \mathbf{Z}$, $X = \mathbf{Q}$, $Y = \mathbf{Z}_n = \mathbf{Z}/(n)$, then $X \otimes_{\mathbf{Z}} Y = \mathbf{Q} \otimes_{\mathbf{Z}} \mathbf{Z}_n = 0$. In fact any element $x \in X$ is of the form $x = nq$ for some $q \in Q$. Thus, for any $y \in Y$ we have $x \otimes y = qn \otimes y = q \otimes ny = q \otimes 0 = 0$.

Example 4.5.2.

Let $A = \mathbf{Z}$, $X = \mathbf{Z}_p$, $Y = \mathbf{Z}_q$, where $1 \leq p, q \in \mathbf{Z}$ and $(p, q) = 1$, the greatest common divisor of the natural number p and q, then $\mathbf{Z}_p \otimes \mathbf{Z}_q = 0$. In fact, since $(p, q) = 1$, there exists $a, b \in \mathbf{Z}$ such that $ap + bq = 1$. Then

$$(x \otimes y) = (x \otimes y)(ap + bq) = (x \otimes y)ap + (x \otimes y)bq =$$

$$= (xap \otimes y) + ((x \otimes bqy) = (0 \otimes y) + (x \otimes 0) = 0.$$

Example 4.5.3.

More generally let $A = \mathbf{Z}$, $X = \mathbf{Z}_p$, $Y = \mathbf{Z}_q$, where $1 \leq p, q \in \mathbf{Z}$ and $(p, q) = d$, the greatest common divisor of the natural number p and q, then $\mathbf{Z}_p \otimes \mathbf{Z}_q \simeq \mathbf{Z}_d$.

[6]) This is an instance of a general observation. Objects (with the appropriate morphisms) defined by a universal property are unique up to isomorphism. We have also already seen that above in the case of direct sums and products.

To see this, observe first that

$$x \otimes y = x \otimes (y \cdot 1) = (xy) \otimes 1 = xy(1 \otimes 1)$$

from which it follows that $\mathbf{Z}_p \otimes \mathbf{Z}_q$ is a cyclic group with $1 \otimes 1$ as generator. Since $p(1 \otimes 1) = p \otimes 1 = 0 \otimes 1 = 0$ and similarly $q(1 \otimes 1) = 1 \otimes q = 1 \otimes 0 = 0$, we have $d(1 \otimes 1) = 0$, so this cyclic group has order dividing d. The map $\varphi : \mathbf{Z}_p \times \mathbf{Z}_q \to \mathbf{Z}_d$ defining by $\varphi(x \bmod p, y \bmod q) = xy \bmod d$ is well defined since d divides both p and q. It is clearly $\mathbf{Z}$-bilinear. The induced map $\psi : \mathbf{Z}_p \otimes \mathbf{Z}_q \to \mathbf{Z}_d$ maps the element $1 \otimes 1$ to the element $1 \in \mathbf{Z}_d$ which is an element of order d. In particular $\mathbf{Z}_p \otimes \mathbf{Z}_q$ has order at least d. Hence $1 \otimes 1$ is an element of order d and ψ gives an isomorphism $\mathbf{Z}_p \otimes \mathbf{Z}_q \simeq \mathbf{Z}_d$.

In general, the Abelian group $X \otimes_A Y$ is not an A-module. But in some cases we can turn it into a module (in a natural way). Suppose, for instance, that we have a right A-module X_A and an (A, B)-bimodule ${}_AY_B$. Then every element $b \in B$ induces an A-module homomorphism $b : Y \to Y$ that assigns to every $y \in Y$ the element $yb \in Y$. This homomorphism induces a homomorphism $\sigma_b : X \otimes Y \to X \otimes Y$ defined by: $\sigma_b(x \otimes y) = x \otimes (yb)$. Clearly, σ_b is an A-balanced map and in this way $X \otimes_A Y$ turns into a right B-module with $(x \otimes y)b = x \otimes (yb)$. A similar situation ${}_BX_A$, ${}_AY$ defines on $X \otimes_A Y$ a left B-module structure by $b(x \otimes y) = (bx) \otimes y$. Finally, in a situation when we have two bimodules ${}_BX_A$ and ${}_AY_C$, the tensor product $X \otimes_A Y$ becomes a (B, C)-bimodule with: $(x \otimes y)c = x \otimes (yc)$ and $b(x \otimes y) = (bx) \otimes y$ for all $b \in B$ and $c \in C$. This allows to iterate the tensor product operation and define a product of three or more modules. The following result shows the associativity of tensor product.

Proposition 4.5.3. *Let A and B be rings and let X_A, ${}_AY_B$ and ${}_BZ$ be appropriate modules. Then there exists a canonical isomorphism:*

$$(X \otimes_A Y) \otimes_B Z \simeq X \otimes_A (Y \otimes_B Z)$$

assigning to $(x \otimes_A y) \otimes_B z$ the element $x \otimes_A (y \otimes_B z)$. If X is (C, A)-bimodule, then this is an isomorphism of C-modules.

Proof. For each fixed element $z \in Z$ we can define the map $\sigma_z : X \times Y \to X \otimes_A (Y \otimes_B Z)$ by $\sigma_z(x, y) = x \otimes_A (y \otimes_B z)$. Clearly, σ_z is an A-balanced map and therefore there exists a unique homomorphism $f_z : X \otimes_A Y \to X \otimes_A (Y \otimes_B Z)$ assigning to $x \otimes_A y$ the element $x \otimes_A (y \otimes_B z)$. Varying z, we obtain a B-balanced map $\varphi : (X \otimes_A Y) \times Z \to X \otimes_A (Y \otimes_B Z)$ that assigns to a pair $(x \otimes_A y, z)$ the element $x \otimes_A (y \otimes_B z)$. In turn, φ defines a unique homomorphism $f : (X \otimes_A Y) \otimes_B Z \to X \otimes_A (Y \otimes_B Z)$ such that $f((x \otimes_A y) \otimes_B z) = x \otimes_A (y \otimes_B z)$. In a similar manner, we can construct a homomorphism $g : X \otimes_A (Y \otimes_B Z) \to (X \otimes_A Y) \otimes_B Z$ such that $g(x \otimes_A (y \otimes_B z)) = (x \otimes_A y) \otimes_B z$. Since all possible elements of the form $x \otimes_A (y \otimes_B z)$ (respectively, $(x \otimes_A y) \otimes_B z$) generate the group $X \otimes_A (Y \otimes_B Z)$ (respectively, $(X \otimes_A Y) \otimes_B Z$), f is inverse of g, as required.

Since A is an (A, A)-bimodule, $X \otimes_A A$ is a right A-module and $A \otimes_A Y$ is a left A-module. In this situation we have the following statement.

Proposition 4.5.4. *Suppose X is a right A-module and Y is a left A-module. Then*

1) *the map $\varphi : X \to X \otimes_A A$ that assigns to every $x \in X$ the element $x \otimes 1$ is an isomorphism of right A-modules*;

2) *the map $\psi : Y \to A \otimes_A Y$ that assigns to every $y \in Y$ the element $1 \otimes y$ is an isomorphism of left A-modules.*

Proof. It is sufficient to observe that the map $X \times A \to X$, sending (x, a) into xa, is evidently a balanced map and that the induced map $X \otimes_A A \to X$ is a homomorphism which is inverse to the map $\varphi : X \to X \otimes_A A$.

4.6 TENSOR PRODUCT FUNCTOR

We now consider some of the basic properties of tensor products. The following statement defines the "tensor product" of two homomorphisms.

Proposition 4.6.1. *Let A be a ring, and let X, X' be right A-modules and Y, Y' be left A-modules. For any pair of A-modules homomorphisms $f : X \to X'$ and $g : Y \to Y'$ there exists a unique group homomorphism $f \otimes_A g : X \otimes_A Y \to X' \otimes_A Y'$ such that $(f \otimes_A g)(x \otimes_A y) = f(x) \otimes_A g(y)$. If X, X' are moreover (B, A)-bimodules for some ring B and f is also a B-module homomorphism, then $f \otimes_A g$ is a homomorphism of left B-modules.*

If $f' : X' \to X''$ and $g' : Y' \to Y''$ is another pair of homomorphisms, then $(f' \otimes_A g')(f \otimes_A g) = f'f \otimes_A g'g$. In particular, if f and g are isomorphisms, then so is $f \otimes g$.

Proof. Consider the map $\sigma : X \times Y \to X' \times Y'$ given by $\sigma(x, y) = (f(x), g(y))$. Then we have a bilinear map $F : X \times Y \to X' \otimes Y'$ such that $F(x, y) = \varphi\sigma(x, y) = (f(x) \otimes_A g(y))$, where $\varphi' : X' \times Y' \to X' \otimes Y'$. Therefore there exists a unique homomorphism $f \otimes_A g : X \otimes_A Y \to X' \otimes_A Y'$ such that $(f \otimes_A g)(x \otimes_A y) = f(x) \otimes_A g(y)$.

If X, X' are also (B, A)-bimodules for some ring B and f is also a B-module homomorphism, then we have

$$(f \otimes g)(b(x \otimes y)) = (f \otimes g)(bx \otimes y) = f(bx) \otimes g(y) = bf(x) \otimes g(y).$$

Since $(f \otimes g)$ is additive, this extends to sum of simple tensors to show that $(f \otimes g)$ is a B-module homomorphism.

The last statement is trivial.

From this proposition it follows that we can consider the tensor product as a functor on a module category. More precisely, fix a left A-module Y and construct

the functor $* \otimes_A Y : \mathbf{M}_A \to \mathbf{Ab}$ as follows. Assign to every right A-module X the Abelian group $X \otimes Y$ and to every homomorphism $f : X \to X'$ the homomorphism $f \otimes_A 1 : X \otimes_A Y \to X' \otimes_A Y$. Proposition 4.6.1 shows that $f \otimes_A 1$ is a group homomorphism and we obtain a functor

$$* \otimes_A : X \to X \otimes_A Y$$

from the category of right A-modules to the category of Abelian groups. If in addition Y is an (A, B)-bimodule for some ring B, then $f \otimes_A 1$ is a homomorphism of right B-modules and we obtain a functor from the category of right A-modules to the category of right B-modules. Similarly, for a fixed right A-module X we can construct the functor

$$X \otimes_A * : Y \to X \otimes_A Y$$

from the category of left A-modules to the category of Abelian groups (respectively, to the category of left B-modules when X is a (B, A)-bimodule for some ring B). Thus we have a functor of two variables which is called the **tensor product** and we denote it by $* \otimes *$. This functor is covariant in both variables, because

$$f'f \otimes 1 = (f' \otimes 1)(f \otimes 1)$$

and

$$1 \otimes g'g = (1 \otimes g')(1 \otimes g)$$

The next proposition states that the tensor product functor preserves direct sums.

Proposition 4.6.2. *Let A be a ring and $X \in \mathbf{M}_A$, $Y \in {}_A\mathbf{M}$.*
1. *If $X = \bigoplus\limits_{i \in I} X_i$, then*

$$X \otimes_A Y \simeq \bigoplus_{i \in I} (X_i \otimes Y)$$

2. *If $Y = \bigoplus\limits_{i \in I} Y_i$, then*

$$X \otimes_A Y \simeq \bigoplus_{i \in I} (X \otimes Y_i)$$

Proof. We prove only the first part of the proposition. The proof of the second part is analogous. Let $\sigma_i : X_i \to X$ be the canonical injection and $\pi_i : X \to X_i$ be the canonical projection for the direct sum $X = \bigoplus\limits_{i \in I} X_i$. These satisfy the following relations:

1) $\pi_i \sigma_i = 1_{X_i}$ and $\pi_i \sigma_j = 0$ for $i \neq j$;

2) each element $x \in X$ can be written in the form of a finite sum $x = \sigma_{i_1} \pi_{i_1} x + \ldots + \sigma_{i_n} \pi_{i_n} x$.

Then, by proposition 4.6.1, we have maps $\bar{\pi}_i = \pi_i \otimes 1_Y : X \otimes Y \to X_i \otimes Y$ and $\bar{\sigma}_i = \sigma_i \otimes 1_Y : X_i \otimes Y \to X \otimes Y$, which satisfy analogous relations. So the set of homomorphisms $\{\bar{\pi}_i\}, \{\bar{\sigma}_i\}$ defines $X \otimes Y$ as the direct sum $\underset{i \in I}{\oplus}(X_i \otimes Y)$.

The following statement shows the connection between Hom and tensor products.

Proposition 4.6.3 (Adjoint isomorphism).
1. *In a situation X_A, ${}_AY_B$ and ${}_BZ$, there exists a canonical isomorphism:*

$$Hom_B(X \otimes_A Y, Z) \simeq Hom_A(X, Hom_B(Y, Z)),$$

assigning to a homomorphism $f : X \otimes_A Y \to Z$ the homomorphism $\bar{f} : X \to Hom_B(Y, Z)$ such that $\bar{f}(x)(y) = f(x \otimes_A y)$.
2. *In a situation ${}_AX$, ${}_BY_A$ and ${}_BZ$, there exists a canonical isomorphism:*

$$Hom_B(Y \otimes_A X, Z) \simeq Hom_A(X, Hom_B(Y, Z)),$$

assigning to a homomorphism $g : Y \otimes_A X \to Z$ the homomorphism $\bar{g} : X \to Hom_B(Y, Z)$ such that $\bar{g}(x)(y) = g(y \otimes_A x)$.

Proof. Like in the previous proposition we prove only the first part of the proposition. The proof of the second part is analogous. We show that the map $\bar{f}$ is an A-module homomorphism, i.e., $\bar{f}(xa) = \bar{f}(x)a$ for any $a \in A$. In fact:

$$\bar{f}(xa)(y) = f(xa \otimes y) = f(x \otimes ay) = \bar{f}(x)(ay) = [\bar{f}(x)a](y).$$

Analogously it is easy to prove the other axioms of A-module homomorphisms. We shall construct an inverse map. Let $g : X \to Hom_B(Y, Z)$ be an A-module homomorphism. Then, evidently, the map $X \times Y \to Z$ sending (x, y) into $g(x)(y)$ is a balanced map, and therefore defines a unique homomorphism $\bar{g} : X \otimes_A Y \to Z$ such that $\bar{g}(x \otimes_A y) = g(x)(y)$. Now, $\bar{g}$ is clearly a B-module homomorphism and the constructions $f \mapsto \bar{f}$ and $g \mapsto \bar{g}$ are mutually inverse.

Proposition 4.6.4. *The tensor product functor is right exact in both variables.*

Proof. We shall show that the tensor product functor is right exact in the first variable, i.e., for any fixed (A, B)-module Y the functor $* \otimes_A Y$ is right exact. Let a sequence of right A-modules

$$X_1 \longrightarrow X \longrightarrow X_2 \longrightarrow 0 \tag{4.6.1}$$

be exact. We need to show the exactness of the sequence

$$X_1 \otimes_A Y \longrightarrow X \otimes_A Y \longrightarrow X_2 \otimes_A Y \longrightarrow 0 \tag{4.6.2}$$

for any (A, B)-bimodule Y. In view of proposition 4.3.2 it is equivalent to verify the exactness of the sequence

$$0 \longrightarrow Hom_B(X_2 \otimes_A Y, Z) \longrightarrow Hom_B(X \otimes_A Y, Z) \longrightarrow$$

$$Hom_B(X_1 \otimes_A Y, Z) \tag{4.6.3}$$

for any B-module Z. By proposition 4.6.3, the latter sequence can be rewritten as

$$0 \longrightarrow Hom_A(X_2, Hom_B(Y, Z)) \longrightarrow Hom_A(X, Hom_B(Y, Z)) \longrightarrow$$

$$Hom_A(X_1, Hom_B(Y, Z)) \tag{4.6.4}$$

and thus its exactness follows immediately from proposition 4.3.2. Analogously we can show that the functor $X \otimes_A *$ is right exact.

4.7 DIRECT AND INVERSE LIMITS

Definition. A partially ordered set S is called (upwards) **directed** if for any pair $a, b \in S$ there is an element $c \in S$ such that $a \leq c$ and $b \leq c$.

Let I be a directed partially ordered set, $\{M_i \ : \ i \in I\}$ be a set of A-modules and suppose that for any pair of indexes $i, j \in I$, where $i \leq j$, there is given a homomorphism $\varphi_{ij} : M_i \to M_j$ such that for all $i \leq j \leq k$ and $n \in I$ the following hold:

(1) $\varphi_{nn} : M_n \to M_n$ is the identity on M_n;

(2) $\varphi_{ik} = \varphi_{jk}\varphi_{ij}$, i.e., the diagram

$$\begin{array}{ccc} M_i & \xrightarrow{\varphi_{ij}} & M_j \\ & {\scriptstyle \varphi_{ik}} \searrow \quad \swarrow {\scriptstyle \varphi_{jk}} & \\ & M_k & \end{array} \tag{4.7.1}$$

commutes.

In this case the triple

$$\mathbf{M} = \{\{I, \leq\}; \{M_i \ : \ i \in I\}; \{\varphi_{ij} \mid i \leq j \in I\}\} \tag{4.7.2}$$

is called a **directed system** of right A-modules.

Let $\mathbf{M}$ be a directed system and $M = \bigoplus\limits_{i \in I} M_i$, where $M_i \in \mathbf{M}$. Consider the submodule $N \subset M$, which is generated by all elements $m_i - \varphi_{ij} m_i$ for $i \leq j$. The quotient module M/N is called the **direct limit** (also called **injective limit**) of the directed system $\mathbf{M}$ and denoted by $\varinjlim M_i$.

There are some important properties concerning the elements of N and M/N.

1. The submodule N consists of all elements of the form

$$m = m_{i_1} + ... + m_{i_k},\ m_i \in M_i$$

such that there exists a $j \in I$ with $j \geq i_1, ..., i_k$ and

$$\varphi_{i_1 j} m_{i_1} + ... + \varphi_{i_k j} m_{i_k} = 0. \tag{4.7.3}$$

Indeed, let $m = m_i - \varphi_{ij} m_i \in M$ be any generator of N. Since

$$\varphi_{ij} m_i - \varphi_{jj}(\varphi_{ij} m_i) = 0$$

for any $i \leq j$, then any generator of N has the required property (4.7.3). Therefore any element of N has that property as well. The inverse follows from the following equality:

$$m_{i_1} + ... + m_{i_k} - \varphi_{i_1 j} m_{i_1} - ... - \varphi_{i_n j} m_{i_k} =$$
$$= (m_{i_1} - \varphi_{i_1 j} m_{i_1}) + ... + (m_{i_n} - \varphi_{i_n j} m_{i_n}) \in N,$$

where $j \geq i_1, i_2, ..., i_k$.

2. Any element $m_* \in \varinjlim M_i$ can be can be written in the form $m_j + N$ for some $j \in I$. Indeed, any element $m \in M$ can be written in the form $m = m_{i_1} + ... + m_{i_k}$, where $m_{i_r} \in M_{i_r}$. Since I is directed, there exists $j \in I$ such that $j \geq i_1, i_2, ..., i_k$. Consider the element $x = \sum_{r=1}^{k} \varphi_{i_r j} m_{i_r} \in M_j$. Then by the previous property $x = m_j \in N$ and $m - x \in N$. Therefore $m = m_j + N$.

3. For each $i \in I$ there exists a natural homomorphism $\pi_i : M_i \longrightarrow \varinjlim M_i = M/N$ given by $\pi(m_i) = m_i + N$. It is easy to verify that these homomorphisms have the following properties:

a) all the diagrams

$$\begin{array}{ccc} M_i & \xrightarrow{\varphi_{ij}} & M_j \\ & {\scriptstyle \varphi_{ik}} \searrow \quad \swarrow {\scriptstyle \varphi_{jk}} & \\ & M_k & \end{array} \tag{4.7.1}$$

commute;

b) if $\pi_i m_i = 0$ for some $m_i \in M_i$, then there exists $j \in I$ such that $j \geq i$ and $\varphi_{ij} m_i = 0$;

c) if each homomorphism φ_{ij} is a monomorphism, then all π_i are monomorphisms;

d) $\varinjlim M_i = \bigcup_{r \in I} \pi_{i_r}(M_{i_r})$, i.e., any element $m_* \in \varinjlim M_i$ can be written in the form $\pi_{i_1} m_{i_1} + ... + \pi_{i_k} m_{i_k}$ for some $i_1, ..., i_k \in I$.

Example 4.7.1.
An ascending union $\cup M_i$ of submodules of a module is a direct limit, i.e., $\cup M_i = \varinjlim M_i$.

Example 4.7.2.
Every module is the direct limit of its finitely generated submodules. In particular, every right ideal $\mathcal{I}$ is the direct limit of finitely generated left ideals contained in $\mathcal{I}$.

The direct limit posses a universal property, which determines the direct limit uniquely up to an isomorphism.

Theorem 4.7.1. *The direct limit $\varinjlim M_i$ of a directed system* **M** *has the following property:*

For any module X and any homomorphisms $f_i : M_i \to X$ such that all diagrams for $i \leq j$

$$\begin{array}{ccc} M_i & \xrightarrow{\varphi_{ij}} & M_j \\ & {\scriptstyle f_i}\searrow & \swarrow{\scriptstyle f_j} \\ & X & \end{array} \tag{4.7.4}$$

commute, there exists a unique homomorphism $\sigma : \varinjlim M_i \longrightarrow X$ such that all diagrams

$$\begin{array}{ccc} M_i & & \\ \downarrow{\scriptstyle \pi_i} & \searrow{\scriptstyle f_i} & \\ \varinjlim M_i & \xrightarrow{\sigma} & X \end{array} \tag{4.7.5}$$

commute. The module $\varinjlim M_i$ with homomorphisms π_i is determined uniquely up to isomorphism.

Proof. Let $m_* \in \varinjlim M_i$, then, by property 2, there exists an $i \in I$ such that $m_* = m_i + N$. In this case we set $\sigma(m_*) = f_i(m_i)$. Since all diagrams (4.7.4) are commutative, $\sigma(m_*)$ does not depend on the index $i \in I$. Moreover, it is easy to see that σ preserves addition and multiplication by an element of the ring A. So that σ is a well-defined A-homomorphism from $\varinjlim M_i$ to X. Obviously, $\sigma(\pi_i m_i) = \sigma(m_*) = f_i(m_i)$, i.e., the diagrams (4.7.5) are commutative.

If σ' is another homomorphism from $\varinjlim M_i$ to X with such properties, then $(\sigma - \sigma')\pi_i = 0$ for each $i \in I$, i.e., $(\sigma - \sigma')(Im\pi_i) = 0$. Then by property 3.d $\sigma - \sigma' = 0$, so that σ is unique.

We shall prove now the last part of the statement.[7]) Let Y be an A-module and

[7]) This is yet another instance of "universal property ⇒ uniqueness".

let the homomorphisms $\tau_i : M_i \to Y$ have the properties for $\varinjlim M_i$ and π_i, which have been proved above. Then we have a unique homomorphism $\sigma : \varinjlim M_i \to Y$ such that $\tau_i = \sigma\pi_i$. On the other hand, by assumptions according to $\varinjlim Y$, we have a unique homomorphism $\tau : Y \to \varinjlim M_i$ such that $\pi_i = \tau\tau_i$. So we obtain $\pi_i = \tau\tau_i = \tau\sigma\pi_i$ and simultaneously $\tau_i = \sigma\pi_i = \sigma\tau\tau_i$. Therefore $\tau\sigma$ is the identity homomorphism on all $Im\pi_i$, and hence, by properties 3.d, on $\varinjlim M_i$. Thus, σ is an isomorphism.

For directed systems with the same index set we can introduce the idea of a homomorphism between them. Suppose we have a partially ordered set I and two directed systems of modules $\mathbf{M} = \{M_i; \varphi_{ij}; i, j \in I\}$ and $\mathbf{N} = \{N_i; \psi_{ij}; i, j \in I\}$. Then a **homomorphism** $\varphi : \mathbf{M} \to \mathbf{N}$ between these directed systems is a family of homomorphisms $f_i :\to N_i$ such that all the following diagrams

$$\begin{array}{ccc} M_i & \xrightarrow{f_i} & N_i \\ \downarrow{\scriptstyle \varphi_{ij}} & & \downarrow{\scriptstyle \psi_{ij}} \\ M_j & \xrightarrow{f_i} & N_j \end{array} \tag{4.7.6}$$

commute.

Let $M_* = \varinjlim M_i$ and $N_* = \varinjlim N_i$. Then we have commutative diagrams

$$\begin{array}{ccccc} M_i & \xrightarrow{f_i} & N_i & & \\ \downarrow{\scriptstyle \varphi_{ij}} & & \downarrow{\scriptstyle \psi_{ij}} & \searrow^{\theta_i} & \\ M_j & \xrightarrow{f_j} & N_j & \xrightarrow{\theta_j} & N_* \end{array}$$

which leads to the commutative diagrams

$$\begin{array}{ccc} M_i & & \\ \downarrow{\scriptstyle \psi_{ij}} & \searrow^{\theta_i f_i} & \\ M_j & \xrightarrow{\theta_j f_j} & N_* \end{array}$$

So, by the universal property of the direct limit, there is a unique homomorphism $f_* : M_* \to N_*$ such that $f_*\pi_i = \theta_i f_i$, i.e., all diagrams

$$\begin{array}{ccc} M_i & & \\ \downarrow{\scriptstyle \pi_i} & \searrow^{\theta_i f_i} & \\ M_* & \xrightarrow{\theta_j f_j} & N_* \end{array} \tag{4.7.7}$$

commute. We shall say that f_* is the homomorphism induced by the family of homomorphisms f_i. If all the f_i are surjective, then $N_* = \bigcup\limits_{i\in I} Im(\theta_i) = \bigcup\limits_{i\in I} Im(\theta_i f_i)$ and so f_* is surjective. Suppose all f_i are injective and $m \in Ker f_*$. Then there exists $i \in I$ such that $m = \pi_i m_i$, where $m_i \in M_i$. Therefore $\theta_i f_i m_i = f_* \pi_i m_i = f_* m = 0$ and so there exists $j \geq i$ such that $\psi_{ij} f_i m_i = 0$. Since $\psi_{ij} f_i = f_j \varphi_{ij}$ and f_i are injective, $\varphi_{ij} m_i = 0$, i.e., $\pi_i m_i = 0$ and $m = 0$. Therefore f_* is injective.

Thus, we have proved the following statement:

Theorem 4.7.2. *If* $\mathbf{M}$, $\mathbf{N}$ *are directed systems of A-modules and* $f : \mathbf{M} \to \mathbf{N}$ *is a homomorphism of directed systems, then there exists a unique homomorphism* $f_* : M_* \to N_*$ *such that all diagrams* (4.7.7) *commute. If* $f = \{f_i\}$ *and all homomorphisms* f_i *are surjective (injective), then* f_* *is also surjective (injective).*

Theorem 4.7.3. *If* $\mathbf{M}$, $\mathbf{N}$, $\mathbf{L}$ *are directed systems of A-modules and for each* $i \in I$ *the sequence*

$$0 \longrightarrow M_i \xrightarrow{f_i} N_i \xrightarrow{g_i} L_i \longrightarrow 0 \tag{4.7.8}$$

is exact, then the sequence of direct limits

$$0 \longrightarrow \varinjlim M_i \xrightarrow{f_*} \varinjlim N_i \xrightarrow{g_*} \varinjlim L_i \longrightarrow 0 \tag{4.7.9}$$

is also exact, where f_* *and* g_* *are the induced homomorphisms.*

Proof. Taking into account theorem 4.7.2 it is sufficient to prove that $Ker(g_*) = Im(f_*)$. Consider a diagram

$$\begin{array}{ccccc} M_i & \xrightarrow{f_i} & N_i & \xrightarrow{g_i} & L_i \\ \downarrow{\scriptstyle \pi_i} & & \downarrow{\scriptstyle \theta_i} & & \downarrow{\scriptstyle \sigma_i} \\ M_* & \xrightarrow{f_*} & N_* & \xrightarrow{g_*} & L_* \end{array} \tag{4.7.10}$$

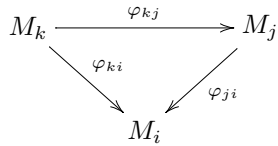
which is commutative by the previous theorem. If $m \in M_*$, then $\pi_i m_i = m$ for some $i \in I$, and so $g_* f_* m = g_* f_* \pi_i m_i = \sigma_i g_i f_i m_i = 0$. Let $n \in Ker(g_*)$. Then $n = \theta_i n_i$ for some $n_i \in N_i$. So $\sigma_i g_i n_i = g_* \theta_i n_i = g_* n = 0$. Therefore there exists $j \geq i$ such that $\sigma_{ij} g_i n_i = 0$ and so $g_j \theta_{ij} n_i = \sigma_{ij} g_i n_i = 0$. Since $Ker(g_j) = Im(f_j)$, there is $m_j \in M_j$ such that $f_j m_j = \theta_{ij} n_i$. If we set $m = \pi_j m_j$, then $f_* m = f_* \pi_j m_j = \theta_j f_j m_j = \theta_j \theta_{ij} n_i = \theta_i n_i = n$, i.e., $n \in Im(f_*)$. Hence, the sequence (4.7.9) is exact.

In a dual way we can define a notion of an inverse limit.

Let I be a partially ordered set, and let $\{M_i : i \in I\}$ be a set of modules and for any pair of indexes $i, j \in I$, where $i \leq j$, there is given a homomorphism $\varphi_{ji} : M_j \to M_i$ such that for all $i \leq j \leq k$ and $n \in I$:

(1) $\varphi_{nn} : M_n \to M_n$ is the identity on M_n;

(2) $\varphi_{ki} = \varphi_{ji}\varphi_{kj}$, i.e., the diagram



(4.7.11)

commutes.

In this case the triple

$$\mathbf{M} = \{(I, \leq); \{M_i \mid i \in I\}; \{\varphi_{ij} \mid i \leq j \in I\}\} \tag{4.7.12}$$

is called an **inverse system** of right A-modules.

So suppose we have an inverse system (4.7.12) of right A-modules. Set $M = \prod_i M_i$, where $M_i \in \mathbf{M}$. Let π_i be the system of canonical projections. Consider the submodule N of M which is generated by all elements $m \in M$ such that

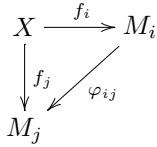
$$\pi_i(m) = \varphi_{ji}(\pi_j(m)) \tag{4.7.13}$$

whenever $i \leq j$. The submodule N is called the **inverse limit** of the inverse system $\mathbf{M}$ and it is denoted by $\varprojlim M_i$. When we write elements of M as $m = (m_i)_{i \in I}$, then condition (4.7.13) takes the form $m_i = \varphi_{ji}(m_j)$.

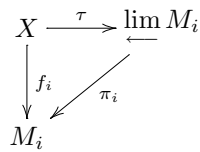
Exactly like the direct limit, the inverse limit has a universal property, which determines it uniquely up to isomorphism.

Theorem 4.7.4. *The inverse limit $\varprojlim M_i$ of an inverse system $\mathbf{M}$ has the following property:*

For any module X and any family of homomorphisms $f_i : X \to M_i$ such that all diagrams for $i \leq j$



commute, there exists a unique homomorphism $\tau : X \longrightarrow \varprojlim M_i$ such that all diagrams



commute. The module $\varprojlim M_i$ with homomorphisms π_i is determined uniquely up to isomorphism.

Proposition 4.7.5. *If F is a left exact functor that preserves direct products, then F preserves inverse limits.*

Proof. Let F be a left exact functor from the category of A-modules to the category of B-modules, which preserves direct products of modules. Let $C = \varprojlim M_i$ be the inverse limit of the inverse system $\mathbf{M}$ with the family of homomorphisms $\pi_i : M \to M_i$ such that for each $\varphi_{ij} : M_i \to M_j$ all diagrams

$$\begin{array}{ccc} C & \xrightarrow{\pi_i} & M_i \\ & \searrow^{\pi_j} & \downarrow{\scriptstyle \varphi_{ij}} \\ & & M_j \end{array}$$

commute, i.e., $\varphi_{ij}\pi_i = \pi_j$. Applying the functor F to these diagrams we obtain that $F(\varphi_{ij})F(\pi_i) = F(\pi_j)$.

Let D be a B-module with the family of homomorphisms $f_i : D \to F(M_i)$ such that all diagrams

$$\begin{array}{ccc} D & \xrightarrow{f_i} & F(M_i) \\ & \searrow^{f_j} & \downarrow{\scriptstyle F(\varphi_{ij})} \\ & & F(M_j) \end{array}$$

are commutative.

Since the functor F preserves direct products, i.e., $F(\prod_{i\in I} M_i)$ is naturally equivalent to $\prod_{i\in I} F(M_i)$, by the universal property of direct products (proposition 4.2.3), there exists a unique homomorphism

$$\psi : D \to F(\prod_{i\in I} M_i)$$

such that all diagrams

$$\begin{array}{ccc} D & & \\ \downarrow{\scriptstyle \varphi} & \searrow^{f_i} & \\ F(\prod_{i\in I} M_i) & \xrightarrow{F(p_i)} & F(M_i) \end{array}$$

are commutative, i.e., $F(p_i)\psi = f_i$, where the $p_i : \prod_{i\in I} M_i \to M_i$ are the canonical projections. Since C is a submodule of $\prod_{i\in I} M_i$, there exists a monomorphism $\alpha : C \to \prod_{i\in I} M_i$ such that $p_i\alpha = \pi_i$. Applying F we have $F(p_i)F(\alpha) = F(\pi_i)$

for all i. Since F is left exact, $F(\alpha)$ is also monomorphism and so there exists a homomorphism $g : D \to F(C)$ such that $F(\alpha)g = \psi$. Therefore $F(\pi_i)g = F(p_i)F(\alpha)g = F(p_i)\psi = f_i$. By the universal property of the inverse limit this means that $F(\varprojlim M_i) = F(C) = \varprojlim F(M_i)$.

Corollary 4.7.6. *For any A-module X the functor $Hom_A(X, *)$ preserves inverse limits.*

Proof. This follows from the facts that, by proposition 4.3.3, $Hom_A(X, *)$ is left exact and, by proposition 4.3.5, $Hom_A(X, *)$ preserves direct products.

The following statement is dual to proposition 4.7.4 and we leave the proof of it as an exercise.

Proposition 4.7.7. *If F is a right exact functor that preserves direct sums, then F preserves direct limits.*

Corollary 4.7.8. *For any A-module X the functor $X \otimes_A *$ preserves direct limits.*

Proof. This follows from the facts that, by proposition 4.6.4, $X \otimes_A *$ is right exact and, by proposition 4.6.2, $X \otimes_A *$ preserves direct sums.

4.8 NOTES AND REFERENCES

The notion of a category was introduced by S.Eilenberg and S.MacLane in the paper *Natural isomorphisms in group theory // Proc. Nat. Sci. USA, 28, 1942, pp.537-547* (see also *S.Eilenberg and S.MacLane, General theory of natural equivalences // Trans. Amer. Math. Soc., 58, 1945, pp.231-294*). The notions of a functor and the functor Hom were introduced in these papers. The functor Hom was deeply studied by H.Cartan, S.Eilenberg in their book *Homological algebra, Princeton Univ. Press., Princeton, New Jersey, 1956.*

It is interesting to note that the fundamental notions of homological algebra (such as projective module and the functor Tor) arose in connection with the study of the behavior of modules over Dedekind rings with respect to the tensor product. These investigations were conducted by H.Cartan in 1948.

The first exact sequences appeared in the works of the famous topologist Witold Hurewicz. The notion of the tensor product of Abelian groups first appeared in the paper *H.Whitney, Tensor products of Abelian groups // Duke Math. J., 4, (1938), pp.495-528.*

The theory of adjoint functors was developed by D.Kan in his paper *Adjoint functors // Trans. Amer. Math. Soc., v.87 (1958), p.294-329*, where, in particular, proposition 4.6.3 was proved, which gives the connection between the functors Hom and the tensor product functor.

Homological methods have invaded much of abstract algebra, and especially

ring theory - both commutative and noncommutative - beginning with the 1950s. In fact, many of the standard concepts and results have been rephrased in homological language. The first time this theory was systematically presented in the book *H.Cartan, S.Eilenberg, Homological Algebra, Princeton Univ. Press., Princeton, New Jersey, 1956.*

For further reading on theory of categories and functors we recommend the following books: *S.MacLane, Homology, Springer-Verlag, 1963*; *S.MacLane, Categories for the working mathematician, Springer-Verlag, 1971*; *B.Mitchell, Theory of categories, Acad. Press, 1965.*

5. Projectives, injectives and flats

5.1. PROJECTIVE MODULES

Definition. A module P is called **projective** if for any epimorphism $\varphi : M \to N$ and for any homomorphism $\psi : P \to N$ there is a homomorphism $h : P \to M$ such that $\psi = \varphi h$. This means that any diagram of the form

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle \psi} & & \\ M & \xrightarrow{\varphi} & N & \longrightarrow & 0 \end{array} \tag{5.1.1}$$

with the bottom row exact can be completed to a commutative diagram

$$\begin{array}{ccccc} & & P & & \\ & \swarrow{\scriptstyle h} & \downarrow{\scriptstyle \psi} & & \\ M & \xrightarrow{\varphi} & N & \longrightarrow & 0 \end{array} \tag{5.1.2}$$

The definition of projective modules can be given in terms of exactness of the Hom functor.

Proposition 5.1.1. *An A-module P is projective if and only if $Hom_A(P, *)$ is an exact functor.*

Proof.

1. Let P be a projective A-module. Suppose we have an arbitrary exact sequence of A-modules:

$$0 \longrightarrow M_1 \xrightarrow{\varphi} M \xrightarrow{\psi} M_2 \longrightarrow 0 \tag{5.1.3}$$

Then by proposition 4.3.1 we have an exact sequence:

$$0 \longrightarrow Hom_A(P, M_1) \xrightarrow{\overline{\varphi}} Hom_A(P, M) \xrightarrow{\overline{\psi}} Hom_A(P, M_2) \tag{5.1.4}$$

where by definition $\overline{\psi}(g) = \psi g$ for any $g \in Hom_A(P, M)$. Since P is projective, for any homomorphism $f \in Hom_A(P, M_2)$ there exists $g \in Hom_A(P, M)$ such that $f = \psi g = \overline{\psi}(g)$, i.e., $\overline{\varphi}$ is an epimorphism and so $Hom_A(P, *)$ is exact.

2. Conversely, suppose $Hom_A(P, *)$ is an exact functor. Let $\varphi : M \to N$ be an epimorphism and $\psi : P \to N$ be an arbitrary homomorphism. Then we have the following diagram

$$\begin{array}{ccccccccc} & & & & & & P & & \\ & & & & & & \downarrow \psi & & \\ 0 & \longrightarrow & Ker\varphi & \longrightarrow & M & \xrightarrow{\varphi} & N & \longrightarrow & 0 \end{array}$$

with the bottom sequence exact.

Since $Hom_A(P, *)$ is exact, $\overline{\varphi} : Hom_A(P, M) \to Hom_A(P, N)$ is an epimorphism. Therefore there exists $h \in Hom_A(P, M)$ such that $\overline{\varphi}(h) = \psi$. Since, by definition, $\overline{\varphi}(h) = \varphi h$, $\psi = \varphi h$, i.e., P is projective.

An important example of projective modules is given by the following statement.

Proposition 5.1.2. *A free module F is projective.*

Proof. Let F be a free A-module with a free basis $\{f_i \in F \ : \ i \in I \}$, i.e., any element $f \in F$ can be uniquely written as a finite sum $f = \sum\limits_{i \in I} f_i a_i$ with $a_i \in A$.

Consider a diagram

$$\begin{array}{ccccc} & & F & & \\ & & \downarrow \psi & & \\ M & \xrightarrow{\varphi} & N & \longrightarrow & 0 \end{array}$$

with the bottom row exact.

Denote $\psi(f_i) = n_i \in N$. Since φ is an epimorphism, there exist elements $m_i \in M$ such that $\varphi(m_i) = n_i$. Define a map $h : F \to M$ by $h(f) = h(\sum f_i a_i) = \sum m_i a_i$. Clearly, the map h is well defined, since any element $f \in F$ can be written uniquely in this form. It is trivial to verify that h is a homomorphism. Clearly, $\psi = \varphi h$. The proposition is proved.

Remark. Note that the converse statement to proposition 5.1.2 is not true in the general case. There exist projective modules, which are not free. Some examples of such modules will be given below in this section.

From propositions 5.1.2 and 1.5.4 we have the following corollary.

Corollary 5.1.3. *Every module is isomorphic to a factor module of a projective module.*

Proposition 5.1.4. *A direct sum $P = \bigoplus\limits_{\alpha \in I} P_\alpha$ of modules P_α is a projective module if and only if each P_α is projective.*

Proof.

1. Let $P = \bigoplus_{\alpha\in I} P_\alpha$. For any $\alpha \in I$ there is the canonical inclusion $i_\alpha : P_\alpha \to P$ and the natural projection $\pi_\alpha : P \to P_\alpha$. Let P be a projective module and suppose that for some $\alpha \in I$ we have a homomorphism $\psi_\alpha : P_\alpha \to N$. Consider the commutative diagram

$$\begin{array}{ccccc} & & P & \xrightarrow{\pi_\alpha} & P_\alpha \\ & & \downarrow{\scriptstyle f_\alpha} & \swarrow{\scriptstyle \psi_\alpha} & \\ M & \xrightarrow{\varphi} & N & \longrightarrow & 0 \end{array}$$

with the bottom row exact where $f_\alpha = \psi_\alpha\pi_\alpha$. Since P is projective, there is a homomorphism $h_\alpha : P \to M$ such that $f_\alpha = \varphi h_\alpha$. Set $\bar{h}_\alpha = h_\alpha i_\alpha$. Since $\pi_\alpha i_\alpha = 1_{P_\alpha}$, $\varphi\bar{h}_\alpha = \varphi h_\alpha i_\alpha = f_\alpha i_\alpha = \psi_\alpha\pi_\alpha i_\alpha = \psi_\alpha$. Thus, P_α is projective.

2. Conversely, let each module P_α be projective and consider a diagram

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle \psi} & & \\ M & \xrightarrow{\varphi} & N & \longrightarrow & 0 \end{array}$$

with bottom row exact. For any $\alpha \in I$ define the homomorphism $\psi_\alpha : P_\alpha \to N$ by $\psi_\alpha = \psi i_\alpha$. Since P_α is projective, there exists a homomorphism $h_\alpha : P_\alpha \to M$ such that $\psi_\alpha = \varphi h_\alpha$. Then we can define a homomorphism $h : P \to M$ by $h(p) = \sum_{\alpha\in I} h_\alpha\pi_\alpha(p)$ for any $p \in P$. We shall show that $\psi = \varphi h$.

Since $\sum_{\alpha\in I} i_\alpha\pi_\alpha(p) = p$ for any $p \in P$, we have $\sum_{\alpha\in I} \psi_\alpha\pi_\alpha(p) = \sum_{\alpha\in I} \psi i_\alpha\pi_\alpha(p) = \psi \sum_{\alpha\in I} i_\alpha\pi_\alpha(p) = \psi(p)$. On the other hand, $\psi(p) = \sum_{\alpha\in I} \psi_\alpha\pi_\alpha(p) = \sum_{\alpha\in I} \varphi h_\alpha\pi_\alpha(p) = \varphi h(p)$. Therefore, P is projective.

Corollary 5.1.5. *Every direct summand of a projective module is projective.*

Remark. Now we can give some examples of projective modules which are not free.

1. Consider the ring $A = \mathbf{Z}_2 \oplus \mathbf{Z}_3$. By proposition 5.1.5, $\mathbf{Z}_2$ and $\mathbf{Z}_3$ are projective modules (over A). But they cannot be free A-modules, because a free A-module contains either an infinite number of elements or a finite number of k elements, where k is a multiply of six.

2. Consider the algebra $A = T_2(\mathbf{R})$ of upper triangular matrices of order 2 over the field of real numbers. Let $P = e_{22}A$, where $e_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. By proposition 5.1.4, the module P is projective but not free, since $dim_{\mathbf{R}} P = 1$ and $dim_{\mathbf{R}} A = 3$.

The following proposition gives another equivalent definition of a projective module.

Proposition 5.1.6. *Let A be a ring. For an A-module P the following statements are equivalent*:

1) *P is projective;*

2) *every short exact sequence $0 \longrightarrow N \longrightarrow M \xrightarrow{\pi} P \longrightarrow 0$ splits*

3) *P is a direct summand of a free A-module F.*

Proof.

1) $\Rightarrow$ 2). Let P be a projective module and consider a diagram

$$\begin{array}{ccccccccc} & & & & & & P & & \\ & & & & & & \downarrow{\scriptstyle 1_P} & & \\ 0 & \longrightarrow & N & \longrightarrow & M & \xrightarrow{\pi} & P & \longrightarrow & 0 \end{array}$$

where π is an epimorphism. Since P is projective, there exists a homomorphism $i : P \to M$ such that $\pi i = 1_P$. Then by proposition 4.2.1 $M \simeq P \oplus N$ and the sequence

$$0 \longrightarrow N \longrightarrow M \xrightarrow{\pi} P \longrightarrow 0$$

splits.

2) $\Rightarrow$ 3). By proposition 1.5.4, for an A-module P there exists a free A-module F such that the sequence $0 \longrightarrow Ker\pi \longrightarrow F \xrightarrow{\pi} P \longrightarrow 0$ is exact. Then, by hypothesis, it is split, i.e., $F \simeq P \oplus Ker\pi$. So, P is a direct summand of a free module.

2) $\Rightarrow$ 3). Since, by proposition 5.1.2, F is projective, from corollary 5.1.5 it follows that P is also projective.

Corollary 5.1.7. *Let A be a ring. For any idempotent $e = e^2 \in A$, eA is a projective A-module.*

Proof. Since eA is a direct summand of the free A-module $A = eA \oplus (1 - e)A$, it is projective.

Remark. It should be noted that proposition 5.1.4 is not true for infinite direct products, which are not direct sums. In general, the direct product of projective modules need not be projective. That can be seen from the following example, which first was considered by R.Baer. The direct product of countable infinite copies of $\mathbf{Z}$

$$M = \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z} \times ...$$

is not a projective $\mathbf{Z}$-module. Assume the $\mathbf{Z}$-module M to be projective. Then, by corollary 5.1.6, it is isomorphic to a direct summand of a free $\mathbf{Z}$-module F, i.e., $F \simeq M \oplus X$. Since F is a free Abelian group, M is also a free Abelian group, because subgroups of free Abelian groups are free. A contradiction will arise if we produce a non-free subgroup of M. One can prove that one such a subgroup is the set of all sequences of the form $(x_1, x_2, ..., x_n, ...)$, where for any $n \in \mathbf{N}$

there exists $m \in \mathbf{N}$ such that x_i divides 2^n for all $i > m$. (For a proof, see, for instance, *J.Rotman, Homological algebra, Academic Press, New York, 1979, p.122.* Another proof of this fact, which does not use the theorem about subgroups of free Abelian groups, is contained in the book *T.Y.Lam, Lectures on Modules and Rings, Springer-Verlag, 1998, p.22.*)

The following proposition gives a simple way to calculate radicals of projective modules.

Proposition 5.1.8. *Let A be a ring. If P is a nonzero projective A-module, then $radP = P \cdot radA \neq P$.*

Proof. Let P be an arbitrary projective A-module and $R = radA$. Then there exists a free A-module F such that we have a decomposition $F = P \oplus Q$. By proposition 3.4.3, $FR = radF \neq F$. Therefore $FR = radF = radP \oplus radQ = PR \oplus QR$, i.e., $radP = PR$. It remains to show that $radP \neq P$. If $PR = P$, then $P \subset FR$. Let x be a nonzero element of the module P and a free basis $\{f_i | i \in I\}$ of the module F be chosen in such a way that in the expression $x = \sum\limits_{i \in I} f_i a_i$ ($a_i \in A$) the number of nonzero coefficients a_i is minimal, say n, so that $a_i \neq 0$ for $i = 1, ..., n$. Since $F = P \oplus Q$, we have $f_i = p_i + q_i$ ($p_i \in P$, $q_i \in Q$, $i = 1, ..., n$). Then $p_i = \sum\limits_{j=1}^{n} f_j r_{ij}$, where $r_{ij} \in R$, since $P \subset FR$. We have $x = \sum\limits_{i=1}^{n} f_i a_i = \sum\limits_{i=1}^{n} p_i a_i + \sum\limits_{i=1}^{n} q_i a_i \in P$, hence $\sum\limits_{i=1}^{n} q_i a_i = 0$. So $x = \sum\limits_{i=1}^{n} p_i a_i = \sum\limits_{i=1}^{n} \sum\limits_{j=1}^{n} f_j r_{ij} a_i = \sum\limits_{i=1}^{n} f_i a_i$. Consequently, $a_1 = \sum\limits_{i=1}^{n} r_{i1} a_i$ and $(1 - r_{11}) a_1 = \sum\limits_{i=2}^{n} r_{i1} a_i$. Since $r_{11} \in R$, we conclude that $1 - r_{11}$ is invertible and $a_1 = \sum\limits_{i=2}^{n} a r_{i1} a_i$, where $a = (1 - r_{11})^{-1}$. Therefore $x = \sum\limits_{i=2}^{n} (f_i + f_1 a r_{i1}) a_i$. The system $\{f_1, f_2 + f_1 a r_{21}, ..., f_n + f_1 a r_{n1}\}$ is linearly independent over A and together with $\{f_i | i > n\}$ forms a basis of the module F such that in the decomposition of the element x with respect to this basis the number of nonzero coefficients is equal to $n - 1$. A contradiction.

Remark. Note that for an arbitrary module M this proposition is not true. But it is true, in particular, for modules over Artinian rings.

5.2. INJECTIVE MODULES

"Dual" to the notion of projectivity is that of injectivity. Under "duality" we mean "inverting all arrows" (maps) and interchanging "epimorphism" with "monomorphism".

Definition. A module Q is called **injective** if for any monomorphism φ :

$M \to N$ and for any homomorphism $\psi : M \to Q$ there exists a homomorphism $h : N \to Q$ such that $\psi = h\varphi$. This means that any diagram of the form

$$\begin{array}{ccccc} 0 & \longrightarrow & M & \xrightarrow{\varphi} & N \\ & & \downarrow{\scriptstyle \psi} & & \\ & & Q & & \end{array} \tag{5.2.1}$$

with the top row exact can be completed to a commutative diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & M & \xrightarrow{\varphi} & N \\ & & \downarrow{\scriptstyle \psi} & \swarrow{\scriptstyle h} & \\ & & Q & & \end{array} \tag{5.2.2}$$

The "duality" between the definitions of projective and injective modules implies that many statements for injective modules can be simply obtained by "inverting the arrows" in the theorems on projective modules. In this way we obtain immediately the following result, which gives an equivalent definition of injectivity in terms of exactness of the Hom functor.

Proposition 5.2.1. *An A-module Q is injective if and only if $Hom_A(*, Q)$ is an exact functor.*

Proposition 5.2.2. *A direct product $Q = \prod_{\alpha \in I} Q_\alpha$ of injective modules Q_α is injective if and only if each Q_α is injective.*

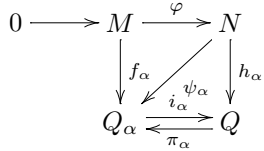
Proof.

1. Let $Q = \prod_{\alpha \in I} Q_\alpha$ be an injective module and consider a homomorphism $f_\alpha : M \to Q_\alpha$. Since Q is a direct product, for any $\alpha \in I$ there is the inclusion $i_\alpha : Q_\alpha \to Q$ and the projection $\pi_\alpha : Q \to Q_\alpha$ such that $\pi_\alpha i_\alpha = 1_{Q_\alpha}$. Consider a diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & M & \xrightarrow{\varphi} & N \\ & & \downarrow{\scriptstyle f_\alpha} & & \\ & & Q_\alpha & \xrightarrow{i_\alpha} & Q \end{array}$$

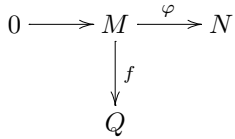
with the top row exact. Since Q is injective, there exists a homomorphism $h_\alpha : N \to Q$ such that $h_\alpha \varphi = i_\alpha f_\alpha$. Now define $\psi_\alpha : N \to Q_\alpha$ by $\psi_\alpha = \pi_\alpha h_\alpha$. Since

$\pi_\alpha i_\alpha = 1_{Q_\alpha}$, it follows that $\psi_\alpha\varphi = \pi_\alpha h_\alpha\varphi = \pi_\alpha i_\alpha f_\alpha = f_\alpha$, i.e., the diagram

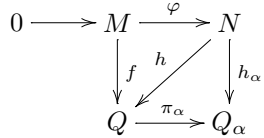


is commutative. Thus, Q_α is injective.

2. Conversely, let $Q = \prod_{\alpha\in I} Q_\alpha$. Suppose that each module Q_α is injective and consider a diagram



with the top row exact. For any $\alpha \in I$ there is the canonical inclusion $i_\alpha : Q_\alpha \to Q$ and the projection $\pi_\alpha : Q \to Q_\alpha$. So there are the homomorphisms $\pi_\alpha f : M \to Q_\alpha$. Since Q_α is injective, there exists a homomorphism $h_\alpha : N \to Q_\alpha$ such that $h_\alpha\varphi = \pi_\alpha f$. Now define a homomorphism $h : N \to Q$ by the formula $h(x) = \{h_\alpha(x)\}_{\alpha\in I}$ for any $n \in N$. We shall show that the diagram



is commutative, i.e., $f = h\varphi$.

Since Q is a direct product, for any $x \in N$ we have

$$h\varphi(x) = \{h_\alpha\varphi(x)\}_{\alpha\in I} = \{\pi_\alpha f(x)\}_{\alpha\in I} = f(x).$$

Hence, $f = h\varphi$ and Q is injective.

Remark. From proposition 5.2.2 it follows that a finite direct sum of injective modules is injective. However, in general this is not true for an infinite direct sum. There exist rings over which an infinite direct sum of injective modules need not to be injective. This fact follows, for example, from proposition 5.2.12 below and some examples of such rings will be presented in section 5.6.

As for projective modules we can easy prove the following proposition for injective modules.

Proposition 5.2.3. *Let A be a ring. If Q is an injective A-module then every exact sequence of A-modules*

$$0 \to Q \to M \to N \to 0$$

splits.

Proof. Let Q be an injective A-module and consider a diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & Q & \xrightarrow{i} & M & \longrightarrow & N \longrightarrow 0 \\ & & \downarrow{\scriptstyle 1_Q} & & & & \\ & & Q & & & & \end{array}$$

with exact top row so that i is a monomorphism. Since Q is injective, there exists a homomorphism $\pi : M \to Q$ such that $i\pi = 1_Q$. Then, by proposition 4.2.1, $M \simeq Q \oplus N$ and the sequence

$$0 \to Q \to M \to N \to 0$$

splits.

To prove the converse of this proposition we need to prove some dual statement to corollary 5.1.3 for injective modules, i.e., that every module is a submodule of an injective one. This is not so easy and it will be our goal for the next part of this section.

Let $M \subset N$ be A-modules and $f : M \to Q$ be any homomorphism of A-modules. An **extension** of f is a pair (L, g), where $M \subseteq L \subseteq N$, $g \in Hom_A(L, Q)$ with $g|_M = f$, where $g|_M$ is a restriction of g to M.

Proposition 5.2.4 (Baer's Criterion). *Let Q be a right module over a ring A. Then the following statements are all equivalent*:

1) *Q is injective*;

2) *for any right ideal $\mathcal{I} \subset A$ and each $f \in Hom_A(\mathcal{I}, Q)$ there exists an extension $\varphi \in Hom_A(A, Q)$ of f, i.e., $\varphi i = f$, where i is the natural embedding from $\mathcal{I}$ to A*;

3) *for any right ideal $\mathcal{I} \subset A$ and each $f \in Hom_A(\mathcal{I}, Q)$ there exists an element $q \in Q$ such that $f(a) = qa$, for all $a \in \mathcal{I}$.*

Proof.

1) $\Rightarrow$ 2). This follows immediately from the definition of injectivity, since a right ideal is just a submodule of A.

2) $\Rightarrow$ 3). Let i be the natural embedding from $\mathcal{I}$ to A and $f \in Hom_A(\mathcal{I}, Q)$, $\varphi \in Hom_A(A, Q)$ such that $f = \varphi i$. Since f, φ are A-homomorphisms, for any $a \in \mathcal{I}$ we have $f(a) = \varphi i(a) = \varphi(1 \cdot a) = \varphi(1)a = qa$,

where $q = \varphi(1) \in Q$.

3) $\Rightarrow$ 1). Let a module Q satisfy the given condition and consider a diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & M & \xrightarrow{\varphi} & N \\ & & \downarrow{\scriptstyle \psi} & & \\ & & Q & & \end{array}$$

with a given submodule M of a module N. Consider the set of extensions $\mathcal{X}$; i.e., the set of all pairs (C, h), where $M \subseteq C \subseteq N$ and $h : C \to Q$ such that $h|_C = \psi$.

Clearly, $\mathcal{X} \neq \emptyset$ because $(M, \psi) \in \mathcal{X}$. We introduce in $\mathcal{X}$ an ordering relation by setting $(C_1, h_1) \leq (C_2, h_2)$ if and only if $C_1 \subseteq C_2$ and h_2 extends h_1. One can easily verify that this relation is a partial order on $\mathcal{X}$. Every nonempty increasing chain $\{(C_i, h_i) \mid i \in I\}$ in $\mathcal{X}$ has an upper bound (C', h'), where $C' = \bigcup\limits_{i \in I} C_i$ and $h'|_{C_i} = h_i$. So, in view of Zorn's Lemma, there exists a maximal element (C^*, h^*) in $\mathcal{X}$. By construction $M \subseteq C^* \subseteq N$. The proof will be complete if we can show that $C^* = N$.

Suppose that there exists a nonzero element $b \in N$ and $b \notin C^*$. Set $\mathcal{I} = \{ a \in A \mid ba \in C^* \}$. Then $\mathcal{I}$ is a right ideal in A and there is a homomorphism $f : \mathcal{I} \to A$ given by $f(a) = h^*(ba)$. By assumption, there exists $q \in Q$ such that $f(a) = qa = h^*(ba)$ for all $a \in \mathcal{I}$. Therefore we can define a homomorphism $g : C^* + bA \to Q$ by setting $g(c + ba) = h^*(c) + qa$ for all $c \in C^*$ and $a \in A$. It extends the homomorphism h^* and it is well defined. Indeed, suppose $c_1 + ba_1 = c_2 + ba_2$ with $c_1, c_2 \in C^*$ and $a_1, a_2 \in A$. Then $b(a_1 - a_2) = c_2 - c_1 \in C^*$. So $a_1 - a_2 \in \mathcal{I}$ and hence $f(a_1 - a_2) = f(a_1) - f(a_2) = qa_1 - qa_2$. On the other hand, $f(a_1) - f(a_2) = h^*(ba_1) - h^*(ba_2) = h^*(ba_1 - ba_2) = h^*(c_2 - c_1) = h^*(c_2) - h^*(c_1)$. Hence, we have $h^*(c_2) - h^*(c_1) = qa_1 - qa_2$. Thus, $g(c_1 + ba_1) = h^*(c_1) + qa_1 = h^*(c_2) + qa_2 = g(c_2 + ba_2)$, as required.

Since $(C^*, h^*) \leq (C^* + bA, g)$, we obtain a contradiction with the maximality of (C^*, h^*). The proposition is proved.

One should note that injective modules were investigated long before the "dual" notion of projective modules was considered. Injective modules first appeared in the context of Abelian groups, in particular, divisible groups. Recall that an additive Abelian group G is said to be **divisible** if for any $g \in G$ and any nonzero $n \in \mathbf{Z}$ there exists a $g' \in G$ with $ng' = g$.

As we saw above every Abelian group can be considered as a $\mathbf{Z}$-module and every $\mathbf{Z}$-module is an Abelian group. Therefore we can say that $\mathbf{Z}$-module M is **divisible** if $nM = M$ for every nonzero $n \in \mathbf{Z}$.

Example 5.2.1.
The additive group of the field of rational numbers $\mathbf{Q}$ is a divisible group.

Example 5.2.2.
The group $\mathbf{Q}/\mathbf{Z}$ of rational numbers modulo 1 is a divisible group. This group is isomorphic to the multiplicative group of roots of unity.

It is easy to show that a direct product and direct sum of divisible groups is a divisible group and that a quotient group of a divisible group is also divisible.

Proposition 5.2.5. *A $\mathbf{Z}$-module Q is injective if and only if it is divisible.*

Proof. Let a $\mathbf{Z}$-module Q be injective. Consider an ideal $\mathcal{I}$ in $\mathbf{Z}$. Since all

ideals in $\mathbf{Z}$ are principal, $\mathcal{I} = n\mathbf{Z}$ for some $n \in \mathbf{Z}$. Let q be an arbitrary element of Q and consider the $\mathbf{Z}$-homomorphism $f : n\mathbf{Z} \to Q$ defined by setting $f(nm) = qm$ for any $m \in \mathbf{Z}$. Since Q is injective, there exists a $\mathbf{Z}$-homomorphism $h : \mathbf{Z} \to Q$ extending f. Then we have $q = f(n) = h(n) = nh(1) = nq' \in nQ$. It follows that $Q = nQ$, i.e., Q is divisible.

Conversely, let Q be a divisible $\mathbf{Z}$-module and consider an arbitrary ideal $n\mathbf{Z}$ in $\mathbf{Z}$. Consider a diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & n\mathbf{Z} & \xrightarrow{\ i\ } & \mathbf{Z} \\ & & \downarrow{\scriptstyle f} & & \\ & & Q & & \end{array}$$

Put $f(n) = q \in Q$. Since Q is divisible, there is $q' \in Q$ such that $q = nq'$. Define a $\mathbf{Z}$-homomorphism $h : \mathbf{Z} \to Q$ by $h(m) = q'm$ for any $m \in \mathbf{Z}$. Since $h(nm) = nh(m) = nq'm = qm = f(nm)$, it follows that h extends f. Therefore, by theorem 5.2.4, Q is injective.

So examples 5.2.1, 5.2.2 give us examples of injective $\mathbf{Z}$-modules.

Proposition 5.2.6. *Every* $\mathbf{Z}$*-module is a submodule of a divisible module.*

Proof. Let M be a $\mathbf{Z}$-module. Then M is isomorphic to a factor module of some free $\mathbf{Z}$-module F. Suppose $M \simeq F/L$, where L is a submodule in F. Let $F = \bigoplus\limits_{i \in I} \mathbf{Z}$ and $D = \bigoplus\limits_{i \in I} \mathbf{Q}$, then $F/L \subset D/L$. Since D and D/L are divisible groups, the proposition follows from proposition 5.2.5.

Let A be a ring and let D be an Abelian group. Since any ring A can be considered as both a right A-module and a left $\mathbf{Z}$-module, the Abelian group $Hom_{\mathbf{Z}}(A, D)$ can be made into a right A-module if we set $(fa)(x) = f(ax)$ for any $a, x \in A$ and $f \in Hom_{\mathbf{Z}}(A, D)$.

Lemma 5.2.7. *If* A *is a ring and* D *is a divisible* $\mathbf{Z}$*-module, then* $H = Hom_{\mathbf{Z}}(A, D)$ *is an injective right* A*-module.*

Proof. Let D be a divisible $\mathbf{Z}$-module and $H = Hom_{\mathbf{Z}}(A, D)$. By proposition 5.2.1, it suffices to show that $Hom_A(*, H)$ is exact. Let $0 \to M \to N \to L \to 0$ be an arbitrary short exact sequence of right A-modules. Since D is divisible, by proposition 5.2.5, D is an injective $\mathbf{Z}$-module. Therefore, by proposition 5.2.1, we have an exact sequence

$$0 \to Hom_{\mathbf{Z}}(L, D) \to Hom_{\mathbf{Z}}(N, D) \to Hom_{\mathbf{Z}}(M, D) \to 0$$

or

$$0 \to Hom_{\mathbf{Z}}(L \otimes_A A, D) \to Hom_{\mathbf{Z}}(N \otimes_A A, D) \to$$
$$Hom_{\mathbf{Z}}(M \otimes_A A, D) \to 0$$

by proposition 4.5.4. Then the adjoint isomorphism (proposition 4.6.3) gives an exact sequence:

$$0 \to Hom_A(L, H) \to Hom_A(N, H) \to Hom_A(M, H) \to 0$$

which shows exactness of $Hom_A(*, H)$.

Theorem 5.2.8 (Baer's Theorem). *Every module is a submodule of an injective module.*

Proof. Let M be a right A-module. It can also be considered as a left $\mathbf{Z}$-module and, by proposition 1.5.4, $M \simeq F/L$, where F is a free $\mathbf{Z}$-module and L is a submodule. By proposition 1.5.3, $F \simeq F_1 = \sum\limits_{i \in I} {}_{\mathbf{Z}}\mathbf{Z}$. Write $E = \sum\limits_{i \in I} {}_{\mathbf{Z}}\mathbf{Q}$, then $F_1 \subset E$ and $F_1/L \subset E/L$. Since direct sums and quotient groups of divisible groups are divisible, E/L is also a divisible group and, by proposition 5.2.5, E/L is an injective group. So we have $M \simeq F_1/L \subset D$, where D is an injective Abelian group. Thus, we have an exact sequence of left $\mathbf{Z}$-modules

$$0 \longrightarrow M \longrightarrow D \longrightarrow D/M \longrightarrow 0$$

and, in view of proposition 4.3.1, the sequence

$$0 \longrightarrow Hom_{\mathbf{Z}}(A, M) \longrightarrow Hom_{\mathbf{Z}}(A, D) \longrightarrow Hom_{\mathbf{Z}}(A, D/M)$$

is also exact. So we have an inclusion

$$Hom_{\mathbf{Z}}(A, M) \subseteq Hom_{\mathbf{Z}}(A, D)$$

where $Hom_{\mathbf{Z}}(A, D)$ is an injective right A-module, by proposition 5.2.7.

For any $m \in M$ there exists a group homomorphism $f_m : A \to M$ given by $f_m(a) = ma$ for any $a \in A$. Let $h : A \to M$ be an arbitrary A-homomorphism, then there is an element $m \in M$ such that $h(1) = m$ and $h(a) = ma$ for any $a \in A$. Therefore we can consider a map $\varphi : Hom_A(A, M) \to Hom_{\mathbf{Z}}(A, M)$ given by $\varphi(h)(a) = f_m(a)$, for any $h \in Hom_A(A, M)$ and $a \in A$. Obviously, it is an A-homomorphism. We shall show that φ is a monomorphism. Suppose, $\varphi(h)(a) = 0 = ma$ for any $a \in A$. Since $h(1) = m$, for any $a \in A$ we have $h(a) = ma = 0$. Hence, $h = 0$, i.e., φ is a monomorphism.

Finally, since there exists a natural isomorphism of right A-modules M and $Hom_A(A, M)$ given by $m \mapsto f_m$, where $f_m(1) = m$, we have a sequence of inclusions of A-modules

$$M \simeq Hom_A(A, M) \subseteq Hom_{\mathbf{Z}}(A, M) \subseteq Hom_{\mathbf{Z}}(A, D)$$

with an injective right A-module $Hom_{\mathbf{Z}}(A, D)$. So we obtain an exact sequence $0 \to M \to Hom_{\mathbf{Z}}(A, D)$. The proposition is proved.

Corollary 5.2.9. *A module Q is injective if and only if any exact sequence of the form*

$$0 \to Q \to M \to N \to 0 \tag{4.3.3}$$

splits.

Proof. The first part of this statement was proved in proposition 5.2.3.

Conversely, let Q be an arbitrary A-module. By proposition 5.2.8, there exists an injective module M which contains the module Q, that is, we have an exact sequence

$$0 \to Q \to M \to M/Q \to 0$$

which is split by hypothesis. So $M \simeq Q \oplus M/Q$. Then, by proposition 5.2.2, Q is injective.

Corollary 5.2.10. *A module Q is injective if and only if it is a direct summand of every module which contains it.*

Proof. Assume Q is injective and Q is a submodule of a module M, then we have an exact sequence

$$0 \to Q \to M \to M/Q \to 0$$

which, in view of corollary 5.2.9, splits. Then Q is a direct summand of M.

Conversely, let Q be an arbitrary A-module, then, by proposition 5.2.8, there exists an injective module M containing Q. Then, by hypothesis, Q is a direct summand of M and from proposition 5.2.2 it follows that Q is injective.

In this section we have considered only divisible $\mathbf{Z}$-modules and their connection with injective modules. As has been shown divisible $\mathbf{Z}$-modules are really injective modules. The notion of divisibility can be generalized to modules over an arbitrary ring.

Definition. An element a of a ring A is called **regular** if $xa \neq 0$ and $ax \neq 0$ for any nonzero element $x \in A$.

Definition. A right A-module M is called **divisible**, if $Ma = M$ for any regular element $a \in A$.

Proposition 5.2.11. *Any injective right A-module is divisible.*

Proof. Let m be an arbitrary nonzero element of a right A-module M and let a be a left nonzero divisor of a ring A. Then there is a homomorphism $f : aA \to M$ given by $f(a) = m$. Since M is injective, by Baer's Criterion (proposition 5.2.4) applied to the homomorphism f, there exists an element $m' \in M$ such that $f(a) = m'a$. Therefore $m = m'a$, i.e., M is a divisible module.

Remark. For some rings the statement inverse to proposition 5.2.11 is true, i.e., divisible implies injective. Examples of such rings are principal ideal domains, as will be shown in chapter 8. But in general this inverse statement is not true.

The following result shows, in particular, that an infinite direct sum of injective modules need not to be injective for an arbitrary ring.

Theorem 5.2.12 (H.Bass, Z.Papp). *A ring A is right Noetherian if and only if every direct sum of injective right A-modules is injective.*

Proof. Suppose A is right Noetherian and $\mathcal{I}$ is a right ideal in A. Then, by proposition 3.1.5, $\mathcal{I}$ is finitely generated, that is, $\mathcal{I}$ has a finite set of generators $\{x_1, x_2, ..., x_n\}$ and any element $x \in \mathcal{I}$ can be written as $x = \sum_{i=1}^{n} x_i a_i$. Suppose $Q = \bigoplus_{j\in J} Q_j$, where the Q_j are injective right A-modules. Consider a homomorphism $\varphi : \mathcal{I} \to Q = \bigoplus_{j} Q_j$. For each generator x_i in $\mathcal{I}$ there are only finitely many j such that $\varphi(x_i)$ has its j-th component unequal to zero. As there are only finitely many x_i it follows that there is a finite subset $\mathcal{I}_0$ of $\mathcal{J}$ such that φ factors through $\bigoplus_{j\in\mathcal{J}_0} Q_j \overset{\sigma}{\subset} \bigoplus_{j\in\mathcal{J}} Q_j$ where σ is the obvious inclusion. Since $\bigoplus_{j\in\mathcal{J}_0} Q_j$ is injective, by proposition 5.2.2, for any diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathcal{I} & \xrightarrow{\theta} & A \\ & & \downarrow{\scriptstyle \varphi} & & \\ & & Q & & \end{array}$$

we can construct a commutative diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathcal{I} & \xrightarrow{\theta} & A \\ & & \downarrow{\scriptstyle \varphi} & \swarrow{\scriptstyle g} & \\ & & \bigoplus_{j\in\mathcal{J}_0} Q_j & & \\ & & \downarrow{\scriptstyle \sigma} & & \\ & & Q & & \end{array}$$

where $g\theta = \varphi$. Setting $g' = \sigma g$ we obtain, by proposition 5.2.4, that Q is injective.

Conversely, suppose $Q = \bigoplus_{j\in J} Q_j$ is injective whenever the Q_j are injective right A-modules. Assume that A is not right Noetherian. Then there exists an infinite strictly ascending chain of right ideals: $\mathcal{I}_1 \subset \mathcal{I}_2 \subset ... \subset \mathcal{I}_n \subset ....$ Let $\mathcal{I} = \bigcup \mathcal{I}_n$. By theorem 5.2.8, for any n there exists an injective module Q_n such that the sequence $0 \to \mathcal{I}/\mathcal{I}_n \overset{\varphi_n}{\to} Q_n$ is exact. Then we can define $\varphi : \mathcal{I} \to Q$ by setting

$\varphi(x) = \oplus\varphi_n(x + \mathcal{I}_n)$ if $x \in \mathcal{I}$. Since $\mathcal{I} = \bigcup \mathcal{I}_n$, for any $x \in \mathcal{I}$ there exists n such that $x \in \mathcal{I}_n$. Therefore $\varphi_n(x + \mathcal{I}_n) = 0$ for all but finitely many n. So that $\varphi(x) \in \underset{n\in S}{\oplus} \varphi_n(x + \mathcal{I}_n) = Q'$, where S is a finite set. By corollary 5.2.10, Q' is injective. Then there exists a homomorphism $g : A \to Q'$ such that the following diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathcal{I} & \xrightarrow{\theta} & A \\ & & \downarrow{\scriptstyle \varphi} & \swarrow{\scriptstyle g} & \\ & & Q' & & \end{array}$$

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathcal{I} & \xrightarrow{\theta} & A \\ & & \downarrow \varphi & \swarrow g & \\ & & Q' & & \end{array}$$

is commutative. In this case $\varphi_n(x + \mathcal{I}_n) = g_n(x)$, where $g(x) = \oplus g_n(x)$. But now $\varphi_n(x + \mathcal{I}_n) = g_n(x) = xg_n(1)$, for $x \in \mathcal{I}_n$, implies that $g_n(1) \neq 0$, for all $n \in S$. Thus, $g(1) \notin Q'$. This contradiction shows that A is right Noetherian.

The structure and properties of semisimple rings have been considered in section 2.2. The following theorem gives a characterization of semisimple rings in terms of projective and injective modules.

Theorem 5.2.13. *For a ring A the following statements are equivalent:*
1. *A is a semisimple ring.*
2. *Any A-module M is projective.*
3. *Any A-module M is injective.*

Proof.

$1 \Longrightarrow 2$. Assume A is a semisimple ring. Then the right regular module A_A decomposes into a direct sum of simple submodules. Therefore any free right A-module F can also be decomposed into a direct sum of simple submodules, that means F is a semisimple A module. Let M be a right A-module. Then M is isomorphic to a quotient module of some free A-module F: $M \simeq F/K$, where K is a submodule of F. Since F is a semisimple A-module, by proposition 2.2.4, any submodule is a direct summand of F. Thus, $F = K \oplus N$, where $N \simeq M$. Then, by proposition 5.1.6, M is projective.

$2 \Longrightarrow 1$. Suppose that any A-module is projective. Let N be a submodule of a module M. Then, by hypothesis, the quotient module M/N is projective. Then in the exact sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

the module M/N is projective. Therefore, by proposition 5.1.6, this sequence splits, i.e., N is isomorphic to a direct summand of the module M. Therefore, by

proposition 2.2.4, M is a semisimple module. Since M is an arbitrary module, it follows that A is a semisimple ring.

$2 \Longrightarrow 3$. Assume that any A-module is projective. Let M be a right A-module. By Baer's Theorem, there exists an injective module Q containing M. Consider the exact sequence

$$0 \longrightarrow M \longrightarrow Q \longrightarrow Q/M \longrightarrow 0$$

where Q/M is projective by hypothesis. Then, by proposition 5.1.6, this sequence splits, i.e., M is isomorphic to a direct summand of the injective module Q. Therefore, by corollary 5.2.10, M is injective.

$3 \Longrightarrow 2$. Assume that any A-module is injective. Let M be a right A-module. By corollary 5.1.3, M is isomorphic to a quotient module of some projective module P. Consider the exact sequence

$$0 \longrightarrow M' \longrightarrow P \longrightarrow M \longrightarrow 0$$

where M' is injective, by hypothesis. Then, by corollary 5.2.9, this sequence splits, i.e., M is isomorphic to a direct summand of the projective module P. Therefore, by proposition 5.1.4, M is projective.

5.3. ESSENTIAL EXTENSIONS AND INJECTIVE HULLS

In the previous section it was shown that any module M can be embedded into an injective module. There may be many such injective modules for a given module M. The goal of this section is to show that among them there exists a minimal one. We shall prove that every module M has such a minimal injective module and we show that it is an essential extension of M, which is unique up to isomorphism.

Definition. If N is a submodule of a module M, we shall say that M is an **extension** of N. A submodule N of M is called **essential** (or **large**) in M if it has nonzero intersection with every nonzero submodule of M. We also say that M is an **essential extension** of N.

For example, any module is always an essential extension of itself. This essential extension is called **trivial**. Other essential extensions are called **proper**. The field of all rational numbers $\mathbf{Q}$ considered as a $\mathbf{Z}$-module is an essential extension of the integers $\mathbf{Z}$.

The next simple lemma gives a very useful test for essential extensions.

Lemma 5.3.1. *An A-module M is an essential extension of an A-module N if and only if for any $0 \neq x \in M$ there exists $a \in A$ such that $0 \neq xa \in N$.*

Proof. Let M be an essential extension of N and $0 \neq x \in M$, then $xA \cap N \neq 0$, that means there exists $a \in A$ such that $0 \neq xa \in N$.

Conversely, let $X \subseteq M$ and $0 \neq x \in M$. By hypothesis there exists $a \in A$ such that $0 \neq xa \in N$. Then $0 \neq xa \in N \cap X$, i.e., N is essential in M.

The following lemma shows that the relation of essential extension is transitive.

Lemma 5.3.2. *Let M be an A-module with submodules $K \subseteq N \subseteq M$, then M is an essential extension of K if and only if N is an essential extension of K and M is an essential extension of N.*

Proof. Let M be an essential extension of K and suppose $0 \neq X \subseteq M$, then $X \cap K \neq 0$. In particular, this is true if $X \subseteq N$, so N is an essential extension of K. Since $K \subseteq N$, we have $X \cap N \neq 0$. Therefore N is essential in M.

Conversely, let N be an essential extension of K and M be an essential extension of N. Suppose $X \subseteq M$, then $X \cap K = 0$ implies $X \cap N = 0$. But the last equality means that $X = 0$. So, M is an essential extension of K.

The connection between injectivity and essential extensions is given by the following theorem.

Theorem 5.3.3 (B.Eckmann, A.Schopf). *A module Q is injective if and only if it has no proper essential extensions.*

Proof. Let M be an injective module and let E be an essential extension of it. By proposition 5.2.10, M is a direct summand of E, i.e., $E = M \oplus N$, where $M \cap N = 0$. If $N \neq 0$, then E is not an essential extension, therefore $N = 0$ and $E = M$.

Conversely, suppose M has no proper essential extensions. By Baer's Theorem, there exists an injective module Q containing M. Consider the set W of all submodules S of Q with the property that $S \cap M = 0$. This set is not empty because $0 \in W$. It is a partially ordered set with respect to the relation of subset inclusion. Then, by Zorn's Lemma, there exists a maximal element in this set. Let $N \subset Q$ be maximal in the set W. Then $M \cap N = 0$ and $M + N \subseteq Q$. We shall show that $Q = M + N$. Suppose $M + N \neq Q$, then $M + N/N \subset Q/N$ and $M+N/N \neq Q/N$. Consider a nonzero submodule $0 \neq X/N \subset Q/N$. Then $N \subset X$ and $N \neq X$. Since N is a maximal element in W, we have $M \cap X \neq 0$. Now taking into account that $M \cap N = 0$ we obtain $M \cap X \not\subseteq N$. Therefore $N \subset X \cap (M+N)$, which means that $X/N \cap (M+N)/N \neq 0$ and so Q/N is an essential extension of $(M + N)/N$. In view of theorem 1.3.3, we have $M \simeq M/M \cap N \simeq (M + N)/N$. Hence M is essential in Q/N. Since, by hypothesis, M has no proper essential extensions, $Q/N = (M + N)/N$ and this implies $Q = M + N$. Since $M \cap N = 0$, we have $Q = M \oplus N$. Hence, by proposition 5.2.2, M is an injective module.

Definition. A module Q is called an **injective hull** or **injective envelope** of a module M if it is both an essential extension of M and an injective module.

Theorem 5.3.4. *Every module M has an injective hull, which is unique up to an isomorphism extending the identity of M.*

Proof. By Baer's Theorem there is an injective module Q containing a given

module M. Consider the set W of all essential extensions of M contained in the module Q. This set is not empty because $M \in W$ and, in view of lemma 5.3.2, it is a partially ordered set with respect to subset inclusion. We shall show that any increasing chain of modules contained in the set W has an upper bound in W. Let

$$M \subseteq E_1 \subseteq E_2 \subseteq ... \subseteq E_n \subseteq ... \subseteq Q$$

be a chain of modules $E_i \in W$. Let $E^* = \bigcup\limits_{i \in I} E_i$, then $M \subseteq E^* \subseteq Q$. If $0 \neq X \subset E^*$, then there is $i \in I$ such that $X \cap E_i \neq 0$ and therefore $(X \cap E_i) \cap M \neq 0$. Hence $X \cap M \neq 0$ and E^* is an essential extension of M, i.e., $E^* \in W$ and it is an upper bound of all E_i for $i \in I$. Therefore we can apply Zorn's lemma to the set W and conclude that there exists a maximal element E in W. We are going to show that E is an injective module. By theorem 5.3.3, it suffices to prove that E has no proper essential extensions.

Suppose that L is an essential extension of E. By construction E is a submodule of Q. Since Q is injective, the diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & E & \xrightarrow{i_L} & L \\ & & \downarrow{\scriptstyle i_Q} & & \\ & & Q & & \end{array}$$

with embeddings i_L and i_Q can be completed to a commutative diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & E & \xrightarrow{i_L} & L \\ & & \downarrow{\scriptstyle i_Q} & \swarrow{\scriptstyle h} & \\ & & Q & & \end{array}$$

Therefore $hi_L = i_Q$ and $Ker h \cap E = 0$. Since L is an essential extension of E, it follows that $Ker h = 0$, i.e., h is a monomorphism. Hence $\overline{L} = Im h \simeq L$ and $\overline{L}$ is an essential extension of E. Then, by lemma 5.3.2, $\overline{L}$ is also an essential extension of the module M. Thus, we have the sequence $M \subseteq E \subseteq \overline{L} \subseteq Q$ and owing to maximality of E we obtain that $E = \overline{L}$, i.e., $E = L$ and E has no proper essential extensions. By theorem 5.3.3, E is an injective module, i.e., E is an injective hull of M.

Now we shall prove the uniqueness of E up to isomorphism. Let E and $\overline{E}$ be two injective hulls of M. Since E and $\overline{E}$ are injective modules, there exists a homomorphism $\tau : \overline{E} \to E$ such that the diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & M & \longrightarrow & E \\ & & \| & & \downarrow{\scriptstyle \tau} \\ 0 & \longrightarrow & M & \longrightarrow & \overline{E} \end{array}$$

with exact top and bottom rows is commutative. Then $Ker\tau \cap M = 0$ and, since E is an essential extension of M, $Ker\tau = 0$, i.e., τ is a monomorphism. So $E \simeq Im\tau \subseteq \overline{E}$ and from the injectivity of E, by proposition 5.2.10, it follows $\overline{E} = Im\tau \oplus N$. Since $M \subseteq Im\tau$, we have $M \cap N = 0$ and, since $\overline{E}$ is an essential extension of M, it follows that $N = 0$. Thus $Im\tau \simeq \overline{E}$, that means τ is an epimorphism and therefore τ is an isomorphism extending the identity 1_M of M. The theorem is proved.

We shall say that E is a **maximal essential extension** of a module M if no module properly containing E can be an essential extension of M. We shall also say that a module Q is **minimal injective** over M if no module properly contained in Q and properly containing M can be injective.

Theorem 5.3.5. *If N is a submodule of a module M, then the following conditions are equivalent:*

(1) *M is a maximal essential extension of N.*

(2) *M is both an essential extension of N and an injective module.*

(3) *M is minimal injective over N.*

Proof.

(1) $\Longrightarrow$ (2). By lemma 5.3.2, hypothesis (1) means that M has no proper essential extensions. Therefore, by theorem 5.3.3, M is injective.

(2) $\Longrightarrow$ (3). Let $N \subseteq Q \subseteq M$ where Q is an injective module. Then, by corollary 5.2.10, $M = Q \oplus L$. Since $N \subseteq Q$, we obtain that $N \cap L = 0$. Because M is an essential extension of N, $L = 0$, and so $Q = M$.

(3) $\Longrightarrow$ (1). Suppose M is minimal injective over N. From the proof of theorem 5.3.4 there exists a module $E \subseteq M$, which is a maximal essential extension of N. Then E is an injective module and from the minimality of M it follows that $E = M$.

Remark. We shall use the notation $E(M)$ for an injective hull of a module M. It is unique up to isomorphism and thus $E(M)$ denotes any injective hull of M.

The following proposition yields some other important properties of injective hulls which will be needed in the sequel.

Proposition 5.3.6.

(1) *$E(M_1 \oplus M_2) \simeq E(M_1) \oplus E(M_2)$ for any A-modules M_1, M_2.*

(2) *If $\varphi : M \to Q$ is a monomorphism and Q is an injective module, then $Q = Q_1 \oplus Q_2$, where $Q_1 \simeq E(M)$.*

Proof.

(1). Since, by proposition 5.2.2, $E = E(M_1) \oplus E(M_2)$ is an injective module, to prove statement (1) it suffices to prove that E is an essential extension of the

module $M = M_1 \oplus M_2$.

Let $x = e_1 + e_2$ be an arbitrary nonzero element of E, where $e_i \in E(M_i)$, $i = 1, 2$. By lemma 5.3.1, there exists an element $a_1 \in A$ such that $0 \neq e_1 a_1 \in M_1$. Consider the element $xa_1 = e_1 a_1 + e_2 a_1$. If $e_2 a_1 = 0$, then $0 \neq xa_1 = e_1 a_1 \in M$ and the statement follows from lemma 5.3.1. Suppose $e_2 a_1 \neq 0$. Then by the same lemma there exists an element $a_2 \in A$ such that $0 \neq (e_2 a_1)a_2 \in M_2$. Hence, $0 \neq xa_1 a_2 = e_1 a_1 a_2 + e_2 a_1 a_2 \in M$ and from lemma 5.3.1 it follows that E is an essential extension of M.

(2). Consider a diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & M & \xrightarrow{i_M} & E(M) \\ & & \downarrow{\scriptstyle \varphi} & & \\ & & Q & & \end{array}$$

with the top row exact, a monomorphism φ and the canonical embedding i_M. Since Q is an injective module, there exists a homomorphism τ extending i_M, which makes the following diagram commutative

$$\begin{array}{ccccc} 0 & \longrightarrow & M & \xrightarrow{i_M} & E(M) \\ & & \downarrow{\scriptstyle \varphi} & \swarrow{\scriptstyle \tau} & \\ & & Q & & \end{array}$$

Assume τ is not a monomorphism, i.e., $Ker\tau \neq 0$. Then $Ker\tau \cap M = 0$, since $\tau i_M = \varphi$ and φ, i_M are monomorphisms. But this contradicts the fact that $E(M)$ is an essential extension of the module M. So, we obtain that τ is a monomorphism. By corollary 5.2.10, $E(M)$ is isomorphic to a direct summand of the module Q, i.e., $Q = Q_1 \oplus Q_2$, where $Q_1 \simeq E(M)$.

Definition. Let M be a right A-module. The **socle** of M, denoted by $\mathrm{soc}(M)$, is the sum of all simple right submodules of M. If there are no such submodules, then $\mathrm{soc}(M) = 0$.

If $M = A_A$, then $\mathrm{soc}(A_A)$ is the sum of all minimal right ideals of A and it is a right ideal of A. If $\mathcal{I}$ is a minimal right ideal in A, then for any $x \in A$ either $x\mathcal{I} = 0$ or $x\mathcal{I}$ is a minimal right ideal, and in both cases $x\mathcal{I} \subset \mathrm{soc}(A_A)$. Therefore $\mathrm{soc}(A_A)$ is an ideal in A. Analogously we can consider $\mathrm{soc}({}_A A)$. However these two socles do not coincide in general. As an example we can consider the ring of all upper triangular 2×2 matrices over a field k.

For a semisimple module M we have $\mathrm{soc}(M) = M$.

Since a homomorphic image of a simple module is a simple module or zero, for any A-homomorphism $\varphi : M \to N$ of A-modules M, N, we have that $\varphi(\mathrm{soc}(M)) \subseteq \mathrm{soc}(N)$.

Proposition 5.3.7. *If M is an A-module, then $E(M) = E(\mathrm{soc}(M))$.*

Proof. Since $\mathrm{soc}(M)$ is the sum of all simple submodules of a module M, for any submodule $X \subseteq M$, we have $X \cap \mathrm{soc}(M) \neq 0$, that means $\mathrm{soc}(M)$ is essential in M. Since $E(M)$ is an essential extension of M, by lemma 5.3.2, $E(M)$ is also an essential extension of $\mathrm{soc}(M)$. Taking into account that $E(M)$ is an injective module completes the proof of the proposition.

Slightly more categorically, the notion of an essential extension can be reformulated as: "An essential monomorphism is a monomorphism $f : N \to M$ such that for each sequence of A-modules

$$N \xrightarrow{f} M \xrightarrow{g} X$$

with gf a monomorphism, g is a monomorphism.

The dual notion is that of an essential epimorphism (surjective homomorphism in the case of modules). An epimorphism $f : N \to M$ is an essential epimorphism if for each sequence of A-modules

$$X \xrightarrow{g} M \xrightarrow{f} N$$

such that fg is surjective, g is surjective.

Definition. A **projective cover** of a module M is a projective module P together with an essential epimorphism $P \to M$.

Proposition 5.3.8. *Projective covers are unique up to isomorphism (assuming there are any). In other words, if $P \xrightarrow{f} M$, $P' \xrightarrow{f'} M$ are two projective covers then there is an isomorphism $\varphi : P \to P'$ such that $f'\varphi = f$.*

The notion of a projective cover is the dual of an injective hull. However, unlike injective hulls, which always exist (the Baer theorem), projective covers do not always exist. For instance the $\mathbf{Z}$-module $\mathbf{Z}/(2)$ has no projective cover.[1])

Definition. A ring A is called **semiperfect** if $A/rad(A)$ is a semisimple ring and if moreover every idempotent in $A/rad(A)$ lifts to an idempotent in A.

Proposition 5.3.9. *Let A be a semiperfect ring. Then every finitely generated right (left) A-module has a right (left) projective cover.*[2])

For more on projective covers and semiperfect rings see chapter 10 below, especially section 10.4.

---

[1]) This is an illustration of the fact that not everything in a category of A-modules dualizes.

[2]) This also goes the other way. If every finitely generated right A-module has a projective cover, the ring A is a semiperfect (see *H.Bass, Finitistic dimension and a homological generalization of semi-primary rings // Trans. Amer. Math. Soc. v.95 (1960), p.466-488*).

5.4. FLAT MODULES

Definition. An A-module X is called **flat** if $X \otimes_A *$ is an exact functor.

In view of proposition 4.6.4, X is flat if and only if $1_X \otimes f$ is a monomorphism whenever f is a monomorphism.

Proposition 5.4.1. *If A is a ring, then the regular module A_A is flat.*

Proof. This follows immediately from proposition 4.5.4.

Proposition 5.4.2. *A direct sum $B = \underset{\alpha\in I}{\oplus} B_\alpha$ of modules B_α is a flat module if and only if each B_α is flat.*

Proof. Let $B = \underset{\alpha\in I}{\oplus} B_\alpha$. Consider an exact sequence of left A-modules: $0 \longrightarrow M \xrightarrow{f} N$. Then, by proposition 4.6.2, we have a commutative diagram

$$\begin{array}{ccc} \underset{\alpha\in I}{\oplus} B_\alpha \otimes_A M & \xrightarrow{1\otimes f} & \underset{\alpha\in I}{\oplus} B_\alpha \otimes_A N \\ \downarrow \varphi & & \downarrow \psi \\ \oplus(B_\alpha \otimes M) & \xrightarrow{\oplus(1_{B_\alpha}\otimes f_\alpha)} & \oplus(B_\alpha \otimes N) \end{array}$$

where φ and ψ are natural isomorphism determined by $\varphi[(\sum b_\alpha)\otimes m] = \sum(b_\alpha \otimes m)$ and $\psi[(\sum b_\alpha) \otimes n] = \sum(b_\alpha \otimes n)$ for any $m \in M$ and $n \in N$. Therefore $1 \otimes f$ is a monomorphism if and only if each $1_{B_\alpha} \otimes f_\alpha$ is a monomorphism, that is, B is flat if and only if each B_α is flat.

Corollary 5.4.3. *Every direct summand of a flat module is flat.*

Corollary 5.4.4. *Every free module is flat.*

Proof. Since, by proposition 5.4.1, A is flat, then from proposition 5.4.2 it follows that every free module is flat.

Corollary 5.4.5. *Every projective module is flat.*

Proof. This follows from corollary 5.4.4, since every projective module is a direct summand of a free module.

Remark. Note that the converse to 5.4.4 and 5.4.5 [3]) need not be true: there are flat modules that are neither free nor projective. For example, if $A = \mathbf{Z}$ then the

[3]) The converse to 5.4.5 is true only for a special class of rings which are perfect rings. One of the equivalent definitions says that a ring A is called right perfect if every right A-module has a projective cover (see *H.Bass, Finitistic dimension and a homological generalization of semi-primary rings // Trans. Amer. Math. Soc. v.95 (1960), p.466-488*). For more on perfect rings see section 10.5 below.

$\mathbf{Z}$-module $\mathbf{Q}$ is flat but it is not projective. If $A = \mathbf{Z}_{(p)} = \{\frac{m}{n} \in \mathbf{Q} \ : \ (n,p) = 1\}$, where p is prime, then the $\mathbf{Z}_{(p)}$-module $\mathbf{Q}$ is flat but it is not projective.

Proposition 5.4.6. *Let* $\mathbf{M} = \{\{I, \leq\}; \{M_i \mid i \in I\}; \{\varphi_{ij} \mid i \leq j \in I\}\}$ *be a directed system of right* A*-modules. If each* M_i *is flat, then* $\varinjlim M_i$ *is also flat.*

Proof. Let X be a left A-module. Consider the submodule N, which is generated by elements $m_i - \varphi_{ij}m_i$ for $i \leq j$, as in the construction of $\varinjlim M_i$, and the corresponding submodule N_0, for the construction of $\varinjlim(M_i \otimes X)$. Then it is easy to verify, that the map $\varphi : \varinjlim M_i \otimes X \to \varinjlim(M_i \otimes X)$ given by $\varphi((\sum m_i + N) \otimes x) = \sum m_i \otimes x + N_0$ is an isomorphism. Consider an exact sequence $0 \to X \xrightarrow{f} Y$ of left A-modules. Then we have the commutative diagram

$$\begin{array}{ccc} \varinjlim M_i \otimes X & \xrightarrow{1 \otimes f} & \varinjlim M_i \otimes Y \\ \downarrow \varphi & & \downarrow \psi \\ \varinjlim(M_i \otimes X) & \xrightarrow{\varinjlim(1_{M_i} \otimes f)} & \varinjlim(M_i \otimes Y) \end{array}$$

where φ and ψ are isomorphisms. By corollary 4.7.8, $1 \otimes f$ is a monomorphism because each $1_{M_i} \otimes f$ is. Therefore $\varinjlim M_i$ is flat.

Corollary 5.4.7. *If every finitely generated submodule of* M *is flat, then* M *is flat.*

Proof. We obtain this statement from the previous proposition, taking into account that every module is the direct limit of its finitely generated submodules.

To establish a connection between flat modules and injectives we introduce the following very important definition.

Definition. If M is a right A-module, then the left A-module $B^* = Hom_{\mathbf{Z}}(M, \mathbf{Q}/\mathbf{Z})$, is called its **character module**, where the action of A is defined by $(af)m = f(ma)$, for all $a \in A$ and $m \in M$.

Lemma 5.4.8. *For any Abelian group* G *with a given element* $0 \neq x \in G$ *there exists a group homomorphism* $f : G \to \mathbf{Q}/\mathbf{Z}$ *such that* $f(x) \neq 0$.

Proof. Let $0 \neq x \in G$ and $\mathbf{Z}x$ be a cyclic subgroup of G generated by x. Since for any $0 \neq n \in \mathbf{N}$ the quotient group $\mathbf{Q}/\mathbf{Z}$ contains an element of order n, namely $1/n + \mathbf{Z}$, there exists a homomorphism $h : \mathbf{Z}x \to \mathbf{Q}/\mathbf{Z}$ with $hx \neq 0$. Since $\mathbf{Q}/\mathbf{Z}$ is injective, h can be extended to a homomorphism $f : G \to \mathbf{Q}/\mathbf{Z}$ such that $f(x) \neq 0$.

The next lemma gives a simple criterion for exactness of sequences in terms of character modules.

Lemma 5.4.9. *A sequence of right A-modules*

$$M \xrightarrow{f} N \xrightarrow{g} L \tag{5.4.1}$$

is exact if and only if the sequence of character modules

$$L^* \xrightarrow{g^*} N^* \xrightarrow{f^*} M^* \tag{5.4.2}$$

is exact.

Proof.

1. Since $\mathbf{Q}/\mathbf{Z}$ is injective, exactness of sequence (5.4.1) implies exactness of sequence (5.4.2).

2. Let sequence (5.4.2) be exact. We shall show that $Kerf^* = Img^*$ implies $Kerg = Imf$.

(a) Suppose $Imf \not\subset Kerg$, then there is an element $n \in Imf \subset N$ such that $g(n) \neq 0$. Since $n \in Imf$, $n = f(m)$ for some $m \in M$. Therefore $gf(m) \in 0$. Then, by lemma 5.4.8, there exists a homomorphism $h \in L^* = Hom_{\mathbf{Z}}(L, \mathbf{Q}/\mathbf{Z})$ such that $h(gf(m)) \neq 0$. Hence, $h(gf(m)) = (f^*g^*(h))(m) \neq 0$, i.e., $f^*g^* \neq 0$, contradicting $f^*g^* = 0$.

(b) Suppose $Kerg \not\subset Imf$, then there is an element $n \in N$ such that $n \notin Imf$ and $n \in Kerg$, i.e., $g(n) = 0$. Applying lemma 5.4.8 to N/Imf, there exists a homomorphism $h \in N^* = Hom_{\mathbf{Z}}((N, \mathbf{Q}/\mathbf{Z})$ such that $h(Imf) = 0$ and $f(n) \neq 0$. The former means that $f^*(h) = 0$. Since $Kerf^* = Img^*$, there exists $\varphi \in L^* = Hom_{\mathbf{Z}}(L, \mathbf{Q}/\mathbf{Z})$. But then $f(n) = G^*(\varphi)(n) = \varphi(g(n)) = 0$, a contradiction.

Theorem 5.4.10 (J.Lambek). *A right A-module B is flat if and only if its character module B^* is injective as a left A-module.*

Proof. 1. Let a right A-module B be flat and consider an exact sequence of left A-modules:

$$0 \longrightarrow M \longrightarrow N \longrightarrow L \longrightarrow 0 \tag{5.4.3}$$

Then the sequence

$$0 \longrightarrow B \otimes_A M \longrightarrow B \otimes_A N \longrightarrow B \otimes_A L \longrightarrow 0 \tag{5.4.4}$$

is also exact. Then, by lemma 5.4.9, the sequence of character modules

$$0 \longrightarrow (B \otimes_A L)^* \longrightarrow (B \otimes_A N)^* \longrightarrow (B \otimes_A M)^* \longrightarrow 0 \tag{5.4.5}$$

is also exact.

Using the adjoint isomorphism for an arbitrary left A-module C we have

$$(B \otimes_A C)^* = Hom_{\mathbf{Z}}((B \otimes_A C), \mathbf{Q}/\mathbf{Z}) \simeq Hom_A(C, Hom_{\mathbf{Z}}(B, \mathbf{Q}/\mathbf{Z})) =$$

$$= Hom_A(C, B^*) \tag{5.4.6}$$

So we have the following exact sequence

$$0 \longrightarrow Hom_A(L \otimes_A B^*) \longrightarrow Hom_A(N \otimes_A B^*) \longrightarrow Hom_A(M \otimes_A B^*) \longrightarrow 0 \tag{5.4.7}$$

Hence, by proposition 5.2.1, it follows that B^* is injective.

2. Conversely, let B^* be injective module and consider an exact sequence of left A-modules (5.4.3). Then, by proposition 5.2.1, the sequence (5.4.7) is exact and using the isomorphisms (5.4.6) we obtain that the sequence (5.4.5) is also exact. Applying lemma 5.4.9 over the ring $\mathbf{Z}$, it follows that the sequence (5.4.4) is also exact. This shows that B is flat.

Proposition 5.4.11 (Flatness test). *A right A-module B is flat if and only if for each finitely generated left ideal $\mathcal{I} \subseteq A$ the natural map $B \otimes_A \mathcal{I} \to B\mathcal{I}$ is an isomorphism of Abelian groups.*

Proof. Consider the natural homomorphism $f : B \otimes_A \mathcal{I} \to B \otimes_A A$. Since $B \otimes_A A \simeq B \simeq B$, $Imf \simeq B\mathcal{I}$. So to show that $B \otimes_A \mathcal{I} \to B\mathcal{I}$ is an isomorphism of Abelian groups is equivalent to show that the sequence

$$0 \to B \otimes_A \mathcal{I} \to B \otimes_A A \tag{5.4.8}$$

is exact.

1. Let a right A-module B be flat. Then for any left ideal $\mathcal{I} \subseteq A$ we have an exact sequence $0 \to \mathcal{I} \to A$ and, by definition, sequence (5.4.8) is exact.

2. Conversely, let the sequence (5.4.8) be exact for every finitely generated left ideal $\mathcal{I} \subseteq A$. Since any left ideal is a direct limit of finitely generated ideals, applying corollary 4.7.8 we obtain that the sequence (5.4.8) is exact for any left ideal $\mathcal{I} \subseteq A$. Then using the isomorphisms (5.4.6) we obtain exactness of the following sequence

$$Hom_A(A, B^*) \longrightarrow Hom_A(\mathcal{I}, B^*) \longrightarrow 0$$

which by Baer's Criterion means that B^* is injective. Therefore B is flat, by theorem 5.4.10.

The following proposition gives a useful criterion for a quotient module of a flat module to be flat.

Proposition 5.4.12. *Let a sequence of right A-modules $0 \longrightarrow M \longrightarrow F \longrightarrow B \longrightarrow 0$ be exact, where F is flat. Then B is flat if and only if $M \cap F\mathcal{I} = M\mathcal{I}$ for each finitely generated left ideal $\mathcal{I} \subseteq A$.*

Proof. Let a sequence of right A-modules $0 \longrightarrow M \longrightarrow F \longrightarrow B \longrightarrow 0$ be exact, where F is flat, and let $\mathcal{I}$ be a finitely generated left ideal of A. Then we have an exact sequence

$$M \otimes_A \mathcal{I} \xrightarrow{f} F \otimes_A \mathcal{I} \xrightarrow{g} B \otimes_A \mathcal{I} \longrightarrow 0 \tag{5.4.9}$$

Since F is flat, by proposition 5.4.11, $F \otimes_A \mathcal{J}$ can be identified with $F\mathcal{I}$. Since from exactness of the sequence 5.4.9 $Imf = Kerg$ and $Imf \simeq M\mathcal{I}$, by theorem 1.3.1, we have an isomorphism

$$\varphi : F\mathcal{I}/M\mathcal{I} \to B \otimes_A \mathcal{I}$$

On the other hand, from the exactness of $F \to B \to 0$, by the Noether theorem, we have an isomorphism

$$\psi : F\mathcal{I}/M \cap F\mathcal{I} \to B\mathcal{I}$$

So we have the following commutative diagram

$$\begin{array}{ccc} B \otimes_A \mathcal{I} & \xrightarrow{\quad f \quad} & B\mathcal{I} \\ \uparrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \psi} \\ F\mathcal{I}/M\mathcal{I} & \xrightarrow{\quad g \quad} & F\mathcal{I}/M \cap F\mathcal{I} \end{array}$$

where φ, ψ are isomorphisms and f is the natural projection. Then g is an isomorphism if and only if f is an isomorphism. By proposition 5.4.9, f is an isomorphism if and only if B is flat, and g is isomorphism if and only if $M \cap F\mathcal{I} = M\mathcal{I}$, Therefore B is flat if and only if $M \cap F\mathcal{I} = M\mathcal{I}$ for every finitely generated left ideal $\mathcal{I}$, as required.

5.5. RIGHT HEREDITARY AND RIGHT SEMIHEREDITARY RINGS

Definition. A ring A is said to be **right** (resp. **left**) **hereditary** if each right (resp. left) ideal is projective. If a ring A is both right and left hereditary, we say that A is a **hereditary ring**.

Example 5.5.1.
In view of theorem 5.2.13, any semisimple ring is hereditary.

Example 5.5.2.
Any principal ideal domain A is hereditary, since every nonzero ideal is isomorphic to A.

Theorem 5.5.1 (I.Kaplansky). *If a ring A is right hereditary, then any submodule of a free A-module is isomorphic to a direct sum of right ideals of A.*

Proof. Let F be a free A-module with a free basis $\{e_\alpha\}$, where $\alpha \in I$ and the index set I is well-ordered. Define the submodules of F: $F_\alpha = \bigoplus\limits_{\beta<\alpha} e_\alpha A$ and $\overline{F}_\alpha = \bigoplus\limits_{\beta\leq\alpha} e_\alpha A$. Let X be an arbitrary submodule of F. Any element $x \in X \cap \overline{F}_\alpha$ has the form $x = x_0 + e_\alpha a$, where $x_0 \in F_\alpha$ and $a \in A$. The assignment $x \mapsto a$

defines an epimorphism $\varphi : X \cap \overline{F_\alpha} \to \mathcal{I}_\alpha$, where $\mathcal{I}_\alpha$ is a right ideal in the ring A. Clearly, $Ker\varphi = X \cap F_\alpha$. So we have an exact sequence

$$0 \longrightarrow X \cap F_\alpha \longrightarrow X \cap \overline{F_\alpha} \longrightarrow \mathcal{I}_\alpha \longrightarrow 0.$$

Since the ideal $\mathcal{I}_\alpha$ is projective, by proposition 5.1.6, this sequence splits, i.e., $X \cap \overline{F_\alpha} = X \cap F_\alpha \oplus C_\alpha$, where $C_\alpha \simeq \mathcal{I}_\alpha$. We shall show that X is the direct sum of the C_α.

Suppose $c_1 + ... + c_n = 0$, where $c_i \in C_{\alpha_i}$ and we may assume that $\alpha_1 < \alpha_2 < ... < \alpha_n$ in I. Then $c_1, ..., c_{n-1} \in X \cap F_{\alpha_n}$ and $c_n \in C_{\alpha_n}$. Since $(X \cap F_{\alpha_n}) \cap C_{\alpha_n} = 0$, $c_n = 0$ and $c_1 + ... + c_{n-1} = 0$. Continuing in this way, we obtain that $c_1 = ... = c_n = 0$. Finally, we need to show that X is the sum of C_α. Evidently, $\sum\limits_\alpha C_\alpha \subset X$. Suppose $X \neq \sum\limits_\alpha C_\alpha$. Then there is an element $x \in X$ and $x \notin \sum\limits_\alpha C_\alpha$. Then there exists a minimal index β such that the submodule $X \cap \overline{F_\beta}$ contains the element x not belonging to $\sum\limits_\alpha C_\alpha$.

Writing the element x in the form $x = x_0 + c$, where $x_0 \in X \cap F_\beta$ and $c \in C_\beta$, we obtain that the submodule $\sum\limits_\alpha C_\alpha$ does not contain the element x_0. At the same time $x_0 \in X \cap \overline{F_\gamma}$ for some $\gamma < \beta$, which contradicts the minimal property of the index β. The theorem is proved.

From this theorem we obtain immediately the following statements.

Corollary 5.5.2. *If A is a right hereditary ring, then every submodule of a projective right A-module is projective.*

Corollary 5.5.3. *If A is a principal ideal domain, then every submodule of a free A-module is free.*

Corollary 5.5.4. *If A is a principal ideal domain, then every projective A-module is free.*

Corollary 5.5.5. *If A is a right hereditary ring, then a right A-module P is projective if and only if it is embeddable into a free right A-module.*

Theorem 5.5.6. *The following conditions are equivalent for a ring A:*
a) *A is a right hereditary ring;*
b) *any submodule of a right projective A-module is projective;*
c) *any quotient of a right injective A-module is injective.*

Proof.
a) $\Longrightarrow$ *b*) follows from corollary 5.5.5.
b) $\Longrightarrow$ *a*) is trivial from the definition of a right hereditary ring.
b) $\Longrightarrow$ *c*). Assume that any submodule of a right projective A-module is projective. In particular, any right ideal $\mathcal{I}$ of the ring A is projective. Let Q/K

be a quotient of an injective A-module Q. Consider a diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathcal{I} & \xrightarrow{i} & A \\ & & \downarrow{\scriptstyle \varphi} & & \\ Q & \xrightarrow{\psi} & Q/K & \longrightarrow & 0 \end{array}$$

with top and bottom rows exact and canonical embedding i. Since the ideal $\mathcal{I}$ is projective, there exists a homomorphism $f : \mathcal{I} \to Q$ such that $\varphi = \psi f$. Since Q is injective, by Baer's Criterion, there exists a homomorphism $g : A \to Q$ extending f, i.e., $gi = f$. Set $h = \psi g$. Then $hi = \psi gi = \psi f = \varphi$. Therefore h is a homomorphism $h : A \to Q/K$ which extends φ. In view of Baer's Criterion, Q/K is injective.

c) $\Longrightarrow$ *a*). Assume that any quotient of a right injective module is injective. Suppose we have a diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathcal{I} & \xrightarrow{i} & A \\ & & \downarrow{\scriptstyle \varphi} & & \\ N & \xrightarrow{\psi} & M & \longrightarrow & 0 \end{array}$$

with top and bottom rows exact and canonical embedding i.

By Baer's theorem, there exists an injective module Q containing N. Let $\alpha : N \to Q$ be the inbedding. Let $Q_1 = Q/Im(\alpha\sigma)$ and $Q_2 = Im(\alpha\sigma)$. Consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Ker\psi & \xrightarrow{\sigma} & N & \xrightarrow{\psi} & M & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle \alpha} & & & & \\ 0 & \longrightarrow & Q_2 & \longrightarrow & Q & \xrightarrow{\pi} & Q_1 & \longrightarrow & 0 \end{array}$$

with top and bottom rows exact, the canonical imbedding α and the projection π. Then we can construct a homomorphism $\beta : M \to Q_1$ by setting $\beta(m) = \pi\alpha\psi(n)$, where $m = \psi(n)$, $n \in N$. Therefore we obtain a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Ker\psi & \xrightarrow{\sigma} & N & \xrightarrow{\psi} & M & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \\ 0 & \longrightarrow & Q_2 & \longrightarrow & Q & \xrightarrow{\pi} & Q_1 & \longrightarrow & 0 \end{array}$$

Then we can set $h = \beta\psi = \pi\alpha$. Since π is an epimorphism and α is a monomor-

phism, h is an epimorphism. So we have the following diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathcal{I} & \xrightarrow{i} & A \\ & & \downarrow{\scriptstyle \beta\varphi} & & \\ N & \xrightarrow{h} & Q_1 & \longrightarrow & 0 \end{array}$$

By hypothesis the module $Q_1 = Q/Im(\alpha\sigma)$ is injective and by Baer's Criterion there exists a homomorphism $\gamma : A \to Q_1$ extending $\beta\varphi$, i.e., $\gamma i = \beta\varphi$. Since A is obviously a projective A-module, there exists a homomorphism $\delta : A \to N$ such that $h\delta = \gamma$. Therefore we can set $\sigma = \delta i : \mathcal{I} \to N$. It is easy to verify that $\psi\sigma = \varphi$, i.e., $\mathcal{I}$ is a right projective ideal in A. The theorem is proved.

Proposition 5.5.7. *Let A be a right hereditary ring. Then for any nonzero idempotent $e^2 = e \in A$ the ring eAe is also right hereditary.*

Proof. Let $\mathcal{I}$ be a right ideal of a ring eAe. Consider the ideal $\tilde{\mathcal{I}} = \mathcal{I}A$ which is a right ideal of A. By assumption, $\tilde{\mathcal{I}}$ is projective. There is a free A-module F for which $\tilde{\mathcal{I}} \simeq F/K$. Then we have an exact sequence

$$0 \longrightarrow K \longrightarrow F \longrightarrow \tilde{\mathcal{I}} \longrightarrow 0.$$

Since $\tilde{\mathcal{I}}$ is projective, this sequence splits and we have $F \simeq \tilde{\mathcal{I}} \oplus K$. Multiplying this equality on the right by e we obtain $Fe \simeq \tilde{\mathcal{I}}e \oplus Ke$. From the decomposition $F = Fe \oplus F(1-e)$ it follows that Fe is projective. Since $\tilde{\mathcal{I}}e = \mathcal{I}$, by proposition 5.1.4, $\mathcal{I}$ is a projective right ideal, i.e., eAe is a right hereditary ring.

Lemma 5.5.8. *If a ring A is right hereditary, then any nonzero homomorphism $\varphi : P_1 \to P_2$ of indecomposable projective right A-modules is a monomorphism.*

Proof. Since $Im\varphi$ is a projective module, $P_1 \simeq Im\varphi \oplus Ker\varphi$. Hence, due to indecomposibility of P_1, it follows that $Ker\varphi = 0$.

Definition. A ring A is said to be **right (left) semihereditary** if each finitely generated right (left) ideal is a projective A-module. A ring A which is both right semihereditary and left semihereditary is called **semihereditary**.

For a right semihereditary ring we have statements, which are similar to propositions 5.5.1 and 5.5.6.

Proposition 5.5.9. *If A is a right semihereditary ring, then every finitely generated submodule of a free A-module is isomorphic to a direct sum of a finite number of finitely generated right ideals of A.*

Proof. Let F be a free A-module with a free basis $\{e_\alpha\}$, where $\alpha \in I$. Suppose X is a finitely generated submodule of F. Then each generator of X is a finite

linear combination of e_α's, so that X is contained in a free summand of F, which has a finite free basis. So we can suppose that F is a free module with finite free basis $e_1, e_2, ..., e_n$.

We shall prove our statement by induction on the number of elements n.

Let $n = 1$, i.e., $F = eA$. Suppose X is a finitely generated submodule of F with a system of generators $\{x_1, x_2, ..., x_k\}$. Then any element $x \in X$ has the form

$$x = \sum_{i=1}^{k} x_i a_i = \sum_{i=1}^{k} e b_i a_i = e \sum_{i=1}^{k} b_i a_i$$

and X is isomorphic to the finitely generated right ideal $\mathcal{I}$ with system of generators $\{b_1a_1, b_2a_2, ..., b_ka_k\}$.

Suppose $n > 1$ and X is a finitely generated submodule of F with free basis $\{e_1, e_2, ..., e_n\}$. We define $Y = X \cap (e_1A \oplus e_2A \oplus ... \oplus e_{n-1}A)$. Any element $x \in X$ has a unique form $x = y + e_n a$, where $y \in Y$, $a \in A$. The assignment $x \mapsto a$ defines an epimorphism $\varphi : X \longrightarrow \mathcal{I}$, where $\mathcal{I}$ is a right ideal of A. So we have an exact sequence:

$$0 \longrightarrow Y \longrightarrow X \xrightarrow{\varphi} \mathcal{I} \longrightarrow 0$$

Since $\mathcal{I}$ is a finitely generated right ideal of A and A is right semihereditary, $\mathcal{I}$ is projective. Then, by proposition 5.1.6, this sequence splits, i.e., $X \simeq Y \oplus \mathcal{I}$. Since Y is a finitely generated submodule of $e_1A \oplus e_2A \oplus ... \oplus e_{n-1}A$, by the induction hypothesis, Y is isomorphic to a direct sum of finitely generated right ideals of A.

Corollary 5.5.10. *A ring A is right semihereditary if and only if every finitely generated submodule of a right projective A-module is projective.*

Proof. 1. Let A be a right semihereditary ring and P be a projective right A-module. Suppose X is a finitely generated submodule of P. Since P is a direct summand of some free A-module F, by theorem 5.5.6, X is isomorphic to a direct sum of a finite number of finitely generated right ideals of A:

$$X \simeq \overset{n}{\underset{i=1}{\oplus}} \mathcal{I}_i$$

Since A is right semihereditary, each $\mathcal{I}_i$ is projective and by proposition 5.1.4 X is also projective.

2. Since A is projective A-module, by hypothesis, each of its finitely generated right ideal is also projective, i.e., A is a right semihereditary ring.

5.6. HERSTEIN-SMALL RINGS

In this section we consider a class of rings, which shows that the notion of a right hereditary ring is different from that of a left hereditary ring. The first example, which shows this difference, was constructed by I.Kaplansky. Another, easier

example, was later constructed by L.Small. He considered an important family of rings and showed that these rings are right Noetherian and right hereditary but they are neither left Noetherian nor left hereditary.

I.N.Herstein used such a ring as an example of a right Noetherian ring in which the intersection of natural powers of the Jacobson radical is not equal to zero.

Let $\mathbf{Q}$ be the field of rational numbers, and let p be a prime integer, $\mathbf{Z}_{(p)} = \{\frac{m}{n} \in \mathbf{Q} \mid (n,p) = 1\}$. As it has been shown in section 1.1 the ring $\mathbf{Z}_{(p)}$ has the unique composition series

$$\mathbf{Z}_{(p)} \supset p\mathbf{Z}_{(p)} \supset p^2\mathbf{Z}_{(p)} \supset ... \supset p^n\mathbf{Z}_{(p)} \supset ...$$

So, $\mathbf{Z}_{(p)}$ is a principal ideal domain, which is Noetherian but not Artinian. Consider the following ring

$$H(\mathbf{Z}_{(p)}, 1, 1) = \begin{pmatrix} \mathbf{Z}_{(p)} & \mathbf{Q} \\ 0 & \mathbf{Q} \end{pmatrix}.$$

We shall show that the ring $A = H(\mathbf{Z}_{(p)}, 1, 1)$ is right Noetherian but not left Noetherian, that it is right hereditary but not left hereditary and that the intersection of natural powers of the Jacobson radical of this ring is not equal to zero. We write $e = e_{11}$ and $f = e_{22}$ (the matrix units). So that $eAe = \mathbf{Z}_{(p)}$ is Noetherian but not Artinian, $fAf = \mathbf{Q}$ is a field, $eAf = \mathbf{Q}$ is a finitely generated right $\mathbf{Q}$-module and an infinitely generated left $\mathbf{Z}_{(p)}$-module. From theorem 3.6.1 it is immediate that the ring A is right Noetherian but not left Noetherian, it is neither right nor left Artinian.

Since $rad\mathbf{Z}_{(p)} = p\mathbf{Z}_{(p)}$, the radical R of $H(\mathbf{Z}_{(p)}, 1, 1)$ has the following form

$$R = \begin{pmatrix} p\mathbf{Z}_{(p)} & \mathbf{Q} \\ 0 & 0 \end{pmatrix}.$$

Hence we obtain that for any $n > 0$

$$R^n = \begin{pmatrix} p^n\mathbf{Z}_{(p)} & \mathbf{Q} \\ 0 & 0 \end{pmatrix}$$

and the intersection of all natural powers of the Jacobson radical of the ring $H(\mathbf{Z}_{(p)}, 1, 1)$ coincides with the ideal

$$\mathcal{I} = \bigcap_{n=1}^{\infty} R^n = \begin{pmatrix} 0 & \mathbf{Q} \\ 0 & 0 \end{pmatrix} \neq 0.$$

Let us describe all right ideals $\mathcal{J}$ in the ring $A = H(\mathbf{Z}_{(p)}, 1, 1)$. If $\mathcal{J}e \neq 0$, then $\mathcal{J}e$ coincides with $p^n\mathbf{Z}_{(p)}$ for some n. Assume that the right ideal $\mathcal{J}$ has an element $\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}$ with $\gamma \neq 0$. Then $\mathcal{J}$ has the following form:

$$\mathcal{J} = \begin{pmatrix} p^n\mathbf{Z}_{(p)} & \mathbf{Q} \\ 0 & \mathbf{Q} \end{pmatrix}.$$

If $\gamma = 0$ for all elements of $\mathcal{J}$, then, obviously, $\mathcal{J} = R^n$. In the case $\mathcal{J}e = 0$ right ideals $\mathcal{J}$ are given by the various $\mathbf{Q}$-subspaces in the two-dimensional space $\begin{pmatrix} 0 & \mathbf{Q} \\ 0 & \mathbf{Q} \end{pmatrix}$.

Thus, all the right ideals of the ring A are given by A, eA, fA, R^n, $R^n \oplus fA$ and various $\mathbf{Q}$-subspaces in the two-dimensional space $\begin{pmatrix} 0 & \mathbf{Q} \\ 0 & \mathbf{Q} \end{pmatrix}$.

Evidently, all these right ideals are projective. Therefore the ring A is right hereditary.

At the same time the left ideal

$$\mathcal{I} = \begin{pmatrix} 0 & \mathbf{Q} \\ 0 & 0 \end{pmatrix}$$

is, in fact, a left $\mathbf{Z}_{(p)}$-module and it is obviously indecomposable. Assume $\mathcal{I}$ is a projective left A-module. Then the $\mathbf{Z}_{(p)}$-module $\mathbf{Q}$ is a submodule of a free $\mathbf{Z}_{(p)}$-module of countable rank. This contradiction shows that $\mathcal{I}$ is not projective and so, the ring A is not left hereditary.

5.7. NOTES AND REFERENCES

It is interesting to note that the fundamental notions of homological algebra (such as projective module and the functor Tor) arose in connection with the study of the behaviour of modules over Dedekind rings with respect to the tensor product. These investigations were carried out by H.Cartan in 1948.

Homological methods have invaded much of abstract algebra, and especially ring theory - both commutative and noncommutative - beginning with the 1950s. In fact, many of the standard concepts and results have been rephrased in homological language. The first systematic theory of projective and injective modules was presented in the book *H.Cartan, S.Eilenberg, Homological Algebra, 1956.*

It is interesting to note that the theory of injective modules was investigated long before the dual notion of projective modules. Injective modules first appeared in the context of Abelian groups. L.Zippin observed in 1935 that an Abelian group is divisible if and only if it is a direct summand of any larger group containing it as a subgroup, and that the divisible Abelian groups can be completely described. The general notion of an injective module over an arbitrary ring was first investigated by R.Baer in the paper *Abelian groups that are direct summands of every containing Abelian group // Bull. Amer. Math., v. 46 (1940), p.800-806* (but the term "injective" was only introduced in the paper: *B.Eckmann and A.Schopf, Über injektive Moduln // Arch. der. Math. v.4 (1953), p.75-78*) where it was also shown that categories of modules are "injective rich".

R.Baer worked with what he called "complete" modules over a ring R, namely modules A such that every homomorphism from a one-sided ideal of R to A extends to a homomorphism from R to A. He proved that every module is a submodule of a complete module, and that a module is complete if and only if it is a direct

summmand of every module that contains it (see *R.Baer, Abelian groups that are direct summands of every containing Abelian group //Bull. Amer. Math. Soc. v.46 (1940), p. 800-806*). The method we have used for the proof of Baer's theorem is due to B.Eckmann and A.Schopf: *B.Eckmann and A.Schopf, Über injektive Moduln // Arch. der. Math. v.4 (1953), p.75-78.* In their elegant little paper it was also proved that a module is injective if and only if it has no proper essential extensions.

The concept of an injective hull was developed by B.Eckmann and A.Schopf in their paper *Über injektive Moduln // Arch. der. Math. v.4 (1953), p.75-78.* The term "injective envelope" appeared in the paper of E.Matlis: *E.Matlis, Injective modules over noetherian rings // Pacific J.Math. v.8 (1958), p.511-528* and the term "injective hull" appeared in the paper of A.Rozenberg and D.Zelinsky *A.Rozenberg and D.Zelinsky, Finiteness of the injective hull // Math. Zeitschrift, v.70 (1959), p.372-380.*

For the proofs of the results on projective covers at the end of sections 5.3 and more information on them see *C.Curtis, I.Reiner, Methods of representation theory, vol.1, §6c, Wiley, 1981.*

That a ring R is right Noetherian if and only if every direct sum of injective right R-modules is injective was proved independently by Z.Papp (see *Z.Papp, On algebraically closed modules // Publ. Math. Debrecen v.6 (1959), v.311-327*) and H.Bass (see *H.Bass, Injective dimension in Noetherian rings // Trans. Amer. Math. Soc. v.102 (1962), p.18-29*).

The notions of torsion and torsionfreeness of an injective left module were first developed systematically by P.Gabriel (see, *Des catégories Abéliennes // Bulletin de la Societé Math.de France, v.90 (1962), p.323-448*) and L.E.Dickson (see, *A torsion theory for Abelian categories // Trans. Amer. Math. Soc., v.121 (1966),p.223-235*).

Theorem 5.4.10, which gives a connection between a flat module and it character module, was proved by J.Lambek in the paper *A module is flat if and only if its character module is injective, Canad. Math. Bull., v. 7 (1964), p.237-243.*

The examples of Herstein-Small rings were first presented in the papers *L.W.Small, An example in Noetherian rings // Proc. Nat. Sci. USA, v.54 (1965), p.1035-1036* and *I.N.Herstein, A counter example in Noetherian rings // Proc. Nat. Sci. USA, v.54 (1965), p.1036-1037.*

6. Homological dimensions

6.1. COMPLEXES AND HOMOLOGY. FREE RESOLUTIONS

In section 4.2 we considered exact sequences. In this section we shall consider a generalization of this notion.

Definition. A **complex S** is a sequence of modules and homomorphisms

$$... \longrightarrow S_n \xrightarrow{d_n} S_{n-1} \xrightarrow{d_{n-1}} S_{n-2} \longrightarrow ... \tag{6.1.1}$$

where $n \in \mathbf{Z}$, such that $d_{n-1}d_n = 0$ for all n, i.e., $Kerd_{n-1} \subset Imd_n$. The maps d_n are called the **differentials** of the given complex $\mathbf{S}$. The modules $H_n(\mathbf{S}) = Kerd_n/Imd_{n+1}$ are called the **homology modules** of $\mathbf{S}$.

Note, that a complex is an exact sequence if and only if $H_n(\mathbf{S}) = 0$ for all n. For this reason exact sequences is often called **acyclic complexes**.

If $\mathbf{S}'$ is another complex, then a **homomorphism of complexes** $f : \mathbf{S} \longrightarrow \mathbf{S}'$ is a family of homomorphisms $f_n : S_n \to S'_n$ making the following diagram

$$\begin{array}{ccccccc} \cdots & \longrightarrow & S_n & \xrightarrow{d_n} & S_{n-1} & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & S'_n & \xrightarrow{d'_n} & S'_{n-1} & \longrightarrow & \cdots \end{array}$$

commutative, i.e., $f_{n-1}d_n = d'_n f_n$ for all n.

The homology coset $x + Imd_{n+1}$, where $x \in Kerd_n$, will be denoted by $[x]$. Clearly, a family of homomorphisms making up a morphism of complexes induces homology morphisms

$$H_n(f) : H_n(\mathbf{S}) \to H_n(\mathbf{S}')$$

defined by $H_n(f)[x] = [f_n(x)]$ for all n.

In this way we can consider the **category of complexes** of A-modules, which we shall denote by *com-A* and the family of functors $H_n : com\text{-}A \to mod\text{-}A$.

Let $f : \mathbf{S} \longrightarrow \mathbf{S}'$ be a homomorphism of complexes. Then, obviously, $d'_n(Imf_n) \subset Imf_{n-1}$ and $d_n(Kerf_n) \subset Kerf_{n-1}$. So we have the complexes $Imf = \{Imf_n\}$ and $Kerf = \{Kerf_n\}$. Therefore we can define exact sequences of complexes just in the same way as exact sequences of modules. In particular, if $\mathbf{S}'$, $\mathbf{S}'$ and $\mathbf{S}''$ are complexes, then a sequence

$$\mathbf{S}' \xrightarrow{f} \mathbf{S} \xrightarrow{g} \mathbf{S}''$$

is exact if $Kerg = Imf$ (at all n).

Theorem 6.1.1. *Let* $0 \longrightarrow \mathbf{S}' \stackrel{f}{\longrightarrow} \mathbf{S} \stackrel{g}{\longrightarrow} \mathbf{S}'' \longrightarrow 0$ *be an exact sequence of complexes. Then for each* n *there exists a homomorphism* $\delta_n : H_n(\mathbf{S}'') \to H_{n-1}(\mathbf{S}')$ *such that the following sequence is exact*:

$$... \longrightarrow H_{n+1}(\mathbf{S}'') \stackrel{\delta_{n+1}}{\longrightarrow} H_n(\mathbf{S}') \stackrel{H_n(f)}{\longrightarrow} H_n(\mathbf{S}) \stackrel{H_n(g)}{\longrightarrow}$$

$$\stackrel{H_n(g)}{\longrightarrow} H_n(\mathbf{S}'') \stackrel{\delta_n}{\longrightarrow} H_{n-1}(\mathbf{S}') \stackrel{H_{n-1}(f)}{\longrightarrow} H_{n-1}(\mathbf{S}) \longrightarrow ... \qquad (6.1.2)$$

Proof. Let $[x]$ be a homology coset of $H_n(\mathbf{S}'')$. Since g_n is surjective for any n, $x = g_n(y)$ for some $y \in S_n$. Now, $g_{n-1}d_n y = d''_n g_n y = d''_n x = 0$. And in view of exactness, there exists $z \in S''_{n-1}$ such that $d_n(y) = f_{n-1}(z)$. Furthermore, $f_{n-2}d'_{n-1}z = d_{n-1}f_{n-1}z = d_{n-1}d_n y = 0$ and therefore $d'_{n-1}z = 0$, because f_{n-2} is a monomorphism.

Then we can set $\delta_n[x] = [z]$. We shall show that it is a well-defined homomorphism from $H_n(\mathbf{S}'')$ to $H_{n-1}(\mathbf{S}')$, i.e., $[z]$ depends neither on the choice of y nor on the choice of x in the homology coset $[x]$. Indeed, if $g_n(y') = g_n(y)$ then $g_n(y' - y) = 0$ and so, in view of exactness, $y' - y = f_n(u)$ for some $u \in S'_n$. Thus, $d_n(y') = d_n(y) + d_n f_n(u) = f_{n-1}(z) + f_{n-1}d'_n(u) = f_{n-1}(z + d'_n(u))$ and so $[z] = [z + d'_n(u)]$. Furthermore, let $[x] = [x']$, i.e., $x' = x + d''_{n+1}(v)$ for some $v \in S''_{n+1}$. Then there exists $w \in S_{n+1}$ such that $v = g_{n+1}(w)$ and therefore $x' = g_n(y) + g_n d_{n+1}(w) = g_n(y + d_{n+1}(w))$. Since $d_n(y + d_{n+1}(w)) = d_n(y)$, the choice of x' does not change the coset $[z]$. Thus, $\delta_n : H_n(\mathbf{S}'') \to H_{n-1}(\mathbf{S}')$ is a well-defined homomorphism.

Now we shall show that sequence (6.1.2) is exact. We shall show that $KerH_n(f) \subset Im\delta_{n+1}$ and $Ker\delta_n \subset ImH_n(g)$ and leave exactness at all other spots to the reader.

1. Let $H_n(f)[x] = 0$, that means $f_n(x) = d_{n+1}(y)$ for some $y \in S_{n+1}$. We put $z = g_{n+1}(y)$, then $d_{n+1}z = g_n d_{n+1}(y) = g_n f_n(x) = 0$ and we obtain $[z] \in H_{n+1}(\mathbf{S}'')$ satisfying $\delta_{n+1}[z] = [x]$ according to the definition of δ.

2. Let $\delta_n[x] = 0$. By the definition of δ this means that if $x = g_n(y)$ and $d_n(y) = f_{n-1}(z)$, then $z = d'_n(u)$ for some $u \in S'_n$. Hence, $x = g_n(y - f_n(u))$ and $d_n(y - f_n(u)) = d_n(y) - f_{n-1}d'_n = 0$, which gives $[x] = H_n(g)[y - f_n(u)]$, as required.

A most important example of homomorphisms of complexes is given by homotopic homomorphisms. Let $\mathbf{S}$ and $\mathbf{S}'$ be two complexes. Two homomorphisms f and $g : \mathbf{S} \to \mathbf{S}'$ are called **homotopic**, and we write $f \sim g$, if there are homomorphisms $\Delta_n : S_n \to S'_{n+1}$ such that $f_n - g_n = d'_{n+1}\Delta_n + \Delta_{n-1}d_n$ for all n.

Proposition 6.1.2. *If two homomorphisms* f *and* $g : \mathbf{S} \to \mathbf{S}'$ *are homotopic, then* $H_n(f) = H_n(g)$ *for all* n.

Proof. Let $[x]$ be a coset of a complex $\mathbf{S}$. Since $d_n(x) = 0$, we have: $H_n(f)[x] = [f_n(x)] = [g_n(x) + d'_{n+1}\Delta_n(x) + \Delta_{n-1}d_n(x)] = [g_n(x) + d'_{n+1}\Delta_n(x)] = [g_n(x)] = H_n(g)[x]$.

Two complexes $\mathbf{S}$ and $\mathbf{S}'$ are called **homotopic** if there exist homomorphisms $f : \mathbf{S} \to \mathbf{S}'$ and $g : \mathbf{S}' \to \mathbf{S}$ such that $fg \sim 1$ and $gf \sim 1$.

Corollary 6.1.3. *If the complexes* $\mathbf{S}$ *and* $\mathbf{S}'$ *are homotopic, then* $H_n(f) = H_n(g)$ *for all* n.

Definition. A **free resolution** of a module M is an exact sequence

$$\ldots \longrightarrow F_n \xrightarrow{d_n} F_{n-1} \longrightarrow \ldots \longrightarrow F_1 \xrightarrow{d_1} F_0 \longrightarrow M \longrightarrow 0,$$

where each F_n is a free module.

Proposition 6.1.4. *Every module has a free resolution.*

Proof. By proposition 1.5.4, for any A-module M there exists an exact sequence

$$0 \longrightarrow K_0 \longrightarrow F_0 \longrightarrow M \longrightarrow 0,$$

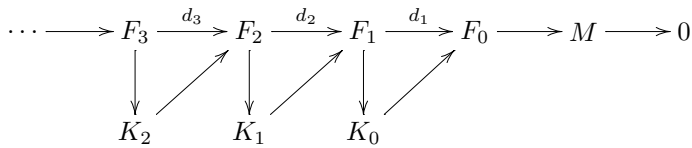
where F_0 is a free module. Now K_0 need not be free, but there exists an exact sequence

$$0 \longrightarrow K_1 \longrightarrow F_1 \longrightarrow K_0 \longrightarrow 0,$$

where F_1 is a free module. Now again K_1 need not be free, so we continue this procedure. By induction, we have an exact sequence

$$0 \longrightarrow K_n \longrightarrow F_n \longrightarrow K_{n-1} \longrightarrow 0,$$

where F_n is a free module. In general, this process can be continued infinitely without arriving at a free kernel. Linking all these exact sequences together we obtain an infinite commutative diagram:



where each F_n is a free module and the maps d_n are just the indicated composites. Since for any n, $Kerd_n = K_n$ and $Imd_n = K_{n-1}$, we have $Kerd_n = Imd_{n+1}$ and so the top sequence is exact.

Remark. A given module M can have many different free resolutions. Exactness of a free resolution means that $Imd_{n+1} = Kerd_n$. Therefore a free resolution is a complex and all its homology is 0. In fact, the homology measures

how much a sequence differs from being exact.

6.2. PROJECTIVE AND INJECTIVE RESOLUTIONS. DERIVED FUNCTORS

A generalization of a free resolution is a projective one. The properties of projective resolutions will be considered in this section.

Definition. Let M be an A-module. A **projective resolution** of M is an exact sequence of A-modules

$$... \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\pi} M \longrightarrow 0 \tag{6.2.1}$$

in which all P_n are projective.

Proposition 6.2.1. *Every module has a projective resolution.*

Proof. This is a corollary of proposition 6.1.4 as free modules are projective.

In a dual way one can define an **injective resolution** of an A-module M as an exact sequence of A-modules

$$0 \longrightarrow M \xrightarrow{i} Q_0 \xrightarrow{d_0} Q_1 \xrightarrow{d_1} Q_2 \longrightarrow \tag{6.2.2}$$

in which all Q_n are injective.

In this chapter we shall generally deal with projective resolutions, leaving the corresponding statements and results for injective resolutions to the reader. [1])

Let $\mathbf{P}$ be a projective resolution of a module M and $\mathbf{P'}$ be a projective resolution of a module M'. Then for every homomorphism of complexes $f : \mathbf{P} \to \mathbf{P'}$, i.e., a commutative diagram:

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \xrightarrow{\pi} & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle \varphi} & & \\
\cdots & \longrightarrow & P'_2 & \xrightarrow{d_2} & P'_1 & \xrightarrow{d_1} & P'_0 & \xrightarrow{\pi'} & M' & \longrightarrow & 0
\end{array}$$

The homomorphism f is called an **extension of φ to the resolutions $\mathbf{P}$ and $\mathbf{P'}$**.

Theorem 6.2.2. *Let $\mathbf{P}$ be a projective resolution of a module M and $\mathbf{P'}$ be a projective resolution of a module M'. Then*

1. *Every homomorphism $\varphi : M \to M'$ can be extended to the resolutions $\mathbf{P}$ and $\mathbf{P'}$.*

[1]) Note that injective resolutions always exist. Just take repeated injective hulls and combine them. Just as in the case of projective or free resolutions where one takes repeated projective or free surjections $P_n \to M_n$.

2. *Any two extensions of φ to a given pair of resolutions $\mathbf{P}$ and $\mathbf{P'}$ are homotopic.*

3. *Any two projective resolutions of a module M are homotopic.*

Proof.

1. Consider the homomorphism $\varphi\pi : P_0 \to M'$. Since P_0 is projective and $\pi' : P'_0 \to M'$ is epimorphism, there exists a homomorphism $f_0 : P_0 \to P'_0$ such that a diagram

$$\begin{array}{ccccc} P_0 & \xrightarrow{\pi} & M & \longrightarrow & 0 \\ \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle \varphi} & & \\ P'_0 & \xrightarrow{\pi'} & M' & \longrightarrow & 0 \end{array}$$

is commutative, i.e., $\pi' f_0 = \varphi\pi$. Therefore $\pi' f_0 d_1 = \varphi\pi d_1$ and thus $f_0(Im d_1) \subset Ker(\pi') = Im(d'_1)$. So we have a sequence of homomorphisms:

$$P_1 \overset{d_1}{\to} Im(d_1) \overset{f_0}{\to} Im(d'_1).$$

Since P_1 is projective, there is a homomorphism $f_1 : P_1 \to P'_1$ such that the diagram

$$\begin{array}{ccccc} P_1 & \xrightarrow{d_1} & Im(d_1) & \longrightarrow & 0 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_0} & & \\ P'_1 & \xrightarrow{d'_1} & Im(d'_1) & \longrightarrow & 0 \end{array}$$

is commutative, i.e., $f_0 d_1 = d'_1 f_1$.

Suppose $f_0, f_1, ..., f_n$ have been defined. We define f_{n+1} recursively. From the commutative property of the constructed diagram we have $f_{n-1} d_n = d'_n f_n$. Since $d_{n+1} d_n = 0$, $0 = d'_n f_n d_{n+1}$, i.e., $f_n(Im d_{n+1}) \subset Ker(d'_n) = Im(d'_{n+1})$. Therefore, we have a sequence of homomorphisms:

$$P_{n+1} \overset{d_{n+1}}{\to} Im(d_{n+1}) \overset{f_n}{\to} Im(d'_{n+1}).$$

Since P_{n+1} is projective, there is a homomorphism $f_{n+1} : P_{n+1} \to P'_{n+1}$ such that $f_n d_{n+1} = d'_{n+1} f_{n+1}$. Continuing this process we obtain an extension $f : \mathbf{P} \to \mathbf{P'}$ of the homomorphism φ.

2. Let $g : \mathbf{P} \to \mathbf{P'}$ be another extension of the homomorphism φ.

We shall show that $f \sim g$. To this end we shall construct homomorphisms Δ_n recursively much like above. Note that $\pi' f_0 = \varphi\pi = \pi' g_0$, that is, $\pi'(f_0 - g_0) = 0$. So $Im(f_0 - g_0) \subset Ker(\pi') = Im(d'_1)$. So there is a Δ_0 making the following diagram

$$\begin{array}{ccccc} & & P_0 & & \\ & \swarrow^{\Delta_0} & \downarrow{\scriptstyle f_0 - g_0} & & \\ P'_1 & \xrightarrow{d'_1} & Im(d'_1) & \longrightarrow & 0 \end{array}$$

commutative.

Suppose $\Delta_0, \Delta_1, ..., \Delta_n$ have been defined. In this case $f_n - g_n = d'_{n+1}\Delta_n + \Delta_{n-1}d_n$. So that

$$d'_{n+1}(f_{n+1} - g_{n+1} - \Delta_n d_{n+1}) = d'_{n+1}f_{n+1} - d'_{n+1}g_{n+1} - d'_{n+1}\Delta_n d_{n+1} =$$

$$= f_n d_{n+1} - g_n d_{n+1} - d'_{n+1}\Delta_n d_{n+1} = (f_n - g_n - d'_{n+1}\Delta_n)d_{n+1} = \Delta_{n-1}d_n d_{n+1} = 0.$$

Therefore, $Im(f_{n+1} - g_{n+1} - \Delta_n d_{n+1}) \subset Ker(d'_{n+1}) = Im(d'_{n+2})$. So that there is a Δ_{n+1} making the following diagram

$$\begin{array}{ccccc} & & P_{n+1} & & \\ & \swarrow^{\Delta_{n+1}} & \downarrow{\scriptstyle f_{n+1}-g_{n+1}-\Delta_n d_{n+1}} & & \\ P'_{n+2} & \xrightarrow{d'_{n+2}} & Im(d'_{n+2}) & \longrightarrow & 0 \end{array}$$

commutative.

3. Let $\mathbf{P}$ and $\mathbf{P'}$ be two projective resolutions of a module M. In this case there are two extensions $f : \mathbf{P} \to \mathbf{P'}$ and $g : \mathbf{P'} \to \mathbf{P}$ of the identity homomorphism $1_M : M \to M$. But then fg and gf also extend $1_M : M \to M$. Since $1_P : \mathbf{P} \to \mathbf{P}$ and $1_{P'} : \mathbf{P'} \to \mathbf{P'}$ extend $1_M : M \to M$ as well, property 2 of the statement of the theorem implies $fg \sim 1$ and $gf \sim 1$, i.e., $\mathbf{P} \sim \mathbf{P'}$.

From this theorem, proposition 6.1.2, and corollary 6.1.3 we obtain the following important consequence:

Proposition 6.2.3.

1. *Let F be a functor from the category of A-modules to the category of B-modules and let $\mathbf{P}$ be a projective resolution of an A-module M. Then the homology $H_n(F(\mathbf{P}))$ is independent of the choice of the resolution $\mathbf{P}$.*

2. *If $\mathbf{P'}$ is a projective resolution of an A-module M' and $f : \mathbf{P} \to \mathbf{P'}$ is an extension of a homomorphism $\varphi : M \to M'$, then $H_n(F(f))$ is independent of the choice of the extension f.*

Taking into account this proposition we can introduce the notion of a derived functor. Let F be a functor from the category of A-modules to the category of B-modules, let $\mathbf{P}$ be a projective resolution of an A-module M, let $\mathbf{P'}$ be a projective resolution of an A-module M' and let $f : \mathbf{P} \to \mathbf{P'}$ be an extension of a homomorphism $\varphi : M \to M'$. Then for each A-module M we shall write $L_nF(M) = H_n(F(\mathbf{P})) = Ker(Fd_n)/Im(Fd_{n+1})$ and $L_nF(\varphi) = H_n(F(f))$. If f is extension of φ and g is extension of $\psi : M' \to M''$, then gf is an extension of $\psi\varphi$ and thus $L_nF(\psi\varphi) = L_nF(\psi)L_nF(\varphi)$, i.e., L_nF is a functor from ${}_A\mathbf{M}$ to ${}_B\mathbf{M}$ and it is called the n-th **left derived functor** of a functor F. In a similar way, replacing projective resolutions by injective resolutions, one can introduce the **right derived functors** R^nF of a functor F. The definitions of left and right

derived functors of a contravariant functor G can be given dually, using injective resolutions for L_nG and projective resolutions for R^nG.

Proposition 6.2.4. *A right (left) exact functor F satisfies $L_0F \simeq F$ (respectively, $R^0f \simeq F$).*

Proof. If $\mathbf{P}$ is a projective resolution of a A-module M, then $P_1 \stackrel{d_1}{\to} P_0 \to M \to 0$ is an exact sequence. Therefore $F(P_1) \stackrel{F(d_1)}{\to} F(P_0) \to F(M) \to 0$ is also an exact sequence. Hence,

$$L_0F(M) = H_0(F(\mathbf{P})) = F(P_0)/ImF(d_1) \simeq F(M).$$

Lemma 6.2.5. *Suppose*

$$0 \to M' \stackrel{\varphi}{\longrightarrow} M \stackrel{\psi}{\longrightarrow} M'' \longrightarrow 0$$

be an exact sequence of modules. Then there is an exact sequence

$$0 \to \mathbf{P}' \stackrel{f}{\longrightarrow} \mathbf{P} \stackrel{g}{\longrightarrow} \mathbf{P}'' \longrightarrow 0$$

of projective resolutions, in which f extends φ and g extends ψ.

Proof. Consider the epimorphisms $P_0' \stackrel{\pi'}{\longrightarrow} M' \longrightarrow 0$ and $P_0'' \stackrel{\pi''}{\longrightarrow} M'' \longrightarrow 0$. Put $P_0 = P_0' \oplus P_0''$ and consider the homomorphism $\pi = (\pi', \alpha) : P_0 \to M$, where α is a homomorphism $\alpha : P_0'' \to M$ such that $\psi\alpha = \pi''$. Then it is easy to verify that π is an epimorphism and that the following diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M_1' & \xrightarrow{\varphi_1} & M_1 & \xrightarrow{\psi_1} & M_1'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P_0' & \xrightarrow{f_0} & P_0 & \xrightarrow{g_0} & P_0'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \pi'} & & \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi''} & & \\
0 & \longrightarrow & M' & \xrightarrow{\varphi} & M & \xrightarrow{\psi} & M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

is commutative, where $M_1' = Ker\pi'$, $M_1 = Ker\pi$ and $M_1'' = Ker\pi''$. Moreover, all columns and all rows of this diagram are exact. Therefore we may apply the

same construction to the first row. Continuing this process we obtain the required exact sequence of resolutions.

Lemma 6.2.6. *Suppose*

$$0 \to \mathbf{S}' \longrightarrow \mathbf{S} \longrightarrow \mathbf{S}'' \longrightarrow 0$$

is an exact sequence of complexes, where all modules S''_n are projective, then the sequence

$$0 \to F\mathbf{S}' \longrightarrow F\mathbf{S} \longrightarrow F\mathbf{S}'' \longrightarrow 0$$

is exact for every functor F.

Proof. Since every sequence $0 \to S'_n \longrightarrow S_n \longrightarrow S''_n \longrightarrow 0$ splits, the sequence $0 \to F(S'_n) \longrightarrow F(S_n) \longrightarrow F(S''_n) \longrightarrow 0$ also splits for every functor F.

Applying lemma 6.2.5, lemma 6.2.6 and theorem 6.1.1 we obtain the following important theorem about long exact sequences:

Theorem 6.2.7. *Suppose*

$$0 \to M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$$

is an exact sequence of modules. Then for any functor F there is a sequence of homomorphisms $\delta_n : L_nF(M'') \to L_{n-1}F(M')$ such that the following sequence

$$... \longrightarrow L_{n+1}F(M'') \xrightarrow{\delta_{n+1}} L_nF(M') \xrightarrow{L_nF(\varphi)} L_nF(M) \xrightarrow{L_nF(\psi)}$$

$$\xrightarrow{L_nF(\psi)} L_nF(M'') \xrightarrow{\delta_n} L_{n-1}F(M') \xrightarrow{L_{n-1}F(\varphi)} L_{n-1}F(M) \longrightarrow ...$$

is exact.

6.3. THE FUNCTOR TOR

We apply the construction of derived functors considered in the previous section to the functors $* \otimes_A Y$, and $X \otimes_A *$. Since they are right exact covariant functors, it is natural to consider left derived functors by means of projective resolutions.

Definition. Let X, Y be A-modules and $F = * \otimes_A Y$, then by definition $Tor_n^A(*, Y) = L_nF$. In particular,

$$Tor_n^A(X, Y) = H_n(\mathbf{P} \otimes_A Y) = Ker(d_n \otimes 1)/Im(d_{n+1} \otimes 1),$$

where $\mathbf{P}$:

$$... \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \to X \to 0$$

is a projective resolution of the A-module X.

In view of proposition 6.2.3, the definition of $Tor_n^A(X,Y)$ is independent of the choice of a projective resolution of X. It is easy to see that $Tor_n^A(*,Y)$ is an additive covariant functor.

Analogously we can introduce the functors $Tor_n^A(X,*)$ as the left derived functors of the functor $F = * \otimes_A Y$, i.e., $Tor_n^A(X,*) = L_nF$. In particular,

$$Tor_n^A(X,Y) = H_n(X \otimes_A \mathbf{P}) = Ker(d_n \otimes 1)/Im(d_{n+1} \otimes 1),$$

where $\mathbf{P}$:

$$... \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \to Y \to 0$$

is a projective resolution of an A-module Y.

$Tor_n^A(X,*)$ is also an additive covariant functor.

So we have two different constructions for $Tor_n^A(X,Y)$ and there arises the natural question: whether the value of $Tor_n^A(X,*)$ on Y is the same as the value of $Tor_n^A(*,Y)$ on X? It is remarkable fact that this is actually true, i.e., these two constructions give the same result:

Theorem 6.3.1. *For any right A-module X and any left A-module Y, and each $n \geq 0$ we have*:

$$H_n(X \otimes_A \mathbf{P}) = H_n(\mathbf{P}' \otimes_A Y),$$

where $\mathbf{P}$ is a projective resolution of Y and $\mathbf{P}'$ is a projective resolution of X.

We leave the proof of this statement to the reader. Alternatively consult one of the standard books on homological algebra such as *S.MacLane, Homology, Springer, 1963* or *Charles A.Weibel, An introduction to homological algebra, Cambr. Univ. P., 1994*, where there are different proofs of this fact.

The common value of these two derived functors as defined in theorem 6.3.1 is denoted by $Tor_n^A(X,Y)$.

Since the functor $X \otimes_A Y$ is right exact in both variables, from proposition 6.2.4 it immediately follows that:

Proposition 6.3.2. *$Tor_0^A(X,Y)$ is naturally equivalent to $X \otimes_A Y$.*

Since in the definition of $Tor_n^A(X,Y)$ we use projective resolutions, i.e., complexes which are 0 for $n < 0$, we have the following statement:

Proposition 6.3.3. *If n is negative, $Tor_n^A(X,Y) = 0$ for all X, Y.*

As a corollary to theorem 6.2.7 we can obtain the following important statement.

Theorem 6.3.4. *Suppose $0 \to X' \to X \to X'' \to 0$ is an exact sequence of A-modules. Then for all A-modules Y there is a long exact sequence*

$$... \to Tor_{n+1}^A(X'',Y) \xrightarrow{\delta_{n+1}} Tor_n^A(X',Y) \to Tor_n^A(X,Y) \to$$

$$\to Tor_n^A(X'',Y) \xrightarrow{\delta_n} ... \to Tor_1^A(X,Y) \to Tor_1^A(X'',Y) \to$$
$$\to X' \otimes_A Y \to X \otimes_A Y \to X'' \otimes_A Y \to 0;$$

and similarly in the other variable.

Proposition 6.3.5. *If P is projective, then $Tor_n^A(P,Y) = 0$ for all Y and for all $n > 0$. Similarly, $Tor_n^A(X,P) = 0$ for all X and for all $n > 0$.*

Proof. Since the $Tor_n^A(P,Y)$ are independent of the choice of a projective resolution of P, we can choose the following projective resolution of P:

$$... \to 0 \longrightarrow 0 \longrightarrow P \xrightarrow{1_P} P \longrightarrow 0$$

Hence $Tor_n^A(P,Y) = 0$ for any Y and all $n > 0$.

Proposition 6.3.6. *If X is a flat A-module, then $Tor_n^A(X,Y) = 0$ for all Y and for all $n > 0$.*

Proof. Let

$$... \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\pi} Y \longrightarrow 0$$

be a projective resolution of Y. If X is flat and $n \geq 1$, then the sequence

$$X \otimes_A P_{n+1} \longrightarrow X \otimes_A P_n \longrightarrow X \otimes_A P_{n-1}$$

is exact, since $X \otimes_A *$ is an exact functor. Hence $Tor_n^A(X,Y) = 0$ for any Y and all $n > 0$.

Proposition 6.3.7. *If $Tor_1^A(X,Y) = 0$ for all Y, then X is flat.*

Proof. If $0 \longrightarrow Y' \xrightarrow{\alpha} Y \longrightarrow Y'' \longrightarrow 0$ is exact, then so is the sequence:

$$Tor_1^A(X,Y'') \longrightarrow X \otimes_A Y' \xrightarrow{1\otimes\alpha} X \otimes_A Y$$

Since $Tor_1^A(X,Y'') = 0$, $1 \otimes \alpha$ is a monomorphism and so X is flat.

Proposition 6.3.8. *If $0 \longrightarrow X' \longrightarrow X \longrightarrow X'' \longrightarrow 0$ is exact with X flat, then $Tor_n^A(X',Y) \simeq Tor_{n+1}^A(X'',Y)$ for all Y and $n > 0$.*

Proof. Since X is flat, we have an exact sequence:

$$0 = Tor_{n+1}^A(X,Y) \longrightarrow Tor_{n+1}^A(X'',Y) \longrightarrow Tor_n^A(X',Y) \longrightarrow Tor_n^A(X,Y) = 0$$

Hence, $Tor_n^A(X',Y) \simeq Tor_{n+1}^A(X'',Y)$.

Proposition 6.3.9. *Suppose Y is a left A-module and $Tor_1^A(A/\mathcal{I},Y) = 0$ for every finitely generated right ideal $\mathcal{I}$. Then Y is flat.*

Proof. Consider the short exact sequence $0 \longrightarrow \mathcal{I} \longrightarrow A \longrightarrow A/\mathcal{I} \longrightarrow 0$ and apply theorem 6.3.4 to it. Then we have an exact sequence $0 = Tor_1^A(A/\mathcal{I}, Y) \longrightarrow \mathcal{I} \otimes_A Y \longrightarrow A \otimes_A Y \simeq Y$. Hence, by the flatness test (proposition 5.4.9), Y is flat.

6.4. THE FUNCTOR EXT

In this section we apply the construction of derived functors to the functors $Hom_A(*, Y)$ and $Hom_A(X, *)$ and consider the properties of these functors.

For the contravariant left exact functor $Hom_A(*, Y)$ we consider right derived functors using projective resolutions.

Definition. Let X, Y be A-modules and $F = Hom_A(*, Y)$, then $Ext_A^n(*, Y) = R^n F$. In particular,

$$Ext_A^n(X, Y) = H_{-n}(Hom_A(\mathbf{P}, Y)) = KerHom(d_{n+1}, Y)/ImHom(d_n, Y),$$

where $\mathbf{P}$:

$$... \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \to X \to 0$$

is a projective resolution of the A-module X.

In view of proposition 6.2.3, the definition of $Ext_A^n(X, Y)$ is independent of the choice of a projective resolution of X. It is easy to see that $Ext_A^n(*, Y)$ is an additive contravariant functor.

For the covariant left exact functor $Hom_A(X, *)$ we consider right derived functors using injective resolutions.

Definition. Let X, Y be A-modules and $F = Hom_A(X, *)$, then $Ext_A^n(X, *) = R^n F$. In particular,

$$Ext_A^n(X, Y) = H_{-n}(Hom_A(X, \mathbf{Q})) = KerHom(X, d_n)/ImHom(X, d_{n-1}),$$

where $\mathbf{Q}$:

$$0 \to Y \to Q_0 \xrightarrow{d_0} Q_1 \xrightarrow{d_1} Q_2 \to ...$$

is an injective resolution of an A-module Y.

$Ext_A^n(X, *)$ is also an additive covariant functor and it is independent of the choice of an injective resolution of Y.

As in the case of the functor Tor we have the following remarkable fact:

Theorem 6.4.1. *For any right A-modules X and Y, and each $n \geq 0$ we have*:

$$H_{-n}(Hom_A(X, \mathbf{Q})) = H_{-n}(Hom_A(\mathbf{P}, Y)),$$

where $\mathbf{P}$ is a projective resolution of X and $\mathbf{Q}$ is an injective resolution of Y.

The common value of these two derived functors as defined in theorem 6.4.1 is denoted by $Ext_n^A(X, Y)$.

Since the functor $Hom_A(X,Y)$ is left exact in both variables, from proposition 6.2.4 there immediately follows the following statement:

Proposition 6.4.2. *$Ext^0_A(X,Y)$ is naturally equivalent to $Hom_A(X,Y)$.*

From the construction of the functor Ext we obtain immediately the following statement:

Proposition 6.4.3. *If n is negative, $Ext^n_A(X,Y) = 0$ for all X, Y.*

As a corollary of theorem 6.3.4 we obtain the following two statements:

Theorem 6.4.4. *If $0 \longrightarrow Y' \longrightarrow Y \longrightarrow Y'' \longrightarrow 0$ is an exact sequence of modules, then there exists a long exact sequence*

$$0 \longrightarrow Hom_A(X,Y') \longrightarrow Hom_A(X,Y) \longrightarrow Hom_A(X,Y) \longrightarrow Ext^1_A(X,Y) \longrightarrow ...$$

$$... \longrightarrow Ext^n_A(X,Y') \longrightarrow Ext^n_A(X,Y) \longrightarrow Ext^n_A(X,Y'') \longrightarrow Ext^{n+1}_A(X,Y') \longrightarrow ...$$

Theorem 6.4.5. *If $0 \longrightarrow X' \longrightarrow X \longrightarrow X'' \longrightarrow 0$ is an exact sequence of modules, then there exists a long exact sequence*

$$0 \longrightarrow Hom_A(X'',Y) \longrightarrow Hom_A(X,Y) \longrightarrow Hom_A(X',Y) \longrightarrow Ext^1_A(X'',Y) \longrightarrow ...$$

$$... \longrightarrow Ext^n_A(X'',Y) \longrightarrow Ext^n_A(X,Y) \longrightarrow Ext^n_A(X',Y) \longrightarrow Ext^{n+1}_A(X'',Y) \longrightarrow ...$$

Proposition 6.4.6. *If P is projective, then $Ext^n_A(P,Y) = 0$ for all Y and all $n > 0$.*

Proof. Since the $Ext^n_A(P,Y)$ are independent of the choice of a projective resolution of P, we can choice the following projective resolution of P:

$$... \to 0 \longrightarrow 0 \longrightarrow P \xrightarrow{1_P} P \longrightarrow 0$$

Hence, $Ext^n_A(P,Y) = 0$ for any Y and all $n > 0$.

Analogously there is the following statement:

Proposition 6.4.7. *If Q is injective, then $Ext^n_A(X,Q) = 0$ for all X and all $n > 0$.*

Proposition 6.4.8. *Suppose $0 \longrightarrow Y \longrightarrow Q \longrightarrow Y' \longrightarrow 0$ is an exact short sequence of A-modules with Q injective. Then $Ext^n_A(X,Y') \simeq Ext^{n+1}_A(X,Y)$ for all A-modules X and $n > 0$.*

Proof. Since Q is injective, by the previous proposition $Ext^n_A(X,Q) = 0$, and by theorem 6.4.4 we have an exact sequence

$$0 = Ext^n_A(X,Q) \longrightarrow Ext^n_A(X,Y') \longrightarrow Ext^{n+1}_A(X,Y) \longrightarrow Ext^{n+1}_A(X,Q) = 0.$$

Hence, $Ext^n_A(X,Y') \simeq Ext^{n+1}_A(X,Y)$ for all A-modules X and $n>0$.

Proposition 6.4.9. *Suppose Y is an A-module. The following conditions are equivalent:*
1) *X is projective.*
2) *$Ext^n_A(X,Y)=0$ for all Y and all $n>0$.*
3) *$Ext^1_A(X,Y)=0$ for all Y.*

Proof.
1) $\Rightarrow$ 2) is proposition 6.4.6.
2) $\Rightarrow$ 3) is trivial.
3) $\Rightarrow$ 1) Consider an exact sequence $0 \longrightarrow Y \longrightarrow Y' \longrightarrow Y'' \longrightarrow 0$. Then, by theorem 6.4.4, we have an exact sequence:

$$0 \longrightarrow Hom_A(X,Y) \longrightarrow Hom_A(X,Y') \longrightarrow Hom_A(X,Y'') \longrightarrow Ext^1_A(X,Y)=0,$$

i.e., $Hom_A(X,*)$ is an exact functor. Hence, by proposition 5.1.1, X is projective.

Dually we have the following statement:

Proposition 6.4.10. *Suppose X is an A-module. The following conditions are equivalent:*
1) *Y is injective.*
2) *$Ext^n_A(X,Y)=0$ for all X and all $n>0$.*
3) *$Ext^1_A(X,Y)=0$ for all X.*

Proposition 6.4.11. *If A is a right hereditary ring, then $Ext^n_A(X,Y)=0$ for all right A-modules X, Y and all $n \geq 2$.*

Proof. For each right A-module X there is an exact sequence

$$0 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow X \longrightarrow 0 \tag{6.4.1}$$

where P_0 is projective. Since A is right hereditary, P_1 is also projective. Hence the sequence 6.4.1 is a projective resolution of X, i.e., $P_n=0$ for $n \geq 2$ and so that $Ext^n_A(X,Y)=0$ for all $n \geq 2$.

6.5. PROJECTIVE AND INJECTIVE DIMENSIONS

In this section we introduce some notions which measure how far a module is from being projective (or injective).

Definition. Let A be a ring and M be a right A-module. We say that the **projective dimension** of M is equal to n and write $proj.dim_A M = n$ if there is a projective resolution of length n:

$$0 \longrightarrow P_n \longrightarrow ... \longrightarrow P_1 \longrightarrow P_0 \longrightarrow X \longrightarrow 0 \tag{6.5.1}$$

and there is no shorter one.

We set $proj.dim_A M = \infty$ if there is no finite length resolution.

Example 6.5.1.
$proj.dim_A M = 0$ if and only if M is projective.

Example 6.5.2.
If A is a right hereditary ring, $proj.dim_A M \leq 1$ for any right A-module M.

From the definition of projective dimension we have immediately the following simple statements, which we formulate as propositions for later reference:

Proposition 6.5.1. *Let* $0 \longrightarrow L \longrightarrow P \longrightarrow M \longrightarrow 0$ *be an exact sequence with a projective module* P. *If* M *is not projective, then* $proj.dim_A M = proj.dim_A L + 1$.

Proposition 6.5.2. *Let*

$$0 \longrightarrow L \longrightarrow P_{k-1} \longrightarrow ... \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

be an exact sequence with projective modules P_0,.P_1,..., P_{k-1}. *If* $proj.dim_A M \geq k$, *then* $proj.dim_A M = proj.dim_A L + k$.

Lemma 6.5.3 *Let*

$$... \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\pi} X \longrightarrow 0 \tag{6.5.1}$$

be a projective resolution of an A*-module* X. *Then for all modules* Y $Ext_A^{n+1}(X, Y) \simeq Ext_A^1(Kerd_{n-1}, Y)$.

Proof. Since $Ext_A^{n+1}(X, Y)$ is computed by using the projective resolution (6.5.1) of X and $Ext_A^n(Kerd_0, Y)$ is computed by using the projective resolution of $Kerd_0$ where $d_0 = \pi$:

$$... \longrightarrow P_k \longrightarrow P_{k-1} \longrightarrow ... \longrightarrow P_1 \longrightarrow Kerd_0 \longrightarrow 0,$$

so $Ext_A^{n+1}(X, Y) \simeq Ext_A^n(Kerd_0, Y)$. Using the iteration process we obtain:

$$Ext_A^{n+1}(X, Y) \simeq Ext_A^n(Kerd_0, Y) \simeq Ext_A^{n-1}(Kerd_1, Y) \simeq ... \simeq Ext_A^1(Kerd_{n-1}, Y)$$

Proposition 6.5.4. *The following conditions are equivalent for a right* A*-module* X:

1) $proj.dim_A X \leq n$;
2) $Ext_A^k(X, Y) = 0$ *for all modules* Y *and all* $k \geq n + 1$;
3) $Ext_A^{n+1}(X, Y) = 0$ *for all modules* Y;
4) *for any projective resolution of* X, $Kerd_{n-1}$ *is a projective module.*

Proof.

1) $\Rightarrow$ 2). By the definition of projective dimension, there is a projective resolution of length n, i.e., $P_k = 0$ for all $k \geq n+1$. Hence $Ext^k_A(X,Y) = 0$ for all modules Y and all $k \geq n+1$.

2) $\Rightarrow$ 3) is trivial.

3) $\Rightarrow$ 4) Consider a projective resolution of X

$$... \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\pi} X \longrightarrow 0$$

By lemma 6.5.3, $Ext^{n+1}_A(X,Y) \simeq Ext^1_A(Kerd_{n-1}, Y)$, therefore $Ext^1_A(Kerd_{n-1}, Y) = 0$ for all Y. Then, by proposition 6.4.9, $Kerd_{n-1}$ is projective.

4) $\Rightarrow$ 1). Consider the projective resolution (6.5.1) of X. Then we have an exact sequence

$$0 \longrightarrow Kerd_{n-1} \longrightarrow P_{n-1} \longrightarrow ... \longrightarrow P_1 \longrightarrow P_0 \longrightarrow X \longrightarrow 0$$

with projective modules P_0,.P_1,..., P_{n-1}, $Kerd_{n-1}$. Hence $proj.dim_A X \leq n$.

Analogously we can introduce the notion of injective dimension.

Definition. Let A be a ring and M be a right A-module. We say that the **injective dimension** of M is equal to n and write $inj.dim_A M = n$ if there is a injective resolution of length n:

$$0 \longrightarrow M \longrightarrow Q_0 \longrightarrow ... \longrightarrow Q_{n-1} \longrightarrow Q_n \longrightarrow 0 \qquad (6.5.2)$$

and there is no shorter one .

Dual to the results pertaining to projective dimension we can obtain the following statements:

Proposition 6.5.5. *Let* $0 \longrightarrow M \longrightarrow Q \longrightarrow N \longrightarrow 0$ *be an exact sequence with an injective module* Q. *If* M *is not injective, then* $inj.dim_A M = inj.dim_A N + 1$.

Proposition 6.5.6. *Let*

$$0 \longrightarrow M \longrightarrow Q_0 \longrightarrow ... \longrightarrow Q_{k-1} \longrightarrow N \longrightarrow 0$$

be an exact sequence with injective modules Q_0,.Q_1,..., Q_{k-1}. *If* $inj.dim_A M \geq k$, *then* $inj.dim_A M = inj.dim_A L + k$.

Lemma 6.5.7. *Let*

$$0 \longrightarrow X \xrightarrow{\epsilon} Q_0 \xrightarrow{d_0} Q_1 \xrightarrow{d_1} Q_2 \longrightarrow ...$$

be an injective resolution of A*-module* X. *Then for all modules* Y

$$Ext^{n+1}_A(X,Y) \simeq Ext^1_A(X, Imd_{n-1})$$

Proposition 6.5.8. *The following conditions are equivalent for a right A-module X:*

1) $inj.dim_A X \leq n$;
2) $Ext^k_A(X,Y) = 0$ *for all modules* Y *and all* $k \geq n+1$;
3) $Ext^{n+1}_A(X,Y) = 0$ *for all modules* Y;
4) *for any injective resolution of* X Imd_{n-1} *is an injective module.*

6.6. GLOBAL DIMENSIONS

We now can define dimensions for a ring A itself.

Definition. If A is a ring, then its **right projective global dimension**, abbreviated as *r.proj.gl.dim*, is defined as follows:

$$r.proj.gl.dim A = sup\{proj.dim_A M : M \in \mathbf{M}_A\}$$

Analogously we can introduce the **left projective global dimension** of A:

$$l.proj.gl.dim A = sup\{proj.dim_A M : M \in {}_A\mathbf{M}\}$$

Theorem 6.5.4 immediately implies:

Corollary 6.6.1. $r.proj.gl.dim A \leq n$ *if and only if* $Ext^{n+1}_A(X,Y) = 0$ *for all right A-modules* X *and* Y.

Proposition 6.6.2. $r.proj.gl.dim A = 0$ *if and only if A is semisimple.*

Proof. By corollary 6.6.1, $r.proj.gl.dim A = 0$ if and only if $Ext^1_A(X,Y) = 0$ for all right A-modules X and Y. This means, by proposition 6.4.9, that all right A-modules are projective and hence, by theorem 5.2.13, A is a semisimple ring.

Proposition 6.6.3. $r.proj.gl.dim A \leq 1$ *if and only if A is right hereditary.*

Proof. Sufficiency is theorem 6.4.11.

Conversely, suppose $r.proj.gl.dim A \leq 1$. Let X be a submodule of a right projective A-module P. Then we have an exact sequence

$$0 \longrightarrow X \longrightarrow P \longrightarrow Y \longrightarrow 0,$$

where $Y = P/X$. In a usual way we can construct a projective resolution of Y with $Ker d_0 = X$. By hypothesis, $r.proj.gl.dim A \leq 1$, so, by theorem 6.5.4, the right A-module X is projective. Hence, by proposition 5.5.3, A is a right hereditary ring.

Dually we can define right injective global dimension of a ring.

Definition. If A is a ring, then its **right injective global dimension**, abbreviated as $r.inj.gl.dim$, is defined as follows:

$$r.inj.gl.dimA = sup\{inj.dim_A M : M \in \mathbf{M}_A\}$$

Analogously we can introduce the **left injective global dimension** of A:

$$l.inj.gl.dimA = sup\{inj.dim_A M : M \in {}_A\mathbf{M}\}$$

Theorem 6.5.4 immediately implies:

Corollary 6.6.4. *$r.inj.gl.dimA \leq n$ if and only if $Ext_A^{n+1}(X, Y) = 0$ for all right A-modules X and Y.*

Comparing corollary 6.6.1 and 6.6.4 we obtain:

Theorem 6.6.5. *For any ring A $r.proj.gl.dimA = r.inj.gl.dimA$.*

In view of this theorem we can define the **right global dimension** of a ring A, abbreviated as $r.gl.dim$, as the common value of $r.proj.gl.dimA$ and $r.inj.gl.dimA$. If we consider left A-modules, then analogously we can define the **left global dimension** of a ring A. From propositions 6.6.2, 6.6.3 and theorem 6.6.5 we immediately obtain the following proposition:

Proposition 6.6.6.
1. *$r.gl.dim = 0$ if and only if A is semisimple.*
2. *$r.gl.dim \leq 1$ if and only if A is right hereditary.*

Remark. As follows from the example of Herstein-Small rings, considered in section 5.6, $r.gl.dim \neq l.gl.dim$ in general. However, as proved by M.Auslander (1955), equality holds in the case when the ring is right and left Noetherian.

6.7. NOTES AND REFERENCES

Homological algebra mainly studies derived functors on various categories. The first steps in studying fundamental algebraic objects by homological methods were made in the papers of S.Eilenberg, S.MacLane, and independently in a paper of D.K.Faddeev (see *On quotient systems in Abelian groups with operators // Dokl. Acad. Nauk SSSR, v.58, N3 (1947), p.361-364 (in Russian)*).

Cohomology and homology groups occur in many areas of mathematics. The formal notions of homology and cohomology groups arose from algebraic topology around the middle of the 20-th century in the study of relations between the higher homotopy groups and the fundamental group of a topological space.

Resolutions (without these names) were used long before by D.Hilbert (see, for example, *Über die Theorie der Algebraischen Formen // Math. Ann., v.36*

(1890), p.473-534). They were also used by H.Hopf in describing homology groups (see, *Über die Bettischen Gruppen, die zu einer beliebigen Gruppe gehören // Comment. Math. Helv., v.17 (19944/1945), s.39-79)*) and by H.Cartan for the theory of cohomology groups (see *Séminaire de topologie algébrique, 1950-1951. (École Norm. Sup.), Paris, 1951*). The functor Ext^n was defined by means of resolutions by H.Cartan and S.Eilenberg (see, *H.Cartan, S.Eilenberg, Homological Algebra, Princeton Univ. Press., Princeton, New Jersey, 1956*). The functor Ext was also studied by N.Yoneda (see, *On the homology theory of modules // J. Fac. Sci. Tokyo, Sec.I, v.7 (1954), p. 193-227; Notes on product in Ext // Proc. AMC, v.9 (1958), p.873-875*).

The homological dimensions of modules and algebras were studied by many authors, for example, by H.Cartan and S.Eilenberg (see their book quoted above); by M.Auslander (see, *On the dimension of modules and algebras. (III). Global dimension // Nagoya Math. J., v.9 (1955), p.67-77*) and I.Kaplansky (see, *On the dimension of modules and algebras. X // Nagoya Math. J., v.13 (1958), p.85-88).* Homological dimension in Noetherian rings was studied by M.Auslander and D.A.Buchsbaum (see, for example, *Homological dimension in Noetherian rings // Proc. NAS USA, v.42 (1956), p.36-38*; *Homological dimension in Noetherian rings II // Trans. AMS, v.88 (1958), p.194-206*); by E.Matlis (see, *Injective modules over Noetherian rings // Pac. J. Math., v.8 (1958), p.511-528*) and by J.P.Jans (see, *Duality in Noetherian rings // Proc. AMS, (1961), p.829-835*).

7. Integral domains

The subject we are dealing with in this chapter is the theory of divisibility in some commutative domains with unique factorization. In fact, the most important notions of the theory of rings, such as the notions of an ideal and a ring, were introduced by R.Dedekind in connection with the problem of non-unique factorization of algebraic integers in algebraic number fields. The ring of integers $\mathbf{Z}$ is the main example of a ring with unique factorization of elements into primes. Another most important example of such rings is the ring of polynomials over a field. In this chapter we shall consider other examples of commutative rings with unique factorization, such as Euclidean rings and principal ideal domains. Our main goal will be to describe finitely generated modules over principal ideal domains. Specializing the principal ideal domain to be $\mathbf{Z}$, we shall also obtain the main structure theorem for finitely generated Abelian groups, and, hence, for finite Abelian groups.

The central concept of the axiomatic development of linear algebra is a vector space over a field. A central problem of linear algebra is the study of linear transformations in a finite dimensional vector space over a field. For the given linear transformation $\mathcal{A}$ in a vector space V over a field K we can use $\mathcal{A}$ to make V into a module over the polynomial ring $K[x]$ in one variable x. The study of this module leads to the theory of canonical forms of matrices of a linear transformation and to the solution of the similarity problem of matrices. In the last section we apply the structure theorem of finitely generated modules over a PID to obtain the decomposition of finitely generated modules over the polynomial ring $K[x]$ and, hence, canonical forms for square matrices.

All the rings considered in this chapter will be commutative with identity $1 \neq 0$. Denote by $\mathbf{N}$ the set of all natural numbers, i.e., the set of all (strictly) positive integers, and by A^* the set of all units (=invertible elements) of a ring A.

7.1 PRINCIPAL IDEAL DOMAINS

Let A be a commutative ring. Recall that a nonzero element $a \in A$ is called a **zero divisor** if there exists a nonzero element $b \in A$ such that $ab = 0$. An element $a \in A$ is called a **unit** (or a **divisor of the identity**) if there exists an element $c \in A$ such that $ac = 1$.

Definition. A commutative ring A is called an **integral domain** if it has no zero divisors.

Since all nonzero elements of any field k are units, a field contains no zero divisors and therefore is a domain. The other obvious examples of integral domains are the ring of integers $\mathbf{Z}$ and a ring of polynomials $k[x]$ over a field k. In this chapter we shall consider integral domains only. Therefore sometimes we shall say domain for short, instead of an integral domain. An integral domain A has an important property, which is usually called the **cancellation law of multiplication**. We give it as the following lemma:

Lemma 7.1.1. *Let A be an integral domain. Then $ax = ay$ implies $x = y$ for any nonzero $a \in A$ and $x, y \in A$.*

Proof. If $ax = ay$, then the ring axioms give $a(x - y) = 0$. Therefore, since a is not a zero divisor, we must have $x - y = 0$. Hence, $x = y$.

Let A be a domain and let $a, b \in A$ be nonzero elements. If there exists a nonzero element $c \in A$ such that $b = ac$, we say that a is a **divisor** of b, or that a **divides** b, and we write $a|b$ or $b \equiv 0(mod\ a)$. If $b = ac$ and c is not a unit, then a is called a **proper divisor** of b.

If $\varepsilon \in A$ is a unit and $a \in A$, then there is always the factorization $a = \varepsilon(\varepsilon^{-1}a)$. Such factorization is considered inessential. Two elements a and b in a domain A are called **associated elements**, or simply **associates**, if there exists a unit $\varepsilon \in A$ such that $a = \varepsilon b$. In other words, two elements $a, b \in A$ are **associates**, if $a|b$ and $b|a$. It is obvious that being associates is an equivalence relation.

Definition. A nonzero element $p \in A$ is called **irreducible** if it is not a unit and every factorization $p = bc$ with $b, c \in A$ implies that either b or c is a unit in A.

In other words, any irreducible element is divisible only by units and its associates.

It is easy to verify the following proposition whose proof we leave to the reader.

Proposition 7.1.2. *Suppose A is a domain and $a, b \in A$. Then $a|b$ if and only if $(b) \subseteq (a)$. Moreover, $(a) = (b)$ if and only if a and b are associates. If a is a proper divisor of b in A, then $(a) \subset (b)$.*

Here (a) is the principal ideal generated by a.

Definition. A nonzero element $d \in A$ is called the **greatest common divisor** of two elements a and b if

1) $d|a$ and $d|b$;

2) if d_1 is a common divisor of both elements a and b, then $d_1|d$.

The greatest common divisor of elements a and b is denoted by (a, b). Clearly, (a, b) is defined uniquely up to a unit factor. And so, (a, b) is really a set, in which every two elements are associates.

Analogously we can introduce the greatest common divisor of n elements

$a_1, a_2, ..., a_n \in A$. We shall denote it as $d = (a_1, a_2, ..., a_n)$. In the ring $\mathbf{Z}$ any n nonzero elements have a greatest common divisor.

This fact is true for more general rings, in particular, for principal ideal domains. We recall, that an integral domain is said to be a **principal ideal domain** (or a PID for short), if each of its ideals is principal. As it was shown in chapter 1 the rings $\mathbf{Z}$ and $k[x]$ are principal ideal domains.

Proposition 7.1.3. *Let A be a principal ideal domain. Then*:

1) *for any nonzero elements $a_1, a_2, ..., a_n \in A$ there exists their greatest common divisor $d = (a_1, a_2, ..., a_n)$;*

2) *for any nonzero elements $a_1, a_2, ..., a_n \in A$ there exist elements $x_1, x_2, ..., x_n \in A$ such that $a_1x_1 + a_2x_2 + ... + a_nx_n = d$, where $d = (a_1, a_2, ..., a_n)$.*

Proof. Let $(a_1, a_2, ..., a_n)$ be the ideal generated by the elements a_1, a_2,..., a_n. Since A is a principal ideal domain, there exists an element $d \in A$ such that $(d) = (a_1, a_2, ..., a_n)$. Therefore there exist elements $x_1, x_2, ..., x_n \in A$ such that $a_1x_1 + a_2x_2 + ... + a_nx_n = d$. Since $a_i \in (d)$, there exist elements $t_i \in A$ such that $a_i = dt_i$ and so $d|a_i$ for $i = 1, 2, ..., n$. Let $d_1|a_i$ for $i = 1, 2, ..., n$. From $a_1x_1 + a_2x_2 + ... + a_nx_n = d$ it follows that $d_1|d$. Thus, d is a greatest common divisor of $a_1, a_2, ..., a_n$. The proposition is proved.

The elements $a_1, a_2, ..., a_n$ of a domain A are said to be **relatively prime** when $(a_1, a_2, ..., a_n) = 1$. From proposition 7.1.3 it follows that for relatively prime elements $a_1, a_2, ..., a_n \in A$ there exist elements $x_1, x_2, ..., x_n \in A$ such that $a_1x_1 + a_2x_2 + ... + a_nx_n = 1$.

Definition. A nonzero element p in a domain A is called **prime** if p is not a unit and $p|ab$ implies either $p|a$ or $p|b$.

Proposition 7.1.4. *Let A be an integral domain. Then any prime element $p \in A$ is irreducible.*

Proof. Let p be a prime element in a domain A. Then p is not a unit, by definition. Let $p = ab$ with $a, b \in A$. Then $p|ab$ and, by definition, either $p|a$ or $p|b$. In the first case there exists $c \in A$ such that $a = pc$. Then $p = pcb$ and by cancellation law $cb = 1$, i.e., b is a unit. Similarly, if $p|b$, then a is a unit. Therefore, p is irreducible.

In a general case the inverse statement is not true, but it is true for a principal integral domain. In particular, this is true for the ring of integers.

Proposition 7.1.5. *Let A be a PID. Then any irreducible element $p \in A$ is prime in A.*

Proof. Let p be an irreducible element in a PID A and let $p|ab$ for $a, b \in A$. Suppose that p does not divide a. Then $(p, a) = 1$ and, by proposition 7.1.2, there

exist $x, y \in A$ such that $1 = px + ay$. Consequently, $b = bpx + bay$ and since p divides the right side of the equality, $p|b$. So p is prime in A.

So, for a PID the notions of prime element and an irreducible element are the same thing. But in general these notions are different. Nevertheless, for some PIDs it is more convenient to use the term prime element (for example, for $\mathbf{Z}$), and in the other cases we prefer to use the term irreducible element (for example, for $k[x]$).

By induction on the number of factors, we can easily obtain the following statement:

Proposition 7.1.6. *Let A be a PID and $a_1, a_2, ..., a_n, p \in A$ such that $p \in A$ is prime and the $a_1, a_2, ..., a_n$ are nonzero elements. If $p|a_1a_2...a_n$, then there exists a k $(1 \leq k \leq n)$ such that $p|a_k$.*

7.2. FACTORIAL RINGS

As we know the ring of integers $\mathbf{Z}$ have an important property which is called the factorization property; that is, any nonzero element in $\mathbf{Z}$ has a factorization into prime integers, and this factorization is unique up to order and association of the factors. The ring of polynomials $k[x]$ over a field k has the same property. In this section we discuss the general class of rings with this property.

We say that a nonzero element a of a ring A has a **unique factorization into irreducible elements** $a = p_1...p_r$ if the $p_1, ..., p_r$ are irreducible elements in A, and this factorization is unique up to order and association of the factors, i.e., if we have two such factorizations $a = p_1....p_r = q_1...q_s$, then $r = s$ and after a suitable renumbering $p_i = \varepsilon_i q_i$, where the ε_i are units in A $(i = 1, ..., s)$.

Definition. An integral domain is called a **factorial ring** or a **unique factorization domain** (or a UFD for short), if every nonzero element, which is not a unit, has a unique factorization into irreducible elements.

The rings $\mathbf{Z}$ and $k[x]$ considered above are factorial rings.

One of the most important discoveries of the 19-th century is that not all number rings are factorial. In particular, the factorization into irreducible elements in some quadratic and cyclotomic fields is not necessarily unique.[1])

Consider a quadratic field K, that is an algebraic extension of degree 2 of the field of rational numbers $\mathbf{Q}$. Then there exists an element $\theta \in K$ such that $K = \mathbf{Q}(\theta)$ and θ is a root of a quadratic equation

$$f(x) = x^2 + ux + v,$$

[1]) The fact that factorization in cyclotomic fields is not necessarily unique was (and is) the main obstruction in proving Fermat's last theorem.The theorem is now proved of course (A.Wiles, R.Taylor, a.o). Had it been true that the cyclotomic fields have unique factorization a proof could (and would) have been written down a 150 years ago.

where $f(x) \in \mathbf{Q}[x]$. After a suitable substitution we can see to it that

$$f(x) = x^2 - D,$$

where $D \neq 1$, D is a square-free integer and so $K = \mathbf{Q}(\sqrt{D})$.

There is a non-identity automorphism of the field K given by:

$$\sqrt{D} \longmapsto -\sqrt{D}$$

which takes one root of the polynomial $f(x)$ to the other one. Therefore the field K has 2 different automorphisms and so it is a Galois extension of $\mathbf{Q}$ with a Galois group of the form $\mathcal{G} = \{1, \sigma\}$, where $\sigma(\sqrt{D}) = -\sqrt{D}$. Any element of the field K has the form

$$\alpha = a + b\sqrt{D},$$

where $a, b \in \mathbf{Q}$. The element $\alpha' = a - b\sqrt{D}$ is called the **conjugate** of the element α. It is easy to see that $(\alpha')' = \alpha$, $(\alpha_1 + \alpha_2)' = \alpha_1' + \alpha_2'$ and $(\alpha_1\alpha_2)' = \alpha_1'\alpha_2'$. For any element $\alpha \in K$ we can define the **norm** of α: $N(\alpha) = \alpha\alpha'$ and the **trace** of α: $Sp(\alpha) = \alpha + \alpha'$ which have the following properties[2]):

$$Sp(\alpha_1 + \alpha_2) = Sp(\alpha_1) + Sp(\alpha_2)$$

$$Sp(c\alpha) = cSp(\alpha) \quad \text{for any } c \in \mathbf{Q}$$

$$N(\alpha_1\alpha_2) = N(\alpha_1)N(\alpha_2)$$

$$N(\alpha) = 0 \quad \text{if and only if} \quad \alpha = 0.$$

An element $\alpha \in K$ is an **algebraic integer over $\mathbf{Q}$** if and only if $N(\alpha) \in \mathbf{Z}$ and $Sp(\alpha) \in \mathbf{Z}$.

Bellow we give some examples of domains which are not factorial rings.

Examples 7.2.1.

1. Let $A = \mathbf{Z}[\sqrt{-5}]$, i.e., the subset of complex numbers of the form $a + b\sqrt{-5}$, where $a, b \in \mathbf{Z}$. Clearly, $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. We shall show that, indeed, these are two different factorizations of the number 6 into irreducible elements of the ring $\mathbf{Z}[\sqrt{-5}]$.

In order to deal with factorization in $\mathbf{Z}[\sqrt{-5}]$ we use the norm from the field of complex numbers to $\mathbf{Q}$. For every element $\alpha = a + b\sqrt{-5}$ we set, as above, $\alpha' = a - \sqrt{-5}$ and $N(\alpha) = \alpha\alpha' = a^2 + 5b^2$. So N is a mapping from $\mathbf{Z}[\sqrt{-5}]$ to $\mathbf{N}$ and it is multiplicative, i.e., if α and β are elements of the ring $\mathbf{Z}[\sqrt{-5}]$, then $N(\alpha\beta) = N(\alpha)N(\beta)$. Note that $N(a + b\sqrt{-5}) = a^2 + 5b^2$. If $\alpha \in \mathbf{Z}[\sqrt{-5}]$ is a unit, it is immediate that $N(\alpha) = 1$. Consequently, ± 1 are the only units of $\mathbf{Z}[\sqrt{-5}]$. Therefore the numbers 2, 3, $1 + \sqrt{-5}$, $1 - \sqrt{-5}$ are not units. We shall show that these elements are irreducible. Assume, conversely, that $2 = \alpha\beta$. Then $4 = N(\alpha)N(\beta)$ and there are three possibilities for the norm of α: $N(\alpha) = 1$,

[2]) The notion "Sp" comes from "Spur", the German word for trace.

$N(\alpha) = 2$, $N(\alpha) = 4$. If $N(\alpha) = 1$, then $\alpha = \pm 1$ are units. If $N(\alpha) = 4$, then β is a unit. Finally, the equation $2 = a^2 + 5b^2$ has no integer solutions. Therefore, 2 is an irreducible element in $\mathbf{Z}[\sqrt{-5}]$. Similarly one can verify that the remaining elements are irreducible.

Also, it is not difficult to show that the elements $2, 3$ are not associates to the elements $1 + \sqrt{-5}, 1 - \sqrt{-5}$. Therefore the ring $\mathbf{Z}[\sqrt{-5}]$ is not factorial.

In a similar way it is easy to prove that all rings given below are not factorial. In each of these rings we indicate one counterexample for unique factorization.

2. In the ring $\mathbf{Z}[\sqrt{-6}]$ we have non-unique factorization into irreducible elements, in particular, $6 = 2 \cdot 3 = -\sqrt{-6} \cdot \sqrt{-6}$.

3. In the ring $\mathbf{Z}[\sqrt{10}]$ there are the equalities: $10 = 2 \cdot 5 = \sqrt{10} \cdot \sqrt{10}$.

4. In the ring $\mathbf{Z}[\sqrt{82}]$ we have the equalities: $-713 = -23 \cdot 21 = (5 + 3\sqrt{82}) \cdot (5 - 3\sqrt{82})$.

All examples quoted above are taken from the remarkable book on the theory of numbers *H.Hasse, Vorlesungen über Zahlentheorie, Berlin, 1950.*

The following example of a domain quoted below, which also is not a factorial ring, was considered by E.Matlis in his article: *The two generator problem for ideals // Michigan Math. J. 1970, v.17, N3, p.257-265.*

5. Let K_1 be the subring of $K[[x]]$ (the ring of formal series in one variable x over a field K), whose elements are formal series that have no linear term, i.e., every element of K_1 is of the form

$$\alpha = a_0 + a_2x^2 + a_3x^3 + ... + a_nx^n + ...$$

where $a_i \in K$, $i = 0, 2, 3, ...$ Obviously, K_1 is a domain and we have the following two different factorizations of x^6 into irreducible elements:

$$x^6 = x^3x^3 = x^2x^2x^2.$$

Theorem 7.2.1. *A principal ideal domain A is a factorial ring.*

Proof. First we shall show that any nonzero element of a ring A can be decomposed into prime factors. Suppose the contrary. Then there is a nonzero element $a \in A$ that cannot be decomposed into a product of prime elements. Then a is not prime itself and so there exist elements a_1, b_1 such that $a = a_1b_1$ and neither a_1 nor b_1 is a unit. Furthermore, since a cannot decomposed into a product of prime elements, then a_1 or b_1 (or both) cannot either. Without loss of generality we may assume that it is a_1. Since b_1 is not a unit, then, by proposition 7.1.2, $(a) \subset (a_1)$. Now since a_1 is not prime, there exist $a_2, b_2 \in A$ such that $a_1 = a_2b_2$ and neither a_2 nor b_2 is a unit. Once again, since a_1 cannot be written as a product of prime elements, then a_2 or b_2 (or both) cannot either. Without loss of generality we may assume that it is a_2. Since b_2 is not a unit then $(a_1) \subset (a_2)$. Continuing in the same way, we can build a family of ideals $\{(a_i) \mid i \in \mathbf{N}\}$ such that $(a_n) \subset (a_{n+1})$

(where the inclusions are strict). This contradicts proposition 1.1.4. Thus, any element of A can be written as a product of prime elements.

We shall show uniqueness of factorization into primes. Let $a = p_1...p_r = q_1...q_s$ be two factorizations of an element a into primes and let r be the least number of prime factors entering into factorizations of a. We shall proceed by induction on r. The base of induction $r = 1$ is trivial. Let $r > 1$. Since $p_1|q_1...q_s$, by proposition 7.1.6, there is an element q_j such that $p_1|g_j$. Renumbering the elements $q_1, ..., q_s$ one may assume that that $q_j = q_1$. Since q_1 is a prime element, $q_1 = \varepsilon_1 p_1$, where ε_1 is a unit. Applying the cancellation law we have $p_2...p_r = \varepsilon_1 q_2...q_s$. Now the induction hypothesis finishes the proof.

The following theorem yields an equivalent definition of a factorial ring.

Theorem 7.2.2. *Let $\mathcal{O}$ be an integral domain, in which any nonzero element, that is not a divisor of identity, is decomposable into a product of irreducible elements. Then the following conditions are equivalent:*

(1) *the ring $\mathcal{O}$ is factorial;*

(2) *any irreducible element $p \in \mathcal{O}$ is prime;*

(3) *for any irreducible element $p \in \mathcal{O}$ there are no divisors of zero in the quotient ring $\mathcal{O}/p\mathcal{O}$.*

Proof.

(1) $\Rightarrow$ (2). Let $p|ab$ and let $a = p_1...p_n$, $b = p_{n+1}...p_{n+m}$ be decompositions of the elements a and b into products of irreducible ones.

Therefore $p|p_1...p_np_{n+1}...p_{n+m}$, i.e., $pu = p_1...p_np_{n+1}...p_{n+m}$ for some $u \in \mathcal{O}$. Since the ring $\mathcal{O}$ is factorial, the irreducible element p is associated with one of the irreducible elements p_j $(j = 1, ..., n + m)$. So either $p|a$ or $p|b$.

(2) $\Rightarrow$ (3). If $(a + p\mathcal{O})(b + p\mathcal{O}) = p\mathcal{O}$, then $ab \in p\mathcal{O}$, i.e., $p|ab$. Then, by hypothesis, it follows that p divides either a or b, i.e., either a or b belongs to $p\mathcal{O}$.

(3) $\Rightarrow$ (1). Suppose that in the domain $\mathcal{O}$ we have two factorizations of a nonzero element, which is not a divisor of identity, into a product of irreducible elements:

$$p_1...p_n = q_1...q_m \tag{7.2.1}$$

Suppose, $m \leq n$. From the fact that $(q_1)(q_2...q_m) \in p_1\mathcal{O}$ it follows that either $q_1 \in p_1\mathcal{O}$ or $q_2...q_m \in p_1\mathcal{O}$. Therefore for some i the element $q_i \in p_1\mathcal{O}$, i.e., q_i is associated with p_1. Renumbering the elements $q_1, q_2, ..., q_m$ we can assume that $q_i = q_1$. Since $\mathcal{O}$ is a domain, we can cancel the factor p_1 on both sides of the equality (7.2.1). Using induction on m, after m steps we shall obtain an equality

$$p_{m+1}...p_n = \varepsilon_1...\varepsilon_m.$$

Since all p_i are irreducible elements, which are not units, it follows that $m = n$ and for any $i = 1, ..., m$ every irreducible element p_i is associated with some irreducible element q_i, i.e., the ring $\mathcal{O}$ is factorial.

Note that from this theorem it follows, in particular, that in a factorial ring the notions of a prime element and an irreducible element coincide.

In the previous section we have proved that any two elements of a principal ideal domain have a greatest common divisor. We shall show that this fact also holds in a factorial ring. Let a, b be nonzero elements of a factorial ring $\mathcal{O}$ and let $\{p_1, p_2, ..., p_n\}$ be the set of different prime elements of the ring $\mathcal{O}$ such that any prime factor of the elements a and b is associated with one and only one element of this set. Then the elements a and b can be written as

$$a = \varepsilon p_1^{r_1} ... p_n^{r_n}, \qquad b = \varepsilon' p_1^{s_1} ... p_n^{s_n} \tag{7.2.2}$$

where $\varepsilon, \varepsilon'$ are units of $\mathcal{O}$ and $r_i \geq 0$, $s_i \geq 0$ for $i = 1, ..., n$. If $c|a$ and $c|b$, then c can be written as $c = \varepsilon'' p_1^{t_1} ... p_n^{t_n}$, where ε'' is a unit of $\mathcal{O}$ and $t_i \geq 0$ for $i = 1, ..., n$. Then the greatest common divisor of a and b is the element $d = p_1^{k_1} ... p_n^{k_n}$, where $k_i = \min(r_i, s_i)$, $i = 1, ..., n$. Therefore any two elements of a factorial ring have a greatest common divisor. It is clear that this fact is also true for any finite number of elements of the ring $\mathcal{O}$, i.e., any finite number of elements $a_1, a_2, ..., a_n$ of a factorial ring have a greatest common divisor, which is unique up to a unit factor. We shall denote the greatest common divisor of the elements $a_1, a_2, ..., a_n$ by $d = (a_1, a_2, ..., a_n)$.

Now consider another useful notion for a ring $\mathcal{O}$. Let $a, b \in \mathcal{O}$. An element $m \in \mathcal{O}$ is called a **common multiple** of a and b if $m = aa_1 = bb_1$ for some $a_1, b_1 \in \mathcal{O}$. An element $m \in \mathcal{O}$ is called a **least common multiple** of a and b if m is a common multiple of a and b and in addition every common multiple of a and b is divisible by m. We shall denote the least common multiple of a and b by $m = [a, b]$.

Now let $\mathcal{O}$ be a factorial ring and a and b have factorizations as in (7.2.2). Then it is easy to see that the element $m = p_1^{k_1} ... p_n^{k_n}$, where $k_i = max(r_i, s_i)$, $i = 1, ..., n$, is a least common multiple of a and b. It is defined uniquely up to a unit factor. Therefore any two elements of a factorial ring have a least common multiple and this fact is also true for any finite number of elements of the ring $\mathcal{O}$, i.e., any finite number of elements $a_1, a_2, ..., a_n$ of a factorial ring have a least common multiple, which is unique up to a unit factor. We shall denote the least common multiple of the elements $a_1, a_2, ..., a_n$ by $m = [a_1, a_2, ..., a_n]$.

So we have the following statement.

Proposition 7.2.3. *Let a and b be two nonzero elements of a factorial ring $\mathcal{O}$. Let $a = \varepsilon p_1^{r_1} ... p_n^{r_n}$ and $b = \varepsilon' p_1^{s_1} ... p_n^{s_n}$ be prime factorizations of a and b, where the $\varepsilon, \varepsilon'$ are units and the $p_1, ..., p_n$ are distinct primes of $\mathcal{O}$. Then*

1. *The element $d = p_1^{k_1} ... p_n^{k_n}$, where $k_i = \min(r_i, s_i)$, $i = 1, ..., n$, is a greatest common divisor of a and b.*

2. *The element $m = p_1^{t_1} ... p_n^{t_n}$, where $t_i = \max(r_i, s_i)$, $i = 1, ..., n$, is a least common multiple of a and b.*

Remark. It is obvious that this statement is also true for any finite set of elements of a factorial ring.

7.3. EUCLIDEAN DOMAINS

As we know the ring of integers $\mathbf{Z}$ possesses a division algorithm, the socalled Euclidean algorithm. This algorithm can be stated formally for $\mathbf{Z}$ as follows:

Division algorithm. Let $a, b \in \mathbf{Z}\backslash\{0\}$. Then there exist unique $q, r \in \mathbf{Z}$ such that $b = aq + r$ and $0 \leq r < |a|$.

Here $|a|$ is the absolute value of a.

In this section we study the class of rings possessing a division algorithm. It is natural to call them Euclidean rings.

Definition. An integral domain A is called a **Euclidean domain** if there exists a map

$$\pi : A \to \mathbf{N} \cup \{0\}$$

satisfying the following conditions:

ED1. $\pi(0) = 0$;

ED2. Given $a \in A\backslash\{0\}$ and $b \in A$ there exist elements $r, g \in A$ such that $b = ga + r$, and either $r = 0$ or $\pi(r) < \pi(a)$.

The map π is called a **Euclidean function** on A. If $\pi(a) > 0$ for all $a \neq 0$, then π is called positive.

Note, there may be different Euclidean functions which make a given integral domain into a Euclidean domain.

Obvious examples of Euclidean domains are the rings $\mathbf{Z}$ and $k[x]$, where k is a field. In the first case $\pi(z) = |z|$ and in the second case $\pi(f(x)) = degf(x)$ is the degree of a polynomial $f(x)$.

Any field K is a trivial example of a Euclidean domain if we define $\pi(a) = 1$ for all $a \neq 0$ or define $\pi(a) = 0$ for all $a \neq 0$, $a \in K$.

Here is another example of a Euclidean domain. Denote by $\mathbf{Z}[i]$ the ring of all Gaussian integers, i.e., elements of the form $a + bi$, where $a, b \in \mathbf{Z}$ and $i^2 = -1$.

Define the map $\pi : \mathbf{Z}[i] \to \mathbf{N} \cup \{0\}$ by $\pi(a + bi) = a^2 + b^2$. We propose to the reader to verify that the ring $\mathbf{Z}[i]$ with this function π is Euclidean.

Theorem 7.3.1. *Any Euclidean domain A is a principal ideal domain.*

Proof. Let $\mathcal{I}$ be an ideal in a Euclidean ring A. If $\mathcal{I} = \{0\}$, then $\mathcal{I}$ is certainly principal. Therefore we may assume $\mathcal{I} \neq 0$. Let $0 \neq d \in \mathcal{I}$ be an element with the least value $\pi(d)$ among all nonzero elements in $\mathcal{I}$. We shall show that $\mathcal{I} = (d) = Ad$. Indeed, by **ED2**, for any $c \in \mathcal{I}$ we have $c = gd + r$, where $r = 0$ or $\pi(r) < \pi(d)$. If $r \neq 0$, then $r = c - gd \in \mathcal{I}$ and $\pi(r) < \pi(d)$, which contradicts

the choice of the element d. Therefore $r = 0$, and so $c = gd \in (d)$. The theorem is proved.

Note that the inverse statement is not always true. Not every principal ideal domain is Euclidean. Examples of such rings will be given below. From theorem 7.2.1 and 7.3.1 we have immediately the following statement:

Corollary 7.3.2. *Any Euclidean domain is a factorial ring.*

Thus, we may summarize the results obtained in these sections as the following chain of classes of rings:

$$(\textit{Euclidean domains}) \subset (\textit{ Principal ideal domains}) \subset (\textit{Factorial rings})$$

It can be shown that these inclusions are strict. First we shall show that there exist principal ideal domains that are not Euclidean. To this end we introduce a new notion that may be considered as a generalization of a Euclidean function.

Definition. Let A be an integral domain. A map $N : A \to \mathbf{N} \cup \{0\}$ satisfying the following conditions:

1) N is a positive norm, i.e., $N(a) = 0$ if and only if $a = 0$;

2) for every nonzero $a, b \in A$ either $b \in (a)$ or there exists a nonzero element $c \in (a, b)$ such that $0 < N(c) < N(a)$

is called a **Dedekind-Hasse norm** on A.

Remark. If A is an Euclidean domain with an Euclidean positive function π, then the Dedekind-Hasse conditions hold with $N = \pi$. Indeed, by condition **ED2**, for any $a, b \in A$ and $a, b \neq 0$, there exists an $r = b - ga \in (a, b)$ such that either $r = 0$, i.e., $b \in (a)$, or $\pi(c) < \pi(a)$.

Proposition 7.3.3. *An integral domain A is a principal ideal domain if and only if it has a Dedekind-Hasse norm.*

Proof. Let A is an integral domain which has a Dedekind-Hasse norm N. Let $\mathcal{I}$ be any nonzero ideal of A and let $a \in \mathcal{I}$ be an element with $N(a)$ minimal. Suppose $b \neq 0$ is any other element of $\mathcal{I}$. Then $(a, b) \subset \mathcal{I}$ and from the minimality property of a it follows that $b \in (a)$. So $\mathcal{I} = (a)$ is principal.

Conversely, suppose A is a principal ideal domain. Then A is a factorial ring. Define a norm N by setting $N(0) = 0$, $N(u) = 1$ if $u \in A^*$, and $N(a) = 2^n$ if $a = p_1 p_2 ... p_n$ is a factorization of a into prime elements p_i. This norm is well defined because we have a unique factorization in A. Obviously, $N(ab) = N(a)N(b)$. So, N is multiplicative and positive. We shall show that N is a Dedekind-Hasse norm. Let $a, b \in A$ and $a, b \neq 0$, then $(a, b) = (r)$ is a principal ideal. If $b \notin (a)$, then $r \notin (a)$ as well. Since $a \in (r)$, $a = rc$ for some $c \in A$. Then c is not a unit of A, because r does not divide a. So $N(a) = N(r)N(c) > N(r)$. Hence, N is a Dedekind-Hasse norm.

Example 7.3.1.

Just as in section 7.2 we consider a quadratic field $K = \mathbf{Q}(\sqrt{D})$ over the field of rational numbers $\mathbf{Q}$. We shall distinguish two cases: if $D < 0$ we have an imaginary quadratic field K, and if $D > 0$ we have a real quadratic field K.

It has been proved (see, for example the book of H.Hasse cited above, or the book *E.Weiss, Algebraic Number Theory, McGraw-Hill, 1963*) that only the imaginary quadratic fields $K = \mathbf{Q}(\sqrt{D})$ for $D = -11, -7, -3, -2, -1$ are Euclidean. So these fields have uniqueness of factorization. Besides these there exists an infinite number of real quadratic fields which are Euclidean. Among them are the fields $K = \mathbf{Q}(\sqrt{D})$ with $D = 2, 3, 5, 13$. So there exist real and imaginary quadratic fields which are not Euclidean. In particular, the imaginary quadratic field $K = \mathbf{Q}(\sqrt{-19})$ is not Euclidean. Consider the ring A of all algebraic integers of the field $K = \mathbf{Q}(\sqrt{-19})$. This is the ring A of all numbers of the form

$$\frac{a + b\sqrt{-19}}{2}$$

where $a, b \in \mathbf{Z}$ and $a \equiv b(mod 2)$. Define the positive norm $N(a+b(1+\sqrt{-19})/2) = a^2 + ab + 5b^2$. It can be show that N is a Dedekind-Hasse norm (see, for example, *J.C.Wilson, A principal ideal ring that is not a Euclidean ring // Math.Mag., v.46, pp.34-38, 1973;* or *D.S.Dummit, R.M.Foote, Abstract algebra, Printice Hall, Upper Saddle River, p.283*). So, by proposition 7.3.3, this ring is a principal ideal domain. But it is not a Euclidean ring, since it is a subring of the field $K = \mathbf{Q}(\sqrt{-19})$ which is not Euclidean and K is the quotient field of A.

Other examples of such rings are $\mathbf{Z}(\sqrt{-43})$, $\mathbf{Z}(\sqrt{-67})$, $\mathbf{Z}(\sqrt{-163})$.

An example of a real quadratic field, which is not Euclidean is the field $K = \mathbf{Q}(\sqrt{53})$. The ring $\mathbf{Z}(\sqrt{53})$ of algebraic integers of this field is a principal ideal domain but it is not Euclidean. (See, *H.Hasse, Vorlesungen über Zahlentheorie, Berlin, 1950*).

There are factorial rings which are not principal ideal domains. Examples of such rings shall be given in section 7.6.

7.4. RINGS OF FRACTIONS AND QUOTIENT FIELDS

In this section we shall show that any commutative ring A with regular elements can be embedded in a ring Q with identity such that any regular element of A is invertible in Q. In particular, any integral domain $\mathcal{O}$ can be embedded into a field k such that any element of the field k has the form ab^{-1}, where $a, b \in \mathcal{O}$ and $b \neq 0$.

Let A be a commutative ring. Recall that a nonzero element $a \in A$ is **regular** if it is not a zero divisor.

Definition. A nonempty subset S of a ring A is called a **multiplicative set** if for all $a, b \in S$ we have $ab \in S$. If, in addition, each element of S is regular, then

S is called a **regular multiplicative set**.

Examples 7.4.1.

1. The set of all regular elements of a ring A is a regular multiplicative set.
2. If A is an integral domain, then $S = A\backslash\{0\}$ is a regular multiplicative set.

Let A be a commutative ring and S be a multiplicative set. Consider the set $A \times S$ of all ordered pairs (a, b), where $a \in A$ and $b \in S$. Introduce on $A \times S$ the relation $(a, b) \sim (c, d)$ if and only if there exists an element $t \in S$ such that $t(ad - bc) = 0$. It is easy to verify that this is an equivalence relation. We denote by a/b or ab^{-1} the equivalence class of (a, b). The set of all equivalence classes is denoted by A_S. Note that all pairs $(0, b)$ form the class $0/b$ which is zero in A_S.

Introduce in the set A_S operations of addition and multiplication by the following rules:

$$a/b + a_1/b_1 = (ab_1 + ba_1)/bb_1 \tag{7.4.1}$$

and

$$(a/b)(a_1/b_1) = aa_1/bb_1. \tag{7.4.2}$$

It is easy to show that these operations are well defined in A_S, and that they are associative and commutative and that multiplication is distributive with respect to addition. The multiplicative identity in A_S is the class b/b for all $b \in S$. The checking of these facts is left to the reader. Thus, the set A_S with respect to addition and multiplication forms a ring.

So there is the following theorem (to be proved by the reader).

Theorem 7.4.1. *If A is a commutative ring and S is a multiplicative set, then A_S is a ring with identity.*

Definition. The ring A_S is called the **ring of fractions** of A with respect to S or the **localization** of A at S. If S consists of all regular elements of A, then A_S is called the **total quotient ring** of A.

Assigning to an element $a \in A$ the class $\varphi(a) = as/s$, where $a \in A$ and $s \in S$ is some fixed element, we obtain a natural homomorphism φ of the ring A into the ring A_S. In fact, if $a, b \in A$, then

$$\varphi(a + b) = (a + b)s/s = as/s + bs/s = \varphi(a) + \varphi(b)$$

$$\varphi(ab) = (ab)s/s = as/s \cdot bs/s = \varphi(a)\varphi(b)$$

Suppose $a \in Ker\varphi$, then $as/s = 0/s$ and $t(as^2 - 0s) = 0$ for some $t \in S$. Hence, $tas^2 = 0$, i.e., there exists $x = ts^2 \in S$ such that $ax = 0$. The converse is also true. Indeed, if $ax = 0$ for some $x \in S$, then $a \in Ker\varphi$. So, φ is a monomorphism if and only if $ax = 0$ for $a \in A$ and $x \in S$ implies $a = 0$.

Now consider the case, when S is the set of all regular elements of A. Then φ is a monomorphism. And we can identify any element $a \in A$ with the element $\varphi(a) = as/s$, where s is some element of S.

Suppose a is a regular element of the ring A and $\varphi(a) = as/s$. Then $s/as \in A_S$ is inverse to as/s, since $as \in S$ and $as/s \cdot s/as$ is the identity of A_S.

Finally, let $a/b \in A_S$, then $(a/b) = (as/s)(s/bs) = \varphi(a)[\varphi(b)]^{-1}$.

Thus, we have proved the following theorem.

Theorem 7.4.2. *Let A be a commutative ring with regular elements. Let S be a set of all regular elements of A. Then the total ring of fractions A_S has the following properties:*

1) *A is embedded in A_S.*

Regarding A as subring of A_S we have

2) *any regular element of A is invertible in A_S.*

3) *any element of A_S has the form ab^{-1}, where $a \in A$ and $b \in S$.*

Let $\mathcal{O}$ be an integral domain and $S = \mathcal{O}\backslash\{0\}$ be a set of all regular elements of $\mathcal{O}$. So S is a regular multiplicative set in $\mathcal{O}$ and from theorem 7.4.2 we obtain that in this case the ring $\mathcal{O}_S$ is a field, which is called the **quotient field** (or the **field of fractions**) of the ring $\mathcal{O}$.

Thus, we have the following statement.

Theorem 7.4.3. *For any integral domain $\mathcal{O}$ there is the quotient field k which has the following properties:*

1) *A is embedded in k.*

Regarding A as subring of k we have

2) *any nonzero element of A is invertible in A_S.*

3) *any element of k has the form ab^{-1}, where $a \in A$ and $b \neq 0$.*

Examples 7.4.2.

1. The field of rational numbers $\mathbf{Q}$ is the quotient field of the ring of integers $\mathbf{Z}$.

2. If k is a field, then its field of fractions is just k itself.

3. If $\mathcal{O}$ is an integral domain, then $\mathcal{O}[x]$ is also an integral domain. And its field of fractions is the field of rational functions in one variable x over $\mathcal{O}$ whose elements have the form $p(x)/q(x)$, where $p(x), q(x) \in \mathcal{O}[x]$ and $q(x) \neq 0$.

Definition. An ideal $\mathcal{P}$ of a commutative ring $\mathcal{O}$ is called **prime** if the quotient ring $\mathcal{O}/\mathcal{P}$ is an integral domain.

According to this definition an ideal $\mathcal{P}$ is prime if $\mathcal{P} \neq \mathcal{O}$ and for any $x, y \in \mathcal{O}$ from $xy \in \mathcal{P}$ it follows that either $x \in \mathcal{P}$ or $y \in \mathcal{P}$.

Definition. A ring A is called **local** if it has a unique maximal right ideal.

Proposition 7.4.4. *Let A be a commutative ring and $\mathcal{P}$ be a prime ideal in A. Then $S = A\backslash\mathcal{P}$ is a multiplicative set and A_S is a local ring with a unique maximal ideal $\mathcal{P}_S = \{a/s \mid a \in \mathcal{P}, s \notin S\}$.*

In this particular case this ring of fractions is called the **localization** at $\mathcal{P}$ and is denoted by $A_{\mathcal{P}}$.

Proof. First we shall show that S is a multiplicative set. Let $a, b \in S$, then $a \notin \mathcal{P}$, $b \notin \mathcal{P}$. Hence, since $\mathcal{P}$ is a prime ideal, $ab \notin \mathcal{P}$, i.e., $ab \in S$.

Now we shall show that $\mathcal{P}_S$ is an ideal in A_S. Let $a/s_1, b/s_2 \in \mathcal{P}_S$ and $r/s \in A_S$. Then

$$a/s_1 - b/s_2 = (as_2 - bs_1)/s_1 s_2 \in \mathcal{P}_S$$

$$(a/s_1)(r/s) = ar/s_1 s_2 \in \mathcal{P}_S$$

Hence, $\mathcal{P}_S$ is an ideal in A_S.

Finally, we shall show that $\mathcal{P}_S$ is the unique maximal ideal in A_S. Suppose $r/s \notin A_S \backslash \mathcal{P}_S)$, then $r \notin \mathcal{P}$. Therefore $s/r \in A_S$ and is invertible in A_S. Hence, all elements which not belong to $\mathcal{P}_S$ are invertible in A_S. Therefore $\mathcal{P}_S$ is the unique maximal ideal in A_S.

7.5. POLYNOMIAL RINGS OVER FACTORIAL RINGS

It is well known that the polynomial ring $k[x]$ over a field k is a factorial ring. We are going to prove that the ring of polynomials $k[x_1, ..., x_n]$ in n variables $x_1, ..., x_n$ over a field k is factorial as well. In fact, we shall prove the following, more general statement.

Theorem 7.5.1 (C.F.Gauss). *The polynomial ring $\mathcal{O}[x]$ over a factorial ring $\mathcal{O}$ is factorial.*

Let $\mathcal{O}$ be a factorial ring. First consider the main properties of the ring $\mathcal{O}[x]$. It is easy to see that the units of this ring can be only the units of the ring $\mathcal{O}$.

Recall that a polynomial $p(x) \in \mathcal{O}[x]$ is called **irreducible** if it is not a unit of the ring $\mathcal{O}[x]$ and from the equality $p(x) = f(x)g(x)$ it follows that either $f(x)$ or $g(x)$ is a unit of $\mathcal{O}[x]$. Also one can see that the ring $\mathcal{O}[x]$ has no divisors of zero, i.e., it is a domain. Therefore, all irreducible elements in $\mathcal{O}$ are also irreducible elements in $\mathcal{O}[x]$.

Lemma 7.5.2. *If an irreducible element of a factorial ring $\mathcal{O}$ divides a product of polynomials $f(x)$ and $g(x)$ of $\mathcal{O}[x]$, then it divides at least one of the factors.*

Proof. Let p be an irreducible element of a factorial ring $\mathcal{O}$. Consider the quotient ring $\mathcal{O}[x]/p\mathcal{O}[x]$. Clearly, it is isomorphic to the ring $\mathcal{O}_1[x]$, where $\mathcal{O}_1 = \mathcal{O}/p\mathcal{O}$. In view of theorem 7.2.2, $\mathcal{O}_1$ is a ring without divisors of zero. Since $p|f(x)g(x)$, it follows that $\bar{f}(x)\bar{g}(x) = \bar{0}$ (where $\bar{h}(x)$ is the image of the polynomial $h(x) \in \mathcal{O}[x]$ in the ring $\mathcal{O}_1[x]$). Because the ring $\mathcal{O}_1[x]$ is also without divisors of zero, we conclude that either $\bar{f}(x)$ or $\bar{g}(x)$ is equal to 0, i.e., either $f(x)$ or $g(x)$ is divisible by p.

Definition. Let $\mathcal{O}$ be a factorial ring. A polynomial $f(x) \in \mathcal{O}[x]$ is said to be **primitive** if the greatest common divisor of all its coefficients is a unit.

If $f(x) \in \mathcal{O}[x]$, then $f(x)$ can be written in the form $f(x) = cf_1(x)$, where $c \in \mathcal{O}$ and $f_1 \in \mathcal{O}[x]$ is primitive. We may choose the element c to be equal to the greatest common divisor of the coefficients of $f(x)$. The element c is determined uniquely up to a unit factor. It is called the **content** of $f(x)$ and denoted by $c(f)$. Note that $f(x)$ is primitive if and only if $c(f)$ is the unit element.

Denote by k the quotient field of the ring $\mathcal{O}$. It is well known that the ring $k[x]$ is a factorial ring. From the unique factorization in the ring $\mathcal{O}$ it follows that any element in k may be uniquely written in the form a/b, where a and b are mutually prime elements in $\mathcal{O}$, i.e., (a, b) is the unit element 1. Then any polynomial $f(x) \in k[x]$ can be written in the form: $f(x) = k_0x^n + k_1x^{n-1} + ... + k_n \in k[x]$, where $k_i = a_i/b_i$, $a_i, b_i \in \mathcal{O}$ and $b_i \in \mathcal{O}^*$. Let $d = (a_0, a_1, ..., a_n)$ be the greatest common divisor and $m = [b_0, b_1, ..., b_n]$ be the least common multiple. We define $c(f) = d/m$. The element $c(f) \in k$ is determined uniquely up to a unit factor and called the **content** of $f(x) \in k[x]$. Note that if $f(x) \in \mathcal{O}[x]$, then $c(f) \in \mathcal{O}$ and this notion coincides with the one defined above.

Lemma 7.5.3. *Let k be the quotient field of a factorial ring $\mathcal{O}$. Then any $f(x) \in k[x]$ is of the form $f(x) = c(f)f_1(x)$, where $f_1(x) \in \mathcal{O}[x]$ is a primitive polynomial.*

Proof. Let $f(x) \in k[x]$ and $f(x) = k_0x^n + k_1x^{n-1} + ... + k_n \in k[x]$, where $k_i = a_i/b_i$, $a_i, b_i \in \mathcal{O}$ and $b_i \in \mathcal{O}^*$. Let $d = (a_0, a_1, ..., a_n)$ be the greatest common divisor and $m = [b_0, b_1, ..., b_n]$ be the least common multiple. Then

$$mf(x) = a_0m/b_0x^n + a_1m/b_1x^{n-1} + ... + a_nm/b_n \in \mathcal{O}[x]$$

Since $a_i = dc_i$ for some $c_i \in \mathcal{O}$, $i = 0, 1, ..., n$, we have

$$mf(x) = d(c_0m/b_0x^n + c_1m/b_1x^{n-1} + ... + c_nm/b_n) = df_1(x),$$

where $f_1(x) \in \mathcal{O}[x]$ and $(c_0, c_1, ..., c_n)$ is 1. We shall prove that $f_1(x)$ is a primitive polynomial. Suppose $f_1(x)$ is not primitive. Then there exists a prime element $p \in \mathcal{O}$ such that p divides all coefficients c_im/b_i for $i = 0, 1, ..., n$. Since the elements m/b_i are relatively prime, i.e., $(m/b_0, m/b_1, ..., m/b_n)$ is 1, and $(c_0, c_1, ..., c_n)$ is 1, there exist $i \neq j$ such that $p|c_i$, while p does not divide m/b_i and $p|m/b_j$, while p does not divide c_j. Since (c_i, b_i) is 1, it follows that p does not divides b_i and, so, p does not divides m. Simultaneously, the same reasoning for for the index j show that $p|m$. A contradiction.

Lemma 7.5.4 (Gauss' lemma). *Let $\mathcal{O}$ be a factorial ring with quotient field k and $f(x), g(x) \in k[x]$. Then*

$$c(fg) = c(f) \cdot c(g). \tag{7.5.1}$$

In particular, the product of primitive polynomials is primitive.

Proof. We begin with the last statement. Let $f(x)$ and $g(x)$ be primitive polynomials of $\mathcal{O}[x]$. Then from lemma 7.5.2 it follows immediately that their product $f(x)g(x)$ is also primitive.

By lemma 7.5.3 we can write polynomials $f(x), g(x) \in k[x]$ in the form $f(x) = c(f)f_1(x)$ and $g(x) = c(g)g_1(x)$, where $f_1(x), g_1(x) \in \mathcal{O}[x]$ are primitive. Then $f(x)g(x) = c(f)c(g)f_1(x)g_1(x)$. Since $f_1(x)g_1(x)$ is primitive, we obtain the required equality (7.5.1).

Corollary 7.5.5. *Let $\mathcal{O}$ be a factorial ring, k its quotient field and let $f(x), g(x) \in \mathcal{O}[x]$. If $f(x)$ is primitive and $f(x)|g(x)$ in $k[x]$, then $f(x)|g(x)$ in $\mathcal{O}[x]$ as well.*

Proof. Let $f(x)$ is primitive and $f(x)|g(x)$ in $k[x]$, then $g(x) = f(x)h(x)$, where $h(x) \in k[x]$. By Gauss' lemma, $c(g) = c(f)c(h)$. Since $f(x)$ is primitive, $c(f) \in \mathcal{O}^*$. Therefore, $c(h) \in \mathcal{O}$ and $h(x) \in \mathcal{O}[x]$.

Corollary 7.5.6. *Let $\mathcal{O}$ be a factorial ring with quotient field k. Any irreducible polynomial in the ring $\mathcal{O}[x]$ is either an irreducible element of $\mathcal{O}$ or a primitive polynomial which is irreducible in the ring $k[x]$.*

Proof. Let $p(x)$ be an irreducible polynomial in $\mathcal{O}[x]$. If $deg(f) < 1$, then, obviously, $p(x)$ is a constant and irreducible in $\mathcal{O}$. Assume that $deg(f) \geq 1$. Then it is, obviously, a primitive polynomial. Suppose, $p(x)$ is not irreducible in $k[x]$, that is, $p(x) = f(x)g(x)$ in $k[x]$. By lemma 7.5.3, $f(x) = c(f)f_1(x)$, where $f_1(x) \in \mathcal{O}[x]$ is primitive. Then $f_1(x)|p(x)$ in $k[x]$ and, by corollary 7.5.5, we have $f_1(x)|p(x)$ in $\mathcal{O}[x]$. A contradiction.

Proof of theorem 7.5.1. For the proof this theorem use theorem 7.2.2. We first show that any nonunit element of $\mathcal{O}[x]$ factors into irreducible polynomials. Without loss of generality it suffices to prove this fact for primitive polynomials. We shall prove this by induction on the degree of a polynomial $f(x) \in \mathcal{O}[x]$. Suppose $deg(f) \leq 0$, then the result follows from the fact that $\mathcal{O}$ is a factorial ring. Assume that $deg(f) = n > 0$, and that the result is true for all polynomials of degree $< n$.

If $f(x)$ is irreducible, we are done. Otherwise we can write $f(x) = f_1(x)f_2(x)$ and $deg(f_1) < n$, $deg(f_2) < n$. Then the result follows by induction.

Now we prove that any irreducible element in $\mathcal{O}[x]$ is prime. Let $p(x)$ be an irreducible polynomial in $\mathcal{O}[x]$ and $p(x)|f(x)g(x)$, where $f(x), g(x) \in \mathcal{O}[x]$. We must prove then that either $p(x)|f(x)$ or $p(x)|g(x)$. If $deg(p) = 0$, then $p(x) \in \mathcal{O}$ and the statement follows from lemma 7.5.2. If $deg(p) > 0$, then, by corollary 7.5.6, $p(x)$ is a primitive polynomial, which is irreducible in $k[x]$. Since $k[x]$ is a factorial ring, $p(x)$ divides one of the factors in $k[x]$ and, by corollary 7.5.5, it divides one of the factors in $\mathcal{O}[x]$. The theorem is proved.

Theorem 7.5.7. *Let $\mathcal{O}$ be a factorial ring, then $\mathcal{O}[x_1, x_2, ..., x_n]$ is a factorial ring as well.*

The proof of this theorem follows from theorem 7.5.1 by induction on the number of variables.

Now we can give examples of factorial rings which are not principal ideal domains.

Example 7.5.1.
Let $R = \mathbf{Z}[x]$ be the polynomial ring in one variable x over the ring of integers $\mathbf{Z}$. Since $\mathbf{Z}$ is a factorial ring, by theorem 7.5.1, the ring $\mathbf{Z}[x]$ is factorial as well. But it is not a principal ideal domain because, for example, the ideal $(2, x)$ is not principal in $\mathbf{Z}[x]$.

Example 7.5.2.
Consider the ring $R = k[x, y]$ of polynomials in two variables x and y over a field k. By theorem 7.5.7, this ring is factorial. However, it is not a principal ideal domain. This follows from the fact that the ideal $\mathcal{I} = (x, y)$ is not principal. Indeed, if $\mathcal{I} = (f(x, y))$, then $x = cf(x, y)$ and $y = df(x, y)$ for some $c, d \in k[x, y]$. Looking at the degree in x and y it immediately follows that $f(x, y)$ must be of the form $a_0 + a_1x + a_2y + a_3xy$. Looking at the total degree gives $a_3 = 0$. Also it cannot be that $a_1 = a_2 = 0$ because then either $(f(x, y)) = 0$ or $(f(x, y)) = k[x, y]$. So $f(x, y) = a_0 + a_1x + a_2y$ with $a_1 \neq 0$ or $a_2 \neq 0$. It is now easy to check that there are no solutions to $x = cf(x, y), y = df(x, y)$, $c, d \in k[x, y]$.

7.6. THE CHINESE REMAINDER THEOREM

There are a lot of different formulations of the well-known "Chinese remainder theorem". We give one of them.

Theorem 7.6.1 (Chinese remainder theorem). *Let A be a principal ideal domain and $n = p_1^{n_1}p_2^{n_2}...p_s^{n_s}$ be a factorization of $n \in A$, where $p_1, p_2, ..., p_s \in A$ are distinct primes. Then*

$$A/(n) \simeq A/(p_1^{n_1}) \times A/(p_2^{n_2}) \times ... \times A/(p_s^{n_s}).$$

In fact we shall prove a certain generalization of this theorem and as corollary of this theorem obtain theorem 7.6.1.

Definition. Two ideals $\mathcal{I}$ and $\mathcal{J}$ in a ring A is called **comaximal** if $\mathcal{I} + \mathcal{J} = A$.

Theorem 7.6.2. *Let $\mathcal{I}_1, \mathcal{I}_2, ..., \mathcal{I}_n$ be pairwise comaximal ideals in a commutative ring A. Then*

$$A/(\mathcal{I}_1\mathcal{I}_2...\mathcal{I}_n) \simeq A/(\mathcal{I}_1) \times A/(\mathcal{I}_2) \times ... \times A/(\mathcal{I}_n).$$

To prove this theorem we need the following lemma often called the "Chinese remainder theorem for two elements":

Lemma 7.6.3. *Let $\mathcal{I}_1$ and $\mathcal{I}_2$ be ideals in a commutative ring A such that $\mathcal{I}_1+\mathcal{I}_2=A$. Then for any $x_1,x_2\in A$ there exists $x\in A$ such that $x\equiv x_i(mod\ \mathcal{I}_i)$ for $i=1,2$. Moreover, $\mathcal{I}_1\mathcal{I}_2=\mathcal{I}_1\cap\mathcal{I}_2$ and*

$$A/\mathcal{I}_1\mathcal{I}_2\simeq A/\mathcal{I}_1\times A/\mathcal{I}_2.$$

Proof. Obviously, $\mathcal{I}_1\mathcal{I}_2\subset\mathcal{I}_1\cap\mathcal{I}_2$. Let $y\in\mathcal{I}_1\cap\mathcal{I}_2$. Since $\mathcal{I}_1+\mathcal{I}_2=A$, there exist $a_i\in\mathcal{I}_i$ $(i=1,2)$ such that $a_1+a_2=1$. Then $a_1y+a_2y=y\in\mathcal{I}_1\mathcal{I}_2$. So, $\mathcal{I}_1\mathcal{I}_2=\mathcal{I}_1\cap\mathcal{I}_2$.

Let $x_1,x_2\in A$ and set $x=x_2a_1+x_1a_2$ where a_1,a_2 are as above. From the equalities $x_1=x_1a_1+x_1a_2$, $x_2=x_2a_1+x_2a_2$ we obtain $x=x_2a_1+(x_1-x_1a_1)=x_1+(x_2-x_1)a_1\equiv x_1(mod\ \mathcal{I}_1)$ and, similarly, $x=x_1a_2+(x_2-x_2a_2)=x_2+(x_1-x_2)a_2\equiv x_2(mod\ \mathcal{I}_2)$.

Now we can form the map $\varphi:A\to A/\mathcal{I}_1\times A/\mathcal{I}_2$ by $\varphi(x)=(x_1,x_2)$, where $x\equiv x_1(mod\ \mathcal{I}_1)$ and $x\equiv x_2(mod\ \mathcal{I}_2)$. From what has just been said it is easy to see that φ is an epimorphism with $Ker\varphi=\mathcal{I}_1\cap\mathcal{I}_2=\mathcal{I}_1\mathcal{I}_2$. Applying the homomorphism theorem we obtain the statement of the lemma.

Proof of theorem 7.6.1. In the general case when $n>2$ we can prove this theorem by induction on the number of ideals n using the previous lemma. To this end we apply lemma 7.6.3 for the two ideals $\mathcal{I}=\mathcal{I}_1$ and $\mathcal{J}=\mathcal{I}_2...\mathcal{I}_n$.

We need only to show that the ideals $\mathcal{I}$ and $\mathcal{J}$ are comaximal, i.e., $\mathcal{I}+\mathcal{I}_2...\mathcal{I}_n=A$. Since the ideals $\mathcal{I}_1,\mathcal{I}_2,...,\mathcal{I}_n$ are pairwise comaximal, for any $i=2,3,...,n$ there exist $a_i\in\mathcal{I}_1$ and $b_i\in\mathcal{I}_i$ such that $a_i+b_i=1$. Since $a_i+b_i\equiv b_i\ (mod\ \mathcal{I}_1)$, we obtain $1=(a_2+b_2)...(a_n+b_n)\equiv b_2b_3...b_n(mod\ \mathcal{I}_1)$, i.e., $1\in\mathcal{I}_1+\mathcal{I}_2...\mathcal{I}_n$. This means that $\mathcal{I}_1+\mathcal{I}_2...\mathcal{I}_n=A$ and this completes the proof.

7.7. SMITH NORMAL FORM OVER A PID

The remainder of this chapter will be devoted to the study of finitely generated modules over a PID. We shall need some general theory connected with this topic. In this section we consider some facts concerning matrices with entries in a PID. Throughout in this section $\mathcal{O}$ is a commutative principal ideal domain. Consider the set $M_{m\times n}(\mathcal{O})$ of all $m\times n$ matrices over $\mathcal{O}$. We write $M_n(\mathcal{O})$ for $M_{n\times n}(\mathcal{O})$.

Definition. Two $m\times n$ matrices $\mathbf{A}$ and $\mathbf{B}$ with entries in $\mathcal{O}$ are said to be **equivalent** if there exists an invertible matrix $\mathbf{P}\in M_m(\mathcal{O})$ and an invertible matrix $\mathbf{Q}\in M_n(\mathcal{O})$ such that $\mathbf{B}=\mathbf{PAQ}$.

Obviously "being equivalent" is an equivalence relation on the set $M_{m\times n}(\mathcal{O})$ and we write $\mathbf{A}\sim\mathbf{B}$ if $\mathbf{A}$ is equivalent to $\mathbf{B}$. This equivalence relation divides the

set $M_{m\times n}(\mathcal{O})$ into equivalence classes. Our purpose is to choose in each equivalence class a representative, which has a particularly simple form.

We first introduce in the ring $M_n(\mathcal{O})$ of all square matrices of order n the following matrices

$$\mathbf{T}_{ij}(\alpha) = \mathbf{E} + \alpha e_{ij}$$

$$\mathbf{D}_i(\gamma) = \mathbf{E} - e_{ii} + \gamma e_{ii}$$

$$\mathbf{P}_{ij} = \mathbf{E} - e_{ii} - e_{jj} + e_{ij} + e_{ji}$$

where $i \neq j$, the e_{ij} are the matrix units of $M_n(\mathcal{O})$, $\mathbf{E} = e_{11} + e_{22} + ... + e_{nn}$, $\alpha \in \mathcal{O}$ and γ is a unit in $\mathcal{O}$.

It is easy to verify that $\mathbf{T}_{ij}(\alpha)^{-1} = \mathbf{T}_{ij}(-\alpha)$, $\mathbf{D}_i(\gamma)^{-1} = \mathbf{D}_i(\gamma^{-1})$ and $\mathbf{P}_{ij}^{-1} = \mathbf{P}_{ij}$. Therefore, the matrices $\mathbf{T}_{ij}(\alpha)$, $\mathbf{D}_i(\gamma)$ and $\mathbf{P}_{ij}$ are all invertible and they are called **elementary matrices**.[3])

Left multiplication of a $m \times n$ matrix $\mathbf{A}$ by elementary matrices $\mathbf{T}_{ij}(\alpha)$, $\mathbf{D}_i(\gamma)$ and $\mathbf{P}_{ij}$ of $M_m(\mathcal{O})$ gives respectively the following elementary operations on the rows of $\mathbf{A}$:

1. Multiplying the jth row by α and adding it to the ith row.
2. Multiplying the ith row by $\gamma \in \mathcal{O}^*$.
3. Interchanging the ith and the jth rows.

Right multiplication of a matrix $\mathbf{A}$ by these elementary matrices of $M_n(\mathcal{O})$ gives analogously elementary operations on the columns of $\mathbf{A}$.

Multiplication of a matrix A by these elementary matrices is called an **elementary operation**.

Obviously, any matrix obtained by a finite sequence of elementary operations on rows and columns of $\mathbf{A}$ is equivalent to $\mathbf{A}$.

We shall say that a matrix $\mathbf{B} \in M_{m\times n}(\mathcal{O})$ is in **diagonal form** if

$$\mathbf{B} = diag\{b_{11}, b_{22}, ..., b_{kk}, 0, ..., 0\} =$$

$$= \begin{pmatrix} b_{11} & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & b_{22} & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & b_{kk} & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$$

where $k \leq \min\{m, n\}$.

Let $\mathcal{O}$ be a principal ideal domain. Then it is a factorial ring, i.e., each nonzero element $a \in \mathcal{O}$ has a unique factorization into prime elements $p_1 p_2 ... p_r$ and the number r of prime factors is an invariant. We shall call the number r the **length**

[3]) The phrase "elementary matrices" has a different meaning in algebraic K-theory.

of the element a and denote it by $l(a)$. By convention $l(\varepsilon) = 0$ if and only if ε is a unit of $\mathcal{O}$.

It is easy to see that
1) $l(ab) = l(a) + l(b)$;
2) if $a|b$ then $l(a) \leq l(b)$;
3) if $a|b$ and $l(a) = l(b)$, then $a = \varepsilon b$, where ε is a unit of $\mathcal{O}$.

Theorem 7.7.1. *Every matrix $\mathbf{A} \in M_{m\times n}(\mathcal{O})$ with entries in a principal ideal domain $\mathcal{O}$ is equivalent to a matrix, which has diagonal form*

$$\mathbf{B} = diag\{b_{11}, b_{22}, ..., b_{kk}, 0, ..., 0\},$$

where $k \leq min\{m, n\}$, $b_{ii} \neq 0$ and moreover $b_{11}|b_{22}|...|b_{kk}$.

Proof. Let $\mathbf{A} \in M_{m\times n}(\mathcal{O})$. On the set $M_{m\times n}(\mathcal{O})$ we have the binary relation of equivalent matrices, which divides this set on equivalence classes. We shall show that the equivalence class containing the matrix $\mathbf{A}$ has a representative which has a diagonal form.

If $\mathbf{A} = \mathbf{0}$ there is nothing to prove. Therefore we may assume that there is at least one nonzero element in the matrix $\mathbf{A}$. Let us consider the matrix $\mathbf{A}$ and the equivalence class $\mathcal{E}$ to which this matrix belongs. In the class $\mathcal{E}$ choose a matrix $\mathbf{B}$ such that it has a nonzero entry of the least length among all matrices equivalent to A.

Since all elementary matrices are invertible, we can perform arbitrary elementary operations on the matrix $\mathbf{B}$ over the ring $\mathcal{O}$.

By elementary operations of type 3 (both column and row) we can move the entry of least length to the $(1, 1)$ position. So, we can assume that the entry b_{11} has least length in the equivalence class $\mathcal{E}$. We shall prove that either $b_{1j} = 0$ or $b_{11}|b_{1j}$ for all $j = 1, ..., n$ and either $b_{i1} = 0$ or $b_{11}|b_{i1}$ for all $i = 1, .., m$. Suppose $b_{12} \neq 0$ and b_{11} does not divide it. Let $d = (b_{11}, b_{12})$ and $b_{11} = d\alpha$, $b_{12} = d\beta$. Then there exist elements $x, y \in \mathcal{O}$ such that $d = b_{11}x + b_{12}y$ and hence $d = d\alpha x + d\beta y$. Since $\mathcal{O}$ is a domain, $\alpha x + \beta y = 1$. Consider the matrix equality

$$\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \begin{bmatrix} x & -\beta \\ y & \alpha \end{bmatrix} = \begin{bmatrix} d & 0 \\ b'_{12} & b'_{22} \end{bmatrix}$$

where the matrix

$$\mathbf{U} = \begin{bmatrix} x & -\beta \\ y & \alpha \end{bmatrix}$$

is invertible, since $det\mathbf{U} = \alpha x + \beta y = 1$. Consequently, the matrix

$$\bar{\mathbf{U}} = \begin{bmatrix} x & -\beta & 0 & \dots & 0 \\ y & \alpha & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \dots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}$$

is also invertible in $M_n(\mathcal{O})$ and multiplying $\mathbf{B}$ on the right side by this matrix $\bar{\mathbf{U}}$ we obtain an equivalent matrix with d at the position $(1,1)$ and zero at the position $(1,2)$. Since b_{11} does not divide b_{12}, the length of d is less than that of b_{11}. So $l(d) < l(b_{11})$. This contradicts the choice of the matrix $\mathbf{B}$ as a matrix with an entry at position (1,1) of least length. Therefore $b_{11}|b_{12}$. Analogously we can prove that if $b_{1j} \neq 0$, then $b_{11}|b_{1j}$ for all $j = 1, ..., n$. In this case instead of the matrix $\bar{\mathbf{U}}$ we use the matrix $\bar{\mathbf{U}}_i = xe_{11} - \beta_j e_{1j} + ye_{j1} + e_{22} + ... + \alpha e_{jj} + e_{j+1,j+1} + ... + e_{nn}$. In a similar way we can prove that either $b_{i1} = 0$ or $b_{11}|b_{i1}$ for all $i = 1, ..., m$. Therefore there exists a matrix $\mathbf{B}$ equivalent to the matrix $\mathbf{A}$ and either $b_{1j} = 0$ or $b_{11}|b_{1j}$ for all $j = 1, ..., n$ and either $b_{i1} = 0$ or $b_{11}|b_{i1}$ for all $i = 1, .., m$. Then elementary operations on the rows and columns of type I give an equivalent matrix of the form:

$$\mathbf{A}^* = \begin{pmatrix} b_{11} & 0 & \dots & 0 \\ 0 & c_{22} & \dots & c_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & c_{m2} & \dots & c_{mn} \end{pmatrix}.$$

By induction applying this process to the matrix

$$\mathbf{C} = \begin{pmatrix} c_{22} & \dots & c_{2n} \\ \dots & \dots & \dots \\ c_{m2} & \dots & c_{mn} \end{pmatrix}$$

we obtain the equivalent matrix, which has a diagonal form

$$\mathbf{PAQ} = diag\{b_{11}, b_{22}, ..., b_{kk}, 0, ..., 0\}.$$

Finally, we show that we can reduce $\mathbf{PAQ}$ further such that $b_{11}|b_{22}|...|b_{kk}$. Assume, b_{11} does not divide b_{22}. Then adding the second row to the first one, we obtain the first row in the form:

$$(b_{11}\ b_{22}\ 0\ \ ...\ \ 0)$$

Then performing the operations described above we can reduce the length of b_{11}. A contradiction. So, $b_{11}|b_{22}$ and, analogously, $b_{11}|b_{ii}$, $i = 3, ..., k$. The theorem is proved.

A matrix equivalent to a given matrix $\mathbf{A}$ and having the diagonal form given in theorem 7.7.1 is called the **Smith normal form** for $\mathbf{A}$. The nonzero diagonal elements of the Smith normal form of a matrix $\mathbf{A}$ are called the **invariant factors** of $\mathbf{A}$. It can be shown that the invariant factors are unique up to unit multipliers and two matrices are equivalent if and only if they have the same invariant factors. We leave the proof of these statements to the reader.

7.8. FINITELY GENERATED MODULES OVER A PID

The purpose of this section is to prove the fundamental structure theorem for finitely generated modules over a principal ideal domain.

Lemma 7.8.1. *Let A be a principal ideal domain, and F be a finitely generated free A-module with a free basis consisting of n elements. Then any submodule K of F is also finitely generated free A-module with a free basis consisting of m elements, where $m \leq n$.*

Proof. Since A is a hereditary Noetherian ring, the proof follows from corollary 3.1.13 and corollary 5.5.3.

Let A be a PID and M be a finitely generated A-module. Then, by proposition 1.5.2, M is isomorphic to a quotient of a free module A^n, i.e., $M \simeq A^n/K$. Since K is a submodule of a finitely generated free A-module, by lemma 7.8.1, K is also a finitely generated free A-module, i.e., $K \simeq A^m$, where $m \leq n$. So, we have a short exact sequence:

$$0 \longrightarrow A^m \xrightarrow{\psi} A^n \longrightarrow M \longrightarrow 0$$

and $M \simeq M_\psi = A^n/Im\psi$. Let ξ be an automorphism of the module A^m and let η be an automorphism of the module A^n. Then it is not difficult to verify that $M_\psi \simeq M_{\eta\psi\xi}$.

Let $e_1, ..., e_m$ be a free basis for module A^m and $f_1, f_2, ..., f_n$ be a free basis for A^n. In the usual way a homomorphism $\psi : A^m \to A^n$ is the same thing as an $(m \times n)$-matrix $[\psi]$ with entries ψ_{ij} in A:

$$\psi(e_1) = \psi_{11}f_1 + \psi_{12}f_2 + ... + \psi_{1n}f_n$$

$$\psi(e_2) = \psi_{21}f_1 + \psi_{22}f_2 + ... + \psi_{2n}f_n$$

$$\dots$$

$$\psi(e_m) = \psi_{m1}f_1 + \psi_{m2}f_2 + ... + \psi_{mn}f_n$$

where $\psi_{ij} \in A$. This matrix is called the matrix of ψ relative to the bases $e_1, ..., e_m$ and $f_1, f_2, ..., f_n$. In a similar way an automorphism $\xi : A^m \to A^m$ corresponds to an invertible matrix $[\xi] \in M_m(A)$ and an automorphism $\eta : A^n \to A^n$ corresponds to an invertible matrix $[\eta] \in M_n(A)$. It is not difficult to verify that $M_\psi \simeq M_{\eta\psi\xi}$ if and only if the matrix $[\psi]$ is equivalent to the matrix $[\eta\psi\xi]$. By theorem 7.7.1, this latter matrix can be assumed to be in Smith normal form:

$$[\psi] \sim diag\{b_1, b_2, ..., b_t, 0, ..., 0\},$$

where $t \leq m$ and $b_1|b_2|...|b_t$

Therefore $Im\psi = b_1A \oplus ... \oplus b_tA \oplus 0$, where $b_1|b_2|...|b_t$. Since $M \simeq A^n/Im\psi$, we have $M \simeq A/b_1A \oplus ... \oplus A/b_tA \oplus A^{n-t}$. As every A-module A/b_iA is cyclic, we obtain the following theorem:

Theorem 7.8.2. *Any finitely generated A-module M over a principal ideal domain A is isomorphic to a finite direct sum of cyclic submodules*:

$$M \simeq A/b_1A \oplus ... \oplus A/b_tA \oplus A^{n-t}$$

where $t \leq n$, and the b_i are nonzero nonunit elements in A such that $b_1|b_2|...|b_t$.

Definition. The integer $r = n - t$ in theorem 7.8.2 is called the **free rank** of M and the elements $b_1, b_2, ..., b_k \in A$ (defined up to multiplication by units in A) are called the **invariant factors** of M.

Let us take a good look at the form of a module $A/\alpha A$, where $\alpha \in A$. Since A is a factorial ring, there is a unique factorization of $\alpha = p_1^{n_1}...p_s^{n_s}$, where $p_1, ..., p_s$ are distinct primes.

Then, by the Chinese remainder theorem (theorem 7.6.1), we have a decomposition into a direct sum: $A/\alpha A \simeq \overset{s}{\underset{i=1}{\oplus}} A/(p_i^{n_i})$. Thus, any submodule of the form A/b_iA is isomorphic to a direct sum of submodules of the form $A/(p_i^{n_i})$. We shall show that each such submodule is indecomposable.

Consider $\mathcal{O} = A/p^nA$, $\pi = p + p^nA$, $\mathcal{M} = \pi\mathcal{O}$ where p is a prime element of A. We shall show that in the ring $\mathcal{O}$ there is only one chain of ideals: $\mathcal{O} \supset \mathcal{M} \supset \mathcal{M}^2 \supset ... \supset \mathcal{M}^{n-1} \supset 0$. Let $\beta \in \mathcal{O}$ and $\beta \neq 0$, $\beta = a + p^nA$. Denote by ν the largest power of the element p such that p^ν divides a. Then $\beta = p^\nu a_1 + p^nA$ and $(p, a_1) = 1$. Therefore $(p^n, a_1) = 1$ and hence $1 = a_1v + p^nu$ for some u, v, i.e., in the ring $\mathcal{O}$ the element $a_1 + p^nA$ is invertible. So we have shown that any element $\beta \in \mathcal{O}$ has the form $\beta = \pi^\nu\varepsilon$, where ε is a unit of $\mathcal{O}$. The number ν is called the **exponent of the element** β. Clearly, any nonzero ideal of $\mathcal{O}$ is generated by a nonzero element contained in it with least exponent. Therefore, any ideal in the ring $\mathcal{O}$ has the form $\pi^\nu\mathcal{O}$. Thus, in particular, $\mathcal{O}$ is an indecomposable A-module. Since $\mathcal{M}^k/\mathcal{M}^{k+1} \simeq F$, where F is the field $A/(p)$, the A-module A/p^nA is Artinian. Thus, A/p^nA is an indecomposable module, which is both Artinian and Noetherian. Since any such module is cyclic, we have proved the following fundamental result:

Theorem 7.8.3. *Any finitely generated module M over a principal ideal domain A is isomorphic to a finite direct sum of indecomposable cyclic modules of the form $A/\alpha A$, where either $\alpha = 0$ or $\alpha = p^n$ (where p is a prime element of the ring A), i.e.,*

$$M \simeq A^r \oplus A/(p_1^{n_1}) \oplus ... \oplus A/(p_k^{n_k})$$

where $r \geq 0$ and the $p_i^{n_i}$ are positive powers of (not necessary distinct) primes in A.

Definition. The prime powers $p_1^{n_1}, p_2^{n_2}, ..., p_k^{n_k} \in A$ in theorem 7.8.3 (defined up to multiplication by units in A) are called the **elementary divisors** of M. The A-module $A/p_i^{n_i}A$ in this theorem is called a **primary component** of M.

Definition. Let M be a right module over a commutative domain A. An element $m \in M$ is called a **torsion element** if there exists a nonzero element $x \in A$ such that $mx = 0$. A nonzero element $m \in M$ is called a **torsion-free**

element if $mx = 0$, $x \in A$ implies $m = 0$. The set of all torsion elements of M is denoted by $t(M)$.

It is easy to verify, that $t(M)$ is submodule of M, and it is called the **torsion submodule** of M. We call M a **torsion module** if and only if $t(M) = M$, and M is a **torsion-free module** if and only if $t(M) = 0$. Clearly, $M/t(M)$ is a torsion-free module. A free module over a commutative domain is torsion-free.

Theorem 7.8.4. *Any finitely generated module M over a PID A decomposes into a direct sum of a finitely generated torsion-free module and a finitely generated torsion module.*

Proof. By the structure theorem for finitely generated modules over a PID, any such A-module is isomorphic to a direct sum:

$$M \simeq A/b_1A \oplus ... \oplus A/b_tA \oplus A^k$$

where b_i are nonzero nonunit elements in A such that $b_1|b_2|...|b_t$. Then it follows that $M = F \oplus T$, where $F \simeq A^k$ and $T \simeq A/b_1A \oplus ... \oplus A/b_tA$. Obviously, F is a finitely generated torsion-free module. We shall show that $T = t(M)$. It is clear, that $b_tT = 0$, i.e., $T \subset t(M)$. Conversely, let $m \in t(M)$. Then $m = m_1 + m_2$, where $m_1 \in F$ and $m_2 \in T$. So $m_1 = m - m_2 \in t(M)$, and hence there exists $a \in A$, $a \neq 0$, such that $m_1a = 0$. Let $e_1, e_2, ..., e_k$ be a free basis of F, then $m_1 = e_1a_1 + e_2a_2 + ... + e_ka_k = 0$ and $m_1a = e_1a_1a + e_2a_2a + ... + e_ka_ka = 0$. Hence, $a_ia = 0$ for each $i = 1, ..., k$. Since A is a PID and $a \neq 0$, $a_i = 0$ for each $i = 1, ..., k$. Therefore $m_1 = 0$, i.e., $m \in T$. Thus, $T = t(M)$.

The uniqueness of decomposition of finitely generated modules over a PID will be proved in chapter 10 as a corollary of the fundamental Krull-Schmidt theorem for semiperfect rings. Now we shall only prove one part of this theorem.

Proposition 7.8.5. *If two finitely generated modules M_1 and M_2 over a PID A are isomorphic, then they have the same free rank.*[4])

Proof. Suppose M_1 and M_2 are isomorphic. Since any isomorphism between M_1 and M_2 maps the torsion submodule of M_1 to the torsion submodule of M_1, we must have $M_1/t(M_1) \simeq M_2/t(M_2)$. Then $A^{r_1} \simeq A^{r_2}$, where r_i is the free rank of M_i for $i = 1, 2$. Then, by proposition 1.5.5, $r_1 = r_2$.

An important example of modules are the Abelian groups which are naturally considered as modules over the ring of integers. Applying theorem 7.8.3 to the case $A = \mathbf{Z}$ we obtain the main theorem on finitely generated Abelian groups:

Theorem 7.8.6. *Every finitely generated Abelian group is isomorphic to a direct product of cyclic groups. Every finite Abelian group is isomorphic to a*

[4]) There are rings A for which $A^n \simeq A^m$ for certain $n \neq m$.

direct sum of cyclic primary groups.

7.9. THE FROBENIUS THEOREM

In this section we apply the fundamental structure theorem of finitely generated modules over a PID to obtain a famous canonical form for square matrices over a field.

From any course on linear algebra it is well known that the problem of describing linear transformations acting on various vector spaces V over a field K, and the problem of describing square matrices over a field K up to similarity is the same problem. This problem reduces to describing up to isomorphism $K[x]$-modules which are finite dimensional vector spaces over the field K.

Let V be a finite dimensional vector space over a field K and let $\mathcal{A}$ be a linear transformation from V to itself. As usual, for any $f(x) = a_0x^n + a_1x^{n-1} + ... + a_n \in K[x]$ we set $f(\mathcal{A}) = a_0\mathcal{A}^n + a_1\mathcal{A}^{n-1} + ... + a_n\mathcal{E}$, where $\mathcal{E}$ is the identity mapping of V into itself. Then $f(\mathcal{A})$ is also a linear transformation acting on V, i.e., $f(\mathcal{A}) \in End_K(V)$. Introduce on V the structure of a $K[x]$-module by setting that $f(x)v = f(\mathcal{A})v$ for every $f(x) \in K[x]$ and $v \in V$.

Note that if V is a finite dimensional vector space over K, then V is a finitely generated $K[x]$-module. Moreover, if $u_1, u_2, ..., u_n$ is a basis of V over K, then $u_1, u_2, ..., u_n$ is a set of generators of V as $K[x]$-module.

Let $m = dim_K V$ be the dimension of a vector space V over a field K. Then the set $End_K(V)$ is simultaneously a ring and a vector space over the field K and its dimension is equal to m^2. Therefore the transformations $\mathcal{E}, \mathcal{A}, \mathcal{A}^2, ..., \mathcal{A}^{m^2}$ are linearly dependent over K for any transformation $\mathcal{A} \in End_K(V)$, and so there exists a nonzero polynomial $g(x) \in K[x]$ such that $g(x)v = g(\mathcal{A})v = 0$ for any $v \in V$. Thus, any finite dimensional vector space V as a $K[x]$-module is a torsion module.

Since $K[x]$ is a PID, from theorem 7.8.3 we immediately obtain the following fundamental structure theorem:

Theorem 7.9.1. *Any finitely generated $K[x]$-module decomposes into a direct sum of indecomposable cyclic submodules.*

Since any finite dimensional vector space V as a $K[x]$-module is a torsion module, from this theorem it follows that any indecomposable $K[x]$-module is of the form $V = K[x]/(p^i(x))$, where $p(x)$ is an irreducible polynomial. Let v be an arbitrary element in V and $g(x) = p^i(x) = x^s + a_1x^{s-1} + ... + a_s$. Consider the linear transformation $\mathcal{A} \in End_K(V)$ giving by $\mathcal{A}v = xv$. Since $g(x)v = 0$ for any $v \in V$, $\mathcal{A}$ is a root of the polynomial $g(x) = x^s + a_1x^{s-1} + ... + a_s$, that is $\mathcal{A}^s + a_1\mathcal{A}^{s-1} + ... + a_s\mathcal{E} = 0$. If v is a generator of V then vectors $v, \mathcal{A}v, ..., \mathcal{A}^{s-1}v$ form a basis of V. Now write down the matrix of the linear transformation $\mathcal{A}$ in this basis. Since

$$\begin{gathered}\mathcal{A}v = \mathcal{A}v \\ \mathcal{A}(\mathcal{A}v) = \mathcal{A}^2 v \\ \dots \\ \mathcal{A}(\mathcal{A}^{s-2}v) = \mathcal{A}^{s-1}v \\ \mathcal{A}(\mathcal{A}^{s-1}v) = -a_s v - a_{s-1}\mathcal{A}v - ... - a_1\mathcal{A}^{s-1}v\end{gathered}$$

we obtain the following matrix

$$\Phi = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -a_s \\ 1 & 0 & 0 & \dots & 0 & -a_{s-1} \\ 0 & 1 & 0 & \dots & 0 & -a_{s-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & -a_2 \\ 0 & 0 & 0 & \dots & 1 & -a_1 \end{pmatrix} \tag{7.9.1}$$

which is called the **Frobenius block** or the **companion matrix** of the polynomial $g(x)$.

Let $\mathbf{A}$ be the matrix of a linear transformation $\mathcal{A}$ acting on a linear vector space V. Taking into account theorem 7.9.1 we obtain the following theorem.

Theorem 7.9.2 (Frobenius theorem). *For any square matrix* $\mathbf{A}$ *over a field* K *with a minimal polynomial* $t(x) = p_1^{n_1}(x)...p_s^{n_s}(x)$ *there is an invertible matrix* $\mathbf{S}$ *such that*

$$\mathbf{SAS}^{-1} = \begin{pmatrix} \mathbf{B}_1 & 0 & \dots & 0 \\ 0 & \mathbf{B}_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \mathbf{B}_n \end{pmatrix} \tag{7.9.2}$$

where $\mathbf{B}_i$ *is a Frobenius block corresponding to the powers* $p_i^{n_i}(x)$ *of an irreducible polynomial* $p_i(x) \in K[x]$, $i = 1, ..., s$. *These blocks are indecomposable.*

We shall call (7.9.2) the **classical canonical form** or the **Frobenius normal form** of the matrix $\mathbf{A}$ over the field K.

Consider the Frobenius theorem for the case that K is an algebraically closed field. Then the minimal polynomial $t(x)$ of a matrix $\mathbf{A}$ decomposes into a product of linear factors. Assume the matrix $\mathbf{A}$ to be indecomposable. In this case an indecomposable module W is isomorphic to a module of the form $K[x]/(x-a)^r$. Choose the following basis for it: $1, x-a, ..., (x-a)^{r-1}$. Then there exists an invertible matrix $\mathbf{S}$ such that

$$\mathbf{S}(\mathbf{A} - a\mathbf{E})\mathbf{S}^{-1} = J_r(0) = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}.$$

which is called the **Jordan block** of order r with zero eigenvalue. Hence

$$\mathbf{SAS}^{-1} = J_r(0) + a\mathbf{E} = \begin{pmatrix} a & 0 & \dots & 0 & 0 \\ 1 & a & \dots & 0 & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & a & 0 \\ 0 & 0 & \dots & 1 & a \end{pmatrix} = J_r(a)$$

A matrix $J_r(a)$ of this form is called the **Jordan block** of order r with an eigenvalue a. The matrix $\mathbf{A}$ of the form (7.9.2), where each $\mathbf{B}_i$ is a Jordan block, is called the **Jordan normal form** of the matrix $\mathbf{A}$.

Note that for the modules M considered in theorem 7.8.3 there holds uniqueness of the decomposition M into a direct sum of indecomposable modules. Let module M be expressed in two different ways into the form of a direct sum of indecomposable modules: $M = \bigoplus_{i=1}^{n} M_i = \bigoplus_{j=1}^{m} N_j$. Then $m = n$ and there is a permutation τ of the numbers from 1 to n such that $M_i \simeq N_{\tau(i)}$ $(i = 1, ..., n)$. Hence, in particular, there follows uniqueness of the Frobenius normal form up to a permutation of blocks.

Uniqueness of the decomposition shall be proved in chapter 10. This is (an instance of) the famous Krull-Schmidt theorem.

7.10. NOTES AND REFERENCES

That the existence of a Dedekind-Hasse norm on a ring A implies that A is a PID is a classical result, which was proved by R.Dedekind and H.Hasse (see, *Über eindeutige Zerlegung in Primelemente oder in Primhauptideale in Integritätsbereichen // J. Reine Angew. Math., v.159 (1928), p.3-12.* The converse statement (proposition 7.3.3) was proved by J.Green in his paper *Principal Ideal Domains are almost Euclidean // Amer. Math. Monthly, v.104 (1997), p.154-156.*

The notions of torsion-free and torsion modules over Noetherian rings were considered by A.W.Goldie in the paper *Torsion-free Modules and Rings // J.Algebra, v.1(1964), p.268-287.*

The Smith normal form for a matrix is called that in honor of Henry John Stephen Smith (1826-1883), Professor of Geometry in Oxford, who was regarded as one of the best number theorists of his time. In his only paper on the Smith normal form (see, *On systems of linear indeterminate equations and congruences // Philos. Trans. Roy. Soc. London, v.CLI (1861), p. 293-326*) he considered the general solution of Diophantine systems of linear equations or congruences.

There are a lot of works devoted to reducing a matrix to a diagonal form. Theorem 7.7.1 in a weak form was proved by J.H.M.Wedderburn for noncommutative Euclidean domains in his work *Non-commutative domains of integrity // J. Reine Angew. Math., v.167 (1932), p.129-142.* This theorem for Euclidean domains was proved by N.Jacobson in the paper *Pseudo-linear transformations // Ann.*

of Math., v.38 (1937), p.484-507. For arbitrary principal ideal domain this theorem was proved by Teichmüller (see *Der Elementarteilersatz für nichtkommutative Ringen // S.-B. Preuss. Acad. Wis., 1937, s. 169-177*).

The proof of the Frobenious theorem on the normal form of a matrix is done in this book in such a way as to bring out its module theoretic content. Such a proof was first produced in the famous book *B.L.Van der Waerden, Moderne Algebra, I,II, Springer, Berlin, 1931.* In the proof at many points we also follow the fundamental book *N.Jacobson, Lectures in Absract Algebra II. Linear Algebra, vol. 31, Springer-Verlag, Berlin-Heidelberg-New Jork, 1975.*

The proof of the decomposition of a finite Abelian group into a direct product of cyclic groups of prime power order was given by G.Frobenius and L.Stickelberger (see *Über Gruppen von vertauschbaren Elementen // J. Reine Angew. Math., v.86 (1878), p.217-262*).

The study of commutative rings constitutes the subject of commutative algebra, of which the reader can find excellent treatments in standard textbooks such as *O.Zariski and P.Samuel, Commutative Algebra, I, II, Graduate Texts in Mathematics, Vol. 28, 29, Springer-Verlag, Berlin-Heidelberg-New York, 1975*; *M.F.Atiyah and I.G.Macdonald, Introduction to Commutative Algebra. Addison-Wesley, Reading, 1969*; *I.Kaplansky, Commutative Rings, Univ. Chicago Press, Chicago, 1974* and *Hideyuki Maksumura, Commutative ring theory, Cambridge Univ. Press, 1989.*

8. Dedekind domains

In this chapter we shall consider some particular examples of commutative rings, such as Dedekind domains and Prüfer rings. We consider the main properties of these rings and describe finitely generated modules over Dedekind domains.

All the rings considered in this chapter will be commutative with $1 \neq 0$. As before, denote by $\mathbf{N}$ the set of all natural numbers and by A^* the set of all units of a ring A.

8.1. INTEGRAL CLOSURE

Let $\mathcal{O}$ be an integral domain with a quotient field k. If a field L contains the ring $\mathcal{O}$, then it contains a field which is isomorphic to k. Therefore one can assume that $L \supset k \supset \mathcal{O}$. We shall say that a polynomial $f(x) \in k[x]$ is **monic** if its leading coefficient is equal to 1.

Proposition 8.1.1. *Let L be a field containing an integral domain $\mathcal{O}$ and $\alpha \in L$. Then the following conditions are equivalent:*

1. *An element α is a root of some monic polynomial $f(x) \in \mathcal{O}[x]$.*
2. *There is a finitely generated nonzero $\mathcal{O}$-module $M \subset L$ such that $\alpha M \subset M$.*

Proof.

$1 \Rightarrow 2$. Let $f(x) = x^n + a_1 x^{n-1} + ... + a_n \in \mathcal{O}[x]$ and $f(\alpha) = 0$. Consider the $\mathcal{O}$-module M generated by the elements $1, \alpha, ..., \alpha^{n-1}$. Clearly, $\alpha M \subset M$.

$2 \Rightarrow 1$. Let $M = \{w_1, ..., w_n\}$ be a nonzero finitely generated $\mathcal{O}$-module such that $\alpha M \subset M$, then there exist elements $a_{ij} \in \mathcal{O}$ such that

$$\alpha w_1 = a_{11} w_1 + ... + a_{1n} w_n$$

$$\dots$$

$$\alpha w_n = a_{n1} w_1 + ... + a_{nn} w_n$$

Denote by A the matrix $(a_{ij}) \in M_n(\mathcal{O})$. So we have a uniform system of linear algebraic equations with respect to variables $w_1, ..., w_n$ with matrix $A - \alpha E$. This system has a nonzero solution in the field L. From linear algebra it is known that in this case $det(\alpha E - A) = 0$, i.e., α is a root of the monic polynomial $f(x) = det(xE - A)$, whose coefficients are linear combinations of products of elements of the matrix A. Thus, $f(x) = det(xE - A) \in \mathcal{O}[x]$ and is monic.

Definition. Let L be a field containing a ring $\mathcal{O}$. An element $\alpha \in L$ is called **integral over the ring** $\mathcal{O}$ if it satisfies one of the equivalent conditions of proposition 8.1.1. If every element of a subring A in L is integral over $\mathcal{O}$, we say that A is **integral over** $\mathcal{O}$. An element α is called **algebraic** over a field k if there exists $f(x) \in k[x]$ such that $f(\alpha) = 0$.

Proposition 8.1.2. *Let $\mathcal{O}$ be an integral domain with a quotient field k contained in some field L, and let $\alpha \in L$ be an algebraic element over k. Then there exists a nonzero element $c \in \mathcal{O}$ such that the element $c\alpha$ is integral over $\mathcal{O}$.*

Proof. Let $\alpha \in L$ and $L \supset k$. Then there exists a polynomial $f(x) = a_0x^n + a_1x^{n-1} + ... + a_n \in k[x]$ such that $a_0 \neq 0$ and

$$a_0\alpha^n + a_1\alpha^{n-1} + ... + a_n = 0.$$

Multiplying this equality by a_0^{n-1} we obtain

$$(a_0\alpha)^n + a_1(a_0\alpha)^{n-1} + ... + a_na_0^{n-1} = 0,$$

that is, the element $a_0\alpha$ is a root of a monic polynomial over $\mathcal{O}$.

Proposition 8.1.3. *Let $\mathcal{O}$ be a ring contained in a field k. Denote by Δ the set of all elements of the field k, which are integral over $\mathcal{O}$. Then Δ is a ring.*

Proof. Let $\alpha, \beta \in \Delta$ and let M, N be finitely generated $\mathcal{O}$-modules such that $\alpha M \subset M$ and $\beta N \subset N$. Then the module MN is finitely generated and $\alpha\beta MN \subset MN$, $(\alpha \pm \beta)MN \subset MN$.

Definition. The ring Δ introduced in theorem 8.1.3, i.e., the set of all elements of k that are integral over $\mathcal{O}$, is called the **integral closure** of the ring $\mathcal{O}$ in the field k. A ring $\mathcal{O}$ contained in a field L is called **integrally closed** in L if any element of this field, which is integral over $\mathcal{O}$, belongs to $\mathcal{O}$. A ring $\mathcal{O}$ is called **integrally closed** if it is integrally closed in its quotient field k.

Proposition 8.1.4. *Any factorial ring $\mathcal{O}$ is integrally closed.*

Proof. Let $\alpha \in k$ be an integral element over $\mathcal{O}$. Suppose $\alpha \notin \mathcal{O}$. Then α can be written in the form a/b, where $a, b \in \mathcal{O}$ and $(a, b) = 1$. Since $\mathcal{O}$ is factorial there exists a prime element $p \in \mathcal{O}$, which divides b and does not divide a. Let $F(x) = x^n + a_1x^{n-1} + ... + a_n \in \mathcal{O}[x]$ and $F(a/b) = 0$. Then $a^n + a_1a^{n-1}b + ... + a_nb^n = 0$. Since $p|b$, we have $p|a^n$ and, hence, $p|a$. A contradiction.

Let L be a finite extension of a field k. For a fixed element $\alpha \in L$ we define an endomorphism $\hat{\alpha}$ of the field L into itself by $\hat{\alpha}(a) = a\alpha$ for an arbitrary element $a \in L$. Clearly, this endomorphism is a linear transformation of L considered as a vector space over k.

Denote by $End_k(L)$ the set of all linear transformations of the field L considered as a vector space over the field k. Clearly, the map $\alpha \mapsto \hat{\alpha}$ gives a monomorphism of the field L into the ring $End_k(L)$.

The characteristic polynomial $\chi_{\hat{\alpha}}(x)$ of the linear transformation $\hat{\alpha}$ is called the **characteristic polynomial of the element** α and is denoted by $\chi_\alpha(x)$; the minimal polynomial $\mu_{\hat{\alpha}}(x)$ of the transformation $\hat{\alpha}$ is called the **minimal polynomial of the element** α and denoted by $\mu_\alpha(x)$. Clearly, $\chi_\alpha(\alpha) = \mu_\alpha(\alpha) = 0$; moreover $\chi_\alpha(x), \mu_\alpha(x) \in k[x]$ and $\mu_\alpha(x)$ is the monic polynomial of least degree, which has α as a root. Therefore, $\mu_\alpha(x)$ is an irreducible polynomial.

Let $\alpha \in L$. Denote by $k(\alpha)$ the smallest subfield of the field L containing both the field k and the element α. Let $\mu_\alpha(x) = x^m + a_1x^{m-1} + ... + a_m \in k[x]$. Since $\mu_\alpha(\alpha) = 0$, we have $\alpha^m = -(a_1\alpha^{m-1} + ... + a_m)$. Therefore any expression $b_0\alpha^n + ... + b_n$ with coefficients from k may be rewritten in the form $c_1\alpha^{m-1}+c_2\alpha^{m-2}+...+c_m$, where $c_i \in k$, $i = 1, 2, ..., m$. The set of all such elements forms a ring. Clearly, the elements $1, \alpha, ..., \alpha^{m-1}$ are linearly independent over the field k.

We shall show that an arbitrary nonzero element $c_1\alpha^{m-1}+c_2\alpha^{m-2}+...+c_m$ is invertible. Let $h(x) = c_1x^{m-1} + c_2x^{m-2} + ... + c_m$. Since the degree of $h(x)$ is less than m, owing to the irreducibility of $\mu_\alpha(x)$, we have $(h(x), \mu_\alpha(x)) = 1$. Therefore, there exist polynomials $u(x)$ and $v(x)$ such that $1 = u(x)h(x) + \mu_\alpha(x)v(x)$. Substituting the element α in this equality we obtain $1 = u(\alpha)h(\alpha)$, i.e., the element $h(\alpha)$ is invertible. Hence, it follows that

$$k(\alpha) = \{c_1\alpha^{m-1} + ... + c_{m-1}\alpha + c_m \mid c_1, ..., c_m \in k\}.$$

Therefore, $[k(\alpha) : k] = m$.

Assume that the elements $\theta_1, ..., \theta_n \in L$ form a basis of the field L over the field $k(\alpha)$. Then, by proposition 1.1.1, the elements $\theta_1, \theta_1\alpha$, ..., $\theta_1\alpha^{m-1}$, ..., θ_n, $\theta_n\alpha$, ..., $\theta_n\alpha^{m-1}$ form a basis of the field L over k. Clearly, the matrix of the linear transformation $\hat{\alpha}$ in this basis is a block diagonal matrix, in which on the main diagonal there are n copies of the Frobenius block corresponding to the polynomial $\mu_\alpha(x)$, i.e., matrices of the form:

$$\Phi = \Phi(\mu_\alpha(x)) = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -a_m \\ 1 & 0 & 0 & \dots & 0 & -a_{m-1} \\ 0 & 1 & 0 & \dots & 0 & -a_{m-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & -a_2 \\ 0 & 0 & 0 & \dots & 1 & -a_1 \end{pmatrix}$$

Since the characteristic and minimal polynomials of the Frobenius block Φ coincide and are equal to $\mu_\alpha(x)$, we have $\chi_\alpha(x) = [\mu_\alpha(x)]^n$.

The trace of the linear transformation $\hat{\alpha}$ is called the **trace of the element** α and denoted by $Sp(\alpha)$. Clearly, $Sp(\alpha) \in k$. The map $Sp : L \to k$ is a linear operator of the k-vector space L into the field k.

A finite extension L of a field k is called **separable** if the linear operator $Sp : L \to k$ is nonzero.

Proposition 8.1.5. *Let $\mathcal{O}$ be a factorial ring with a quotient field k, and let L be a finite extension of k. Assume $\alpha \in L$ is integral over $\mathcal{O}$. Then $Sp(\alpha) \in \mathcal{O}$.*

Proof. Let $\alpha \in L$ be an integral element over the factorial ring $\mathcal{O}$. Therefore, there exists a monic polynomial $F(x) \in \mathcal{O}[x]$ such that $F(\alpha) = 0$. Let $\mu_\alpha(x) = x^m + a_1 x^{m-1} + ... + a_m \in k[x]$ be the minimal polynomial of the element α. Applying the arguments above we obtain that $Sp(\alpha) = -na_1$. Therefore, to prove the proposition it is sufficient to show that $\mu_\alpha(x) \in \mathcal{O}[x]$. Since $\mu_\alpha(\alpha) = 0$, we have $\mu_\alpha(x)|F(x)$ in $k[x]$, that is, there exists a polynomial $h(x) \in k[x]$ such that $F(x) = \mu_\alpha(x)h(x)$. Since $F(x)$ is a monic polynomial in $\mathcal{O}[x]$, by the Gauss lemma, $c(F) = c(\mu_\alpha)c(h)$ is a unit of the ring $\mathcal{O}$. By lemma 7.5.3 we can write $\mu_\alpha(x) = c(\mu_\alpha(x))\bar{\mu}_\alpha(x)$ and $h(x) = c(h(x))\bar{h}(x)$ where $\bar{\mu}_\alpha(x)$ and $\bar{h}(x)$ are primitive polynomials in $\mathcal{O}[x]$. Then $F(x) = \bar{\mu}_\alpha(x)\bar{h}(x)$. Let a'_0 and b'_0 be the leading coefficients of the polynomials $\bar{\mu}_\alpha(x)$ and $\bar{h}(x)$, respectively. Then $a'_0 b'_0$ is a unit and, since $a'_0 c(\mu_\alpha)$ is a also unit, we obtain $\mu_\alpha(x) \in \mathcal{O}[x]$. Therefore, $Sp(\alpha) \in \mathcal{O}$.

Theorem 8.1.6. *Let $\mathcal{O}$ be a Noetherian factorial ring, and let L be a finite separable extension of its quotient field k. Then the integral closure Δ of the ring $\mathcal{O}$ in the field L is finitely generated over $\mathcal{O}$.*

To prove this theorem we shall need the following lemma.

Lemma 8.1.7. *Let L be a finite separable extension of a field k and let $w_1, ..., w_n$ be a basis of the field L over k. Then the matrix $S = (Sp(w_i w_j)) \in M_n(k)$, $(i, j = 1, ..., n)$, is invertible.*

Proof. The entries of the matrix S belong to the field k. Assume that the matrix S is not invertible. Then the rows of the matrix S are linearly dependent over the field k, i.e., there are elements $c_1, ..., c_n \in k$, which are all not equal to zero and such that $c_1 Sp(w_1 w_i) + c_2 Sp(w_2 w_i) + ... + c_n Sp(w_n w_i) = 0$ for $i = 1, 2, ..., n$. Let $\alpha = c_1 w_1 + ... + c_n w_n$. Then $\alpha \neq 0$ and, because Sp is a linear operator, we obtain that $Sp(\alpha w_i) = 0$ for every $i = 1, 2, ..., n$. Therefore $Sp(\alpha\beta) = 0$ for any $\beta \in L$, contradicting the separability of the field L.

Proof of theorem 8.1.6. By proposition 8.1.2, one may assume that the elements $w_1, ..., w_n$ are integral over $\mathcal{O}$. Denote by $M = w_1\mathcal{O} + ... + w_n\mathcal{O}$ the finitely generated $\mathcal{O}$-module generated by $w_1, w_2, ..., w_n$. It is a submodule of Δ. Set $M^* = \{\alpha \in L \mid Sp(\alpha m) \in \mathcal{O} \text{ for any } m \in M\}$. It is easy to verify that if there exist elements $w_1^*, ..., w_n^* \in L$ such that $Sp(w_i w_j^*) = \delta_{ij}$ $(i, j = 1, 2, ..., n)$, then $M^* = w_1^*\mathcal{O} + ... + w_n^*\mathcal{O}$.

We now show that such elements exist. We shall look for w_j^* in the form

$w_j^* = x_1^j w_1 + ... + x_n^j w_n$, where $x_1^j, ..., x_n^j$ are variables. For each $j = 1, .., n$ this yields a system of linear equations:

$$\sum_{i=1}^{n} Sp(w_i w_k) x_i^j = Sp(w_k w_j^*) \quad (k = 1, .., n)$$

with respect to the variables $x_1^j, ..., x_n^j$ with matrix S. In view of lemma 8.1.7, by Cramer's rule such a system has a unique solution.

Since $M \subset \Delta$, for any $\delta \in \Delta$ and any $m \in M$ we have $\delta m \in \Delta$ and, by proposition 8.1.5, $Sp(\delta m) \in \mathcal{O}$. So, $\Delta \subset M^*$. Since Δ is an $\mathcal{O}$-module and the ring $\mathcal{O}$ is Noetherian, the ring Δ is a finitely generated $\mathcal{O}$-module as a submodule of the finitely generated $\mathcal{O}$-module M^*. The theorem is proved.

Theorem 8.1.8. *Let $\mathcal{O}$ be a principal ideal domain and let L be a finite separable extension of its quotient field k with degree equal to n. Then there exist elements $w_1, ..., w_n \in \Delta$ such that $\Delta = w_1\mathcal{O} \oplus ... \oplus w_n\mathcal{O}$, where Δ is the integral closure of the ring $\mathcal{O}$ in L.*

Proof. By theorem 8.1.6 the ring Δ is a finitely generated as $\mathcal{O}$-module. Therefore, by theorem 7.8.2, Δ decomposes into a direct sum of cyclic $\mathcal{O}$-modules. Since Δ is a torsion free $\mathcal{O}$-module, all its summands are isomorphic to $\mathcal{O}$. Therefore there are elements $w_1, ..., w_m \in \Delta$ such that $\Delta = w_1\mathcal{O} \oplus w_2\mathcal{O} \oplus ... \oplus w_m\mathcal{O}$. Clearly, the elements $w_1, ..., w_n$ are linearly independent over k. By proposition 1.1.1, any element of L can be written as a linear combination of elements $w_1, ..., w_m$ with coefficients of k. Therefore, the elements $w_1, ..., w_m$ form a basis of the field L over k, and, hence, $m = n$. The theorem is proved.

8.2. DEDEKIND DOMAINS

Let k be a finite extension of the field $\mathbf{Q}$ of rational numbers. Consider the integral closure $\mathcal{O}$ of the integers $\mathbf{Z}$ in the field k. The ring $\mathcal{O}$ consists of all algebraic integers, which are in the field k. By proposition 8.1.2, the field k is the quotient field of the ring $\mathcal{O}$.

Let $[k : \mathbf{Q}] = n$. Then $Sp(1) = n \neq 0$ and, therefore, k is a separable extension of the field $\mathbf{Q}$. By theorem 8.1.8 the additive group of the ring $\mathcal{O}$ is a free Abelian group of rank n, i.e., $\mathcal{O} \simeq \mathbf{Z}^n$. Since any subgroup of a free Abelian group of rank n is free of rank $m \leq n$, it follows that the ring $\mathcal{O}$ is Noetherian.

Lemma 8.2.1. *An ideal $\mathcal{P}$ of a ring $\mathcal{O}$ is prime if and only if for any ideals $\mathcal{A}, \mathcal{B} \subset \mathcal{O}$ the inclusion $\mathcal{AB} \subset \mathcal{P}$ implies that either $\mathcal{A} \subset \mathcal{P}$ or $\mathcal{B} \subset \mathcal{P}$.*

Proof. Let $\mathcal{P}$ be a prime ideal. Suppose that $\mathcal{AB} \subset \mathcal{P}$ but $\mathcal{A} \not\subset \mathcal{P}$ and $\mathcal{B} \not\subset \mathcal{P}$. Then there are elements $a \in \mathcal{A}$, $b \in \mathcal{B}$ such that $ab \in \mathcal{P}$ but $a, b \notin \mathcal{P}$. A contradiction.

Conversely, assume that from the inclusion $\mathcal{AB} \subset \mathcal{P}$ it follows that either $\mathcal{A} \subset \mathcal{P}$ or $\mathcal{B} \subset \mathcal{P}$. Suppose that an ideal $\mathcal{P}$ is not prime. Then there are elements $a, b \notin \mathcal{P}$ such that $ab \in \mathcal{P}$. Considering the principal ideals (a) and (b) we obtain that $(a) \not\subset \mathcal{P}$, $(b) \not\subset \mathcal{P}$, but $(a)(b) \subset \mathcal{P}$.

Recall that an ideal $\mathcal{M}$ in a ring A is called **maximal** if there is no ideal $\mathcal{I}$ in A, distinct from $\mathcal{M}$ and A, such that $\mathcal{M} \subset \mathcal{I} \subset A$.

Proposition 8.2.2. *An ideal $\mathcal{M}$ in a commutative ring A is maximal if and only if $A/\mathcal{M}$ is a field.*

Proof. Let $\pi : A \to A/\mathcal{M}$ be the natural projection. Then $A/\mathcal{M}$ is a field if and only if any element of the form $\pi(a)$, $a \notin \mathcal{M}$, is invertible.

Let $\mathcal{M}$ be a maximal ideal in a ring A. Consider an arbitrary nonzero element $\pi(x) \in A/\mathcal{M}$. Then $x \in A$ and $x \notin \mathcal{M}$. Consider the ideal $\mathcal{I} = (x) + \mathcal{M} \neq \mathcal{M}$. Since $\mathcal{M}$ is a maximal ideal, $\mathcal{I} = A$. Therefore, there exists an element $y \in A$ and an element $m \in \mathcal{M}$ such that $xy + m = 1$. Then $\pi(x)\pi(y) = 1$ in $A/\mathcal{M}$ so that $\pi(x)$ is invertible in $A/\mathcal{M}$, i.e., $A/\mathcal{M}$ is a field.

Conversely, let $A/\mathcal{M}$ be a field for some ideal $\mathcal{M}$ in A. Consider an ideal $\mathcal{I}$ such that $\mathcal{M} \subset \mathcal{I} \subset A$. Suppose $\mathcal{I} \neq \mathcal{M}$. Then there exists an element $x \in \mathcal{I}$ and $x \notin \mathcal{M}$. Then $\pi(x) \neq 0$ and, since $A/\mathcal{M}$ is a field, there exists a nonzero element $\pi(y) \in A/\mathcal{M}$ such that $\pi(x)\pi(y) = 1$ with $y \in A$, $y \notin \mathcal{M}$. Therefore there is an element $m \in M$ such that $xy = 1 + m$. Since $x \in \mathcal{I}$ and $m \in \mathcal{M} \subset \mathcal{I}$, we have $1 \in \mathcal{I}$, i.e., $\mathcal{I} = A$. This completes the proof of the proposition.

From this proposition it immediately follows that all elements of a local ring, which do not belong to the unique maximal ideal are invertible.

Proposition 8.2.3. *A maximal ideal $\mathcal{M}$ of a commutative ring $\mathcal{O}$ is prime.*

Proof. This proposition immediately follows from proposition 8.2.2 and the simple fact that any field is, obviously, a domain.

Let $\mathcal{A} \subset \mathcal{O}$ be an ideal of the integral closure $\mathcal{O}$ of the integers $\mathbf{Z}$ in a field k and let $w_1, ..., w_n$ be a basis of the additive group $\mathcal{O}$ as a free Abelian group. If $\alpha \in \mathcal{A}$ and $\alpha \neq 0$, then the elements $w_1\alpha, ..., w_n\alpha$ are linearly independent over $\mathbf{Z}$ and are in $\mathcal{A}$. Therefore the rank of the additive group $\mathcal{A}$ is equal to n and the quotient ring $\mathcal{O}/\mathcal{A}$ is finite. Since a finite commutative domain is a field, any nonzero prime ideal in the ring $\mathcal{O}$ is maximal.

We shall show that the ring $\mathcal{O}$ is integrally closed. Let α be an element of the field k which is integral over $\mathcal{O}$. Set $M = \mathcal{O}[\alpha]$. Clearly, M is a finitely generated $\mathbf{Z}$-module and $\alpha M \subset M$. Then, by definition, the element α is integral over $\mathbf{Z}$ and $\alpha \in \mathcal{O}$. Therefore, the ring $\mathcal{O}$ is integrally closed.

Thus, we have shown that the ring $\mathcal{O}$ of all algebraic integers, which are in a finite extension of the field of rational numbers, is a Noetherian commutative

integrally closed domain in which any nonzero prime ideal is maximal. Such rings were a subject of study in connection with the problem of the uniqueness of factorization into prime elements. These rings play an important role in the theory of rings; they are called Dedekind rings.

Definition. A Noetherian commutative integrally closed domain in which any nonzero prime ideal is maximal is called a **Dedekind domain**.

Thus, we have already proved above the following theorem.

Theorem 8.2.4. *The ring of all algebraic integers in a field of algebraic numbers is a Dedekind domain.*

In fact, Dedekind domains first appeared precisely as rings of integers of algebraic number fields. For such rings R.Dedekind introduced the notion of an ideal.[1]) It was shown that uniqueness of factorization into prime elements usually does not hold in such rings but uniqueness of factorization into prime ideals does hold. The main purpose of this section is to show that any nonzero ideal of a Dedekind domain can be uniquely decomposed into a product of prime ideals.

Note that there are rings which are factorial but not Dedekind and vice versa.

Example 8.2.1.

Let $k[x, y]$ be the ring of polynomials in two variables x and y over a field k. By theorem 7.5.7, it is a factorial ring. On the other hand, it is clear that the ideal (x), generated by the variable x, is prime but it is not maximal. Therefore $k[x, y]$ is not a Dedekind domain.

Example 8.2.2.

Now we give an example of a ring which is Dedekind but not factorial. For this purpose we consider the integral closure of the ring $\mathbf{Z}$ in the quadratic field $\mathbf{Q}(\sqrt{-5})$ and show that it is the ring $\mathbf{Z}[\sqrt{-5}]$. The minimal polynomial of any element $r + r_1\sqrt{-5}$ over $\mathbf{Q}$ has the form $x^2 + ax + b$ with $a, b \in \mathbf{Q}$. The quadratic field $\mathbf{Q}(\sqrt{-5})$ is a Galois extension of $\mathbf{Q}$ of degree 2 with Galois group $\{1, \sigma\}$, where

$$\sigma(r + r_1\sqrt{-5}) = r - r_1\sqrt{-5}$$

for all $r, r_1 \in \mathbf{Q}$. Since the element $\bar{\alpha} = r - r_1\sqrt{-5}$ is conjugate to the element $\alpha = r + r_1\sqrt{-5}$, we have $Sp(\alpha) = \alpha + \bar{\alpha} = 2r$ and $N(\alpha) = \alpha\bar{\alpha} = r^2 + 5r_1^2$. Let $\alpha = r + r_1\sqrt{-5} \in \mathbf{Q}(\sqrt{-5})$ be an algebraic integer. Then the minimal polynomial of α has the form $\mu_\alpha(x) = x^2 - Sp(\alpha)x + N(\alpha)$, where $N(\alpha), Sp(\alpha) \in \mathbf{Z}$. Therefore $2r$, $r^2 + 5r_1^2 \in \mathbf{Z}$, whence we obtain $r = \dfrac{m}{2}$, $r_1 = \dfrac{n}{2}$, where $m, n \in \mathbf{Z}$. Hence,

$$m^2 + 5n^2 \equiv 0 (mod\ 4). \tag{8.2.1}$$

[1]) The word "ideal" historically comes from "ideal number". That is, to preserve unique factorization one has to introduce ideal numbers besides "normal" algebraic numbers.

Since we have either $b^2 \equiv 0(mod\ 4)$ or $b^2 \equiv 1(mod\ 4)$ for any $b \in \mathbf{Z}$, equality (8.2.1) is true in $\mathbf{Z}$ if and only if $m \equiv n \equiv 0(mod\ 2)$, i.e., $r, r_1 \in \mathbf{Z}$. Thus, $\mathbf{Z}[\sqrt{-5}]$ is the ring of all algebraic integers of the quadratic field $\mathbf{Q}(\sqrt{-5})$ and by theorem 8.2.4 it is a Dedekind domain. On the other hand, in section 7.2 it was shown that this ring is not factorial.

Definition. Let $\mathcal{O}$ be a domain with a quotient field k. A **fractional ideal** of the ring $\mathcal{O}$ in the field k is any $\mathcal{O}$-module $\mathcal{A} \subset k$, for which there exists an element $c \neq 0$, $c \in \mathcal{O}$ such that $c\mathcal{A} \subset \mathcal{O}$. In particular, an ordinary ideal $\mathcal{I} \subset \mathcal{O}$ is a fractional ideal and we shall also call it an **integral ideal**.

Any finitely generated $\mathcal{O}$-module M contained in the field k is a fractional ideal in k. Indeed, let M be generated by elements $x_1, x_2, ..., x_n \in k$. Suppose, $x_i = a_i/b_i$, where $a_i, b_i \in \mathcal{O}$. If $m = \prod_{i=1}^{n} b_i$, then x_i may be rewritten in the form $x_i = y_i/m$, where $y_i \in \mathcal{O}$. Therefore $mM \subseteq \mathcal{O}$ and $m \neq 0$, $m \in \mathcal{O}$. On the other hand, if the ring $\mathcal{O}$ is Noetherian, then the module $c\mathcal{A}$ and hence $\mathcal{A}$ is finitely generated. So, any fractional ideal in a Noetherian ring $\mathcal{O}$ is a finitely generated $\mathcal{O}$-module.

The intersection of any set of fractional ideals is also a fractional ideal. We can also define the product of fractional ideals $\mathcal{A}$, $\mathcal{B}$ as a module generated by all products ab, where $a \in \mathcal{A}$ and $b \in \mathcal{B}$. It is clear that a product of finitely generated modules is a finitely generated module. Therefore in a Dedekind domain the product of fractional ideals is also a fractional ideal. Since the multiplication of ideals is associative and commutative and, since the product of nonzero fractional ideals is not equal to zero, we can talk about a semigroup of nonzero fractional ideals. The identity of this semigroup is the domain $\mathcal{O}$ itself. Thus, we have proved the following statement.

Lemma 8.2.5. *The set of all fractional ideals of a Dedekind domain forms a semigroup with respect to ideal multiplication.*

The main purpose of this section is to prove that the nonzero fractional ideals of a Dedekind domain, in fact, form an Abelian group with respect to multiplication.

A fractional ideal $\mathcal{A}$ in the field k is called **invertible** if there exists a fractional ideal $\mathcal{A}^{-1}$ such that $\mathcal{A}\mathcal{A}^{-1} = \mathcal{O}$.

Theorem 8.2.6. *The nonzero fractional ideals of a Dedekind domain $\mathcal{O}$ with a quotient field k form an Abelian group with respect to multiplication.*

Proof. We shall prove this theorem following E.Noether. Let $\mathcal{A}$ be a nonzero ideal of the ring $\mathcal{O}$. We shall show that there is a product of nonzero prime ideals $\mathcal{P}_1, ..., \mathcal{P}_r$ contained in $\mathcal{A}$. If this is not so, then, in view of the Noetherianness of the ring $\mathcal{O}$, there exists a nonzero ideal $\mathcal{B}$, which is maximal in the set of ideals

not containing a product of prime ideals. By hypothesis, this ideal is not prime. Therefore, there are elements $b_1, b_2 \in \mathcal{B}$ such that $b_1 b_2 \in \mathcal{B}$ but $b_1 \notin \mathcal{B}$ and $b_2 \notin \mathcal{B}$. Let $\mathcal{B}_1 = (\mathcal{B}, b_1)$ and $\mathcal{B}_2 = (\mathcal{B}, b_2)$. Clearly, $\mathcal{B}_i \neq \mathcal{B}$ $(i = 1, 2)$ and $\mathcal{B}_1 \mathcal{B}_2 \subset \mathcal{B}$. Since the ideal $\mathcal{B}$ is maximal in the set described above, then the ideals $\mathcal{B}_1$ and $\mathcal{B}_2$ contain some products of prime ideals. But then $\mathcal{B}$ also contains a product of prime ideals. A contradiction.

Now, let's show that any maximal ideal $\mathcal{P} \subset \mathcal{O}$ is invertible. Let $\mathcal{P}^{-1} = \{\alpha \in k \mid \alpha\mathcal{P} \subset \mathcal{O}\}$. It is clear that $\mathcal{P}^{-1}$ is a fractional ideal in k. We claim that $\mathcal{P}^{-1} \neq \mathcal{O}$. Indeed, let $a \in \mathcal{P}$, $a \neq 0$ and consider the least number r for which there is a product $\mathcal{P}_1 ... \mathcal{P}_r \subset (a) \subset \mathcal{P}$. Since the ideal $\mathcal{P}$ is prime, one of the ideals, for example $\mathcal{P}_1$, is contained in $\mathcal{P}$, i.e., $\mathcal{P}_1 \subset \mathcal{P}$. Because the ideal $\mathcal{P}_1$ is maximal, we obtain that $\mathcal{P} = \mathcal{P}_1$. Since r is minimal, we have $\mathcal{P}_2 ... \mathcal{P}_r \not\subset (a)$. Therefore there is an element $b \in \mathcal{P}_2 ... \mathcal{P}_r$, $b \notin (a)$ and $b\mathcal{P} \subset (a)$. But then $ba^{-1}\mathcal{P} \subset \mathcal{O}$, i.e., $ba^{-1} \in \mathcal{P}^{-1}$. Since $b \notin (a)$, we have $ba^{-1} \notin \mathcal{O}$. Therefore, $\mathcal{P}^{-1} \neq \mathcal{O}$.

Thus, there are the inclusions $\mathcal{P} \subseteq \mathcal{P}\mathcal{P}^{-1} \subseteq \mathcal{O}$. Since the ideal $\mathcal{P}$ is maximal, we obtain that either $\mathcal{P}\mathcal{P}^{-1} = \mathcal{P}$ or $\mathcal{P}\mathcal{P}^{-1} = \mathcal{O}$. Suppose, we have the first case, that is, $\mathcal{P}\mathcal{P}^{-1} = \mathcal{P}$. Let $\alpha \in \mathcal{P}^{-1} \backslash \mathcal{O}$. Then $\alpha\mathcal{P} \subset \mathcal{P}$. Since the ring $\mathcal{O}$ is Noetherian and integrally closed, by proposition 8.1.1, $\alpha \in \mathcal{O}$. The obtained contradiction shows that $\mathcal{P}\mathcal{P}^{-1} = \mathcal{O}$.

The next step of the proof is to show that every nonzero ideal $\mathcal{A} \subset \mathcal{O}$ has a fractional inverse. Suppose that this is not the case. Then the set of proper ideals that has not a fractional inverse is not empty. Therefore, by the Noetherian property of $\mathcal{O}$, this set contains a maximal element $\mathcal{B}$. Thus, $\mathcal{B}$ is a noninvertible ideal and this ideal cannot be maximal in $\mathcal{O}$. Therefore there exists a maximal ideal $\mathcal{P} \neq \mathcal{O}$ such that $\mathcal{B} \subset \mathcal{P} \subset \mathcal{O}$. Then we have

$$\mathcal{B} \subset \mathcal{B}\mathcal{P}^{-1} \subset \mathcal{B}\mathcal{B}^{-1} \subset \mathcal{O}.$$

Moreover, $\mathcal{B} \neq \mathcal{B}\mathcal{P}^{-1}$, since the ring $\mathcal{O}$ is integrally closed and $\mathcal{O} \neq \mathcal{P}^{-1}$. Therefore, by the maximal property of $\mathcal{B}$, there is a fractional ideal $\mathcal{C} \subset k$, which is the inverse of $\mathcal{B}\mathcal{P}^{-1}$, i.e., $\mathcal{B}\mathcal{P}^{-1}\mathcal{C} = \mathcal{O}$. Hence, the ideal $\mathcal{C}_1 = \mathcal{P}^{-1}\mathcal{C}$ is an inverse of $\mathcal{B}$. A contradiction.

It remains to prove that any nonzero fractional ideal $\mathcal{A}$ of the ring $\mathcal{O}$ is invertible. There exists an element $c \in \mathcal{O}$, $c \neq 0$ such that $c\mathcal{A} \subset \mathcal{A}$. Since the ideal $c\mathcal{A}$ is invertible, for some fractional ideal $\mathcal{B}$ we have $c\mathcal{A}\mathcal{B} = \mathcal{O}$, i.e., the ideal $c\mathcal{B}$ is then an inverse of $\mathcal{A}$.

Taking into account lemma 8.2.5 the theorem is proved.

Definition. Let $\mathcal{A}$ and $\mathcal{B}$ be ideals of an integral domain $\mathcal{O}$. We shall say that $\mathcal{A}$ **divides** $\mathcal{B}$ and write $\mathcal{A}|\mathcal{B}$ if there is an ideal $\mathcal{C}$ such that $\mathcal{A}\mathcal{C} = \mathcal{B}$.

If $\mathcal{A}$ divides $\mathcal{B}$, then certainly $\mathcal{B} \subset \mathcal{A}$. If $\mathcal{O}$ is a Dedekind domain the converse is also true. In fact, the inclusion $\mathcal{B} \subset \mathcal{A}$ is equivalent to an equality $\mathcal{A}\mathcal{C} = \mathcal{B}$, since we can put $\mathcal{C} = \mathcal{A}^{-1}\mathcal{B} \subset \mathcal{A}^{-1}\mathcal{A} = \mathcal{O}$.

Lemma 8.2.1 states that for a prime ideal $\mathcal{P} \subset \mathcal{O}$ from $\mathcal{P}|\mathcal{AB}$ it follows that either $\mathcal{P}|\mathcal{A}$ or $\mathcal{P}|\mathcal{B}$.

Now we can prove the uniqueness of factorization of ideals into prime ideals in a Dedekind domain.

Theorem 8.2.7. *Any nonzero integral ideal $\mathcal{A}$ of a Dedekind domain $\mathcal{O}$ with a quotient field k can be uniquely decomposed into a product of prime ideals.*

Proof. Suppose that there is a nonzero integral ideal, which cannot be decomposed into a product of prime ideals. Consider the set of all integral ideals with such a property. Then, by the Noetherian property of $\mathcal{O}$, this set contains a maximal element. Let the ideal $\mathcal{B}$ be a maximal element in this set. Clearly, it is not prime. Therefore, there exists a prime ideal $\mathcal{P} \neq \mathcal{O}$ such that $\mathcal{B} \subset \mathcal{P} \subset \mathcal{O}$. But then $\mathcal{B} \subset \mathcal{BP}^{-1} \subset \mathcal{O}$ and, because the ring $\mathcal{O}$ is integrally closed and Noetherian, the inclusion $\mathcal{B} \subset \mathcal{BP}^{-1}$ is strict. By the maximal property of $\mathcal{B}$, $\mathcal{BP}^{-1} = \mathcal{P}_2...\mathcal{P}_r$, and, hence, $\mathcal{B} = \mathcal{PP}_2...\mathcal{P}_r$. A contradiction.

The uniqueness of factorization of an ideal into a product of prime ideals is established by induction on the least number of prime ideals in its factorization. Let $\mathcal{P}_1...\mathcal{P}_r = \mathcal{Q}_1...\mathcal{Q}_s$ be two factorizations of an ideal into products of prime ones. Then $\mathcal{P}_1|\mathcal{Q}_1...\mathcal{Q}_s$ and, hence, $\mathcal{P}_1$ divides one of the ideals $\mathcal{Q}_1, ..., \mathcal{Q}_s$ and, in view of the maximal property, it coincides with one of them. Multiplying both sides of the equality by $\mathcal{P}_1^{-1}$, by the induction hypothesis, we obtain that $r = s$ and the prime factors on the right side and on the left side coincide up to a permutation. The theorem is proved.

Let $\mathcal{O}$ be a Dedekind domain with a quotient field k. If $\mathcal{I}$ is a nonzero fractional ideal of the ring $\mathcal{O}$, then there exists a nonzero element $c \in \mathcal{O}$ such that $c\mathcal{I} \subset \mathcal{O}$. Let $(c) = \mathcal{P}_1...\mathcal{P}_r$ and $c\mathcal{I} = \mathcal{Q}_1...\mathcal{Q}_s$ be decompositions of these ideals into products of prime ideals. Then, obviously, $\mathcal{I} = \mathcal{Q}_1...\mathcal{Q}_s\mathcal{P}_1^{-1}...\mathcal{P}_r^{-1}$. Grouping the same prime ideals together we obtain $\mathcal{I} = \prod\limits_{\mathcal{P}} \mathcal{P}^{r_\mathcal{P}}$, where the $r_\mathcal{P}$ are integers, and only a finite number of them are not equal to zero. The number $r_\mathcal{P}$ is called the **exponent of the ideal** $\mathcal{I}$ with respect to $\mathcal{P}$ and denoted by $ord_\mathcal{P}\mathcal{I}$.

Proposition 8.2.8. *Let $\mathcal{O}$ be a Dedekind domain and let $\mathcal{I}$ and $\mathcal{J}$ be two nonzero integral ideals in $\mathcal{O}$ with prime ideal factorizations $\mathcal{I} = \prod\limits_{\mathcal{P}} \mathcal{P}^{r_\mathcal{P}}$ and $\mathcal{J} = \prod\limits_{\mathcal{P}} \mathcal{P}^{s_\mathcal{P}}$, where $r_\mathcal{P}, s_\mathcal{P} \geq 0$ for all prime ideals $\mathcal{P} \subset \mathcal{O}$. Then*

(1) *$\mathcal{I} \supset \mathcal{J}$ if and only if $ord_\mathcal{P}\mathcal{I} \leq ord_\mathcal{P}\mathcal{J}$ for all prime ideals $\mathcal{P} \subset \mathcal{O}$.*

(2) *$\mathcal{I} + \mathcal{J} = (\mathcal{I}, \mathcal{J})$ and $ord_\mathcal{P}(\mathcal{I} + \mathcal{J}) = min\{ord_\mathcal{P}\mathcal{I}, ord_\mathcal{P}\mathcal{J}\}$. In particular, $\mathcal{I}$ and $\mathcal{J}$ are comaximal, i.e., $\mathcal{I} + \mathcal{J} = \mathcal{O}$ if and only if they have no common prime ideal factors.*

(3) *$ord_\mathcal{P}(\mathcal{I} \cap \mathcal{J}) = max\{ord_\mathcal{P}\mathcal{I}, ord_\mathcal{P}\mathcal{J}\}$.*

Proof. Statement (1) follows from the definition of prime ideals and the fact proved above that $\mathcal{I} \subset \mathcal{J}$ if and only if $\mathcal{J}$ divides $\mathcal{I}$.

Since $\mathcal{I}+\mathcal{J}$ is the smallest ideal containing both $\mathcal{I}$ and $\mathcal{J}$, statement (2) follows from statement (1).

Statement (3) is obvious.

Consider fractional ideals $\mathcal{I} = \prod_{\mathcal{P}} \mathcal{P}^{r_\mathcal{P}}$ and $\mathcal{J} = \prod_{\mathcal{P}} \mathcal{P}^{s_\mathcal{P}}$. We have $\mathcal{I}\mathcal{J} = \prod_{\mathcal{P}} \mathcal{P}^{r_\mathcal{P}+s_\mathcal{P}}$. Let the ideals $\mathcal{I}$ and $\mathcal{J}$ have the property that the nonzero exponents of ideals $\mathcal{I}$ and $\mathcal{J}$ belong to distinct prime ideals. Then from proposition 8.2.8 it immediately follows that $\mathcal{I}\mathcal{J} = \mathcal{I} \cap \mathcal{J}$.

In particular, if $\mathcal{I} \subset \mathcal{O}$ is an integral ideal of the ring $\mathcal{O}$ and $\mathcal{I} = \mathcal{P}_1^{n_1}...\mathcal{P}_s^{n_s}$, where the prime ideals $\mathcal{P}_1, ..., \mathcal{P}_s$ are all distinct, then $\mathcal{P}_1^{n_1} \cap \mathcal{P}_2^{n_2} \cap ... \cap \mathcal{P}_s^{n_s} = \mathcal{I}$. Taking into account that the $\mathcal{P}^{n_i}$ are pairwise comaximal ideals and using theorem 7.6.2 we obtain a Chinese remainder theorem for Dedekind domains:

Theorem 8.2.9. *Let $\mathcal{O}$ be a Dedekind domain, let $\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_s$ be distinct prime ideals in $\mathcal{O}$ and let $n_i \geq 0$ be integers, $i = 1, 2, ..., s$. Then*

$$\mathcal{O}/\mathcal{P}_1^{n_1}...\mathcal{P}_s^{n_s} \simeq \mathcal{O}/\mathcal{P}_1^{n_1} \times ... \times \mathcal{O}/\mathcal{P}_s^{n_s}$$

Equivalently, for any sets of s elements $a_1, a_2, ..., a_s \in \mathcal{O}$ there exists an element $a \in \mathcal{O}$ such that $a \equiv a_i (mod \mathcal{P}_i^{n_i})$ for $i = 1, 2, ..., s$.

8.3. HEREDITARY DOMAINS

Recall that a ring A is called **right hereditary** if every right ideal of it is projective. In this section we shall study the connection of Dedekind domains with commutative hereditary rings.

First we shall prove the following criterion of the projective property of a module over an arbitrary ring.

Proposition 8.3.1. *An A-module P is projective if and only if there is a system of elements $\{p_\alpha\}$ of P and a system of homomorphisms $\{\varphi_\alpha\}$, $\varphi_\alpha : P \to A$ such that any element $p \in P$ may be written in the form:*

$$p = \sum_\alpha p_\alpha(\varphi_\alpha(p)), \tag{8.3.1}$$

where only a finite number of elements $\varphi_\alpha(p) \in A$ are not equal to zero.

Proof. Let $\pi : F \to P$ be an epimorphism of a free module F with free basis $\{e_\alpha\}$ onto the module P and let $p_\alpha = \pi(e_\alpha)$. By proposition 5.1.6, P is projective if and only if there is a homomorphism $i : P \to F$ such that $\pi i = 1_P$. Any element $i(p)$ may be written in the form $i(p) = \sum_\alpha (\varphi_\alpha p) e_\alpha$ and the maps $p \to \varphi_\alpha(p)$

define a system of homomorphisms $\varphi_\alpha : P \to A$ with the property that for any element $p \in P$ only a finite number of elements $\varphi_\alpha(p)$ are not equal to zero. Since $\pi i = 1_P$, we have $p = \sum\limits_\alpha p_\alpha(\varphi_\alpha p)$. So, if the module P is projective, then there is a representation (8.3.1).

Conversely, assume there exist a system of elements, homomorphisms and a representation (8.3.1). Then setting $\pi(\sum\limits_\alpha e_\alpha a_\alpha) = \sum\limits_\alpha p_\alpha a_\alpha$ we obtain a homomorphism $\pi : F \to P$. Using the system of homomorphisms φ_α construct a homomorphism $i : P \to F$ defined by $i(p) = \sum\limits_\alpha e_\alpha(\varphi_\alpha p)$. Clearly, from the representation (8.3.1) it follows that $1_P = \pi i$. The proposition is proved.

In the following two propositions we assume that $\mathcal{O}$ is an integral domain with quotient field k.

Proposition 8.3.2. *A nonzero ideal $\mathcal{I}$ of an integral domain $\mathcal{O}$ is projective if and only if it is invertible.*

Proof. Let $\mathcal{I}$ be a nonzero invertible ideal. Then there exists a fractional ideal $\mathcal{J}$ of the ring $\mathcal{O}$ such that $\mathcal{I}\mathcal{J} = \mathcal{O}$. This means that there are elements $\alpha_1, ..., \alpha_n \in \mathcal{I}$ and $q_1, ..., q_n \in k$ such that $\sum\limits_i \alpha_i q_i = 1$ and $q_i\mathcal{I} \subset \mathcal{O}$ for $i = 1, ..., n$. Set $\varphi_i\alpha = q_i\alpha$ for $i = 1, 2, .., n$, where $\alpha \in \mathcal{I}$. Then there is a system of homomorphisms $\varphi_i : \mathcal{I} \to \mathcal{O}$ for which $\sum\limits_i \alpha_i(\varphi_i\alpha) = \sum\limits_i \alpha_i(q_i\alpha) = \alpha$. By the previous proposition, the ideal $\mathcal{I}$ is projective.

Conversely, let a nonzero ideal $\mathcal{I}$ be projective and let $\{p_i\}$, $\{\varphi_i\}$ be systems of elements and homomorphisms as specified in proposition 8.3.1. Let $\alpha \in \mathcal{I}$ and $\alpha \neq 0$. Set $q_i = \varphi_i(\alpha)/\alpha$. By the properties of the homomorphisms φ_i there are only a finite number of elements q_i such that $q_i \neq 0$. Let these be the elements $q_1, ..., q_n$. For any $\beta \in \mathcal{I}$ we have $\varphi_i(\alpha\beta) = \varphi_i(\alpha)\beta = \varphi_i(\beta)\alpha$. Therefore $\varphi_i(\beta) = q_i\beta$. So $q_i\mathcal{I} \subset \mathcal{O}$. Since $\alpha = \sum\limits_i(\varphi_i\alpha)p_i = \sum\limits_i(q_i\alpha)p_i = \sum\limits_i(q_ip_i)\alpha$, it follows that $\sum\limits_i q_ip_i = 1$ and the ideal $\mathcal{I}$ is invertible. The proposition is proved.

Proposition 8.3.3. *Any invertible ideal $\mathcal{I}$ in an integral domain $\mathcal{O}$ has a finite number of generators.*

Proof. Let $1 = \sum\limits_i q_i\alpha_i$, where $\alpha_i \in \mathcal{I}$, $q_i \in k$ and $q_i\mathcal{I} \in \mathcal{O}$ for $i = 1, 2, ..., n$. Then for any element $\alpha \in \mathcal{I}$ we have the equality $\alpha = \sum\limits_i(q_i\alpha)\alpha_i$. Since $q_i\alpha \in \mathcal{O}$, $\{\alpha_1, ..., \alpha_n\}$ is the system of generators of the ideal $\mathcal{I}$ and $\mathcal{I} = \sum\limits_i \alpha_i\mathcal{O}$.

Theorem 8.3.4. *The following conditions are equivalent for an integral domain $\mathcal{O}$:*

(a) *$\mathcal{O}$ is a Dedekind domain*;

(b) $\mathcal{O}$ *is a hereditary ring.*

Proof.

The implication $(a) \Rightarrow (b)$ follows from proposition 8.3.2.

$(b) \Rightarrow (a)$.

1. From propositions 8.3.2 and 8.3.3 it follows that the ring $\mathcal{O}$ is Noetherian.

2. Let $\mathcal{J}$ be a fractional ideal of the ring $\mathcal{O}$. There exists an element $\alpha \in \mathcal{O}$ such that $\alpha\mathcal{J}$ is an integral ideal in $\mathcal{O}$. By proposition 8.3.2, the ideal $\alpha\mathcal{J} \subset \mathcal{O}$ is invertible and, by proposition 8.3.3, it is finitely generated as an $\mathcal{O}$-module, i.e., $\alpha\mathcal{J} = \sum_{i \in I} \alpha_i \mathcal{O}$. Then $\{\alpha_i/\alpha \mid i \in I\}$ will be a system of generators of $\mathcal{J}$ as an $\mathcal{O}$-module. Thus, any fractional ideal of the ring $\mathcal{O}$ has a finite number of generators. We shall show that the fractional ideal $\mathcal{J}$ is invertible. Since the ideal $\alpha\mathcal{J} \subset \mathcal{O}$ is invertible, there exists a fractional ideal $\mathcal{A}$ such that $\alpha\mathcal{J}\mathcal{A} = \mathcal{O}$, and hence the ideal $\mathcal{J}$ is invertible as well. Thus, all nonzero fractional ideals of the ring $\mathcal{O}$ form a group with respect to multiplication.

We shall show that the ring $\mathcal{O}$ is integrally closed. Let $\alpha\mathcal{I} \subset \mathcal{I}$ for some fractional ideal of the ring $\mathcal{O}$ and $\alpha \in k$. Multiplying both sides of this inclusion by $\mathcal{I}^{-1}$ we obtain $\alpha\mathcal{O} \subset \mathcal{O}$, i.e., $\alpha \in \mathcal{O}$. By proposition 8.1.1, this means that the ring $\mathcal{O}$ is integrally closed.

3. Let $\mathcal{P}$ be a prime ideal in the ring $\mathcal{O}$ and suppose it is not maximal, i.e., $\mathcal{P}$ is strongly contained in some maximal ideal $\mathcal{M}$. Then

$$\mathcal{P} \subset \mathcal{P}\mathcal{M}^{-1} \subset \mathcal{M}\mathcal{M}^{-1} = \mathcal{O}.$$

Since $(\mathcal{P}\mathcal{M}^{-1})\mathcal{M} \subset \mathcal{P}$ and $\mathcal{P}$ is a prime ideal, $\mathcal{M} \not\subset \mathcal{P}$, it follows that $\mathcal{P}\mathcal{M}^{-1} \subset \mathcal{P}$. Therefore $\mathcal{P} \subset \mathcal{P}\mathcal{M}^{-1} \subset \mathcal{P}$, and thus $\mathcal{P}\mathcal{M}^{-1} = \mathcal{P}$. Multiplying this equality by $\mathcal{M}\mathcal{P}^{-1}$ we obtain that $\mathcal{M} = \mathcal{O}$. Therefore any prime ideal is maximal.

The theorem is proved.

8.4. DISCRETE VALUATION RINGS

In this section we discuss an important class of rings which are called discrete valuation rings.

Definition. Let k be a field. A **discrete valuation** on k is a function $\nu : k^* \to \mathbf{Z}$ satisfying

(i) $\nu(xy) = \nu(x) + \nu(y)$ for all $x, y \in k^*$;

(ii) ν is surjective;

(iii) $\nu(x + y) \geq min\{\nu(x), \nu(y)\}$ for all $x, y \in k^*$ with $x + y \neq 0$.

The set $R = \{x \in k^* \mid \nu(x) \geq 0\} \cup \{0\}$ is a subring of k which is called the **valuation ring** of ν. Consider the set $M = \{x \in k^* \mid \nu(x) > 0\}$. It is easy to verify, that M is a maximal ideal in R. An integral domain $\mathcal{O}$ is called a **discrete valuation ring** if there is a valuation ν on its quotient field such that $\mathcal{O}$ is the valuation ring of ν.

Examples 8.4.1.

1. Let k be a field. The formal series ring $k[[x]]$ is a discrete valuation ring.[2])
2. Let $p \in \mathbf{Z}$ be a prime integer, then $\mathbf{Z}_{(p)}$ is a discrete valuation ring.[3])

Proposition 8.4.1. *Any discrete valuation ring is a Euclidean domain.*

Proof. Let $\mathcal{O}$ be a discrete valuation ring with valuation ν and a quotient field k. Note that $\nu(1) = \nu(1) + \nu(1)$ implies $\nu(1) = 0$. Therefore $\nu(a^{-1}) = -\nu(a)$ for any nonzero $a \in k$. Define $N(0) = 0$ and $N(x) = \nu(x)$ for any nonzero element $x \in \mathcal{O}$. We show that N is a Euclidean function. Let $a, b \in \mathcal{O}\backslash\{0\}$. Then

ED1. $N(0) = 0$

ED2. Suppose $\nu(b) < \nu(a)$, then $b = 0 \cdot a + b$ and for $r = b$ we have $N(r) = \nu(b) < \nu(a) = N(a)$. If $\nu(b) \geq \nu(a)$, we set $g = a^{-1}b$. Since $\nu(g) = \nu(a^{-1}) + \nu(b) = \nu(b) - \nu(a) \geq 0$, we have $g \in \mathcal{O}$. Therefore $b = ga$ and $r = 0$.

From propositions 7.3.1, 7.2.1, 8.1.4 and 8.4.1 we immediately obtain the following statement:

Corollary 8.4.2. *If $\mathcal{O}$ is a discrete valuation ring, then*

1. *$\mathcal{O}$ is a PID.*
2. *$\mathcal{O}$ is a hereditary ring.*
3. *$\mathcal{O}$ is a factorial ring.*
4. *$\mathcal{O}$ is integrally closed.*

Proposition 8.4.3. *Let $\mathcal{O}$ be a discrete valuation ring with valuation ν and quotient field k. Let t be any element of $\mathcal{O}$ with $\nu(t) = 1$. Then*

1. *A nonzero element $u \in \mathcal{O}$ is a unit if and only if $\nu(u) = 0$.*
2. *Every nonzero element $r \in \mathcal{O}$ can be written in the form $r = ut^n$ for some unit $u \in \mathcal{O}^*$ and some $n \geq 0$. Every nonzero element $x \in k^*$ can be written in the form $x = ut^n$ for some unit $u \in \mathcal{O}^*$ and some $n \in \mathbf{Z}$.*
3. *Every nonzero ideal of $\mathcal{O}$ is principal and of the form $(t^n) = M^n$ for some $n \geq 0$, where $M = \{x \in k^* \mid \nu(x) > 0\}$.*
4. *$\bigcap_{n=0}^{\infty} M^n = 0$, where $M = \{x \in k^* \mid \nu(x) > 0\}$.*

Proof.

1. Let $u \in \mathcal{O}^*$, then there is an element $v \in \mathcal{O}$ such that $uv = 1$. Therefore $0 = \nu(uv) = \nu(u) + \nu(v)$. Since $\nu(u), \nu(v) \geq 0$, we have $\nu(u) = \nu(v) = 0$.

Conversely, suppose $u \neq 0$ and $\nu(u) = 0$, then for $u^{-1} \in k^*$ and we have $\nu(u^{-1}) = -\nu(u) = 0$, hence $u^{-1} \in \mathcal{O}$, so u is a unit in $\mathcal{O}$.

2. Suppose $r \in \mathcal{O}$ and $\nu(r) = n$, then $\nu(rt^{-n}) = \nu(r) + \nu(t^{-n}) = 0$. Hence $rt^{-n} = u$ is a unit and $r = ut^n$. If $x \in k^*$, then $x = ab^{-1}$, with $a, b \in \mathcal{O}$. Let

---

[2]) Here $\nu(\sum_{i=1}^{\infty} a_i x^i)$ = largest n such that $a_0 = a_1 = \ldots = a_{n-1} = 0$.

[3]) With $\nu(p^i a) = i$ if and only if $(p, a) = 1$.

$a = ut^n$ and $b = vt^m$, where $u, v \in \mathcal{O}^*$. Then $x = (uv^{-1})t^{n-m} = \varepsilon t^s$, where $\varepsilon \in \mathcal{O}^*$ and $s \in \mathbf{Z}$.

3. Let $\mathcal{I}$ be an ideal in $\mathcal{O}$, and let $x \in \mathcal{I}$ be an element with $\nu(x)$ minimal. If $\nu(x) = n$, then $x = ut^n$, where u is a unit. Hence $(t^n) \subset \mathcal{I}$. Let a be an arbitrary element in $\mathcal{I}$, then $\nu(a) \geq n$. So $\nu(at^{-n}) \geq 0$, whence $\nu(at^{-n}) \in \mathcal{O}$ and $a \in (t^n)$. Therefore $\mathcal{I} = (t^n) = t^n\mathcal{O}$. In particular, $M = t\mathcal{O}$. And therefore $\mathcal{I} = M^n$. This means, that M is the unique prime ideal in $\mathcal{O}$.

4. Let $x \in \mathcal{O}$, $x \neq 0$. Let $n = \nu(x)$. Then $x \notin M^{n+1}$ because $\nu(y) \geq n+1$ for all $y \in M^{n+1}$ by 3. Thus $\bigcap_{n=0}^{\infty} M^n = 0$.

From this proposition we can immediately obtain the main properties of discrete valuation rings which we formulate as the following statement:

Corollary 8.4.4. *Let $\mathcal{O}$ be a discrete valuation ring. Then*

1. *$\mathcal{O}$ is a local ring with a unique maximal ideal $M = \{x \in \mathcal{O} \mid \nu(x) > 0\}$ and any nonzero ideal of $\mathcal{O}$ is of the form M^n for some integer $n \geq 0$.*

2. *The only nonzero prime ideal of $\mathcal{O}$ is M.*

The next two statements give properties of a ring which may be used as other equivalent definitions of a discrete valuation ring without using valuations.

Proposition 8.4.5. *The following properties of a ring $\mathcal{O}$ are equivalent*:

1. *$\mathcal{O}$ is a discrete valuation ring.*

2. *$\mathcal{O}$ is a PID with a unique prime ideal $M \neq 0$.*

3. *$\mathcal{O}$ is a PID with a unique maximal ideal $M \neq 0$.*

4. *$\mathcal{O}$ is a Noetherian integral domain that is also a local ring whose unique maximal ideal is nonzero and principal.*

5. *$\mathcal{O}$ is a Noetherian integrally closed integral domain that is also a local ring with unique nonzero prime ideal.*

Proof.

That statement 1 implies the others was proved above.

Since any maximal ideal in commutative ring is prime we have statement $2 \Rightarrow 3$.

$3 \Rightarrow 1$. Let $\mathcal{O}$ be a PID with a unique maximal ideal $M \neq 0$. Let $t_1, t_2 \in \mathcal{O}$ be distinct irreducible elements , then $(t_1) \subset M$ and $(t_2) \subset M$ are distinct prime ideals. Then $(t_1) + (t_2) \in M$ and $(t_1) + (t_2) = \mathcal{O}$. A contradiction. Therefore there is a unique irreducible element of $\mathcal{O}$. Since $\mathcal{O}$ is a factorial ring, any element $x \in \mathcal{O}$ can be written uniquely in the form $x = ut^n$, where $u \in \mathcal{O}^*$ and $n \geq 0$. Then it is easy to verify, that $\nu(x) = n$ is a valuation on $\mathcal{O}$.

$4 \Rightarrow 2$. Suppose $M = (t)$ is a unique maximal ideal in $\mathcal{O}$. Note that $M^n \neq M^{n+1}$ for all $n \geq 0$, since otherwise, by Nakayama's lemma, we obtain $M^n = 0$ and so $t^n = 0$. Since $\mathcal{O}$ is a domain, $t = 0$. A contradiction. We now prove that

$\bigcap_{n=0}^{\infty} M^n = 0$. Let $x \in \bigcap_{n=0}^{\infty} M^n$, $x \neq 0$. Then for suitable $a_i \in \mathcal{O}$

$$x = a_0 = a_1 t = a_2 t^2 = ... = a_n t^n = ...$$

This gives a chain of ideals $(a_1) \subset (a_2) \subset ...$ which must stabilize because $\mathcal{O}$ is Noetherian. So $(a_n) = (a_{n+1})$ for some n, and $a_{n+1} = a_n b$ for some $b \in \mathcal{O}$. Also $a_n t^n = a_{n+1} t^{n+1}$ so $a_n = a_{n+1} t$ using that $\mathcal{O}$ is a domain, and $a_{n+1} = a_n b = a_{n+1} tb$. So using again that $\mathcal{O}$ is a domain, $tb = 1$. This would make t a unit which is not the case.

Let $\mathcal{I}$ be an arbitrary ideal in $\mathcal{O}$. Since $\mathcal{I} \subseteq M$ and $\bigcap_{n=0}^{\infty} M^n = 0$, there exists $n \geq 1$ such that $\mathcal{I} \subseteq M^n$ but $\mathcal{I} \nsubseteq M^{n+1}$. Let $x \in \mathcal{I}$. Then $x \in M^n$ but $x \notin M^{n+1}$. Therefore $x = ut^n$, where $u \notin M$ and so u is a unit in the local ring $\mathcal{O}$. So any element $a \in \mathcal{I}$ is of the form $t^n u$, i.e., the ideal $\mathcal{I} = (t^n)$ and is principal.

$5 \Rightarrow 4$. Let M be a unique prime ideal in a local domain $\mathcal{O}$ with quotient field k. Since any ideal is contained in some maximal ideal of $\mathcal{O}$ and any maximal ideal in a commutative domain is prime, M is also the unique maximal ideal in $\mathcal{O}$.

Let $\mathcal{I}$ be an arbitrary nonzero ideal in $\mathcal{O}$. Then $\mathcal{I} \subseteq M$. We shall show that there exists an integer $n > 0$ such that $M^n \subset \mathcal{I}$. Suppose the contrary. Then by the Noetherian property of $\mathcal{O}$ there is a nonzero ideal $\mathcal{J}$ in $\mathcal{O}$ which is maximal in the set of all ideals not containing M^n for any n. Obviously, $\mathcal{J} \neq M$, i.e., it is not prime. Therefore there are elements $x, y \in \mathcal{J}$ with $xy \in \mathcal{J}$, but $x \notin \mathcal{J}$ and $y \notin \mathcal{J}$. Let $\mathcal{J}_1 = (\mathcal{J}, x)$ and $\mathcal{J}_1 = (\mathcal{J}, y)$. It is clear, that $\mathcal{J}_i \neq \mathcal{J}$ for $i = 1, 2$, and $\mathcal{J}_1 \mathcal{J}_2 \subseteq \mathcal{J}$. Since $\mathcal{J}$ is a maximal element, then $\mathcal{J}_1$ and $\mathcal{J}_2$ contain some power of M. But then $\mathcal{J}$ is also contains some power of M. A contradiction. Thus, any nonzero ideal of $\mathcal{O}$ contains some power of M.

Suppose $M^n = M^{n+1}$. Since $\mathcal{O}$ is a Noetherian ring, by Nakayama's lemma, it follows that $M^n = 0$. Since $\mathcal{O}$ is a domain, we have that $M = 0$. A contradiction. Therefore $M^{n+1} \neq M^n$ for any n and so there is always an element $x \in M^n$ with $x \notin M^{n+1}$.

Let $M^{-1} = \{x \in k \ : xM \subset \mathcal{O}\}$. It is clear that M^{-1} is a fractional ideal in k. Let a be an arbitrary element of M. Consider the principal ideal $(a) \subseteq M$. By the proof above there is an integer $n > 0$ such that $M^n \subseteq (a)$. Let n be the least such number, i.e., $M^{n-1} \nsubseteq (a)$. Then there is an element $b \in M^{n-1}$ such that $b \notin (a)$ and $bM \subseteq (a)$. But then $ba^{-1}M \subseteq \mathcal{O}$, i.e., $ba^{-1} \in M^{-1}$. Since $b \notin (a)$, we have $ba^{-1} \notin \mathcal{O}$. Thus, $M^{-1} \neq \mathcal{O}$.

Thus, we have inclusions $M \subseteq MM^{-1} \subseteq \mathcal{O}$. Since the ideal M is maximal, we obtain that either $MM^{-1} = M$ or $MM^{-1} = \mathcal{O}$. Suppose, we have the first case, that is, $MM^{-1} = M$. Let $y \in M^{-1} \backslash \mathcal{O}$. Then $yM \subset M$. Since the ring $\mathcal{O}$ is Noetherian and integrally closed, by proposition 8.1.1, $y \in \mathcal{O}$. The obtained contradiction shows that $MM^{-1} = \mathcal{O}$, i.e., M would be an invertible ideal.

Since $M^2 \neq M$ there is an element $a \in M$ and $a \notin M^2$. Then we have $aM^{-1} \subseteq \mathcal{O}$ and $a\mathcal{O} \nsubseteq M^2$. Since $MM^{-1} = \mathcal{O}$, we have that $aM^{-1} \nsubseteq M$. So aM^{-1} is an ideal in $\mathcal{O}$ and aM^{-1} is not contained in any maximal ideal. Therefore $aM^{-1} = \mathcal{O}$, i.e., $M = (a)$ is principal.

Finally it is trivial that $2 \Rightarrow 3$. This finishes the proof of the proposition.

Corollary 8.4.6. *Let $\mathcal{P}$ be a nonzero prime ideal of a Dedekind domain $\mathcal{O}$. Then the localization $\mathcal{O}_{\mathcal{P}}$ is a discrete valuation ring.*

Proof. We use property 5 of the previous proposition. Let $\mathcal{O}$ be a Dedekind ring with a quotient field k.

Since any ideal of the ring $\mathcal{O}_{\mathcal{P}}$ is of the form $\mathcal{I}\mathcal{O}_{\mathcal{P}}$, where $\mathcal{I}$ is some ideal of $\mathcal{O}$, a finite set of generators of $\mathcal{I}$ over $\mathcal{O}$ is also a set of generators of $\mathcal{I}\mathcal{O}_{\mathcal{P}}$ over $\mathcal{O}_{\mathcal{P}}$. Therefore, $\mathcal{O}_{\mathcal{P}}$ is a Noetherian ring.

Let $x \in k$ be a integral element over $\mathcal{O}_{\mathcal{P}}$, i.e., $x^n + b^{-1}a_1x^{n-1} + ... + b^{-1}a_n = 0$, where $b, a_i \in \mathcal{O}$ and $b \notin \mathcal{P}$. Then the element bx is integral over $\mathcal{O}$. Since $\mathcal{O}$ is integrally closed, $bx \in \mathcal{O}$ and $x \in \mathcal{O}_{\mathcal{P}}$. So $\mathcal{O}_{\mathcal{P}}$ is integrally closed.

By proposition 7.4.4 $\mathcal{O}_{\mathcal{P}}$ is a local ring with a unique prime ideal. Thus, the ring $\mathcal{O}_{\mathcal{P}}$ satisfies all conditions of property 5 of proposition 8.4.5 and so it is a discrete valuation ring.

Dedekind domains are generalization of PIDs, for which each ideal is principal, i.e., can be generated by only one element. The following proposition proves the interesting fact that every ideal of Dedekind domain can be generated by only two elements.

Proposition 8.4.7. *Let $\mathcal{I}$ be a nonzero ideal of a Dedekind domain $\mathcal{O}$. Then*

1. *There exists an ideal $\mathcal{J}$ of $\mathcal{O}$ relatively prime to $\mathcal{I}$ such that the product $\mathcal{I}\mathcal{J} = (a)$ is a principal ideal.*
2. *The quotient ring $\mathcal{O}/\mathcal{I}$ is a PID.*
3. *Every ideal of $\mathcal{O}$ can be generated by two elements.*

Proof.

1. Suppose $\mathcal{I} = \mathcal{P}_1^{n_1}...\mathcal{P}_s^{n_s}$ is a factorization of $\mathcal{I}$ into prime ideals of $\mathcal{O}$. Let $a_i \in \mathcal{P}_i^{n_i} \backslash \mathcal{P}_i^{n_i+1}$ for $i = 1, 2, ..., s$. Then by the previous theorem there exists an element $a \in \mathcal{O}$ such that $a \equiv a_i (mod \mathcal{P}_i^{n_i+1})$ for all i. Hence $a \in \mathcal{P}_i^{n_i} \backslash \mathcal{P}_i^{n_i+1}$ for all i. Then, by proposition 8.2.8, $ord_{\mathcal{P}_i}(a) = n_i$ for $i = 1, 2, ..., s$. Therefore the factorization of (a) into prime ideals of $\mathcal{O}$ has the form $(a) = \mathcal{P}_1^{n_1}...\mathcal{P}_s^{n_s}\mathcal{P}_{s+1}^{n_{s+1}}...\mathcal{P}_k^{n_k} = \mathcal{I}\mathcal{J}$.

2. By theorem 8.2.9 it suffices to prove that every ideal $\mathcal{O}/\mathcal{P}^n$ is principal for any prime ideal $\mathcal{P}$. But since $\mathcal{O}/\mathcal{P}^n \simeq \mathcal{O}_{\mathcal{P}}/\mathcal{P}^n\mathcal{O}_{\mathcal{P}}$ and by corollary 8.4.6 $\mathcal{O}_{\mathcal{P}}$ is a PID, $\mathcal{O}/\mathcal{P}^n$ is also a PID.

3. For any nonzero ideal $\mathcal{J}$ and any ideal $\mathcal{I}$ of $\mathcal{O}$ containing $\mathcal{J}$ from property 2 it follows that $\mathcal{I} = \mathcal{J} + b\mathcal{O}$ for some $b \in \mathcal{O}$. Then $b \in \mathcal{I}$ as well. Let $a \in \mathcal{I}$, then taking $\mathcal{J} = a\mathcal{O}$ we obtain $\mathcal{I} = a\mathcal{O} + b\mathcal{O}$ as required.

8.5. FINITELY GENERATED MODULES OVER DEDEKIND DOMAINS

We shall begin by studying properties of injective modules over integral domains.

In section 4.3 we introduced the notion of divisible modules and showed that any injective module is divisible. The converse statement is not true in general, that is, a divisible module over an arbitrary ring need not be injective, but this is true for a principal ideal domain.

Proposition 8.5.1. *If A is a principal ideal domain, then a right A-module M is injective if and only if it is divisible.*

Proof. Let M be a divisible module. Since any element of A is regular, by Baer's Criterion, it is sufficient to prove that for any nonzero right ideal $\mathcal{I}$ in A and homomorphism $f : \mathcal{I} \to M$ there exists an element $m' \in M$ such that $f(a) = m'a$, $a \in \mathcal{I}$. Since A is a principal ideal domain, any right ideal in A has the form $\mathcal{I} = aA$ for some nonzero element $a \in A$. Let $f : \mathcal{I} \to M$ be a homomorphism and $f(a) = m$. Since M is a divisible module, there exists an element $m' \in M$ such that $m = m'a$. An arbitrary element of the ideal $\mathcal{I}$ has the form ab, where $b \in A$. Therefore $f(ab) = f(a)b = mb = m'ab = m'(ab)$, as required.

Proposition 8.5.2. *Let A be an integral domain and let M be a torsion-free right A-module. Then M is injective if and only if it is divisible.*

Proof. From proposition 5.2.11 it follows that it sufficient to prove the inverse part of the statement. Let M be a divisible A-module and let f be a homomorphism from an ideal $\mathcal{I} \subseteq A$ to the module M. Suppose that for a fixed element $a \in \mathcal{I}$ we have $f(a) = m$. Since M is a divisible module, there exists an element $m' \in M$ such that $m = m'a$. For any element $b \in \mathcal{I}$ we have $f(b)a = f(ba) = f(ab) = f(a)b = mb = m'ab = m'ba = (m'b)a$. Since M is torsion-free, $f(b) = m'b$ for all $b \in \mathcal{I}$, and from Baer's Criterion it follows that M is injective.

Proposition 8.5.3. *Any finitely generated torsion-free module M over an integral domain $\mathcal{O}$ can be embedded into a finitely generated free module.*

Proof. Let $\mathcal{O}$ be an integral domain with quotient field k and let M be a finitely generated torsion-free right A-module. Let $\tilde{M} = M \otimes_{\mathcal{O}} k$. Clearly, $\tilde{M}$ is a finite dimensional vector space over the field k. The natural homomorphism from M to $M \otimes_{\mathcal{O}} k$ is injective. So we can consider M as $\mathcal{O}$-submodule of $\tilde{M}$. We denote by $e_1, ..., e_n$ a basis of $\tilde{M}$ over k. Let $m_1, ..., m_t$ be a system of generators of the module M. Then $m_i = \sum\limits_j \alpha_{ij} e_j$, where $\alpha_{ij} \in k$, for $i = 1, ..., t$ and $j = 1, ..., n$. Let $\alpha_{ij} = a_{ij}/b_{ij}$, where $a_{ij}, b_{ij} \in \mathcal{O}$. Let $s = \prod\limits_{i,j} b_{ij}$, and set $y_j = s^{-1} e_j$ for $j = 1, ..., n$ and $\beta_{ij} = \alpha_{ij} s \in \mathcal{O}$. Then $m_i = \sum\limits_j \beta_{ij} y_j$, i.e., M is contained in the $\mathcal{O}$-module $N = \mathcal{O}y_1 + ... + \mathcal{O}y_n$. Since the system of elements $e_1, ..., e_n$ is independent over k, it is easy to see that the system of elements $f_1, ..., f_n$ is independent over $\mathcal{O}$,

i.e., is a free basis of the module N. Thus, M can be embedded into the finitely generated free module N.

From theorems 8.5.3 and 5.5.1 we obtain the following corollary.

Corollary 8.5.4. *A finitely generated torsion-free module M over a Dedekind ring $\mathcal{O}$ decomposes into a direct sum of ideals of the ring $\mathcal{O}$, and therefore it is a projective module.*

Definition. A module is called **uniserial** if its submodules form a chain. A commutative ring is called **uniserial** if the set of its ideals is linearly ordered, i.e., it is a chain.

Let $\mathcal{O}$ be a Dedekind ring with quotient field k and let M be a finitely generated $\mathcal{O}$-module. If $t(M)$ is the torsion submodule of M, then $M/t(M)$ is a finitely generated torsion-free module and by corollary 8.5.4 it is projective. Therefore the exact sequence

$$0 \to t(M) \to M \to M/t(M) \to 0$$

splits, i.e., $M \simeq t(M) \oplus M/t(M)$. Since the structure of finitely generated torsion-free modules is given by corollary 8.5.4 it remains to study finitely generated torsion modules.

Let M be a torsion finitely generated module over a Dedekind domain $\mathcal{O}$ and let $\mathcal{I} = AnnM = \{a \in \mathcal{O} \mid ma = 0 \quad \text{for all} \quad m \in M\}$. Let $\mathcal{I} = \mathcal{P}_1^{n_1} ... \mathcal{P}_s^{n_s}$ be the prime ideal factorization of $\mathcal{I}$, where $\mathcal{P}_1, ..., \mathcal{P}_s$ are distinct prime ideals. Then by the Chinese remainder theorem for Dedekind rings (theorem 8.2.9) we have

$$\mathcal{O}/\mathcal{I} \simeq \mathcal{O}/\mathcal{P}_1^{n_1} \times ... \times \mathcal{O}/\mathcal{P}_s^{n_s}$$

Since M is an $\mathcal{O}/\mathcal{I}$-module, it decomposes into a direct sum of modules $M = M_1 \oplus ... \oplus M_n$, where $M_i = M/MP_i^{n_i}$ is a finitely generated $\bar{\mathcal{O}}_i = \mathcal{O}/\mathcal{P}_i^{n_i}$-module. Therefore to describe finitely generated torsion $\mathcal{O}$-modules it is sufficient to describe modules over rings of the form $\mathcal{O}/\mathcal{P}^n$.

We have $\mathcal{O}/\mathcal{P}^n \simeq \mathcal{O}_\mathcal{P}/\mathcal{P}^n\mathcal{O}_\mathcal{P}$, where $\mathcal{O}_\mathcal{P}$ is the localization of $\mathcal{O}$ at the prime ideal $\mathcal{P}$. Since $\mathcal{O}$ is a Dedekind ring, by corollary 8.4.5 each $\mathcal{O}_\mathcal{P}$ is a PID. So we can apply the fundamental theorem for finitely generated modules over a PID (theorem 7.8.3) which say that any f.g. torsion module M/MP^n is isomorphic as an $\mathcal{O}_\mathcal{P}$-module to a finite direct sum of modules of the form $\mathcal{O}_\mathcal{P}/\mathcal{P}^m\mathcal{O}_\mathcal{P}$, where $m \leq n$. Therefore each module M/MP^n is isomorphic as an $\mathcal{O}$-module to a finite direct sum of modules of the form $\mathcal{O}/\mathcal{P}^m\mathcal{O}$, where $m \leq n$.

Finally, using the fact that $\mathcal{O}/\mathcal{P}^n$ is an Artinian uniserial module of finite length, we obtain the following main theorem of this section:

Theorem 8.5.5. *Any finitely generated module M over a Dedekind domain $\mathcal{O}$ is isomorphic to a direct sum of a finite number of ideals of the ring $\mathcal{O}$ and a finite direct sum of modules of the form $\mathcal{O}/\mathcal{P}^n$, which are Artinian uniserial*

modules of finite length.

8.6. PRÜFER RINGS

Because of the equivalence of (a) and (b) of theorem 8.3.4, the characterization of Dedekind ring as a hereditary domain is often taken as the definition. A natural generalization of this definition of a Dedekind ring is the notion of a Prüfer ring.

Definition. A semihereditary [4]) domain is called a **Prüfer ring**.

Theorem 8.6.1. *A domain A is a Prüfer ring if and only if every finitely generated torsion-free module is projective.*

Proof. Suppose A is a Prüfer ring and M is a finitely generated torsion-free module. Then by proposition 8.5.3 it can be imbedded in a finitely generated free module. Since A is semihereditary, by corollary 5.5.10, M is projective.

Conversely, let every finitely generated torsion-free module is projective. Since for a domain an ideal is torsion-free, we have that every finitely generated ideal is projective, i.e., A is a semihereditary domain, that is A is a Prüfer ring.

Theorem 8.6.2. *If A is a Prüfer ring, an A-module M is flat if and only if it is torsion free.*

Proof. Let M be a flat A-module. Consider an exact sequence

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0$$

where F is a free module. Since F is flat as well, by proposition 5.4.10, $K \cap F\mathcal{I} = K\mathcal{I}$ for any f.g. ideal $\mathcal{I} \subset A$.

Let $t(M)$ be the torsion submodule of M and $m \in t(M)$. Then there exists $x \in A$ such that $mx = 0$. Consider the principal ideal $\mathcal{I} = (x)$. Then $K \cap Fx = Kx$. Since $\varphi : M \to F/K$ is an A-homomorphism, then there exists an $f \in F$ such that $\varphi(m) = f + K$. So $0 = \varphi(mx) = \varphi(m)x = fx + K$, i.e., $fx \in K \cap Fx = Kx$. Therefore there exists a $k \in K$ such that $fx = kx$, i.e., $(f - k)x = 0$. Since F is torsion free, we have $f = k \in K$, i.e., $m = 0$ and $t(M) = 0$. Thus, M is torsion free.

Conversely, let M be torsion free and let $P \subset M$ be a finitely generated submodule in M. Then P is torsion free as well and, by theorem 8.6.1, P is projective. This means that P is flat as well. So that any finitely generated submodule of M is flat. By corollary 5.4.7, it follows that M is flat.

[4]) See section 5.5.

8.7. NOTES AND REFERENCES

The development of the general theory of ideals in a commutative ring, from the historical point of view, has two sources: the theory of integral algebraic numbers and the theory of ideals in a polynomial ring. The main problem of the theory of integral algebraic numbers is the uniqueness of the factorization into prime factors.

Basically, the papers of R.Dedekind, starting in 1871, were the basis of the theory of algebraic numbers. R.Dedekind created and fully completed a theory of modules and ideals for rings of integral algebraic numbers. These results and the essence of his methods were published in the paper: *R.Dedekind, Über die Theorie der ganzen algebraischen Zahlen, vol. III, p.1-222 (= Supplement XI von Dirichlets Vorlesungen ɥber Zahlentheorie, 4, Aufl. (1894), p.434-657)*, which has become recognized as his masterpiece. In this paper the notion of the ring of all integral elements of a number field was put in the central place of his theory. R.Dedekind proved the existence of a basis of this ring and introduced the notion of the discriminant of a field. The central result of this paper was the theorem on existence and uniqueness of the factorization of ideals into prime ones. In two subsequent publications R.Dedekind gave two different proofs of his theorem. In his third proof there appeared the notion of fractional ideals and it was proved that they form a group.

All these results, up to terminology, were known by L.Kronecker in 1860 as particular cases of his general theory.

From the viewpoint of commutative algebra the theory of Dedekind domains was practically completed in 1895, except for the study of structure of finitely generated modules over these rings. The beginning of the study such modules over the ring of integral numbers is also due to R.Dedekind. In the papers *Rechteckige Systeme und Moduln in algebraischen Zahlköpern // Math. Ann., LXXI (1912), p. 328-354; and LXXII (1912), p.297-345*, E.Steinitz investigated the structure of modules over a number field. Except for these papers the first important contributions in the field of general commutative rings are two large papers of Emmy Noether on the theory of ideals: *Idealtheorie in Ringbereichen // Math. Ann., LXXXIII (1921), p.24-66* and *Abstracter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern // Math. Ann., XCVI (1927), 26-61.* In the second paper there was given a full axiomatic description of Dedekind domains. At this time the study of the factorization of ideals was completed and the beginning of modern commutative algebra was laid down.

In this chapter we followed the classical Dedekind theory of ideals in the modern form as proposed by Emmy Noether.

The transition from Dedekind domains to hereditary domains first occurred in the famous book "Homological algebra" of H.Cartan, S.Eilenberg.

Prüfer domains (without this name) were studied by H.Prüfer in 1932 and W.Krull in 1936. The name *Prüfer ring* was introduced by H.Cartan and S.Eilenberg in their book "Homological algebra".

9. Goldie rings

9.1. THE ORE CONDITION. CLASSICAL RINGS OF FRACTIONS

In chapter 7 we have shown that any commutative domain $\mathcal{O}$ can be embedded in a field k in such a way that every element of k has the form $\alpha\beta^{-1}$, where $\alpha \in \mathcal{O}$ and $\beta \in \mathcal{O}^*$. The field k is called the quotient field of the commutative domain $\mathcal{O}$.

Unfortunately not every noncommutative ring can be embedded in a division ring in a similar way. But for some rings which have some particular properties such a construction can be realized.

Recall, that an element y of a ring A is called **regular** if $ay \neq 0$ and $ya \neq 0$ for any nonzero element $a \in A$.

Definition. Let A be a subring of a ring Q. The ring Q is called a **classical right ring of fractions** (or **classical right ring of quotients**) of the ring A if and only if the following conditions are satisfied:

a) all regular elements of the ring A are invertible in the ring Q;

b) each element of the ring Q has the form ab^{-1}, where $a, b \in A$ and b is a regular element in A.

Analogously we can define a **classical left ring of fractions**.

Assume Q is a classical right ring of fractions of a ring A. Let $a, r \in Q$ and r be a regular element in A. By condition b) we can write $r^{-1}a = by^{-1}$, where $b, y \in A$ and y is a regular element of A. Multiplying this equality on the left side by r and on the right side by y we obtain a necessary condition for the existences of a classical right ring of fractions in the following form:

The **(right) Ore condition:** *Let A be a ring with nonempty set S of all regular elements in A. For any element $a \in A$ and any regular element $r \in S$ there exists a regular element $y \in S$ and an element $b \in A$ such that $ay = rb$.*

Analogously we can define the left Ore condition.

Definition. A ring A satisfying the right (resp. left) Ore condition is called a **right** (resp. **left**) **Ore ring**. A ring which is both a right and left Ore ring is called an **Ore ring**. If, in addition, the ring is a domain, then it is called an **Ore domain**.

Example 9.1.1.

1. Any commutative ring with regular elements is an Ore ring.
2. Any commutative integral domain is an Ore domain.

Note that from the right Ore condition it follows that $aS \cap bA \neq 0$ for any $a \in A$ and $b \in S$, where S is a set of all regular elements of the ring A. If A is a domain, then the right Ore condition may be expressed in the equivalent form: $aA \cap bA \neq 0$ for any nonzero $a, b \in A$.

Example 9.1.2.
Consider the associative ring $A = k\langle X, Y\rangle$ over a field k (or any other suitable ring) in two noncommuting indeterminates X, Y. This is the free ring over k in two indeterminates. (The elements of A are polynomials in the noncommuting variables X, Y with coefficients from k.) Then A is not an Ore ring.

Theorem 9.1.1. *A ring A has a classical right ring of fractions if and only if it satisfies the right Ore condition, i.e., A is a right Ore ring.*

Proof. Let a ring A satisfy the right Ore condition and S be a set of all regular elements of A.

We introduce a relation $\sim$ on the direct product $A \times S$ as follows: $(a, b) \sim (c, d)$ if and only if there exist $x, y \in A$, such that $bx = dy \in S$ and $ax = cy \in A$.

First we shall prove that $\sim$ is an equivalence relation on $A \times S$. Reflexivity and symmetry are obvious from the definition of $\sim$. So we need only to prove transitivity. Assume that $(a, b) \sim (c, d)$ and $(c, d) \sim (f, g)$. Then by definition there exist $x, y, x_1, y_1 \in A$ such that $bx = dy \in S$, $ax = cy \in A$ and $dx_1 = gy_1 \in S$, $cx_1 = fy_1 \in A$. From the right Ore condition it follows that $bxS \cap dx_1A \neq 0$, hence there exists $s \in S$ and $a \in A$ such that $bxs = dx_1a \in S$. Since $bx = dy$, we have $dys = bxs = dx_1a$, or $d(ys - x_1a) = 0$. Since d is a regular element, $ys = x_1a$. Then from the obtained equalities we have $a(xs) = (ax)s = cys = cx_1a = fy_1a = f(y_1a) \in A$ and $b(xs) = (bx)s = dys = dx_1a = gy_1a = g(y_1a) \in S$. This means that $(a, b) \sim (f, g)$. Thus, the relation $\sim$ is an equivalence relation on the set $A \times S$. Denote the set of all equivalence classes by AS^{-1} and denote the equivalence class of (a, b) by a/b or ab^{-1}. If $a/b, c/d \in AS^{-1}$, then, by the Ore condition, there exist $x, y \in S$ such that $m = bx = dy \in S$. Define

$$a/b + c/d = (ax + cy)/m. \tag{9.1.1}$$

(Clearly, $a/b = ax/m$ and $c/d = cy/m$). The definition of the addition (9.1.1) does not depend on the choice of m, since if $m' = bx' = dy'$, where $x', y' \in S$, and $mu = m'v$ for $u, v \in S$, we have $bxu = bx'v$, i.e., $xu = x'v$. Analogously, $yu = y'v$ and therefore $(ax + cy)u = (ax' + cy')v$. Hence, $(ax + cy)/m = (ax' + cy')/m'$.

We shall show that the definition of the addition (9.1.1) also does not depend on the choice of a representative of the class a/b. Indeed, if $a/b = a'/b'$, then there are elements $x', y', z \in S$ such that $m' = bx' = dy' = b'z$. Hence, $ax' = a'z$. Then $t = a/b + c/d = (ax + cy)/m = (ax' + cy')/m'$. Therefore, $t = (a'z + cy')m' = a'/b' + c/d$.

Analogously, by the Ore condition there are elements $y_1 \in S$, $x_1 \in A$ such that

$n = bx_1 = cy_1 \in S$, then we define

$$(a/b)(c/d) = ax_1/dy_1. \tag{9.1.2}$$

(Note that $a/b = ax_1/n$ and $c/d = n/dy_1$). The definition of the multiplication (9.1.2) also does not depend on the choice of elements x_1, y_1 in the equality $bx_1 = cy_1$ and does not depend on the choice of representatives for the classes a/b and c/d. Let $a/b = a'/b'$. Choose $u, v \in S$ such that $bu = b'v$. Then $au = a'v$. Let $x, y \in A$, $y \in S$ such that $n' = bux = cvy$. Then, since the definition (9.2.2) does not depend on the choice of $n = bx_1 = cy_1$, we obtain $t = (a/b)(c/d) = (aux)/(dvy)$. However, $au = a'v$ and $bu = b'v$. Hence, $n' = b'vx = cvy$ and $t = a'vx/dvy = (a'/b')(c/d)$.

It is not difficult to verify that with respect to the addition (9.1.1) and the multiplication (9.1.2) the set of equivalence classes AS^{-1} forms a ring with multiplicative identity $1/1$. The map $\varphi : A \to AS^{-1}$, given by $\varphi(a) = a/1$, is a monomorphism of rings. Moreover, if $a \in S$, then $a/1$ is an invertible element of the ring AS^{-1} and $(a/1)^{-1} = 1/a$. Finally, if $a/b \in AS^{-1}$, then $a/b = (a/1)(b/1)$. This shows that AS^{-1} is a classical right ring of fractions of the subring $Im\varphi$. Therefore, the ring A has a right classical ring of fractions.

Theorem 9.1.2. *A is a right Ore domain if and only if A has a classical right ring of fractions which is a division ring.*

Proof. If A is a right Ore domain, then by previous theorem it has a classical right ring of fractions AS^{-1}. We shall show that AS^{-1} is a division ring. Let $a/b \in AS^{-1}$ and $a/b \neq 0$. Then $a \neq 0$ and since A is a domain, $a \in S$. Therefore $b/a \in AS^{-1}$ and it is an inverse of a/b, i.e., AS^{-1} is a division ring.

Conversely, let $a, b \in A$ and $a, b \neq 0$. Since all regular elements are invertible in AS^{-1}, $a^{-1}b \in AS^{-1}$, so $a^{-1}b = xy^{-1}$ for some nonzero elements $x, y \in A$. This implies $ax = by$, i.e., A is a right Ore ring. Since AS^{-1} is a division ring, all nonzero elements of A are not zero divisors, i.e., A is a domain.

If A is an Ore ring, then it has a classical right ring of fractions AS^{-1} and a classical left ring of fractions $S^{-1}A$. In this case it is easy to prove that both these rings are the same. This common ring is called a **classical ring of fractions** of A.

Corollary 9.1.3.

1. *A ring A has a classical ring of fractions if and only if A is an Ore ring.*
2. *A is an Ore domain if and only if its classical ring of fractions is a division ring.*

The remainder of this section will be devoted to studying the relationship between ideals of a ring A and ideals in its classical ring of fractions AS^{-1} and their properties.

Lemma 9.1.4. *Let A be a right Ore ring and let S be the nonempty set of all*

regular elements of A. Then for any $a_1b_1^{-1}, a_2b_2^{-1} \in AS^{-1}$ there exists $s \in S$ and $t_i \in A$ such that $a_ib_i^{-1} = (a_it_i)s^{-1}$ for $i = 1, 2$.

Proof. From the right Ore condition it follows that for any $b_1, b_2 \in S$ there exist $t_1 \in S$ and $t_2 \in A$ such that $s = b_1t_1 = b_2t_2 \in S$. Then $a_ib_i^{-1} = (a_ib_i^{-1})ss^{-1} = a_ib_i^{-1}b_it_is^{-1} = (a_it_i)s^{-1}$.

Lemma 9.1.5. *Let A be a right Ore ring and let S be the nonempty set of all regular elements of A. Then*

1. If $\mathcal{I}$ is a right ideal of A, then $\mathcal{I}S^{-1} = \{xs^{-1} \mid x \in \mathcal{I}, s \in S\}$ is a right ideal of AS^{-1}.

2. If $\mathcal{I}_1 \oplus \mathcal{I}_2 \oplus ... \oplus \mathcal{I}_n$ is a direct sum of right ideals of A, then $\mathcal{I}_1S^{-1} \oplus \mathcal{I}_2S^{-1} \oplus ... \oplus \mathcal{I}_nS^{-1}$ is also a direct sum of right ideals of AS^{-1}.

Proof.

1. Let $a_i \in \mathcal{I}$ and $a_ib_i^{-1} \in \mathcal{I}S^{-1}$ for $i = 1, 2$. By lemma 9.1.4 there exist $s \in S$ and $t_i \in A$ such that $a_ib_i^{-1} = (a_it_i)s^{-1}$ for $i = 1, 2$. Then we have $a_1b_1^{-1} + a_2b_2^{-1} = (a_1t_1)s^{-1} + (a_2t_2)s^{-1} = (a_1t_1 + a_2t_2)s^{-1} \in \mathcal{I}S^{-1}$. Thus, $\mathcal{I}S^{-1}$ is closed under addition.

Since $S^{-1}A \subseteq AS^{-1}$, we have $\mathcal{I}S^{-1} \cdot AS^{-1} \subseteq \mathcal{I}A \cdot S^{-1} = \mathcal{I}S^{-1}$. Therefore, $\mathcal{I}S^{-1}$ is a right ideal of AS^{-1}.

2. Let $a_ib_i^{-1} \in \mathcal{I}S^{-1}$ for $i = 1, 2, ..., n$ and $a_1b_1^{-1} + a_1b_1^{-1} + ... + a_1b_1^{-1} = 0$. Using lemma 9.1.4 by induction we obtain that there exist $s \in S$ and $t_i \in A$ such that $a_ib_i^{-1} = (a_it_i)s^{-1}$ for $i = 1, 2, ..., n$. Then we have $(a_1t_1)s^{-1} + (a_2t_2)s^{-1} + ... + (a_nt_n)s^{-1} = 0$ or $(a_1t_1) + (a_2t_2) + ... + (a_nt_n) = 0$. Thefore $a_it_i = 0$ for all i, since $\mathcal{I}_1 \oplus \mathcal{I}_2 \oplus ... \oplus \mathcal{I}_n$ is a direct sum of right ideals of A. Then $a_ib_i^{-1} = (a_it_i)s^{-1} = 0$ for $i = 1, 2, ..., n$, i.e., $\mathcal{I}_1S^{-1} \oplus \mathcal{I}_2S^{-1} \oplus ... \oplus \mathcal{I}_nS^{-1}$ is also a direct sum of right ideals of AS^{-1}.

Lemma 9.1.6. *Let A be a right Ore ring and let S be the nonempty set of all regular elements of A. Then*

1. If $\mathcal{I}$ is a right ideal of AS^{-1}, then $\mathcal{I} \cap A$ is a right ideal of A and $(\mathcal{I} \cap A)S^{-1} = (\mathcal{I} \cap A)(AS^{-1})$.

2. If $\mathcal{I}_1 \oplus \mathcal{I}_2 \oplus ... \oplus \mathcal{I}_n$ is a direct sum of right ideals of AS^{-1}, then $(\mathcal{I}_1 \cap A) \oplus (\mathcal{I}_2 \cap A) \oplus ... \oplus (\mathcal{I}_n \cap A)$ is also a direct sum of right ideals of A.

Proof.

1. Obviously, $(\mathcal{I} \cap A)S^{-1} \subseteq \mathcal{I}$. Conversely, if $x = ab^{-1} \in \mathcal{I}$, then $a = xb \in \mathcal{I} \cap A$, whence $x \in (\mathcal{I} \cap A)S^{-1}$.

2. This is obvious.

Definition. Let $A \subseteq Q$ be rings. Then A is called a **right order** in Q if

(1) each regular element of A is invertible in Q;

(2) every element of Q has the form as^{-1}, where $a \in A$ and s is a regular element of A.

Analogously one can define a left order. If A is both a right and left order in Q, then A is called an **order** in Q.

Using this notions we can obtain the following result:

Proposition 9.1.7. *A ring A is a right Ore ring if and only if it is a right order in some ring Q. In this case Q is isomorphic to the classical right ring of fractions of A. If, in addition, A is a domain, then Q is a division ring.*

9.2. PRIME AND SEMIPRIME RINGS

Recall that a **prime ideal** in a ring A is a two-sided ideal $\mathcal{I}$ in A such that $\mathcal{J}_1\mathcal{J}_2 \subseteq \mathcal{I}$ implies that either $\mathcal{J}_1 \subseteq \mathcal{I}$ or $\mathcal{J}_2 \subseteq \mathcal{I}$ for any two-sided ideals $\mathcal{J}_1$, $\mathcal{J}_2$ of A.

Definition. The ring A is called **prime** if 0 is a prime ideal in A, i.e., the product of any two nonzero two-sided ideals of A is not equal to zero.

Proposition 9.2.1. *For a proper ideal $\mathcal{I}$ in a ring A the following conditions are equivalent:*

(1) *$\mathcal{I}$ is a prime ideal.*

(2) *$A/\mathcal{I}$ is a prime ring.*

(3) *If $\mathcal{J}_1$ and $\mathcal{J}_2$ are any right ideals in A such that $\mathcal{J}_1\mathcal{J}_2 \subseteq \mathcal{I}$, then $\mathcal{J}_1 \subseteq \mathcal{I}$ or $\mathcal{J}_2 \subseteq \mathcal{I}$.*

(4) *If $\mathcal{J}_1$ and $\mathcal{J}_2$ are any left ideals in A such that $\mathcal{J}_1\mathcal{J}_2 \subseteq \mathcal{I}$, then $\mathcal{J}_1 \subseteq \mathcal{I}$ or $\mathcal{J}_2 \subseteq \mathcal{I}$.*

(5) *If $x, y \in A$ with $(x)(y) \subseteq \mathcal{I}$, then $x \in \mathcal{I}$ or $y \in \mathcal{I}$.*

(6) *If $x, y \in A$ with $xAy \subseteq \mathcal{I}$, then $x \in \mathcal{I}$ or $y \in \mathcal{I}$.*

Proof.

(1) $\Longrightarrow$ (2). Let $\mathcal{A}$ and $\mathcal{B}$ be ideals in $A/\mathcal{I}$, where $\mathcal{I}$ is a prime ideal in A. Then there exist ideals $\mathcal{A}_1 \supseteq \mathcal{I}$ and $\mathcal{B}_1 \supseteq \mathcal{I}$ such that $\mathcal{A} = \mathcal{A}_1/\mathcal{I}$ and $\mathcal{B} = \mathcal{B}_1/\mathcal{I}$. Suppose $\mathcal{AB} = 0$, then $\mathcal{A}_1\mathcal{B}_1 \subseteq \mathcal{I}$. Since $\mathcal{I}$ is a prime ideal in A, it follows that either $\mathcal{A}_1 \subseteq \mathcal{I}$ or $\mathcal{B}_1 \subseteq \mathcal{I}$, and so either $\mathcal{A} = 0$ or $\mathcal{B} = 0$.

(2) $\Longrightarrow$ (1). Let $A/\mathcal{I}$ be a prime ring and $\mathcal{A}$, $\mathcal{B}$ be ideals of A satisfying $\mathcal{AB} \subseteq \mathcal{I}$, then $(\mathcal{A}+\mathcal{I})/\mathcal{I}$ and $(\mathcal{B}+\mathcal{I})/\mathcal{I}$ are ideals in $A/\mathcal{I}$ whose product is equal to zero. Since $A/\mathcal{I}$ is a prime ring, we have that $(\mathcal{A}+\mathcal{I})/\mathcal{I} = 0$ or $(\mathcal{B}+\mathcal{I})/\mathcal{I} = 0$. Hence, $\mathcal{A} \subseteq \mathcal{I}$ or $\mathcal{B} \subseteq \mathcal{I}$.

(1) $\Longrightarrow$ (3). Since $\mathcal{J}_1$ is a right ideal, $(A\mathcal{J}_1)(A\mathcal{J}_2) = A\mathcal{J}_1\mathcal{J}_2 \subseteq \mathcal{I}$. Thus $A\mathcal{J}_1 \subseteq \mathcal{I}$ or $A\mathcal{J}_2 \subseteq \mathcal{I}$, and so $\mathcal{J}_1 \subseteq \mathcal{I}$ or $\mathcal{J}_2 \subseteq \mathcal{I}$.

(1) $\Longrightarrow$ (5). This is trivial.

(3) $\Longrightarrow$ (6). Since $(xA)(yA) \subseteq \mathcal{I}A = \mathcal{I}$, $xA \subseteq \mathcal{I}$ or $yA \subseteq \mathcal{I}$, and so $x \in \mathcal{I}$ or $y \in \mathcal{I}$.

(5) $\Longrightarrow$ (6). Since $xAy \subseteq (x)(y) \subseteq \mathcal{I}$, by hypothesis $x \in \mathcal{I}$ or $y \in \mathcal{I}$.

(6) $\Longrightarrow$ (1). Let $\mathcal{A}$ and $\mathcal{B}$ be ideals of the ring A such that $\mathcal{AB} \subseteq \mathcal{I}$. Assume that $\mathcal{A} \not\subseteq \mathcal{I}$. Choose an element $x \in \mathcal{A}$ such that $x \notin \mathcal{I}$. Then for any $y \in \mathcal{B}$ we have $xAy \subseteq \mathcal{AB} \subseteq \mathcal{I}$ and so, by hypothesis, $y \in \mathcal{I}$, i.e., $\mathcal{B} \subset \mathcal{I}$.

(1) $\Longrightarrow$ (4) and (4) $\Longrightarrow$ (1) by symmetry.

By induction from this proposition it immediately follows that if $\mathcal{I}$ is a prime ideal in A and $\mathcal{J}_1, \mathcal{J}_2, ..., \mathcal{J}_n$ are right ideals in A such that $\mathcal{J}_1\mathcal{J}_2...\mathcal{J}_n \subseteq \mathcal{I}$, then $\mathcal{J}_i \subseteq \mathcal{I}$ for some $i \in \{1, ..., n\}$.

Proposition 9.2.2. *Every maximal ideal M in a ring A is a prime ideal.*

Proof. If $\mathcal{I}$ and $\mathcal{J}$ are ideals in A not contained in M, then $\mathcal{I} + M = A$ and $\mathcal{J} + M = A$. Therefore

$$A = (\mathcal{I} + M)(\mathcal{J} + M) = \mathcal{IJ} + \mathcal{I}M + M\mathcal{J} + M^2 \subseteq \mathcal{IJ} + M$$

and hence $\mathcal{IJ} \not\subseteq M$.

Corollary 9.2.3. *Every nonzero ring has at least one prime ideal.*

The proof follows immediately from Zorn's lemma and proposition 9.2.2.

Denote by $C(P) = A\backslash P$ the complement of an ideal P in a ring A, that is, the set of all elements of A which do not belong to P. We shall need the following definition.

Definition. A nonempty set S of a ring A is called an **m-system** if for any $a, b \in S$ there exists $x \in A$ such that $axb \in S$.

As a corollary of proposition 9.2.1 (equivalence 1 and 6) we have the following statement which gives a characterization of a prime ideal P in terms of properties of $C(P)$.

Proposition 9.2.4. *An ideal P in a ring A is a prime ideal in A if and only if $C(P)$ is an m-system.*

Definition. An ideal $\mathcal{I}$ in a ring A is called **semiprime** if it has the following property:

If $\mathcal{J}$ is a right (or left) ideal in the ring A such that $\mathcal{J}^2 \subseteq \mathcal{I}$, then $\mathcal{J} \subseteq \mathcal{I}$.

It is clear that any prime ideal is semiprime. Moreover, the intersection of any set of semiprime ideals is a semiprime ideal.

Proposition 9.2.5. *Let $\mathcal{I}$ be a semiprime ideal in a ring A. If $\mathcal{J}$ is a right (or left) ideal in the ring A such that $\mathcal{J}^n \subseteq \mathcal{I}$ for some positive integer n, then $\mathcal{J} \subseteq \mathcal{I}$.*

Proof. We shall prove the statement of proposition by induction on n. If $n = 2$ the statement follows from definition of a semiprime ideal. Let $n > 2$. Assume that the statement is true for all $m < n$. Then we have $2n - 2 \geq n$, whence

$$(\mathcal{J}^{n-1})^2 = \mathcal{J}^{2n-2} \subseteq \mathcal{J}^n \subseteq \mathcal{I}.$$

Then from the definition of a semiprime ideal it follows that $\mathcal{J}^{n-1} \subseteq \mathcal{I}$ and therefore, by the induction hypothesis, $\mathcal{J} \subseteq \mathcal{I}$.

Definition. The ring A is called **semiprime** if 0 is a semiprime ideal, i.e., A does not contain nonzero nilpotent ideals.

Proposition 9.2.6. *For any ideal $\mathcal{I}$ in a ring A the following statements are equivalent:*
(1) *$\mathcal{I}$ is a semiprime ideal.*
(2) *$A/\mathcal{I}$ is a semiprime ring.*
(3) *If $x \in A$ and $(x)^2 \subseteq \mathcal{I}$, then $x \in \mathcal{I}$.*
(4) *If $x \in A$ and $xAx \subseteq \mathcal{I}$, then $x \in \mathcal{I}$.*
(5) *If $\mathcal{J}$ is any right ideal of A such that $\mathcal{J}^2 \subseteq \mathcal{I}$, then $\mathcal{J} \subseteq \mathcal{I}$.*
(6) *If $\mathcal{J}$ is any left ideal of A such that $\mathcal{J}^2 \subseteq \mathcal{I}$, then $\mathcal{J} \subseteq \mathcal{I}$.*

Proof. The proof of this statement is a very easy modification of the proof of proposition 9.2.1 and is omitted.

As a simple corollary of this statement is the following proposition.

Proposition 9.2.7. *For a ring A the following conditions are equivalent:*
(a) *A is semiprime;*
(b) *A has no nonzero nilpotent ideals;*
(c) *A has no nonzero nilpotent right ideals.*

Lemma 9.2.8 (R.Brauer).
If $\mathcal{I}$ is a minimal right ideal of a ring A, then either $\mathcal{I}^2 = 0$ or $\mathcal{I} = eA$, where e is an idempotent.

Proof. Assume that $\mathcal{I}^2 \neq 0$, i.e., there are nonzero elements $a, b \in \mathcal{I}$ such that $ab \neq 0$. Then the map $f : \mathcal{I} \to \mathcal{I}$ given by $f(x) = ax$ is a nonzero homomorphism and since $\mathcal{I}$ is a simple right A-module, by proposition 2.2.1, f is an isomorphism. Therefore, there is a nonzero element $e \in \mathcal{I}$ such that $ae = a$. But then $ae = ae^2$, i.e., $f(e) = f(e^2)$ and since f is an isomorphism, $e = e^2$, i.e., e is an idempotent. Since $0 \neq eA \subseteq \mathcal{I}$ and $\mathcal{I}$ is a minimal right ideal in A, we have $\mathcal{I} = eA$.

Proposition 9.2.9. *For an Artinian ring A the following statements are equivalent:*
(a) *A is semisimple;*
(b) *every right ideal of A is of the form eA, where e is an idempotent;*

(c) *every nonzero ideal in A contains a nonzero idempotent;*
(d) *A has no nonzero nilpotent ideals;*
(e) *A has no nonzero nilpotent right ideals.*

Proof.
$(a) \Rightarrow (b)$. If $\mathcal{I}$ is a right ideal of a semisimple ring A, then, by theorem 2.2.5 and proposition 2.2.4, $A = \mathcal{I} \oplus \mathcal{I}'$. Let $1 = e + e'$ be a corresponding decomposition of the identity of the ring A in a sum of orthogonal idempotents, then, by proposition 2.1.1, $\mathcal{I} = eA$.
$(b) \Rightarrow (c)$ is trivial.
$(c) \Rightarrow (d)$ follows from the fact that if e is a nonzero idempotent, then $e^n = e \neq 0$ for every n.
$(d) \Rightarrow (e)$. If $\mathcal{I} \neq 0$ is a nilpotent right ideal, then $A\mathcal{I}$ is a two-sided ideal of A and $(A\mathcal{I})^n = A\mathcal{I}^n$ implies that $A\mathcal{I}$ is nilpotent as well.
$(e) \Rightarrow (a)$. If $\mathcal{I}$ is a simple submodule of the right regular module, i.e., a minimal right ideal in the ring A, then by hypothesis $\mathcal{I}^2 \neq 0$ and, by lemma 9.2.8, $\mathcal{I} = eA$, where e is a nonzero idempotent. Therefore, by proposition 2.1.1, there is a decomposition of A in the form $A = \mathcal{I} \oplus \mathcal{I}'$, where $\mathcal{I}' = (1 - e)A$, and taking into account that A is Artinian, by proposition 2.2.4, the ring A is semisimple.

From propositions 9.2.7 and 9.2.9 we immediately obtain the following statement:

Proposition 9.2.10. *For a ring A the following statements are equivalent:*
1. *A is semisimple.*
2. *A is a right Artinian and semiprime.*

The following definition is analogous to the definition of an m-system.

Definition. A nonempty set S of a ring A is called an **n-system** if for any $a \in S$, there exists $x \in A$ such that $axa \in S$.

As a corollary of proposition 9.2.6 (equivalence 1 and 6) we have the following statement which gives a characterization of a semiprime ideal P in terms of properties of $C(P)$.

Proposition 9.2.11. *An ideal P in a ring A is a semiprime ideal in A if and only if $C(P)$ is an n-system.*

The following statement gives another useful characterization of a semiprime ideal which is taken as the definition of a semiprime ideal in many books.

Proposition 9.2.12. *An ideal $\mathcal{I}$ in a ring A is a semiprime ideal if and only if $\mathcal{I}$ is an intersection of prime ideals in A.*

Proof. Assume that $\mathcal{I}$ is the intersection of some set of prime ideals $\{P_i \mid i \in I\}$.

Let $x \in A$ be an element such that $xAx \in \mathcal{I}$. Then $xAx \in P_i$ for each $i \in I$. By proposition 9.2.1, $x \in P_i$ for each $i \in I$, i.e., $x \in \mathcal{I}$. From proposition 9.2.6 it follows that $\mathcal{I}$ is a semiprime ideal in A.

Conversely, assume that $\mathcal{I}$ is a semiprime ideal. We shall prove that $\mathcal{I}$ equals the intersection of all those prime ideals in A which contain $\mathcal{I}$.

Let $\mathcal{J} = \bigcap\limits_{i \in I} P_i$, where P_i is a prime ideal such that $\mathcal{I} \subseteq P_i \subseteq A$. Obviously, $\mathcal{I} \subset \mathcal{J}$. Suppose, $\mathcal{I} \neq \mathcal{J}$. Then there exists an element $a \in \mathcal{J}$ such that $a \notin \mathcal{I}$. We now form an m-system M such that $a \in M$ and $M \subset C(\mathcal{I})$. First, set $a_1 = a$. Since $a = a_1 \in C(\mathcal{I})$ and $\mathcal{I}$ is a semiprime ideal, by proposition 9.2.6, $a_1 A a_1 \not\subseteq \mathcal{I}$. Therefore there exists a nonzero element $a_2 \in C(\mathcal{I})$ and $a_2 \in a_1 A a_1$. In general, if a_n is defined, with $a_n \in C(\mathcal{I})$, choose $a_{n+1} \in C(\mathcal{I})$ and $a_{n+1} \in a_n A a_n$. Thus, we can form a set $M = \{a_1, a_2, ..., a_n, ...\}$ such that $a \in M$ and $M \subseteq C(\mathcal{I})$. We shall show that M is an m-system. Suppose, $a_i, a_j \in M$ and let $m = max(i, j)$. Then $a_{m+1} \in a_m A a_m \subseteq a_i A a_j$. Therefore there exists $x \in A$ such that $a_i x a_j = a_{m+1} \in M$, that is, M is an m-system.

So, if there exists an element $a \in C(\mathcal{I}) \cap \mathcal{J}$, then we can form an m-system M such that $a \in M$ and $M \cap \mathcal{I} = \emptyset$. Now consider the set W of all ideals K in A such that $\mathcal{I} \subseteq K$ and $M \cap K = \emptyset$. This set is not empty since $\mathcal{I}$ is one such ideal. By Zorn's Lemma there is an ideal $P \supseteq \mathcal{I}$ which is maximal in the set W. It is clear that $a \notin P$ and $M \cap P = \emptyset$.

We shall show that P is a prime ideal in A. Assume, $a, b \in A$ and $a, b \notin P$. Since P is a maximal element in the set W, we have $(P + (a)) \cap M \neq \emptyset$ and $(P + (b)) \cap M \neq \emptyset$. Hence there exist elements $m_1, m_2 \in M$ and $m_1 \in P + (a)$, $m_2 \in P + (b)$. Since M is an m-system, there exists an element $x \in A$ such that $m_1 x m_2 \in M$. Moreover, $m_1 x m_2 \in (P + (a))(P + (b))$. Now, if $(a)(b) \subseteq P$, then $(P + (a))(P + (b)) \subseteq P$ and therefore $m_1 x m_2 \in P$. But this is impossible, since $m_1 x m_2 \in M$ and $M \cap P = \emptyset$. Hence $(a)(b) \not\subseteq P$ And, by proposition 9.2.1, P is a prime ideal.

So, starting from the assumption $\mathcal{I} \neq \mathcal{J}$ we have constructed a prime ideal P such that $\mathcal{I} \subseteq P$ but $\mathcal{J} \not\subseteq P$. This contradiction completes the proof.

We shall need the following useful statements.

Proposition 9.2.13. *Let A be a prime (resp. semiprime) ring, $e^2 = e \in A$. Then the ring eAe is prime (resp. semiprime).*

Proof. Let A be a prime ring. Suppose that eAe is not a prime ring. Then, by proposition 9.2.1, there are non-zero elements $a, b \in eAe$ such that $a(eAe)b = 0$. Write $e_1 = e$ and $e_2 = 1 - e$, then we have the following two-sided Peirce decomposition of the ring A:

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$$

where $A_{ij} = e_i A e_j$ $(i, j = 1, 2)$. We set

$$\bar{a} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, \qquad \bar{b} = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}.$$

Then

$$\bar{a} A \bar{b} = \begin{pmatrix} aA_{11}b & 0 \\ 0 & 0 \end{pmatrix} = 0,$$

which contradicts the fact that A is a prime ring.

If A is a semiprime ring, then we set $b = a \neq 0$ and apply proposition 9.2.6.

Proposition 9.2.14. *A ring A is prime (resp. semiprime) if and only if the full matrix ring $M_n(A)$ is prime (resp. semiprime).*

Proof. If $M_n(A)$ is a prime (resp. semiprime) ring, then from the previous proposition it follows that A is a prime (resp. semiprime) ring.

Conversely, if $M_n(A)$ is not prime, then it has nonzero ideals $\bar{\mathcal{I}}$, $\bar{\mathcal{J}}$ such that $\bar{\mathcal{I}}\bar{\mathcal{J}} = 0$. Since $\bar{\mathcal{I}} = M_n(\mathcal{I})$ and $\bar{\mathcal{J}} = M_n(\mathcal{J})$, where $\mathcal{I}$, $\mathcal{J}$ are certain nonzero ideals in A, we obtain $\mathcal{I}\mathcal{J} = 0$, i.e., A is not a prime ring.

Analogously we can prove the inverse statement for the semiprime case.

9.3. GOLDIE RINGS. GOLDIE'S THEOREM

We have seen above that if a ring is an Ore domain then it has a classical ring of fractions which is a division ring. The next main problem which we shall study in this section is to answer the question: which rings have classical rings of fractions that are semisimple. The answer to this question was given by the famous Goldie theorem, which we shall prove here.

Let S be a subset in a ring A. Then $r.ann_A(S) = \{x \in A \mid sx = 0 \text{ for all } s \in S\}$ is the **right annihilator** of S. A right ideal $\mathcal{I}$ of A is called a **right annihilator** if there is a set $S \subseteq A$ such that $\mathcal{I} = r.ann_A(S)$. In a similar way we can define the **left annihilator** $l.ann_A(S)$ of S. And an ideal of the form $l.ann_A(S)$ is called a **left annihilator**.

In this section we shall write for short $r_A(S)$ or $r(S)$ instead of $r.ann_A(S)$ and $l_A(S)$ or $l(S)$ instead of $l.ann_A(S)$.

Note that a right ideal $\mathcal{I}$ of A is a right annihilator if and only if $\mathcal{I} = r(l(\mathcal{I}))$. Indeed, if $\mathcal{I} = r(X)$ for some set $X \subseteq A$, then $X \subseteq l(\mathcal{I})$, whence $\mathcal{I} = r(X) \supseteq r(l(\mathcal{I})) \supseteq \mathcal{I}$.

Definition. We say that A is a **right Goldie ring** if

1) A satisfies the ascending chain condition on right annihilators;

2) A contains no infinite direct sum of nonzero right ideals.

Analogously we can define a **left Goldie ring.** A ring A, which is both a right and left Goldie ring, is called a **Goldie ring.**

Examples 9.3.1.
1. Any right Noetherian ring is a right Goldie ring.
2. Any commutative domain is a Goldie ring.

The main purpose of this section is to give the proof of a remarkable theorem proved by A.Goldie in the late 1950's.

Theorem 9.3.1. *If A is a semiprime right Goldie ring, then it has a classical right ring of fractions, which is a semisimple ring.*

We shall prove this statement following C.Procesi and L.W.Small.[1]) Before proving it we need to prove a number of lemmas.

Lemma 9.3.2. *Let A be a semiprime ring satisfying the ascending chain condition on right annihilators. If $\mathcal{I}$ and $\mathcal{J}$ are right ideals of A, $\mathcal{J} \subseteq \mathcal{I}$ and $l(\mathcal{I}) \neq l(\mathcal{J})$, then there is an element $a \in \mathcal{I}$ such that $a\mathcal{I} \neq 0$ and $a\mathcal{I} \cap \mathcal{J} = 0$.*

Proof. Because taking annihilators reverses inclusion, it follows from $\mathcal{J} \subseteq \mathcal{I}$, that $l(\mathcal{J}) \supseteq l(\mathcal{I})$ and hence $l(\mathcal{J}) \supset l(\mathcal{I})$ by the assumptions in the statement of the lemma. Again, because taking annihilators reverses inclusions, the ascending chain condition on right annihilators implies the descending chain condition on left annihilators. (This also uses that a left ideal is a left annihilator if and only if it is the left annihilator of a right annihilator, see above just after the definition of annihilators.)

Now let U be a left annihilator that is minimal with respect to the property: $l(\mathcal{J}) \supseteq U \supset l(\mathcal{I})$ (where the right inclusion is strict). It follows that $U\mathcal{I} \neq 0$. and so, because A is semiprime, $U\mathcal{I}U\mathcal{I} \neq 0$. So there exists an $au \in \mathcal{I}U$ such that

$$Uau\mathcal{I} \neq 0. \tag{9.3.1}$$

The claim is now that $au\mathcal{I} \cap \mathcal{J} = 0$, which suffices to prove the lemma. Suppose this is not the case. Then there is an $x \in \mathcal{I}$ such that $0 \neq aux \in \mathcal{J}$. Now $x \in \mathcal{I}$ and so $l(x) \supseteq l(\mathcal{I})$ and thus $U \cap l(x) \supseteq l(\mathcal{I})$. By the minimality of U this means either $U \cap l(x) = l(\mathcal{I})$ or $U \cap l(x) = U$ (because intersections of left annihilators are left annihilators). In the latter case $U \subset l(x)$ so that $ux = 0$ contradicting $aux \neq 0$. In the former case, note that $l(\mathcal{J}) \supseteq U$, $aux \in \mathcal{J}$, so that $Uaux = 0$ and hence $Uau \subset l(x)$. Also $Uau \subset U$ and that would give $Uau \subset l(\mathcal{I})$ which is not the case because of (9.3.1). This proves the lemma.

Corollary 9.3.3. *Let A be a semiprime ring satisfying the ascending chain condition on right annihilators. If xA and yA are right essential ideals of A, then yxA is a right essential ideal of A as well.*

Proof. Let $\mathcal{I}$ be a nonzero right ideal of a ring A and let $B = \{a \in A \,:\, ya \in \mathcal{I}\}$. Since the ideal yA is essential, $B \neq 0$ and $yB = yA \cap \mathcal{I} \neq 0$. By the definition

[1]) See *C.Procesi, L.Small, On a theorem of Goldie // J. of Algebra, v.2 (1965), p.80-84.*

of B, it follows that $r(y) \subseteq B$. Since $yB \neq 0$ and $yr(y) = 0$, it follows that $l(B) \neq l(r(y))$. Then by lemma 9.3.2, there exists an $u \in B$ such that $uB \neq 0$ and $uB \cap r(y) = 0$. It is easy to see that uB is a right ideal in A and $uB \subset B$. Write $\mathcal{J} = uB$. Then $\mathcal{J} \neq 0$ and $\mathcal{J} \cap r(y) = 0$. Suppose $K = \{a \in A \ : \ xa \in \mathcal{J}\}$. Since xA is an essential ideal, $xK = xA \cap \mathcal{J} \neq 0$. Then $yxK \neq 0$. In the same time $yxK \subseteq y\mathcal{J} \subseteq yA \subseteq A$. So, $yxA \cap \mathcal{I} \neq 0$. Therefore, the ideal yxA is essential.

Corollary 9.3.4. *Let A be a semiprime ring satisfying the ascending chain condition on right annihilators. If xA is a right essential ideal in A, then the element x is regular in A.*

Proof. Since A is semiprime, $l(A) = 0$. If $l(x) \neq 0$, then we have the conditions of lemma 9.3.2 for the ideals $\mathcal{I} = A$ and $\mathcal{J} = xA$. Since xA is essential, we have $l(x) = 0$.

Consider $r(x)$. By the ascending chain condition on right annihilators the chain $r(x) \subseteq r(x^2) \subset ...$ stabilizes, i.e., there exists $n > 0$ such that $r(x^n) = r(x^{n+1})$. If $a \in x^nA \cap r(x)$, then $a = x^ny$ and $xa = 0 = x^{n+1}y$, whence $y \in r(x^{n+1}) = r(x^n)$ and $a = 0$. Thus, $x^nA \cap r(x) = 0$. Since, by corollary 9.3.3, the ideal x^nA is essential, we have $r(x) = 0$.

Lemma 9.3.5. *Let A be a semiprime right Goldie ring. Then A satisfies the descending chain condition on right annihilators.*

Proof. Let $R_1 \supset R_2 \supset ... \supset R_n \supset ...$ be a strong descending chain of right annihilators, i.e., $l(R_n) \neq l(R_{n+1})$ for any n. Applying lemma 9.3.2 we find a nonzero right ideal $\mathcal{I}_i \subseteq R_i$ such that $\mathcal{I}_i \cap R_{i+1} = 0$. Then the $\mathcal{I}_i$ form an infinite direct sum of right ideals in A. This contradicts the fact that A is a right Goldie ring.

Lemma 9.3.6. *Let A be a semiprime right Goldie ring. If $x \in A$ and $r(x) = 0$, then xA is an essential ideal, and so x is a regular element.*

Proof. Suppose that there exists a nonzero right ideal $\mathcal{I}$ of a ring A such that $\mathcal{I} \cap xA = 0$. We shall show that in this case the right ideals $x^n\mathcal{I}$ for $n \geq 0$ form an infinite direct sum. Note that $x^n\mathcal{I} \neq 0$ (by induction because $r(x) = 0$). In fact, let there be an equality $a_0 + xa_1 + x^2a_2 + ... + x^na_n = 0$, where $a_i \in \mathcal{I}$ and n is a minimal integer with this property. Then $a_0 \in \mathcal{I} \cap xA = 0$ and the equality has the form $x(a_1 + xa_2 + ... + x^{n-1}a_n) = 0$. Since $r(x) = 0$, $a_1 + xa_2 + ... + x^{n-1}a_n = 0$ which contradicts the minimal property of n. Therefore $a_0 = a_1 = ... = a_n = 0$. Since A does not contain an infinite direct sum of right ideals, we obtain $\mathcal{I} \cap xA \neq 0$, i.e., xA is an essential right ideal and, by corollary 9.3.4, x is regular.

Lemma 9.3.7. *Let A be a semiprime right Goldie ring. If $\mathcal{I}$ is an essential right ideal of A, then $\mathcal{I}$ contains a regular element of A.*

Proof. We first prove that any nonzero right ideal $\mathcal{I}$ of A contains an element

x with $r(x) = r(x^2)$. Since A is semiprime, it contains non-nilpotent elements. Consider the set of right annihilators $S = \{r(y) \mid y \in \mathcal{I}, y^n \neq 0\}$. Since A is a right Goldie ring, any descending chain of elements of the set S has a maximal element. Therefore, by Zorn's lemma, S has a maximal element $r(x)$. Since $r(x) \subseteq r(x^2)$, we have a strong equality $r(x) = r(x^2)$.

Now let $\mathcal{I}$ be an essential ideal of the ring A. We suppose that $\mathcal{I}$ does not contain any element $d \in A$ with $r(d) = 0$. In this case we can construct for each n a sequence of nonzero elements $a_1, a_2, ..., a_n \in \mathcal{I}$ satisfying the following conditions:

1. $r(a_i) = r(a_i^2)$ for all i.
2. $a_i a_j = 0$ for all $i < j$.
3. $a_1A \oplus a_2A \oplus ... \oplus a_nA$ is a direct sum.

The first induction step $n = 1$ was proved above. Suppose, we have formed a sequence $a_1, a_2, ..., a_n \in \mathcal{I}$ satisfying (1)-(3). Let $b = a_1 + a_2 + ... + a_n \in a_1A \oplus a_2A \oplus ... \oplus a_nA$. Since by assumption $\mathcal{I}$ does not contain any element d with $r(d) = 0$, it follows that $b \neq 0$ and $r(b) = \bigcap_{i=1}^{n} r(a_i) \neq 0$. Let $X = r(b) \cap \mathcal{I}$. Since $\mathcal{I}$ is an essential right ideal and $r(b) \neq 0$, we have $X \neq 0$. Therefore by the proof above X contains a nonzero non-nilpotent element a_{n+1} such that $r(a_{n+1}) = r(a_{n+1}^2)$. Since $a_{n+1} \in r(b)$, we have $a_i a_{n+1} = 0$ for all $i < n+1$. We shall show that $a_1A \oplus a_2A \oplus ... \oplus a_nA \oplus a_{n+1}A$ is a direct sum. Let $y \in (a_1A \oplus a_2A \oplus ... \oplus a_nA) \cap a_{n+1}A$. Then $y = a_{n+1}x = \sum_{i=1}^{n} a_i x_i$ for some $x, x_i \in A$ and we have $0 = a_1 a_{n+1} x = \sum_{i=1}^{n} a_1 a_i x_i = a_1^2 x_1$. Hence $x_1 \in r(a_1^2) = r(a_1)$, i.e., $a_1 x_1 = 0$. Therefore $a_{n+1}x = \sum_{i=2}^{n} a_i x_i$. Suppose $a_j x_j = 0$ for all $j < i \leq n$, i.e., $a_{n+1}x = \sum_{j=i}^{n} a_j x_j$. Then $0 = a_i a_{n+1} x = \sum_{j=i}^{n} a_i a_j x_j = a_i^2 x_i$, whence $a_i x_i = 0$. Continuing this process we conclude that $y = 0$. In other words we can construct an infinite direct sum $a_1A \oplus a_2A \oplus ... \oplus a_nA \oplus a_{n+1}A \oplus ...$ of nonzero right ideals. A contradiction. Thus $\mathcal{I}$ must contain an element d with $r(d) = 0$. Then, by lemma 9.3.5, d is a regular element in A.

Proof of theorem 9.3.1. We first show that A is a right Ore ring. Let $a \in A$ and $b \in S$. Then, by lemma 9.3.6, bA is essential in A. Then $X = \{u \in A \ : \ au \in bA$ is also a right essential ideal in A. By lemma 9.3.7, X contains a regular element $x \in S$. So, $ax = by$ for some $y \in A$. By theorem 9.1.1, A has a classical right ring of fractions $Q = AS^{-1}$.

We now show that Q is semisimple. Let $\mathcal{I}$ be a right ideal of Q. Then $\mathcal{I}_1 = \mathcal{I} \cap A$ is a right ideal of A, by lemma 9.1.6. By lemma 9.1.5, there is a maximal direct sum of right ideals $\mathcal{J} = \mathcal{I}_1 \oplus \mathcal{I}_2 \oplus ... \oplus \mathcal{I}_n$ of A that contains $\mathcal{I}_1$ as a direct summand. From the maximal property of $\mathcal{J}$ it follows that $\mathcal{J}$ is an essential ideal. Then, by lemma 9.3.7, it contains a regular element. Hence, by lemma 9.1.5, $\mathcal{J}Q = Q$. Write

$P = \mathcal{I}_2 \oplus ... \oplus \mathcal{I}_n$, then by lemma 9.1.5 we have $Q = \mathcal{J}Q = (\mathcal{I}_1 \oplus P)Q = \mathcal{I} \oplus PQ$. By proposition 2.1.1, there is an idempotent $e \in Q$ such that $\mathcal{I} = eQ$. Thus, any right ideal of Q is principal. Therefore the ring Q is right Noetherian and right Goldie. Since any right ideal of Q is generated by an idempotent, Q does not contain nilpotent ideals. This follows from the fact that if e is a nonzero idempotent, then $e^n = e \neq 0$ for every n. Therefore Q is semiprime.

Let $\mathcal{I}$ be a right ideal of Q, then $\mathcal{I} = eQ$, where $e^2 = e$ is an idempotent of Q. Since e and $f = 1 - e$ are pairwise orthogonal idempotents, $l(\mathcal{I}) = l(e) = fQ$ and $eQ = r(f) = r(fQ)$. Hence, any right ideal of Q is a right annihilator. Since Q is a semiprime right Goldie ring, by lemma 9.3.5, Q satisfies the descending chain condition on right annihilators and therefore it is a right Artinian ring. By proposition 9.2.10, the ring Q is semisimple.

Remark. If A is a semiprime Goldie ring, then from theorem 9.3.1 and its left-sided analog it follows that A has a classical right ring of fractions and a classical left ring of fractions, which coincide. Thus, a semiprime Goldie ring has a classical ring of fractions, which is a semisimple ring.

Proposition 9.3.8. *Let Q be a semisimple ring and A be a right order in Q. Then A is a semiprime right Goldie ring. Moreover, if Q is a simple ring, then A is prime.*

Proof. First we shall show that A is a right Goldie ring. Let $\mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq ...$ be an ascending chain of right annihilators in A. As it was remarked above for any right annihilator $\mathcal{I}_n$ we have $\mathcal{I}_n = r(l(\mathcal{I}_n))$. Set $\mathcal{J}_n = l(\mathcal{I}_n)$. Then $\mathcal{J}_1 \supseteq \mathcal{J}_2 \supseteq ...$ and $\mathcal{I}_n = r(\mathcal{J}_n)$. Then in the ring Q we have an ascending chain of right annihilators: $r_Q(\mathcal{J}_1) \subseteq r_Q(\mathcal{J}_2) \subseteq ....$ Since Q is semisimple, it is Noetherian, and so this chain stabilizes, i.e., there is n such that such that $r_Q(\mathcal{J}_n) = r_Q(\mathcal{J}_m)$ for all $m \geq n$. Therefore $\mathcal{I}_n = r_Q(\mathcal{J}_n) \cap A = r_Q(\mathcal{J}_m) \cap A = \mathcal{I}_m$ for all $m \geq n$.

From lemma 9.1.5 it follows that A does not contain infinite direct sum of right ideals. Thus, A is a right Goldie ring.

Let N be a nonzero nilpotent ideal in A. Assume $N^m = 0$ and $N^{m-1} \neq 0$. Then QNQ is an ideal in Q and since Q is semisimple there is a central idempotent $e \in Q$ such that $QNQ = eQ = Qe$. Let $e = \sum a_i x_i b_i$, where $a_i, b_i \in Q$ and $x_i \in N$. By lemma 9.1.4, there exists a regular element $a \in A$ such that $a_i = a^{-1}c_i$ and $c_i \in A$ for all i. Then $e = a^{-1} \sum c_i x_i b_i = a^{-1} \sum d_i b_i$, where $d_i \in N$ for all i. Since e is a central idempotent, we have $N^{m-1}ea = N^{m-1}ae = N^{m-1} \sum d_i b_i = 0$. Since a is a regular element in A, we have $N^{m-1}e = 0$, whence $N^{m-1} = 0$. A contradiction. Therefore A is semiprime.

Suppose Q is simple and $\mathcal{I} \neq 0$, $\mathcal{J}$ are arbitrary ideals in A such that $\mathcal{I}\mathcal{J} = 0$. Then $Q\mathcal{I}Q$ is an ideal in Q. Since Q is simple, $Q\mathcal{I}Q = Q$. Therefore $1 = \sum a_i x_i b_i$ for some $a_i, b_i \in Q$ and $x_i \in \mathcal{I}$. By lemma 9.1.4, there exists a regular element $a \in A$ such that $a_i = a^{-1}c_i$ and $c_i \in A$ for all i. Then $1 = a^{-1} \sum c_i x_i b_i$. So $a\mathcal{J} = \sum c_i x_i b_i \mathcal{J} = 0$. Since a is regular, $\mathcal{J} = 0$. Therefore A is prime.

Theorem 9.3.9 (Goldie's theorem). *A ring A has a classical right ring of fractions, which is a semisimple ring, if and only if A is a semiprime right Goldie ring.*

Proof. This is just the combination of theorem 9.3.1 and proposition 9.3.8.

Proposition 9.3.10. *Let Q be a semisimple ring and A be a right order in Q. Then Q is a simple ring if and only if A is prime.*

Proof. Necessity is implied by proposition 9.3.8.

Conversely, assume A is prime. Let $\mathcal{I}$, $\mathcal{J}$ be nonzero ideals of Q such that $\mathcal{I}\mathcal{J} = 0$. By lemma 9.1.5, $\mathcal{I} \cap A$, $\mathcal{J} \cap A$ are nonzero ideals in A and $(\mathcal{I} \cap A)(\mathcal{J} \cap A) = 0$. Since A is prime, $\mathcal{I} \cap A$ or $\mathcal{J} \cap A$ must be zero. A contradiction. So Q is a prime semisimple ring. Then it is clear that Q is simple.

Theorem 9.3.11 (A.W.Goldie, L.Lesieur-R.Croisot). *A ring A is a right order in a simple ring Q if and only if A is a prime right Goldie ring.*

Proof. This is proved by proposition 9.3.8 and proposition 9.3.10.

9.4. NOTES AND REFERENCES

The name for the Ore condition comes from Ore's result that a domain is a right order in a division ring if and only if its nonzero elements satisfy the right Ore condition (see *O.Ore, Linear equations in non-commutative fields // Annals of Math. v.32 (1931), p. 463-477*).

The definition of a prime ideal was introduced by W.Krull in both the commutative and noncommutative cases in the papers *W.Krull, Primidealketten in allgemeinen Ringbereichen // Sitzungsberichte Heidelberg. Acad. Wissenschaften (1928) 7. Abhandl., p.3-14* and *W.Krull, Zur Theorie der zweiseitigen Ideale in nichtkommutativen Bereichen // Math. Zeitschrift v.28 (1928), p.481-503.*

Semiprime ideals were introduced in the commutative case by W.Krull in the paper *W.Krull, Idealtheorie in Ringen ohne Endlichkeitsbedingung // Math. Annalen, v. 101 (1929), p.729-744* and in the noncommutative case by M.Nagata in the paper: *On the theory of radicals in a ring // J.Math. Soc. Japan, v.3 (1951), p.330-3444.*

M.Nagata in the paper: *On the theory of radicals in a ring // J.Math. Soc. Japan, v.3 (1951), p.330-3444* first introduced the term semiprime ring for a ring with zero prime radical. The properties of prime and semiprime rings were studied by R.E.Johnson in the papers: *Representations of prime rings // Trans. Amer. Math. Soc. v.74 (1953), p.351-357* and *Semi-prime rings // Trans. Amer. Math. Soc. v.76 (1954), p.375-388.*

One of the most important results in the theory of noncommutative rings was obtained by A.W.Goldie. First A.W.Goldie proved that a ring A is a right and left order in a simple ring if and only if A is a prime Goldie ring (see *A. W. Goldie,*

The structure of prime rings with maximum conditions // Proc. Nat. Acad. Sci. v.44, !958, pp. 584-586 and *A.W.Goldie, The structure of prime rings under ascending chain conditions // Proc. London Math. Soc. V.3 (10), 1958, pp. 589-608*). Later his method was modified by L.Lesieur and R.Croisot to obtain a one-sided version of this result (see *L.Lesieur and R.Croisot, Structure des anneaux premiers Noethériens a gauche // C.R. Acad. Sci. Paris v.248, 1959, pp.2545-2547* and *L.Lesieur and R.Croisot, Sur les anneaux premiers Noethériens a gauche // Ann. Sci. Ecole Norm. Sup. (Paris), v. 76 (3), 1959, pp.161-183*). After that A.W.Goldie gave the characterization of right orders in semisimple rings (see *A.W.Goldie, Semi-prime rings with maximum condition // Proc. London Math. Soc. V.10 (3), 1960, pp. 201-220*).

10. Semiperfect rings

10.1. LOCAL AND SEMILOCAL RINGS

Recall that a nonzero ring A is called **local** if it has a unique maximal right ideal. The first order of business in this chapter is to study the basic properties of local rings.

Proposition 10.1.1. *The following conditions are equivalent for a ring A with radical R:*

(a) *A is local;*

(b) *R is the unique maximal right ideal in A;*

(c) *all non-invertible elements of A form a proper ideal;*

(d) *R is the set of all non-invertible elements of A;*

(e) *the quotient ring A/R is a division ring.*

Proof.

$(a) \Rightarrow (b)$. This follows from the fact that the radical R is the intersection of all maximal right ideals of A.

$(b) \Rightarrow (c)$. Let S be the set of all non-invertible elements of the ring A with radical R and let $x \in S$. Then, by proposition 1.1.3, the right ideal $xA \neq A$ is contained in some maximal right ideal and therefore it is contained in R. Hence $S \subseteq R$. If $x, y \in S$, then $x, y \in R$, whence $x + y \in R$. So $x + y$ is a non-invertible element, that is, $x + y \in S$. If $x \in S$ and $a \in A$, then $xa \in R$ and $ax \in R$, and hence $xa, ax \in S$. Thus, S is a two-sided proper ideal of A.

$(c) \Rightarrow (d)$. Since any element of R is not invertible, $R \subseteq S$. Taking into account that $S \subseteq R$ we obtain that the radical R is just the set of all non-invertible elements, as required.

$(d) \Rightarrow (e)$. Since R is the set of all non-invertible elements of A, every element of A, which is not contained in R, is invertible. Therefore any element of A/R is invertible, thus A/R is a division ring.

$(e) \Rightarrow (a)$. This is clear, since A/R has no nontrivial one-sided ideals.

In view of the symmetry of condition 10.1.1 (e) we have the following result.

Corollary 10.1.2. *For any nonzero ring A the following statements are equivalent:*

1) *A has a unique maximal right ideal.*

2) *A has a unique maximal left ideal.*

The following result is often used to verify whether a ring is local or not.

Proposition 10.1.3. *For any nonzero ring A the following statements are equivalent:*

1) *A is a local ring.*

2) *if $a \in A$, then either a or $1 - a$ is invertible.*

Proof.

1) $\Rightarrow$ 2). Let A be a local ring with radical R and let a be a non-invertible element of A. Then by proposition 10.1.1 (d) $a \in R$ and by proposition 3.4.6 the element $1 - a$ is invertible in A.

2) $\Rightarrow$ 1). Let A be a ring with radical R and let a be a non-invertible element of A. Then the element $xa \in A$ is non-invertible for any $x \in A$. Since by hypothesis the element $1 - xa$ is invertible for any $x \in A$, by proposition 3.4.5, $a \in R$. The statement now follows from proposition 10.1.1 (d).

Corollary 10.1.4. *Let A be a ring, all of whose non-invertible elements are nilpotent. Then A is a local ring.*

Proof. Let x be a non-invertible element of a ring A. Then it is nilpotent, i.e., there exists an integer $n > 0$ such that $x^n = 0$. From the equality $1 = 1 - x^n = (1-x)(1+x+x^2+...+x^{n-1})$ it follows that $1-x$ is invertible and, by proposition 10.1.3, A is a local ring.

As a consequence of this result and corollary 3.1.9 using Fitting's lemma we obtain the following classical statement.

Proposition 10.1.5. *The endomorphism ring $End_A(M)$ of an indecomposable A-module M, which is both Artinian and Noetherian, is local.*

Proof. Let φ be an endomorphism of an indecomposable A-module M, which is both Noetherian and Artinian. Then by Fitting's lemma 3.1.8 there exists a positive integer n such that M decomposes into the direct sum of $Im(\varphi^n)$ and $Ker(\varphi^n)$. But then from the indecomposability of M it follows that either $M = Ker(\varphi^n)$ or $M = Im(\varphi^n)$. Consequently, any endomorphism M is either an automorphism or is nilpotent. Therefore the ring $End_A M$ is local.

Another simple corollary from proposition 10.1.3 can be formulated as follows.

Proposition 10.1.6. *A local ring A has no nontrivial idempotents (i.e., any idempotent in A is either 0 or 1).*

Proof. Let A be a local ring and $e = e^2$ be an idempotent in A. Consider the element $f = 1 - e$, which is an idempotent in A as well. By proposition 10.1.3, it follows that either e or f is invertible in A. From $ef = e(1 - e) = 0$ it follows that either e or f is equal to 0, as required.

Proposition 10.1.7. *Any local hereditary ring is a domain.*

Proof.
This follows from lemma 5.5.8.

Theorem 10.1.8. *If A is a local ring, then each finitely generated projective A-module is free.*

Proof. Let A be a local ring with radical R and let P be a finitely generated projective A-module. Then A/R is a division ring and P/PR is a finitely generated module over A/R. So P/PR is a finitely generated free A/R-module. Therefore $P/PR \simeq \overset{n}{\underset{i=1}{\oplus}}(A/R)$. Let F be the free A-module $F = \overset{n}{\underset{i=1}{\oplus}}(A)$, then $P/PR \simeq F/FR$. Let $\psi : F/FR \to P/PR$ be the corresponding isomorphism of A/R modules, and let $\pi : F \to F/FR$ and $\sigma : P \to P/PR$ be the natural projections. Then $\alpha = \psi\pi$ is a homomorphism from F to P/PR. Since F is a free module, and so a projective module, there exists a homomorphism $\varphi : F \to P$ such that the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & FR & \longrightarrow & F & \xrightarrow{\pi} & F/FR & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle\varphi} & \searrow{\scriptstyle\alpha} & \downarrow{\scriptstyle\psi} & & \\ 0 & \longrightarrow & PR & \longrightarrow & P & \xrightarrow{\sigma} & P/PR & \longrightarrow & 0 \end{array}$$

is commutative, i.e., $\sigma\varphi = \alpha = \psi\pi$.

We shall show that φ is an isomorphism.

For any $f \in F$ we have $\psi\pi(f) = \psi(f+FR) = \varphi(f)+PR$. Since ψ is surjective, $Im\varphi + PR = P$. Since P is finitely generated, by Nakayama's lemma $Im\varphi = P$, i.e., φ is also surjective.

Consider the exact sequence

$$0 \longrightarrow Ker\varphi \longrightarrow F \xrightarrow{\varphi} P \longrightarrow 0$$

Since P is projective, we have $F = W \oplus X \simeq Ker\varphi \oplus P$, where $W \simeq Ker\varphi$ and $X \simeq P$. Then $FR = WR \oplus XR$. Since $WR \subset W \subset FR$, we have $W = WR \oplus (W \cap XR)$. But $W \cap XR \subset W \cap X = 0$, therefore $W = WR$. Since W is a direct summand of a finitely generated module, it is also finitely generated and, by Nakayama's lemma, we obtain that $W = 0$, i.e., φ is a monomorphism. Thus, φ is an isomorphism, and so P is free.

Remark. This theorem still holds in a more general setting. Namely, I.Kaplansky proved that all projective modules over a local ring are free (see *I.Kaplansky, Projective modules // Ann. of Math., v.68, 1958, pp.372-377.*)

We introduce a new class of rings which are a generalization both of local rings and of one-sided Artinian rings. These rings arise naturally in the theory of rings and play an important role in it.

Definition. A ring A is called **semilocal** if $\bar{A} = A/R$ is a right Artinian ring.

From the results of section 3.5 it follows that in this case $\bar{A}$ can be decomposed into a direct sum of a finite number of simple modules (minimal right ideals), i.e., it is a semisimple ring.

Examples 10.1.1.

1. Any division ring is a local ring.
2. Any right Artinian ring is semilocal.
3. Any local ring is semilocal.
4. Let $K[[x]]$ be the ring of formal power series over a field K and let $M = (x)$. As has been shown in section 1.1, M is a maximal ideal in $K[[x]]$. Therefore the quotient ring $K[[x]]/M$ is a field isomorphic to the field K. Thus, $K[[x]]$ is a local ring. Recall that a ring is said to be **uniserial** if all its ideals are linearly ordered with respect to inclusion. Since all ideals in $K[[x]]$ form a linear chain

$$K[[x]] \supset (x) \supset (x^2) \supset (x^3) \supset ... \supset (x^n) \supset ....$$

the ring $K[[x]]$ is a local uniserial ring.

5. Let p be a prime integer and let $\mathbf{Z}_{(p)}$ be the ring of p-integral numbers. Then as it has been shown in section 1.1 $\mathbf{Z}_{(p)}$ has a unique maximal ideal (p) and all ideals in $\mathbf{Z}_{(p)}$ form a linear chain. Therefore $\mathbf{Z}_{(p)}$ is a local uniserial ring.

6. Let q be an arbitrary natural number, $\mathbf{Z}_{(q)} = \{\frac{m}{n} \in \mathbf{Q} | (n, q) = 1\}$ be the ring of q-integral numbers. The ring $\mathbf{Z}_{(q)}$ is semilocal. This follows from the fact that if $q = p_1^{\alpha_1}...p_s^{\alpha_s}$, where $p_1, ..., p_s$ are distinct primes and $r = p_1...p_s$, then $rad(\mathbf{Z}_{(q)}) = r\mathbf{Z}_{(q)}$.

7. A finite direct product of local rings is semilocal.

8. Let A be a semilocal ring. Then $B = M_n(A)$ is also a semilocal ring. In fact, by proposition 3.4.10, we have $radB = M_n(radA)$. Thus, $B/radB \simeq M_n(A/radA)$. Since $A/radA$ is semisimple, by proposition 2.2.6, $M_n(A/radA)$ is also semisimple. Therefore B is a semilocal ring.

10.2. NONCOMMUTATIVE DISCRETE VALUATION RINGS

In section 8.4 commutative discrete valuation rings were discussed. As a matter of fact this notion can be generalized to noncommutative rings as well.

Definition. Let D be a division ring. A **discrete valuation** on D is a function $\nu : D^* \to \mathbf{Z}$ satisfying

(i) $\nu(xy) = \nu(x) + \nu(y)$ for all $x, y \in D^*$;

(ii) ν is surjective;

(iii) $\nu(x + y) \geq min\{\nu(x), \nu(y)\}$ for all $x, y \in D^*$ with $x + y \neq 0$.

The set $\mathcal{O} = \{x \in D^* : \nu(x) \geq 0\} \cup \{0\}$ is a subring of D called the **valuation ring** of ν. Consider the set $M = \{x \in \mathcal{O} : \nu(x) > 0\}$. It is easy to verify, that M is a maximal ideal in $\mathcal{O}$.

A domain (not necessary commutative) $\mathcal{O}$ is called a **discrete valuation ring** if there is a valuation ν on its division ring of fractions such that $\mathcal{O}$ is the valuation ring of ν.

Examples 10.2.1.

Let K be a field, and $\sigma : K \to K$ be a nontrivial automorphism of K. Then the ring of $K[[x, \sigma]]$ with $xa = \sigma(a)x$ and, hence, multiplication defined by:

$$(\sum a_i x^i)(\sum b_i x^i) = (\sum a_i \sigma^i(b_j) x^{i+j})$$

is a noncommutative discrete valuation ring. This ring is called a **skew formal series ring**.

Proposition 10.2.1. *Let $\mathcal{O}$ be a discrete valuation ring with a valuation ν and division ring of fractions D. Let t be any element of $\mathcal{O}$ with $\nu(t) = 1$. Then*

1. *A nonzero element $u \in \mathcal{O}$ is a unit if and only if $\nu(u) = 0$.*

2. *Every nonzero element $r \in \mathcal{O}$ can be written in the form $r = ut^n = t^n v$ for some units $u, v \in \mathcal{O}^*$ and some $n \geq 0$. Every nonzero element $x \in D^*$ can be written in the form $x = ut^n = t^n v$ for some units $u, v \in \mathcal{O}^*$ and some $n \in \mathbf{Z}$.*

3. *Every nonzero right (left) ideal of $\mathcal{O}$ is right (left) principal of the form $t^n\mathcal{O}$ ($\mathcal{O}t^n$) for some $n \geq 0$.*

4. *If $M = t\mathcal{O} = \mathcal{O}t$, then $\bigcap_{n=0}^{\infty} t^n A = \bigcap_{n=0}^{\infty} At^n = 0$.*

Proof. 1. Let $u \in \mathcal{O}^*$, then there is an element $v \in \mathcal{O}$ such that $uv = 1$, whence $0 = \nu(uv) = \nu(u) + \nu(v)$. Since $\nu(u), \nu(v) \geq 0$, we have $\nu(u) = \nu(v) = 0$.

Conversely, let $u \neq 0$ and $\nu(u) = 0$, then for $u^{-1} \in D$ we have $\nu(u^{-1}) = \nu(u) = 0$, hence $u^{-1} \in \mathcal{O}$, so u is a unit in $\mathcal{O}$.

2. Suppose $x \in \mathcal{O}$ and $\nu(x) = n$, then $\nu(xt^{-n}) = \nu(x) + \nu(t^{-n}) = 0$. Hence $xt^{-n} = u$ is a unit and $x = ut^n$. Analogously, $t^{-n}x = v \in \mathcal{O}^*$ and so $x = t^n v$. If $x \in D^*$, then $x = ab^{-1}$, where $a, b \in \mathcal{O}$. Let $a = ut^n = t^n u_1$ and $b = vt^m = t^m v_1$, where $u, v, u_1, v_1 \in \mathcal{O}^*$. Then $x = wt^{n-m}$, where $w \in \mathcal{O}^*$ and $n - m \in \mathbf{Z}$.

3. Let $\mathcal{I}$ be a right ideal in $\mathcal{O}$, and let $x \in \mathcal{O}$ be an element with $\nu(x)$ minimal. If $\nu(x) = n$, then $x = t^n v$, where v is a unit. Hence $t^n \subset \mathcal{I}$ and so $t^n\mathcal{O} \subset \mathcal{I}$. Let a be an arbitrary element in $\mathcal{I}$, then $\nu(a) \geq n$. Then $\nu(at^{-n}) \geq 0$, whence $\nu(at^{-n}) \in \mathcal{O}$ and $a \in t^n\mathcal{O}$. Therefore $\mathcal{I} = t^n\mathcal{O}$. Analogously, any left ideal in $\mathcal{O}$ is principal and it is of the form $\mathcal{O}t^n$ for some $n \geq 0$. In particular, since $t \in M$, we have that $M = t\mathcal{O} = \mathcal{O}t$ is a two-sided principal ideal in $\mathcal{O}$. Since any ideal of $\mathcal{O}$ is contained in M and any element which does not contained in M is invertible, we obtain that $\mathcal{O}$ is a local ring with radical M.

4. Assume $\mathcal{I} = \bigcap_{n=0}^{\infty} t^n\mathcal{O} \neq 0$. Then there is a nonzero element $a \in \mathcal{I}$. By property 3 there is $n \geq 0$ and $u \in \mathcal{O}^*$ such that $a = t^n u$. Since $a \in \bigcap_{n=0}^{\infty} t^n\mathcal{O}$, $a \in t^{n+1}\mathcal{O}$, i.e., there is $v \in \mathcal{O}^*$ such that $a = t^{n+1}v$. So $a = t^n u = t^{n+1}v$, whence

$t^n(u - tv) = 0$. Since $\mathcal{O}$ is a domain, we have $u - tv = 0$. Therefore $u = tv \in M$. A contradiction. Thus, $a = 0$. Analogously, we can prove, that $\bigcap_{n=0}^{\infty} \mathcal{O}t^n = 0$.

An element $t \in M$ with $\nu(t) = 1$ and $M = t\mathcal{O} = \mathcal{O}t$ is called a **uniformizing parameter** or a **prime element** of $\mathcal{O}$ and it is defined uniquely up to multiplication by a unit.

From this proposition we can immediately obtain the main properties of discrete valuation rings which we formulate as the following statement:

Corollary 10.2.2. *Let $\mathcal{O}$ be a discrete valuation ring. Then*

1. *$\mathcal{O}$ is both a right and left PID.*
2. *$\mathcal{O}$ is a local ring with the radical $M = \{x \in \mathcal{O} \mid \nu(x) > 0\}$ which is a two-sided principal ideal of the form $M = t\mathcal{O} = \mathcal{O}t$ and any nonzero right (left) ideal of $\mathcal{O}$ is of the form $t^n\mathcal{O}$ ($\mathcal{O}t^n$) for some integer $n \geq 0$.*
3. *$\mathcal{O}$ is a Noetherian ring.*
4. *$\mathcal{O}$ is a hereditary ring.*

The next statement gives properties of a ring which may be used as other equivalent definitions of a discrete valuation ring without using the notion of a valuation.

Theorem 10.2.3. *The following properties of a ring $\mathcal{O}$ are equivalent*:

1. *$\mathcal{O}$ is a discrete valuation ring.*
2. *$\mathcal{O}$ is both a right and left PID, which is also a local ring with radical $M \neq 0$.*
3. *$\mathcal{O}$ is a local Noetherian domain with radical $M \neq 0$, which is a two-sided principal ideal.*
4. *$\mathcal{O}$ is a local right Noetherian ring with radical of the form $M = t\mathcal{O} = \mathcal{O}t$ and $t \in \mathcal{O}$ is not nilpotent.*

Proof. That statement 1 implies the others was proved above. The implications $2 \Rightarrow 3$ and $3 \Rightarrow 4$ are trivial.

$4 \Rightarrow 1$. Let $\mathcal{O}$ be a local right Noetherian ring with radical of the form $M = t\mathcal{O} = \mathcal{O}t$. We shall prove that $\mathcal{I} = \bigcap_{n=0}^{\infty} \mathcal{O}t^n = 0$. Note that $\mathcal{O}t^n \neq \mathcal{O}t^{n+1}$ for all $n \geq 0$, since otherwise, by Nakayama's lemma, we obtain $M^n = \mathcal{O}t^n = 0$ and so $t^n = 0$. Assume $\mathcal{I} \neq 0$, then there is a nonzero element $a \in \mathcal{I}$. If $a = bt^n = ct^{n+1}$, then $(b - ct)t^n = 0$. If b is invertible, then $(b - ct)$ is also invertible, by proposition 3.4.5. Hence $t^n = 0$. Since t is not nilpotent, we obtain a contradiction. So b is not invertible, and since $\mathcal{O}$ is a local ring, $b \in M$. Thus, there is a sequence of nonzero elements $a_1, a_2, ...$ such that $a = a_1t = a_2t^2 = ... = a_nt^n = ...$ and $a_n = a_{n+1}t$ for all $n > 0$. Consider the ascending chain of right ideals

$$a_1\mathcal{O} \subset a_2\mathcal{O} \subset ... \subset a_n\mathcal{O} \subset a_{n+1}\mathcal{O} \subset ...$$

Since $\mathcal{O}$ is a right Noetherian ring, this sequence stabilizes, i.e., there is $n > 0$

such that $a_n\mathcal{O} = a_{n+1}\mathcal{O}$. Then $a_{n+1} = a_n x = a_{n+1}tx$, or $a_{n+1}(1-tx) = 0$. Since $(1-tx)$ is invertible in $\mathcal{O}$, we obtain $a_{n+1} = 0$ and $a = 0$.

Thus, $\mathcal{I} = \bigcap_{n=0}^{\infty} \mathcal{O}t^n = 0$. Since $M = t\mathcal{O} = \mathcal{O}t$ is a maximal ideal in $\mathcal{O}$, then for any $x \in \mathcal{O}$ there is an integer $n \geq 0$ such that $x \in t^n\mathcal{O}$ and $x \notin t^{n+1}\mathcal{O}$. We set $n = \nu(x)$. Thus any element $a \in \mathcal{O}$ can be uniquely written in the form $x = t^{\nu(x)}\varepsilon = \varepsilon' t^{\nu(x)}$, where $\varepsilon, \varepsilon'$ are units in $\mathcal{O}$. If $x = t^n u$ and $y = t^m v$, where $u, v \in \mathcal{O}^*$, then $xy = t^{n+m}w$, where $w \in \mathcal{O}^*$. So, in particular, we obtain that $\mathcal{O}$ is a domain. Therefore it has a classical ring of fractions D, which is a division ring and we can assume that $\mathcal{O}$ is embedded in D. Any element of D is of the form ab^{-1}, where $a, b \in \mathcal{O}$ and b is a regular element of $\mathcal{O}$. Therefore we can set $\nu(ab^{-1}) = \nu(a) - \nu(b)$. The function ν thus defined is a valuation on D and so $\mathcal{O}$ is a discrete valuation ring.

Lemma 10.2.4. *Let M be a finitely generated A-module. If it has a unique maximal submodule, then M is a cyclic module.*

Proof. Let M be a finitely generated A-module and N be its unique maximal submodule. We can choose an element $x \in M$ and $x \notin N$. Then $xA \subset M$ and $xA \not\subset N$. Since N is a unique maximal submodule in M, we obtain $xA = M$, i.e., M is cyclic.

Theorem 10.2.5. *Let $\mathcal{O}$ be a local prime right Noetherian ring. Then the following statements are equivalent:*

1. *$\mathcal{O}$ is a discrete valuation ring.*

2. *$\mathcal{O}$ is a maximal (under inclusion) order in its classical ring of fractions Q, and the socle of the right $\mathcal{O}$-module $Q/\mathcal{O}$ is not equal to zero.*

Proof.

$1 \Rightarrow 2$ is trivial.

$2 \Rightarrow 1$. By Goldie's theorem Q is a simple ring. Note that the radical R of $\mathcal{O}$ contains a regular element, because otherwise $\mathcal{O} = Q$, that contradicting the formulation of the theorem. Let M be a minimal $\mathcal{O}$-submodule in Q. Suppose M has a maximal submodule X in Q which is different from $\mathcal{O}$. Then $X \cap \mathcal{O} = R$ and $XR \subset R$. Therefore $\mathcal{O} \subset S = \{x \in Q \mid xR \subset R\}$ and this inclusion is strict. Hence $S = Q$. Since R contains a regular element, $Q = \mathcal{O}$. A contradiction. Thus, M has a unique maximal submodule $\mathcal{O}$ and, by lemma 10.2.4, M is a cyclic module, i.e., $M = m\mathcal{O}$. Since $\mathcal{O} \subset m\mathcal{O}$, m is a regular element and so $R = m^{-1}\mathcal{O}$. Denote $t = m^{-1}$. Since $\mathcal{O}$ is a maximal order, $R = t\mathcal{O} = \mathcal{O}t$ is a two-sided principal ideal and t is not nilpotent. Applying theorem 10.2.3 we obtain that $\mathcal{O}$ is a discrete valuation ring.

Corollary 10.2.6. *Let $\mathcal{O}_1$, $\mathcal{O}_2$ be different local right Noetherian orders in a division ring D, which satisfy statement 2 of theorem 10.2.5. Then $\mathcal{O}_1\mathcal{O}_2 = D$,*

where

$$\mathcal{O}_1\mathcal{O}_2 = \{\sum a_i b_i \mid a_i \in \mathcal{O}_1, b_i \in \mathcal{O}_2\}.$$

Theorem 10.2.7. *If A is a local hereditary Noetherian ring, then A is either a division ring or a discrete valuation ring.*

Proof. Let A be a local hereditary Noetherian ring with radical R. By proposition 10.1.7, A is a domain. Therefore if $R = 0$, then A is a division ring. Suppose $R \neq 0$. Since A is a Noetherian hereditary ring, R is a finitely generated projective A-module and, by theorem 10.1.8, R is a finitely generated free A-module, i.e., $R \simeq A^n$. Since A is a domain, we obtain that $R \simeq A$, i.e., R is a principal right and left ideal. By proposition 10.2.3, A is a discrete valuation ring.

10.3. LIFTING IDEMPOTENTS. SEMIPERFECT RINGS

An idempotent $e \in A$ is called **local** if the ring eAe is local. Clearly, a local idempotent is always a primitive idempotent.

Assume that a ring A is semilocal. Then the quotient ring $\bar{A} = A/R$ can be decomposed into a direct sum of minimal right ideals: $\bar{A} = \bar{e}_1\bar{A} \oplus ... \oplus \bar{e}_n\bar{A}$. Since all rings $\bar{e}_i\bar{A}\bar{e}_i$ are division rings, all idempotents $\bar{e}_i$ are local. Then there arises a natural question: when, starting from a decomposition of $\bar{A}$, can one form a decomposition of the ring $A = e_1A \oplus ... \oplus e_nA$ such that $e_i + R = \bar{e}_i$.

The example of the ring $\mathbf{Z}_{(q)}$ shows that this cannot always be done. However, there are a lot of important cases when it is possible. We shall say that **idempotents may be lifted modulo an ideal** $\mathcal{I}$ of a ring A if from the fact that $g^2 - g \in \mathcal{I}$, where $g \in A$, it follows that there exists an idempotent $e^2 = e \in A$ such that $e - g \in \mathcal{I}$.

Proposition 10.3.1. *Idempotents can be lifted modulo any nil-ideal $\mathcal{I}$ of a ring A.*

Proof. Let $g^2 - g \in \mathcal{I}$ and set $r = g^2 - g$, $g_1 = g + r - 2gr$. Obviously, $gr = rg$. Calculating $g_1^2 - g_1$ we obtain $g^2 + r^2 + 4g^2r^2 + 2gr - 4g^2r - 4gr^2 - g - r + 2gr = r^2 + 4g^2r^2 + 4gr - 4g^2r - 4gr^2 = r^2 + 4r^3 - 4r^2 = r^2(4r - 3)$.

Setting $r_1 = r^2(4r - 3) \in \mathcal{I}$ and $g_2 = g_1 + r_1 - 2g_1r_1$ we obtain that $r_2 = g_2^2 - g_2 = r_1^2(4r_1 - 3)$, i.e., in the expression of r_2 the element r^4 enters as a factor. Since $r^k = 0$ for some integer $k > 0$, continuing this process we obtain that $r_n = 0$ for some n, i.e., $g_n^2 = g_n$. Since $g_1 - g \in \mathcal{I}$ and $g_i - g_{i-1} \in \mathcal{I}$ for all $i = 1, 2, ..., n$, we have that $g_n = e$ is an idempotent and $g - e \in \mathcal{I}$.

In view of this proposition and proposition 3.5.1, we have the following corollary.

Corollary 10.3.2. *Idempotents can be lifted modulo the radical of an Artinian ring.*

In general, if we have a pair of orthogonal idempotents $g_1 + \mathcal{I}$ and $g_2 + \mathcal{I}$ in $A/\mathcal{I}$, which lift to idempotents $e_1, e_2 \in A$, there is no guarantee that e_1 and e_2 will be orthogonal. However, in the case of nil-ideals orthogonality of idempotents can be preserved. For this purpose the following statement will be useful which we shall prove following J.Lambek.[1])

Lemma 10.3.3. *Let $\mathcal{I} \subseteq R$ be an ideal of a ring A with radical R such that idempotents in $A/\mathcal{I}$ can be lifted modulo the ideal $\mathcal{I}$. If $g^2 = g \in A$ and $u^2 - u \in \mathcal{I}$, $ug, gu \in \mathcal{I}$, then there exists an idempotent $e \in A$ such that $e - u \in \mathcal{I}$ and $eg = ge = 0$.*

Proof. Let $u^2 - u \in \mathcal{I}$, $g^2 = g \in A$, and $ug, gu \in \mathcal{I}$. According to proposition 10.3.1 there exists an idempotent $f^2 = f \in A$ such that $f - u \in \mathcal{I}$. Since $gu, ug \in \mathcal{I}$, we have $fg, gf \in \mathcal{I}$. From $\mathcal{I} \subseteq R$ it follows in particular, that $1 - fg$ is an invertible element of the ring A. Consider the element $h = (1 - fg)^{-1} f(1 - fg)$. Clearly, h is an idempotent of A and $hg = 0$. Multiplying h on the left side by $1 - fg$ we obtain $h - f = fg - fgh \in \mathcal{I}$.

Set $e = h - gh = (1 - g)h$. Obviously, $ge = 0 = eg$. Since $e - f = h - gh - f \in \mathcal{I}$ and $f - u \in \mathcal{I}$, we have $e - u \in \mathcal{I}$. Moreover, $e^2 = (1 - g)h(1 - g)h = (1 - g)h = e$, i.e., e is an idempotent of the ring A and $e - u \in \mathcal{I}$, as required.

Proposition 10.3.4. *Let $\mathcal{I} \subseteq R$ be an ideal in a ring A with radical R such that idempotents in $A/\mathcal{I}$ can be lifted modulo the ideal $\mathcal{I}$. Then for any finite or countable set of pairwise orthogonal idempotents $u_1, u_2, ..., u_n, ...$ in A such that $u_i u_j - \delta_{ij} u_i \in \mathcal{I}$, there exists a set of pairwise orthogonal idempotents $e_1, e_2, ..., e_n, ...$ in A such that $e_i - u_i \in \mathcal{I}$ and $e_i e_j = \delta_{ij} e_i$ for all i, j.*

Proof. Suppose we have already found the elements $e_1, e_2, ..., e_{k-1}$ satisfying the conditions of the proposition. It suffices to show how to find an element e_k. Set $g = e_1 + e_2 + ... + e_{k-1}$.

Obviously, $g^2 = g$, and $gu_k, u_k g \in \mathcal{I}$. Then by lemma 10.3.3 there exists an idempotent $e_k^2 = e_k \in A$ such that $e_k - u_k \in \mathcal{I}$ and $ge_k = e_k g = 0$.

Then $e_k e_i = e_i e_k = 0$ for all $i < k$. Since $u_k \notin \mathcal{I}$, we have $e_k \neq 0$.

Definition. A semilocal ring A is called **semiperfect** if idempotents can be lifted modulo the radical R of the ring A.

Semiperfect rings were introduced by H.Bass in 1960. From corollary 10.3.2 we obtain the following theorem.

Theorem 10.3.5. *A right Artinian ring is semiperfect.*

We are going to give two criteria for a ring to be semiperfect. To this end we shall need the following lemma.

[1]) See *J.Lambek, Lectures on rings and modules, Blaidell Publishing Company, 1966.*

Lemma 10.3.6. *Let a ring A have two different decompositions into a direct sum of right ideals: $A = e_1A \oplus ... \oplus e_nA = f_1A \oplus ... \oplus f_nA$ (where $1 = e_1 + ... + e_n = f_1 + ... + f_n$ are two decompositions of $1 \in A$ into a sum of pairwise orthogonal idempotents), and suppose, moreover, after renumbering if necessary, $e_iA \simeq f_iA$ $(i = 1, ..., n)$. Then there is an invertible element $a \in A$ such that $f_i = ae_ia^{-1}$.*

Proof. By theorem 2.1.2 the isomorphism $e_iA \simeq f_iA$ is realized by multiplication on the left side by some element $a_i \in f_iAe_i$. Then $f_ia_i = a_ie_i = a_i$. We set $a = a_1 + ... + a_n$. Obviously, $ae_i = a_i$ and $f_ia = a_i$. Consider the elements $b_i \in e_iAf_i$ realizing the inverse isomorphisms. We set $b = b_1 + ... + b_n$. Then $e_ib = b_i = bf_i$ and $a_ib_i = f_i$, $b_ia_i = e_i$. Clearly, $ab = \sum\limits_{i=1}^{n} a_ib_i = \sum\limits_{i=1}^{n} f_i = 1$ and $ba = \sum\limits_{i=1}^{n} b_ia_i = \sum\limits_{i=1}^{n} e_i = 1$, i.e., $b = a^{-1}$. Since $ae_i = f_ia$, we have $f_i = ae_ia^{-1}$.

Theorem 10.3.7. *A ring A is semiperfect if and only if it can be decomposed into a direct sum of right ideals each of which has exactly one maximal submodule.*

Proof. Let $\bar{A} = A/R = \bar{e}_1\bar{A} \oplus ... \oplus \bar{e}_n\bar{A}$ be a decomposition of $\bar{A}$ into a direct sum of minimal right ideals. Since the ring A is semiperfect, for each idempotent $\bar{e}_i$ there is an idempotent e_i such that $e_i + R = \bar{e}_i$. Write $\bar{e}_i\bar{A} = U_i$ and $P_i = e_iA$. Since R is a two-sided ideal, $P_i \cap R = P_iR$ and therefore by the first isomorphism theorem $(P_i + R)/R \simeq P_i/P_iR \simeq U_i$. Therefore every module P_i has exactly one maximal submodule. Let $P = \bigoplus\limits_{i=1}^{n} P_i$. Obviously, there is an epimorphism $\varphi : P \to \bar{A}$. Denote by π the natural projection A onto $\bar{A}$. Since the module P is projective, there exists a homomorphism $\psi : P \to A$ such that $\pi\psi = \varphi$. It is not difficult to verify that $Im\psi + R = A$. By Nakayama's lemma, $Im\psi = A$. We shall show that $X = Ker\psi = 0$. Because the module A is projective, we have $P \simeq Im\psi \oplus Ker\psi = A \oplus Ker\psi$. Consider P/PR. Then $P/PR \simeq \bar{A}$ and, on the other hand, $P/PR \simeq \bar{A} \oplus X/XR$. By the Krull-Schmidt theorem for semisimple modules (theorem 3.2.5), the module X/XR is equal to zero. Because the module X is finitely generated as the image of P, by Nakayama's lemma $X = 0$, i.e., ψ is an isomorphism. Therefore A decomposes into a direct sum of right ideals $\psi(e_iA)$, each of which has exactly one maximal submodule.

Conversely, let $A = P_1 \oplus ... \oplus P_n$ be a decomposition of a ring A into a direct sum of right ideals, each of which has exactly one maximal submodule. Then $R = radP_1 \oplus ... \oplus radP_n$, and it follows that $\bar{A} = A/R$ is a right semisimple ring. Let $1 = f_1 + ... + f_n$ be a decomposition of the identity of the ring A into a sum of pairwise orthogonal idempotents such that $P_i = f_iA$ $(i = 1, ..., n)$. We shall show that for any idempotent $\bar{e}^2 = \bar{e} \in \bar{A}$ there is an idempotent $e \in A$ such that $e + R = \bar{e}$. By proposition 2.2.4 the right ideal $\bar{e}\bar{A}$ is semisimple as a right module over the semisimple ring $\bar{A}$. Therefore there is a decomposition of $\bar{1} \in \bar{A}$ into a sum of pairwise orthogonal idempotents $\bar{1} = \bar{e}_1 + ... + \bar{e}_s + ... + \bar{e}_n$ such that $\bar{e} = \bar{e}_1 + ... + \bar{e}_s$ and all modules $\bar{e}_i\bar{A}$ are simple. On the other hand, let

$\bar{1} = \bar{f}_1 + ... + \bar{f}_n$ be a decomposition of $\bar{1} \in \bar{A}$ into a sum of pairwise orthogonal idempotents such that the modules $\bar{f}_i\bar{A}$ are simple. By the Krull-Schmidt theorem for semisimple modules (theorem 3.2.5), for an appropriate renumeration we have $\bar{e}_i\bar{A} \simeq \bar{f}_i\bar{A}$ $(i = 1, ..., n)$. By lemma 10.3.6, there exists an element $\bar{a} \in \bar{A}$ such that $\bar{e}_i = \bar{a}^{-1}\bar{f}_i\bar{a}$ $(i = 1, ..., n)$. Let $\bar{a}$ be the image of a and $\bar{a}^{-1}$ be the image of $b = a^{-1}$. Obviously, $ab = 1 + r$, where $r \in R$. Since $(1 + r)x = 1$, we have $x = 1 - rx = 1 - r_1$, where $r_1 \in R$. Therefore $b(1 - r_1) = a^{-1}$, and, moreover, the image of the element a^{-1} under the epimorphism π coincides with $\bar{a}^{-1}$. Then $\pi(e) = \sum \pi(a^{-1}f_ia) = \sum \bar{a}^{-1}\bar{f}_i\bar{a} = \bar{e}$. The theorem is proved.

Theorem 10.3.8 (B.J.Müller). *A ring A is semiperfect if and only if $1 \in A$ can be decomposed into a sum of a finite number of pairwise orthogonal local idempotents.*

Proof. Let a ring A be semiperfect. By theorem 10.3.7, $A = e_1A \oplus ... \oplus e_nA$, where the $e_1, ..., e_n$ are idempotents and each right ideal $P_i = e_iA$ $(i = 1, ..., n)$ has exactly one maximal submodule. Then $Hom(P_i, P_i) \simeq e_iAe_i$ and for any $\psi : P_i \to P_i$ either $Im\psi = P_i$ or $Im\psi \subseteq P_iR$. In the first case, since P_i is projective, we have $P_i = Im\psi \oplus Ker\psi$, which implies $Ker\psi = 0$ and so ψ is an automorphism. In the second case, ψ is a non-invertible element and, obviously, all non-invertible elements form an ideal. By proposition 10.1.1, the ring e_iAe_i is local.

Conversely, let $\pi : A \to \bar{A}$ be the natural projection of the ring A on the ring $\bar{A} = A/R$ (R is the radical of the ring A). We write $\pi(a) = \bar{a}$. Let e be a local idempotent of the ring A. We shall show that the module $\pi(eA) = \bar{e}\bar{A}$ is simple. Suppose, the ring A is not local (a local ring is, obviously, semiperfect). Consider $(\bar{1} - \bar{e})\bar{A}$. Since it is a proper right ideal in the ring $\bar{A}$, it is contained in a maximal right ideal $\bar{\mathcal{I}}$ of the ring $\bar{A}$. We shall show that $\bar{e}\bar{A} \cap \bar{\mathcal{I}} = 0$. If this is not so, then $(\bar{e}\bar{A} \cap \bar{\mathcal{I}})^2 \neq 0$, since $\bar{A}$ is a semiprimitive ring and therefore it has no nilpotent right ideals. Then there is an element $\bar{e}\bar{a} \in \bar{\mathcal{I}}$ and $\bar{e}\bar{a}\bar{e} \neq 0$. Since eAe is a local ring and $rad(eAe) = eRe$, we conclude that the ring $\bar{e}\bar{A}\bar{e}$ is a division ring. Therefore there is an element $\bar{e}\bar{x}\bar{e} \in \bar{e}\bar{A}\bar{e}$ such that $\bar{e}\bar{a}\bar{e}\bar{x}\bar{e} = \bar{e}$. Therefore $\bar{e} \in \bar{\mathcal{I}}$ and, thus, $\bar{1} \in \bar{\mathcal{I}}$. A contradiction. Therefore $\bar{e}\bar{A} \cap \bar{\mathcal{I}} = 0$ and $\bar{A} = \bar{e}\bar{A} \oplus \bar{\mathcal{I}}$. Since $\bar{\mathcal{I}}$ is a maximal ideal in the ring $\bar{A}$, the module $\bar{e}\bar{A}$ is simple. The theorem is proved.

Corollary 10.3.9. *A semiperfect ring A is an FD-ring.*

The proof is immediate from Müller's theorem and corollary 2.4.15.

As a corollary of this statement and theorem 2.4.11 we have the following theorem.

Theorem 10.3.10.

Any semiperfect ring A can be uniquely decomposed into a finite direct product of indecomposable rings, that is, if $A = B_1 \times B_2 \times ... \times B_s = C_1 \times C_2 \times ... \times C_t$

are two different decompositions, then $s = t$ and there is a permutation σ of the numbers $\{1, 2, ..., t\}$ such that $B_i = C_{\sigma(i)}$ for $i = 1, 2, ..., t$.

Corollary 10.3.11. *Let A be a semiperfect ring, $e^2 = e \in A$. Then the ring eAe is semiperfect.*

The proof immediately follows from theorem 10.3.8.

Examples 10.3.1.

1. Let $p_1, p_2, ..., p_n$ be primes (not necessary distinct), let $\mathbf{Z}_{(p_i)}$ be the ring of p_i-integral numbers, and let $\mathbf{Q}$ be a ring of rational numbers. Then a ring of the form

$$A = \begin{pmatrix} \mathbf{Z}_{(p_1)} & \mathbf{Q} & \dots & \mathbf{Q} \\ 0 & \mathbf{Z}_{(p_2)} & \dots & \mathbf{Q} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \mathbf{Z}_{(p_n)} \end{pmatrix}$$

is a semiperfect ring.

2. Any finite direct product of local rings is semiperfect.

3. A commutative ring is semiperfect if and only if it is a finite direct product of commutative local rings.

4. Let $\mathcal{O}$ be a local ring. Then $A = M_n(\mathcal{O})$ is a semiperfect ring.

5. If $\mathcal{O}$ is a semiperfect ring, then so is $A = M_n(\mathcal{O})$ and vica versa.

6. The ring of integers $\mathbf{Z}$ is not semiperfect.

7. The ring of polynomials $k[x]$ is also not semiperfect.

8. If B is a non-local ring in which $1 \in B$ is a primitive idempotent (e.g. $B = \mathbf{Z}$), then $M_n(B)$ is a noncommutative non-semiperfect ring.

10.4. PROJECTIVE COVERS. THE KRULL-SCHMIDT THEOREM

In this section we shall introduce the notion of a projective cover, which is "dual" to the notion of an injective hull. However, whereas any module has an injective hull, a module has a projective cover only in special cases.

A submodule N of a module M is called **small** (or **superfluous**) if the equality $N + X = M$ implies $X = M$ for any submodule X of the module M.

Examples 10.4.1.

1. If A is an Artinian ring with Jacobson radical R and M is a right A-module, then by Nakayama's lemma MR is a small submodule in M.

2. If M is a finitely generated A-module, then by Nakayama's lemma MR is small in M.

3. A nonzero direct summand of A-module M is never small. In particular, if M is semisimple, the only small submodule is the zero submodule.

Definition. A projective module P is called a **projective cover** of a module M and it is denoted by $P(M)$ if there is an epimorphism $\varphi : P \to M$ such that $Ker\varphi$ is a small submodule in P.

Lemma 10.4.1. *If $P \xrightarrow{\varphi} M \longrightarrow 0$ is a projective cover of a module M, then $Ker\varphi \subseteq rad(P)$.*

Proof. Suppose that $Ker\varphi \not\subset rad(P)$. Then $Ker\varphi + rad(P) = P$. Since $Ker\varphi$ is a small submodule in P, we have $rad(P) = P$. Because $P \neq 0$, we obtain a contradiction with proposition 5.1.8. Therefore $Ker\varphi \subseteq rad(P)$.

Corollary 10.4.2. *If $P \xrightarrow{\varphi} U \longrightarrow 0$ is a projective cover of a simple module M, then $Ker\varphi = rad(P)$. So, a projective cover of a simple module has exactly one maximal submodule.*

Proof. From lemma 10.4.1 it follows that $Ker\varphi \subseteq rad(P)$. If this inclusion is strict, then the simple module U contains a proper submodule $rad(P)/Ker\varphi$. This contradiction shows that $Ker\varphi = rad(P)$ and so a projective cover has a single maximal submodule $radP = PR$, by proposition 5.1.8.

Corollary 10.4.3. *If A is a semiprimitive ring and $P(U)$ is a projective cover of a simple A-module U, then $P(U) \simeq U$.*

Proof. Let $P(U) \xrightarrow{\varphi} U \longrightarrow 0$ be a projective cover of a simple A-module U. Since $R = radA = 0$, by proposition 5.1.8, $radP(U) = P(U)R = 0$. So from the previous lemma it follows that $Ker\varphi = 0$, i.e., $P(U) \simeq U$.

Thus, if A is a semiprimitive ring, then only projective A-modules have projective covers.

Note that in general the inverse statement to lemma 10.4.1 is not true. But it is true if P is a finitely generated module.

Lemma 10.4.4. *Let P be a projective finitely generated A-module, and let $\varphi : P \to M$ be an epimorphism with $Ker\varphi \subseteq rad(P)$. Then P is a projective cover of M.*

Proof. Suppose that $Ker\varphi \subseteq rad(P)$. Suppose for some submodule $X \subset P$ we have $X + Ker\varphi = P$ and therefore $X + rad(P) = P$. Since $rad(P) = PR$, we have $X + PR = P$. Applying Nakayama's lemma we obtain that $X = P$, i.e., $Ker\varphi$ is a small submodule in P. The proof is complete.

Lemma 10.4.5 (H.Bass). *Let $\psi : P \to M$ be an epimorphism of a projective module P onto a module M, $K = Ker\psi$ and let $\varphi : P(M) \to M$ be a projective cover of M. Then there is a decomposition $P \simeq P(M) \oplus P'$, where $P' \subset K$ and $P(M) \cap K$ is a small submodule in $P(M)$.*

Proof. Since P is projective, there is a homomorphism $\pi : P \to P(M)$ such that $\varphi\pi = \psi$. It is easy to see that $Im\pi + Ker\varphi = P(M)$. Since $Ker\varphi$ is a small submodule, we obtain that $Im\pi = P(M)$. Identifying $P(M)$ with a direct summand of P we may write $P = P(M) \oplus P'$, where $P' = Ker\pi$. Clearly, $\psi(P') = 0$ and ψ induces an epimorphism $P(M) \to M$ whose kernel coincides with $P(M) \cap K = N$. We shall show that N is a small submodule in $P(M)$. Let $N+X = P(M)$ for a submodule $X \subset P(M)$. Then $P(M) = N+X \subseteq Ker\varphi+X \subseteq P(M)$ and so $Ker\varphi + X = P(M)$. Since $Ker\varphi$ is a small submodule in $P(M)$, we have $X = P(M)$. This means that N is also a small submodule in $P(M)$.

From this lemma we obtain the following corollary.

Corollary 10.4.6. *If a module M has a projective cover $P(M)$, then the cover is unique up to isomorphism.*

Proposition 10.4.7. *The projective cover $P(M)$ of M, where $M = M_1 \oplus M_2$, is equal to $P(M_1) \oplus P(M_2)$.*

The proof of this proposition we leave to the reader as an exercise.
We are going to prove the following main theorem due to H.Bass.

Theorem 10.4.8 (H.Bass). *The following conditions are equivalent for a ring A:*
(a) *A is semiperfect;*
(b) *any finitely generated right A-module has a projective cover.*
(c) *any cyclic right A-module has a projective cover.*

Before we shall start with the proof of this theorem we note that if condition (c) holds for a ring A, then it holds for any quotient ring of the ring A. We shall need the following lemma.

Lemma 10.4.9. *A semiprimitive ring satisfying condition (c) of theorem 10.4.8 is semisimple.*

Proof. Let A be a semiprimitive ring, i.e., $radA = R = 0$ and suppose every cyclic right A-module has a projective cover. We shall show that A is the sum of all its minimal right ideals. Let $S = \mathrm{soc}(A_A)$ be the sum of all minimal right ideals of the ring A. If $S \neq A$, then S is contained in a maximal right ideal $\mathcal{I}$ of the ring A. The module $A/\mathcal{I} = U$ is simple and by hypothesis it has a projective cover $P(U)$, which is isomorphic to U by corollary 10.4.3. Because $U \simeq P(U)$ is a projective module, it follows that $A \simeq \mathcal{I} \oplus U$. Since $U \cap \mathcal{I} = 0$ and $S \subset \mathcal{I}$, we obtain $U \not\subset S$. This contradiction shows that $A = \mathrm{soc}\ (A_A)$ and by proposition 2.2.4 A is a semisimple ring. The lemma is proved.

Proof of theorem 10.4.8.
$(c) \Rightarrow (a)$. By lemma 10.4.9, the ring $\bar{A} = A/R$ is semisimple: $\bar{A} = U_1 \oplus ... \oplus U_n$,

where the U_i $(i = 1, .., n)$ are simple modules. By proposition 10.4.7, $P(\bar{A}) = P(U_1) \oplus ... \oplus P(U_n)$ and, by corollary 10.4.2, every module $P(U_i)$ $(i = 1, ..., n)$ has exactly one maximal submodule. Denote by π the natural projection of the ring A on $\bar{A}$ and by φ an epimorphism of $P(\bar{A})$ onto $U_1 \oplus ... \oplus U_n$. Since $P = P(\bar{A})$ is a projective module, there is a homomorphism ψ such that $\pi\psi = \varphi$. Obviously, $Im\psi + Ker\pi = A$ and since $Ker\pi = R$, by Nakayama's lemma, $Im\psi = A$. Because ψ is an epimorphism and A is a projective module, we have $P \simeq Im\psi \oplus Ker\psi = A \oplus Ker\psi$. Since $P/PR \simeq \bar{A}$, by the Krull-Schmidt theorem for semisimple modules, $Ker\psi/(Ker\psi R) = 0$ and from Nakayama's lemma it follows that $Ker\psi = 0$. Therefore the ring A is isomorphic to a direct sum of indecomposable right ideals, each of which has exactly one maximal submodule. By theorem 10.3.7, the ring A is semiperfect.

$(a) \Rightarrow (b)$. We are going to show that any finitely generated module M has a projective cover. Obviously, M/MR is an $\bar{A}$-module and, by Nakayama's lemma, $M \neq MR$, since M is finitely generated. The module M/MR decomposes into a direct sum of a finite number of simple modules: $M/MR = U_{i_1} \oplus ... \oplus U_{i_m}$. Since A is a semiperfect ring, from theorem 10.3.7 it follows that any simple $\bar{A}$-module U has the form $U = P/PR$, where P is an indecomposable projective A-module. Let $P_{i_k}/P_{i_k}R = U_{i_k}$ $(k = 1, ..., m)$, where P_{i_k} is an indecomposable projective A-module. In a similar way as above it can now be shown that there is an epimorphism $\psi : P_{i_1} \oplus ... \oplus P_{i_m} \to M$, and, moreover, $Ker\psi \subset (P_{i_1} \oplus ... \oplus P_{i_m})R$. By Nakayama's lemma, $Ker\psi$ is a small submodule in $P_{i_1} \oplus ... \oplus P_{i_m}$ and hence $P_{i_1} \oplus ... \oplus P_{i_m}$ is a projective cover of M.

$(b) \Rightarrow (c)$ trivial.

So the theorem is proved.

Remark. In the proof of the implication $(c) \Rightarrow (a)$ we have actually given a method of constructing a projective cover for an arbitrary finitely generated module over a semiperfect ring.

Clearly, M/MR is a module over the semisimple Artinian ring $\bar{A}$. Therefore it is isomorphic to a finite direct sum of simple $\bar{A}$-modules: $M/MR = \overset{s}{\underset{j=1}{\oplus}} U_j^{m_j}$, where $U_1, ..., U_s$ are all mutually nonisomorphic simple $\bar{A}$-modules. Lifting the idempotents we obtain that $U_j \simeq e_j A/e_j R$ where $e_j^2 = e_j \in A$. Then $P(M) = \overset{s}{\underset{j=1}{\oplus}} (e_j A)^{m_j}$.

The following theorem describes projective modules over a semiperfect ring.

Theorem 10.4.10. *Any indecomposable projective module over a semiperfect ring A is finitely generated, it is a projective cover of a simple A-module and has exactly one maximal submodule. There is a one-to-one correspondence between mutually nonisomorphic indecomposable projective A-modules $P_1, ..., P_s$ and mutually nonisomorphic simple A-modules which is given by the following correspondences:*

$P_i \mapsto P_i/P_iR = U_i$ *and* $U_i \mapsto P(U_i)$.

Proof. Let P be an indecomposable projective module over a semiperfect ring A. If $P \neq 0$, then $P \neq PR$ and P/PR is a nonzero semisimple A-module. Let a simple module U be a direct summand of the module P/PR. Then there is an epimorphism $\psi : P \to U$. By lemma 10.4.4, $P \simeq P(U) \oplus P'$. Since P is indecomposable, $P \simeq P(U)$. The remaining statements of the theorem follow from the above.

Definition. An indecomposable projective right module over a semiperfect ring A is called a **principal right module**. A **principal left module** can be defined analogously.

Any principal right (resp. left) A-module has the form eA (resp. Ae), where e is a local idempotent.

We shall use the results obtained to prove the famous Krull-Schmidt theorem. This theorem is often formulated in the following form:

Theorem 10.4.11 (Krull-Schmidt theorem). *Let an A-module M have two different decompositions as a direct sum of submodules $M = \overset{n}{\underset{i=1}{\oplus}} M_i = \overset{m}{\underset{i=1}{\oplus}} N_i$, whose endomorphism rings are local. Then $m = n$ and there is a permutation τ of the numbers $i = 1, 2, ..., n$ such that $M_i \simeq N_{\tau(i)}$ $(i = 1, ..., n)$.*

Proof. Denote by π_i the projection of the module M onto the submodule M_i and by p_i the projection of M onto N_i. Obviously, $1_M = \pi_1 + ... + \pi_n = p_1 + ... + p_m$ are two decompositions of $1_M \in End_A M$ into a sum of pairwise orthogonal local idempotents. Therefore, by theorem 10.3.8, the ring $End_A M$ is semiperfect.

Assume that there are two different decompositions of the semiperfect ring A into a direct sum of principal right modules $A = P_1 \oplus ... \oplus P_n = Q_1 \oplus ... \oplus Q_m$. Then $\bar{A} = P_1/P_1R \oplus ... \oplus P_n/P_nR = Q_1/Q_1R \oplus ... \oplus Q_m/Q_mR$. Since all modules $P_1/P_1R, ..., P_n/P_nR, Q_1/Q_1R, ..., Q_m/Q_mR$ are simple, from the Krull-Schmidt theorem for semisimple modules, taking into account corollary 10.4.6, we obtain that $m = n$ and for a suitable numeration $P_i \simeq Q_i$ $(i = 1, ..., n)$.

From lemma 10.3.6 we have the following statement.

Lemma 10.4.12. *Let the identity of a semiperfect ring A be decomposed into a sum of pairwise orthogonal local idempotents in two different ways $1 = e_1 + ... + e_n = f_1 + ... + f_m$. Then $m = n$ and there exists a permutation τ of numbers from 1 to n and an invertible element $a \in A$ such that $f_{\tau(i)} = ae_ia^{-1}$ for $i = 1, 2, ..., n$.*

Taking into account theorems 10.3.9 and 10.3.10, the Krull-Schmidt theorem may be reformulated in the following way:

Theorem 10.4.13 (Krull-Schmidt Theorem). *If the endomorphism ring $End_A(M)$ of an A-module M is semiperfect, then the module M has a unique decomposition into a direct sum of indecomposable modules.*

Proof. Let $M = \overset{n}{\underset{i=1}{\oplus}} M_i = \overset{n}{\underset{i=1}{\oplus}} N_i$ be two different decompositions of an A-module M into a direct sum of indecomposable modules. Consider the corresponding decompositions of the identity of M: $1_M = \pi_1 + ... + \pi_n = p_1 + ... + p_m$, where π_i is the projection of M onto M_i and p_j is the projection of M onto N_j. Since the ring $End_A(M)$ is semiperfect and the submodules $M_1, ..., M_n, N_1, ..., N_m$ are indecomposable, by theorem 10.3.8, the idempotents $\pi_1, ..., \pi_n, p_1, ..., p_m$ are local. By lemma 10.4.12, $m = n$ and there exists a permutation τ of the numbers $i = 1, ..., n$ and an automorphism $\psi \in End_A(M)$ such that $\pi_{\tau(i)} = \psi p_i \psi^{-1}$.

Consider $\psi : M \to M$. Obviously, $\psi(N_i) = \psi p_i(N_i) = \pi_{\tau(i)}\psi(N_i) \subset M_{\tau(i)}$, i.e., the module N_i is embedded in $M_{\tau(i)}$. On the other hand, let $m \in M_{\tau(i)}$. Then $m = \pi_{\tau(i)}m = \pi_{\tau(i)}\psi(m') = \psi(p_i(m'))$, i.e., the map $\psi : N_i \to M_{\tau(i)}$ is an isomorphism. The theorem is proved.

Note that under the stated hypothesis the Krull-Schmidt theorem can be considered as a corollary of the Jordan-Hölder theorem.

Corollary 10.4.14. *Any finitely generated projective right module over a semiperfect ring can be uniquely decomposed into a direct sum of principal right modules.*

It is not difficult to see that if M is an Artinian or Noetherian module then it can be decomposed into a direct sum of indecomposable modules. Besides, a finitely generated module over a right Artinian ring is, obviously, both an Artinian and Noetherian module. Note that the Krull-Schmidt theorem holds for finitely generated modules over right Artinian rings.

Proposition 10.4.15. *Any finitely generated module over a commutative principal ideal domain uniquely decomposes into a finite direct sum of indecomposable cyclic modules, in the other words, any two finitely generated modules over a commutative PID is isomorphic if and only if they have the same free rank and the same list of elementary divisors.*

Proof. Let A be a commutative principal ideal domain. If two A-modules M_1 and M_2 have the same free rank and list of elementary divisors, then they are clearly isomorphic.

Suppose two A-modules M_1 and M_2 are isomorphic. Then by proposition 7.8.5 they have the same free rank. So we can consider the case when M_1 and M_2 are torsion modules and have the same list of elementary divisors. Since each primary component of each module M_1 and M_2 is indecomposable Artinian and Noetherian module, by proposition 10.1.6, its endomorphism ring is local.

Therefore our theorem follows from the Krull-Schmidt theorem.

10.5. PERFECT RINGS

One of the main properties that are characteristic of a semiperfect ring is that every finitely generated module has a projective cover. This restriction to finitely generated modules is absent for perfect rings, the object of study in this section.

Some fundamental properties of perfect rings depend on a generalization of the idea of nilpotence, which is T-nilpotence. We shall now discus the important concept of a T-nilpotent ideal (right, left, two-sided).[2])

Definition. An ideal (right, left, two-sided) $\mathcal{J}$ is called **right** (resp. **left**) **T-nilpotent** if for any sequence $a_1, a_2, \ldots, a_n \ldots$ of elements $a_i \in \mathcal{J}$ there exists a positive integer k such that $a_k a_{k-1} \ldots a_1 = 0$ (resp. $a_1 a_2 \ldots a_k = 0$). An ideal $\mathcal{J}$ is called **T-nilpotent** if it is right and left T-nilpotent.

Clearly, any T-nilpotent ideal is a nil-ideal. However, not every T-nilpotent ideal is nilpotent. Nor is every nil-ideal necessarily a T-nilpotent ideal. So, T-nilpotent ideals are situated between nilpotent ideals and nil-ideals.

Example 10.5.1.
Let k be a field of two elements and let $k[x_1, x_2, ..., x_n, ...]$ be the polynomial ring over the field k in a countable number of variables $x_1, x_2, ..., x_n, ...$ Consider the ring $B = k[x_1, x_2, ..., x_n, ...]/(x_1^2, x_2^2, ..., x_n^2, ...)$. Let $\mathcal{I}$ be the ideal of B generated by the elements $\bar{x}_1$, $\bar{x}_2$,...,$\bar{x}_n$,... which are images of $x_1, x_2, ..., x_n, ...$ Then $b^2 = 0$ for every $b \in \mathcal{I}$ and $\bar{x}_1 \bar{x}_2 ... \bar{x}_n \neq \bar{0}$ for all n. Thus, $\mathcal{I}$ is a nil-ideal but is not T-nilpotent.

The following theorem may be considered as some kind of generalization of Nakayama's lemma for arbitrary right modules.

Theorem 10.5.1. *For any right ideal $\mathcal{I}$ in a ring A the following conditions are equivalent:*

(1) *$\mathcal{I}$ is right T-nilpotent;*

(2) *a right A-module M satisfying the equality $M\mathcal{I} = M$ is equal to zero;*

(3) *$M\mathcal{I}$ is a small submodule in M for any non-zero right A-module;*

(4) *$A^{\mathcal{N}}\mathcal{I}$ is a small submodule in $A^{\mathcal{N}}$, where $A^{\mathcal{N}}$ is a free module of countable rank.*

Proof.
(1) $\Rightarrow$ (2). Suppose $M\mathcal{I} = M$ and $M \neq 0$. Then there exist elements $m_1 \in M$ and $a_1 \in \mathcal{I}$ such that $m_1 a_1 \neq 0$. Let $m_1 = \sum n_i b_i$, where $n_i \in M$, $b_i \in \mathcal{I}$. Then

[2]) The notions of perfect rings and T-nilpotent ideals were introduced by H.Bass (see *H.Bass, Finitistic dimension and a homological generalization of semi-primary rings, Trans. AMS, v. 95, 1960, the definition on p.466*).

$m_1a_1 = \sum n_ib_ia_1$. As $m_1a_1 \neq 0$ there exists an index i such that $n_ib_ia_1 \neq 0$. Set $m_2 = n_i$, $a_2 = b_i$. Then $m_2a_2a_1 \neq 0$. Let $m_2 = \sum n'_ic_i$, where $n'_i \in M$, $c_i \in \mathcal{I}$, then $m_2a_2a_1 = \sum n'_ic_ia_2a_1 \neq 0$. Therefore there exists an index i such that $n'_ic_ia_2a_1 \neq 0$. Set $m_3 = n'_i$, $a_3 = c_i$. Then $m_3a_3a_2a_1 \neq 0$. Continuing this process, we can build a sequence $a_1, a_2, ..., a_n, ...$ of elements of the ideal $\mathcal{I}$ such that $a_na_{n-1}...a_2a_1 \neq 0$ for any positive integer n. But this contradicts the hypothesis that the ideal $\mathcal{I}$ is right T-nilpotent.

(2) $\Rightarrow$ (3). Let N be a non-zero right A-module and let $M\mathcal{I} + N = M$. Then $(M/N)\mathcal{I} = M/N$. So, by (2), $M/N = 0$. This means that $n = M$ and so MI is a small submodule in M.

(3) $\Rightarrow$ (4). This is obvious, because (4) is a particular case of (3).

(4) $\Rightarrow$ (1). Consider $F = A^I$ as a right A-module with a free basis $x_1, x_2, ..., x_n, ...$ For a given sequence $a_1, a_2, ..., a_n, ...$ of elements of the ideal $\mathcal{I}$ consider the submodule G of the module F given by $G = \sum\limits_{i=1}^{\infty} g_iA$, where $g_i = x_i - x_{i+1}a_i$, $i \in N$. Clearly, $F\mathcal{I} + G = F$, then by hypothesis $G = F$. In particular, $x_1 \in G$ and therefore there exists a decomposition of the element x_1 in the basis $g_1, g_2, ..., g_n, ...$: $x_1 = \sum\limits_{i=1}^{k} g_ib_i$, where $b_i \in A$ for $i = 1, ..., k$. Therefore we have:

$$x_1 = \sum_{i=1}^{k} g_ib_i = x_1b_1 + x_2(b_2 - a_1b_1) + x_3(b_3 - a_2b_2) + ...$$

$$+x_k(b_k - a_{k-1}b_{k-1}) - x_{k+1}a_kb_k.$$

Since the elements $x_1, x_2, ..., x_k, x_{k+1}$ are part of a free basis of the module F, we obtain the following system of equalities: $b_1 = 1$, $b_2 = a_1$, $b_3 = a_2a_1$, ..., $b_k = a_{k-1}...a_1$, $a_kb_k = 0$. Therefore $a_ka_{k-1}...a_1 = 0$, i.e., $\mathcal{I}$ is a right T-nilpotent ideal. The theorem is proved.

Corollary 10.5.2. *Let $\mathcal{I}$ be a right T-nilpotent right ideal of A and let P and Q be any two projective right A-modules. Then $P/P\mathcal{I} \simeq Q/Q\mathcal{I}$ implies that $P \simeq Q$.*

Proof. Let $\bar{f}$ be a given isomorphism from $P/P\mathcal{I}$ to $Q/Q\mathcal{I}$. Since P is a projective module, there exists an A-homomorphism $f : P \to Q$ which makes the diagram:

$$\begin{array}{ccc} P & \longrightarrow & P/P\mathcal{I} \\ \downarrow & & \downarrow \bar{f} \\ Q & \longrightarrow & Q/Q\mathcal{I} \end{array}$$

commutative. The surjectivity of $\bar{f}$ implies that $Imf + Q\mathcal{I} = Q$. Since $\mathcal{I}$ is T-nilpotent, by theorem 10.5.1, $Imf = Q$, i.e., f is epimorphism. From projectivity

of Q it follows that there exists a decomposition $P = P' \oplus Q'$, where $P' = Kerf$ and $Q' \simeq Q$. Reducing modulo $\mathcal{I}$, we obtain $P/P\mathcal{I} \simeq P'/P'\mathcal{I} \oplus Q'/Q'\mathcal{I}$. Since $P/P\mathcal{I} \simeq Q'/Q'\mathcal{I}$, we obtain that $P'/P'\mathcal{I} = 0$. And applying theorem 10.5.1 again, we see that $P' = 0$. This means that $P = Q' \simeq Q$.

Definition. A ring A with Jacobson radical R is called **right** (resp., **left**) **perfect** if A/R is semisimple and R is right (resp., left) T-nilpotent. If A is both right and left perfect, R is called a **perfect ring**.

Examples 10.5.2.

1. Any right (resp., left) Artinian ring is perfect, because the Jacobson radical of it is nilpotent, and so is both right and left T-nilpotent.

2. Since the Jacobson radical R of a right (resp., left) perfect ring is right (resp., left) T-nilpotent, R is a nil-ideal. So idempotents of A can be lifted modulo R. Consequently, a right (or left) perfect ring is semiperfect.

3. Note that the notion right perfect is not symmetric, i.e., there are right perfect rings that are not left perfect (and vice versa). Here we give the example of a ring which is left perfect but not right perfect.[3]) Let k be a field, and let k_w be the algebra of all infinite matrices over k. We denote by N the set of all strictly lower triangular matrices in k_w having a finite number of nonzero entries. Let A be the subalgebra of k_w generated by N together with the identity. Then N is the radical of A, $A/R \simeq k$, and N is left T-nilpotent, but N is not right T-nilpotent. Thus, A is left perfect, but not right perfect. Note that every nilpotent ideal is right and left T-nilpotent. Consequently, N is not nilpotent ideal, that gives us the example of the left T-nilpotent ideal that is not nilpotent.

Theorem 10.5.3 (H.Bass). *Let A be a ring with Jacobson radical R. Then the following are equivalent:*

1. *A is right perfect.*
2. *Every right A-module has a projective cover.*

Proof.

(1) $\Rightarrow$ (2). Let A be a right perfect ring with Jacobson radical R and let M be a right A-module. Let $1 = e_1 + e_2 ... + e_n$ be a decomposition into a sum of orthogonal local idempotents. Then A/R is semisimple and M/MR as an A/R-module decomposes into a direct sum of a finite number of right simple A/R-modules: $M/MR = U_{i_1} \oplus ... \oplus U_{i_m}$. Since every right perfect ring is semiperfect, from theorem 10.3.7 it follows that any right simple $\bar{A}$-module U has the form $U = P/PR$, where P is an indecomposable projective A-module. Let $P_{i_k}/P_{i_k}R = U_{i_k}$ $(k = 1, ..., m)$, where P_{i_k} is an indecomposable projective A-module. Set $P = P_{i_1} \oplus ... \oplus P_{i_m}$, which is a projective A-module. Then using the projectivity

[3]) See *H.Bass, Finitistic dimension and a homological generalization of semi-primary rings // Trans. Amer. Math. Soc., v.95 (1960), p.466-488).*

of P we have the following commutative diagram:

$$\begin{array}{ccccccccc} & & & & P & \longrightarrow & P_{i_1}/P_{i_1}R \oplus ... \oplus P_{i_k}/P_{i_k}R & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle \psi} & & \| & & \\ 0 & \longrightarrow & MR & \longrightarrow & M & \longrightarrow & M/MR \simeq U_{i_1} \oplus ... \oplus U_{i_m} & \longrightarrow & 0 \end{array}$$

for a suitable homomorphism ψ. Then $Im(\psi) + MR = M$ and $Ker(\psi) \subseteq (P_{i_1} \oplus ... \oplus P_{i_m})R = PR$. Since R is right T-nilpotent, from theorem 10.5.1 it follows that $Im(\psi) = M$, i.e., ψ is an epimorphism. Since PR is a small submodule in P, $Ker(\psi) \subseteq PR$ implies that $Ker(\psi)$ is a small submodule in P. So, $\psi : P \to M$ is a projective cover of M.

(2) $\Rightarrow$ (1). By theorem 10.4.8, A is a semiperfect ring. We need only to check that the Jacobson radical R of A is T-nilpotent. Let M be a right A-module. Since M has a projective cover, we have $MR \subseteq radM \subset M$ and $radM \neq M$. In particular, for any right A-module M, $MR = M$ implies that $M = 0$. This means, by theorem 10.5.1, that R is right T-nilpotent and A is right perfect.

Proposition 10.5.4. *Let $\{a_1, a_2, ...\} \subseteq A$ be given. Let $F = \overset{\infty}{\underset{i=0}{\oplus}} e_i A$ be a free A-module, and let K be its free submodule generated by*

$$\{f_i = e_i - e_{i+1}a_{i+1} \ : \ i \geq 0\}.$$

Then the right A-module $M = F/K$ is flat. Moreover, M is projective only if the descending chain of principal left ideals

$$Aa_1 \supseteq Aa_2a_1 \supseteq ...$$

stabilizes.

Proof. To see that $M = F/K$ is flat it suffices, by proposition 6.3.7, to show that, for any left A-module X, $K \otimes_A X \to F \otimes_A X$ is injective. Note that $K \otimes_A X = \overset{\infty}{\underset{i=0}{\oplus}} (f_i \otimes X)$ and $F \otimes_A X = \overset{\infty}{\underset{i=0}{\oplus}} (e_i \otimes X)$. Suppose $y = \sum\limits_{i=0}^{\infty} (f_i \otimes x_i) \in K \otimes_A X$ maps to zero, then

$$0 = (e_0 - e_1a_1) \otimes x_0 + ... + (e_n - e_{n+1}a_{n+1}) \otimes x_n =$$

$$= e_0 \otimes x_0 + e_1 \otimes (x_1 - a_1x_0) + ... + e_n \otimes (x_n - a_nx_{n-1}) -$$

$$-e_{n+1} \otimes a_{n+1}x_n.$$

Therefore, $x_0 = x_1 = ... = x_n = 0$ and so $y = 0$. Thus, M is flat.

Now assume that M is projective. Then the short exact sequence

$$0 \to K \to F \to M$$

splits, i.e., $F \simeq K \oplus M$. Therefore there exists a projection $\pi : F \to K$. Let $\pi(e_i) = \sum\limits_j f_j b_{ij}$ (where the $b_{ij} \in A$ are almost all zero for any given i). Then

$$f_i = \pi(f_i) = \sum_j f_j b_{ij} - \sum_j f_j b_{i+1,j} a_{i+1},$$

and we have $b_{ii} - b_{i+1,i} a_{i+1} = 1$ for all $i \neq j$. For sufficiently large j we have

$$0 = b_{0j} = b_{1j} a_1 = b_{2j} a_2 a_1 = ... = b_{jj} a_j ... a_2 a_1.$$

As a result, we have

$$a_j ... a_2 a_1 = a_j ... a_2 a_1 - b_{jj} a_j ... a_2 a_1 = (1 - b_{jj}) a_j ... a_2 a_1 =$$

$$= -b_{j+1,j} a_{j+1} a_j ... a_2 a_1$$

for sufficiently large j's. This means that the descending chain of ideals $Aa_1 \supseteq Aa_2 a_1 \supseteq ...$ stabilizes.

Theorem 10.5.5 (H.Bass). *Let A be a ring with Jacobson radical R. Then the following are equivalent:*

1. *A is right perfect.*
2. *Every flat right A-module is projective.*
3. *A satisfies the descending chain condition on principal left ideals.*

Proof.

(1) $\Rightarrow$ (2). Let M be a flat right A-module. By theorem 10.5.3 it has a projective cover $\varphi : P \to M$ which induces a short exact sequence:

$$0 \to K \longrightarrow P \xrightarrow{\varphi} M \to 0$$

Since M is flat, the sequence

$$0 \to K \otimes_A \bar{A} \longrightarrow P \otimes_A \bar{A} \xrightarrow{\varphi \otimes 1} M \otimes_A \bar{A} \to 0$$

is also exact, where $\bar{A} = A/R$. Since $M \otimes_A \bar{A} \simeq M/MR$ and φ is the projective cover, $\varphi \otimes 1$ defines an isomorophism $P/PR \simeq M/MR$. This means that $K/KR = 0$. Since R is T-nilpotent, from theorem 10.5.1 it follows that $K = 0$, that is $M \simeq P$ is projective.

(2) $\Rightarrow$ (3). Consider a descending chain of principal right ideals, we can write by

$$Aa_1 \supseteq Aa_1 a_2 \supseteq .... \tag{10.5.1}$$

As in proposition 10.5.4 we can associate a flat module M to the sequence $\{a_1, a_2, ...\}$. Since by hypothesis M is projective, by proposition 10.5.4, the sequence (10.5.1) stabilizes.

(3) $\Rightarrow$ (4). We now show that the Jacobson radical R of A is right T-nilpotent. Consider an arbitrary sequence $\{a_1, a_2, ...\} \subseteq R$. Since the sequence (10.5.1) stabilizes, we have $a_n..a_1 = ba_{n+1}a_n...a_1$ for some n and some $b \in A$. Then $(1 - ba_{n+1})a_n...a_1 = 0$. Since, by proposition 3.4.5, the element $1 - ba_{n+1}$ is invertible in A, $a_n...a_1 = 0$, that is R is right T-nilpotent.

Since every descending chain of principal right ideals in $\bar{A} = A/R$ can be written in the form

$$\bar{A}\bar{a}_1 \supseteq \bar{A}\bar{a}_1\bar{a}_2 \supseteq .... \tag{10.5.2}$$

the d.c.c. on principal left ideals of A implies the same for $\bar{A}$. Thus, A/R is semisimple, and so A is right perfect.

10.6. EQUIVALENT CATEGORIES

In chapter 4 we introduced the general notions of category and functor. In this chapter we are interested only in categories of modules over rings and additive functors between them. The main notion in this section will be the notion of an equivalence of categories of modules, which is a mathematical formulation of the idea "having the same structure".

Definition. Two categories $\mathcal{C}$ and $\mathcal{D}$ are **isomorphic** if there are functors $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ such that $GF = 1_{\mathcal{C}}$ and $FG = 1_{\mathcal{D}}$, where $1_{\mathcal{C}}$ and $1_{\mathcal{D}}$ are the respective identity functors.

Unfortunately this notion of an isomorphism of categories is not very useful in the theory of modules. Very often categories which intuitively must be 'equal' are not isomorphic according to this definition. So we introduce a weaker, but more useful definition.

Recall that a functor F from a category $\mathcal{C}$ to a category $\mathcal{D}$ is additive if $F(f + g) = F(f) + F(g)$ for any morphisms $f, g \in Mor\mathcal{C}$. The most important functors in the theory of modules, the functors Hom and $\otimes$, are additive.

Recall the definition of a natural isomorphism of functors which we introduced in section 4.1.

Definition. Let F and G be two functors from a category C to a category D. A **morphism** (or a **natural transformation**) from the functor F to the functor G is a map φ which assigns to each object $X \in ObC$ a morphism $\varphi(X) : F(X) \to G(X)$ of the category D with the following property: for any pair of objects $X, Y \in ObC$ and any any morphism $f : X \to Y$ of the category C we have

$G(f)\varphi(X) = \varphi(Y)F(f)$, i.e., the following diagram commutes:

$$\begin{array}{ccc} F(X) & \xrightarrow{\varphi(X)} & G(X) \\ \downarrow{\scriptstyle F(f)} & & \downarrow{\scriptstyle G(f)} \\ F(Y) & \xrightarrow{\varphi(Y)} & G(Y) \end{array}$$

A morphism of functors will simply be denoted by $\varphi : F \to G$. If for every $X \in ObC$ the morphism $\varphi(X)$ is an isomorphism, then one says that φ is an **natural isomorphism of functors** and writes $\varphi : F \simeq G$. Then there is a natural transformation $\varphi^{-1} : G \to F$ defined by $\varphi^{-1}(X) = \varphi(A)^{-1}$. In this case the two functors F, G from the category $\mathcal{C}$ to the category $\mathcal{D}$ are said to be **isomorphic** and we shall write $F \simeq G$.

Definition. An additive covariant functor $F : \mathcal{C} \to \mathcal{D}$ is called an **equivalence** of categories $\mathcal{C}$ and $\mathcal{D}$ if there exists a covariant additive functor $G : \mathcal{D} \to \mathcal{C}$ such that $GF \simeq 1_{\mathcal{C}}$ and $FG \simeq 1_{\mathcal{D}}$. A functor G with this property is called an **inverse equivalence** to F. In this case we shall also say that a pair of functors F and G give an equivalence of the categories $\mathcal{C}$ and $\mathcal{D}$. If there is such an equivalence, the categories $\mathcal{C}$ and $\mathcal{D}$ are called **equivalent**, written as $\mathcal{C} \approx \mathcal{D}$.

Obviously, isomorphic categories are equivalent, but not conversely.

This section is devoted to the study of some of the main properties of equivalent categories.

Proposition 10.6.1. *If the functors $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ are an equivalence of categories, then*

1. *The correspondence $Hom_{\mathcal{C}}(X, Y) \to Hom_{\mathcal{D}}(F(X), F(Y))$ mapping f to $F(f)$ is bijective;*

2. *The correspondence $Hom_{\mathcal{D}}(U, V) \to Hom_{\mathcal{C}}(G(U), G(V))$ mapping g to $G(g)$ is bijective;*

3. *A morphism $f \in Mor\mathcal{C}$ is an isomorphism if and only if $F(f)$ is an isomorphism;*

4. *A morphism $g \in Mor\mathcal{D}$ is an isomorphism if and only if $G(g)$ is an isomorphism;*

5. *Every object $X \in Ob\mathcal{C}$ is isomorphic to an object of the form $G(U)$, where $U \in Ob\mathcal{D}$;*

6. *Every object $U \in Ob\mathcal{D}$ is isomorphic to an object of the form $F(X)$, where $X \in Ob\mathcal{C}$.*

Proof. 1. Let $G : \mathcal{D} \to \mathcal{C}$ be a functor inverse to F. Let $f : X \to Y$ be a morphism of the category $\mathcal{C}$ and $\varphi : GF \to 1_{\mathcal{C}}$ be a natural isomorphism of

functors. Consider the commutative diagram:

$$\begin{array}{ccc} GF(X) & \xrightarrow{\varphi(X)} & X \\ \downarrow{\scriptstyle GF(f)} & & \downarrow{\scriptstyle f} \\ GF(Y) & \xrightarrow{\varphi(Y)} & Y \end{array}$$

Since $\varphi(X)$ is an isomorphism, $f = \varphi(Y)GF(f)\varphi^{-1}(X)$. So if $F(f) = F(f_1)$, $GF(f) = GF(f_1)$ and hence $f = f_1$ for $f_1 \in Mor\mathcal{C}$. Thus, the map $Hom_{\mathcal{C}}(X,Y) \to Hom_{\mathcal{D}}(F(X),F(Y))$ is injective.

Let $g : F(X) \to F(Y)$ be an arbitrary monomorphism. We consider $f = \varphi(Y)G(g)\varphi^{-1}(X)$ and $g_1 = F(f)$. Then, as before, $f = \varphi(Y)G(g_1)\varphi^{-1}(X)$ and thus $G(g) = G(g_1)$. Consequently, $g = g_1 = F(f)$, i.e., the map $Hom_{\mathcal{C}}(X,Y) \to Hom_{\mathcal{D}}(F(X),F(Y))$ is surjective, and therefore it is bijective.

3. If f is an isomorphism, then $F(f)$ is an isomorphism without any special assumption on the functor F.

Conversely, suppose $F(f) : F(X) \to F(Y)$ is an isomorphism. Then there exists a homomorphism $\alpha : F(Y) \to F(X)$ such that $F(f)\alpha = 1_{F(Y)}$ and $\alpha F(f) = 1_{F(X)}$. By property 1, there is a homomorphism $g : Y \to X$ such that $F(g) = \alpha$. Hence $F(gf) = F(g)F(f) = \alpha F(f) = F(1_{F(X)})$ and $F(fg) = F(f)F(g) = F(f)\alpha = F(1_{F(Y)})$. Again, by property 1, we obtain that $fg = 1_{F(Y)}$ and $gf = 1_{F(X)}$. Thus, f is an isomorphism.

5. Since $GF \simeq 1_{\mathcal{C}}$, $GF(X) \simeq X$ for any $X \in Ob\mathcal{C}$. Then $X \simeq G(U)$, where $U = F(X) \in Ob\mathcal{D}$.

The other statements of the proposition are proved similarly.

Definition. An additive functor $F : \mathcal{C} \to \mathcal{D}$ is called **faithful** if $F(f) = 0$ implies $f = 0$, where $f \in Mor\mathcal{C}$. In other words, F is faithful if the homomorphism $Hom_{\mathcal{C}}(X,Y) \to Hom_{\mathcal{D}}(F(X),F(Y))$ is injective for all X, Y.

An additive functor $F : \mathcal{C} \to \mathcal{D}$ is said to be **full** if the homomorphism $Hom_{\mathcal{C}}(X,Y) \to Hom_{\mathcal{D}}(F(X),F(Y))$ is surjective for all X, Y.

From proposition 10.6.1 we now obtain the following statement:

Proposition 10.6.2. *An additive covariant functor $F : \mathcal{C} \to \mathcal{D}$ is an equivalence of categories if and only if*

1. *F is a faithful functor;*
2. *F is a full functor;*
3. *Every object $U \in Ob\mathcal{D}$ is isomorphic to an object of the form $F(X)$, where $X \in Ob\mathcal{C}$.*

Proposition 10.6.3. *If two functors F : mod-$A \to$ mod-B and G : mod-$B \to$ mod-A constitute an equivalence of categories, then there exist natural isomorphisms*

$$Hom_B(N, F(M)) \simeq Hom_A(G(N), M)$$

$$Hom_B(F(M), N) \simeq Hom_A(M, G(N))$$

of Abelian groups in each variable.

Proof. Let N be a right B-module. Since $FG \simeq 1_B$, there is an isomorphism $\omega_N : FG(N) \simeq N$. For any right A-module M this isomorphism induces an isomorphism of Abelian groups

$$Hom_B(F(M), FG(N)) \simeq Hom_B(F(M), N)$$

Since F is an equivalence, by proposition 10.6.2, F is faithful and full, and so we have an isomorphism

$$Hom_A(M, G(N)) \simeq Hom_B(F(M), FG(N)) \simeq Hom_B(F(M), N))$$

in which $f \in Hom_A(M, G(N))$ corresponds to $\omega_N F(f) \in Hom_B(F(M), N))$. We shall show that this isomorphism is a natural transformation in each variable. Suppose we have a homomorphism $u : N \to N_1$ in mod-B.

Then because $u\omega_N = \omega_{N_1} FG(u)$, we have

$$\omega_{N_1} F((G(u)f) = \omega_{N_1}(FG(u))F(f) = u(\omega_N F(f))$$

which shows that the diagram

$$\begin{array}{ccc} Hom_A(M, G(N)) & \longrightarrow & Hom_B(F(M), N) \\ \downarrow & & \downarrow \\ Hom_A(M, G(N_1)) & \longrightarrow & Hom_B(F(M), N_1) \end{array}$$

is commutative. The statement for the other variable is proved similarly. This completes the proof.

Proposition 10.6.4. *Let a functor F be an equivalence of the categories mod-A and mod-B, then a sequence of A-modules*

$$0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0 \tag{10.6.1}$$

is exact if and only if the sequence of B-modules

$$0 \longrightarrow F(M_1) \xrightarrow{F(f)} F(M_2) \xrightarrow{F(g)} F(M_3) \longrightarrow 0 \tag{10.6.2}$$

is exact.

Proof. Assume that the sequence (10.6.1) is exact. We shall prove that sequence (10.6.2) is also exact. Since f is a monomorphism and g is an epimorphism, by proposition 10.6.1, it follows that $F(f)$ is a monomorphism and $F(g)$ is an epimorphism. Since $gf = 0$, we obtain that $F(g)F(f) = F(gf) = 0$ and therefore $ImF(f) \subseteq KerF(g)$. Thus all that remains to be proved is

that $KerF(g) \subseteq ImF(f)$. Write $K = KerF(g)$. Let $i_K : K \to F(M)$ be a natural inclusion. By proposition 10.6.3, there is an isomorphism $\varphi : Hom_B(K, F(M)) \simeq Hom_A(G(K), M)$, where G is the inverse functor to F. Then $\varphi(i_K) \in Hom_B(K, F(M))$ and by this proposition we have $g\varphi(i_K) = \varphi(F(g)(i_K)) = \varphi(0) = 0$. Therefore $Im\varphi(i_K) \subseteq Kerg = Imf$. Then by proposition 1.2.1 there is a homomorphism $h : G(K) \to M_1$ such that $fh = \varphi(i_K)$. Since φ is an isomorphism, we obtain $i_K = \varphi^{-1}(fh) = F(f)\varphi^{-1}(h)$. Hence $K = KerF(g) = Imi_K \subseteq ImF(f)$. This proves that sequence (10.6.2) is exact.

Conversely, let sequence (10.6.1) be exact. Since G is also an equivalence, then by the proof above the sequence

$$0 \longrightarrow GF(M_1) \stackrel{GF(f)}{\longrightarrow} GF(M_2) \stackrel{GF(g)}{\longrightarrow} GF(M_3) \longrightarrow 0$$

is also exact. But $GF \simeq 1_{mod-A}$, so the sequence (10.5.1) is exact, as required.

Corollary 10.6.5. *If a functor F is an equivalence of categories between mod-A and mod-B, then it is exact.*

Proposition 10.6.6. *If a functor F is an equivalence of the categories mod-A and mod-B, then a right A-module P is projective if and only if the right B-module $F(P)$ is projective.*

Proof. Suppose P is a projective right A-module and

$$0 \to N_1 \to N \to N_2 \to 0$$

is an exact sequence of right B-modules. Let G be the functor inverse to F. Since G is an equivalence, G is exact by corollary 10.6.5, and so we have an exact sequence of right A-modules:

$$0 \to G(N_1) \to G(N) \to G(N_2) \to 0$$

Since P is projective, $Hom_A(P, *)$ is an exact functor, and so we have an exact sequence:

$$0 \to Hom_A(P, G(N_1)) \to Hom_A(P, G(N)) \to Hom_A(P, G(N_2)) \to 0$$

By proposition 10.6.3 we have also the following exact sequence:

$$0 \to Hom_B(F(P), N_1) \to Hom_B(F(P), N) \to Hom_B(F(P), N_2) \to 0$$

which shows that $F(P)$ is a projective right B-module.

Conversely, let $F(P)$ be projective, then $GF(P)$ is also projective, since G is an equivalence. Since $GF(P) \simeq P$, we obtain that P is projective.

Definition. We say that a right A-module P is a **generator** for the category mod-A, if for every right A-module M there is an epimorphism

$$P^{(I)} \longrightarrow M \longrightarrow 0$$

for some set I, where $P^{(I)}$ denotes the direct sum of the modules P_i $(i \in I)$, all P_i being isomorphic to P.

For example, A_A is a generator for the category mod-A, since any right A-module is a quotient of a free module.

Proposition 10.6.7. *A right A-module P is a generator for the category mod-A if and only if there exists an isomorphism $P^n \simeq A \oplus X$ of A-modules for some integer $n > 0$ and some A-module X.*

Proof. Since P is a generator, it generates the right regular A-module A_A. However A_A is finitely generated, so P is finitely generates A_A, i.e., there is an epimorphism

$$P^n \longrightarrow A \longrightarrow 0$$

for some integer $n > 0$. Since A_A is projective, this sequence splits, i.e., $P^n \simeq A \oplus X$.

The inverse statement is obvious, since any module is a quotient of a free module.

The following statement may be considered as giving equivalent definitions of the concept of a generator.

Proposition 10.6.8. *For a right A-module P the following statements are equivalent:*

1. *P is a generator for the category mod-A;*
2. *For any right A-module M we have $M = Hom_A(P, M)P = \sum\{\varphi P \mid \varphi \in Hom_A(P, M)\}$;*
3. *$Hom_A(P, *)$ is a faithful functor from mod-A to the category of Abelian groups.*

Proof.

(1) $\Rightarrow$ (2) and (2) $\Rightarrow$ (1) are obvious.

(2) $\Rightarrow$ (3). Note that $Hom_A(P, *)$ is a faithful functor means that for any nonzero $f \in Hom_A(M, N)$ there exists $g \in Hom_A(P, M)$ such that $fg \neq 0$.

Let $f \in Hom_A(M, N)$ be given and $f \neq 0$. Take an $m \in M$ for which $fm \neq 0$. By hypothesis $m = \varphi_1 x_1 + \varphi_2 x_2 + ... + \varphi_n x_n$ for some $\varphi_1, \varphi_2, ..., \varphi_n \in Hom_A(P, M)$ and $x_1, x_2, ..., x_n \in P$. Thus $f\varphi_1 x_1 + f\varphi_2 x_2 + ... + f\varphi_n x_n \neq 0$. Without loss of generality, let $f\varphi_1 x_1 \neq 0$. Then $f\varphi_1 \neq 0$, as required.

(3) $\Rightarrow$ (2). Suppose there exists a right A-module M such that $K = Hom_A(P, M)P \neq M$, i.e., the inclusion $K = Hom_A(P, M)P \subset M$ is strict. Let $f : M \to M/K$ be the natural projection, then $f \neq 0$. By hypothesis there is $g \in Hom_A(P, M)$ such that $fg \neq 0$. But $Img \subseteq K$. A contradiction. Hence, $K = M$.

From this proposition we see that the property of being a generator is a categorical one and so we have the following statement.

Proposition 10.6.9. *If a functor F is an equivalence of categories mod-A and mod-B, then a right A-module P is a generator of mod-A if and only if the right B-module $F(P)$ is a generator of mod-B.*

Proposition 10.6.10. *A right A-module P is projective and finitely generated if and only if there is an isomorphism $P \oplus X \simeq A^n$ for some integer $n > 0$ and some A-module X.*

Proof. Since a module P is projective and finitely generated if and only if it is a direct summand of a finitely generated free module, we have an epimorphism $A^n \longrightarrow P \longrightarrow 0$ for some integer $n > 0$. Since P is projective, this sequence is split, i.e., $A^n \simeq P \oplus X$ for some module X.

Definition. We say that a right A-module P is a **progenerator** for mod-A, if it is a finitely generated projective generator.

In particular, A_A is a progenerator for mod-A and ${}_AA$ is a progenerator for A-mod.

From propositions 10.6.7 and 10.6.10 there follows immediately the next statement:

Proposition 10.6.11. *A right A-module P is a progenerator for mod-A if and only if there are integers $n > 0$, $m > 0$, and A-modules X, Y such that $P^n \simeq A \oplus X$ and $A^m \simeq P \oplus Y$.*

Since the property of being a finitely generated module is a categorical property, propositions 10.6.6 and 10.6.9 yield the following statement:

Proposition 10.6.12. *If a functor F is an equivalence of the categories mod-A and mod-B, then a right A-module P is a progenerator of mod-A if and only if the right B-module $F(P)$ is a progenerator of mod-B.*

Consider the category mod-A of right A-modules. Let P be a right A-module. Put $B = End_A(P)$. Then P becomes a left B-module, by $\varphi p = \varphi(p)$. It is easy to check that this turns P into a left B-module. Since $\varphi(pa) = ((\varphi(p))a = (\varphi p)a$, P is an (B, A)-bimodule. Then $Hom_A(P, *)$ is an additive covariant functor from mod-A to mod-B. Moreover, for any right A-module M, $Hom_A(P, M)$ is a right B-module. Indeed, for any $f : P \to M$ and any $\varphi : P \to P$ we can consider $f\varphi$ as a composition of two homomorphisms. If we take $M = P$, then we can consider $Hom_A(P, P) = End_A(P) = B$ as a right module over itself. And by proposition 2.1.2 we have a ring isomorphism:

$$B = End_A(P) \to Hom_B(F(P), F(P)) = End_B(B)$$

Thus we obtain the following statement.

Proposition 10.6.13. *Let functors F : mod-$A \to$ mod-B and G : mod-$B \to$ mod-A constitute an equivalence of categories and let $P = G(B)$. Then P is a progenerator of mod-A such that $End_A(P) \simeq B$.*

Proposition 4.3.5 shows that the functor $Hom_A(P, *)$ preserves finite direct sums. In the situation when P is a finitely generated module we have a stronger statement, namely that this functor preserves any direct sum as well.

Proposition 10.6.14. *Let the M_i $(i \in I)$ be right A-modules. If P is a finitely generated right A-module, then there is an isomorphism*

$$Hom_A(P, \underset{i\in I}{\oplus} M_i) \simeq \underset{i\in I}{\oplus} Hom_A(P, M_i)$$

as Abelian groups. If $B = End_A(P)$, then this is in addition an isomorphism of right B-modules.

Proof. Let $M = \underset{i\in I}{\oplus} M_i$, let $\pi_i : M \to M_i$ be a natural projection and let $f \in Hom_A(P, A)$. Since P is a finitely generated A-module, $\pi_i f$ is the zero homomorphism for almost all i and hence $\{\pi_i f\}_{i\in I}$ is in $\underset{i\in I}{\oplus} Hom_A(P, M_i)$. Then the mapping $\alpha : Hom_A(P, \underset{i\in I}{\oplus} M_i) \to \underset{i\in I}{\oplus} Hom_A(P, M_i)$ such that $\alpha(f) = \{\pi_i f\}_{i\in I}$ is a homomorphism of Abelian groups, which is obviously a monomorphism. We shall show that α is an epimorphism as well. Let $\{g_i\}_{i\in I}$ be in $\underset{i\in I}{\oplus} Hom_A(P, M_i)$. For any $p \in P$ we put $g(b) = \{g_i(b)\}_{i\in I}$. Then $g \in Hom_A(P, M)$ and $\alpha(g) = \{g_i\}_{i\in I}$. Thus, α is an epimorphism, and so an isomorphism of Abelian groups.

If $B = End_A(P)$, then, as was shown above, the $Hom_A(P, M)$ and each $Hom_A(P, M_i)$ can be regarded as right B-modules. If $\varphi \in B$, then $\{\pi_i f\varphi\}_{i\in I}$ is the product of $\{\pi_i f\}_{i\in I}$ and φ. Therefore the constructed isomorphism φ is not only an isomorphism of Abelian groups but also an isomorphism of B-modules.

10.7. THE MORITA THEOREM

In this section we shall prove the famous Morita theorem, which gives the answer to the question: which rings A and B are such the categories of modules over them have the "same" structure?

Theorem 10.7.1. *Let P be a progenerator in the category mod-A, $B = End_A(P)$, $F = Hom_A(P, *)$ and $G = * \otimes_B P$. Then F, G give an equivalence of the categories mod-A and mod-B.*

Proof. For the functors F and G we can construct a functor morphism $\varphi : 1_{mod-B} \to FG$ in the following way. For every B-module N we define $\varphi(N)$ to be the homomorphism $N \to Hom_A(P, N \otimes_B P)$, mapping an element $x \in N$ into the A-homomorphism $u_x : P \to N \otimes_B P$ giving by $u_x(p) = x \otimes_B p$. Also there is

a functor morphism $\psi : 1_{mod-A} \to GF$ defined as follows. For every A-module M define $\psi(M)$ to be the homomorphism $Hom_A(P, M) \otimes_B P \to M$ mapping $f \otimes_B p$ into $f(p) \in M$, where $f \in Hom_A(P, M)$ and $p \in P$. It is easy to verify that φ and ψ are functor morphisms. We shall show that they are, indeed, functor isomorphisms, i.e., natural.

Indeed, $\varphi(B)$ is a natural isomorphism, since $B = Hom_A(P, P) \simeq Hom_A(P, B \otimes_B P) = FG(B)$. As P is a finitely generated A-module, using propositions 10.6.14 and 4.6.2 we obtain that $FG(B^{(I)}) = Hom_A(P, B^{(I)} \otimes_B P) \simeq Hom_A(P, P^{(I)}) \simeq B^{(I)}$ for any index set I.

Since B is a progenerator of mod-B, for any right B-module N there is an epimorphism $f : B^{(I)} \to N$. Let $N_1 = Kerf$. There is also an epimorphism $g : B^{(J)} \to N_1$. Then the sequence

$$B^{(J)} \xrightarrow{g} B^{(I)} \xrightarrow{f} N \longrightarrow 0 \tag{10.7.1}$$

is exact. Since P is projective, the functor F is exact, and G is right exact, so the functor FG is also right exact. Applying the functor FG to the sequence (10.7.1) we obtain again an exact sequence

$$FG(B^{(J)}) \xrightarrow{FG(g)} FG(B^{(I)}) \xrightarrow{FG(f)} FG(N) \longrightarrow 0 \tag{10.7.2}$$

Since we have isomorphisms $\varphi_1 : B^{(I)} \to FG(B^{(I)})$ and $\varphi_2 : B^{(J)} \to FG(B^{(J)})$, we obtain the following commutative diagram

$$\begin{array}{ccccccc} B^{(J)} & \xrightarrow{g} & B^{(I)} & \xrightarrow{f} & N & \longrightarrow & 0 \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi(N)} & & \\ FG(B^{(J)}) & \xrightarrow{FG(g)} & FG(B^{(I)}) & \xrightarrow{FG(f)} & FG(N) & \longrightarrow & 0 \end{array}$$

with exact rows and isomorphisms φ_1 and φ_2. Then by corollary 4.2.6 $\varphi(N)$ is also an isomorphism. Thus $FG(N) \simeq N$ for any right B-module N.

In a similar way we shall show that $GF(M) \simeq M$ for any right A-module M.

Since P is a progenerator of mod-A, for any right A-module M there is an epimorphism $f : P^{(I)} \to M$. Let $M_1 = Kerf$. There is also an epimorphism $g : P^{(J)} \to M_1$. Then the sequence

$$P^{(J)} \xrightarrow{g} P^{(I)} \xrightarrow{f} M \longrightarrow 0 \tag{10.7.3}$$

is exact. We have natural isomorphisms

$$GF(P) = Hom_A(P, P) \otimes_B P \simeq End_A(P) \otimes_B P = B \otimes_B P \simeq P$$

On the other hand, since P is a finitely generated A module, applying propositions 10.6.14 and 4.6.2 gives that

$$GF(P^{(I)}) = Hom_A(P, P^{(I)}) \otimes_B P \simeq B^{(I)} \otimes_B P \simeq \bigotimes_I (B \otimes_B P) \simeq P^{(I)}$$

for any index set I. Therefore applying the functor GF to the sequence (10.6.2) we obtain the following commutative diagram

$$\begin{array}{ccccccc} P^{(J)} & \xrightarrow{g} & P^{(I)} & \xrightarrow{f} & M & \longrightarrow & 0 \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi(N)} & & \\ GF(P^{(J)}) & \xrightarrow{GF(g)} & GF(P^{(I)}) & \xrightarrow{GF(f)} & GF(M) & \longrightarrow & 0 \end{array}$$

with exact rows and isomorphisms φ_1 and φ_2. Then by corollary 4.2.6 $\varphi(M)$ is also an isomorphism. Thus $GF(M) \simeq M$ for any right A-module M.

Definition. Two rings A and B are said to be **Morita equivalent** if their categories of modules mod-A and mod-B are equivalent.

From proposition 10.6.13 and theorem 10.7.1 we immediately obtain the following famous theorem:

Theorem 10.7.2 (K.Morita). *Two rings A and B are Morita equivalent if and only if there is a progenerator P in mod-A such that $B \simeq End_A(P)$. In this case, an equivalence of the categories of mod-A and mod-B is realized by the pair of functors $F = Hom_A(P, *)$ and $G = * \otimes_B P$.*

Corollary 10.7.3. *Let A be a ring and $n > 0$ be a natural number. Then the rings A and $M_n(A)$ are Morita equivalent.*

Proof. Since A is a progenerator for mod-A, the module A^n is also a progenerator for mod-A for any integer $n > 0$. Then A is Morita equivalent to the ring $B \simeq End_A(A^n) \simeq M_n(A)$.

Corollary 10.7.4. *If A and B are Morita equivalent rings, then there is an idempotent $e \in M_n(A)$ such that $B \simeq eM_n(A)e$.*

Proof. Since the rings A and B are Morita equivalent, there is a progenerator P such that $B \simeq End_A(P)$. By proposition 10.6.11 it follows that there is an integer $n > 0$ such that $A^n \simeq P \oplus Y$. Then $M_n(A) \simeq End_A(A^n) \simeq End_A(P \oplus Y)$. And from the two-sided Peirce decomposition we obtain that there is an idempotent $e \in M_n(A)$ such that $End_A(P) \simeq eM_n(A)e$.

Let A be an FDI-ring (see section 2.4). Then the identity of A can be decomposed into a sum of pairwise orthogonal primitive idempotents and A can be decomposed into a direct sum of a finite number of indecomposable right ideals of the form e_iA. Each such ideal is an indecomposable principal right A-module. Writing $e_iA = P_i$ and grouping isomorphic modules together we can write this decomposition in the form: $A = P_1^{n_1} \oplus ... \oplus P_s^{n_s}$ where the $P_1, ..., P_s$ are pairwise nonisomorphic indecomposable right ideals. Clearly, an FDI-ring A can also be decomposed into a sum of indecomposable left ideals.

Corollary 10.7.5. *Let A be an FDI-ring with a decomposition $A = P_1^{n_1} \oplus ... \oplus P_s^{n_s}$ into a direct sum of pairwise nonisomorphic right ideals. Let $B = End_A(P)$ be the ring of endomorphisms of the module $P = P_1 \oplus ... \oplus P_s$. Then the rings A and B are Morita equivalent.*

Proof. It is obvious that there are integers $n > 0$ and $m > 0$ such that $P^n \simeq A \oplus X$ and $A^m \simeq P \oplus Y$. Then from proposition 10.5.11 it follows that P is a progenerator. Then the statement is immediately follows from the Morita theorem.

A nonzero subset $\mathcal{I} \subset MorC$ is called an **ideal** of a category C if $\mathcal{I}(MorC) \subset \mathcal{I}$ and $(MorC)\mathcal{I} \subset \mathcal{I}$ (products are understood in the usual sense).

A morphism $f : X \to Y$ is called **right invertible** if there is a morphism $g : Y \to X$ such that $fg = 1_Y$. A left invertible morphism is defined analogously. A right and left invertible morphism is called **invertible** or an **isomorphism**.

A category is called **local** if the set of its nonivertible morphisms forms an ideal.

Consider an FDI-ring A. We construct a category $C(P_1, ..., P_s)$ for a decomposition $A = P_1^{n_1} \oplus ... \oplus P_s^{n_s}$ of A by the following way: the objects of this category are the right ideals $P_1, ..., P_s$ and $Hom(P_i, P_j)$ is the set of all homomorphisms from the module P_i to the module P_j $(i, j = 1, ..., s)$.

Theorem 10.7.6. *An FDI-ring A is semiperfect if and only if there is a decomposition $A = P_1^{n_1} \oplus ... \oplus P_s^{n_s}$ such that the category $C(P_1, ..., P_s)$ is local.*

Proof. Let the category $C(P_1, ..., P_s)$ be local. Then the rings $Hom(P_i, P_i)$ $(i = 1, ..., s)$ are local. By theorem 10.3.8 the ring A is semiperfect.

Conversely, if the ring A is semiperfect, then it can be represented in the form $A = P_1^{n_1} \oplus ... \oplus P_s^{n_s}$ and by theorem 10.3.7 every right ideal P_i has exactly one maximal submodule. By theorem 10.3.8 the rings $Hom(P_i, P_i)$ $(i = 1, ..., s)$ are local. Since the modules P_i and P_j for $i \neq j$ are nonisomorphic, $Hom(P_i, P_j)$ consists of non-invertible morphisms for $i \neq j$. Therefore the category $C(P_1, ..., P_s)$ is local.

Proposition 10.7.7. *Let A be an FDI-ring and $A = P_1^{n_1} \oplus ... \oplus P_s^{n_s}$. In the category $C(P_1, ..., P_s)$ any nonzero morphism is an epimorphism if and only if the ring A is a semisimple ring.*

Proof. If A is a semisimple ring, then the statement follows from the Wedderburn-Artin theorem.

Conversely, since each P_i is an indecomposable principal A-module, by proposition 5.1.6, any nonzero morphism $\psi : P_i \to P_i$ $(i = 1, ..., s)$ is an isomorphism and all morphisms between nonisomorphic modules P_i and P_j are zeroes. By theorem 2.1.2, proposition 2.1.3 and the Wedderburn-Artin theorem, the ring A is isomorphic to a direct product of a finite number of full matrix rings over division

rings, i.e., is a semisimple ring.

Proposition 10.7.8. *Let A be a ring and $1 = \sum_{i=1}^{n} e_i$ be a decomposition of $1 \in A$ into a sum of mutually orthogonal idempotents. Then the following statements are equivalent*:

1. *For any e_i and e_k each nonzero homomorphism $\varphi \in Hom_A(e_iA, e_kA)$ is a monomorphism.*

2. *For any e_i each nonzero homomorphism $\varphi \in Hom_A(e_iA, A)$ is a monomorphism.*

3. *For all e_i, e_j, e_k we have $ab \neq 0$ for any nonzero elements $a \in e_iAe_j$ and $b \in e_jAe_k$.*

Proof. These equivalences can be directly verified and are left to the reader.

Remark. Since condition (3) is symmetrical, conditions (1) and (2) can be replaced by their left-side analogs.

Definition. Let A be a ring and let $1 = \sum_{i=1}^{n} e_i$ be a decomposition of $1 \in A$ into a sum of mutually orthogonal idempotents. A ring A is called a **piecewise domain** (with respect to $\{e_1, e_2, ..., e_n\}$) if it satisfies the equivalent statements of proposition 10.7.8.

Recall that a ring A is called right semihereditary if any finitely generated right ideal in the ring A is projective.

Proposition 10.7.9. *In the category $C(P_1, .., P_s)$ of a right semihereditary FDI-ring $A = P_1^{n_1} \oplus ... \oplus P_s^{n_s}$ any nonzero morphism is a monomorphism, that is, a right semihereditary FDI-ring is a piecewise domain.*

Proof. Let $\psi : P_i \to P_j$ be a nonzero homomorphism $(i, j = 1, ..., s)$. Since P_j is a principal module and A is a semihereditary ring, $Im\psi \subset P_j$ is a projective module and by proposition 5.1.6, $P_i \simeq Im\psi \oplus Ker\psi$. Hence, $Ker\psi = 0$ because P_i is indecomposable.

Let $A = P_1^{n_1} \oplus ... \oplus P_s^{n_s}$ be a decomposition of an FDI-ring A into a direct sum of pairwise nonisomorphic right ideals. Denote $B = End_A P$, where $P = P_1 \oplus ... \oplus P_s$.

Definition. We say that a property $\mathcal{P}$ is **Morita invariant**, if whenever a ring A has this property, so does any other ring B which is Morita equivalent to A.

Many ring-theoretical properties are Morita invariant. Examples of such properties are being semisimple, right Noetherian, right hereditary, right semihereditary, right primitive, right semiprimitive.

10.8. NOTES AND REFERENCES

In noncommutative algebra, there is a natural generalization of the notion of a local ring. However in noncommutative algebra, the theory of localization does not work nearly as well as in the commutative case. Due to the lack of a good localization theory, the role of local rings in noncommutative algebra is not nearly as prominent as in the commutative case. Nevertheless, noncommutative local rings do arise naturally, and form an important class for study.

Many rings which arise naturally in the theory of rings are semilocal rings. The importance of semilocal rings is determined by a large number of applications in such different domains, as algebraic geometry, commutative and noncommutative algebra, the theory of groups, the theory of modules and the theory of categories.

Proposition 10.1.5 was proved by H.Fitting in his paper *H.Fitting, Die Theorie der Automorphismenringe Abelscher Gruppen und ihr Analogon bei nicht kommutativen Gruppen // Math. Ann. , v.107 (1933), p.514-542).*

Note, that C.Faith in his book *Algebra: Rings, Modules and Categories. I, Springer-Verlag, Berlin-Heidelberg-New York, 1973* introduced a notion of a **lift-ring**, i.e., a ring for which idempotents may lifted modulo any right ideal. Rings for which idempotents can be lifted modulo the radical of the ring were considered by I.Kaplansky and N.Jacobson, and were called **SBI-rings** (see *N. Jacobson, Structure of Rings. American Mathematical Society Colloquium Publications, Vol. 37, American Mathematical Society, Providence, 1956*).

In 1960 H.Bass introduced perfect and semiperfect rings in his famous paper *Finitistic dimension and homological generalization of semiprimary rings // Trans. Amer. Math. Soc., v.95 (1960), p.466-488.* He called a ring A left semiperfect if every cyclic left A-module has a projective cover. The definition of a perfect (resp. semiperfect) ring in this book is one of the equivalent conditions of theorem P. (resp. theorem 2.1) in this paper of H.Bass.

Classically, there was a rich and very well-developed theory of modules over one-sided Artinian rings. In the early 1960's, part of this theory was extended to the wider class of semiperfect rings. However, the passage from one-sided Artinian rings to semiperfect rings is not just a generalization for generalization's sake. Semiperfect rings turn out to be a significant class of rings from the viewpoint of homological algebra, since they are precisely the rings whose finitely generated (left or right) modules have projective covers. At the same time, right perfect rings are precisely the rings for which all right flat modules are projective. These interesting module-theoretic characterizations led to many more applications of homological methods in ring theory, and helped establish the notions of perfect and semiperfect rings firmly in the literature.

Theorem 10.3.8 first was proved by B.Müller in his paper *B.Müller, On semi-perfect rings // Ill. J. Math., v.14, N.3 (1970), p.464-467.*

The formulation of theorem 10.4.13 in this form is due to V.V.Kirichenko in *Rings and Modules, Kiev University, 1981.*

Theorem 10.6.6 shows that semiperfect rings from the categorial point of view are a naturally generalization of local rings.

Chapter 22 of the book *C.Faith, Algebra: Rings, Modules and Categories II. Springer-Verlag, Berlin-Heidelberg-New York, 1976* and Chapter 11 of the book *F.Kasch, Modules and Rings. Academic Press, New York, 1982* are devoted to the theory of semiperfect rings.

The famous Morita theorems were proved in the paper *K.Morita, Duality for modules and its applications to the theory of rings with minimum condition // Sci. Rep. Tokyo Kyoiku Daigaku, v.6 (1958), p.83-142.*

Piecewise domains were studied by R.Gordon and L.W.Small in the paper *Piecewise domains // J. Algebra, v.23, 1972, p.553-564.*

11. Quivers of rings [1])

11.1 QUIVERS OF A SEMIPERFECT RING

In this section we define the quiver of a right Noetherian semiperfect ring and consider its properties. The notion of a quiver for a finite dimensional algebra over an algebraically closed field was introduced by P.Gabriel in 1972 in connection with problems of the representation theory of finite dimensional algebras. In 1975 V.V.Kirichenko carried over this notion to the case of semiperfect right Noetherian rings. For the case of finite dimensional algebras over an algebraically closed field the notion of a quiver for semiperfect right Noetherian rings coincides with the notion of a Gabriel quiver.

Recall the definition of the Gabriel quiver for a finite dimensional algebra A over a field k. We can restrict ourselves to basic split algebras. (An algebra A is called **basic** if A/R is isomorphic to a product of division algebras, where R is the Jacobson radical of A. An algebra A over a field k is called **split** if $A/R \simeq M_{n_1}(k) \times M_{n_2}(k) \times .... \times M_{n_s}(k)$.) All algebras over algebraically closed fields are split.

Let $P_1, ..., P_s$ be all pairwise nonisomorphic principal right A-modules. Write $R_i = P_iR$ $(i = 1, ..., s)$ and $V_i = R_i/R_iR$. Since V_i is a semisimple module, $V_i = \bigoplus\limits_{j=1}^{s} U_j^{t_{ij}}$, where $U_j = P_j/R_j$ are simple modules. It is equivalent to the isomorphism $P(R_i) \simeq \bigoplus\limits_{j=1}^{s} P_j^{t_{ij}}$. To each module P_i assign a point i in the plane and join the point i with the point j by t_{ij} arrows. The so constructed graph is called the **quiver** of A in the sense of P.Gabriel and denoted by $Q(A)$.

Let $A_A = P_1^{n_1} \oplus \ldots \oplus P_s^{n_s}$ be the decomposition of a semiperfect ring A into a direct sum of principal right A-modules, and let $P = P_1 \oplus ... \oplus P_s$, $B = End_A(P)$. By the Morita theorem the category of right A-modules is equivalent to the category of right B-modules. Obviously, $B/radB$ is a direct sum of division rings. The ring B is called the **basic ring** of the ring A.

Definition. A semiperfect ring A is called **reduced** if its quotient ring by the Jacobson radical R is a direct sum of division rings.

[1]) That is, this chapter is about the various quivers (of modules) that are defined for certain rings. The title phrase of this chapter does not refer to quivers (i.e., oriented graphs) with a ring attached to each vertex.

This is equivalent to the fact that there are no isomorphic modules in the decomposition of the ring A into a direct sum of principal right A-modules.

Examples 11.1.1.

1. Let D be a division ring, and $P = \{\alpha_1, ..., \alpha_n\}$ be a poset with partial order $\leq$. Consider the subring A in $M_n(D)$ with $e_{ii}Ae_{jj} = D$ if $\alpha_i \leq \alpha_j$ and $e_{ii}Ae_{jj} = 0$ otherwise. Then $M_n(D)$ is a nonreduced semiperfect ring, while A is a reduced semiperfect ring, moreover, A is an Artinian ring.

2. Analogously, let $\mathcal{O}$ be a discrete valuation ring, and $P = \{\alpha_1, ..., \alpha_n\}$ be a poset with partial order $\leq$. Consider a subring A in $M_n(\mathcal{O})$ with $e_{ii}Ae_{jj} = \mathcal{O}$ if $\alpha_i \leq \alpha_j$ and $e_{ii}Ae_{jj} = 0$ otherwise. Then $M_n(\mathcal{O})$ is a nonreduced semiperfect ring, while A is a reduced semiperfect ring, moreover, A is a non-Artinian ring.

From the Morita theorem it follows that the category of modules over a semiperfect ring A is equivalent to the category of modules over a reduced semiperfect ring, i.e., the basic ring of the ring A. A semiperfect ring is called **self-basic** if it coincides with its basic ring.

Let A be a semiperfect right Noetherian ring, $P_1, ..., P_s$ be all pairwise non-isomorphic principal right A-modules. Consider the projective cover of $R_i = P_iR$ $(i = 1, ..., s)$, which, as above, we shall denote by $P(R_i)$. Let $P(R_i) = \bigoplus\limits_{j=1}^{s} P_j^{t_{ij}}$. We assign to the principal modules $P_1, ..., P_s$ points $1, .., s$ in the plane and join the point i with the point j by t_{ij} arrows. The so constructed graph is called the **right quiver** (or simply the **quiver**) of the semiperfect right Noetherian ring A and will be denoted by $Q(A)$.

Analogously, one can define the left quiver $Q'(A)$ of a left Noetherian semiperfect ring.

One can show that the right quiver of a finite dimensional algebra A over a field K coincides with the Gabriel quiver of A.

Note, that the quiver of a semiperfect right Noetherian ring does not change by switching to its basic ring. Indeed, from the definition of projective cover it follows that $Q(A) = Q(A/R^2)$.

Definition. Let A be a semiperfect ring such that A/R^2 is a right Artinian ring. The quiver of the ring A/R^2 is called the **quiver** of the ring A and is denoted by $Q(A)$.

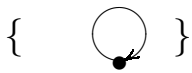
Examples 11.1.2.

1) The quiver of a semisimple ring is a disconnected union of points and so it has the form:

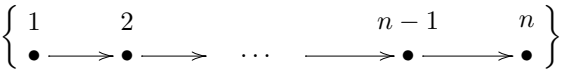
$$\{ \bullet \qquad \bullet \qquad \cdots \qquad \bullet \}$$

2) Consider the quiver of the ring of p-integral numbers $A = \mathbf{Z}_{(p)}$, where p is a prime integer. It is a local ring with a unique principal module which is regular. The projective cover of this module is the radical $R = p\mathbf{Z}_{(p)}$ of the ring A. Since

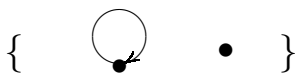
R is cyclic, the quiver of $\mathbf{Z}_{(p)}$ is a one-pointed cycle and so it has the following form:



3) Let $A = T_n(D)$ be the ring of upper triangular matrices of degree n over a division ring D. It has n principal A-modules of the form $e_{ii}A$, where the e_{ii} are the matrix units. It is easy to verify that $R_i \simeq P_{i+1}$ for $i = 1, 2, .., n-1$ and $R_n = 0$. Therefore, the quiver of A is a chain which has the following form:



4) Let $A = \begin{pmatrix} \mathbf{Z}_{(p)} & \mathbf{Q} \\ 0 & \mathbf{Q} \end{pmatrix}$, where $\mathbf{Z}_{(p)}$ is the ring of p-integral numbers, and $\mathbf{Q}$ is the field of rational numbers. It is easy to verify that the quiver $Q(A)$ has the form:



Let $A_A = P_1^{n_1} \oplus ... \oplus P_s^{n_s}$ be the decomposition of a semiperfect ring A into a direct sum of principal right A-modules and let $1 = f_1 + ... + f_s$ be the corresponding decomposition of the identity of A into a sum of pairwise orthogonal idempotents, i.e., $f_iA = P_i^{n_i}$. Then ${}_AA = Af_1 \oplus \ldots \oplus Af_s = Q_1^{n_1} \oplus \ldots \oplus Q_s^{n_s}$ is the decomposition of the semiperfect ring A into a direct sum of principal left A-modules, i.e. $Af_i = Q_i^{n_i}$, where Q_i is an indecomposable projective left A-module $(i = 1, \ldots, s)$. Now consider the two-sided Peirce decomposition of the ring A

$$A = \begin{pmatrix} A_{11} & A_{12} & \ldots & A_{1n} \\ A_{21} & A_{22} & \ldots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n2} & \ldots & A_{nn} \end{pmatrix}.$$

Consider also the two-sided Peirce decomposition of the Jacobson radical R of A: $R = \bigoplus_{i,j} f_iRf_j$. Since R is a two-sided ideal, $f_iRf_j \subset R$ for all i, j. By proposition 3.4.8 we have $R_{ii} = f_iRf_i = rad(f_iAf_i)$ for $i = 1, ..., n$. We shall show that $f_iRf_j = f_iAf_j$ for $i \neq j$. Indeed, multiplying on the left elements from f_jA by an element f_iaf_j we obtain a homomorphism φ_{ji} of the module f_jA to f_iA. If $Im(\varphi_{ji}) = f_iA$, then φ_{ji} is an epimorphism. Since $f_iA = P_i^{n_i}$, $f_jA = P_j^{n_j}$ are projective modules, by proposition 5.1.6, and $P_i^{n_i}$ is isomorphic to a direct summand of the module $P_j^{n_j}$. But this is impossible, since the indecomposable modules P_i and P_j are non-isomorphic. Therefore $Im(\varphi_{ji}) \subset f_iA$. We can write the homomorphism φ_{ji} in the form of a matrix $\varphi_{ji} = (\varphi_{ji}^{rs})$, where $\varphi_{ji}^{rs} : P_j \longrightarrow P_i$

are homomorphisms of indecomposable non-isomorphic projective modules P_j and P_i for $r = 1, ..., n_i$, $s = 1, ..., n_j$. Since $Im(\varphi_{ji}^{rs}) \neq P_i$, we have $Im(\varphi_{ji}^{rs}) \subseteq P_iR$. Therefore $Im(\varphi_{ji}) \subseteq f_iAR = f_iR$, i.e., $f_iAf_j \subseteq f_iR$. Hence $A_{ij} = f_iAf_j = f_iRf_j$ for $i \neq j$. Thus, we obtain the following result.

Proposition 11.1.1. *Let $A = P_1^{n_1} \oplus ... \oplus P_s^{n_s}$ be the decomposition of a semiperfect ring A into a direct sum of principal right A-modules and let $1 = f_1 + ... + f_s$ be a corresponding decomposition of the identity of A into a sum of pairwise orthogonal idempotents, i.e., $f_iA = P_i^{n_i}$. Then the Jacobson radical of the ring A has a two-sided Peirce decomposition of the following form:*

$$R = \begin{pmatrix} R_{11} & A_{12} & \dots & A_{1n} \\ A_{21} & R_{22} & \dots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n2} & \dots & R_{nn} \end{pmatrix}, \tag{11.1.1}$$

where $R_{ii} = rad(f_iAf_i)$, $A_{ij} = f_iAf_j$ for $i, j = 1, ..., n$.

The ring f_iAf_i is isomorphic to $End_A(P_i^{n_i}) \simeq M_{n_i}(End(P_i))$, where $End_A(P_i) = \mathcal{O}$ is a local ring by theorem 10.3.8. By proposition 3.4.10 $radM_{n_i}(\mathcal{O}) = M_{n_i}(rad\mathcal{O}_i)$.

We now set $U_i = P_i/P_iR$. Since $\bar{A} = A/R = U_1^{n_1} \oplus \ldots \oplus U_s^{n_s}$, the idempotents $f_1, \ldots, f_s$ are central modulo the radical and all simple right A-modules are exhausted by the modules $U_1, \ldots, U_s$. Analogously, let $V_i = Q_i/RQ_i$, then all simple left A-modules are exhausted by the modules $V_1, \ldots, V_s$.

Definition. An idempotent $f \in A$ is called **canonical** if $\bar{f}\bar{A} = \bar{A}\bar{f} = M_{n_k}(\mathcal{D}_k)$ for some $k = 1, \ldots, s$; $\bar{f} = f + R$.

Equivalently, f is a minimal central idempotent modulo R.

A decomposition $1 = f_1 + \ldots + f_s$ into a sum of pairwise orthogonal canonical idempotents will be called **a canonical decomposition of the identity of a ring** A.

It is clear that the decomposition of identity, used in proposition 11.1.1, is a canonical decomposition of the identity of the ring A.

Lemma 11.1.2. (Annihilation lemma). *Let $1 = f_1 + \ldots + f_s$ be a canonical decomposition of $1 \in A$. For every simple right A-module U_i and for each f_j we have $U_if_j = \delta_{ij}U_i$, $i, j = 1, \ldots, s$. Similarly, for every simple left A-module V_i and for each f_j, $f_jV_i = \delta_{ij}V_i$, $i, j = 1, \ldots, s$.*

Proof. We shall give the proof for the case of right modules. From the previous proposition we obtain that $f_iRf_j = f_iAf_j$ for $i \neq j$. Hence $P_i^{n_i}f_j \subset f_iR$. But $f_iA/f_iR \simeq U_i^{n_i}$. Therefore $U_i^{n_i}f_j = 0$ and so $U_if_j = 0$ for $i \neq j$.

We are going to show that $U_if_i = U_i$. Let $u \in U_i$. Then $u \cdot 1 = u(f_1 + ... + f_s) = uf_i$ since $uf_j = 0$ for $i \neq j$. The lemma is proved.

Let A be a reduced semiperfect ring, and let $1 = e_1 + ... + e_s$ be a decomposition of $1 \in A$ into a sum of mutually orthogonal local idempotents.

Set $U_i = e_iA/e_iR$ and $V_i = Ae_i/Re_i$.

Lemma 11.1.3 (Q-Lemma). *The simple module U_k (resp. V_k) appears in the direct sum decomposition of the module e_iR/e_iR^2 (resp. Re_i/R^2e_i) if and only if $e_iR^2e_k$ (resp. $e_kR^2e_i$) is strictly contained in e_iRe_k (resp. e_kRe_i).*

Proof. If U_k is a direct summand of the module $W_i = e_iR/e_iR^2$, then by proposition 2.2.4 and lemma 11.1.2, $W_ie_k \neq 0$. Therefore e_iRe_k does not equal $e_iR^2e_k$ and the inclusion $e_iRe_k \supset e_iR^2e_k$ is strict.

Conversely, suppose that $e_iR^2e_k$ is strictly contained in e_iRe_k. Consider a submodule X_k contained in e_iR,

$$X_k = e_iRe_i \oplus ... \oplus e_iRe_{k-1} \oplus e_iR^2e_k \oplus e_iRe_{k+1} \oplus ... \oplus e_iRe_s$$

(here the direct sum sign denotes a direct sum of Abelian groups).

From the inclusions $e_iR \supset X_k \supset e_iR^2$ it follows that e_iR/X_k is a semisimple module. We have the equalities $e_iR/X_k = e_iRe_k/e_iR^2e_k = (e_iR/X_k)e_k$. By lemma 11.1.2 the module e_iR/X_k decomposes into a direct sum of some copies of the module U_k. Since e_iR/X_k is isomorphic to a direct summand W_i, the module U_k is contained in W_i as a direct summand.

For left modules V_k the statement is proved analogously. The lemma is proved.

Lemma 11.1.4. *Let A be a semiperfect ring, and e, f be nonzero idempotents of the ring A such that $\bar{e} = \bar{f} \in \bar{A}$. Then there exists an invertible element $a \in A$ such that $f = aea^{-1}$.*

Proof. Let $W_1 = \bar{e}\bar{A} = \bar{f}\bar{A}$. Obviously, eA and fA are projective covers of the semisimple A-module W_1. Therefore they are isomorphic. The modules $(1-e)A$ and $(1-f)A$ are projective covers of the semiperfect A-module $W_2 = (\bar{1}-\bar{f})\bar{A} = (\bar{1}-\bar{e})\bar{A}$. Consequently, they are isomorphic too. Write $e_1 = e$, $e_2 = 1-e$ and $f_1 = f$, $f_2 = 1-f$.

Now using lemma 10.3.6 we obtain that $f_i = ae_ia^{-1}$ and $f = aea^{-1}$.

Lemma 11.1.5. *Let $1 = f_1 + \ldots + f_s$ be a canonical decomposition of the identity $1 \in A$ into a sum of pairwise canonical idempotents and g be a central idempotent modulo R. There exists an invertible element $a \in A$ such that $f_{i_1} + \ldots + f_{i_k} = aga^{-1}$ for a suitable subset $\{i_1, i_2, ..., i_k\}$ of $\{1, 2, ..., s\}$.*

Proof. Let $\bar{g}\bar{A} = \bar{A}\bar{g} = M_{n_{i_1}}(\mathcal{D}_{i_1}) \times \ldots \times M_{n_{i_k}}(\mathcal{D}_{i_k})$. Then $f = f_{i_1} + \ldots + f_{i_k}$ is a central idempotent modulo R and $\bar{f}\bar{A} = \bar{g}\bar{A}$. By lemma 10.3.6 we have $f = aga^{-1}$.

Corollary 11.1.6. *Each central idempotent modulo R g is a sum of canonical idempotents and there exists a canonical decomposition of $1 \in A$ into a sum of*

pairwise orthogonal canonical idempotents such that $1 = g_1 + \ldots + g_k + g_{k+1} + \ldots + g_s$, *where* $g = g_1 + \ldots + g_k$ *and* $f = f_{i_1} + \ldots + f_{i_k} = ag_1a^{-1} + \ldots + ag_ka^{-1}$ *for some invertible* $a \in A$.

Theorem 11.1.7. *Let* A *be a semiperfect ring and* $1 = f_1 + \ldots + f_s = g_1 + \ldots + g_t$ *be two canonical decompositions of* $1 \in A$ *into a sum of pairwise orthogonal canonical idempotents. Then* $s = t$ *and there exist an invertible element* $a \in A$ *and a permutation* τ *of* $\{1, \ldots, s\}$ *such that* $f_i = ag_{\tau(i)}a^{-1}$ *for each* $i = 1, \ldots, s$.

Proof. Applying the Wedderburn-Artin theorem to $\bar{A}$, we immediately obtain that $s = t$. Let $f_i = e_1^{(i)} + \ldots + e_{n_i}^{(i)}$ be a decomposition of f_i into a sum of pairwise orthogonal local idempotents. Then, obviously, $U_i e_k^{(i)} \neq 0$ for $k = 1, \ldots, n_i$. From the annihilation lemma it follows that $U_i g_{\sigma(i)} = U_i$ for some $g_{\sigma(i)}$ and, moreover, $U_i g_j = 0$ for $j \neq \sigma(i)$. Renumber the idempotents $g_1, \ldots g_s$ such that $U_i g_i = U_i$ $(i = 1, \ldots, s)$. Now decompose $g_i = h_1^{(i)} + \ldots + h_{n_i}^{(i)}$ into a sum of pairwise orthogonal local idempotents. Then we obtain two decompositions of $1 \in A$, which satisfy the assumptions of lemma 10.3.6. Hence, there exists a conjugating element $a \in A$ which transforms one decomposition into the other, up to a permutation. From our numeration of the idempotents $g_1, \ldots g_s$ it follows that $a\{h_1^{(i)}, \ldots, h_{n_i}^{(i)}\}a^{-1} = \{e_1^{(i)}, \ldots, e_{n_i}^{(i)}\}$ for each $i = 1, \ldots, s$ and, consequently, $ag_ia^{-1} = f_i$ $(i = 1, \ldots, s)$.

We shall need a lemma, which allows one to compute the minimal number of generators $\mu_A(X)$ of a finite dimensional module X over a semiperfect ring A.

Lemma 11.1.8. *Let* $A = \bigoplus_{i=1}^{s} P_i^{n_i}$ *be the decomposition of a semiperfect ring* A *into a direct sum of principal right* A*-modules, let* $\mu_A(X)$ *be the minimal number of generators of a finite generated right* A*-module* X *and* $P(X) = \bigoplus_{i=1}^{s} P_i^{m_i}$. *If* $m = max\frac{m_i}{n_i}$ *is an integer, then* $\mu_A(X) = m$. *Otherwise,* $\mu_A(X) = [m] + 1$.[2])

Proof. Suppose m is not an integer and set $\mu = [m] + 1$. Then $\mu n_i \geq m_i$ for all i. Therefore, $A^\mu = P(X) \oplus P'$, where P' is a projective module. Clearly, there is an epimorphism $A^\mu \to X \to 0$, i.e., $\mu_A(X) \leq \mu$.

Conversely, from the exact sequence $A^{\mu_A(X)} \to X \to 0$, in view of lemma 10.4.5, we obtain a decomposition $A^{\mu_A(X)} = P(X) \oplus P'$. Hence $\mu_A(X) \geq m_i$ for all i. Therefore $\mu_A(X) \geq \mu$.

In the second case the proof is analogous. The lemma is proved.

Definition. The quiver $Q(A)$ of a ring A is called **connected** if it cannot be represented in the form of a union of two nonempty disjoint subsets Q_1 and Q_2 which are not connected by any arrows.

[2]) Here $[m]$ is the entire of m, i.e., the largest integer $\leq m$.

Theorem 11.1.9. *The following conditions are equivalent for a semiperfect Noetherian ring A:*

(a) *A is an indecomposable ring;*

(b) *A/R^2 is an indecomposable ring;*

(c) *the quiver of A is connected.*

Proof. Obviously, the conditions of the theorem are preserved by passing to the Morita equivalent rings. Therefore we can assume that the ring A is reduced.

$(a) \Rightarrow (b)$. Let $\bar{A} = A/R^2 \simeq \bar{A}_1 \times \bar{A}_2$ and let $\bar{1} = \bar{f}_1 + \bar{f}_2$ be the corresponding decomposition of the identity of the ring A/R^2 into a sum of orthogonal idempotents. Let $g_1,\ g_2 \in A$ be elements such that $g_1 + R^2 = \bar{f}_1$ and $g_2 + R^2 = \bar{f}_2$. There are idempotents $f_1, f_2 \in A$ such that $f_1 = g_1 + r_1$ and $f_2 = g_2 + r_2$, where $r_1, r_2 \in R^2$. Since $\bar{f}_1\bar{A}\bar{f}_2 = 0$ and $\bar{f}_2\bar{A}\bar{f}_1 = 0$, we have $g_1ag_2 \in R^2$ and $g_2ag_1 \in R^2$ for any $a \in A$. Clearly, $f_i = f_ig_if_i + f_ir_if_i$ $(i = 1, 2)$. Then the element $f_1af_2 = f_1g_1f_1af_2g_2f_2 + f_1g_1f_1af_2r_2f_2 + f_1r_1f_1af_2g_2f_2 + f_1r_1f_1af_2r_2f_2$ belongs to R^2 for any $a \in A$. This is immediate from proposition 11.1.1. Exactly in the same way $f_2Af_1 \subset R^2$. Therefore $f_2Af_1 = f_2R^2f_1$ and $f_1Af_2 = f_1R^2f_2$. By proposition 11.1.1, the two-sided Peirce decomposition of R has the form: $R = \begin{pmatrix} R_1 & A_{12} \\ A_{21} & R_2 \end{pmatrix}$, where $R_i = Rad(f_iAf_i)$ $(i = 1, 2)$ and $A_{ij} = f_iAf_j$ for $i \neq j$. Calculating R^2 we obtain

$$R^2 = \begin{pmatrix} R_1^2 + A_{12}A_{21} & R_1A_{12} + A_{12}R_2 \\ A_{21}R_1 + R_2A_{21} & A_{21}A_{12} + R_2^2 \end{pmatrix}.$$

From the above we have: $A_{12} = R_1A_{12} + A_{12}R_2$ and $A_{21} = R_2A_{21} + A_{21}R_1$. By theorem 3.6.1, taking into account Nakayama's lemma, we obtain that $A_{12} = 0$ and $A_{21} = 0$ and therefore $A = A_{11} \times A_{22}$, where $A_{ii} = f_iAf_i$ $(i = 1, 2)$.

$(a) \Rightarrow (c)$. Let the quiver of the ring A be disconnected. Then $Q(A) = Q_1 \cup Q_2$ and $Q_1 \cap Q_2 = \emptyset$, and the points of the sets Q_1 and Q_2 are not connected by any arrows. Renumbering, if necessary, the principal right A-modules $P_1, ..., P_s$ one may assume that $Q_1 = \{1, ..., k\}$ and $Q_2 = \{k+1, ..., s\}$. Let $A = P_1 \oplus ... \oplus P_s$ be a decomposition of the ring A into a direct sum of principal right A-modules (where $P_i = e_iA, e_i^2 = e_i \in A,\ 1 = e_1 + ... + e_s$) and $1 = f_1 + f_2$, where $f_1A = P_1 \oplus ... \oplus P_k$ and $f_2A = P_{k+1} \oplus ... \oplus P_s$. We set $A_{ij} = f_iAf_j$, $R_i = radA_{ii}$ $(i = 1, 2)$. If $A_{12} \neq 0$, then by theorem 3.6.1, taking into account Nakayama's lemma, we obtain that the inclusion $A_{12} \supset R_1A_{12} + A_{12}R_2$ is strict. But $R_1A_{12} + A_{12}R_2 = f_1R^2f_2$. Therefore there are local idempotents e_i and e_j such that e_i is a summand of f_1 and e_j is a summand of f_2 and $e_iR^2e_j$ is strictly contained in e_iRe_j. By lemma 11.1.3 we obtain that there is an arrow which connects the point i with the point j. A contradiction. Analogously it can be proved that $A_{21} = 0$.

$(c) \Rightarrow (a)$. If the ring A is decomposable then A/R^2 is also decomposable. Clearly, in this case $Q(A)$ is disconnected.

$(b) \Rightarrow (a)$ is trivial.

The theorem is proved.

Remark. Theorem 11.1.9 is not true for semiperfect one-sided Noetherian rings. As an example one can consider the ring $A = \begin{pmatrix} \mathbf{Z}_{(p)} & \mathbf{Q} \\ 0 & \mathbf{Q} \end{pmatrix}$ introduced in section 5.6. As was pointed out at the beginning of the section its quiver has the form:

As was shown in section 5.6 $R^2 = \begin{pmatrix} p^2\mathbf{Z}_{(p)} & \mathbf{Q} \\ 0 & \mathbf{Q} \end{pmatrix}$. So the ring A/R^2 decomposes into a direct product of rings:

$$A/R^2 \simeq \mathbf{Z}_{(p)}/p^2\mathbf{Z}_{(p)} \times \mathbf{Q}.$$

However, the ring A itself is indecomposable into a direct product of rings.

One can prove that if the quiver of a semiperfect right Noetherian indecomposable ring is disconnected, then the intersection of natural powers of the radical of this ring is not equal to zero.

Proposition 11.1.10. *Let A be a semiperfect ring such that A/R^2 is left and right Artinian. Then:*

(1) *if $Q(A)$ has an arrow from i to j, the left quiver $Q'(A)$ has an arrow from j to i;*

(2) *if $Q(A)$ has an arrow σ_{ij} from i to j, there exist a nonzero homomorphisms from P_j to P_i and from Q_i to Q_j.*

The proof immediately follows from the definition of $Q(A)$.

Denote by Q_u the quiver obtained from Q by replacing all arrows from i to j by a single arrow (we allow $i = j$). If Q has no arrows from i to j then neither does Q_u.

Let $\overline{Q}$ be the non-oriented graph obtained from Q by ignoring the orientation of the arrows.

Corollary 11.1.11. *Let A be a ring such that A/R^2 is right and left Artinian. Then $\overline{Q_u(A)} = \overline{Q'_u(A)}$.*

The proof follows from proposition 11.1.10.

11.2 THE PRIME RADICAL

Definition. The **prime radical** of a ring $\mathcal{A}$ is the intersection of all prime ideals in A. We shall denote it by $Pr(A)$.

Since by proposition 9.2.2 any maximal ideal is prime, for any ring A the Jacobson radical $rad(A)$ contains the prime radical $Pr(A)$, i.e.,

$$Pr(A) \subseteq rad(A). \tag{11.2.1}$$

The next useful statement follows immediately from this definition and proposition 9.2.12.

Proposition 11.2.1. *The prime radical $Pr(A)$ of a ring A is a semiprime ideal which is contained in every semiprime ideal in A, i.e., $Pr(A)$ is the smallest semiprime ideal in A.*

Recall that a right (or left) ideal $\mathcal{I}$ in a ring A is called **nilpotent** if $\mathcal{I}^n = 0$ for some positive integer n. An element $a \in A$ is **nilpotent** if $a^n = 0$ for some positive integer n. A right (or left) ideal $\mathcal{I}$ is called **nil-ideal** if every element of $\mathcal{I}$ is nilpotent.

Proposition 11.2.2. *The prime radical of a ring A contains all nilpotent one-sided ideals of A.*

Proof. Let $\mathcal{I}$ be a right (or left) nilpotent ideal in A so that $\mathcal{I}^n = 0$ for some positive integer n, then, obviously, $\mathcal{I}^n \subseteq Pr(A)$. Since $Pr(A)$ is a semiprime ideal, by proposition 9.2.5 it follows that $\mathcal{I} \subseteq Pr(A)$.

Proposition 11.2.3. *For a right Artinian ring A the Jacobson radical $rad(A)$ is equal to the prime radical $Pr(A)$, i.e., $rad(A) = Pr(A)$.*

Proof. By proposition 3.5.1 the Jacobson radical $rad(A)$ of a right Artinian ring A is nilpotent and so by proposition 11.2.2 we have the inclusion $rad(A) \subseteq Pr(A)$. Taking into account the inverse inclusion (11.2.1), which holds for any ring A, we obtain the required equality.

Proposition 11.2.4. *For any ring A the following statements are equivalent:*
(1) *A is a semiprime ring.*
(2) *The prime radical of A is equal to zero.*
(3) *A has no nonzero nilpotent ideals.*
(4) *A has no nonzero right nilpotent ideals.*
(5) *A has no nonzero left nilpotent ideals.*

Proof. The equivalence (1) $\Longleftrightarrow$ (2) follows immediately from the definition of a semiprime ring and proposition 11.2.1.

All other implications are clear.

Corollary 11.2.5. *If $Pr(A)$ denotes the prime radical of a ring A then $Pr(A/Pr(A)) = 0$.*

The proof of this statement follows immediately from propositions 11.2.4 and 9.2.4.

Let us give an internal characterization of the prime radical. We need the following definition.

Definition. An element $a \in A$ is called **strongly nilpotent** if all terms of any sequence $\{a_i\}_{i=0}^{\infty}$ such that $a_0 = a$ and $a_{n+1} \in a_n A a_n$ are equal to zero for sufficiently large n.

It is easy to show that each strongly nilpotent element is nilpotent. Indeed, let $a \in A$ be a strongly nilpotent element. Consider the sequence $\{a_i\}_{i=0}^{\infty}$ given by $a_0 = a$, $a_1 = a^2$, $a_2 = a_1^2 = a^4$,...,$a_{n+1} = a_n^2 = a^{2^{n+1}} \in a_n A a_n$. Then for some positive integer k we have $a_k = a^{2^{k+1}} = 0$, i.e., the element a is nilpotent.

Proposition 11.2.6 (J.Levitzki). *The prime radical of a ring A coincides with the set of all strongly nilpotent elements of A.*

Proof. Let $a \in A$ be an element which does not belong to the prime radical $Pr(A)$. Then there exists a prime ideal P such that $a_0 = a \notin P$. By proposition 9.2.1 $a_0 A a_0 \notin P$. Therefore there exists an element $a_1 \in a_0 A a_0$ such that $a_1 \notin P$. Continuing this process, we obtain for each n an element $a_{n+1} \in a_n A a_n$ such that $a_{n+1} \notin P$. So, there is a sequence $\{a_i\}_{i=0}^{\infty}$ of elements such that $a_{n+1} \in a_n A a_n$ and $a_n \notin P$. Therefore $a_n \neq 0$ for all n, i.e., the element a is not strongly nilpotent.

Conversely, let an element $a \in A$ be not strongly nilpotent and $\{a_i\}_{i=0}^{\infty}$ be a sequence such that $a_{n+1} \in a_n A a_n$ for all n and with $a_n \neq 0$ for all n. Let $M = \{a_0, a_1, ..., a_n, ...\}$. Then $0 \notin M$. By Zorn's lemma there exists an ideal P which is maximal among all ideals which does not contain elements of the set M, i.e., such that $P \cap M = \emptyset$.

We shall show that P is a prime ideal in A. Assume $\mathcal{I}$ and $\mathcal{J}$ are right (or left) ideals of the ring A such that $\mathcal{I} \not\subseteq P$ and $\mathcal{J} \not\subseteq P$. Since $P + \mathcal{I} \neq P$ and $P + \mathcal{J} \neq P$, by the maximality of the ideal P it follows that $(P + \mathcal{I}) \cap M \neq \emptyset$ and $(P + \mathcal{J}) \cap M \neq \emptyset$. Let $a_i \in P + \mathcal{I}$, $a_j \in P + \mathcal{J}$ and $m = max(i, j)$, then

$$a_{m+1} \in a_m A a_m \subseteq (P + \mathcal{I})(P + \mathcal{J}) \subseteq P + \mathcal{I}\mathcal{J}.$$

But $a_{m+1} \notin P$, therefore $\mathcal{I}\mathcal{J} \not\subseteq P$. By proposition 9.2.1

P is a prime ideal and $a_0 = a \notin P$. Therefore $a \notin Pr(A)$.

Since each strongly nilpotent element is nilpotent, we have the following corollary.

Corollary 11.2.7. *The prime radical of a ring A is a nil-ideal.*

Since idempotents can be lifted modulo any nil-ideal, by proposition 10.3.1 the following proposition is true.

Proposition 11.2.8. *In any ring idempotents can be lifted modulo the prime radical.*

Proposition 11.2.9. *Let $Pr(A)$ be the prime radical of a ring A, $e^2 = e \in A$ and $e \neq 0$. Then $ePr(A)e$ coincides with the prime radical of the ring eAe.*

Proof. Let $a \in ePr(A)e$. Then $a = eae$ is a strongly nilpotent element, moreover all elements of the sequence $a_0, a_1, a_2, ...$, such that $a_0 = a$ and $a_{n+1} \in a_n A a_n$ belongs to eAe.

Conversely, let an element a belong to the prime radical $Pr(eAe)$ of the ring eAe. Then, obviously, an arbitrary sequence $a_0 = a, a_1, ..., a_n, ...$ such that $a_{n+1} \in a_n A a_n$ belongs to eAe. Therefore $a_m = 0$ for some positive integer m, and so $a \in Pr(A)$.

Proposition 11.2.10. *For any ring A we have $Pr(M_n(A)) = M_n(Pr(A))$.*

Proof. Let $\mathcal{J} = Pr(A)$ be the prime radical of the ring A. Then $A/\mathcal{J}$ is a semiprime ring and by proposition 9.2.14 it follows that $M_n(A/\mathcal{J})$ is also a semiprime ring. Since $M_n(A/\mathcal{J}) \simeq M_n(A)/M_n(\mathcal{J})$, $M_n(\mathcal{J})$ is a semiprime ideal in $M_n(A)$. Therefore, by proposition 11.2.1, $Pr(M_n(A)) \subseteq M_n(\mathcal{J})$.

We shall show that the reverse inclusion also holds. For this we need to show that $M_n(\mathcal{J}) \subseteq P$ for any prime ideal P in $M_n(A)$. Note that $P = M_n(T)$, where T is an ideal in A. It is easy to see that T is a prime ideal in A. If $aAb \in T$, then $ae_{ii}Abe_{ii} \in P$ for any matrix unit e_{ii}, and so by proposition 9.2.14 we have either $a \in T$ or $b \in T$. Since T is prime, we have $\mathcal{J} \subseteq T \subseteq P$, therefore $M_n(\mathcal{J}) \subseteq P$.

Proposition 11.2.11. *The prime radical $Pr(A)$ of a Noetherian ring A is the largest nilpotent right ideal in A.*

Let A be a Noetherian ring. Consider the set S of all nilpotent right ideals in A. Let N be a maximal element in S with respect to inclusion. Suppose $N^n = 0$. If N_1 is another nilpotent ideal in A and $N_1^k = 0$ then $(N + N_1)^{n+k} = 0$ and $N \subseteq N + N_1$. Since N is a maximal element in S, $N_1 \subseteq N + N_1 = N$, and so N is the largest nilpotent right ideal in A.

If N is a nilpotent ideal then, by proposition 11.2.2, $N \subseteq Pr(A)$. We shall show that the inverse inclusion is also true. Suppose $\mathcal{I}$ is a right ideal in A and $\mathcal{I}^m \subseteq N$ for some positive integer m. Then $\mathcal{I}^{mn} = 0$, i.e., $\mathcal{I}$ is a nilpotent right ideal in A. Since N is the largest nilpotent right ideal, $\mathcal{I} \subseteq N$. Therefore, by definition, N is a semiprime ideal in A. Since by proposition 11.2.1 $Pr(A)$ is the smallest semiprime ideal, $Pr(A) \subseteq N$. So, $Pr(A) = N$ is the largest nilpotent right ideal in A.

11.3 QUIVERS (FINITE DIRECTED GRAPHS)

Definition. Following P.Gabriel, a finite directed graph (with possibly multiple

arrows and loops) will be called a **quiver**.

Denote by $1, \ldots, s$ the vertices of a quiver Q and assume that we have t_{ij} arrows starting at the point i and ending at the point j. The matrix

$$\begin{pmatrix} t_{11} & t_{12} & \cdots & t_{1s} \\ \cdots & \cdots & \cdots & \cdots \\ t_{s1} & t_{s2} & \cdots & t_{ss} \end{pmatrix}$$

is called the **adjacency matrix** of the quiver Q and denoted by $[Q]$.

A real matrix $A = (a_{ij})$ is called **non-negative** if all elements a_{ij} are non-negative. Note that every adjacency matrix is non-negative. Moreover, all elements of the adjacency matrix of a simply laced quiver[3]) are equal to 0 or 1.

Denote by $M_n(\mathbf{R})$ the set of all real square matrices of order n.

Let τ be a permutation of the numbers $1, 2, \ldots, n$ and let

$$P_\tau = \sum_{i=1}^{n} e_{i\tau(i)}$$

be the corresponding permutation matrix where the e_{ij} are matrix units. Clearly, $P_\tau^T P_\tau = P_\tau P_\tau^T = E$ is the identity matrix of $M_n(\mathbf{R})$.

Definition. A matrix $B \in M_n(\mathbf{R})$ is called **permutationally reducible** if there exists a permutation matrix P_τ such that

$$P_\tau^T B P_\tau = \begin{pmatrix} B_1 & B_{12} \\ 0 & B_2 \end{pmatrix}, \tag{11.3.1}$$

where B_1 and B_2 are square matrices of order less that n. Otherwise, the matrix is called **permutationally irreducible**.

Note that the transformation of a matrix B to the form $P_\tau^T B P_\tau$, where P_τ is a permutation matrix, amounts to a special permutation of the elements of the matrix B. The rows are permuted according to τ while at the same time the columns are permuted according to τ^{-1}.

Consider a matrix $B \in M_n(\mathbf{R})$. If it is permutationally reducible then there exists a permutation matrix P_1 such that

$$P_1^T B P_1 = \begin{pmatrix} C & E \\ 0 & D \end{pmatrix},$$

where C and D are square matrices of order less that n.

[3]) "Simply laced" means no multiple arrows and (hence) no multiple loops.

If one of matrices C or D is permutationally reducible then it can be expressed in the form analogous to (11.3.1). This means that the matrix B can be transformed by means of a permutation matrix P_2 to the form:

$$P_2^T B P_2 = \begin{pmatrix} K & L & M \\ 0 & H & G \\ 0 & 0 & F \end{pmatrix}.$$

If any of matrices K, H, F is permutationally reducible, then this process can be continued. Continuing the matrix B can be transformed by means of some permutation matrix P to the following form:

$$P^T B P = \begin{pmatrix} B_1 & B_{12} & \cdots & B_{1t} \\ 0 & B_2 & \cdots & B_{2t} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & B_t \end{pmatrix}, \tag{11.3.2}$$

where the square matrices $B_1, B_2, \ldots, B_t$ are permutationally irreducible.

Thus we have obtained the following statement:

Proposition 11.3.1. *Let $B \in M_n(\mathbf{R})$. Then there exists a permutation matrix P such that $P^T B P$ has the form (11.3.2).*

Let $Q = (VQ, AQ, s, e)$ be a quiver, which is given by two sets VQ, AQ and two mappings $s, e : AQ \to VQ$. The elements of VQ are called vertices or points, and those of AQ arrows. Usually the vertices of Q will be denoted by numbers $1, 2, \ldots, s$. If an arrow $\sigma \in AQ$ connects the vertex $i \in VQ$ with the vertex $j \in VQ$, then $i = s(\sigma)$ is called its **start vertex** (or **source vertex**) and $j = e(\sigma)$ is called its **end vertex** (or **target vertex**). This will be denoted as $\sigma : s(\sigma) \to e(\sigma)$, or short $\sigma : i \to j$.

A **path of the quiver** Q from the vertex i to the vertex j is an ordered set of k arrows $\{\sigma_1, \sigma_2, ..., \sigma_k\}$ such that the start vertex of each arrow σ_m coincides with the end vertex of the previous one σ_{m-1} for $1 < m \leq k$, and moreover, vertex i is the start vertex of σ_1, while vertex j is the end vertex of σ_k. The number k of arrows is called the **length of the path**.

The start vertex i of the arrow σ_1 is called the **start of the path** and the end j of the arrow σ_k is called the **end of the path**. We shall say that the path connects the vertex i with the vertex j and this is denoted by $\sigma_1\sigma_2...\sigma_k : i \to j$.

By convention we shall consider that the path ε_i of length zero connects vertex i with itself without any arrow.

Definition. A path, connecting a vertex of a quiver with itself and of length not equal to zero, is called an **oriented cycle**. An oriented cycle of the length 1 is called a **one-pointed cycle** or a **loop**. A quiver without multiple arrows and multiple loops is called a **simply laced quiver**.

For a quiver Q and a field k one can define the **path algebra** kQ of Q over k. It is the (free) vector space with a k-basis consisting of all paths of Q. Multiplication in kQ is defined by obviously way: if the path $\sigma_1 \dots \sigma_m$ connects i and j and the path $\sigma_{m+1} \dots \sigma_n$ connects j and k, then the product $\sigma_1 \dots \sigma_m \sigma_{m+1} \dots \sigma_n$ connects i with k. Otherwise, the product of these paths equals 0.

The identity of this algebra is the sum of all paths ε_i of length zero. Extending the multiplication by the distributivity, we obtain a k-algebra (not necessarily finite dimensional).

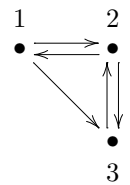
Note that kQ is finite dimensional if and only if Q is finite and has no cyclic path. Moreover, in this case kQ is a basic split algebra. If k is an algebraically closed field and Q is a finite quiver without oriented cycles, then the quiver of kQ can be constructed from Q by reversing of all arrows.

Definition. Denote by VQ the set of all vertices and by AQ the set of all arrows of a quiver Q. A quiver Q_1 with $VQ_1 \subseteq VQ$ and $AQ_1 \subseteq AQ$ is called a **subquiver** of the quiver Q.

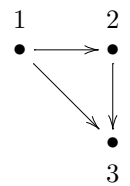
Let Q_1 and Q_2 be subquivers of a quiver Q. We shall say that the subquiver Q_1 contains the subquiver Q_2 and write $Q_2 \subseteq Q_1$ if $VQ_2 \subseteq VQ_1$ and $AQ_2 \subseteq AQ_1$.

Definition. A quiver is called **strongly connected** if there is a path between any two of its vertices. By convention, the one-pointed graph without arrows will be considered to be a strongly connected quiver.

Example 11.3.1.
The quiver of the following form:



is strongly connected. But the following quiver



is not strongly connected.

Let $B \in M_n(\mathbf{R})$ be a matrix with real entries. Using B one can construct a simply laced quiver $Q(B)$ in the following way:

1) the set of vertices $VQ(B)$ of $Q(B)$ is $\{1, 2, ..., n\}$;

2) the set of arrows $AQ(B)$ is defined as follows: There is an arrow from i to j if and only if $b_{ij} \neq 0$.

Proposition 11.3.2. *A matrix $B \in M_n(\mathbf{R})$ is permutationally irreducible if and only if the quiver $Q(B)$ is strongly connected.*

Proof. Let the quiver $Q(B)$ be strongly connected. Then if the matrix B is permutationally reducible then there exists a permutation matrix P_τ such that

$$P_\tau^T B P_\tau = \begin{pmatrix} B_1 & B_{12} \\ 0 & B_2 \end{pmatrix},$$

where $B_1 \in M_p(\mathbf{R})$, $B_2 \in M_q(\mathbf{R})$; $p < n$; $q < n$ and $p + q = n$. We can renumber the vertices of $Q(B)$ in such a way that there are no arrows in $Q(B)$ which connect vertices of the set $\{p + 1, ..., n\}$ with vertices of the set $\{1, ..., p\}$. Therefore the matrix B is permutationally irreducible.

Conversely, let a matrix B be permutationally irreducible. If the quiver $Q(B)$ is not strongly connected, then there exists a pair of vertices k and l ($k \neq l$) such that there is no path between vertices k and l.

Denote by $VQ(k)$ the set of all vertices of the quiver Q which are the ends of each path with the start vertex k, $VQ = VQ(B)$. Clearly, $l \notin VQ(k)$. Denote $X = VQ(k)$, $Y = VQ \backslash VQ(k)$. Since $X \neq \emptyset$, $Y \neq \emptyset$, $X \cup Y = VQ$, $X \cap Y = \emptyset$ and there are no arrows $\sigma : x \to y$, where $x \in X$, $y \in Y$, the matrix B is permutationally reducible. The obtained contradiction proves the proposition.

Corollary 11.3.3. *A quiver Q is strongly connected if and only if the matrix $[Q]$ is permutationally irreducible.*

Note that a renumbering of vertices of the quiver Q transforms the matrix $[Q]$ into the matrix $P_\tau^T [Q] P_\tau$. As an immediate corollary of proposition 11.3.1 we have the following statement:

Proposition 11.3.4. *Let Q be a quiver with adjacency matrix $[Q]$. Then there exists a permutation matrix P such that*

$$P^T [Q] P = \begin{pmatrix} B_1 & B_{12} & \cdots & B_{1t} \\ 0 & B_2 & \cdots & B_{2t} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & B_t \end{pmatrix}, \tag{11.3.3}$$

where the square matrices $B_1, B_2, \ldots, B_t$ are permutationally irreducible.

Definition. The numeration of the vertices of Q will be called **standard** if $[Q]$ is of the form as in the proposition 11.3.4.

Definition. A maximal (with respect to inclusion) strongly connected subquiver of Q is called a **strongly connected component**.

Definition. A partition of the set of vertices of a quiver Q into non-intersecting subsets such that the subquivers corresponding to these subsets are strongly connected quivers (strongly connected components of the quiver Q) shall be called the **partition of the quiver** Q into strongly connected components $Q_1, Q_2, ..., Q_m$; it is denoted by $P(Q; Q_1, ..., Q_m)$.

The existence of a partition of a quiver Q immediately follows from proposition 11.3.4. We shall show that partition is unique up to a renumbering of vertices.

To show the uniqueness of such a decomposition we introduce a binary relation on the set $VS(Q) = \{v_1, v_2, ..., v_n\}$ of all vertices of the quiver Q. We say that $v_i \sim v_j$ if and only if there exists a path from the vertex v_i to the vertex v_j and there exists a path from the vertex v_j to the vertex v_i. Obviously, this relation is symmetric, reflexive and transitive, so it is an equivalence relation.

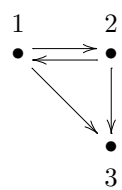
Let $E_1, E_2, ..., E_m$ be equivalence classes of $VS(Q)$. Then $S = \bigcup\limits_{i=1}^{m} E_i$ and $E_i \cap E_j = \emptyset$ for $i \neq j$. Moreover, these equivalence classes are strongly connected components of the quiver Q. Now the uniqueness of the partition of the quiver Q follows from the uniqueness of the partition of the set $VS(Q)$ into the equivalence classes $E_1, E_2, ..., E_m$.

Thus, we have proved the following statement.

Theorem 11.3.5. *Every quiver Q has a partition $P(Q; Q_1, ..., Q_m)$ into strongly connected components Q_1, Q_2,...,Q_m. This partition is unique up to a renumbering of vertices of the quiver Q, that is, if $P(Q; Q_1, ..., Q_m)$ and $P(Q; G_1, ..., G_n)$ are two such partitions, then $m = n$ and there exists a permutation σ of the set $\{1, 2, ..., m\}$ such that $Q_i = G_{\sigma(i)}$ for $i = 1, 2, ..., m$.*

Definition. Let $P(Q; Q_1, ..., Q_m)$ be a partition of a quiver Q into strongly connected components $Q_1, \ldots, Q_m$. The **condensation** Q^* of the quiver Q is the quiver, whose vertices are the points $q_1, \ldots, q_m$ corresponding to strongly connected components $Q_1, \ldots, Q_m$, and, moreover, there is an arrow with start vertex q_i and end vertex q_j if and only if Q has an arrow with the start vertex belonging to VQ_i and the end vertex belonging to VQ_j $(i \neq j;\ i, j = 1, 2, ..., m)$.

Example 11.3.2.
Consider the following quiver



Then its strongly connected components are

$$Q_1 = \left\{ \begin{array}{c} 1 \qquad\qquad 2 \\ \bullet \rightleftarrows \bullet \end{array} \right\}$$

and

$$Q_2 = \left\{ \begin{array}{c} 3 \\ \bullet \end{array} \right\}$$

The condensation of this quiver is:

$$Q^* = \left\{ \begin{array}{c} 1 \qquad\qquad 2 \\ \bullet \longrightarrow \bullet \end{array} \right\}$$

Definition. A quiver without oriented cycles is called an **acyclic quiver**.

The following statement is clear.

Proposition 11.3.6. *A strongly connected acyclic quiver is a point.*

The next statement follows immediately from proposition 11.3.4.

Proposition 11.3.7. *The condensation of any quiver is an acyclic simply laced graph.*

Definition. A vertex of a quiver Q is called a **sink** (resp. a **source**) if there is no arrow with end (resp. start) at this vertex.

Proposition 11.3.8. *Every acyclic quiver has a sink and a source.*

Proof. Due to proposition 11.3.4 the adjacency matrix $[Q]$ of the quiver Q can be transformed to the form (11.3.3). Since Q has no cycles, any diagonal matrix B_i in this decomposition has order 1. Since Q has no loops, all these matrices are equal to zero. So there exists a permutation matrix P such that

$$P^T[Q]P = \begin{pmatrix} 0 & * & \cdots & * & * \\ 0 & 0 & \cdots & * & * \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & * \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix}. \tag{11.3.4}$$

From the form (11.3.4) of the adjacency matrix $[Q]$ of an acyclic quiver Q we immediately obtain the following corollaries.

Corollary 11.3.9. *The adjacency matrix $[Q]$ of an acyclic quiver Q is nilpotent.*

Corollary 11.3.10. *Suppose that the set of vertices of an acyclic quiver consists of t elements. Then we can enumerate these elements by numbers $1, \dots, t$ in such a way that the existence of an arrow from i to j implies $i < j$.*

Definition. Let $S = \{\alpha_1, \dots, \alpha_n\}$ be a finite poset with an ordering relation $\leq$. The **diagram** of S is the quiver $Q(S)$ with as set of vertices $VQ(S) = \{1, \dots, n\}$ and the set of arrows $AQ(S)$ is given by: there is an arrow $\sigma : i \to j$ $(i \neq j)$ if and only if $\alpha_i \leq \alpha_j$, and moreover, there is no element α_k such that $\alpha_i \leq \alpha_k \leq \alpha_j$, where $\alpha_k \neq \alpha_i,\ \alpha_k \neq \alpha_j$.[4])

An arrow $\sigma : i \to j$ of an acyclic quiver Q is called **extra** if there exists a path from i to j of length greater than 1.

Clearly, the diagram of a finite poset S is an acyclic simply laced quiver without extra arrows.

Proposition 11.3.11. *Let Q be an acyclic simply laced quiver without extra arrows. Then Q is the diagram of some finite poset S. Conversely, the diagram $Q(S)$ of a finite poset S is an acyclic simply laced quiver without extra arrows.*

Proof. By corollary 11.3.10 there exists a numbering of the vertices of the quiver Q by the numbers $\{1, \dots, t\}$ such that $i < j$ whenever there is an arrow from i to j. Since there are no extra arrows, the existence of an arrow $\sigma : i \to j$ implies that there is no vertex k, $(k \neq i,\ k \neq j)$ such that there is a path from i to k and from k to j. It follows immediately that Q is the diagram of the poset of its vertices. The converse statement was discussed above. Thus, the proposition is proved.

Remark. Let $Q = (VQ, AQ, s, e)$ be a quiver and let k be a field. A **representation** $V = (V_x, V_\sigma)$ of Q over k is given by a family of vector spaces V_x $(x \in VQ)$ and a family of linear mappings $V_\sigma : V_{s(\sigma)} \to V_{e(\sigma)}$ $(\sigma \in AQ)$. Given two representations V, V', a mapping $f = (f_x) : V \to V'$ is given by linear mappings $f_x : V_x \to V'_x$ such that for each $\sigma \in AQ$ one has $f_{s(\sigma)} V'_\sigma = V_\sigma f_{e(\sigma)}$. If Q is finite, then the category of right kQ-modules is equivalent to the category of representations of Q.

Let A be an associative algebra over a field k. A **representation** of A is an algebra homomorphism $T : A \to End_k(V)$, where V is a vector space over k. If the space V is finite dimensional, then its dimension is called the **dimension** (or **degree**) of the representation T.

For any representation of the algebra A we can construct a right module over that algebra, and vice versa: for any right module we can construct a representation.

Let $T : A \to End_k(V)$ be a representation of the algebra A. Define $va = vT(a)$ for $v \in V$, $a \in A$. It follows immediately from the definition of representation that,

[4]) This diagram is often called the Hasse diagram of the poset S (see e.g. *Encyclopaedia of Mathematics, Vol.7, p.100, KAP, 1991).*

in this way, V becomes a right A-module. We say that this module is corresponds to the representation T. On the other hand, any right A-module is obtained in this way. Indeed, if M is a right A-module, then for a fixed $a \in A$, the map $T(a) : m \mapsto ma$ is a linear transformation in M. Assigning to every $a \in A$ the operator $T(a)$ we obtain a representation of the algebra A corresponding to the module M.

Given two representations $T_1 : A \to End_k(V_1)$ and $T_2 : A \to End_k(V_2)$, a mapping $f : T_1 \to T_2$ is a linear transformtation $f : V_1 \to V_2$ satisfying $f(vT_1(a)) = f(v)T_2(a)$ for $v \in V$, $a \in A$, or, rewritten, $f(va) = f(v)a$; hence it is an A-module homomorphism. Thus, the category of all representations of A is equivalent to the category of all right A-modules.

We say that a representation T of A is **indecomposable** if its corresponding right A-module is indecomposable. The algebra A is said to be **finite representation type** (or short **finite type**) if there are only finitely many isomorphism classes of indecomposable representations of A.

A finite quiver Q is said to be **finite representation type** (or short **finite type**) if the path algebra kQ has this property.

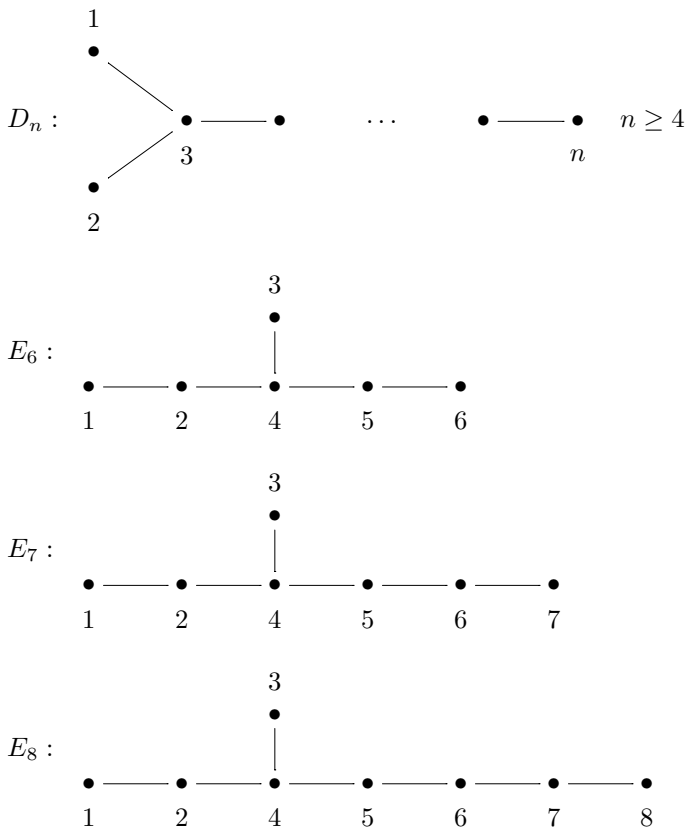
Theorem 11.3.12 (P.Gabriel).[5]) *A connected quiver Q is of a finite type if and only if the underlying undirected graph $\overline{Q}$ of Q (obtained from Q by deleting the orientation of the arrows) is a Dynkin diagram of the form A_n, D_n, E_6, E_7, E_8.*

This theorem was applied to describe some classes of algebras of finite representation type.

For any finite quiver $Q = (VQ, AQ, s, e)$ we can construct a bipartite quiver $Q^b = (VQ^b, AQ^b, s_1, e_1)$ in the following way. Let $VQ = \{1, 2, ..., s\}$, $AQ = \{\sigma_1, \sigma_2, ..., \sigma_k\}$. Then $VQ^b = \{1, 2, ..., s, b(1), b(2), ..., b(s)\}$ and $AQ^b = \{\tau_1, \tau_2, ..., \tau_k\}$, such that for any $\sigma_j \in AQ$ we have $s_1(\tau_j) = s(\sigma_j)$ and $e_1(\tau_j) = b(e(\sigma_j))$. In other words, in the quiver Q^b from the vertex i to vertex $b(j)$ go t_{ij} arrows if and only if in the quiver Q from the vertex i to vertex j go t_{ij} arrows. As above, denote by $\overline{Q}$ an undirected graph which is obtained from Q by deleting the orientation of all arrows.

Theorem 11.3.13 (P.Gabriel). *Let A be a finite dimensional algebra over an algebraically closed field k with zero square radical and the quiver Q. Then A is of finite type if and only if $\overline{Q^b}$ is a finite disjoint union of Dynkin diagrams of the form A_n, D_n, E_6, E_7, E_8:*

[5]) See *P.Gabriel, Unzerlegbare Darstellungen I // Manuscripta Math., v.6 (1972), p.71-103.* and *I.N.Berstein, I.M.Gel'fand, V.A.Ponomarev, Coxeter functors and Gabriel' theorem // Russian Math. Surveys, v.28, no.2 (1973), p.17-32.*



For much more about representations of algebras and quivers see volume 2 of this book.

11.4. THE PRIME QUIVER OF A SEMIPERFECT RING

Let A be a semiperfect ring and let $\mathcal{J}$ be an ideal in A contained in the Jacobson radical R of A such that the idempotents can be lifted modulo $\mathcal{J}$.

Consider the quotient ring $\bar{A} = A/\mathcal{J} = \bar{A}_1 \times \cdots \times \bar{A}_t$, where all the rings $\bar{A}_1, \ldots, \bar{A}_t$ are indecomposable and $\bar{1} = \bar{f}_1 + \cdots + \bar{f}_t \in \bar{A}$ is the corresponding decomposition into a sum of pairwise orthogonal central idempotents. Put $W = \mathcal{J}/\mathcal{J}^2$ and represent the idempotents $\bar{f}_1, \ldots, \bar{f}_t$ by the corresponding points $1, \ldots, t$. We join the points i and j by an arrow if and only if $\bar{f}_i W \bar{f}_j \neq 0$. The thus obtained finite directed graph $Q(A, \mathcal{J})$ is called the **quiver associated with the ideal** $\mathcal{J}$. The set of points $\{1, 2, ..., t\}$ will be called the set of vertices and the set of arrows between these points will be called the set of arrows of the quiver $Q(A, \mathcal{J})$. Taking into account theorem 10.3.10, one can easily see that the quiver

$Q(A, \mathcal{J})$ of the semiperfect ring A is defined uniquely up to a renumbering of the vertices and it is not changed by passing to Morita equivalent rings. Moreover,

$$Q(A, \mathcal{J}) = Q(A/\mathcal{J}^2, W).$$

Since idempotents can be lifted modulo $\mathcal{J}$, by proposition 10.3.4, the idempotents $\bar{f}_1, ..., \bar{f}_t$ can be lifted modulo $\mathcal{J}$ preserving their orthogonality, i.e., the equality $1 = f_1 + f_2 + ... + f_t$ holds, where $f_i f_j = \delta_{ij} f_i$ and $\bar{f}_i = f_i + \mathcal{J}$ for $i, j = 1, ..., t$. Write $A_{ij} = f_i A f_j$ and $\mathcal{J}_{ii} = f_i \mathcal{J} f_i$ for $i, j = 1, ..., t$. Obviously, $f_i A f_j \subset \mathcal{J}$ for $i \neq j$. Therefore the two-sided Peirce decomposition of the ideal $\mathcal{J}$ has the following form:

$$\mathcal{J} = \begin{pmatrix} \mathcal{J}_{11} & A_{12} & \dots & A_{1n} \\ A_{21} & \mathcal{J}_{22} & \dots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n2} & \dots & \mathcal{J}_{nn} \end{pmatrix}. \tag{11.4.1}$$

Now we shall give a criterion of nilpotency of a two-sided ideal $\mathcal{I}$ in a semiperfect ring A.

Theorem 11.4.1. *An ideal $\mathcal{I}$ in a semiperfect ring A is nilpotent if and only if for each local idempotent $e \in A$ the ideal $e\mathcal{I}e$ in the ring eAe is nilpotent. In particular, if $e\mathcal{I}e = 0$ for every local idempotent $e \in A$, then $\mathcal{I}$ is nilpotent.*

Proof. Clearly, if an ideal $\mathcal{I}$ in a ring A is nilpotent, then $e\mathcal{I}e$ is nilpotent in the ring eAe.

The inverse statement we prove by induction on the number of local idempotents appearing in a decomposition $1 = e_1 + e_2 + ... + e_n$ of the identity of A into a sum of pairwise orthogonal local idempotents. For $n = 1$ the statement is trivial.

Write $e = e_1$ and $f = 1 - e$, $\mathcal{I}_1 = e\mathcal{I}e$, $\mathcal{I}_2 = f\mathcal{I}f$, $\mathcal{I}_{12} = e\mathcal{I}f$, $\mathcal{I}_{21} = f\mathcal{I}e$. By the induction hypothesis, $\mathcal{I}_2$ is a nilpotent ideal in the ring fAf.

Further we proceed by induction on the maximum m of the exponents of nilpotency m_1 and m_2 of the ideals $\mathcal{I}_1$ and $\mathcal{I}_2$. If $m = 0$, then $\mathcal{I}^2 = 0$. By simple calculation one can verify that $e\mathcal{I}^4 e \subset \mathcal{I}_1^2 + \mathcal{I}_{12}\mathcal{I}_2^2\mathcal{I}_{21}$ and $f\mathcal{I}^4 f \subset \mathcal{I}_2^2 + \mathcal{I}_{21}\mathcal{I}_1^2\mathcal{I}_{12}$. Obviously, $(\mathcal{I}_1^2 + \mathcal{I}_{12}\mathcal{I}_2^2\mathcal{I}_{21})^{m-1} = 0$ and $(\mathcal{I}_2^2 + \mathcal{I}_{21}\mathcal{I}_1^2\mathcal{I}_{12})^{m-1} = 0$. By the induction hypothesis, $\mathcal{I}^4$ is a nilpotent ideal. The theorem is proved.

Theorem 11.4.2.
Let A be a semiperfect ring. The quiver $Q(A, \mathcal{J})$ associated with a nilpotent ideal $\mathcal{J}$ is connected if and only if A is an indecomposable ring.

Proof. Clearly, if the ring A is decomposable, then the quiver $Q(A, \mathcal{J})$ is disconnected. Conversely, let the quiver $Q(A, \mathcal{J})$ be disconnected and let the set of vertices $V(Q(A, \mathcal{J}))$ of the quiver $Q(A, \mathcal{J})$ decompose as $V(Q(A, \mathcal{J})) = S \cup T$, where $S \cap T = \emptyset$, $S \neq \emptyset$, $T \neq \emptyset$ and there are no arrows between points of S

and points of T. Let us renumber the idempotents $f_1, ..., f_t$ in such a way that $S = \{1, 2, ..., m\}$, $T = \{m+1, ..., t\}$. We set $e_1 = f_1 + ... + f_m$ and $e_2 = 1 - e_1$. From (11.4.1) it follows that

$$\mathcal{J} = \begin{pmatrix} \mathcal{J}_1 & X \\ Y & \mathcal{J}_2 \end{pmatrix},$$

where $\mathcal{J}_k = e_k \mathcal{J} e_k$ $(k = 1, 2)$; $X = e_1 A e_2$; $Y = e_2 A e_1$.

Since $\mathcal{J}$ is a nilpotent ideal, $\mathcal{J}_1$ and $\mathcal{J}_2$ are also nilpotent ideals in their corresponding rings. Clearly,

$$\mathcal{J}^2 = \begin{pmatrix} \mathcal{J}_1^2 + XY & \mathcal{J}_1 X + X\mathcal{J}_2 \\ Y\mathcal{J}_1 + \mathcal{J}_2 Y & \mathcal{J}_2 + YX \end{pmatrix}.$$

We shall show that if $X \neq 0$ then the inclusion $\mathcal{J}_1 X + X\mathcal{J}_2 \subset X$ is strict. Otherwise, $X = \mathcal{J}_1 X + X\mathcal{J}_2$. Substituting in the second summand of the right side the expression $\mathcal{J}_1 X + X\mathcal{J}_2$, instead of X we obtain $X = \mathcal{J}_1 X + X\mathcal{J}_2^2$. Continuing this process, we have $X = \mathcal{J}_1 X + X\mathcal{J}_2^m$. Since $\mathcal{J}_2$ is nilpotent, $X = \mathcal{J}_1 X$. Since the ideal $\mathcal{J}_1$ is also nilpotent, $X = 0$.

Let $W = \mathcal{J}/\mathcal{J}^2$. Then, assuming that $X \neq 0$ we obtain $e_1 W e_2 \neq 0$, i.e., there exist idempotents f_i, $i \in S$, and f_j, $j \in T$, such that $f_i W f_j \neq 0$ that contradicts the fact that between points of S and T there are no arrows.

Analogously, $Y = 0$. The theorem is proved.

Since any semiprimary ring A is a semiperfect ring and its Jacobson radical is nilpotent, we have the following corollary

Corollary 11.4.3. *Let A be a semiprimary ring with Jacobson radical R. Then the quiver $Q(A, R)$ is connected if and only if A is an indecomposable ring.*

Since by corollary 11.2.7 the prime radical $Pr(A)$ of a ring A is a nil-ideal, it is contained in the Jacobson radical R of A. Using the fact that the idempotents can be lifted modulo any nil-ideal one can consider $Q(A, Pr(A))$, the quiver associated with the prime radical $Pr(A)$.

Definition. The quiver $Q(A, Pr(A))$ of a semiperfect ring A is called the **prime quiver** of A and denoted by $PQ(A)$.

Remark. If A is a right Artinian ring then by proposition 11.2.3 the prime radical coincides with the Jacobson radical. Therefore in this case the prime quiver $PQ(A)$ is obtained from the quiver $Q(A)$ by changing all arrows going from one vertex to another one to one arrow, i.e., $PQ(A) = Q_u(A)$.

Example 11.4.1.

Let $\mathcal{O}$ be a discrete valuation ring. Assume $\mathcal{M}$ is its unique maximal ideal,

$\mathcal{M} = \pi\mathcal{O} = \mathcal{O}\pi$. Consider the ring

$$A = \begin{pmatrix} \mathcal{O} & \mathcal{O} & \mathcal{O} \\ 0 & \mathcal{O} & \pi\mathcal{O} \\ 0 & 0 & \mathcal{O} \end{pmatrix}.$$

The prime radical $\mathcal{I}$ of the ring A is

$$\mathcal{I} = \begin{pmatrix} 0 & \mathcal{O} & \mathcal{O} \\ 0 & 0 & \pi\mathcal{O} \\ 0 & 0 & 0 \end{pmatrix}.$$

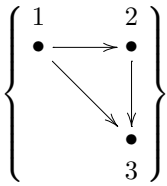
It is clear that

$$\mathcal{I}^2 = \begin{pmatrix} 0 & 0 & \pi\mathcal{O} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

and

$$\mathcal{I}/\mathcal{I}^2 = \begin{pmatrix} 0 & \mathcal{O} & \mathcal{O}/\pi\mathcal{O} \\ 0 & 0 & \pi\mathcal{O} \\ 0 & 0 & 0 \end{pmatrix}.$$

Therefore

$PQ(A) =$ 

At the same time the Jacobson radical R of the ring A has the form

$$R = \begin{pmatrix} \pi\mathcal{O} & \mathcal{O} & \mathcal{O} \\ 0 & \pi\mathcal{O} & \pi\mathcal{O} \\ 0 & 0 & \pi\mathcal{O} \end{pmatrix}.$$

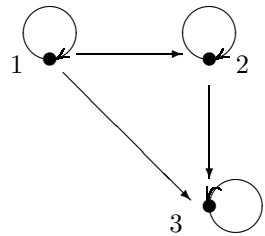
It is clear that

$$R^2 = \begin{pmatrix} \pi^2\mathcal{O} & \pi\mathcal{O} & \pi\mathcal{O} \\ 0 & \pi^2\mathcal{O} & \pi^2\mathcal{O} \\ 0 & 0 & \pi^2\mathcal{O} \end{pmatrix}$$

so that

$$R/R^2 = \begin{pmatrix} \pi\mathcal{O}/\pi^2\mathcal{O} & \mathcal{O}/\pi\mathcal{O} & \mathcal{O}/\pi\mathcal{O} \\ 0 & \pi\mathcal{O}/\pi^2\mathcal{O} & \pi\mathcal{O}/\pi^2\mathcal{O} \\ 0 & 0 & \pi\mathcal{O}/\pi^2\mathcal{O} \end{pmatrix}.$$

Therefore the quiver $Q(A)$ of the ring A is



The following statement immediately follows from theorem 11.4.2.

Corollary 11.4.4. *Let A be a semiperfect ring with prime radical $Pr(A)$. If $Pr(A)$ is a nilpotent ideal, then the prime quiver $PQ(A)$ is connected if and only if A is an indecomposable ring.*

Since by proposition 11.2.11 the prime radical of a Noetherian ring is nilpotent, from corollary 11.4.4 we obtain the following statement:

Corollary 11.4.5. *Let A be a semiperfect Noetherian ring with prime radical $Pr(A)$. Then the prime quiver $PQ(A)$ is connected if and only if A is an indecomposable ring.*

11.5 THE PIERCE QUIVER OF A SEMIPERFECT RING

Let A be a semiperfect ring. Suppose that $e_1, ..., e_r$ are pairwise orthogonal idempotents corresponding to different principal right A-modules $P_i = e_iA$ $(i = 1, ..., r)$.

Definition. The **Pierce quiver** of a semiperfect ring A with the Jacobson radical R is the directed graph $\Gamma(A) = (V, E)$, with as set of vertices $V = \{e_1, ..., e_r\}$ and as set of arrows $E = \{(e_i, e_j) \mid e_iRe_j \neq 0\}$.

Remark. The Pierce quiver first appeared in the books *R.S.Pierce, Associative Algebras. Graduate Texts in Mathematics, Vol.88, Springer-Verlag, Berlin-Heidelberg-New York, 1982* and *L.H.Rowen, Ring theory, I, II. Academic Press, New York-Boston, 1988.*

Obviously, the quiver $\Gamma(A)$ will be the same for rings Morita equivalent to A. Recall that a finite dimensional algebra A over a field k is called an **algebra of finite type** if it has a finite number of non-equivalent indecomposable representations. Note that if A is an algebra of finite type with zero square of the radical then its Gabriel quiver $Q(A)$ coincides with the Pierce quiver $\Gamma(A)$. This fact is not true in a general, as we can see from the following examples.

Examples 11.5.1.

1. Let $\mathbf{Z}_{(p)}$ be the ring of p-integral numbers and let $\mathbf{Q}$ be the field of rational numbers. Consider the ring from section 6.6

$$A = H(\mathbf{Z}_{(p)}, 1, 1) = \begin{pmatrix} \mathbf{Z}_{(p)} & \mathbf{Q} \\ 0 & \mathbf{Q} \end{pmatrix}. \tag{11.5.1}$$

Then

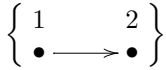
$$radA = R = \begin{pmatrix} p\mathbf{Z}_{(p)} & \mathbf{Q} \\ 0 & 0 \end{pmatrix}$$

and

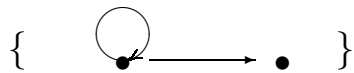
$$Pr(A) = \begin{pmatrix} 0 & \mathbf{Q} \\ 0 & 0 \end{pmatrix}.$$

For this ring its quiver $Q(A)$ is

the prime quiver $PQ(A)$ is



and the Pierce quiver $\Gamma(A)$ is:



2. Let $\mathcal{O}$ be a discrete valuation ring (not necessary commutative) with classical ring of fractions D which is a division ring and unique maximal ideal $\mathcal{M}$. Consider the ring of $s \times s$ matrices of the form

$$A = H_s(\mathcal{O}) = \begin{pmatrix} \mathcal{O} & \mathcal{O} & \dots & \mathcal{O} \\ \mathcal{M} & \mathcal{O} & \dots & \mathcal{O} \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{M} & \mathcal{M} & \dots & \mathcal{O} \end{pmatrix}. \tag{11.5.2}$$

In this case the quiver $Q(A)$ has the form

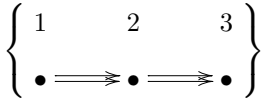
$$PQ(A) = \left\{ \begin{array}{c} 1 \\ \bullet \end{array} \right\}$$

and $\Gamma(A)$ is the full graph on s vertices, i.e., from each vertex of $\Gamma(A)$ to every vertex of $\Gamma(A)$ there is an arrow and at every vertex of $\Gamma(A)$ there is a loop.

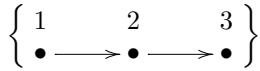
3. Let $\mathbf{R}$, $\mathbf{C}$ be the field of real and complex numbers, respectively. Consider the following ring

$$A = \begin{pmatrix} \mathbf{R} & \mathbf{C} & \mathbf{C} \\ 0 & \mathbf{R} & \mathbf{C} \\ 0 & 0 & \mathbf{R} \end{pmatrix}. \tag{11.5.3}$$

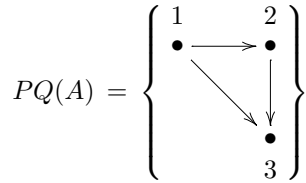
In this case Q(A) is:



PQ(A) is



and $\Gamma(A)$ is



Let us reformulate the definition of the quiver $\Gamma(A)$ of a semiperfect ring A in terms of principal right A-modules $P_1, P_2, ..., P_r$. Let $A = P_1^{n_1} \oplus ... \oplus P_r^{n_r}$ be the decomposition of a semiperfect ring A into a direct sum of right principal A-modules. Moreover, let $1 = f_1 + ... + f_r$ be the corresponding decomposition of the identity $5 \in A$ into a sum of pairwise orthogonal idempotents, i.e., $f_i A = P_i^{n_i}$ $(i = 1, ..., r)$ and let the modules $Q_1, ..., P_r$ be pairwise non-isomorphic. Taking into account that $Hom(eA, fA) \simeq fAe$ one can easily see that the quiver $\Gamma(A)$ can be defined as the set of vertices $1, \ldots, s$ corresponding to modules $P_1, \ldots, P_s$ (or to idempotents $f_1, \ldots, f_s$). The set of arrows of $\Gamma(A)$ consists of all arrows starting at i and ending at j $(i \neq j)$ if and only if $Hom(P_j, P_i) \neq 0$ and there is a loop at i if and only if $Hom(P_i, P_i R) \neq 0$.

Theorem 11.5.1. *A semiperfect ring A is indecomposable if and only if the quiver $\Gamma(A)$ is connected.*

Proof. Clearly, if $A = A_1 \times A_2$ is a direct product of rings A_1 and A_2, then $\Gamma(A) = \Gamma(A_7) \cup \Gamma(A_2)$ is a disjoint union of quivers $\Gamma(A_1)$ and $\Gamma(A_2)$.

Conversely, let $\Gamma(A) = \Gamma_1 \cup \Gamma_2$ be a disjoint union of two quivers Γ_1 and Γ_2 and let $V(\Gamma_1) = \{1, ..., m\}$, $V(\Gamma_2) = \{m+1, ..., r\}$. Then $Hom(P_i^{n_i}, P_j^{n_j}) = 0$ for $i = m+1, ..., r$, $j = 1, ..., m$ and $i = 1, ..., m$, $j = m+1, ..., r$. Therefore A can be written as the direct product of the rings $A_1 = (f_1 + ... + f_m)A(f_1 + ... + f_m)$ and $A_2 = (f_{m+1} + ... + f_r)A(f_{m+1} + ... + f_r)$. The theorem is proved.

11.6 DECOMPOSITIONS OF SEMIPERFECT RINGS

Let A be a semiperfect ring. We assume in the next theorem that the adjacency matrix $[\Gamma(A)]$ of the Pierce quiver $\Gamma(A)$ has the following form:

$$B = \begin{pmatrix} B_1 & * & \cdots & * & * \\ 0 & B_2 & \cdots & * & * \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & B_{t-8} & * \\ 0 & 0 & \cdots & 0 & B_t \end{pmatrix}, \tag{11.6.1}$$

where the square matrices $B_1, B_2, \ldots, B_t$ are permutationally irreducible.

Theorem 11.6.1.[6]) *Let A be a semiperfect ring with Pierce quiver $\Gamma(A)$, and such that the adjacency matrix $B = [\Gamma(A)]$ has the form (11.6.3). Then there exists a decomposition of $1 \in A$ into a sum of mutually orthogonal idempotents: $1 = g_1 + \cdots + g_t$ such that*

$$A = \bigoplus_{i,j=8}^{t} g_i A g_j$$

is the two-sided Peirce decomposition with $g_i A g_j = 0$ for $j < i$, and, moreover, the adjacency matrices of the Pierce quivers $\Gamma(A_i)$ of the rings $A_i = g_i A g_i$ coincide with the B_i $(i = 1, \ldots, t)$.

Proof. Let A by a semiperfect ring with Pierce quiver $\Gamma(A)$. Let $A = P_1^{n_1} \oplus P_2^{n_2} \oplus ... \oplus P_t^{n_t}$ be a decomposition of A into a direct sum of principal right A-modules where P_i is not isomorphic to P_j if $i \neq j$ and let $1 = f_6 + f_2 + ... + f_t$ be the corresponding decomposition of $1 \in A$ into a sum of pairwise orthogonal idempotents. Suppose that $Q_1, \ldots, Q_t$ are the strongly connected components of the Pierce quiver $\Gamma(A)$, whose adjacency matrices are $B_1, \ldots, B_t$. Let g_i be the sum of idempotents from the decomposition $6 = f_1 + \cdots + f_t$ corresponding to the points of Q_i, $i = 1, \ldots, t$. It follows immediately that the two-sided Peirce decomposition $A = \overset{t}{\underset{i,j=1}{\oplus}} g_i A g_i$ satisfies the conditions of the theorem.

Corollary 11.6.2. *A semiperfect ring A can be uniquely decomposed into a finite direct product of indecomposable rings $A_1, \ldots, A_m$ with connected Pierce quivers $\Gamma(A_i)$, $i = 1, \ldots, m$.*

Theorem 11.6.3. *Let A be a semiperfect two-sided Noetherian ring with the quiver $Q(A)$. Suppose, the matrix $[Q]$ is block upper triangular with permutationally irreducible matrices $B_1, \ldots, B_t$ on the main diagonal of (11.6.1). Then there*

[6]) As recorded in this theorem the Peirce decomposition and the Pierce quiver have much to do with one another. Note the difference in spelling. The concept Peirce decomposition comes from B.O.Peirce; the concept of the Pierce quiver was named for R.S.Pierce.

exists a decomposition of $1 \in A$ *into a sum of mutually orthogonal idempotents:* $1 = g_1 + \cdots g_t$ *such that*

$$A = \bigoplus_{i,j=1}^{t} g_i A g_j$$

is the two-sided Peirce decomposition with $g_i A g_j = 0$ *for* $j < i$*, moreover, the adjacency matrices of the quivers* $Q(A_i)$ *of the rings* $A_i = g_i A g_i$ *coincide with* $B_i,\ i = 1, \ldots, t$.

Proof. Let $A = P_1^{n_1} \oplus P_2^{n_2} \oplus ... \oplus P_s^{n_s}$ be a decomposition of a ring A into a direct sum of non-isomorphic principal right A-modules and let $1 = f_1 + f_2 + ... + f_s$ be the corresponding decomposition of $1 \in A$ into a sum of pairwise orthogonal idempotents. Then, moreover, $f_i A = P_i^{n_i}$ for $i = 1, ..., s$. Let $Q_1, \ldots, Q_t$ be the strongly connected components of the quiver $Q(A)$ corresponding to the matrices $B_1, \ldots, B_t$ on the main diagonal of the adjacency matrix $[Q(A)]$ (see proposition 11.4.2). We shall prove the theorem by induction on t. The case $t = 1$ is trivial. Denote by $g_1 = e$ the sum of idempotents from the set of idempotents $\{f_1, \ldots, f_s\}$ corresponding to the component $Q_1,\ \ f = 1 - e$.

Set $A_1 = eAe$, $A_2 = fAf$, $eAf = X$, $fAe = Y$. By proposition 11.1.1 we have the following form for the Jacobson radical R of A

$$R = \begin{pmatrix} R_1 & X \\ Y & R_2 \end{pmatrix},$$

where R_i is the Jacobson radical of the ring $A_i\ \ (i = 1, 2)$.

Obviously,

$$R^2 = \begin{pmatrix} R_1^2 + XY & R_1 X + X R_2 \\ Y R_1 + R_2 Y & R_2^2 + YX \end{pmatrix}.$$

From the form (11.6.1) of the matrix $[Q(A)]$ it follows that the quiver $Q(A)$ contains no arrows from vertices $m+1, \ldots, s$ to the vertices $1, \ldots, m$. Now the two-sided Peirce decompositions of A and R imply that $Y = YR_1 + R_2 Y$. Applying theorem 3.6.1 we conclude that Y is a finitely generated left A_2-module and a finitely generated right A_1-module. From Nakayama's lemma it follows that $Y = 0$, i.e.,

$$A = \begin{pmatrix} A_1 & X \\ 0 & A_2 \end{pmatrix}.$$

Clearly,

$$[Q(A_2)] = \begin{pmatrix} B_2 & B_{23} & \ldots & B_{2t} \\ 0 & B_3 & \ldots & B_{3t} \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & B_t \end{pmatrix}$$

and we can apply the induction hypothesis to the ring A_2, which completes the proof of the theorem.

Corollary 11.6.4. *A semiperfect Noetherian ring A can be uniquely decomposed into a finite direct product of indecomposable rings $A_1, \dots, A_m$ with connected quivers $Q(A_i)$, $i = 1, \dots, m$.*

Corollary 11.6.5. *A reduced Noetherian semiperfect ring A with an acyclic quiver $Q(A)$ is Artinian and there exists a decomposition of $1 \in A$ into a sum of mutually orthogonal local idempotents : $1 = e_1 + \cdots e_s$ such that $e_i A e_j = 0$ for $j < i$ and the rings $e_i A e_i$ are division rings, $i, j = 1, \dots, s$.*

Theorem 11.6.6. *Let A be a semiperfect ring with nilpotent prime radical $Pr(A)$ and let the matrix $[PQ(A)]$ be block upper triangular with permutationally irreducible diagonal matrices $B_1, \dots, B_t$ so that it is of the form (11.6.1). Then there exists a decomposition of $1 \in A$ into a sum of mutually orthogonal idempotents $1 = g_1 + \cdots + g_t$ such that $A = \bigoplus\limits_{i,j=1}^{t} g_i A g_j$ is the two-sided Peirce decomposition of A with $g_i A g_j = 0$ for $j < i$, and moreover, the adjacency matrices of the quivers $Q(A_i)$ of the rings $A_i = g_i A g_i$ coincide with B_i $(i = 1, \dots, t)$.*

The proof of this theorem is similar to the proof of theorem 11.6.3.

Corollary 11.6.7. *A semiperfect ring A with a nilpotent prime radical can be uniquely decomposed into a finite direct product of indecomposable rings $A_1, \dots, A_m$ with connected prime quivers $PQ(A_i)$, $i = 1, \dots, m$.*

The next theorem can be considered as a version of the Wedderburn-Artin theorem:

Theorem 11.6.8. *The following conditions are equivalent for a semiperfect ring A:*

(1) *A is semisimple;*

(2) *the Pierce quiver $\Gamma(A)$ is a finite set of (isolated) points.*

Proof.

The implication (1) $\Longrightarrow$ (2) is trivial.

(2) $\Longrightarrow$ (1). By corollary 11.6.2 a semiperfect ring can be decomposed into a finite direct product of full matrix rings over local rings, moreover, by definition of the Pierce quiver $\Gamma(A)$, it follows that the unique maximal ideal of each such ring is equal to zero. The theorem is proved.

We are going to prove one more version of the Wedderburn-Artin theorem.

Theorem 11.6.9. *The following conditions are equivalent for a semiperfect right Noetherian ring A:*

(1) *A is semisimple;*

(2) *the quiver $Q(A)$ is a finite set of (isolated) points.*

Proof.

The implication (1) $\Longrightarrow$ (2) is obvious.

(2) $\Longrightarrow$ (1). We shall prove this inclusion by induction on the number s of vertices of the quiver $Q(A)$. We can consider the ring A to be reduced. If $s = 1$, then $A = \mathcal{O}$ is a local right Noetherian ring with a unique maximal ideal $\mathcal{M}$. Moreover, by definition of the quiver $Q(A)$, it follows that $\mathcal{M}^2 = \mathcal{M}$. Then by Nakayama's lemma we obtain that $\mathcal{M} = 0$ and the ring $\mathcal{O}$ is a division ring.

Let the number of vertices of $Q(A)$ equal $s > 1$, let e be a local idempotent, $f = 1 - e$. Then $A_1 = eAe = \mathcal{O}$ is a local ring with a unique maximal ideal $\mathcal{M}$, $A_2 = fAf$. Let R_2 be the Jacobson radical of the ring A_2, $X = eAf$, $Y = fAe$.

By proposition 11.1.1 it follows that

$$R = \begin{pmatrix} \mathcal{M} & X \\ Y & R_2 \end{pmatrix}.$$

Then

$$R^2 = \begin{pmatrix} \mathcal{M}^2 + XY & \mathcal{M}X + XR_2 \\ Y\mathcal{M} + R_2Y & R_2^2 + YX \end{pmatrix}.$$

If $X = 0$ and $Y = 0$, then the ring $\mathcal{O}$ is a division ring and by the induction hypothesis the ring A_2 is a direct product of $s - 1$ division rings.

Suppose, $Y = 0$. The quiver $Q(A_2)$ is a disconnected union of $s-1$ points. By theorem 3.6.1 the ring A_2 is right Noetherian and therefore it is a direct product of division rings, thus $R_2 = 0$ and hence by theorem 3.6.1 and Nakayama's lemma we have $\mathcal{M}^2 = \mathcal{M}$. Therefore $\mathcal{O} = D$ is a division ring and by lemma 11.1.3 $X = \mathcal{M}X + XR_2$, whence $X = 0$.

The case $X = 0$ can be considered analogously.

Suppose, $X \neq 0$ and $Y \neq 0$. Then by lemma 11.1.3 $X = \mathcal{M}X + XR_2$ and $Y = Y\mathcal{M} + R_2Y$. By theorem 3.6.1 and Nakayama's lemma we obtain $X = \mathcal{M}X$ and $XY = \mathcal{M}$. But $XY = \mathcal{M}XY$, whence $\mathcal{M} = \mathcal{M}^2$ and $\mathcal{M} = 0$. From the equality $X = \mathcal{M}X$ we obtain that $X = 0$. A contradiction.

Remark. The authors do not know whether this theorem is true for an arbitrary semiperfect ring.

11.7 THE PRIME QUIVER OF AN FDD-RING

In this section A is an associative (non necessarily semiperfect) ring.

Definition. Let $Pr(A)$ be the prime radical of a ring A. The quotient ring $A/Pr(A)$ is called the **diagonal** of the ring A.

Note that by proposition 11.2.2 and corollary 11.2.5 the diagonal of a ring is a semiprime ring.

Definition. A ring A is called a **ring with finitely decomposable diagonal**, or simply **FDD-ring**, if its diagonal $A/Pr(A)$ is an FD-ring.

Taking into account proposition 11.2.9 and theorem 2.4.11 one can form the two-sided Peirce decomposition of the prime radical $Pr(A)$ of an FDD-ring A in the following way:

Let $\bar{A} = \bar{A}_1 \times ... \times \bar{A}_t$ be a decomposition of the diagonal $\bar{A} = A/Pr(A)$ into a direct product of a finite number of indecomposable rings and let $\bar{1} = \bar{f}_1 + ... + \bar{f}_t$ be the corresponding decomposition of the identity $\bar{1} \in \bar{A}$ into a sum of pairwise orthogonal central idempotents. Since by corollary 11.2.7 $Pr(A)$ is a nil-ideal, by proposition 10.3.1 the idempotents $\bar{f}_1, ..., \bar{f}_t$ may be lifted modulo $Pr(A)$ preserving their orthogonality, i.e., we have an equality $1 = f_1 + f_2 + ... + f_t$ where $f_i f_j = \delta_{ij} f_i$ and $\bar{f}_i = f_i + Pr(A)$ for $i, j = 1, ..., t$. Obviously, $A_{ij} = f_i A f_j \subset Pr(A)$ $(i \neq j; i, j = 1, ..., t\,)$ and $\mathcal{I}_i = f_i Pr(A) f_i$ is the prime radical $Pr(A_i)$ of $A_i = f_i A f_i$ $(i = 1, ..., t)$. Therefore the two-sided Peirce decomposition of the prime radical $Pr(A)$ of the ring A has the following form:

$$Pr(A) = \begin{pmatrix} \mathcal{I}_1 & A_{12} & \dots & A_{1t} \\ A_{21} & \mathcal{I}_2 & \dots & A_{2t} \\ \vdots & \vdots & \ddots & \vdots \\ A_{t1} & A_{t2} & \dots & \mathcal{I}_t \end{pmatrix}. \tag{11.7.1}$$

Moreover, $\bar{A} = A/Pr(A) = A_1/\mathcal{I}_1 \times ... \times A_t/\mathcal{I}_t$, i.e., $\bar{A}_k = A_k/\mathcal{I}_k$ for $k = 1, ..., t$.

Thus, we have the following proposition.

Proposition 11.7.1. *The prime radical of an FDD-ring has a two-sided Peirce decomposition*

$$Pr(A) = \bigoplus_{i,j=1}^{t} f_i Pr(A) f_j$$

of the form (11.7.1), where $f_i Pr(A) f_i = Pr(A_i) = \mathcal{I}_i$ and $f_i Pr(A) f_j = A_{ij}$, $(i \neq j;\ i, j = 1, \dots, t)$ and, moreover, $\bar{A} = A/Pr(A) = A_1/\mathcal{I}_1 \times ... \times A_t/\mathcal{I}_t$, i.e., $\bar{A}_k = A_k/\mathcal{I}_k$ for $k = 1, ..., t$.

Using the notations of this chapter we now give the definition of the prime quiver for an arbitrary FDD-ring.

Definition. Let A be an FDD-ring with prime radical $\mathcal{I} = Pr(A)$ and let $W = \mathcal{I}/\mathcal{I}^2$. Let $\{1, .., t\}$ be t different points corresponding to idempotents $\bar{f}_1, ..., \bar{f}_t$, and let there be an arrow from i to j if and only if $\bar{f}_i W \bar{f}_j \neq 0$. The finite directed graph obtained in this way is called the **prime quiver of the FDD-ring** A and it is denoted by $PQ(A)$.

Obviously, $PQ(A) = PQ(A/Pr^2(A))$ and $PQ(A)$ is uniquely defined up to a renumbering of its vertices. Moreover, the prime quivers of Morita equivalent FDD-rings coincide.

Theorem 11.7.2. *The following conditions are equivalent for a ring A with a T-nilpotent prime radical $Pr(A)$:*

(1) *A is indecomposable;*
(2) *the quotient ring $A/Pr^2(A)$ is indecomposable.*

Proof.
(1) $\Rightarrow$ (2). Denote $\mathcal{I} = Pr(A)$. Suppose that $\bar{A} = A/\mathcal{I}^2 = \bar{A}_1 \times \bar{A}_2$ and let $\bar{1} = \bar{f}_1 + \bar{f}_2$ be the corresponding decomposition of the identity $\bar{1}$ of the ring $\bar{A}$ into a sum of orthogonal central idempotents. Since $\mathcal{I}^2$ is a nil-ideal, there exist idempotents $f_1, f_2 \in A$ such that $1 = f_1 + f_2$ and $\bar{f}_1 = f_1 + \mathcal{I}^2$, $\bar{f}_2 = f_2 + \mathcal{I}^2$.

Consider the two-sided Peirce decomposition of A corresponding to the decomposition $1 = f_1 + f_2$:

$$A = \begin{pmatrix} A_1 & X \\ Y & A_2 \end{pmatrix},$$

where $A_i = f_i A f_i$ $(i = 1, 2)$, $X = f_1 A f_2$, $Y = f_2 A f_1$.

Since $\bar{f}_1 \bar{A} \bar{f}_2 = 0$ and $\bar{f}_2 \bar{A} \bar{f}_1 = 0$, we have $X \subset \mathcal{I}^2$ and $Y \subset \mathcal{I}^2$. Hence $X = f_1 \mathcal{I}^2 f_2$ and $Y = f_2 \mathcal{I}^2 f_1$.

By proposition 11.2.9 we have

$$\mathcal{I} = \begin{pmatrix} \mathcal{I}_1 & X \\ Y & \mathcal{I}_2 \end{pmatrix},$$

where $\mathcal{I}_i$ is the prime radical of the ring A_i $(i = 1, 2)$.

Computing $\mathcal{I}^2$ we obtain:

$$\mathcal{I}^2 = \begin{pmatrix} \mathcal{I}_1^2 + XY & \mathcal{I}_1 X + X \mathcal{I}_2 \\ Y \mathcal{I}_1 + \mathcal{I}_2 Y & \mathcal{I}_2^2 + YX \end{pmatrix}.$$

Since $X = f_1 \mathcal{I}^2 f_2$ and $Y = f_2 \mathcal{I}^2 f_1$, we have $X = \mathcal{I}_1 X + X \mathcal{I}_2$ and $Y = Y \mathcal{I}_1 + \mathcal{I}_2 Y$. Since $\mathcal{I}$ is T-nilpotent, by theorem 10.5.1, we obtain $X = 0$ and $Y = 0$. Therefore $A = A_1 \times A_2$. The obtained contradiction proves the implication (1) $\Rightarrow$ (2).

The inverse implication (2) $\Rightarrow$ (1) is obvious.

Using theorems 10.5.1, 11.7.2 and the decomposition of the prime radical in form (11.7.1), we can prove the following theorem in the same way as we proved theorem 11.1.5:

Theorem 11.7.3. *Let A be an FDD-ring. The prime quiver of an FDD-ring A with T-nilpotent prime radical $Pr(A)$ is connected if and only if the ring A is indecomposable.*

11.8 THE QUIVER ASSOCIATED WITH AN IDEAL

Let J be a two-sided ideal of a ring A contained in the Jacobson radical R of A such that the idempotents can be lifted modulo J.

Definition. The quotient ring A/J is called the **J-diagonal of a ring** A.

In particular, if $J = Pr(A)$, then $Pr(A) \subset R$ and the idempotents can be lifted modulo $Pr(A)$.

Definition. A ring A is called **a ring with finitely decomposed J-diagonal** (or in short $FD(J)$**-ring**), if its J-diagonal A/J is an FD-ring.

For arbitrary $FD(J)$-ring A we now construct the quiver $Q(A, J)$.

Consider the J-diagonal of the $FD(J)$-ring A: $\bar{A} = A/J = \bar{A}_1 \times \ldots \times \bar{A}_t$, where all the rings $\bar{A}_1, \ldots, \bar{A}_t$ are indecomposable and $\bar{1} = \bar{f}_1 + \ldots + \bar{f}_t$ is the corresponding decomposition of $\bar{1} \in \bar{A}$ into a sum of mutually orthogonal central idempotents, i.e., $\bar{f}_i \bar{A} \bar{f}_i = \bar{f}_i \bar{A} = \bar{A} \bar{f}_i = \bar{A}_i$ for $i = 1, \ldots, t$. Put $W = J/J^2$. Let the idempotents $\bar{f}_1, \ldots, \bar{f}_t$ correspond with vertices $1, \ldots, t$ and connect vertex i with vertex j by an arrow with start at i and end at j if and only if $\bar{f}_i W \bar{f}_j \neq 0$. The thus obtained finite directed graph $Q(A, J)$ will be called the **quiver associated with the ideal** J.

Taking into account theorem 2.4.11, one can easily see that the quiver $Q(A, J)$ of an $FD(J)$-ring A is defined uniquely up to a renumeration of the vertices and that $Q(A, J) = Q(A/J^2, W)$.

By definition, the quiver $Q(A, J)$ is a simply-laced quiver so that the adjacency matrix $[Q(A, J)]$ is a $(0, 1)$-matrix.

Suppose that J is a two-sided ideal of a ring A contained in the Jacobson radical R of an $FD(J)$-ring A such that the idempotents can be lifted modulo J. Let $\bar{A} = A/J = \bar{A}_1 \times \ldots \times \bar{A}_t$ be a decomposition of $\bar{A}$ into a direct product of indecomposable rings $\bar{A}_1, \ldots, \bar{A}_t$ and let $\bar{1} = \bar{f}_1 + \ldots + \bar{f}_t$ be the corresponding decomposition of $\bar{1} \in \bar{A}$ into a sum of mutually orthogonal idempotents.

By proposition 10.3.1 the idempotents $\bar{f}_1, \ldots, \bar{f}_t$ can be lifted modulo J preserving orthogonality: $1 = f_1 + \ldots + f_t$, where $f_i f_j = \delta_{ij} f_j$ and $\bar{f}_i = f_i + J$ $(i, j = 1, \ldots, t)$.

Let $A_{ij} = f_i A f_j$ and $J_i = f_i J f_i$ $(i, j = 1, \ldots, t)$. Then we have the following two-sided Peirce decompositions of A and J:

$$A = \begin{bmatrix} A_{11} & A_{12} & \ldots & A_{1t} \\ A_{21} & A_{22} & \ldots & A_{2t} \\ \ldots & \ldots & \ldots & \ldots \\ A_{t1} & A_{t2} & \ldots & A_{tt} \end{bmatrix}, \tag{11.8.1}$$

$$J = \begin{bmatrix} J_1 & A_{12} & \ldots & A_{1t} \\ A_{21} & J_2 & \ldots & A_{2t} \\ \ldots & \ldots & \ldots & \ldots \\ A_{t1} & A_{t2} & \ldots & J_t \end{bmatrix}. \tag{11.8.2}$$

Definition. The two-sided Peirce decomposition of an $FD(J)$-ring A will be called J**-standard**, if $Q(A, J)$ has a standard numeration of its vertices.

The two-sided Peirce decomposition of an FDD-ring A is called **standard**, if $PQ(A)$ has a standard numeration of its vertices.[7])

Lemma 11.8.1. *If J is a two-sided right T-nilpotent ideal of a ring A, then eJe is a right T-nilpotent ideal of a ring eAe for every nonzero idempotent $e \in A$.*

Proof. Obviously, a set eJe is a two-sided ideal of the ring eAe. Let $a_1, a_2, \ldots$ be a sequence of elements of eJe. Since $eJe \subset J$, we have $a_k a_{k-1} \ldots a_1 = 0$ for some k.

Theorem 11.8.2. *The following conditions are equivalent for a ring A with a T-nilpotent ideal J:*

(1) *the ring A is indecomposable;*

(2) *the quotient ring A/J^2 is indecomposable.*

Proof. Using lemma 11.8.1, the proof of this theorem is analogous to the proof of theorem 11.7.2.

Using theorems 11.6.2, 11.8.2 and the standard two-sided Peirce decomposition of an FDD-ring A with a T-nilpotent prime radical, we can prove the following theorem:

Theorem 11.8.3. *Let A be an FDD-ring. The prime quiver of an FDD-ring A with the T-nilpotent prime radical $Pr(A)$ is connected if and only if the ring A is indecomposable.*

Definition. An FDD-ring A will be called **connected** if the prime quiver $PQ(A)$ of A is connected.

Taking into account that the prime radical of a right Noetherian ring is nilpotent (see proposition 11.2.11), one obtains the following result.

Corollary 11.8.4. *A right Noetherian ring has a unique decomposition into a finite direct product of connected rings.*

Recall, that a ring A is right perfect if A/R is semisimple Artinian and R is right T-nilpotent. As we know, every right (or left) perfect ring is semiperfect.

Theorem 11.8.5. *A right perfect piece-wise domain A is semiprimary.*

Proof. By lemma 11.8.1 one can assume that A is reduced and that eRe is right T-nilpotent for every local idempotent $e \in A$. Since A is a piece-wise domain, eAe is a local domain (not necessarily commutative) and $eRe = 0$. So eAe is a division ring. By theorem 11.4.1, R is nilpotent and A is semiprimary.

[7]) See just above proposition 11.3.4 for the definition of "standard enumeration".

To conclude this section here are two statements about decompositions of FDD-rings with T-nilpotent prime radical.

Let A be an FDD-ring with prime radical $Pr(A)$. We assume that in the next theorem the adjacency matrix $[PQ(A)]$ of the prime quiver $PQ(A)$ has the following form:

$$[PQ(A)] = \begin{pmatrix} B_1 & * & \cdots & * & * \\ 0 & B_2 & \cdots & * & * \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & B_{t-1} & * \\ 0 & 0 & \cdots & 0 & B_t \end{pmatrix}, \tag{11.8.3}$$

where the square matrices $B_1, B_2, \ldots, B_t$ are permutationally irreducible, i.e., that the numeration of the vertices of $PQ(A)$ is standard.

Theorem 11.8.6. *Let A be an FDD-ring with prime quiver $PQ(A)$, whose adjacency matrix $[PQ(A)]$ has the form (11.8.3). Then there exists a decomposition of $1 \in A$ into a sum of mutually orthogonal idempotents : $1 = g_1 + \cdots + g_t$ such that*

$$A = \bigoplus_{i,j=1}^{t} g_i A g_j$$

is the two-sided Peirce decomposition with $g_i A g_j = 0$ for $j < i$, and, moreover, the adjacency matrices of the prime quivers $PQ(A_i)$ of the rings $A_i = g_i A g_i$ coincide with B_i $(i = 1, \ldots, t)$.

Proof. Taking into account theorem 10.5.1 the proof of this theorem is analogous to the proof of theorem 11.6.3.

Corollary 11.8.7. *An FDD-ring A with a T-nilpotent prime radical can be uniquely decomposed into a finite direct product of indecomposable rings $A_1, \ldots, A_m$ with connected prime quivers $PQ(A_i)$, $i = 1, \ldots, m$.*

11.9 THE LINK GRAPH OF A SEMIPERFECT RING

Let $A_A = P_1^{n_1} \oplus \ldots \oplus P_s^{n_s}$ be a decomposition of a ring A into a direct sum of the indecomposable projective modules, where $P_1, \ldots, P_s$ represent, up to isomorphism, all (different) indecomposable right projective modules.

Let

$$M_k = P_1^{n_1} \oplus \ldots \oplus P_{k-1}^{n_{k-1}} \oplus (P_k R)^{n_k} \oplus P_{k+1}^{n_{k+1}} \oplus \ldots \oplus P_s^{n_s}$$

for $1 \leq k \leq s$. Then $M_1, \ldots, M_s$ are maximal (two-sided) ideals in A and $\bigcap_{k=1}^{s} M_k = R$. Conversely, every maximal (two-sided) ideal M coincides with some M_k.

We assign to the maximal ideals $M_1, \ldots, M_s$ the vertices $1, \ldots, s$ and join vertex i with vertex j by one arrow if and only if the product M_iM_j is strictly contained in $M_i \cap M_j$.

The thus obtained simply laced quiver is called the **link graph** of a semiperfect ring A (or, simply, link graph of A) and is denoted by $\mathcal{L}G(A)$. (cf. *B.J.Müller Localization in fully bounded Noetherian rings, Pacific J. Math., 67, 1976, pp. 233-245*).

Let Q be a quiver. Denote by Q_u the quiver, obtained from Q, by replacing the set of arrows from i to j by a single arrow if that set is nonempty (we allow $i = j$). If Q has no arrows from i to j, then neither does Q_u.

Theorem 11.9.1 *If A is a right Noetherian semiperfect ring, then $\mathcal{L}G(A) = Q_u(A)$.*

Proof. From proposition 11.1.1 it follows that M_k has the following two-sided Peirce decomposition:

$$M_k = \begin{pmatrix} A_{11} & \ldots & A_{1k} & \ldots & A_{1s} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ A_{k1} & \ldots & R_{kk} & \ldots & A_{ks} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ A_{s1} & \ldots & A_{sk} & \ldots & A_{ss} \end{pmatrix}$$

Consider $M_i \cap M_j$.

Case (a) $i = j$: $M_i \cap M_i = M_i$. Consequently, there is a loop at the i-th vertex of the link graph $\mathcal{L}G(A)$ if and only if M_i^2 is strictly contained in M_i. Obviously, M_i^2 is strictly contained in M_i if and only if $f_iR^2f_i$ is strictly contained in f_iRf_i. Therefore, by the Q-Lemma there exists a loop at the i-th vertex of $Q(A)$ if and only if there is a loop at the i-th vertex of $\mathcal{L}G(A)$.

Case (b) $i < j$:

$$M_i \cap M_j = \begin{pmatrix} A_{11} & \ldots & A_{1i} & \ldots & A_{1j} & \ldots & A_{1s} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ A_{i1} & \ldots & R_{ii} & \ldots & A_{ij} & \ldots & A_{is} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ A_{j1} & \ldots & A_{ji} & \ldots & R_{jj} & \ldots & A_{js} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ A_{s1} & \ldots & A_{si} & \ldots & A_{sj} & \ldots & A_{ss} \end{pmatrix}$$

and

$$M_iM_j = \begin{pmatrix} \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & R_{ii} & \ldots & R_{ii}A_{ij} + A_{ij}R_{jj} + \sum\limits_{k \neq i} A_{ik}A_{kj} & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & R_{jj} & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots \end{pmatrix}.$$

Consequently, $f_iR^2f_j$ is strictly contained in f_iRf_j if and only if the product M_iM_j is strictly contained in $M_i \cap M_j$. Therefore, by the Q-lemma, there exists an arrow from i to j in $Q(A)$ if and only if this is the case for $\mathcal{L}G(A)$.

Case (c) $i > j$ is handled analogously. The theorem is proved.

Remark. In general for a semiperfect ring A with Jacobson radical R the link graph $\mathcal{L}G(A)$ coincides with the quiver $Q(A, R)$ associated with R.

11.10 NOTES AND REFERENCES

The notion of a quiver and its representations was introduced by P.Gabriel in his paper: *Unserlegbare Darstellungen 1 // Man. Math., 1972, v.6, p.71-103* in connection with description of finitely dimensional algebras over algebraic closed field with zero square radical. Simultaneously and independently this problem was solved by S.A.Krugliak in his paper: *Representations of algebras with zero square radical // Zap. Nauchn. Sem. LOMI, v.28, 1972, p.60-68.* He reduced the solving of this problem to representations of primitive posets.[8]) These results were generalized to the case of finite dimensional hereditary algebras and radical square zero Artinian algebras of finite representation type over an arbitrary field by V.Dlab and C.M.Ringel (see *V.Dlab, C.M.Ringel, On algebras of finite representation type // J. Algebra, v.33, 1975, N.2, p.306-394* and *V.Dlab, C.M.Ringel, Indecomposable Representations of Graphs and Algebras // Memoirs Amer. Math. Soc., v.173, 1976*).

The notion of representations of a poset[9]) first was introduced by L.A.Nazarova and A.V.Roiter in their paper *Representations of partially ordered sets // Zap. Nauchn. Sem. LOMI, v.28, 1972, p.5-31.* In the paper *Partially ordered sets of finite type // Zap. Nauchn. Sem. LOMI, v.28, 1972, p.32-41.* M.M.Kleiner gave a criterion of finiteness of type for representations of posets. The fundamental monograph of D.Simson: *Linear representations of partially ordered sets and vector space categories. Algebra, Logic and Applic. v.4, Gordon and Breach Science Publishers, 1992*, is devoted to the theory of representations of posets.

V.V.Kirichenko in his papers *Generalized uniserial rings // Preprint IM-75-1, Kiev, 1975* and *Generalized uniserial rings // Mat. sb. v.99(141), N4 (1976), p.559-581* (English translation in *Math. USSR Sbornik, v.28, N.4, 1976, p.501-520*) carried over the notion of a Gabriel quiver to semiperfect right Noetherian rings. He termed them "right schemes".

The notion of the prime quiver of a semiperfect ring first was introduced in the paper *V.V.Kirichenko, Semichain hereditary and semihereditary rings // Modules and algebraic groups. Zap. Nauchn. Sem. LOMI, v.114 (1982), p. 137-147.*

---

[8]) A poset is primitive if its diagram is a disjoint union of linearly ordered sets.

[9]) By a representation of a finite partially ordered set $P = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ with partial order $\leq$ over a field k one means a set $V_1, V_2, ..., V_n$ of subspaces of a finite dimensional vector k-space V such that $V = \sum_{i=1}^{n} V_i$ and $V_i \subset V_j$ whenever $\alpha_i \leq \alpha_j$.

(English translation in *Journal of Soviet Mathematics, v.27, N.4, November, 1984, p.2933-2941*).

These notions have been applied systematically to the structural theory of rings (see, for example, *V.V.Kirichenko, Decompositions theorems for semi-perfect rings //Mat. Stud., v.8 (1997), N.2, p.157-161; Kh.M.Danlyev, V.V.Kirichenko, Yu.V.Yaremenko, On weakly prime Noetherian semiperfect rings with two-generated right ideals // Dopov. Nats. Akad. Nauk Ukr., 1996, N.12, p.7-9; V.V.Kirichenko, Semi-perfect rings and their quivers // An. Ştiinţ. Univ. Ovidius Constanţa Ser Mat. v.4 (1996), N.2, p.89-97; V.V.Kirichenko, S.Valio, Semiperfect rings and their quivers // Infinite groups and related algebraic structures, Acad. Nauk Ukr., Inst. Mat., Kiev, 1993, p.438-456.* In particular, quivers and prime quivers are used for the description of semihereditary semiperfect semidistributive rings (see *V.V.Kirichenko, Semi-Perfect Semi-Distributive Rings // Algebras and Representation Theory, v.3, 2000, p.81-98*). Moreover, $PQ(A) = Q(\tilde{A})$, where $\tilde{A}$ is the classical quotient ring of the ring A.

N.H.McCoy in his paper *N.H.McCoy, Prime ideals in general rings // Amer. J. Math., v.71 (1949), p.823-833* showed that the prime radical, which is the intersection of prime ideals, can be characterized as the set of all elements r such that any "m-system containing it contains also 0". McCoy proved also that the prime radical coincides with the intersection of all minimal prime ideals.

J.Levitzki in the paper: *Prime ideals and the lower radical // Amer. J. Math., v.73 (1951), p.25-29* proved that the prime radical is the set of all strongly nilpotent elements.

In addition to the two radicals of a ring which have been studied in this book, a number of other radicals have been introduced and studied from various points of view. As references, we may mention the following papers: of S.A.Amitsur (see *A general theory of radicals, I,II,III, Amer. J.Math., v.74, 1952, p.774-786; v.76, 1954, p.100-125; v.76, 1954, p.355-361*), R.Baer (see *Radical ideals //Amer. J.Math., v.65, 1943, p.537-568*), B.Brown and N.H.McCoy (see *Radicals and subdirect sums // Amer. J. Math., v.69, 1947, p.46-58*; *The radical of a ring // Duke Math. J., v.15, 1948, p.495-499*), J.Levitzki (see *On the radical of a general ring // Bul. Amer. Math. Soc., v.49, 1943, p.462-466; Prime ideals and the lower radical // Amer. J. Math., v.73, 1951, p.25-29*), J.Krempa (see *Lower radical properties for alternative rings // Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys, v.23, 1975, N2, p.139-142*; *Radicals of semi-group rings // Fund. Math., v.85, N.1, 1974, p.57-71*).

The prime quiver of an associative ring with some finiteness conditions, which are automatically valid for semiperfect rings, was considered in the paper *V.V.Kirichenko, L.Mashchenko, Yu.V.Yaremenko, Decomposition theorem for associative rings // Problems in Algebra, N.11, 1997, p.42-47.* (see also the paper *N.M.Gubareni, V.V.Kirichenko, U.S.Revitskaya, Semiperfect semidistributive semihereditary rings of bounded representation type // Proc. Gomel. State Univ., v.1, N.1 (15), 1999, Problems in Algebra, p.18-36*).

12. Serial rings and modules

12.1 QUIVERS OF SERIAL RINGS

Definition. A module is called **uniserial** if the lattice of its submodules is a chain, i.e., the set of all its submodules is linearly ordered by inclusion. A module is called **serial** if it decomposes into a direct sum of uniserial submodules.

A ring is called **right** (resp. **left**) **uniserial** if it is a right (resp. left) uniserial module over itself, i.e., the lattice of right ideals is linearly ordered. A ring is called **right** (resp. **left**) **serial** if it is a right (resp. left) serial module over itself. A ring which is both a right and left serial ring is called a **serial ring**.

Examples 12.1.1.

1. Let G be a finite Abelian group. The main theorem about finite Abelian groups implies that G is a serial $\mathbf{Z}$-module.

2. Let $A \in M_n(k)$ be a square matrix of order n with elements in a field k, and let V be the module over the ring $k[x]$ obtained by letting x act on k^n like the matrix A. The Frobenius theorem says that V is a serial $k[x]$-module.

Rings, over which all modules are serial, were first systematically considered by G.Köthe and T.Nakayama. T.Nakayama introduced generalized uniserial rings and showed that all modules over them are serial.

In our terminology generalized uniserial rings are Artinian serial rings.

A right (left) serial ring can be decomposed into a direct sum of a finite number of right (left) ideals each of which has exactly one maximal submodule. By theorem 10.3.7 such rings are semiperfect. So, serial rings are a special case of semiperfect rings.

Example 12.1.2.

Let $A = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} \;\middle|\; \alpha \in \mathbf{R}; \beta, \gamma \in \mathbf{C} \right\}$, where $\mathbf{R}$ is the field of real numbers and $\mathbf{C}$ is the field of complex numbers.

It is not difficult to see that A is a right serial ring which is not left serial.

Obviously, the basic ring of a right (resp. left) serial ring is right (resp. left) serial.

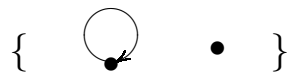
Proposition 12.1.1. *A right (left) serial ring A with nilpotent Jacobson radical R is right (left) Artinian.*

Proof. Let R be the radical of a right serial ring A and $R^m = 0$. It is sufficient to show that any principal module P is Artinian. Indeed, since the ideal R is nilpotent, there is a strictly descending chain of submodules: $P \supset PR \supset ... \supset PR^m = 0$. The factors of this sequence are semisimple A-modules, and since P is a uniserial module they are simple. So there exists a composition series for P and A is a right Artinian ring. The proposition is proved.

We now define the quiver $Q(A)$ of a serial ring A with Jacobson radical R by the formula: $Q(A) = Q(A/R^2)$. Since, by proposition 12.1.1, A/R^2 is an Artinian serial ring, this is well defined. Analogously we can introduce the left quiver $Q'(A)$ of a serial ring A.

Example 12.1.3.

Let $A = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} \;\middle|\; \alpha, \gamma \in \mathbf{Z}_{(p)}; \beta \in \mathbf{Q} \right\}$. Obviously, A is a serial ring which is right Noetherian but not left Noetherian. Clearly, $A/R^2 = \mathbf{Z}_{(p)}/p^2\mathbf{Z}_{(p)} \times \mathbf{Q}$ and the quiver $Q(A)$ looks as follows



Theorem 12.1.2. *The quiver of a serial ring A is a disconnected union of cycles and chains.*

Proof. Assume that the ring A is reduced. Since A is a right serial module over itself it follows that from every vertex of the quiver of A there exits not more that one arrow.

We are going to show that, also, each vertex is an end of not more than one arrow. Indeed, let us assume that the vertex k is an end of arrows with starting vertices j_1, ..., j_m $(m > 1)$. From the above it follows that all these points are distinct. By the Q-Lemma, there are strict inclusions

$$e_{j_1}R^2e_k \subset e_{j_1}Re_k, ..., e_{j_m}R^2e_k \subset e_{j_m}Re_k.$$

Consider the left quotient module Re_k/R^2e_k. By the Q-lemma, it contains as direct summands the left simple modules $V_{j_1}, ..., V_{j_m} (V_i = Ae_i/Re_i)$. Therefore the left module Ae_k is not uniserial and we have a contradiction. As there are only two types of finite connected graphs having the properties pointed out – a cycle and a chain. The theorem is proved.

From this theorem and theorem 11.1.5 we obtain the following corollary.

Corollary 12.1.3. *The quiver of a serial two-sided Noetherian indecomposable ring is either a cycle or a chain.*

This corollary is a generalization of H.Kupisch's results for serial two-sided Noetherian rings, see the notes at the end of the chapter for a precise reference.

12.2 SEMIPERFECT PRINCIPAL IDEAL RINGS

Definition. A ring A is called a **principal ideal ring** if all its right ideals are right principal and all its left ideals are left principal.

Recall that the ring $\mathcal{O}$ (not necessary commutative) is called a **principal ideal domain** if it has no zero divisors and all its right and left ideals are principal.

In the fourth chapter of *N.Jacobson's book "The Theory of Rings" (Amer. Math. Soc. Surveys, v.2, New York, 1943)*, there is theorem 37, which can be formulated in modern terminology as follows:

Theorem 12.2.1. *If every two-sided ideal in an Artinian ring A is a right principal ideal and also a left principal ideal then A is isomorphic to a finite direct product of full matrix rings over Artinian uniserial rings.*

Note that, conversely, each right ideal in such a ring is a right principal ideal and every left ideal is a left principal ideal.

Theorem 12.2.2. *Let A be a semiperfect ring such that every two-sided ideal in A is both a right principal ideal and a left principal ideal. Then A is a principal ideal ring isomorphic to a direct product of a finite number of full matrix rings over Artinian uniserial rings and local principal ideal domains. Conversely, all such rings are semiperfect principal ideal rings.*

Proof. Suppose a semiperfect ring A satisfies the conditions of the theorem and $A = A_1 \times \ldots \times A_t$ is a decomposition of A into a direct product of a finite number of indecomposable rings $A_1, \ldots, A_t$. Let $1 = g_1 + \ldots + g_t$ be the corresponding decomposition of the identity of A into a sum of pairwise orthogonal central idempotents, i.e., $g_i A = A g_i = A_i$ for $i = 1, \ldots, t$. Let $\mathcal{I}_k$ be a two-sided ideal of A_k. Obviously, $\mathcal{I}_k$ is also a two-sided ideal of A. We have $I_k = xA = Ay$ and

(1) $\mathcal{I}_k = g_k \mathcal{I}_k = g_k xA = x g_k A = x g_k g_k A = x_k A_k$, where $x_k \in A_k$.

(2) $\mathcal{I}_k = \mathcal{I}_k g_k = A y g_k = A g_k y = A g_k g_k y = A_k y_k$, where $y_k \in A_k$.

Therefore $\mathcal{I}_k$ is both a right principal ideal and a left principal ideal of A_k. Thus, the conditions of the theorem are true for any indecomposable ring A_k and we can assume that A is an indecomposable ring.

Let $A = P_1^{n_1} \oplus ... \oplus P_s^{n_s}$ be a decomposition of a ring A into a direct sum of principal modules and let $1 = f_1 + ... + f_s$ be the corresponding decomposition of the identity of A into a sum of pairwise orthogonal idempotents, i.e., $f_i A = P_i^{n_i}$. Then $A f_i = Q_i^{n_i}$, where $Q_1, ..., Q_s$ are pairwise nonisomorphic principal left modules.

From proposition 11.1.1 it follows that

$$P_1^{n_1} \oplus ... \oplus P_{k-1}^{n_{k-1}} \oplus (P_k R)^{n_k} \oplus P_{k+1}^{n_{k+1}} \oplus ... \oplus P_s^{n_s} = \mathcal{I}_k$$

is a two-sided ideal. If $P_k R \neq 0$ then, by lemma 11.1.8, $P_k R / P_k R^2 \simeq U_k$. Hence it follows immediately that both the right quiver and the left quiver of the ring $\bar{A} = A/R^2$ is a disconnected union of points and loops.

Assume that P is an Artinian principal A-module. Since $P/PR \simeq PR/PR^2$, we have $P(PR) \simeq P$ and therefore $PR/PR^2 \simeq PR^2/PR^3$. Continuing this process, we conclude that the module P has exactly one composition series, all factors of which are isomorphic. Without loss of generality one may assume that $P = P_1$. Then $Hom_A(P', P_1^{n_1}) = 0$, where $P' = P_2^{n_2} \oplus ... \oplus P_s^{n_s}$. Let $1 = e + f$ be a decomposition of $1 \in A$ into a sum of idempotents such that $eA = P_1^{n_1}$ and $fA = P'$. Analogously one can prove that $Hom_A(eA, fA) = 0$. From the above we conclude that $A = eAe$ is a two-sided Artinian ring, whose quiver is either a loop or a point (when $PR = 0$).

Therefore one may assume that among both the left and the right principal A-modules there are no Artinian modules.

Consider the ring $\bar{A} = A/R^2$. It decomposes into a direct product of rings, whose quivers are either points or loops. Hence it follows that $\bar{R} = \bar{p}\bar{A} = \bar{A}\bar{p}$, where $\bar{R}$ is the radical of the ring $\bar{A}$. Denote by p an element, whose image is $\bar{p}$ under the natural projection A onto $\bar{A}$. We have the equalities $pA + R^2 = R = Ap + R^2$, and hence, by Nakayama's lemma, $R = Ap = pA$.

Let $N = \bigcap_{m=0}^{\infty} R^m$. We shall show that $N = 0$. If this is not so, then $NR + RN$ is strictly contained in N. Factoring A by the ideal $NR + RN$ one can assume that in the initial ring we have $NR + RN = 0$. Thus, $RN = 0$ and $NR = 0$, hence N is a semisimple cyclic right A-module and a semisimple cyclic left A-module.

Consider the two-sided Peirce decomposition: $N = \bigoplus_{i,j=1}^{s} f_i N f_j$. By proposition 11.1.1, every set $N_{ij} = f_i N f_j$ is a two-sided ideal in the ring A.

It is easy to verify that the set

$$L_i = f_1 N \oplus ... \oplus f_{i-1} N \oplus P_i^{n_i} \oplus f_{i+1} N \oplus ... \oplus f_s N$$

is a two-sided ideal in the ring A $(i = 1, ..., s)$.

If every two-sided ideal

$$N_{1i} \oplus ... \oplus N_{i-1i} \oplus N_{i+1i} \oplus ... \oplus N_{si}$$

is nonzero, then $\mu_A(L_i) > 1$ by lemmas 11.1.3 and 11.1.8.

Therefore the two-sided Peirce decomposition of the ideal N is of the form: $N = N_{11} \oplus ... \oplus N_{ss}$.

Without loss of generality one can assume that $N_{11} \neq 0$. Using the same lemmas we obtain that $N_{11} = U_1^{n_1}$ as a right module and $M_{11} = V_1^{n_1}$ as a left module.

Therefore each principal module P has a countable chain of submodules:

$$P \supset PR \supset ... \supset PR^k \supset PR^{k+1} \supset ...$$

where PR^{k+1} is a unique maximal submodule in PR^k for each positive integer k. If $\bigcap\limits_{m=1}^{\infty} PR^m \neq 0$, then $\bigcap\limits_{m=1}^{\infty} PR^m = U$, where $U = P/PR$. Then it follows that $Hom(P_i, P_j) = 0$ for all principal modules P_i, P_j $(i \neq j)$.

Since the ring A is indecomposable, $A = P^n = Q^n$, where P is a principal uniserial right A-module, and Q is a principle uniserial left A-module.

Multiplication on the left side by p is an endomorphism of the ring A as a right A-module. We shall denote it by the same letter p. If we can show that $Kerp = 0$, then $N = 0$. We are going to prove that $Kerp \subset R^m$ for all natural m. Indeed, let $px = 0$, $x \notin N$ and $x \neq 0$. Let $1 = e_1 + ... + e_n$ be a decomposition of the identity of the ring A into a sum of local pairwise orthogonal idempotents. If $xe_i \in R^m e_i$ for all i and m, then $x \in N$. Therefore there exists an index j such that $xe_j \in R^m e_j$ but $xe_j \notin R^{m+1} e_j$. As above $R^{m+1} e_j$ is the unique maximal submodule in $R^m e_j$ for any natural m. Therefore by Nakayama's lemma $Axe_j = R^m e_j$. Hence $pAxe_j = Apxe_j = 0$. On the other hand,

$$R^{m+1} e_j = RAxe_j = pAAxe_j = pAxe_j.$$

Therefore the module Ae_j is Artinian and we obtain a contradiction. So we have shown that the two-sided ideal $Kerp$ is contained in N. Therefore $Kerp = N$. So $x = p^m a_m$ for some a_m for any natural m. Hence $a_m \notin Kerp^m$, but $a_m \in Kerp^{m+1}$ since $px = 0$. Therefore the inclusion $Kerp^m \subset Kerp^{m+1}$ is strict and we have formed an infinite ascending chain of two-sided ideals $0 \subset Kerp \subset Kerp^2 \subset ....$

Write $Kerp^2 = M$. Note that $e_i N \neq 0$ and $Ne_i \neq 0$ for $i = 1, ..., n$. Moreover, $RM = pAM = pM$ belongs to $Kerp$. As above, we obtain that the module P is Artinian. Therefore $N = 0$. So all submodules of $e_i A$ (Ae_i) are exhausted by the modules $e_i R^m$ $(R^m e_i)$ and the ring A is two-sided Noetherian as a direct sum of Noetherian modules.

Therefore one can assume that $A = P^n$, the module P is uniserial and all factors PR^i/PR^{i+1} are isomorphic. Since $A \simeq End_A A \simeq End_A P^n \simeq M_n(End_A P)$, it follows that $\mathcal{O} \simeq End_A P$ is a local uniserial ring, and it is not difficult to see that it is either a local Artinian uniserial ring or a local principal ideal domain.

Conversely, all rings of the form given in the formulation of the theorem are semiperfect principal ideal rings. The theorem is proved.

12.3 SERIAL TWO-SIDED NOETHERIAN RINGS

In this section we are going to describe all serial two-sided Noetherian rings.

Proposition 12.3.1 (Yu.A.Drozd) *For a semiperfect ring A the following conditions are equivalent:*

1) *A is a right (left) serial ring*;

2) *for any two nonzero homomorphisms of right (left) principal A-modules* $f_i : P_i \to P$ $(i = 1, 2)$ *one of the two equations:* $f_1 = f_2 x$ *or* $f_2 = f_1 y$ *is solvable*;

3) *for any two nonzero homomorphisms of left (right) principal A-modules* $f_i : P \to P_i$ $(i = 1, 2)$ *one of the two equations* $f_1 = x f_2$ *or* $f_2 = y f_1$ *is solvable, with* $x \in Hom_A(P_1, P_2)$, $y \in Hom_A(P_1, P_2)$.

Proof.

1) $\Rightarrow$ 2). If the ring A is right serial, then either $Imf_1 \subset Imf_2$, or $Imf_2 \subset Imf_1$. In the first case the solvability of the equation $f_1 = f_2 x$ follows from the projectivity of P_1 and in the second case the solvability of the equation $f_2 = f_1 y$ follows from the projectivity of P_2.

2) $\Rightarrow$ 1). If the ring A is not right serial then in some right principal A-module P there are nonzero submodules M_1, M_2 and nonzero elements $a_1 \in M_1 \backslash M_2$, $a_2 \in M_2 \backslash M_1$. Then there are local idempotents e_1 and e_2 of the ring A such that $a_1 e_1 \in M_1 \backslash M_2$ and $a_2 e_2 \in M_2 \backslash M_1$. Denote by $P_i = e_i A$ and $f_i : P_i \to P$ the homomorphisms which transform e_i into $a_i e_i$ for $i = 1, 2$. Since $Imf_1 \not\subset Imf_2$ and $Imf_2 \not\subset Imf_1$, both equations $f_1 = f_2 x$ and $f_2 = f_1 y$ are not solvable.

The equivalence of conditions 2) and 3) follows from the isomorphisms: $Hom(eA, fA) \simeq fAe \simeq Hom(Af, Ae)$, when f and e are idempotents of the ring A.

From this proposition we obtain the following corollary.

Corollary 12.3.2. *Let A be a semiperfect ring and let* $1 = e_1 + ... + e_n$ *be a decomposition of* $1 \in A$ *into a sum of local pairwise orthogonal idempotents. The ring A is right serial if and only if for each idempotent e, which is a sum of not more than three different local idempotents from the set* $\{e_1, e_2, ..., e_n\}$, *the ring eAe is right serial.*

Proof. Let A be a right serial ring and let $e \in A$ be a nonzero idempotent. Then the ring eAe is right serial. Write $1 = e + f$, $eAe = A_1$, $eAf = X$, $fAe = Y$, $fAf = A_2$. Let $e = e_1 + ... + e_m$ be the decomposition e in the sum of pairwise orthogonal local idempotents. Suppose the module $e_i Ae$ is not uniserial. Then in $e_i Ae$ there exist two eAe-submodules M_1 and M_2 such that $M_1 \cap M_2 \neq M_1$ and $= M_1 \cap M_2 \neq M_2$. Write $\overline{M}_1 = M_1 A$ and $\overline{M}_2 = M_2 A$. Clearly, $\overline{M}_1 \subset e_i A$ and $\overline{M}_1 e = M_i$ for $i = 1, 2$. Therefore the principal A-module $e_i A$ is not uniserial and so we have a contradiction.

Conversely, if a principal A-module $P = e_i A$ is not uniserial, then there exist two submodules K and L of P such that $= K \cap L \neq K$ and $K \cap L \neq L$. So one can choice $k \in K$ and $l \in L$ such that $k \notin L$ and $l \notin K$. Let $K_1 = kA$ and $L_1 = lA$. Let $P(K_1) = \overset{s}{\underset{j=1}{\oplus}} P_j^{m_j}$, where $P_j = e_j A$, and $= m_1 + .. + m_s \geq 2$. If there exists t such that $m_t \geq 2$, then the ring $= (e_i + e_t)A(e_i + e_t)$ is not right serial. In the case if there exist two numbers $m_p = 1$ and $m_q = 1$, then the ring $(e_i + e_p + e_q)A(e_i + e_p + e_q)$

is not righ serial. So, K_1 is a local module, i.e., $P(K_1) = P_j$. Analogously, $P(L_1) = P_m$. Therefore the ring $(e_i + e_j + e_m)A(e_i + e_j + e_m)$ is not right serial. A contradiction.

We are going to consider serial two-sided Noetherian rings. According to theorems 11.1.9 and 12.1.2 one can assume that the quiver of a serial two-sided Noetherian indecomposable ring is either a chain or a cycle. Such a ring will be called a **ring of the first type** if its quiver is a chain and a **ring of the second type** if its quiver is a cycle.

Since the basic ring of a serial ring is also a serial ring, in future we shall assume that the serial ring A is reduced.

First we consider a ring A of the first type. Suppose, the quiver $Q(A)$ is of the form

$$\left\{ \begin{array}{ccccccccc} 1 & & 2 & & & & t-1 & & t \\ \bullet & \longrightarrow & \bullet & \longrightarrow & \cdots & \longrightarrow & \bullet & \longrightarrow & \bullet \end{array} \right\}$$

Consider the corresponding decomposition of the ring A into a direct sum of principal A-modules: $A = P_1 \oplus ... \oplus P_t$. Let $1 = e_1 + ... + e_t$ be a decomposition of the identity of A such that $P_i = e_i A$. The corresponding two-sided Peirce decomposition has the form:

$$A = \begin{pmatrix} A_{11} & \dots & A_{1t} \\ \dots & \dots & \dots \\ A_{t1} & \dots & A_{tt} \end{pmatrix}$$

The components $A_{12}, A_{23}, ...A_{(t-1),t}$ are nonzero, because there is an arrow $i \to i+1$ for each i in the quiver.

By theorem 11.6.3 we have $A_{ij} = 0$ for $i > j$ and $Q(A_{ii})$ is a point for all i. Consequently, A_{ii} is a division ring for $i = 1, \dots, t$.

The two-sided Peirce decomposition of the radical R of the ring A has the form $R = \underset{i<j}{\oplus} A_{ij}$. Therefore $R^t = 0$ and by proposition 12.1.1 A is a two-sided Artinian ring.

Since $e_i R/e_i R^2 \simeq U_{i+1}$ $(i = 1, ..., t-1)$, by the Q-Lemma, it follows that $e_i R^2 e_{i+1}$ is the unique maximal $A_{(i+1),(i+1)}$-submodule in $e_i R e_{i+1} = e_i A e_{i+1}$, $i = 1, 2, ..., t-1$. Since $e_i R^2 e_{i+1}$ is strictly contained in $e_i R e_{i+1}$, and the ring A is serial, it follows that $Re_i/R^2 e_i \simeq V_{i-1}$ for $i = 2, ..., t$ (where the $V_1, ..., V_t$ are simple left A-modules). Choosing an element $a_{i,(i+1)} \in e_i R e_{i+1} \backslash e_i R^2 e_{i+1}$ we have, by Nakayama's lemma, that $A_{i,(i+1)} = a_{i,(i+1)} A_{(i+1),(i+1)} = A_{ii} a_{i,(i+1)}$, $i = 1, ..., t-1$. We set $p = a_{12} + a_{23} + ... + a_{(t-1),t}$. Obviously, $a_{i,(i+1)} A + e_i R^2 = e_i R$, $i = 1, ..., t-1$. By Nakayama's lemma, $e_i R = a_{i,(i+1)} A$. Therefore $R = pA$. Analogously, $R = Ap$. Note that $e_i p = p e_{i+1}$, $i = 1, ..., t-1$.

Since $A_{ii} = D_i$ is a division ring for $i = 1, ..., t$ and $A_{i,(i+1)} = a_{i,(i+1)} D_{i+1} = = D_i a_{i,(i+1)}$, the map $\sigma_{i,(i+1)} : D_i \to D_{i+1}$, given by $d_i a_{i,(i+1)} = a_{i,(i+1)} d_i^{\sigma_{i,(i+1)}}$, $d_i \in D_i$, is an isomorphism from the division ring D_i to the division ring D_{i+1}.

Here $d_i^{\sigma_{i,(i+1)}}$ means "apply the mapping $\sigma_{i,(i+1)}$ to d_i". Write $\tau_{i,(i+1)} = \sigma_{i,(i+1)}^{-1}$, $i = 1, ..., t-1$.

Let B be a ring and let $1 = f_1 + ... + f_n$ be a decomposition of the identity of B into a sum of pairwise orthogonal idempotents, $B_{ij} = f_i B f_j$, $b_{ij} \in B_{ij}$ for $i, j = 1, 2, ..., n$, and let Δ be a ring. Consider for a fixed integer $k = 1, 2, ..., n$ an isomorphism $\tau : B_{kk} \to \Delta$ of rings. Using the isomorphism τ one can form a ring C in the following way: the components of the two-sided Peirce decomposition of the ring C are given by the rule: $C_{pq} = B_{pq}$ for $(p, q) \neq (k, k)$ and $C_{kk} = \Delta$. The multiplication in the ring C, which will be denoted by a little circle, is given by the rule: $c_{sr} \circ c_{rp} = c_{sr} c_{rp}$ if c_{sr}, $c_{rp} \notin \Delta$; $c_{kk} \circ c_{kp} = c_{kk}^{\sigma^{-1}} c_{kp}$ and $c_{pk} c_{kk}^{\sigma^{-1}} = c_{pk} \circ c_{kk}$ if $p \neq k$; $c_{kk} \circ c'_{kk} = c_{kk} c'_{kk}$. It is trivial to verify that the map $\psi : C \to B$, given by the formula $\psi[(c_{ij})] = (b_{ij})$, where $b_{ij} = c_{ij}$ for $(i, j) \neq (k, k)$ and $b_{kk} = c_{kk}^{\sigma^{-1}}$, is an isomorphism of the rings C and B. In future we shall refer to this construction as the (K.12.3) construction.

Using the construction (K.12.3) with the automorphism $\tau_{12} = \sigma_{12}^{-1}$ and keeping the same symbols for the new ring, we have $\alpha_1 \circ a_{12} = \alpha_1 a_{12} = a_{12} \alpha_1^{\sigma_{12}} = a_{12} \alpha_1^{\tau_{12}^{-1}} = a_{12} \circ \alpha_1$ in the new ring. Therefore we have identified the division ring D_2 with the division ring D_1. Moreover, in the new ring, σ_{12} is the identity automorphism. Keeping for the remaining automorphisms previous symbols we shall identify the division ring D_3 with the division ring D_1 by means of the automorphism σ_{23}, moreover, in the new ring σ_{12} and σ_{23} are identity automorphisms of the division ring D_1. Continuing this process, we obtain a ring B in which the automorphisms $\tau_{i,(i+1)}$ $(i = 1, ..., t-1)$ are identity automorphisms of the division ring D_1 and $B_{ii} = D_1$ for $i = 1, ..., t$. Write $D_1 = D$. Let $1 = b_{11} + ... + b_{tt}$ be the corresponding decomposition of the identity of the ring B into a sum of pairwise orthogonal idempotents. Let $b_{i,(i+1)} \in B_{i,(i+1)}$ be nonzero elements such that $d b_{i,(i+1)} = b_{i,(i+1)} d$ for any element $d \in D$ $(i = 1, ..., t)$. As above for the element $p = b_{12} + b_{23} + ... + b_{(t-1),t}$ we have $R = pB = Bp$ (R is the radical of B) and $b_{ii} p = p b_{i+1,i+1} = b_{i,(i+1)}$. Suppose that $i < j$ and $B_{ij} \neq 0$. Then

$$b_{ii} R b_{jj} = b_{ii} p B b_{jj} = b_{ii} p b_{(i+1),(i+1)} B b_{jj}$$

$$= b_{i,(i+1)} b_{(i+1),(i+1)} B b_{jj} = b_{i,(i+1)} b_{(i+1),(i+1)} p B b_{jj} =$$

$$= b_{i,(i+1)} b_{(i+1),(i+2)} b_{(i+2),(i+2)} p B_{jj} = b_{i,(i+1)} ... b_{(j-1),j} b_{jj} B b_{jj}.$$

Let $b_{ij} = b_{i,(i+1)} ... b_{(j-1),j}$. Clearly, $D b_{ij} = b_{ij} D = B_{ij}$ and $d b_{ij} = b_{ij} d$ for any $d \in D$. If $B_{pq} = 0$ then we set $b_{pq} = 0$.

Consider the ring $T_t(D)$ of the upper triangular matrices over the division ring D. The $\sum_{i \leq j} d_{ij} e_{ij}$ are the elements from $T_t(D)$ (where the e_{ij} are the matrix units, $d_{ij} \in D$). The correspondence $\psi : T_t(D) \to B$ such that $\psi(\sum_{i \leq j} d_{ij} e_{ij}) = \sum_{i \leq j} d_{ij} b_{ij}$ yields an epimorphism of additive groups from the ring $T_t(D)$ onto B.

Note that $Ker\psi$ is a two-sided ideal in the ring $T_t(D)$. This follows from the fact that if $b_{jk} = 0$ then $b_{ik} = 0$ for $i < j$. Therefore the ring B is isomorphic to a quotient ring of the ring of upper triangular matrices over a division ring.

To consider a ring of the second type we shall need the well known Schanuel lemma.

Lemma 12.3.3 (Schanuel's lemma). *Let $P_1/X_1 \simeq P_2/X_2$, where P_1 and P_2 are projective modules. Then $P_1 \oplus X_2 \simeq P_2 \oplus X_1$.*

Proof. Let $P_1/X_1 \simeq P_2/X_2 = W$. Denote by $\pi_i : P_i \to W$ the corresponding natural projections, $X_i = Ker\pi_i$, $i = 1, 2$. Denote by Q the submodule in $P_1 \oplus P_2$ consisting of the pairs (p_1, p_2) such that $\pi_1(p_1) = \pi_2(p_2)$, and define the homomorphisms $\psi_1 : Q \to P_1$ and $\psi_2 : Q \to P_2$ by $\psi_1(p_1, p_2) = p_1$ and $\psi_2(p_1, p_2) = p_2$.[1]) Clearly, $Ker\psi_1 \simeq X_2$, $Ker\psi_2 \simeq X_1$ and $Im\psi_1 = P_1$, $Im\psi_2 = P_2$. Then we have two exact sequences

$$0 \to X_2 \longrightarrow Q \xrightarrow{\psi_1} P_1 \to 0$$

$$0 \to X_1 \longrightarrow Q \xrightarrow{\psi_2} P_2 \to 0$$

with projective modules P_1, P_2. So they must split and therefore $Q \simeq P_1 \oplus X_2$ and $Q \simeq P_2 \oplus X_1$. The lemma is proved.

Assume that A is a ring of the second type. Let $A = P_1 \oplus ... \oplus P_t$ be the corresponding decomposition of A into a direct sum of principal A-modules, let $1 = e_1 + ... + e_t$ be a decomposition of the identity of A into a sum of pairwise orthogonal idempotents such that $P_i = e_iA$, $i = 1, ..., t$; $A_{ij} = e_iAe_j$, $i, j = 1, ..., t$.

Let the quiver $Q(A)$ have the form

$$\left\{ \begin{array}{ccccccccc} 1 & & 2 & & & & t & & 1 \\ \bullet & \longrightarrow & \bullet & \longrightarrow & \cdots & \longrightarrow & \bullet & \longrightarrow & \bullet \end{array} \right\}$$

Since $e_iR/e_iR^2 \simeq U_{i+1}$ $(i = 1, ..., t-1)$ and $e_tR/e_tR^2 \simeq U_1$, by the Q-Lemma, $e_iR^2e_{i+1}$ is the unique maximal $A_{(i+1),(i+1)}$-submodule in $e_iRe_{i+1} = e_iAe_{i+1}$ $(i = 1, ..., t-1)$ and $e_tR^2e_1$ is the unique maximal A_{11}-submodule in $e_tRe_1 = e_tAe_1$. Since $e_tR^2e_1$ is strictly contained in e_tRe_1, it follows from the fact that the ring A is serial that $Re_1/R^2e_1 \simeq V_t$ and therefore that $e_tR^2e_1$ is the unique maximal left A_{tt}-submodule in e_tAe_1. Exactly in the same way $Re_i/R^2e_i \simeq V_{i-1}$ for $i = 2, ..., t$ (where the $V_1, ..., V_t$ are simple left A-modules). Choosing an element $a_{i,(i+1)} \in$

---

[1]) Q is the socalled pushout or fibred product of the diagram $\begin{array}{ccc} & & P_2 \\ & & \downarrow \\ P_1 & \longrightarrow & W \end{array}$ which is a commutative diagram $\begin{array}{ccc} Q & \longrightarrow & P_2 \\ \downarrow & & \downarrow \\ P_1 & \longrightarrow & W \end{array}$ with certain universality properties.

$e_iRe_{i+1}\backslash e_iR^2e_{i+1}$, by Nakayama's lemma, we have that $A_{i,(i+1)} = a_{i,i+1}A_{i+1,i+1}$ $(i = 1, ..., t-1)$.

Exactly in the same way one can choose a_{t1} and then $A_{t1} = a_{t1}A_{11} = A_{tt}a_{t1}$. We set $p = a_{12} + ... + a_{t-1,t} + a_{t1}$. Obviously, $a_{i,i+1}A + e_iR^2 = e_iR$ $(i = 1, ..., t-1)$ and $a_{t1}A + e_tR^2 = e_tR$. By Nakayama's lemma $a_{i,i+1}A = e_iR$ and $a_{t1}A = e_tR$. Therefore $R = pA$. Analogously $R = Ap$. Note that $e_ip = pe_{i+1}$ for $i = 1, ..., t-1$ and $e_1p = pe_t$.

Multiplication of elements of A on the left (right) side by p is an endomorphism of A as a right (left) module over itself. Therefore we have the following equalities:

$$pP_j = P_{j-1}R = a_{j-1,j}P_j; \tag{12.3.1}$$

$$pP_1 = P_tR = a_{t1}P_1.$$

Suppose that the ring A is not Artinian. From equality (12.3.1) it immediately follows that all modules P_1,...,P_t are not Artinian.

We shall show that $Ker(p) = 0$. Consider $N = \bigcap_{m=0}^{\infty} R^m$. If $N \neq 0$ then $RN + NR$ is a proper submodule in N and factoring the ring A by it we may consider that in the initial ring $RN + NR = 0$.

We are going to show that $Ker(p) \subset N$. Suppose the contrary. Let $x \in Ker(p)$, $x \notin N$ and $x \neq 0$. Consider xe_i $(i = 1, ..., t)$. If $xe_i \subset R^me_i$ for all i, m then $x \in N$. Therefore there is an index j and an integer m such that $xe_j \in R^me_j\backslash R^{m+1}e_j$. By Nakayama's lemma, $Axe_j = R^me_j$. Hence $R^{m+1}e_j = RAxe_j = pAAxe_j = pAxe_j = Apxe_j = 0$, i.e., the module Ae_j is Artinian. A contradiction. So $x = p^ma_m$ for any natural m, where $a_m \notin Ker(p^m)$. But $a_m \in Ker(p^{m+1})$, because $px = 0$. Therefore the inclusion $Ker(p^m) \subset Ker(p^{m+1})$ is strict and we have built the infinite strictly ascending chain of ideals:

$$0 \subset Ker(p) \subset Ker(p^2) \subset ...,$$

which contradicts the Noetherian property of the ring A. Hence it follows that $N = \bigcap_{m=0}^{\infty} R^m = 0$. So all proper submodules of the principal modules e_iA (Ae_i) are exhausted by the e_iR^m (R^me_i) (where m is a natural number).

Since multiplication by p is a monomorphism, from the equality (12.3.1) it follows that all modules P_iR^m are projective. Analogously, all submodules of the left principal modules are projective.

We are going to show that any right ideal $\mathcal{I}$ in the ring A is projective as well. We shall carry out the proof by induction on the minimal number of principal A-modules in the decomposition of the ideal $\mathcal{I}$. The base of induction has been proved above. Let $\mathcal{I} \subset P_{i_1} \oplus ... \oplus P_{i_n}$. Consider the ideal $\mathcal{I} + P_{i_1}$. Obviously, $\mathcal{I} + P_{i_1} = \mathcal{I}' \oplus P_{i_1}$, where $\mathcal{I}'$ is the image of the projection from $\mathcal{I}$ onto $P_{i_2} \oplus ... \oplus P_{i_n}$. By the induction hypothesis $\mathcal{I}'$ is a projective A-module. Since $(\mathcal{I} + P_{i_1})/\mathcal{I} \simeq P_{i_1}/(P_{i_1} \cap \mathcal{I})$, by Schanuel's lemma $\mathcal{I} \oplus P_{i_1} \simeq (\mathcal{I} + P_{i_1}) \oplus (\mathcal{I} \cap P_{i_1})$. Hence $\mathcal{I}$ is a projective A-module. Therefore the ring A is right hereditary. Exactly in the same way one can show that A is left hereditary.

We are going to show that every nonzero two-sided ideal in the ring A contains a power of the radical R of A. Since $\mathcal{I} \neq 0$, there is a principal module P such that $P \cap \mathcal{I} \neq 0$. Then $P \cap I = PR^m$ for some natural number m. Then from the equality (12.3.1) it follows that $\mathcal{I} \supset R^{m+t}$. Therefore the product of nonzero two-sided ideals of A is not equal to zero and the ring A is prime, by definition. (Recall that the ring is called prime if the product of every two of its nonzero two-sided ideals is not equal to zero.) So we have shown that A is a two-sided Noetherian and two-sided hereditary prime semiperfect ring.

Denote by $H_t(\mathcal{O})$ the ring of $t \times t$ matrices of the form:

$$H_t(\mathcal{O}) = \begin{pmatrix} \mathcal{O} & \mathcal{O} & \dots & \mathcal{O} \\ \mathcal{M} & \mathcal{O} & \dots & \mathcal{O} \\ \mathcal{M} & \mathcal{M} & \dots & \mathcal{O} \end{pmatrix}$$

where $\mathcal{O}$ is a a discrete valuation ring.

Note that the statement: Artinian (resp. hereditary and so on) ring denotes two-sided Artinian (resp. two-sided hereditary ring and so on). In future we shall not again explicity recall that.

It is easy to see that the ring $H_t(\mathcal{O})$ is a Noetherian serial prime hereditary ring.

Theorem 12.3.4. *A Noetherian semiperfect prime reduced hereditary ring A is either a division ring or is isomorphic to a ring of the form $H_t(\mathcal{O})$ where $\mathcal{O}$ is a discrete valuation ring.*

To prove this theorem we shall need some more statements that are also of independent interest.

Lemma 12.3.5. *Let A be a semiperfect semiprime two-sided Noetherian ring whose quiver is connected. If the ring A is not a division ring then each vertex of $Q(A)$ is the end of at least one arrow and each vertex of $Q(A)$ is the start of at least one arrow.*

Proof. Let A be a semiperfect semiprime two-sided Noetherian ring whose quiver is connected. One may assume that the ring A is reduced. Suppose that no arrow enters to the point 1 (this can be assumed without any loss of generality). Consider the corresponding two-sided Peirce decomposition of the ring A: $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$, and the corresponding decomposition of the identity $1 = e_1 + e_2$ of A into a sum of orthogonal idempotents. Then $e_1 A = P_1$ is a principal A-module. By proposition 11.1.1 $A_{21}R_1 + R_2A_{21} = A_{21}$, where R_i is the Jacobson radical of the ring A_{ii} $(i = 1, 2)$. Hence, by theorem 3.6.1 and Nakayama's lemma, $A_{21} = 0$. Since the ring A is semiprime, it follows that $A_{12} = 0$. Therefore, since $Q(A)$ is a connected quiver, we obtain that the ring A is a division ring. The rest is proved analogously.

Proposition 12.3.6. *The quiver (left quiver) of a semiperfect prime Noetherian hereditary ring A is either a point or a cycle.*

Proof. Suppose there exist arrows going from the vertex 1 to two different vertices i and j. Then P_1R contains as a direct summand a module N, which is isomorphic to $P_i \oplus P_j$. Fix monomorphisms $\varphi : P_i \to P_1$, $\psi : P_j \to P_1$, such that $Im(\varphi \oplus \psi) = N$.

Due to the fact that the ring A is prime, the sets $Hom(P_1, P_i)$ and $Hom(P_1, P_j)$ are both different from zero. Obviously, the sets $\varphi Hom(P_1, P_i)$ and $\psi Hom(P_1, P_j)$ are right ideals in the ring $End(P_1)$ and they are not contained in one another. This contradicts theorem 10.2.7. By propositions 9.2.13 and 5.5.7 one may assume that the ring A is reduced. We are going to show that not more than one arrow ends at one and the same vertex. Consider the vertex with number k. It is sufficient to consider the case when there exist arrows going from two different vertices j_1 and j_2 to vertex k. Then by the Q-Lemma there are strict inclusions: $e_{j_1}R^2e_k \subset e_{j_1}Re_k$, $e_{j_2}R^2e_k \subset e_{j_2}Re_k$. We set $Q_k = Ae_k$, where e_k is an idempotent corresponding to the principal module P_k. By the Q-lemma we conclude that the simple modules V_{j_1} and V_{j_2} enter into the quotient module RQ_k/R^2Q_k. Therefore $RQ_k = Q_{j_1} \oplus Q_{j_2} \oplus X$. This again contradicts the fact that $End(Q_k)$ is a discrete valuation ring. Now the statement of the proposition follows from lemma 12.3.5. The proposition is proved.

Proof of theorem 12.3.4. By proposition 12.3.6, the quiver of such a ring is either a point or a cycle. If the quiver of A is a point, then $A \simeq P$, where P is a simple module, and therefore $A \simeq End_A(P)$ is a division ring. Let the quiver $Q(A)$ be a cycle:

$$\left\{ \begin{array}{ccccccccccc} 1 & & 2 & & & & t-1 & & t & & 1 \\ \bullet & \longrightarrow & \bullet & \longrightarrow & \cdots & \longrightarrow & \bullet & \longrightarrow & \bullet & \longrightarrow & \bullet \end{array} \right\}$$

Note that the left quiver of the ring A is also a cycle consisting of t points. Therefore the quotient ring A/R^2 is a serial ring. Keeping the same symbols, we find the elements $a_{i,i+1} \in A_{i,i+1}$ $(i = 1, ..., t-1)$ and $a_{t1} \in A_{t1}$, such that $A_{i,i+1} = a_{i,i+1}A_{i+1,i+1} = A_{ii}a_{i,i+1}$ $(i = 1, ..., t-1)$ and $A_{t1} = a_{t1}A_{11} = A_{tt}a_{t1}$. We set $p = a_{12} + a_{23} + ... + a_{t-1,t} + a_{t1}$. Clearly, $e_ip = pe_{i+1}$ $(i = 1, ..., t-1)$ and $e_1 = pe_t$. By proposition 10.7.9, A is a piecewise domain. Define the isomorphisms $\sigma_{i,i+1} : A_{ii} \to A_{i+1,i+1}$ $(i = 1, ..., t-1)$ by $\alpha_i a_{i,i+1} = a_i a_{i+1} \alpha_i^{\sigma_{i,i+1}}$. Analogously one can define the isomorphism σ_{t1}.

Using the (K.12.3) construction one can identify the rings A_{11}, ..., A_{tt} and assume that the automorphisms $\sigma_{12}, ..., \sigma_{t-1,t}$ are identity automorphisms of the discrete valuation ring A_{11} which we shall denote by $\mathcal{O}$. We denote by σ the automorphism σ_{t1}.

Let us set $e_i = e_{ii}$ $(i = 1, ..., t)$ and $e_{ij} = a_{i,j+1}...a_{j-1,j}$ for $i < j$. Clearly, the product $a_{i,i+1}...a_{t-1,t}a_{t1}a_{12}...a_{i-1,i} \in (e_{ii}Re_{ii})\backslash(e_{ii}Re_{ii})^2$. Denote this product by $e_{ii}\pi e_{ii}$ $(i = 1, ..., t)$. Let us set $a_{t1} = e_{tt}\pi e_{11}$ and $e_{jj}\pi e_{ii} =$

$e_{j,j+1}...e_{t-1,t}e_{tt}\pi e_{11}e_{12}...e_{i-1,i}$. It is not difficult to verify that the map which to the element

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1t} \\ \pi\alpha_{21} & \alpha_{22} & \dots & \alpha_{2t} \\ \dots & \dots & \dots & \dots \\ \pi\alpha_{t1} & \pi\alpha_{t2} & \dots & \alpha_{tt} \end{pmatrix} \in H_t(\mathcal{O})$$

assigns the element

$$\sum_{i\le j} e_{ii}\alpha_{ij}e_{ij} + \sum_{m<n} e_{nn}\pi e_{mm}\alpha_{nm}e_{mm},$$

is an isomorphism. The theorem is proved.

Using corollary 10.7.5, theorem 2.1.2 and proposition 2.1.3, we obtain the following corollary which yields the structure of Noetherian semiperfect prime hereditary rings.

Corollary 12.3.7. *Any prime Noetherian hereditary semiperfect ring is isomorphic to either the ring $M_n(D)$, where D is a division ring, or a ring of the form:*

$$\begin{pmatrix} M_{n_1\times n_1}(\mathcal{O}) & M_{n_1\times n_2}(\mathcal{O}) & \dots & M_{n_1\times n_t}(\mathcal{O}) \\ M_{n_2\times n_1}(\pi\mathcal{O}) & M_{n_2\times n_2}(\mathcal{O}) & \dots & M_{n_2\times n_t}(\mathcal{O}) \\ \dots & \dots & \dots & \dots \\ M_{n_t\times n_1}(\pi\mathcal{O}) & M_{n_t\times n_2}(\pi\mathcal{O}) & \dots & M_{n_t\times n_t}(\mathcal{O}) \end{pmatrix}$$

where $\mathcal{O}$ is a discrete valuation ring. Clearly, the above rings are serial hereditary Noetherian prime rings.

Therefore we have proved the following structural theorem for Noetherian serial rings.

Theorem 12.3.8. *Any serial Noetherian ring can be decomposed into a finite direct product of an Artinian serial ring and a number of semiperfect Noetherian prime hereditary rings. Conversely, all such rings are serial and Noetherian.*

Lemma 12.3.9. *If A is a semiperfect right (left) Noetherian ring with Jacobson radical R, then the quotient ring $\bar{A} = A/R^2$ is right (left) Artinian.*

Proof. Obviously, it is sufficient to prove the lemma for a right Noetherian ring. We shall show that the quotient ring $\bar{A} = A/R^2$ has a composition series. Indeed, if $\bar{R} = R/R^2$, then $\bar{A} \supset \bar{R} \supset 0$. Since $\bar{A}/\bar{R} \simeq A/R$, between $\bar{A}$ and $\bar{R}$ one can find only a finite chain of right ideals with simple factors. Since $\bar{R}$ is an A/R-module, it is semisimple. The ideal R is finitely generated and by Nakayama's lemma $\mu_A(\bar{R}) = \mu_A(R)$. Therefore in the decomposition of $\bar{R}$ there are only a finite number of simple modules. Hence $\bar{R}$ is an Artinian module and $\bar{A}$ is a right Artinian ring. The lemma is proved.

Since in the proof of theorem 12.3.8 we have used only the fact that the quiver of an indecomposable direct summand is either a chain or a cycle, taking into account lemma 12.3.9, we have proved the following theorem.

Theorem 12.3.10. *A semiperfect Noetherian ring is serial if and only if A/R^2 is a serial Artinian ring.*

Theorem 12.3.11. *A semiperfect Noetherian ring is serial if and only if its right and left quivers are disconnected unions of cycles and chains.*

Proof. Let R be the Jacobson radical of a semiperfect Noetherian ring A and let the right and left quiver of the ring A be disconnected unions of cycles and chains. Then the ring A/R^2 is a serial right (left) module and by theorem 12.3.10 the ring A is serial. The converse statement follows from theorem 12.1.2.

Remark. We have introduced the quiver of a serial ring A by $Q(A) = Q(A/R^2)$. Note that theorem 12.3.11 is not true even in the class of semiperfect right Noetherian rings. Let $\mathcal{O}$ be a local principal ideal domain with classical ring of fractions D, which is a division ring, and

$$A = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} \middle| \alpha \in \mathcal{O}, \beta \in D \times D, \gamma \in D \right\}.$$

Obviously,

$$R = \left\{ \begin{pmatrix} \alpha_1 & \beta_1 \\ 0 & 0 \end{pmatrix} \middle| \alpha_1 \in \mathcal{M}, \beta_1 \in D \times D \right\}$$

($\mathcal{M}$ is the unique maximal ideal of $\mathcal{O}$). So

$$R^2 = \left\{ \begin{pmatrix} \alpha_2 & \beta_2 \\ 0 & 0 \end{pmatrix} \middle| \alpha_2 \in \mathcal{M}^2, \beta_2 \in D \times D \right\}.$$

Hence it follows immediately that both the right and left quiver of the ring A is a disconnected union of a cycle and a point, but the ring A is not serial.

12.4 PROPERTIES OF SERIAL TWO-SIDED NOETHERIAN RINGS

In this section we shall assume that A is a serial two-sided Noetherian ring.

Lemma 12.4.1. *Let A be a serial reduced ring with radical R such that $R^2 = 0$. Then $R = pA = Ap$ (for some suitable p). Conversely, if the radical of a right Artinian ring A with $R^2 = 0$ has the form $R = pA = Ap$, then A is a serial ring.*

Proof. Let A be a serial reduced ring with the radical R such that $R^2 = 0$. Obviously, one may assume that the ring A cannot be decomposed into a direct product of rings, i.e., A is indecomposable. Indeed, if $A = A_1 \times A_2 \times ... \times A_t$ is a direct product of indecomposable rings A_1, A_2,..., A_t with Jacobson radicals

R_1, R_2,...,R_t and $R_i = p_iA = Ap_i$ for $i = 1, 2, ..., t$, then $R = pA = Ap$ where $p = p_1 + ... + p_t$. Thus, one can assume that the ring A is indecomposable. Then by theorem 11.1.9, proposition 12.1.1 and theorem 12.1.2 one may assume that the quiver of the ring A is either a cycle or a chain. In this case the left quiver of the ring A is either a cycle or a chain. If $Q(A)$ is a one-pointed cycle then the left quiver of A is a one-pointed cycle as well. Then R is a one-dimensional left and right space over A/R. Therefore $R = pA = Ap$. Let $1 = e_1 + ... + e_t$ be a decomposition of the identity of the ring A into a sum of pairwise orthogonal local idempotents ($t > 1$). Then if $Q(A)$ is a cycle, we can assume without loss of generality that $A_{12} \neq 0$, $A_{23} \neq 0$,..., $A_{t-1,t} \neq 0$, $A_{t1} \neq 0$ where $A_{ij} = e_iAe_j$ $(i, j = 1, 2, ..., t)$. Moreover, A_{ii} is obviously a division ring $(i = 1, ..., t)$. By the Q-Lemma all the remaining A_{ij} are equal to zero. Since A is a serial ring, it follows that $A_{i,i+1}$ is a one-dimensional left A_{ii}-space and a one-dimensional right $A_{i+1,i+1}$-space $(i = 1, ..., t-1)$, and A_{t1} is a one-dimensional left A_{tt}-space and a one-dimensional right A_{11}-space. Let $x_{i,i+1} \in A_{i,i+1}$ $(i = 1, ..., s-1)$, $x_{s1} \in A_{s1}$ be nonzero elements, and $x = x_{12} + x_{23} + ... + x_{s-1,s} + x_{s1}$. Then, obviously, $xA = R = Ax$. In a similar way, in the case of a chain, we obtain $R = Ax = xA$.

Conversely, assume that A is a right Artinian ring with the radical R such that $R^2 = 0$ and $R = pA = Ap$. Let the length of the module e_iR be equal to $m > 1$. Since e_iR is a cyclic module and the ring A is reduced (lemma 11.1.8), there are no isomorphic principal modules in the projective cover of e_iR. Therefore all simple modules, containing in the decomposition of the semisimple module e_iR, are distinct.

By the Q-Lemma, it follows from here that there exist numbers j_1, ..., j_m such that $e_iRe_{j_k} \neq 0$ and $e_iR^2e_{j_k} = 0$ for $k = 1, ..., m$. Let us consider Re_{j_k} $(k = 1, .., m)$. By the same lemma, a left simple module V_i is contained in the module Re_{j_k} as a direct summand. Hence the principal left A-module Ae_i is contained in the projective cover of the ideal R at least twice and therefore, by lemma 11.1.8 the ideal R is not left cyclic. The lemma is proved.

Corollary 12.4.2. *Let A be a serial two-sided Noetherian indecomposable ring. Then the endomorphism rings of all simple A-modules are all isomorphic.*

Proof. Obviously, the conditions of the corollary are not changed by passing to Morita equivalent rings. Therefore we shall consider that the ring A is reduced. A simple module U is a module over the ring A/R^2 which is Artinian and, by theorem 12.1.2, its quiver is either a cycle or a chain. Keeping the notations of lemma 12.4.1 we have $a_ix_{i,i+1} = x_{i,i+1}a_i^{\sigma_i}$ $(i = 1, ..., s-1)$, $a_sx_{s1} = x_{s1}a_s^{\sigma_s}$. Moreover, σ_i is an isomorphism of A_{ii} to $A_{i+1,i+1}$ $(i = 1, ..., s-1)$ and $\sigma_s : A_{ss} \to A_{11}$ is an isomorphism of A_{ss} to A_{11}. Since the A_{ii} are endomorphism rings of simple A-modules, they are all isomorphic.

Corollary 12.4.3. *A semiperfect two-sided Noetherian reduced ring A is serial if and only if its Jacobson radical R is both a right and left principal ideal.*

The proof follows immediately from lemma 12.4.1 and Nakayama's lemma.

Lemma 12.4.4. *Let A be a right Artinian indecomposable ring with the radical R. Suppose R is a right and left principal ideal and $R^2 = 0$. Let $A = P_1^{n_1} \oplus ... \oplus P_s^{n_s}$ be a decomposition of the ring into a direct sum of principal A-modules. Then the ring A is a serial ring and $n_1 = ... = n_s$.*

Proof. Let $1 = f_1 + ... + f_t$ be a decomposition of $1 \in A$ into a sum of pairwise orthogonal idempotents such that $f_i A = P_i^{n_i}$ $(i = 1, ..., s)$; $A = Q_1^{n_1} \oplus ... \oplus Q_s^{n_s}$, where $Q_i^{n_i} = Af_i$ $(i = 1, ..., s)$. Since R is a principal left ideal, A is a left Artinian ring. Consider the projective covers $P(P_iR)$ and $P(RQ_i)$. Let $P(P_iR) = \overset{m}{\underset{j=1}{\oplus}} P_j^{t_{ij}}$ and $P(RQ_i) = \overset{m}{\underset{j=1}{\oplus}} Q_j^{t'_{ij}}$. Clearly, if $t_{ij} = 0$, then $t'_{ji} = 0$ and vice versa. Consider the matrices $K = (t_{ij})$ and $K' = (t'_{ij})$. Let $\vec{a} = (a_1, ..., a_s)$ and $\vec{b} = (b_1, ..., b_s)$ be integral vectors. We shall say that $\vec{a} \leq \vec{b}$ if $a_i \leq b_i$ for $i = 1, ..., s$. By lemma 11.1.8 from the conditions of the lemma we obtain that $(n_1, ..., n_s)K \leq (n_1, ..., n_s)$ and $(n_1, ..., n_s)K' \leq (n_1, ..., n_s)$. But then $(n_1, ..., n_s)KK' \leq (n_1, ..., n_s)$. This means that $\sum\limits_{j,i=1}^{s} n_i t_{ij} t'_{jk} \leq n_k$ for any fixed k. Set $i = k$ and consider the sum $\sum\limits_{j=1}^{s} n_k t_{kj} t'_{jk}$. Obviously, this is not more than n_k. Therefore, $\sum\limits_{j=1}^{s} t_{kj} t'_{jk} \leq 1$ and hence $\sum\limits_{j=1}^{s} t_{kj} \leq 1$. Analogously, $\sum\limits_{j=1}^{s} t'_{jk} \leq 1$. Therefore the left quiver and the right quiver of the ring A are disconnected unions of cycles and chains and by theorem 12.3.11 the ring A is serial. Supposing the ring A to be indecomposable, we may assume that $Q(A)$ is either a cycle or a chain. If $Q(A)$ is a cycle, then $K = (t_{ij})$ where $t_{i,i+1} = 1$ for $i = 1, ..., s-1$, $t_{s1} = 1$, and the other t_{ij} are equal to zero. Since $(n_1, ...n_s)K \leq (n_1, ..., n_s)$, we have $n_s \leq n_1 \leq n_2 \leq ... \leq n_{s-1} \leq n_s$ and so $n_1 = n_2 = ... = n_s$. The case of a chain is treated analogously. The lemma is proved.

By theorem 12.3.10, taking into account the fact that the ring A is semiperfect, the statement of lemma 12.4.4 carries over to semiperfect two-sided Noetherian rings.

Remark. If the Jacobson radical of a reduced ring A is a right principal ideal, but not a left principal ideal, the ring A is not necessarily serial. As an example consider the algebra A of the matrices over a field k of the following form:

$$A = \begin{pmatrix} a & b & c \\ 0 & d & 0 \\ 0 & 0 & e \end{pmatrix}$$

where $a, b, c, d, e \in k$; then $radA = R = (e_{12} + e_{13})A$. At the same time $R \simeq$

$Ae_{11} \oplus Ae_{11}$ is not a left principal ideal, by lemma 11.1.8.

Definition. A ring A with Jacobson radical R is called **primary** if the quotient ring A/R is a simple Artinian ring.

A serial ring is called a **primary decomposable serial ring** if it is isomorphic to a finite direct product of primary rings.

Theorem 12.4.6. *For a semiperfect two-sided Noetherian ring A the following conditions are equivalent*:

(a) *A is a principal ideal ring;*

(b) *A is a primary decomposable serial ring;*

(c) *both the right and left quiver of A is a disconnected union of points and one-pointed cycles.*

Proof.

The implications $(a) \Rightarrow (b)$ and $(b) \Rightarrow (c)$ follow from theorems 12.1.2 and 12.2.1.

$(c) \Rightarrow (a)$. One may assume that A is an indecomposable ring. Then the quiver of A is either a point or a one-pointed cycle. If the quiver is a point, then the corresponding principal module is simple and $A \simeq M_n(D)$, where D is a division ring. Suppose that the quiver of the ring A is a one-pointed cycle. In this case $A = P^n$ and $P/PR \simeq PR/PR^2$. Clearly, in this case $Q/RQ \simeq RQ/R^2Q$, where Q is the unique principal left A-module. Hence, it follows that $P(PR) \simeq P$ and therefore $PR/PR^2 \simeq PR^2/PR^3$, $RQ/R^2Q \simeq R^2Q/R^3Q$. Continuing this process in the Artinian case we conclude that all simple factors of the modules P and Q are isomorphic. Therefore $A \simeq End_A A = M_n(End_A P)$ and the ring $End_A P$ is a local uniserial ring. If the ring A is not Artinian, then by theorems 12.3.9 and 12.3.4 $End_A P \simeq \mathcal{O}$, where $\mathcal{O}$ is a local principal ideal domain. Again $A \simeq M_n(\mathcal{O})$. In each case A is a principal ideal ring. The theorem is proved.

Remark. The rings considered in theorem 12.4.6 for the Artinian case were introduced for the first time by G.Köthe in his paper *Verallgemeinerte Abelsche Gruppen mit hyperkomplexen Operatorenring // Math. Z., v.39 (1934), p.29-44.* He used the term "Einreihig" for such rings. In the general case R.Warfield in his paper *Serial rings and finitely presented modules // J.Algebra, v. 37 (1975), p.187-222* used the term "homogeneously serial ring". We use the term "primary decomposable serial rings" for such rings.

12.5 NOTES AND REFERENCES

Artinian uniserial, or primary decomposable serial rings, were first introduced and studied by G.Köthe in the paper *G.Köthe, Verallgemeinerte Abelsche Gruppen mit Hyperkomplexen Operatorenring // Math. Z., v.39 (1935), p.31-44*, where he proved that any module over such a ring is a direct sum of cyclic modules (he

called such rings "Einreihige Ringen"). This result was generalized by T.Nakayama for Artinian serial rings, who called these rings "generalized uniserial rings", (see *T.Nakayama, On Frobeniusean algebras I,II // Ann. of Math., v.40 (1939), p.611-633; v.42(1941), p.1-21* and *Note on uniserial and generalized uniserial rings // Proc. Imp. Acad. Tokyo, v.16 (1940), p.285-289*). In these papers T.Nakayama proved that any module over such a ring is a direct sum of uniserial submodules each of which is a homomorphic image of an ideal generated by a primitive idempotent. T.Nakayama also showed that, conversely, these are the only rings whose indecomposable finitely generated modules (both left and right) are homomorphic images of ideals generated by primitive idempotents.

Artinian principal ideal rings were studied in papers of G.Köthe and K.Asano (see *K.Asano, Über verallgemeinerte Abelsche Gruppen mit hyperkomplexen Operatorenring und ihre Anwendungen // Japan J. Math., v.15 (1939), p.231-253* and *K.Asano, Über Hauptidealringe mit Kettensatz // Osaka Math. J., v.1 (1949), p.52-61*), where it was proved that any Artinian principal right ideal ring is right uniserial. In fact, K.Asano proved that an Artinian ring is uniserial if and only if each ideal is a principal right ideal and a principal left ideal. The classical proof of this theorem is given in the book of N.Jacobson *The theory of rings. Amer. Math. Soc., v.2, Surveys, New Jork, 1943.* For such rings K.Asano also proved an analogue of the Wedderburn-Artin theorem, namely, he proved that any Artinian uniserial ring can be decomposed into a direct sum of full matrix rings of the form $M_n(A)$, where A is a local Artinian ring with a cyclic radical. A one-sided characterization of Artinian principal ideal rings and its connection with primary decomposable serial rings is given in theorem 2.1 of the paper *D.Eisenbud, P.Griffith, The structure of serial rings // Pacific J. Math., v.36, N1, 1971, p.109-121*). So theorems 12.2.2 and 12.4.6 can be considered as a generalization of these theorems for the case of semiperfect rings.

L.A.Skornyakov studied serial rings, which he called "semi-chain rings", in his paper *When are all modules semi-chained? // Mat. Zametki, v.5, 1969, p.173-182.* He proved there that A is a right and left Artinian serial ring if and only if every left A-module is a direct sum of uniserial modules. His result generalizes a theorem proved by K.R.Fuller (see *On indecomposable injectives over artinian rings // Pacific J. Math., v. 29, 1969, p.115-135*), to the effect that if each left module over a ring A is a direct sum of uniserial modules, then A is a serial left Artinian ring.

With each serial Artinian indecomposable ring one can associate a series of principal modules, first studied by H.Kupisch (see *Beiträge zur Theorie nichthalbeinfacher Ringe mit Minimalbedingung // Crelles Journal, v.201, 1959, p.100-112*), and later by I.Murase in his classification of these rings (see *On the structure of generalized uniserial rings. I, II, III // Sci. Pap. Coll. Gen. Educ., Univ. Tokyo, v. 13, 1963, p.1-13; v. 13, 1963, p. 131-158; v.14, 1964, p. 11-25*). The generalization of Murasa's results was obtained in the papers of D.Eisenbud and P.Griffith, where the full description, in module-theoretic terms, of the structure

of serial Artinian rings is given (see *D.Eisenbud, P.Griffith, Serial rings // J. Algebra, v.17, 1971, p.389-400* and *D.Eisenbud, P.Griffith, The structure of serial rings // Pacific J. Math., v.36, N1, 1971, p.109-121*). H.Kupisch obtained a description of serial Artinian algebras over an algebraically closed field in his paper *Beiträge zur Theorie nichthalbeinfacher Ringe mit Minimalbedingung // Crelles Journal, v.201, 1959, p.100-112* and in the general case in the paper *Über eine Klasse von Ringen mit Minimalbedingung I., Arch. Math., v.17, 1966, p. 20-35.*

The paper of G.Ivanov *Left Generalized Uniserial Rings // J. Algebra, v. 31, 1974, p.166-181* gives a description of the two-sided Peirce decomposition of left serial rings.

Theorem 12.3.4, which gives the full description of semiperfect two-sided Noetherian and hereditary prime rings using the technique of quivers, was first proved by G.Michler in his paper *Structure of semi-perfect hereditary Noetherian rings // J. Algebra, v. 13, N.3, 1969, p.327-344.*

Local Noetherian and hereditary rings were studied by P.M.Cohn (see *Hereditary local rings // Nagoya Math. J., v.27, N1, 1966, p.223-230*) and A.Zaks (see *Hereditary local rings // Michigan Math. J., v.17, 1970, p.267-272*).

The first serial non-Artinian rings were studied and described by R.B.Warfield and V.V.Kirichenko. In particular, they gave a full description of the structure of serial Noetherian rings.

In this chapter we have followed the papers *V.V.Kirichenko, Generalized uniserial rings // Preprint IM-75-1, Kiev, 1975* and *V.V.Kirichenko, Generalized uniserial rings // Mat. sb. v.99(141), N4 (1976), p.559-581*, where the technique of quivers was used systematically.

Using a different approach to the study of serial Noetherian rings, analogous results about the structure of such rings to those presented in this chapter, were obtained simultaneously and independently by R.B.Warfield in his paper: *R.B.Warfield, Serial rings and finitely presented modules // J. Algebra, v. 37 (1975), p.187-222.*

The readers are also recommended to look at the book *C.Faith, Algebra II: Ring Theory, chapter 25*, where the results of this chapter are presented using the approach of R.B.Warfield.

13. Serial rings and their properties

13.1. FINITELY PRESENTED MODULES

In this section we give a method for describing finitely presented modules over a semiperfect ring A.

Definition. A module M is called **finitely presented** if it is finitely generated and there is an epimorphism ψ of a finitely generated projective module P onto the module M such that $Ker\psi$ is a finitely generated module.[1])

In view of lemma 10.4.4 to show that a module M over a semiperfect ring is finitely presented it is sufficient to verify that M is finitely generated and the module $Ker\pi$ is finitely generated as well, where $\pi : P(M) \to M$ is the epimorphism of the projective cover $P(M)$ to M.

Let M be a finitely presented module over a semiperfect ring A. Write $P_0 = P(M)$, $X = Ker\pi_0$, $P = P(X)$ and $\pi : P \to X$. In this case we have an exact sequence: $P \xrightarrow{\pi} P_0 \xrightarrow{\pi_0} M \longrightarrow 0$.

Lemma 13.1.1. *If $P \xrightarrow{\pi} P_0 \xrightarrow{\pi_0} M \to 0$ and $Q \xrightarrow{f} Q_0 \xrightarrow{f_0} M \to 0$ are two exact sequences, where P_0 and Q_0 are projective covers of the module M, and P (resp. Q) is the projective cover of $Ker\pi_0$ (resp. $Kerf_0$), then there is a commutative diagram*

$$\begin{array}{ccccccc} P & \xrightarrow{\pi} & P_0 & \xrightarrow{\pi_0} & M & \longrightarrow & 0 \\ \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\varphi_0} & & \downarrow{\scriptstyle 1_M} & & \\ Q & \xrightarrow{f} & Q_0 & \xrightarrow{f_0} & M & \longrightarrow & 0 \end{array}$$

where φ_0 and φ are isomorphisms.

Proof. By the definition of a projective module, there is a homomorphism φ_0 such that $\pi_0 = f_0\varphi_0$. We shall show that φ_0 is an isomorphism. For any element $q_0 \in Q_0$ there exists an element $p_0 \in P_0$ such that $f(q_0) = \pi_0(p_0)$. Since $q_0 = q_0 - \varphi_0(p_0) + \varphi_0(p_0)$, where $q_0 - \varphi_0(p_0) \in Ker(f_0)$, we obtain $Q_0 = Im\varphi_0 + Kerf_0$. By the definition of projective cover $Ker(f_0)$ is small and so $Im\varphi_0 = Q_0$. Therefore by proposition 5.1.6 $P_0 \simeq Im\varphi_0 \oplus Ker\varphi_0$ and, due to the uniqueness of a projective cover, $Ker\varphi_0 = 0$, i.e., φ_0 is an isomorphism. Write $Y = Kerf_0$. Clearly, $Im(\varphi_0\pi_0) = Y$. Since $Imf = Y$, by the definition of a projective module, there is a homomorphism $\varphi : P \to Q$ such that $\varphi_0\pi = f\varphi$. Applying the assertions mentioned above to the module Y and taking into account that Q is a projective cover of Y, we conclude that φ is an isomorphism. The lemma is proved.

[1]) Equivalently M is a quotient of a finitely generated free module with finitely generated kernel.

Let P and P_0 be finitely generated projective A-modules and let $\pi : P \to P_0$ be a homomorphism such that $Im\pi \subset P_0R$ and $Ker\pi \subset PR$. Clearly, the module $M_\pi = P_0/Im\pi$ is a finitely presented module. Moreover, P_0 is the projective cover of the module M_π and P is the projective cover of the module $Im\pi$. If $\varphi : P \to Q$ and $\varphi_0 : P_0 \to Q_0$ are isomorphisms then we have $M_{\varphi_0\pi\varphi^{-1}} \simeq M_\pi$. Conversely, if $\pi : P \to P_0$ is the homomorphism indicated above and $f : Q \to Q_0$ is a homomorphism such that $Imf \subset Q_0R$, $Kerf \subset QR$ and $M_\pi \simeq M_f$, then, by lemma 13.1.1, $f = \varphi_0\pi\varphi^{-1}$. Any finitely generated projective module over a semiperfect ring A uniquely decomposes into a direct sum of principal ones. Let P and P_0 be finitely generated projective A-modules with decompositions $P = P_1^{k_1} \oplus ... \oplus P_s^{k_s}$, $P_0 = P_1^{m_1} \oplus ... \oplus P_s^{m_s}$ into direct sums of principal A-modules and let $\pi : P \to P_0$ be a homomorphism.

The homomorphism π can be written in the form of a matrix $[\pi]$ with elements in $Hom_A(P_j^{k_j}, P_i^{m_i})$ $(i, j = 1, 2, ..., s)$, where $Hom_A(P_j^{k_j}, P_i^{m_i})$ is a $m_i \times k_j$ matrix with entries in $Hom_A(P_j, P_i)$. Let $e_1, ..., e_s$ be pairwise orthogonal local idempotents of the decomposition of $1 \in A$ into a sum of pairwise orthogonal idempotents and $P_i \simeq e_iA$ $(i = 1, ..., s)$. Then $Hom_A(P_j, P_i) \simeq e_iAe_j$. Therefore one can assume that $[\pi]$ is a block matrix with elements in e_iAe_j $(i, j = 1, ..., s)$. Divide the matrix $[\pi]$ (permuting rows and columns if necessary) into s horizontal and s vertical strips so that in the block of intersection of i-th horizontal and j-th vertical strips there are the elements from e_iAe_j.

Let us clarify the conditions which such a matrix $[\pi]$ must satisfy so that $P_0 = P(M_\pi)$ and $P = P(Im\pi)$. Since $P_0 = P(M_\pi)$, it follows that $[\pi]$ is a block matrix with elements in e_iRe_j $(i, j = 1, ..., s)$. Recall that since the modules $P_1, ..., P_s$ are pairwise non-isomorphic, $e_iRe_j = e_iAe_j$ $(i \neq j)$. Then one can assume that $P = P(Im\pi)$. In fact, this reduces to the fact that some columns may be thrown out of the matrix $[\pi]$.

If a finitely presented module M is decomposable and $M = M_1 \oplus M_2$, then $P_0 = P(M_1) \oplus P(M_2)$ and $M = P(M_1)/X_1 \oplus P(M_2)/X_2$ where $Ker\pi_0 = X_1 \oplus X_2$. Then $Im\pi = X_1 \oplus X_2$ and $P(Im\pi) = P(X_1) \oplus P(X_2)$. Hence it immediately follows that the matrix $[\pi]$ has block-diagonal form.

Lemma 13.1.2. *A finitely presented module $M = M_\psi$ is decomposable if and only if for a homomorphism $\psi : Q \to P$ of finitely generated projective modules such that $Im\psi \subset PR$ and Q is a projective cover of $Im\psi$ there exist automorphisms α and β of modules Q and P such that $[\beta\psi\alpha]$ is a block-diagonal matrix.*

Proof. Suppose there exist automorphisms α and β of modules Q and P such that $[\beta\psi\alpha]$ is a block-diagonal matrix. Then $M_\psi \simeq M_{\beta\psi\alpha}$ and since the homomorphism $\beta\psi\alpha : Q \to P$ satisfies the same conditions as ψ, the module $M_{\beta\psi\alpha}$ is decomposable in accordance with the decomposition of the matrix $[\beta\psi\alpha]$.

Conversely, let the module M be decomposable. Then we consider the com-

mutative diagram:

$$\begin{array}{ccccccc} Q & \xrightarrow{\psi} & P & \xrightarrow{\theta} & M & \longrightarrow & 0 \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow & & \\ P(X_1)\oplus P(X_2) & \xrightarrow{\pi} & P(M_1)\oplus P(M_2) & \xrightarrow{\nu} & M_1\oplus M_2 & \longrightarrow & 0 \end{array}$$

which exists by lemma 13.1.1. Clearly, $\pi = \beta\psi\alpha^{-1}$. Fix isomorphisms $\alpha_0 : Q \to P(X_1) \oplus P(X_2)$ and $\beta_0 : P \to P(M_1) \oplus P(M_2)$. We set $Q_i = \alpha_0^{-1}P(X_i)$ and $P_i' = \beta_0^{-1}P(M_i)$ $(i = 1, 2)$. Then $\beta_0^{-1}\pi\alpha_0 = \beta_0^{-1}\beta\psi\alpha^{-1}\alpha_0$ where $\alpha^{-1}\alpha_0$ and $\beta_0^{-1}\beta$ are automorphisms of modules Q and P. Moreover, the homomorphism $\beta_0^{-1}\beta\psi\alpha^{-1}\alpha_0 : Q_1 \oplus Q_2 \to P_1' \oplus P_2'$ is obviously block-diagonal. The lemma is proved.

Now we turn our attention to the study of automorphisms of finitely generated modules over a semiperfect ring.

Let $\mathcal{O}$ be a local ring with unique maximal ideal $\mathcal{M}$.

Any automorphism of a finitely generated projective $\mathcal{O}$-module P is given by an invertible[2]) matrix B of order n with elements in the ring $\mathcal{O}$.[3])

Consider the following elementary matrices over $\mathcal{O}$

$$T_{ij}(\alpha) = E + \alpha e_{ij}$$

$$D_i(\gamma) = E - e_{ii} + \gamma e_{ii}$$

where $i \neq j$, the e_{ij} are the matrix units of the ring $M_n(\mathcal{O})$, $E = e_{11}+e_{22}+...+e_{nn}$ is the identity matrix, $\alpha \in \mathcal{O}$ and γ is a unit in $\mathcal{O}$.

An automorphism of a module P, corresponding to an elementary matrix, is called **elementary automorphism**. Multiplications on the left (right) side of a matrix B by elementary matrices correspond to **elementary row (column) operations** on the matrix B.

Proposition 13.1.3. *Any invertible matrix B over a local ring $\mathcal{O}$ can be reduced by elementary row (columns) operations on B to the identity matrix.*

Proof. We shall carry out the proof for the case of elementary row operations. Since all elementary matrices are invertible, after elementary row operations the newly obtained matrix will be invertible as well.

First, suppose that $b_{11} \notin \mathcal{M}$. Multiplying the first row on the left by b_{11}^{-1} we obtain at position $(1, 1)$ the identity of the ring $\mathcal{O}$. After that by elementary row

[2]) Invertible over $\mathcal{O}$.

[3]) Because each finitely generated projective module over a local rings is free, see theorem 10.1.8.

operations we reduce the matrix B to the form:

$$B = \begin{pmatrix} 1 & | & * \\ - & - & - \\ 0 & | & \\ 0 & | & B_1 \\ \vdots & | & \\ 0 & | & \end{pmatrix}$$

The matrix B_1 is obviously invertible and by induction it can be reduced to the identity matrix. But then, clearly, the first row entries except the first one, which remains fixed can be made zeroes.

If $b_{11} \in \mathcal{M}$, then as B is invertible, there exists an element $b_{j1} \notin \mathcal{M}$ $(j \neq 1)$. Adding to the first row the j-th one we obtain at the position $(1,1)$ an invertible element from $\mathcal{O}$. This reduces things to the previous case. The proposition is proved.

Corollary 13.1.4. *An invertible matrix B over a local ring $\mathcal{O}$ can be decomposed into a product of elementary matrices.*

The proof of this corollary and the next one is obvious.

Corollary 13.1.5. *A matrix $B = (b_{ij})$ over a local ring $\mathcal{O}$ is invertible if and only if the matrix $\bar{B} = (\bar{b}_{ij})$ is invertible, where $\bar{b}_{ij} = b_{ij} + \mathcal{M}$.*

Consider the matrix $[\psi]$ corresponding to an automorphism ψ of a finitely generated module $P = P_1^{k_1} \oplus ... \oplus P_s^{k_s}$. As above

$$[\psi] \in \begin{pmatrix} M_{n_1 \times n_1}(e_1 A e_1) & M_{n_1 \times n_2}(e_1 A e_2) & \dots & M_{n_1 \times n_s}(e_1 A e_s) \\ M_{n_2 \times n_1}(e_2 A e_1) & M_{n_2 \times n_2}(e_2 A e_2) & \dots & M_{n_2 \times n_s}(e_2 A e_s) \\ \dots & \dots & \dots & \dots \\ M_{n_s \times n_1}(e_s A e_1) & M_{n_s \times n_2}(e_s A e_2) & \dots & M_{n_s \times n_s}(e_s A e_s) \end{pmatrix}$$

where the rings $\mathcal{O}_i = e_i A e_i$ are local by theorem 10.3.8. We shall show that the matrix $[\psi_i]$ consisting of all elements of the matrix $[\psi]$ from $M_{n_i}(e_i A e_i)$ is invertible for all $i = 1, ..., s$. If it is not the case, after some elementary transformation of rows one obtains that in some row of the matrix $[\psi_i]$ all elements will belong to $\mathcal{M}_i$, where $\mathcal{M}_i$ is the unique maximal ideal of $\mathcal{O}_i$. The new matrix also corresponds to an automorphism θ of the module P. Let $[\theta^{-1}]$ be a matrix corresponding to the automorphism θ^{-1}. Then $[\theta][\theta^{-1}] = diag(e_1, ..., e_1, e_2, ..., e_2, ..., e_s, ..., e_s)$, where the element e_i appears n_i times $(i = 1, ..., s)$ along the main diagonal. From the form of the matrix θ we obtain $e_i \in R$; but that is impossible. Indeed, $e(1-e) = 0$, where $1 - e$ is an invertible element. Therefore $e = 0$. Hence all the matrices $[\psi_i]$ are invertible.

As above one can prove the following theorem.

Theorem 13.1.6. *Any matrix $[\psi]$, corresponding to an automorphism ψ of a finitely generated projective module P, can be decomposed into a product of elementary matrices. Any automorphism ψ can be decomposed into a product of elementary automorphisms.*

13.2. THE DROZD-WARFIELD THEOREM. THE ORE CONDITION FOR SERIAL RINGS

In this section we aim to prove a theorem characterizing serial rings in terms of finitely presented modules and we shall discuss the Ore condition for serial rings.

Theorem 13.2.1 (Yu.A.Drozd-R.B.Warfield). *For a ring A the following conditions are equivalent:*

(1) *A is serial;*

(2) *any finitely presented right A-module is serial;*

(3) *any finitely presented left A-module is serial.*

Proof.

(1) $\Rightarrow$ (2). As was shown above any finitely presented A-module is isomorphic to the cokernel of a homomorphism $f : P \to Q$, where P and Q are finitely generated projective modules. Decompose the modules P and Q into direct sums of principal A-modules: $P = P_1^{k_1} \oplus ... \oplus P_s^{k_s}$, $Q = P_1^{m_1} \oplus ... \oplus P_s^{m_s}$. Then the homomorphism f can be described by a matrix

$$[\psi] = \begin{pmatrix} \psi_{11} & \dots & \psi_{1n} \\ \dots & \dots & \dots \\ \psi_{m1} & \dots & \psi_{mn} \end{pmatrix},$$

where the elements ψ_{ij} are homomorphisms of the principal modules P_j and P_i.

We are going to show that there exist automorphisms $\alpha : P \to P$ and $\beta : Q \to Q$ such that $\beta f \alpha : P \to Q$ can be described by a diagonal matrix $[g] = (g_{ij})$. I.e., $g_{ij} = 0$ if $i \neq j$ for a suitable numbering of the principal modules.

We carry out the proof by induction on $m + n$ where it can be assumed that $m \leq n$. We shall show that the matrix $[\psi]$ can be reduced by elementary operations to a diagonal form. The basis of induction, $m + n = 2$, is trivial.

Suppose that the statement has been already proved for all numbers less than $m + n$. The matrix consisting of the first $m - 1$ rows of the matrix $[\psi]$ by the induction hypothesis can be reduced to diagonal form, so that $[\psi]$ can be reduced to something of the form:

$$[\psi] = \begin{pmatrix} \psi_{11} & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & \psi_{22} & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \psi_{m-1,m-1} & 0 & \dots & 0 \\ \psi_{m1} & \psi_{m2} & \dots & \psi_{m,m-1} & \psi_{mm} & \dots & \psi_{mn} \end{pmatrix}$$

If for some j the equation $\psi_{mj} = x\psi_{jj}$ is solvable, then applying the corresponding elementary row operation to the matrix $[\psi]$, we obtain $\psi_{mj} = 0$. Otherwise, by proposition 12.3.1, there exists a $x_j : P_m \to P_j$ such that $\psi_{jj} = x_j\psi_{mj}$. From the same proposition it follows that there exists a number k such that $\psi_{mj} = \psi_{mk}y_j$ for all $j \neq k$. Again applying the corresponding elementary row and column operations on the matrix $[\psi]$ we reduce it to the form:

$$[\psi] = \begin{pmatrix} & & & 0 & & & \\ & * & & \vdots & & * & \\ & & & 0 & & & \\ 0 & \dots & 0 & \psi_{mn} & 0 & \dots & 0 \end{pmatrix}$$

To finish the proof we use the induction hypothesis.

(2) $\Rightarrow$ (1). The ring A is automatically right serial. If it is not left serial, then by proposition 12.3.1 there exist two homomorphisms of principal right A-modules $\psi_i : P \to P_i$ $(i = 1, 2)$ such that equations $\psi_1 = x\psi_2$ and $\psi_2 = y\psi_1$ cannot be solved. Let $\psi : P \to P_1 \oplus P_2$ be a homomorphism given by the matrix $[\psi] = \begin{pmatrix} \psi_1 \\ \psi_2 \end{pmatrix}$. Clearly, ψ satisfies the condition of lemma 13.1.2. By theorem 13.1.6 the matrix ψ is indecomposable. Hence the module $(P_1 \oplus P_2)/Im\psi$ is indecomposable and it is not uniserial.

The remaining implications are proved exactly in the same way.

The theorem is proved.

Theorem 13.2.2. *Every serial ring satisfies the Ore condition, i.e., every serial ring has the classical ring of fractions.*

To prove this theorem, the following two lemmas will be used.

Suppose A is a serial ring. Denote by $N_{ij}^l (N_{ij}^r)$ the set of all elements of A_{ij} which have nonzero right (left) annihilators; $N_{ij} = N_{ij}^l + N_{ij}^r$, $X_{ij} = A_{ij} \backslash N_{ij}$. Clearly, $e_i \in X_{ii}$ for $i = 1, \dots, n$. Besides, we have $X_{ij}X_{ji} \subseteq X_{ii}$ for $i, j = 1, \dots, n$. Indeed, if $x_{ij}x_{ji}a = 0$ for $a \in A_{ik}$, then $x_{ji}a \in A_{jk}$, and since $x_{ij} \in X_{ij}$, then $x_{ji}a = 0$ and therefore $a = 0$. Exactly in the same way from $bx_{ij}x_{ji} = 0$ $(b \in A_{ki})$ it follows that $b = 0$.

Lemma 13.2.3. *The set N_{ij} is an A_{ii}-A_{jj}-bimodule. If $x_{ij}x_{ji} \in X_{ii}$ where $x_{ij} \in A_{ij}$, $x_{ji} \in A_{ji}$ then $x_{ij} \in X_{ij}$ and $x_{ji} \in X_{ji}$.*

Proof. To prove that N_{ij} is an A_{ii}-A_{jj}-bimodule it suffices to show that N_{ij}^l and N_{ij}^r are both A_{ii}-A_{jj}-bimodules. Let $m \in N_{ij}^l$ have a nonzero right annihilator $0 \neq z \in A_{jk}$. Then for every $a \in A_{ii}$ we have $amz = 0$, i.e., $am \in N_{ij}^l$. Let us show that for every $b \in A_{jj}$ the element mb belongs to N_{ij}^l. Consider the right ideals zA and bA. They are submodules of the uniserial module e_jA. Thus either

$zA \supset bA$, or $zA \subset bA$. The first case yields relations $b = zc$ and $mb = mzc = 0$, the second one gives $z = by$ and $mz = mby = 0$, i.e., $mb \in N_{ij}^l$.

Let $x_{ij}x_{ji} \in X_{ii}$ and $x_{ij} \in N_{ij}$. Assume $x_{ij} \in N_{ij}^l$. Then there exists $0 \neq y \in A_{jk}$ such that $x_{ij}y = 0$. Consider the right ideals $x_{ji}A$ and yA. As above either $x_{ji}A \supset yA$, or $yA \supset x_{ji}A$. If $x_{ji}A \supset yA$, then $y = x_{ji}b$ and $x_{ij}x_{ji}b = 0$, and therefore $b = 0$ and $y = 0$. If $yA \supset x_{ji}A$, then $x_{ji} = ya$ and $x_{ij}x_{ji} = x_{ij}ya = 0$. This contradiction proves that $x_{ij} \in X_{ij}$.

Lemma 13.2.4. *For any $a \in A$ and $x = x_1 + ... + x_n$, $x_i \in X_{ii}$, there exist $y = y_1 + ... + y_n$, $y_i \in X_{ii}$, and $b \in A$ such that $ay = xb$.*

Proof. Set $a_{ij} = e_iae_j$. Let us show that for every a_{ij} there exists a $k_j^{(i)} \in X_{jj}$ such that $a_{ij}k_j^{(i)} \in x_iA$. Consider the right ideals x_iA and $a_{ij}A$. If $a_{ij}A \subset x_iA$, then $a_{ij}e_j \in x_iA$, where $e_j \in X_{jj}$. If $x_iA \subset a_{ij}A$, then $x_i = a_{ij}a_{ji}$. By lemma 13.2.3, $a_{ij} \in X_{ij}$ and $a_{ji} \in X_{ji}$. Hence, $a_{jj} = a_{ji}a_{ij} \in X_{jj}$ and $a_{ij}a_{jj} = a_{ij}a_{ji}a_{ij} = x_ia_{ij}$. Set $k_j^{(i)} = a_{jj}$. Let us consider the right ideals $k_j^{(i)}A$, $i = 1, \ldots, n$. These ideals are linearly ordered, and suppose $k_j^{(i_0)}A$ is the least of them. Write $y_j = k_j^{(i_0)}$. Obviously, $a_{ij}y_j \in x_iA$ for $i = 1, \ldots, n$. Let us set $y = y_1 + \cdots + y_n$. Clearly $ay = xb$. The proof of the lemma is completed.

Proof of theorem 13.2.2. We shall show how the statement of theorem 13.2.2 follows from lemmas 13.2.3 and 13.2.4. Let us prove that for any $a \in A$ and any regular element $r \in A$ there exists a regular element $y \in A$ and an element $b \in A$ such that $ay = rb$. By theorem 13.2.1, there exist invertible elements k_1 and k_2 such that in the two-sided Peirce decomposition of the element k_1rk_2 in any row and any column there exists exactly one nonzero element belonging to X_{ij} for some i and j. Therefore for some positive integer n the element $(k_1rk_2)^n = x = k_1rb_1$ is of diagonal form and its diagonal elements lie in X_{ii}.

Let us consider the elements k_1a and x. By lemma 13.2.4 there exists a "diagonal" regular element $y \in A$ and a $b \in A$ such that $k_1ay = xb$. Hence, $k_1ay = k_1rb_1b$, and therefore $ay = rb_1b$. The proof of theorem is complete.

Remark. Obviously, the classical ring of fractions of a serial ring is also a serial ring.

13.3. MINORS OF SERIAL RIGHT NOETHERIAN RINGS

Let A be a ring, P a finitely generated projective A-module which can be decomposed into a direct sum of n indecomposable modules. The endomorphism ring $B = End_A(P)$ of the module P is called a **minor** of order n of the ring A.

Many properties of a ring are reflected by its minors. By theorem 10.3.8 a ring is semiperfect if and only if any minor of the first order of this ring is semiperfect (or what is the same, is local).

From theorem 3.6.1 it immediately follows that minors of (right) Noetherian, (right) Artinian rings are (right) Noetherian, (right) Artinian, respectively. By corollary 12.3.2 the ring is serial if and only if all its minors of order three are serial.

The next goal is to describe serial right Noetherian rings. To this end we are going to describe minors of the first and second order of serial right Noetherian rings. It will be shown that they are either uniserial right Noetherian, or serial right Noetherian rings, whose identity decomposes into a sum of two local idempotents.

Proposition 13.3.1. *A local right Noetherian ring $\mathcal{O}$ is serial if and only if it is either a discrete valuation ring or an Artinian uniserial ring.*

Proof. Obviously, a discrete valuation ring is a serial two-sided Noetherian ring.

Let $\mathcal{O}$ be a local serial (so uniserial) right Noetherian ring with unique maximal ideal $\mathcal{M}$. Since $\mathcal{M}$ is strictly contained in $\mathcal{M}^2$ and the quotient module $\mathcal{M}/\mathcal{M}^2$ is simple, $\mathcal{M} = \pi\mathcal{O}$ by Nakayama's lemma, where π is any element of $M\backslash M^2$. Note that $\mathcal{M}/\mathcal{M}^2$ is a simple left module as well. Obviously, $\mathcal{M} \supset \mathcal{O}\pi \supset \mathcal{M}^2$. But then $\mathcal{M} = \mathcal{O}\pi$. Denote also by π the endomorphism of $\mathcal{O}$ of multiplication on the right side by π. Let $N = \bigcap\limits_{n=0}^{\infty} \mathcal{M}^n$. If the endomorphism π is nilpotent then by proposition 12.1.1 $\mathcal{O}$ is an Artinian uniserial ring. Suppose that π is not nilpotent. We shall prove that in this case $Ker(\pi) = 0$. Suppose $Ker(\pi) \neq 0$, $x \in Ker(\pi)$, $x \neq 0$. Let us show that $Ker(\pi) \subset N$. If this is not the case, then there is a natural number m such that $\mathcal{M}x\mathcal{O} = \mathcal{O}\pi x\mathcal{O} = 0$ and $\mathcal{M}x\mathcal{O} = \mathcal{M}^{m+1}$. Therefore $\mathcal{M}^{m+1} = 0$, which contradicts the hypothesis. Therefore $x = \pi^n x_n$ for any positive integer n for a suitable x_n. Clearly, $x_n \in Ker(\pi^{n+1})$ but $x_n \notin Ker(\pi^n)$. Therefore there is a strictly increasing chain of two-sided ideals:

$$0 \subset Ker(\pi) \subset Ker(\pi^2) \subset ... \subset Ker(\pi^n) \subset Ker(\pi^{n+1}) \subset ...$$

Since the ring $\mathcal{O}$ is right Noetherian, we obtain a contradiction. Therefore $Ker\pi = 0$. Let us show that $N = 0$. Passing to the quotient ring $\mathcal{O}/(N\mathcal{M})$ if necessary, one can assume that in the initial ring $\mathcal{O}$ there holds $N\mathcal{M} = 0$. Consider the set $N' = \{n' \in \mathcal{O} | \pi n = n'\pi, n \in N\}$. Clearly, $N' \neq 0$. We shall show that N' is a two-sided ideal. If $n' \in N'$, then there exists $n \in N$ such that $n'\pi = \pi n$. Then $n'a\pi = n'\pi a' = \pi na'$ and since $na' \in N$, also $n'a \in N'$. Analogously N' is a left ideal. Let us show that $N' \subseteq N$. Obviously, $\pi N = N'\pi = N'\mathcal{O}\pi = N'\mathcal{M}$. If $N' \not\subseteq N$, then there exists a natural number t such that $N' \supset \mathcal{M}^t$. Therefore $N'\mathcal{M} \supset \mathcal{M}^{t+1}$ which contradicts the inclusion $N'\mathcal{M} \subseteq N$. Therefore $N' \subseteq N$. Since N' is a submodule of the simple module N, we have $N'\mathcal{M} = 0$ which contradicts the equality $Ker(\pi) = 0$. So all ideals (right, left, two-sided) of the ring $\mathcal{O}$ are natural powers of the ideal $\mathcal{M}$. Since $Ker(\pi) = 0$, we conclude that $\mathcal{O}$ is a discrete valuation ring. The proposition is proved.

Let $\mathcal{O}$ be a discrete valuation ring (not necessary commutative) with a classical

ring of fraction D which is a division ring. Denote by $H_m(\mathcal{O})$ the ring of $m \times m$ matrices of the following form:

$$H_m(\mathcal{O}) = \begin{pmatrix} \mathcal{O} & \mathcal{O} & \dots & \mathcal{O} \\ \mathcal{M} & \mathcal{O} & \dots & \mathcal{O} \\ \dots & \dots & \dots & \dots \\ \mathcal{M} & \mathcal{M} & \dots & \mathcal{O} \end{pmatrix}$$

($\mathcal{M}$ is the unique maximal ideal in $\mathcal{O}$). We shall also use the ring of matrices $H(\mathcal{O}, m, n)$ of the form

$$H(\mathcal{O}, m, n) = \begin{pmatrix} H_m(\mathcal{O}) & X \\ 0 & T_n(D) \end{pmatrix},$$

where $T_n(D)$ is the ring of upper triangular matrices of order n over the division ring D, and X is a set of all rectangular matrices of size $m \times n$ over the division ring D.

Lemma 13.3.2. *$H(\mathcal{O}, m, n)$ is a serial right Noetherian ring.*

Proof. The proof immediately follows from theorem 3.6.1 and corollary 12.3.2.

Lemma 13.3.3. *Let A be a serial ring, $1 = e + f$, where e and f are idempotents of A. Then eAf is a right serial fAf- (resp. left eAe-) module. In particular, if e (resp. f) is a local idempotent, then eAf is a uniserial right fAf- (resp. left eAe-) module.*

Proof. We carry out the proof for right modules. Let $1 = e_1 + ... + e_s + f_1 + ... + f_t$ be a decomposition of $1 \in A$ into a sum of pairwise orthogonal local idempotents, with, moreover, $e_1 + ... + e_s = e$ and $f_1 + ... + f_t = f$. Obviously, $eAf = \overset{s}{\underset{i=1}{\oplus}} e_iAf$. Let us show that e_iAf is a uniserial right fAf-module. Suppose that this is not the case. Then there exist fAf-submodules M_1 and M_2 belonging to e_iAf which are not contained one in the other. Then $\tilde{M}_1 = (M_1fAe,\ M_1)$ and $\tilde{M}_2 = (M_2fAe,\ M_2)$ are submodules of e_iA which are not contained one in the other. The lemma is proved.

Lemma 13.3.4. *The right uniserial modules over the ring $H_m(\mathcal{O})$ are exhausted by the D^m, all principal $H_m(\mathcal{O})$-modules and quotient modules of these modules.*

Proof. Obviously, the modules listed in the formulation are uniserial. The ring $H_m(\mathcal{O})$ is two-sided hereditary because of corollary 8.3.8. It is easy to see that D^m is an injective $H_m(\mathcal{O})$-module and that any quotient module of D^m is also injective by theorem 5.5.6. Set $P_i = e_iH_m(\mathcal{O})$ and $P_i/P_iR = U_i$. Obviously, D^m is an injective hull of P_i for $i = 1, ..., m$.

The module $D^m/P_i = C_i$ is an injective hull of the module U_{i-1} for $i = 2, ..., m$ and the module $D^m/P_1 = C_1$ is an injective hull of U_m. Let M be a uniserial

module. If it is finitely generated, then, obviously, it is a quotient module of a principal module. If M is not finitely generated, then it contains either a principal module P or a nontrivial quotient module of it and hence a simple module U. The injective hull D^m of the module P coincides with the injective hull of M and the injective hull C_i of the module U coincides with the injective hull of M. Since all the proper modules C_i and D^m are finitely generated, we obtain the statement of the lemma.

Proposition 13.3.5. *A semiperfect reduced indecomposable ring B is a minor of the second order of a serial right Noetherian ring if and only if it is isomorphic to one of the following rings:*

a) *a reduced serial two-sided Noetherian ring B whose identity is a sum of two local idempotents;*

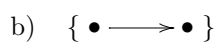
b) *a ring $H(\mathcal{O}, 1, 1)$, where $\mathcal{O}$ is a discrete valuation ring.*

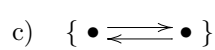
Proof. Let $1 = e_1 + e_2$ be a decomposition of the identity of the ring B into a sum of local idempotents, and let $B = \bigoplus\limits_{i,j=1}^{2} e_i B e_j$ be the corresponding two-sided Peirce decomposition. Write $B_{ij} = e_i B e_j$ $(i, j = 1, 2)$. By the above, B_{ii} is a uniserial two-sided Noetherian ring $(i = 1, 2)$. The Jacobson radical R of the ring B has the form: $R = \begin{pmatrix} R_1 & B_{12} \\ B_{21} & R_2 \end{pmatrix}$, where R_i is the Jacobson radical of B_{ii} $(i = 1, 2)$. As usual,

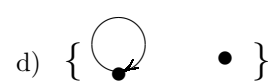
$$R^2 = \begin{pmatrix} R_1^2 + B_{12}B_{21} & R_1 B_{12} + B_{12} R_2 \\ R_2 B_{21} + B_{21} R_1 & R_2^2 + B_{21} B_{12} \end{pmatrix}.$$

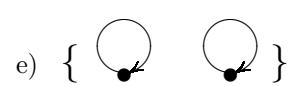
By theorem 12.1.2 we have the following possibilities for the quiver of B:

a) 

b) 

c) 

d) 

e) 

In case a) $e_1BR = 0$ and $e_2BR = 0$, i.e., $rad(B) = 0$ and B is a semisimple Artinian ring.

In case b) e_2B is a simple module, hence $B_{21} = 0$ and B_{22} is a division ring. By the Q-Lemma , $R_1^2 = R_1$, whence $R_1 = 0$ and by proposition 12.1.1 B is an Artinian serial ring.

In case c) by the Q-Lemma we obtain $B_{12}B_{21} = R_1$, $B_{21}B_{21} = R_2$ and strict inclusions $R_1B_{12} + B_{12}R_2 \subset B_{12}$, $R_2B_{21} + B_{21}R_1 \subset B_{21}$. But then $R_1B_{12} = B_{12}R_2$ and $R_2B_{21} = B_{21}R_1$. Let $b_{21} \in B_{21}\backslash B_{21}R_1$ and $b_{12} \in B_{12}\backslash B_{12}R_2$. Then, obviously, $B_{22}b_{21} = B_{21}$ and $B_{11}B_{12} = B_{12}$. By theorem 3.6.1, B is a two-sided Noetherian ring.

In case d) by the Q-Lemma we obtain $B_{21} = 0$, $R_2 = 0$, and hence B_{22} is a division ring, $R_1B_{12} = B_{12}$. Therefore B_{11} is a discrete valuation ring. Write $\mathcal{O} = B_{11}$ and $D = B_{22}$. So $B = \begin{pmatrix} \mathcal{O} & B_{12} \\ 0 & D \end{pmatrix}$. By lemma 13.3.3, B_{12} is a right uniserial D-module and a left uniserial $\mathcal{O}$-module. Therefore $B_{12} = bD$, where $b \in D$. By lemma 13.3.4, taking into account the equality $R_1B_{12} = B_{12}$, we obtain that $B_{12} = D_1b$ where D_1 is the division ring of the ring $\mathcal{O}$. Since $B_{12} = D_1b = bD$, the mapping $\sigma : D_1 \to D$ given by the formula $\alpha b = b\alpha^\sigma$, where $\alpha \in D_1$ and σ is an isomorphism of the division rings D_1 and D. Assigning to an element $\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} \in H(\mathcal{O}, 1, 1)$ the element $\begin{pmatrix} \alpha & \beta b \\ 0 & \gamma^\sigma \end{pmatrix} \in B$ we obtain an isomorphism between the rings $H(\mathcal{O}, 1, 1)$ and B.

In case e) we have the equalities: $R_1^2 + B_{12}B_{21} = R_1^2$, $R_1B_{12} + B_{12}R_2 = B_{12}$, $R_2B_{21} + B_{21}R_1 = B_{21}$, $R_2^2 + B_{21}B_{12} = R_2^2$. By Nakayama's lemma, $R_1B_{12} = B_{12}$ and $B_{21} = R_2B_{21}$. Obviously, $B_{12}B_{21}$ is an ideal in the ring B_{11}. If the ring B_{11} is Artinian then $B_{12} = 0$. Consider the ideal $\mathcal{I} = \begin{pmatrix} R_1 & 0 \\ B_{21}R_1 & 0 \end{pmatrix}$ (R_1 is the radical of the ring B_{11}) and the quotient ring $B = B/\mathcal{I}$. If $B_{21} \neq 0$ then B_{22} is a discrete valuation ring and $B_{21}/B_{12}R_1$ as a left B_{22}-module is isomorphic to the quotient division ring of B_{22}. By theorem 3.6.1, the ring B is not right Noetherian. Exactly in the same way, if B_{22} is an Artinian ring, then $B_{12} = 0$ and $B_{21} = 0$. Therefore B_{11} and B_{22} are discrete valuation rings. If $B_{12}B_{21} \neq 0$, then $B_{12}B_{21} = R_1^m$. Since $R_1B_{12} = B_{12}$, we have $R_1^m = B_{12}B_{21} = R_1B_{12}B_{21} = R_1^{m+1}$ which leads to a contradiction. Analogously, $B_{21}B_{12} = 0$. If at least one from B_{12} and B_{21} is not equal to zero, then without loss of generality one can assume that $B_{12} = 0$. The left ideals $\begin{bmatrix} B_{12} \\ R_2^2 \end{bmatrix}$ and $\begin{bmatrix} B_{12}R_2^2 \\ R_2 \end{bmatrix}$ are not contained one in another. Therefore the left module $\begin{bmatrix} B_{12} \\ B_{22} \end{bmatrix}$ is not uniserial. Hence $B_{12} = 0$ and $B_{21} = 0$. The proposition is proved.

13.4. STRUCTURE OF SERIAL RIGHT NOETHERIAN RINGS

Let A be a serial right Noetherian ring. Assume that it is reduced. Order all the non-isomorphic principal A-modules in the following way: first all non-Artinian modules $P_1, ..., P_t$ (in some order) and then the Artinian modules $P_{t+1}, ..., P_{t+m}$, where $t + m = s$. Denote by P the direct sum of the modules $P_1, ..., P_t$ and by Q the direct sum of the modules $P_{t+1}, ..., P_{t+m}$. Then $A = P \oplus Q$. Let $1 = e_1 + e_2$ be the corresponding decomposition of the identity of the ring A into a sum of idempotents.

The two-sided Peirce decomposition corresponding to this decomposition of the identity looks like:

$$A = \begin{pmatrix} A_1 & X \\ Y & A_2 \end{pmatrix}$$

where $A_i = e_i A e_i$ $(i = 1, 2)$, $X = e_1 A e_2$, $Y = e_2 A e_1$.

The two-sided Peirce decomposition of the Jacobson radical R of the ring A has the form:

$$R = \begin{pmatrix} R_1 & X \\ Y & R_2 \end{pmatrix}$$

where R_i is the Jacobson radical of the ring A_i $(i = 1, 2)$.

Lemma 13.4.1. *In the quiver of a serial right Noetherian ring A there is no arrow going from a vertex corresponding to a non-Artinian principal module P_i $(i = 1, ..., t)$ to a vertex corresponding to an Artinian principal module P_{t+j} $(j = 1, ..., m)$. If at least one point of a cycle corresponds to an Artinian principal module, then all points of this cycle correspond to Artinian principal modules. All points of a chain correspond to Artinian modules.*

Proof. Suppose, P_i is a non-Artinian principal A-module. Let P_k be the projective cover of the module $P_i R$. This means that there is an arrow going from the vertex i to the vertex k. If the module P_k is Artinian then, obviously, the module P_i is also Artinian and this leads to a contradiction. Hence it follows that either all points of a cycle correspond to Artinian modules or all points of the cycle correspond to non-Artinian modules, and all points of a chain correspond to Artinian modules. The lemma is proved.

Let us show that $Hom_A(P, Q) \simeq e_2 A e_1 = 0$. By lemma 13.4.1 and theorem 12.1.2 there are no arrows between points of the subset $\{1, ..., t\}$ and $\{t + 1, ..., t + m\}$. By the Q-Lemma we have the following equalities $X = R_1 X + X R_2$, $Y = Y R_1 + R_2 Y$. By theorem 3.6.1, X (resp. Y) is a finitely generated right A_1(resp. A_2)-module. By Nakayama's lemma, we obtain $X = R_1 X$ and $Y = R_2 Y$. The right ideal (Y, R_2) is an Artinian and Noetherian module therefore there is a natural number n such that $(Y, R_2)R^n = 0$. It is easy to verify that $(Y, R_2)R^n = (Y, YX + R_2^{n+1}) = (0, 0)$. Therefore $Y = 0$ and $R_2^{n+1} = 0$. By

proposition 12.1.1, the ring A_2 is Artinian. So, the ring A has the form:

$$A = \begin{pmatrix} A_1 & X \\ 0 & A_2 \end{pmatrix},$$

where A_2 is a serial Artinian ring.

By theorem 12.1.2 the ring A_2 can be decomposed into a direct product of rings whose quivers are cycles and chains:

$$A_2 = A_2^{(1)} \times \ldots \times A_2^{(r)}.$$

It is natural to assume that the ring A is indecomposable. We are going to show that in this case all the quivers of the rings $A_2^{(1)}, \ldots, A_2^{(r)}$ are chains.

Assume that this is not so. Without loss of generality one can assume that $A_2^{(1)} = A_2$ and that the quiver of the ring A_2 is a cycle.

Obviously, the set

$$\mathcal{I} = \begin{pmatrix} 0 & XR_2 \\ 0 & R_2^2 \end{pmatrix}$$

is a two-sided ideal in the ring A. Let $\bar{A} = A/\mathcal{I}$. Write $\bar{X} = X/XR_2$ and $\bar{R}_2 = R_2/R_2^2$. Obviously, the left ideals in the ring $\bar{A}$ given by $\begin{pmatrix} 0 & \bar{X} \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & \bar{R}_2 \end{pmatrix}$ are nonzero and neither contains the other. On the other hand, $\bar{X}$ and $\bar{R}_2$ are semisimple $\bar{A}_2$-modules ($\bar{A}_2 = A_2/R_2^2$). Therefore by the Q-Lemma there exists a local idempotent g in the ring $\bar{A}_2$ such that $\bar{X}g \neq 0$ and $\bar{R}_2 g \neq 0$. But then the left ideals $\bar{X}g$, $\bar{R}_2 g$ are submodules of the uniserial module $\bar{A}g$ which are not contained one in another. This contradicts the fact that the principal $\bar{A}$-module $\bar{A}g$ is uniserial. So, all quivers of the rings $A_2^{(1)}$,..., $A_2^{(r)}$ are chains and from the results of section 12.3 it follows that the ring A_2 is isomorphic to a direct product of quotient rings of upper triangular matrices over division rings.

We are going to describe the ring A_1 from the decomposition

$$A = \begin{pmatrix} A_1 & X \\ 0 & A_2 \end{pmatrix}.$$

From lemma 13.4.1 it follows that the quiver of the ring A_1 is a disconnected union of cycles. We shall show that the ring of endomorphisms of any principal A_1-module is a discrete valuation ring.

Let $1 \in A$ and let $1 = h_1 + \ldots + h_t + h_{t+1} + \ldots + h_{t+m}$ be a decomposition of the identity of the ring A into a sum of pairwise orthogonal local idempotents, where, moreover, the rings $h_i A_1 h_i$ are not Artinian and the rings $h_j A h_j$ are Artinian for $j \geq t+1$. By proposition 13.3.1, the $h_i A h_i$ $(i = 1, ..., t)$ are discrete valuation

rings. Because the quiver of the ring A_1 is a disconnected union of cycles, one can assume that the two-sided Peirce decomposition of A_1 has the form:

$$A_1 = \begin{pmatrix} A_{11} & A_{12} & \dots & A_{1q} \\ A_{21} & A_{22} & \dots & A_{2q} \\ \dots & \dots & \dots & \dots \\ A_{q1} & A_{q2} & \dots & A_{qq} \end{pmatrix},$$

where the quiver of the ring A_{ii} is a cycle $(i = 1, \dots, q)$ and $A_{ij}A_{ji} \subset R_i^2$ for $i \neq j$ (R_i is the Jacobson radical of the ring A_{ii}). Obviously, the sets

$$\mathcal{I}_1 = \begin{pmatrix} A_{1i} \\ \vdots \\ A_{i-1,i} \\ R_i^2 \\ A_{i+1,i} \\ \vdots \\ A_{iq} \end{pmatrix} \quad \text{and} \quad \mathcal{I}_2 = \begin{pmatrix} A_{1i}R_i \\ \vdots \\ A_{i-1,i}R_i \\ R_i \\ A_{i+1,i}R_i \\ \vdots \\ A_{iq}R_i \end{pmatrix}$$

are left ideals in the ring A_1 $(i = 2, \dots q)$. If $A_{1i} \neq 0$, then $\bar{A}_{1i} = A_{1i}/A_{1i}R_i \neq 0$. By the Q-Lemma there is a local idempotent g such that $\bar{A}_{1i}g \neq 0$ and $\bar{R}_i g = (R_i/R_i^2)g \neq 0$. This follows from the fact that the quiver of the ring A_{ii} is a cycle. The submodules $\mathcal{I}_1 g$ and $\mathcal{I}_2 g$ of the left serial module Ag are not contained one in another. Therefore $A_{1i} = 0$ for $i = 2, \dots, q$. By proposition 13.3.5 $A_{j1} = 0$ for $i \neq j$. Hence the ring A_1 is a direct product of rings whose quivers are cycles.

Theorem 13.4.2. *A serial right Noetherian reduced ring, which is not Artinian and whose quiver is a cycle, is isomorphic to a ring of the form $H_s(\mathcal{O})$.*

Proof. We shall carry out the proof by induction on the number of principal modules in the direct decomposition $A = P_1 \oplus \dots \oplus P_s$. Let $1 = e_1 + \dots + e_s$ be the corresponding decomposition of the identity of the ring A into a sum of local pairwise orthogonal idempotents, let $A = \bigoplus\limits_{i,j=1}^{s} (A_{ij})$ be the corresponding two-sided Peirce decomposition. For $s = 1$ the statement follows from proposition 13.3.1.

Let the quiver $Q(A)$ have the form

$$\left\{ \begin{array}{ccccccccc} 1 & & 2 & & & & s-1 & & s & & 1 \\ \bullet & \longrightarrow & \bullet & \longrightarrow & \dots & \longrightarrow & \bullet & \longrightarrow & \bullet & \longrightarrow & \bullet \end{array} \right\}$$

Then $A_{i,i+1} \neq 0$ for $i = 1, \dots, s-1$ and $A_{s1} \neq 0$. Consider the ring $A' = (1 - e_1)A(1 - e_1)$. Obviously, the quiver $Q(A')$ has a path $2 \to \dots \to s-1 \to s$. By proposition 13.3.5, $Q(A')$ cannot be a chain. Therefore $Q(A')$ has the form

$$\left\{ \begin{array}{ccccccccc} 2 & & 3 & & & & s-1 & & s & & 2 \\ \bullet & \longrightarrow & \bullet & \longrightarrow & \dots & \longrightarrow & \bullet & \longrightarrow & \bullet & \longrightarrow & \bullet \end{array} \right\}$$

Hence, by the induction hypothesis, A' is isomorphic to the ring $H_{s-1}(\mathcal{O})$. The module

$$Y = \begin{bmatrix} A_{21} \\ \vdots \\ A_{s1} \end{bmatrix}$$

is a left uniserial A'-module. By lemma 13.3.4 and proposition 13.3.5, Y is a finitely generated left A'-module. Consider the ring $A'' = (1 - e_s)A(1 - e_s)$. Again by induction we conclude that $A_{12}, ..., A_{1,s-1}$ are finitely generated left A_{11}-modules. By proposition 13.3.5, A_{1s} is a finitely generated left A_{11}-module. Hence, $X = (A_{12}, \ldots, A_{1s})$ is a finitely generated left A_{11}-module. By theorem 3.6.1, A is a two-sided Noetherian ring. The statement now follows from theorem 12.3.8 and corollary 12.3.7. The theorem is proved.

Thus, the two-sided Peirce decomposition of a serial right Noetherian ring A has the form $A = \begin{pmatrix} A_1 & X \\ 0 & A_2 \end{pmatrix}$, where $A_1 = H_1 \times \ldots \times H_q$ is a direct product of rings which are isomorphic to rings of the form $H_s(\mathcal{O})$ and $A_2 = B_1 \times \ldots \times B_r$ is a direct product of quotient rings of the rings of upper triangular matrices over division rings.

We shall need the following useful construction. Let Λ and Γ be rings and let ${}_\Lambda X_\Gamma$ be a Λ-Γ-bimodule. In this situation one can construct the ring $A = \begin{pmatrix} \Lambda & X \\ 0 & \Gamma \end{pmatrix}$ with coordinatewise addition and matrix multiplication. Let $\varphi : \Lambda \to \Delta$ and $\psi : \Gamma \to \mathcal{A}$ be ring isomorphisms. We can make X into a Δ-$\mathcal{A}$-bimodule by the rule: $\delta x w = \delta^{\varphi^{-1}} x w^{\psi^{-1}}$, where $\delta \in \Delta$, $w \in \mathcal{A}$, $x \in X$. Consider the ring $A' = \begin{pmatrix} \Delta & X \\ 0 & \mathcal{A} \end{pmatrix}$ with multiplication:

$$\begin{pmatrix} \delta & x \\ 0 & w \end{pmatrix} \begin{pmatrix} \delta_1 & x_1 \\ 0 & w_1 \end{pmatrix} = \begin{pmatrix} \delta\delta_1 & \delta^{\varphi^{-1}} x_1 + x w_1^{\psi^{-1}} \\ 0 & w w_1 \end{pmatrix}$$

and coordinatewise addition. It is easy to verify that the map $\Phi : A \to A'$ given by $\Phi\left[\begin{pmatrix} \lambda & x \\ 0 & \gamma \end{pmatrix}\right] = \begin{bmatrix} \lambda^\varphi & x \\ 0 & \gamma^\psi \end{bmatrix}$ is an isomorphism.

Therefore, using this construction, we can assume $H_i = H_{s_i}(\mathcal{O}_i)$ for $i = 1, 2, ..., q$ and $B_j = T_{m_j}(D_j)/\mathcal{I}_j$ for $j = 1, ..., r$. Let $1 = h_1 + \ldots + h_q + f_1 + \ldots + f_r$ be a decomposition of the identity of A into a sum of pairwise orthogonal idempotents such that $h_i A h_i = H_i$ and $f_j A f_j = B_j$ $(i = 1, \ldots, q;\ j = 1, \ldots, r)$.

Suppose that $X_{i_0 j_0} = h_{i_0} A f_{j_0} \neq 0$. Consider the ring $H = (h_{i_0} + f_{j_0})A(h_{i_0} + f_{j_0}) = \begin{pmatrix} H_{i_0} & X_{i_0 j_0} \\ 0 & B_{j_0} \end{pmatrix}$. We can assume that $H_{i_0} = H_s(\mathcal{O})$ and $B_{j_0} = T_m(D)/\mathcal{I}$. As pairwise orthogonal local idempotents of the ring A, whose sum is equal to the identity of the ring H, we have the matrix units

$e_{11},\dots,e_{ss},e_{s+1,s+1},\dots,e_{s+m,s+m}$. The right B_{j_0}-module $e_{ii}X_{i_0j_0}$ $(i=1,\dots,s)$ is a finitely generated uniserial $T_m(D)$-module. Therefore it is isomorphic to a quotient module of $e_{s+j,s+j}T_m(D)$ where j is one of the integers from 1 to m. We shall show that $j=1$. Suppose that this is not true. We set $h=e_{ii}+e_{s+j-1,s+j-1}+e_{s+j,s+j}$ $(j>1)$. Then the ring hAh has the form:

$$hAh=\begin{pmatrix}\mathcal{O} & 0 & X_{13}\\ 0 & D & D\\ 0 & 0 & D\end{pmatrix}$$

where $X_{13}\neq 0$. Obviously, the ring hAh is not serial. By proposition 12.3.1 the ring A is not serial. Thus, $e_{ii}X_{i_0j_0}\simeq e_{s+1,s+1}T_m(D)/\mathcal{I}$ is a finite dimensional D-space. Because of lemma 13.3.4, all the modules $e_{ii}X_{i_0j_0}$ $(i=1,\dots,s)$ are pairwise isomorphic. Therefore $h_iAf_{j_0}=0$ for $i\neq i_0$ and $h_{i_0}Af_j=0$ for $j\neq j_0$. If the ring A cannot be decomposed into a direct product, then $t=r=1$. Thus, the ring A has the form:

$$A=\begin{pmatrix}H_s(\mathcal{O}) & X\\ 0 & T_m(D)/\mathcal{I}\end{pmatrix}$$

Since $e_{ii}X$ is isomorphic to a quotient module of the first principal module of $T_m(D)$, taking into account lemma 13.3.4, we can find a nonzero element $x_{s,s+1}\in e_{ss}Xe_{s+1,s+1}$ such that elements $e_{is}x_{s,s+1}e_{s+1,s+j}$ $(j=1,\dots,q)$, where $q\leq m$ $(i=1,\dots,s)$, form a basis of the right vector D-space X. As above we denote by $\sigma:\mathcal{O}\to D$ the monomorphism defined by $\alpha x_{s,s+1}=x_{s,s+1}\alpha^{\sigma}$, where $\alpha\in\mathcal{O}$. Write $\mathcal{O}_1=Im\sigma$. By proposition 13.3.5 the classical ring of fractions of $\mathcal{O}_1$ coincides with D. We shall construct an isomorphism $\bar{\sigma}$ between the rings $H_s(\mathcal{O})$ and $H_s(\mathcal{O}_1)$. Let $h\in H_s(\mathcal{O})$, $h=(\alpha_{ij})$, $(i,j=1,\dots,s)$. We set $h^{\bar{\sigma}}=(\alpha_{ij}^{\sigma})$. Now form a new ring A_0, whose elements are matrices of the form $\begin{pmatrix}\bar{h} & x\\ 0 & t\end{pmatrix}$, where $\bar{h}\in H_s(\mathcal{O}_1)$, $t\in T_m(D)/\mathcal{I}$. Addition of elements is coordinatewise and multiplication is defined by the rule:

$$\begin{pmatrix}\bar{h} & x\\ 0 & t\end{pmatrix}\begin{pmatrix}\bar{h}_1 & x_1\\ 0 & t_1\end{pmatrix}=\begin{pmatrix}\bar{h}\bar{h}_1 & \bar{h}^{\bar{\sigma}^{-1}}x_1+xt_1\\ 0 & tt_1\end{pmatrix}.$$

The mapping $\psi:A_0\to A$, $\psi\Big[\begin{pmatrix}\bar{h} & x\\ 0 & t\end{pmatrix}\Big]=\begin{pmatrix}\bar{h}^{\bar{\sigma}^{-1}} & x\\ 0 & t\end{pmatrix}$ is an isomorphism of the rings A_0 and A.

The monomorphism $\sigma_0:\mathcal{O}_1\to D$ given by the formula $\beta x_{s,s+1}=x_{s,s+1}\beta^{\sigma_0}$, where $\beta\in\mathcal{O}_1$, is the identity map.

Consider the ring

$$H'(\mathcal{O}_1,s,m)=\begin{pmatrix}H_s(\mathcal{O}_1) & X_1\\ 0 & T_m(D)\end{pmatrix}$$

where

$$X_1 = \{(e_{ii}x_{s,s+1}e_{s+1,s+j}\alpha_{ij}) \mid \alpha_{ij} \in D; i = 1, \ldots, s; j = 1, \ldots, m;$$

$$\alpha x_{s,s+1} = x_{s,s+1}\alpha, \qquad \text{where } \alpha \in \mathcal{O}_1\}.$$

The ring $H'(\mathcal{O}_1, s, m)$ is isomorphic to $H(\mathcal{O}_1, s, m)$. This isomorphism is given by the rule:

$$\begin{pmatrix} h & x_1 \\ 0 & t \end{pmatrix} \to \begin{pmatrix} h & (\alpha_{ij}) \\ 0 & t \end{pmatrix}$$

where $x_1 \in X_1$. We shall show that $H'(\mathcal{O}_1, s, m)$ is surjectively mapped onto A_0. Every element $b \in H'(\mathcal{O}_1, s, m)$ can be uniquely written in the form $b = a_0 + b_1$ where $a_0 \in A_0$. The elements b for which $a_0 = 0$ form a two-sided ideal in the ring $H'(\mathcal{O}_1, s, m)$. Assigning to an element b the element a_0, we obtain an epimorphism of the ring $H'(\mathcal{O}_1, s, m)$ on the ring A_0.

Thus, taking into account lemma 13.3.2 we obtain a full description of serial right Noetherian rings.

Theorem 13.4.3. *Any serial right Noetherian ring is Morita equivalent to a direct product of a finite number of rings of the following types:*

1) *Artinian serial rings*;

2) *rings isomorphic to rings of the form* $H_s(\mathcal{O})$;

3) *rings isomorphic to quotient rings of* $H(\mathcal{O}, s, m)$,

where $\mathcal{O}$ *is a discrete valuation ring.*

Conversely, all rings of this form are serial and right Noetherian.

13.5. SERIAL RIGHT HEREDITARY RINGS. SERIAL SEMIPRIME AND RIGHT NOETHERIAN RINGS

This section is devoted to descriptions of the rings from the section title.

Theorem 13.5.1. *A serial right hereditary ring is right Noetherian.*

Proof. Suppose that $A = P_1^{n_1} \oplus \ldots \oplus P_s^{n_s}$ is a decomposition of the ring A into a direct sum of principal right A-modules. Consider a nonzero submodule N of the principle module P_i. Since P_i is a uniserial module, N is indecomposable and projective. As follows from 5.5.1 the module N is isomorphic to a principal module. Therefore any submodule of a principal module is finitely generated. Hence the ring A is right Noetherian as a direct sum of Noetherian modules. The theorem is proved.

Theorem 13.5.2. *A serial right hereditary ring* A *is Morita equivalent to a direct product of rings isomorphic to rings of upper triangular matrices over division rings, rings of the form* $H_m(\mathcal{O})$ *and rings of the form* $H(\mathcal{O}, m, n)$, *where* $\mathcal{O}$ *is a discrete valuation ring.*

Proof. Obviously, one can assume that the ring A is indecomposable and reduced. By theorem 13.4.3 in this case A is either a two-sided Noetherian ring or it is isomorphic to a quotient ring of $H(\mathcal{O}, m, n)$. A two-sided Noetherian reduced ring A is either non-Artinian or it is an Artinian ring having a simple projective module. In the first case it is isomorphic to a ring of the form $H_m(\mathcal{O})$, where $\mathcal{O}$ is a discrete valuation ring. Conversely, a ring of the form $H_m(\mathcal{O})$ is a two-sided hereditary and serial ring.

In the second case $A \simeq T_n(D)/\mathcal{I}$, where $\mathcal{I}$ is a two-sided ideal in the ring $T_n(D)$. Obviously, $e_{ii}Ae_{jj} = D$ or $e_{ii}Ae_{jj} = 0$ for $i < j$ $(i, j = 1, \ldots, n$; the e_{ii} are matrix units). Since the ring A is indecomposable, one may assume that the quiver $Q(A)$ of the ring A is a chain:

$$\left\{ \begin{array}{ccccccccc} 1 & & 2 & & & & n-1 & & n \\ \bullet & \longrightarrow & \bullet & \longrightarrow & \cdots & \longrightarrow & \bullet & \longrightarrow & \bullet \end{array} \right\}$$

Therefore A contains the matrix units $e_{12}, e_{23}, \ldots, e_{n-1,n}$. But then by lemma 5.5.8 there is a chain of submodules in P_1 isomorphic to $P_2, ..., P_n : P_1 \supset P_2 \supset \ldots \supset P_n$ where $P_i \simeq e_{ii}A$ $(i = 1, \ldots, n)$. Since $dim_D P_1 \leq n$ and all inclusions $P_i \supset P_{i+1}$ $(i = 1, \ldots, n-1)$ are strict, $dim_D P_i = n - i + 1$. Hence $\mathcal{I} = 0$. Thus, $A \simeq T_n(D)$. Conversely, a ring of the form $T_n(D)$ is serial and two-sided hereditary.

When A is only right Noetherian and right hereditary by means of analogous arguments one can show that $A \simeq H(\mathcal{O}, m, n)$. It is easy to see that $H(\mathcal{O}, m, n)$ is right hereditary. The theorem is proved.

Recall that a ring A is called **semiprime** if it does not have nonzero nilpotent ideals. A ring A is called **prime** if a product of any two nonzero ideals is not equal to zero. From the definition it follows that a prime ring is always semiprime.

The following theorem gives a description of serial semiprime and right Noetherian rings.

Theorem 13.5.3. *A serial semiprime and right Noetherian ring can be decomposed into a direct product of prime rings. A serial prime and right Noetherian ring is also left Noetherian and two-sided hereditary. In the Artinian case such a ring is Morita equivalent to a division ring and in the non-Artinian case it is Morita equivalent to a ring isomorphic to $H_m(\mathcal{O})$, where $\mathcal{O}$ is a discrete valuation ring. Conversely, all such rings are prime two-sided hereditary and Noetherian.*

Proof. By proposition 11.2.9 we can assume that the ring A is reduced and indecomposable. We again use theorem 13.4.3. If A is an Artinian ring, then its radical R is equal to zero. Therefore the ring A is isomorphic to a division ring. If the ring A is two-sided Noetherian and non-Artinian then $A \simeq H_m(\mathcal{O})$, where $\mathcal{O}$ is a discrete valuation ring. If the ring A is isomorphic to a quotient ring of the ring $H(\mathcal{O}, m, n)$, then the ideal $\begin{pmatrix} 0 & X \\ 0 & 0 \end{pmatrix}$ is nilpotent. Hence, the right Noetherian

quotient ring of the ring $H(\mathcal{O}, m, n)$ is not semiprime. The converse statement follows from theorem 13.5.2.

To conclude this section we shall give a proof of Michler's theorem, which gives a description of two-sided hereditary semiprime semiperfect rings. This proof uses the notion of the quiver of a semiperfect ring.

Lemma 13.5.4. *Let A be a semiperfect semiprime two-sided Noetherian ring whose quiver is connected. If the ring A is not a division ring then for any point of $Q(A)$ there exists an arrow going out from it and there exists an arrow going in to it.*

Proof. One can assume that the ring A is reduced. Suppose no arrow enters vertex 1 (this may be assumed without loss of generality). Consider the corresponding two-sided Peirce decomposition A: $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$, where $1 = e_1 + e_2$, $e_1 A = P_1$, P_1 is a principal A-module, $e_1^2 = e_1$. By proposition 11.1.1, $A_{21}R_1 + R_2A_{21} = A_{21}$, where R_i is the Jacobson radical of the ring A_{ii} $(i = 1, 2)$. Hence by theorem 3.6.1 and Nakayama's lemma $A_{21} = 0$. Since the ring A is semiprime, it follows that $A_{12} = 0$. Therefore, since $Q(A)$ is a connected quiver, it follows that the ring A is a division ring.

The remaining statement is proved by similar arguments.

Theorem 13.5.5. *The quiver (left quiver) of a semiperfect semiprime two-sided Noetherian hereditary ring A is a disconnected union of points and cycles.*

Proof. Suppose that there exist arrows going from vertex 1 to two different vertices i and j. Then P_1R contains as a direct summand a module N which is isomorphic to $P_i \oplus P_j$. Fix monomorphisms $\varphi : P_i \to P_1$, $\psi : P_j \to P_1$ and write $Im(\varphi \oplus \psi) = N$.

Because the ring A is semiprime, the sets $Hom(P_1, P_i)$ and $Hom(P_1, P_j)$ are both different from zero. Obviously, the sets $\varphi Hom(P_1, P_i)$ and $\psi Hom(P_1, P_j)$ are right ideals in the ring $EndP_1$ which are not contained one in another. This contradicts proposition 10.2.7. By propositions 5.5.7 and 11.2.9 one can assume that the ring A is reduced. We are going to show that there does not exist more than one arrow going to each vertex. Consider the vertex with number k. Suppose that there exist two arrows going to the vertex k from different vertices j_1 and j_2. Then by the Q-Lemma we have strict inclusions:

$$e_{j_1} R^2 E_k \subset e_{j_1} R e_k, \quad e_{j_2} R^2 e_k \subset e_{j_2} R e_k.$$

Set $Q_k = Ae_k$, where e_k is an idempotent corresponding to the principal module P_k. By the Q-lemma, the simple modules V_{j_1} and V_{j_2} are contained in the quotient module RQ_k/R^2Q_k. Therefore $RQ_k = Q_{j_k} \oplus Q_{j_2} \oplus X$. This again contradicts the

fact that $EndQ_k$ is a discrete valuation ring. Now the theorem follows from lemma 13.5.4.

Corollary 13.5.6. *A semiperfect semiprime two-sided Noetherian hereditary ring is serial.*

The proof follows immediately from the theorem 13.5.5.

Proposition 13.5.7. *Let* $A = \begin{pmatrix} A_1 & X \\ Y & A_2 \end{pmatrix}$ *be a two-sided Peirce decomposition of a ring* A *and let* $\sigma : A_1 \to A_0$ *be an isomorphism of rings. There exists a ring* $\bar{A} = \begin{pmatrix} A_0 & X \\ Y & A_2 \end{pmatrix}$ *isomorphic to* A.

Proof. Any element α_0 in A_0 can be written in the form $\alpha_0 = \alpha^\sigma$ for some $\alpha \in A_1$. In the ring $\bar{A} = \begin{pmatrix} A_0 & X \\ Y & A_2 \end{pmatrix}$ we introduce multiplication by the rule:

$$\begin{pmatrix} \alpha^\sigma & x \\ y & \beta \end{pmatrix} \begin{pmatrix} \alpha_1^\sigma & x_1 \\ y_1 & \beta_1 \end{pmatrix} = \begin{pmatrix} (\alpha\alpha_1)^\sigma + (xy_1)^\sigma & \alpha x_1 + x\beta_1 \\ y\alpha_1 + \beta y_1 & yx_1 + \beta\beta_1 \end{pmatrix},$$

and addition coordinatewise. The map $\varphi : A \to \bar{A}$ given by $\varphi\Big[\begin{pmatrix} \alpha & x \\ y & \beta \end{pmatrix}\Big] = \begin{pmatrix} \alpha^\sigma & x \\ y & \beta \end{pmatrix}$ is, obviously, an isomorphism.

Proposition 13.5.8. *Let* A *be a reduced semiperfect semiprime two-sided Noetherian hereditary ring, whose quiver is a cycle consisting of two points. Then* A *is isomorphic to the ring* $H_2(\mathcal{O})$*, where* $\mathcal{O}$ *is a discrete valuation ring. In particular, if* $A = \begin{pmatrix} A_1 & A_3 \\ Y & A_2 \end{pmatrix}$*, where* A_1, A_2, A_3 *are rings, then* $A_1 = A_2 = A_3$.

Proof. The quiver $Q(A)$ is

$$\left\{ \begin{array}{ccccc} 1 & & 2 & & 1 \\ \bullet & \longrightarrow & \bullet & \longrightarrow & \bullet \end{array} \right\}$$

Let $A = \begin{pmatrix} A_1 & X \\ Y & A_2 \end{pmatrix}$ be the corresponding two-sided Peirce decomposition. By proposition 11.1.1 we have the equalities $XY = R_1$, $YX = R_2$ (R_i is the Jacobson radical of the ring A_i, $i = 1, 2$) and strict inclusions $R_1X + XR_2 \subset X$, $R_2Y + YR_1 \subset Y$. Since by corollary 13.5.6 A is a serial Noetherian ring, by theorem 10.3.8, lemma 11.1.3 and proposition 12.3.6 there exist elements $x \in X$ and $y \in Y$ such that $X = xA_2 = A_1x$ and $Y = yA_1 = A_2y$. Moreover, A_1 and A_2 are discrete valuation rings. The map $\sigma : A_1 \to A_2$, defined by $a_1x = xa_1^\sigma$, is an isomorphism. Applying proposition 13.5.8 one can assume that: $A = \begin{pmatrix} A_2 & X \\ Y & A_2 \end{pmatrix}$

and $a_2x = xa_1^\sigma$ for any $a_2 \in A_2$. But then this ring is, obviously, isomorphic to $A = \begin{pmatrix} A_2 & A_2 \\ Y & A_2 \end{pmatrix}$, moreover, Y is the unique maximal ideal of the ring A_2.

If $X = A_3$ is a ring, then $A_1 \subset A_3$ and $A_2 \subset A_3$. From the equality $A_3 = a_2A_2 = A_1a_2$ it follows that a_2 is an invertible element of the ring A_2. Therefore $A_1 = A_2 = A_3$. The proposition is proved.

We shall prove that a reduced semiprime semiperfect two-sided Noetherian hereditary ring is isomorphic to a direct product of division rings and rings of the form $H_s(\mathcal{O})$ where $\mathcal{O}$ is a discrete valuation ring. By theorems 13.5.5 and 11.1.9 one can assume that $Q(A)$ is a cycle:

$$\left\{ \begin{array}{ccccccccc} 1 & & 2 & & & & s & & 1 \\ \bullet & \longrightarrow & \bullet & \longrightarrow & \cdots & \longrightarrow & \bullet & \longrightarrow & \bullet \end{array} \right\}$$

Let $1 = f_1 + \ldots + f_s$ be the corresponding decomposition of the identity of the ring A into a sum of pairwise orthogonal idempotents. Let $A = (A_{ij})$ be the corresponding two-sided Peirce decomposition $(i, j = 1, \ldots, s)$. We shall carry out the proof by induction on s. By proposition 13.5.4 and 13.5.8 one may assume that $s > 2$.

Set $\hat{f}_i = f_1 + \ldots + f_{i-1} + f_{i+1} + \ldots + f_s$. By theorem 3.6.1, proposition 5.5.7 and lemma 11.2.9 the ring $\hat{A}_s = \hat{f}_s A \hat{f}_s$ satisfies the conditions listed above. From the fact that $A_{12}, \ldots, A_{s-2,s-1}$ are not equal to zero it follows that $Q(\hat{A}_s)$ is a cycle:

$$\left\{ \begin{array}{ccccccccc} 1 & & 2 & & & & s-2 & & s-1 & & 1 \\ \bullet & \longrightarrow & \bullet & \longrightarrow & \cdots & \longrightarrow & \bullet & \longrightarrow & \bullet & \longrightarrow & \bullet \end{array} \right\}$$

Therefore by induction and proposition 13.5.7 one can assume that $\hat{A}_s = H_{s-1}(\mathcal{O})$. Considering the ring $\hat{A}_1 = \hat{f}_1 A \hat{f}_1$, by induction, we again have $\hat{A}_1 = H_{s-1}(\mathcal{O}_1)$. So all A_{ij} for $i \leq j$ besides A_{1s} are rings. We set $A_{1s} = (f_1 + f_s)A(f_1 + f_s)$. Since $A_{s1} \neq 0$, $Q(A_{1s})$ is a cycle consisting of two points. Therefore $A_{1s} = H_2(\mathcal{O}_2)$. Hence all A_{ij} are rings for $i \leq j$. By proposition 13.5.8, $A_{ij} = A_{11}$ for $i \leq j$ and $A_{ij} = \mathcal{M}$ for $j < i$, where $\mathcal{M}$ is the unique maximal ideal in the ring A_{11}. Therefore A is isomorphic to the ring $H_s(A_{11})$.

13.6. NOTES AND REFERENCES

Finitely presented modules are studied in the book *M.Auslander, I.Reiten, S.O.Smalø, Representation Theory of Artin Algebras, 1995.*

The Drozd-Warfield theorem was proved in two different ways in the papers: *R.B.Warfield, Serial rings and finitely presented modules // J. Algebra, v.37, N.2 (1975), p.187-222* and *Yu.A.Drozd, On generalized uniserial rings // Mat. Zam., V.18, N.5 (1975), p.705-710.*

The Ore condition for serial rings was studied in the paper: *O.E.Gregul', V.V.Kirichenko, On semihereditary semichain rings// Ukrain. Mat. Zh. V.39 (1987), N.2, p.156-161.*

Minors of rings were introduced in the paper: *Yu.A.Drozd, Minors and reduction theorems // Coll. Math. Soc. J. Bolyai, V.6 (1971), p.173-176.*

The structure of right Noetherian serial rings was studied in the papers: *V.V.Kirichenko, Generalized uniserial rings // Preprint IM-75-1, Kiev, 1975*, *V.V.Kirichenko, Generalized uniserial rings // Mat. sb. v.99(141), N4 (1976), p.559-581* and *V.V.Kirichenko, Right Noetherian rings over which all finitely generated modules are semi-chain modules // Dokl. Akad. Nauk Ukrain. SSR Ser.A, 1976, N.1, p. 9-12.* The description of the structure of such rings was also given by S.Singh in the paper *Serial right Noetherian rings // Can. J. Math., v.36 (1984), p.22-37.*

The Michler theorem, giving the full description of semiperfect two-sided Noetherian and hereditary semiprime rings, was first proved in the paper *G.Michler, Structure of semi-perfect hereditary noetherian rings // J. Algebra, v. 13, N.3, 1969, p.327-344.* It uses the structure theorem of right hereditary, right Noetherian semiprime rings given by L.Levy in the paper *Torsion-free and divisible modules over non-integral domains // Can. J. Math., v.15, 1963, p.132-151* and the description of hereditary orders and Asano orders given in the papers *M.Harada, Hereditary orders // Trans. Amer. Math. Soc., v. 107, 1963, p.272-290*, *M.Harada, On a generalization of Asano's maximal orders in a ring // Osaka J. Math., v.1, 1964, p.61-68* and *G.Michler, Asano orders // Proc. London Math. Soc., v.19, 1969, p.421-443.*

14. Semiperfect semidistributive rings

14.1 DISTRIBUTIVE MODULES

Recall that a module M is called **distributive** if for all submodules K, L, N

$$K \cap (L + N) = K \cap L + K \cap N.$$

Clearly, a submodule and a quotient module of a distributive module is distributive. A module is called **semidistributive** if it is a direct sum of distributive modules. A ring A is called **right** (**left**) **semidistributive** if the right (left) regular module A_A ($_AA$) is semidistributive. A right and left semidistributive ring is called **semidistributive**.

Obviously, every uniserial module is a distributive module and every serial module is a semidistributive module.

Example 14.1.1.

Let $S = \{\alpha_1, \dots, \alpha_n\}$ be a finite poset with ordering relation $\leq$ and let D be a division ring. Denote by $A(S, D)$ the following subring of $M_n(D)$:

$$A(S, D) = \{ \sum_{\alpha_i \leq \alpha_j} d_{ij} e_{ij} \,|\, d_{ij} \in D\}.$$

It is not difficult to check that $A(S, D)$ is a semidistributive Artinian ring.

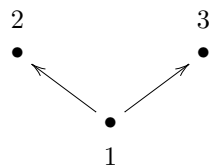
In particular, the hereditary semidistributive ring

$$A_3 = \left\{ \begin{pmatrix} d_{11} & d_{12} & d_{13} \\ 0 & d_{22} & 0 \\ 0 & 0 & d_{33} \end{pmatrix} \mid d_{ij} \in D \right\}$$

is of the form:

$$A_3 = A(P_3, D),$$

where P_3 is the poset with the diagram



It is also clear that A_3 is the semidistributive ring, which is left serial, but not right serial.

Proposition 14.1.1. *Let M be an A-module. Then M is a distributive module if and only if all submodules of M with two generators are distributive modules.*

Proof. Suppose that all two-generated submodules of M are distributive modules. Let K, L, N be submodules of M and $k = l + n \in K \cap (L + N)$; $l \in L$, $n \in N$. Obviously, $kA \subset lA + nA$ and $kA = kA \cap (lA + nA) = kA \cap lA + kA \cap nA$. Therefore, $k \in K \cap L + K \cap N$, i.e., $K \cap (L + N) \subseteq K \cap L + K \cap N$. The inclusion $K \cap L + K \cap N \subseteq K \cap (L + N)$ is always valid.

Lemma 14.1.2. *Let M be a distributive module over a ring A. Then for any $m, n \in M$ there exist $a, b \in A$ such that $1 = a + b$ and $maA + nbA \subset mA \cap nA$.*

Proof. Write $t = m + n$ and $H = mA \cap nA$. Obviously, $tA \subseteq mA + nA$ and $tA \cap (mA + nA) = tA = (tA \cap mA) + (tA + nA)$. So there exist $b, d \in A$ such that $tb \in mA$, $td \in nA$ and $t = tb + td$. Then $nb = tb - mb \in H$ and $md = td - nd \in H$. Let $a = 1 - b$ and $g = 1 - b - d$. We have $tg = t - tb - td = 0$ and $ng = tg - mg = -mg \in H$. So $ma = md + mg \in H$ and $maA + nbA \subseteq mA \cap nA$.

Lemma 14.1.3. *Let M be a A-module. Then M is a distributive module if and only if for any $m, n \in M$ there exist four elements a, b, c, d of A such that $1 = a + b$ and $ma = nc$, $nb = md$.*

Proof. Necessity follows from lemma 14.1.2. Conversely, let $k \in K \cap (L + N)$, where K, L, N are submodules of M. Then $k = m + n$, where $m \in L$ and $n \in N$. By assumption there exist $a, b \in A$ such that $1 = a + b$ and $ma \in mA \cap nA$, $nb \in mA \cap nA$. Consequently, $ka = ma + na \in kA \cap nA$ and $kb = mb + nb \in kA \cap mA$. Therefore, $k = ka + kb \in (kA \cap nA) + (kA \cap mA) \subset K \cap L + K \cap N$, i.e., $K \cap (L + N) = K \cap L + K \cap N$.

Let M be an A-module. Given two elements $m, n \in M$ we set

$$(m : n) = \{a \in A \,|\, na \in mA\}.$$

Theorem 14.1.4 (W.Stephenson). *A module M is distributive if and only if*

$$(m : n) + (n : m) = A$$

for all $m, n \in M$.

Proof. This immediately follows from lemma 14.1.3.

Definition. A module M **has square-free socle** if its socle contains at most one copy of each simple module.

Theorem 14.1.5 (V.Camillo). *Let M be an A-module. Then M is a distributive module if and only if M/N has square-free socle for every submodule N.*

Proof. Necessity. Every quotient and submodule of a distributive module is distributive, so that if M/N contains a submodule of the form $U \oplus U$, then M is not a distributive module. Simply because $U \oplus U$ is not distributive module. Indeed, for the diagonal $D(U \oplus U) = \{(u,u) \mid n \in U\}$ of $U \oplus U$ we have $D(U) \cap (U \oplus U) = D(U)$ and $D(U) \cap (U \oplus 0) = 0$ and $D(U) \cap (0 \oplus U) = 0$.

Conversely. Let $m, n \in M$. We show that $(m : n) + (n : m) = A$. Let K be a maximal right ideal of A and $U = A/K$. Consider the quotient module $mA + nA/mK + nK$. The socle of $mA + nA/mK + nK$ doesn't contain $U \oplus U$ if one of the following conditions hold:

(1) $m \in nA + mK + nK = nA + mK$;

(2) $n \in mA + mK + nK = mA + nK$.

In case (1) we have $m = na + nK$ or $m(1-k) = na$. So $(1-k) \in (n : m)$. Since $(1-k) \notin K$, we have $(n : m) \not\subseteq K$. In case (2) analogously $(m : n) \not\subseteq K$.

Theorem 14.1.6. *A semiprimary right semidistributive ring A is right Artinian.*

Proof. It is sufficient to show that each indecomposable projective A-module $P = eA$ is Artinian (e is a nonzero idempotent of A). Let m be the minimal natural number with $PR^m = 0$. Since the module P is distributive, by theorem 14.1.5, the quotient module PR^i/PR^{i+1} decomposes into a finite direct sum of simple modules ($i = 1, \ldots, m-1$). Thus, the module P possesses a composition series and the module P is Artinian.

14.2 REDUCTION THEOREM FOR $SPSD$-RINGS

We write $SPSDR$**-ring** ($SPSDL$**-ring**) for a semiperfect right (left) semidistributive ring and $SPSD$**-ring** for a semiperfect semidistributive ring.

Theorem 14.2.1 (A.Tuganbaev). *A semiperfect ring A is right (left) semidistributive if and only if for any local idempotents e and f of the ring A the set eAf is a uniserial right fAf-module (uniserial left eAe-module).*

Proof. Obviously one may take A to be reduced. We shall prove the theorem for the right case.

Let $A_A = P_1 \oplus \ldots \oplus P_s$ be the decomposition of the ring A into a direct sum of the pairwise non-isomorphic projective indecomposable A-modules, with $1 = f_1 + \ldots + f_s$ the corresponding decomposition of $1 \in A$ into a sum of pairwise orthogonal local idempotents, $A_{ij} = f_i A f_j$. We shall show that if A is right semidistributive, then A_{ij} is a uniserial right A_{jj}-module. Indeed, if A_{ij} is not a right uniserial A_{jj}-module, then there exist submodules X_1 and X_2 of module A_{ij} such that one can find elements $x_1 \in X_1$ and $x_2 \in X_2$, satisfying $x_1 \notin X_2$ and $x_2 \notin X_1$. Set $N = x_1 A_{jj} + x_2 A_{jj}$ and $\tilde{N} = NA$. If N is a cyclic A_{jj}-module, then there exists a unique maximal submodule (since A_{jj} is local)

and either $N = x_1A_{jj}$ or $N = x_2A_{jj}$. We have $\tilde{N}/\tilde{N}R = U_j \oplus U_j$, where $U_j = P_j/P_jR$. So, by theorem 14.1.5 the submodule $\tilde{N}$ of P_i is not distributive. Consequently, A_{ij} is a right uniserial A_{jj}-module. Now let's show that for any two local idempotents e and f of the ring A the set eAf is a right uniserial fAf-module. Write $f = f_1$ and $e = e_1$. Let $1 = e_1 + \ldots + e_n = f_1 + \ldots + f_n$ be two decompositions of $1 \in A$ into a sum of pairwise orthogonal local idempotents. By lemma 11.1.4 $e_1 = af_{\sigma(1)}a^{-1}$ for a certain $a \in A$. Then the right A_{11}-module $e_1Af_1 = af_{\sigma(1)}a^{-1}Af_1 = af_{\sigma(1)}Af_1 = aA_{\sigma(1)1}$ is isomorphic to the right A_{11}-module $A_{\sigma(1)1}$ (the isomorphism is realized by multiplying by the invertible element $a \in A$). So eAf is a right uniserial fAf-module.

The next step is to show that if eAf is a right uniserial fAf-module for any local idempotents e, $f \in A$, then A is right semidistributive.

Any submodule N of a indecomposable projective module $P = eA$ has the following Peirce decomposition $N = Nf_1 \oplus \ldots \oplus Nf_s$, where $Nf_1, \ldots, Nf_s$ are Abelian groups.

Finally, the socle of the quotient module P/N is square-free. Indeed, let Y be a submodule of N such that Y/N is simple. By the Q-Lemma there exist a unique number i such that $Yf_k = Nf_k$ for $k \neq i$ and Yf_i strictly contains Nf_i. This means $Y/N \simeq U_i$. If $P \supset Y_1 \supset N$ and $Y_1/N \simeq U_i$ then by the Q-Lemma $Y_1f_k = Nf_k$ for $k \neq i$ and Y_1f_i strictly contains Nf_i. Then $Y_1f_i = Yf_i$ and $Y = Y_1$. So P is distributive by theorem 14.1.5.

Theorem 14.2.1 has the following corollary.

Corollary 14.2.2. *Let A be a semiperfect ring, and let $1 = e_1 + ... + e_n$ be a decomposition of $1 \in A$ into a sum of mutually orthogonal local idempotents. The ring A is right (left) semidistributive if and only if for any idempotents e_i and e_j of the above decomposition, the set e_iAe_j is a uniserial right e_jAe_j-module (left e_iAe_i-module).*

Corollary 14.2.3 (Reduction Theorem for $SPSD$-rings). *Let A be a semiperfect ring, and let $1 = e_1 + ... + e_n$ be a decomposition of $1 \in A$ in a sum of mutually orthogonal local idempotents. The ring A is right (left) semidistributive if and only if for any idempotents e_i and e_j $(i \neq j)$ of the above decomposition the ring $(e_i + e_j)A(e_i + e_j)$ is right (left) semidistributive.*

Proof. It is sufficient to prove the corollary for a reduced ring A. If A is right semidistributive, then e_iAe_j is right uniserial e_jAe_j-module $(i \neq j)$ and the ring e_iAe_i is right uniserial for $i = 1, \ldots, n$. By corollary 14.2.2, the ring $(e_i+e_j)A(e_i+e_j)$ is right semidistributive. Conversely, if the ring $(e_i+e_j)A(e_i+e_j)$ is right semidistributive, then, by theorem 14.2.1, the set e_iAe_j is a uniserial right A_{jj}-module and, by corollary 14.2.2, the ring A is right semidistributive.

Corollary 14.2.4. *Let A be a Noetherian $SPSD$-ring, and let $1 = e_1 + \cdots + e_n$ be a decomposition of the identity $1 \in A$ into a sum of mutually orthogonal local*

idempotents, let $A_{ij} = e_i A e_j$ *and let* R_i *be the Jacobson radical of a ring* A_{ii}. *Then* $R_i A_{ij} = A_{ij} R_j$ *for* $i, j = 1, \ldots, n$.

Proof. By theorems 3.6.1 and 14.2.1, A_{ij} is a cyclic uniserial right A_{jj}-module and a cyclic uniserial left A_{ii}-module. By Nakayama's Lemma, $A_{ij}R_j$ is the unique proper maximal A_{jj}-submodule in A_{ij} and $R_i A_{ij}$ is the unique maximal left A_{ii}-submodule in A_{ij}. Since $R_i A_{ij}$ is a right A_{jj}-module and a left A_{ii}-module, we have $R_i A_{ij} = A_{ij} R_{jj}$.

Example 14.2.1.
Consider

$$A = \begin{pmatrix} \mathbf{R} & \mathbf{C} \\ 0 & \mathbf{C} \end{pmatrix}$$

as an $\mathbf{R}$-algebra ($\mathbf{R}$ is the field of real numbers, $\mathbf{C}$ is the field of complex numbers). The Peirce decomposition of the Jacobson radical $R = R(A)$ has the form

$$R = \begin{pmatrix} 0 & \mathbf{C} \\ 0 & 0 \end{pmatrix}$$

and the $\mathbf{R}$-algebra A is right serial, i.e., right semidistributive.

The left indecomposable projective $Q_2 = \begin{pmatrix} \mathbf{C} \\ \mathbf{C} \end{pmatrix}$ has socle $\begin{pmatrix} \mathbf{C} \\ 0 \end{pmatrix}$, which is a direct sum of two copies of the left simple module $\begin{pmatrix} \mathbf{R} \\ 0 \end{pmatrix}$. Consequently, by theorem 14.1.1, the $\mathbf{R}$-algebra A is an $SPSDR$-ring but it is not an $SPSDL$-ring.

14.3 QUIVERS OF *SPSD*-RINGS

Recall that a quiver without multiple arrows and multiple loops is called a **simply laced quiver**. Let A be an $SPSD$-ring. By theorem 14.1.6, the quotient ring A/R^2 is right Artinian and its quiver $Q(A)$ is defined by $Q(A) = Q(A/R^2)$.

Theorem 14.3.1. *The quiver* $Q(A)$ *of an SPSD-ring* A *is simply laced. Conversely, for any simply laced quiver* Q *there exists an SPSD-ring* A *such that* $Q(A) = Q$.

Proof. We may assume that A is reduced and $R^2 = 0$. Let $A_A = P_1 \oplus \ldots \oplus P_s$, where $P_1, \ldots, P_s$ are indecomposable. Then $P_i R$ is a semisimple A-module:

$$P_i R = \bigoplus_{j=1}^{s} U_j^{t_{ij}},$$

where $U_J = P_j / P_j R$ are simple. The A-module $P_i R$ is a submodule of a distributive A-module and, therefore, $P_i R$ is distributive. By the definition of $Q(A)$ we

have $[Q(A)] = (t_{ij})$ and, by theorem 14.1.5, $0 \leq t_{ij} \leq 1$. So $Q(A)$ is a simply laced quiver.

Conversely, let kQ be the path k-algebra of a simply laced quiver Q and J be its fundamental ideal, i.e., the ideal generated by all arrows of Q. Write $B = kQ/J^2$ and $\pi : kQ \to B$ for the natural epimorphism. Let $\pi(\varepsilon_i) = e_i$, where $\varepsilon_1, \ldots, \varepsilon_s$ are all paths of length zero. Then $B = e_1B \oplus \ldots \oplus e_sB$, where $e_1B, \ldots, e_sB$ are indecomposable. Let R be the Jacobson radical of B and $AQ = \{\sigma_{ij}\}$ be the set of all arrows of Q. The elements $\pi(\sigma_{mp})$, where $\sigma_{mp} \in AQ$ form a basis of e_mR. Obviously, $e_mR^2 = 0$ for $m = 1, \ldots, s$. So, e_mR is the semisimple module and $e_mR = \underset{p}{\oplus} U_p$ for all those p, where $\sigma_{mp} \in AQ$. Therefore $Q(B) = Q$ and e_mR is a distributive module, by theorem 14.5.1. Thus, B is a right semidistributive ring. The analogous arguments show that B is a left semidistributive ring.

So $B = kQ/J^2$ is an $SPSD$-algebra over a field k and $Q(B) = Q$.

Corollary 14.3.2. *The link graph $\mathcal{L}G(A)$ of an $SPSD$-ring A coincides with a $Q(A)$.*

Proof. For any $SPSD$-ring A the following equalities hold: $\mathcal{L}G(A) = Q(A, R) = Q(A)$.

Theorem 14.3.3. *For an Artinian ring A with $R^2 = 0$ the following conditions are equivalent:*

(a) *A is semidistributive;*

(b) *$Q(A)$ is simply laced and the left quiver $Q'(A)$ can be obtained from $Q(A)$ by reversing all arrows.*

Proof.

$(a) \Longrightarrow (b)$. By theorem 14.3.1 it is sufficient to show that $Q'(A)$ can be obtained from $Q(A)$ by reversing all arrows. One can assume that A is reduced. Write A_A as a direct sum $A_A = P_1 \oplus \ldots \oplus P_s$, where the P_i are indecomposable projective and let $1 = e_1 + \cdots e_s$ be the corresponding decomposition of $1 \in A$ into a sum of mutually orthogonal local idempotents. If $A_{ij} = e_iAe_j \neq 0$, then, in view of corollary 14.2.4,

$$A_{ij}R_j = R_iA_{ij} \text{ and } A_{ij} \subset R \text{ for } i \neq j.$$

Hence, $A_{ij}R_j = R_iA_{ij} = 0$ for $i \neq j$ and, in view of the Q-Lemma, it follows that there is a loop at the vertex i both in $Q(A)$ and in $Q'(A)$. Thus the left quiver $Q'(A)$ can be obtained from $Q(A)$ by reversing all arrows.

$(b) \Longrightarrow (a)$. By the Peirce decomposition for R we have: $R = \underset{i,j=1}{\overset{s}{\bigoplus}} e_iRe_j$, $e_iRe_i = R_i$ and $e_iRe_j = A$, $i \neq j$; $i, j = 1, \ldots, s$.

It follows that

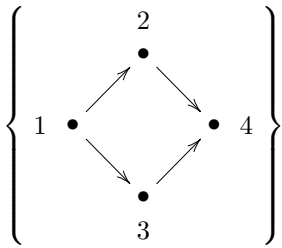
$$P_iR = (A_{i1}, \ldots, A_{ii-1}, R_i, A_{ii+1}, \ldots, A_{is})$$

for $i = 1, \ldots, s$. If $A_{ij} \neq 0$, for $i \neq j$, then, in view of the Q-Lemma, A_{ij} is a

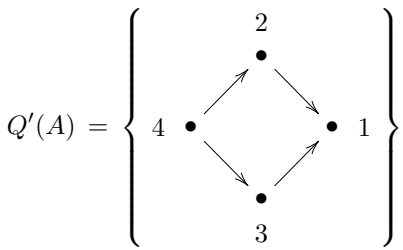
simple right A_{jj}-module and a simple left A_{ii}-module. If $R_i \neq 0$, then R_i is a simple A_{ii}-module and a left simple A_{ii}-module. Thus, in view of theorem 14.2.1, the ring A is semidistributive.

Remark. The implication $(b) \Longrightarrow (a)$ isn't true even in the case of finite dimensional algebras as is shown by the following example.

Let $A = kQ_4$ be the path k-algebra of the quiver Q_4

$Q_4 =$ 

The basis of kQ_4 is $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \sigma_{12}, \sigma_{13}, \sigma_{24}, \sigma_{34}, \sigma_{12}\sigma_{24}, \sigma_{13}\sigma_{34}$. The indecomposable projective A-modules are: $P_1 = \{\varepsilon_1, \sigma_{12}, \sigma_{13}, \sigma_{12}\sigma_{24}, \sigma_{13}\sigma_{34}\}$; $P_2 = \{\varepsilon_2, \sigma_{24}\}$; $P_3 = \{\varepsilon_3, \sigma_{34}\}$; $P_4 = \{\varepsilon_4\}$. Obviously, $soc\, P_1 \simeq P_4 \oplus P_4$. By theorem 14.1.5, P_1 is not distributive, but $Q(A) = Q_4$ and

$Q'(A) =$ 

i.e., A satisfies condition (b) of theorem 14.3.3.

Definition. A semiperfect ring A such that A/R^2 is Artinian will be called **Q-symmetric** if the left quiver $Q'(A)$ can be obtained from the right quiver $Q(A)$ by reversing all arrows.

Corollary 14.3.4. *Every SPSD-ring is Q-symmetric.*

Remark. Example 14.2.1 shows that an $SPSDR$-ring is not always Q-symmetric.

14.4 SEMIPRIME SEMIPERFECT RINGS

In this section we shall describe the minors of first and second order of right Noetherian semiprime $SPSD$-rings.

Definition. The endomorphism ring of an indecomposable projective module over a semiperfect ring is called a **principal endomorphism ring**.

Proposition 14.4.1. *An Artinian principal endomorphism ring of a semiprime semiperfect ring is a division ring.*

Proof. This ring is an Artinian prime local ring and, consequently, is a division ring.

Lemma 14.4.2. *Let* $A_A = P_1^{n_1} \oplus P_2^{n_2} \oplus \ldots \oplus P_s^{n_s}$ *be the decomposition of a semiprime semiperfect ring* A *into principal modules and let* $End_A(P_1) = D_1$ *be a division ring. Then* $A = M_{n_1}(D_1) \times End(P_2^{n_2} \oplus \ldots \oplus P_s^{n_s})$.

Proof. Let $1 = f_1 + \ldots + f_s$ be a canonical decomposition of $1 \in A$ into a sum of pairwise orthogonal idempotents, i.e., $f_iA = P_i^{n_i}$ for $i = 1, \ldots, s$. Let $f_1Af_1 = A_1$, $(1 - f_1)A(1 - f_1) = A_2$, $X = f_1A(1 - f_1)$, $Y = (1 - f_1)Af_1$. If either $X \neq 0$ or $Y \neq 0$, then $K = \begin{pmatrix} 0 & X \\ Y & YX \end{pmatrix}$ is a nilpotent ideal and we have the contradiction. So $X = 0$, $Y = 0$, proving the lemma.

Theorem 14.4.3 (Decomposition theorem for semiprime semiperfect rings). *A semiprime semiperfect ring is a finite direct product of indecomposable rings. An indecomposable semiprime semiperfect ring is either a simple Artinian ring or an indecomposable semiprime semiperfect ring such that all its principal endomorphism rings are non-Artinian.*

A proof immediately follows from lemma 14.4.2.

Let $1 = g_1 + g_2$ be a decomposition of the identity of A into a sum of the mutually orthogonal idempotents, and let $A = (A_{ij})$ be the corresponding Peirce decomposition of A, i.e., $A_{ij} = g_iAg_j$, $i, j = 1, 2$. Similarly, if M is a two-sided ideal of A, then $M = (M_{ij})$ is the Peirce decomposition of M, where $M_{ij} = g_iMg_j$, $i, j = 1, 2$.

Lemma 14.4.4. *Let* $M = (M_{ij})$ *be a two-sided ideal of a semiprime ring* A. *If* $M_{ij} \neq 0$ *for* $i \neq j$, *then* $M_{ji} \neq 0$. *Moreover, if* $M_{ij} \neq 0$ *for* $i \neq j$, *then* $M_{ij}M_{ji} \neq 0$ *and* $M_{ji}M_{ij} \neq 0$.

Proof. Let $M_{ij}M_{ji} = 0$. Clearly, $Z = M_{ij}A_{ji} + A_{ij}M_{ji} + M_{ij} + M_{ji}$ is a two-sided ideal and $Z^8 = 0$. The remaining cases are treated analogously.

Corollary 14.4.5. *Let* $1 = e_1 + \ldots + e_n$ *be a decomposition of the identity of* A *into a sum of the mutually orthogonal idempotents,* $A_{ij} = e_iAe_j$, $i, j = 1, \ldots, n$, *and let* M *be a two sided ideal in* A, $M_{ij} = e_iMe_j$, $i, j = 1, \ldots, n$. *If* $M_{ij} \neq 0$ *for* $i \neq j$, *then* $M_{ji} \neq 0$ *and* $M_{ij}M_{ji} \neq 0$, $M_{ji}M_{ij} \neq 0$. *Moreover, from the equality* $A_{ij}A_{ji} = 0$ *it follows that* $A_{ij} = 0$ *and* $A_{ji} = 0$.

Theorem 14.4.6. *For a semiprime semiperfect ring A the following conditions are equivalent:*

(1) *A is a finite direct product of prime rings;*

(2) *all principal endomorphism rings of A are prime.*

Proof.

(1) $\Rightarrow$ (2) follows from proposition 9.2.13.

(2) $\Rightarrow$ (1). Obviously, we can assume that A is indecomposable and reduced. Let $1 = e_1 + \ldots + e_n$ be a decomposition of $1 \in A$ into the sum of pair-wise orthogonal local idempotents. We shall prove the theorem by induction on n. The case $n = 1$ is obvious. Suppose that A is not prime. Then there exist two-sided nonzero ideals M, N such that $MN = 0$. Let $h_1 = e_1 + \ldots + e_{n-1}$ and $h_2 = e_n$. We have the equality $h_1Mh_1Nh_1 = 0$. By the induction hypothesis either $h_1Mh_1 = 0$ or $h_1Nh_1 = 0$. Let $h_1Mh_1 = 0$, then by corollary 14.4.5 $h_1Mh_2 = 0$ and $h_2Mh_1 = 0$. If $h_2Mh_2 = 0$, then the theorem is proved, so $h_2Mh_2 \neq 0$ and $h_2Nh_2 = 0$. We have again $h_2Nh_1 = 0$ and $h_1Nh_2 = 0$. One can assume that $e_iNe_i \neq 0$ for $i = 1, \ldots, t$ and $e_jNe_j = 0$ for $j = t+1, \ldots, n$. So $N_{ii}A_{ij} = 0$ for $i = 1, \ldots, t$ and $j = t+1, \ldots, n$. Consequently, $N_{ii}A_{ij}A_{ji} = 0$ for the same i and j. Since the A_{ii} are prime, it follows that $A_{ij}A_{ji} = 0$. By corollary 14.4.5, we obtain $A_{ij} = 0$ and $A_{ji} = 0$ for $i = 1, \ldots, t$ and $j = t+1, \ldots, n$. Hence, the ring A is decomposable and we obtain a contradiction, which proves the theorem.

Proposition 14.4.7. *Every minor of an SPSD-ring is an SPSD-ring.*

The proof follows from theorem 14.2.1 and corollary 14.2.2.

Corollary 14.4.8. *Every minor of a right Noetherian semiprime SPSD-ring is a right Noetherian semiprime SPSD-ring.*

The proof follows from theorem 3.6.1 and proposition 9.2.13.

From theorems 14.2.1 and 3.6.1 we obtain the following statement.

Corollary 14.4.9. *Every minor of a Noetherian SPSD-ring is a Noetherian SPSD-ring.*

Proposition 14.4.10. *A minor of the first order of a right Noetherian SPSD-ring is uniserial and it is either a discrete valuation ring or an Artinian uniserial ring.*

A proof follows from theorem 14.2.1, theorem 3.6.1 and proposition 13.3.1.

Corollary 14.4.11. *A minor of the first order of a right Noetherian semiprime SPSD-ring is either a discrete valuation ring or a division ring.*

Definition. A ring A is called **semimaximal** if it is a semiperfect semiprime

right Noetherian ring such that for each local idempotent $e \in A$ the ring eAe is a discrete valuation ring (not necessarily commutative), i.e., all principal endomorphism rings of A are discrete valuation rings.

Proposition 14.4.12. *A semimaximal ring is a finite direct product of prime semimaximal rings.*

A proof follows from theorem 14.4.6.

So, a semimaximal ring A is indecomposable if and only if A is prime.

Proposition 14.4.13. *A semiperfect reduced indecomposable ring B is a second order minor of a right Noetherian semiprime SPSD-ring if and only if B is semimaximal.*

Proof. Let $1 = e_1 + e_2$ be a decomposition of $1 \in B$ into a sum of local idempotents, let $B = \bigoplus\limits_{i,j=1}^{2} e_i B e_j$ be the corresponding two-sided Peirce decomposition, and let $B_{ij} = e_i B e_j$ $(i, j = 1, 2)$. The Jacobson radical R of B has the form: $R = \begin{pmatrix} R_1 & B_{12} \\ B_{21} & R_2 \end{pmatrix}$, where R_i is the Jacobson radical of B_{ii} $(i = 1, 2)$. Obviously,

$$R^2 = \begin{pmatrix} R_1^2 + B_{12}B_{21} & R_1B_{12} + B_{12}R_2 \\ R_2B_{21} + B_{21}R_1 & R_2^2 + B_{21}B_{12} \end{pmatrix}.$$

By corollary 14.4.10, B_{ii} is either a discrete valuation ring or a division ring. If $B_{11} = D$ is a division ring, then $R = \begin{pmatrix} 0 & B_{12} \\ B_{21} & R_2 \end{pmatrix}$. Obviously, $J = \begin{pmatrix} 0 & B_{12} \\ B_{21} & B_{21}B_{12} \end{pmatrix}$ is a nonzero ideal in B and $J^2 = 0$. So B is semimaximal.

Let's now show that a semimaximal ring B is semidistributive. We can assume that B is prime. Let $R_i = \pi_i B_{ii} = B_{ii}\pi_i$ $(i = 1, 2)$. Now $b_{12}b_2 \neq 0$ for any $b_{12} \neq 0$ and $b_2 \neq 0$ $(b_{12} \in B_{12}, b_2 \in B_{22})$. Indeed, we can suppose that $b_2 = \pi_2^m$. Then $\begin{pmatrix} 0 & b_{12} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & b_2 \end{pmatrix} \neq 0$ and, consequently, $b_{12}B_{22}\pi_2^m = b_{12}\pi_2^m B_{22} \neq 0$. So, $b_{12}\pi_2^m \neq 0$. Analogously, $b_{ij}b_j \neq 0$ and $b_i b_{ij} \neq 0$ for $i, j = 1, 2$. Further $b_{ij}b_{ji} \neq 0$ for $i \neq j$ and both factors are nonzero. We shall prove that $b_{21}b_{12} \neq 0$ for $b_{12} \neq 0$ and $b_{21} \neq 0$. Indeed, $\begin{pmatrix} 0 & b_{12} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} \begin{pmatrix} 0 & 0 \\ b_{21} & 0 \end{pmatrix} \neq 0$. So, $b_{12}B_{22}b_{21} \neq 0$ and thus there exists $b_2 \in B_{22}$ such that $b_{12}b_{22}b_{21} \neq 0$. If $b_{21}b_{12} = 0$, then $b_{21}b_{12}b_{22}b_{21} = 0$ and we obtain a contradiction.

Next B_{12} is a uniserial right B_{22}-module and a uniserial left B_{11}-module. By theorem 3.6.1, B_{12} is a finitely generated B_{22}-module. Consequently, if B_{12} isn't uniserial, then $B_{12} = B_{12}^{(1)} \oplus B_{12}^{(2)}$, where $B_{12}^{(1)}$ and $B_{12}^{(2)}$ are nonzero B_{22}-

submodules of B_{12}. Let $b_{21} \neq 0$. Then $b_{21}B_{12} = b_{21}B_{12}^{(1)} \oplus b_{21}B_{12}^{(2)}$, where $b_{21}B_{12}^{(1)}$ and $b_{21}B_{12}^{(1)}$ are the nonzero right ideals in $\mathcal{O}_2$. This is a contradiction. Consequently, B_{12} is a uniserial right B_{22}-module.

Finally B_{12} is a uniserial left B_{11}-module. If this isn't true, then there exists a left B_{11}-submodule N_{12} with two noncyclic generators in B_{12}. Consequently, $N_{12} = N_{12}^{(1)} \oplus N_{12}^{(2)}$ is a direct sum of two nonzero left B_{11}-submodules and so $N_{12}b_{21} = N_{12}^{(1)}b_{21} \oplus N_{12}^{(2)}b_{21}$ is a direct sum of two nonzero left ideals in B_{11} for any nonzero b_{21}. This is a contradiction and so B_{12} is a uniserial left B_{11}-module. Analogously, B_{21} is a uniserial right B_{11}-module and a uniserial left B_{22}-module. Thus, by theorem 14.2.1 B is semidistributive. The proposition is proved.

Corollary 14.4.14. *An intersection of a finite number of nonzero submodules of an indecomposable projective module over a Noetherian prime SPSD- ring is nonzero.*

We leave the proof of this corollary to the reader as an exercise.

Lemma 14.4.15. *A local idempotent of a Noetherian prime SPSD-ring A is a local idempotent of its classical ring of fractions.*

Proof. By proposition 9.3.10 A is a right order in the simple Artinian ring $Q = M_n(\mathcal{D})$. One can assume that the local idempotent $e \in A$ is a sum of matrix idempotents $e = e_{i_1i_1} + \ldots + e_{i_ki_k}$. Let $k \geq 2$. Then there exist $q_1, \ldots, q_k \in Q$ such that $e_{i_1i_1}q_1, \ldots, e_{i_ki_k}q_k \in A$ and, consequently, $e_{i_1i_1}q_1A, \ldots, e_{i_ki_k}q_kA$ are nonzero right submodules of the right indecomposable projective module eA and $e_{i_mi_m}q_mA \cap e_{i_pi_p}q_pA = 0$ for $m \neq p$. We obtain a contradiction with corollary 14.4.14.

14.5 RIGHT NOETHERIAN SEMIPRIME *SPSD*-RINGS

The following is a **decomposition theorem** for semiprime right Noetherian *SPSD*-rings.

Theorem 14.5.1. *The following conditions for a semiperfect semiprime right Noetherian ring A are equivalent:*

(a) *the ring A is semidistributive;*

(b) *the ring A is a direct product of a semisimple Artinian ring and a semimaximal ring.*

Proof.

(a)⇒(b). From theorem 14.4.3 it follows that A is a finite direct product of indecomposable semiprime rings. Every indecomposable ring is either a simple Artinian ring or a semiprime semiperfect ring such that all its principal endomorphism rings are non-Artinian. In the second case, by corollary 14.4.11, such a ring is semimaximal.

(b)⇒(a). Obviously, a semiprime Artinian ring is a semiprime $SPSD$-ring. A semimaximal ring is an $SPSD$-ring, by proposition 14.4.3 and the reduction theorem for $SPSD$-rings.

Theorem 14.5.2. *Each semimaximal ring is isomorphic to a finite direct product of prime rings of the following form:*

$$A = \begin{pmatrix} \mathcal{O} & \pi^{\alpha_{12}}\mathcal{O} & \dots & \pi^{\alpha_{1n}}\mathcal{O} \\ \pi^{\alpha_{21}}\mathcal{O} & \mathcal{O} & \dots & \pi^{\alpha_{2n}}\mathcal{O} \\ \dots & \dots & \dots & \dots \\ \pi^{\alpha_{n1}}\mathcal{O} & \pi^{\alpha_{n2}}\mathcal{O} & \dots & \mathcal{O} \end{pmatrix}, \tag{14.5.1}$$

where $n \geq 1$, $\mathcal{O}$ is a discrete valuation ring with a prime element π, and the α_{ij} are integers such that $\alpha_{ij} + \alpha_{jk} \geq \alpha_{ik}$ for all i, j, k ($\alpha_{ii} = 0$ for any i).

Proof. By proposition 14.4.12 a semimaximal ring is a finite direct product of prime semimaximal rings. We shall show, that a prime semimaximal ring is isomorphic to a ring of form (14.5.1).

Let $1 = e_1 + \ldots + e_m$ be a decomposition of $1 \in A$ into a sum of pairwise orthogonal local idempotents, $A_{ij} = e_i A e_j$ for $i, j = 1, \ldots, m$. Denote by B_{ij} ($i \neq j$) the following second order minor: $B_{ij} = \begin{pmatrix} A_{ii} & A_{ij} \\ A_{ji} & A_{jj} \end{pmatrix}$. If B_{ij} isn't reduced, then $B_{ij} \simeq M_2(A_{ii})$ and B_{ij} is left Noetherian. If B_{ij} is reduced, then $A_{ij}a_{ji} \subset A_{ij}$, $\varphi_{ji} : A_{ij} \to A_{ii}$ being the monomorphism of left A_{ii}-modules (for any nonzero a_{ji}) such that $\varphi_{ji}(a_{ij}) = a_{ij}a_{ji}$. If A_{ij} isn't finitely generated, then A_{ii} contains a non finitely generated left A_{ii}-submodule $A_{ij}a_{ji}$, where $a_{ji} \neq 0$. This gives a contradiction. So, by lemma 13.3.4, $A_{ij} \simeq A_{ii}$ and B_{ij} is left Noetherian, by theorem 3.6.1. Applying induction on m and theorem 3.6.1, we see that A is left Noetherian. Consequently, A is a prime Noetherian $SPSD$-ring. By proposition 9.3.10, A is a right order in a simple Artinian ring $Q = M_n(\mathcal{D})$. Suppose that every local idempotent e_i from the above decomposition $1 = e_1 + \ldots + e_m$ is local in $M_n(\mathcal{D})$. Hence, the two decompositions: $1 = e_1 + \ldots + e_m$ and $1 = e_{11} + \ldots + e_{nn}$ are conjugate. Consequently, $m = n$ and we can assume that the matrix idempotents are the local idempotents of A.

Denote A_{ii} by A_i. We have $Q = \sum\limits_{i,j=1}^{n} e_{ij}\mathcal{D}$ ($\mathcal{D}$ is a division ring, the e_{ij} are matrix units commuting with the elements from $\mathcal{D}$) and $A = \sum\limits_{i,j=1}^{n} e_{ij}A_{ij}$, where $A_{ij} \subset \mathcal{D}$. All A_i are discrete valuations rings, $A_{ij}A_{jk} \subset A_{ik}$ and $A_{ij} \neq 0$ for $i, j = 1, \ldots, n$ (A is prime and $e_{ii}Ae_{jj} = A_{ij} \neq 0$).

We shall prove that $A_{ij} = d_{ij}A_j = A_i d_{ij}$, where $d_{ij} \in A_{ij} \subset \mathcal{D}$. Indeed, let R_i be the Jacobson radical of A_i and let $\pi_i A_i = A_i \pi_i = R_i$. By corollary 14.2.4, $R_i A_{ij} = A_{ij} R_j$. Take an element $0 \neq d_{ij} \in A_{ij}$ so that $A_i d_{ij} + R_i A_{ij} = A_{ij}$. By Nakayama's Lemma $A_{ij} = d_{ij}A_j = A_i d_{ij}$. Let

$T = diag\,(d_{12}^{-1}, d_{23}^{-1}, \ldots, d_{n-1n}^{-1}, 1)$. Consider TAT^{-1}. One can assume that the following equalities $d_{12} = \ldots = d_{n-1n}$ hold in A, hence $A_1 = A_2 = \ldots = A_n$. Write $A_1 = \mathcal{O}$, where $\mathcal{O}$ is a discrete valuation ring (non-necessarily commutative). Consequently, $A_{ij} \supset \mathcal{O}$ for $i \leq j$. From $A_{ij}A_{ji} \subset \mathcal{O}$ we have $A_{ij}A_{ji} \supset A_{ji}$ and $A_{ji} \subset \mathcal{O}$ for $j \leq i$. So, one can assume that $d_{ji} = \pi^{\alpha_{ji}}$, where $\mathcal{M} = \pi\mathcal{O} = \mathcal{O}\pi$ is the unique maximal ideal of $\mathcal{O}$, $\alpha_{ji} \geq 0$ for $j \geq i$. Obviously, $d_{ij} = \pi^{\alpha_{ij}}$, where $\alpha_{ij} \geq -\alpha_{ji}$. Hence, we obtain a ring of the form 14.5.1. The converse assertion follows from the definition of a semimaximal ring.

Definition. A ring A is called a **tiled order** if it is a prime Noetherian SPSD-ring with nonzero Jacobson radical.

Remark. Let $\mathcal{O}$ be a discrete valuation ring. Then from theorems 14.5.1 and 14.5.2 it follows that each tiled order is of the form (14.5.1).

The ring $\mathcal{O}$ is embedded into a classical ring of fractions $\mathcal{D}$, which is a division ring. Therefore (14.5.1) denotes the set of all matrices $(a_{ij}) \in M_n(\mathcal{D})$ such that $a_{ij} \in \pi^{\alpha_{ij}}\mathcal{O} = e_{ii}Ae_{jj}$, where the $e_{11}, \ldots, e_{nn}$ are the matrix units of $M_n(\mathcal{D})$. It is clear that $M_n(\mathcal{D})$ is the classical ring of fractions of A.

According to the terminology of V.A.Jategaonkar and R.B.Tarsy, a ring $A \subset M_n(K)$, where K is the quotient field of a commutative discrete valuation ring $\mathcal{O}$, is called a tiled order over $\mathcal{O}$, if $M_n(K)$ is the classical ring of fractions of A, $e_{ii} \in A$ and $e_{ii}Ae_{ii} = \mathcal{O}$ for $i = 1, \ldots, n$, where the $e_{11}, \ldots, e_{nn}$ are the matrix units of $M_n(K)$ (see *V.A.Jategaonkar, Global dimension of tiled orders over a discrete valuation ring // Trans. Amer. Math. Soc., 196, 1974, pp. 313-330*).

Thus, our definition of a tiled order is a generalization of the definition of a tiled order over a discrete valuation ring in the sense of V.A.Jategaonkar and R.B.Tarsy.

Denote by $M_n(\mathbf{Z})$ the ring of all square $n \times n$-matrices over the ring of integers $\mathbf{Z}$. Let $\mathcal{E} \in M_n(\mathbf{Z})$. We shall call a matrix $\mathcal{E} = (\alpha_{ij})$ an **exponent matrix** if $\alpha_{ij} + \alpha_{jk} \geq \alpha_{ik}$ for $i, j, k = 1, \ldots, n$ and $\alpha_{ii} = 0$ for $i = 1, \ldots, n$. A matrix $\mathcal{E}$ is called a **reduced exponent matrix** if $\alpha_{ij} + \alpha_{ji} > 0$ for $i, j = 1, \ldots, n$.

We shall use the following notation: $A = \{\mathcal{O}, \mathcal{E}(A)\}$, where $\mathcal{E}(A) = (\alpha_{ij})$ is the exponent matrix of a ring A, i.e., $A = \sum_{i,j=1}^{n} e_{ij}\pi^{\alpha_{ij}}\mathcal{O}$, where the e_{ij} are the matrix units. If a tiled order is reduced, then $\alpha_{ij} + \alpha_{ji} > 0$ for $i, j = 1, \ldots, n$, $i \neq j$, i.e., $\mathcal{E}(A)$ is reduced.

Definition. Let $\mathcal{O}$ be a discrete valuation ring. A right (resp. left) A-module M (resp. N) is called a **right** (resp. **left**) **A-lattice** if M (resp. N) is a finitely generated free $\mathcal{O}$-module.

For example, all finitely generated projective A-modules are A-lattices.

Given a tiled order A we denote by $Lat_r(A)$ (resp. $Lat_l(A)$) the category of right (resp. left) A-lattices. We denote by $S_r(A)$ (resp. $S_l(A)$) the partially

ordered set (by inclusion), formed by all A-lattices contained in a fixed simple $M_n(\mathcal{D})$-module U (resp. in a left simple $M_n(\mathcal{D})$-module V). Such A-lattices are called **irreducible**.

Note that every simple right $M_n(\mathcal{D})$-module is isomorphic to a simple $M_n(\mathcal{D})$-module U with $\mathcal{D}$-basis $e_1, \ldots, e_n$ such that $e_i e_{jk} = \delta_{ij} e_k$, where $e_{jk} \in M_n(\mathcal{D})$ are the matrix units. Respectively, every simple left $M_n(\mathcal{D})$-module is isomorphic to a left simple $M_n(\mathcal{D})$-module V with $\mathcal{D}$-basis $e_1, \ldots, e_n$ such that $e_{ij} e_k = \delta_{jk} e_i$.

Let $A = \{\mathcal{O}, \mathcal{E}(A)\}$ be a tiled order, and let U (resp. V) be a simple right (resp. left) $M_n(\mathcal{D})$-module as above.

Then any right (resp. left) irreducible A-lattice M (resp. N) lying in U (resp. in V) is an A-module with $\mathcal{O}$-basis $(\pi^{\alpha_1} e_1, \ldots, \pi^{\alpha_n} e_n)$, while

$$\begin{cases} \alpha_i + \alpha_{ij} \geq \alpha_j, \text{ for the right case;} \\ \alpha_{ij} + \alpha_j \geq \alpha_i, \text{ for the left case.} \end{cases} \tag{14.5.2}$$

Thus, irreducible A-lattices M can be identified with integer-valued vector $(\alpha_1, \ldots, \alpha_n)$ satisfying (14.5.2). We shall write $[M] = (\alpha_1, \ldots, \alpha_n)$ or $M = (\alpha_1, \ldots, \alpha_n)$.

The order relation on the set of such vectors and the operations on them corresponding to sum and intersection of irreducible lattices are obvious.

Remark. Obviously, two irreducible A-lattices $M_1 = (\alpha_1, \ldots, \alpha_n)$ and $M_2 = (\beta_1, \ldots, \beta_n)$ are isomorphic if and only if $\alpha_i = \beta_i + z$ for $i = 1, \ldots, n$ and (a fixed) $z \in \mathbf{Z}$. We shall denote by $(\alpha_1, ..., \alpha_n)^T$ the column vector with coordinates $\alpha_1, ..., \alpha_n$.

Note that the posets $S_r(A)$ and $S_l(A)$ do not depend on the choice of simple $M_n(\mathcal{D})$-modules U and V.

Proposition 14.5.3. *The posets $S_r(A)$ and $S_l(A)$ are anti-isomorphic distributive lattices.*

Proof. Since A is a semidistributive ring, $S_r(A)$ (resp. $S_l(A)$) is a distributive lattice with respect to sum and intersection of submodules.

Let $M = (\alpha_1, \ldots, \alpha_n) \in S_r(A)$. We put $M^* = (-\alpha_1, \ldots, -\alpha_n)^T \in S_l(A)$. If $N = (\beta_1, \ldots, \beta_n)^T \in S_l(A)$, then $N^* = (-\beta_1, \ldots, -\beta_n) \in S_r(A)$.

Obviously, the operation $*$ satisfies the following conditions:

1. $M^{**} = M$; 2. $(M_1 + M_2)^* = M_1^* \cap M_2^*$; 3. $(M_1 \cap M_2)^* = M_1^* + M_2^*$ in the right case and there are analogous rules in the left case. Thus, the map $*$: $S_r(A) \longrightarrow S_l(A)$ is the anti-isomorphism.

Remark. The map $*$ defines a duality for irreducible A-lattices.

If $M_1 \subset M_2$, $(M_1, M_2 \in S_r(A))$, then $M_2^* \subset M_1^*$. In this case, the A-lattice M_2 is called an **overmodule** of the A-lattice M_1 (resp. M_1^* is an **overmodule** of M_2^*).

14.6 QUIVERS OF TILED ORDERS

Recall that a quiver is called **strongly connected** if there is a path between any two vertices. By convention, a one-point graph without arrows will be considered a strongly connected quiver. A quiver Q without multiple arrows and multiple loops is called **simply laced**, i.e., Q is a simply laced quiver if and only if its adjacency matrix $[Q]$ is a $(0,1)$-matrix.

Theorem 14.6.1. *The quiver $Q(A)$ of a right and left Noetherian indecomposable semiprime semiperfect ring A is strongly connected.*

A proof follows from theorem 11.6.3 and proposition 9.2.13. We use notations from theorem 11.6.3. If $Q(A)$ isn't strongly connected, then the ring $(g_1+g_2)A(g_1+g_2)$ isn't semiprime. Indeed, for the nonzero ideal $J = \begin{pmatrix} 0 & g_1Ag_2 \\ 0 & 0 \end{pmatrix}$ we have $J^2 = 0$.

Let I be a two-sided ideal of a tiled order A. Obviously,

$$I = \sum_{i,j=1}^{n} e_{ij}\pi^{\mu_{ij}}\mathcal{O},$$

where the e_{ij} are matrix units. Denote by $\mathcal{E}(I) = (\mu_{ij})$ the exponent matrix of the ideal I. Suppose that I and J are two-sided ideals of the ring A, $\mathcal{E}(I) = (\mu_{ij})$, and $\mathcal{E}(J) = (\nu_{ij})$. It follows easily that $\mathcal{E}(IJ) = (\delta_{ij})$, where $\delta_{ij} = \min\limits_{k}\{\mu_{ik}+\nu_{kj}\}$.

Theorem 14.6.2. *The quiver $Q(A)$ of a tiled order A over a discrete valuation ring $\mathcal{O}$ is strongly connected and simply laced. If A is reduced, then $Q(A) = \mathcal{E}(R^2) - \mathcal{E}(R)$.*

Proof. Taking into account that A is a prime Noetherian semiperfect ring, it follows from theorem 14.6.1, that $Q(A)$ is a strongly connected quiver. Let A be a reduced order. Then $[Q(A)]$ is a reduced matrix. We shall use the following notation: $\mathcal{E}(A) = (\alpha_{ij})$; $\mathcal{E}(R) = (\beta_{ij})$, where $\beta_{ii} = 1$ for $i = 1,\dots,n$ and $\beta_{ij} = \alpha_{ij}$ for $i \neq j$ $(i,j = 1,\dots,n)$; $\mathcal{E}(R^2) = (\gamma_{ij})$, where $\gamma_{ij} = \min\limits_{1\le k\le n}\{\beta_{ik} + \beta_{kj}\}$ for $i,j = 1,\dots,n$. Since, $\mathcal{E}(A)$ is reduced, we have $\alpha_{ij} + \alpha_{ji} \ge 1$ for $i,j = 1,\dots,n$, i.e., $\gamma_{ii} = \min\limits_{1\le k\le n}\{\beta_{ik} + \beta_{ki}\} = \min\limits_{1\le k\le n,\, k\neq i}\{\beta_{ik} + \beta_{ki}\}$. Hence γ_{ii} is equal to 1 or 2. If $i \neq j$, then $\beta_{ij} = \alpha_{ij}$ and $\gamma_{ij} = \min\{\min\limits_{1\le k\le n,\, k\neq i,j}\{\alpha_{ik} + \alpha_{kj}\},\, \alpha_{ij}+1\}$, i.e., γ_{ij} equals α_{ij} or $\alpha_{ij} + 1$.

To any irreducible A-lattice M with $\mathcal{O}$-basis $(\pi^{\alpha_1}e_1,\dots,\pi^{\alpha_n}e_n)$ associate the n-tuple $[M] = (\alpha_1,\dots,\alpha_n)$. Let us consider

$$[P_i] = (\alpha_{i1},\dots,0,\dots,\alpha_{in}),$$

$$[P_iR] = (\alpha_{i1}, \ldots, 1, \ldots, \alpha_{in}) = (\beta_{i1}, \ldots, \beta_{in}).$$

Set $[P_iR^2] = (\gamma_{i1}, \ldots, \gamma_{in})$. Then $\vec{q_i} = [P_iR^2] - [P_iR]$ is a $(0,1)$-vector. Suppose that the positions of the units of $\vec{q_j}$ are $j_1, \ldots, j_m$. In view of the annihilation lemma, this means that $P_iR/P_iR^2 = U_{j_1} \oplus \ldots \oplus U_{j_m}$. By the definition of $Q(A)$ we have exactly one arrow from the vertex i to each of $j_1, \ldots, j_m$. Thus, the adjacency matrix $[Q(A)]$ is:

$$[Q(A)] = \mathcal{E}(R^2) - \mathcal{E}(R).$$

The theorem is proved.

Definition. A tiled order $A = \{\mathcal{O}, \mathcal{E}(A)\}$ is called a $(0,1)$**-order** if $\mathcal{E}(A)$ is a $(0,1)$-matrix.

Henceforth a $(0,1)$-order will always mean a tiled $(0,1)$-order over a discrete valuation ring $\mathcal{O}$.

With a reduced $(0,1)$-order A we associate the partially ordered set

$$P_A = \{1, \ldots, n\}$$

with the relation $\leq$ defined by $i \leq j \Leftrightarrow \alpha_{ij} = 0$.

Obviously, $(P, \leq)$ is a partially ordered set (poset).

Conversely, to any finite poset $P = \{1, \ldots, n\}$ assign a reduced $(0,1)$-matrix $\mathcal{E}_p = (A_{ij})$ in the following way: $A_{ij} = 0 \Leftrightarrow i \leq j$, otherwise $A_{ij} = 1$. Then $A(P) = \{\mathcal{O}, \mathcal{E}_P\}$ is a reduced $(0,1)$-order.

We give a construction which for a given finite partially ordered set $P = \{p_1, \ldots, p_n\}$ yields a strongly connected quiver without multiple arrows and multiple loops.

Denote by P_{max} (respectively P_{min}) the set of the maximal (respectively minimal) elements of P and by $P_{max} \times P_{min}$ their Cartesian product.

Definition. The quiver $\tilde{Q}(P)$ obtained from the diagram $Q(P)$ by adding the arrows $\sigma_{ij} : i \to j$ for all $(p_i, p_j) \in P_{max} \times P_{min}$ is called the **quiver associated with the partially ordered set** P.

Obviously, $\tilde{Q}(P)$ is a strongly connected simply laced quiver.

Theorem 14.6.3. *The quiver $Q(A(P))$ coincides with the quiver $\tilde{Q}(P)$.*

Proof. Recall that $[Q(A(P))] = \mathcal{E}(R^2) - \mathcal{E}(R)$. Suppose that in $Q(P)$ there is an arrow from s to t. This means that $\alpha_{st} = 0$ and there is no positive integer k $(k \neq s, t)$ such that $\alpha_{sk} = 0$ and $\alpha_{kt} = 0$. The elements β_{ss} and β_{tt} of the exponent matrix $\mathcal{E}(R) = (\beta_{ij})$ are equal to 1. We have that $\mathcal{E}(R^2) = (\gamma_{ij})$, where $\gamma_{ij} = \min\limits_{1 \leq k \leq n} (\beta_{sk} + \beta_{kt}) = 1$. Thus, in $[Q(A(P))]$ at the (s,t)-th position we have $\gamma_{st} - \beta_{st} = 1 - \alpha_{st} = 1 - 0 = 1$. Consequently, $Q(A(P))$ has an arrow from s to t.

Suppose that $p \in P_{max}$. This means that $\alpha_{pk} = 1$ for $k \neq p$. Therefore the entries of the p-th row of $\mathcal{E}(R)$ are all 1, i.e., $(\beta_{p1}, \ldots, \beta_{pp}, \ldots, \beta_{pn}) = (1, \ldots, 1, \ldots, 1)$.

Similarly, if $q \in P_{min}$, then the q-th column $(\beta_{1q}, \ldots, \beta_{qq}, \ldots, \beta_{nq})^T$ of $\mathcal{E}(R)$ is $(1, \ldots, 1, \ldots, 1)^T$. Hence, $\gamma_{pq} = 2$, $\beta_{pq} = 1$, and $Q(A(P))$ has an arrow from p to q. Consequently, we proved that $\tilde{Q}(P)$ is a subquiver of $Q(A(P))$.

We show now the converse inclusion. Suppose that $\gamma_{pq} = 2$. Then obviously

$$(\beta_{p1}, \ldots, \beta_{pp}, \ldots, \beta_{pq}) = (1, \ldots, 1, \ldots, 1)$$

and

$$(\beta_{1q}, \ldots, \beta_{qq}, \ldots, \beta_{nq})^T = (1, \ldots, 1, \ldots, 1)^T.$$

Therefore $p \in P_{max}$, $q \in P_{min}$ and there is an arrow, which goes from p to q.

Suppose $\gamma_{pq} = 1$ and $\beta_{pq} = 0$. Consequently, $p \neq q$, $\beta_{pq} = \alpha_{pq} = 0$ and $p < q$. Since $\gamma_{pq} = \min\limits_{1 \leq k \leq n} (\beta_{pk} + \beta_{kp})$, then $\beta_{pk} + \beta_{kq} \geq 1$ for $k = 1, \ldots, n$. Thus, for $k \neq p, q$ we have $\beta_{pk} + \beta_{kq} \geq 1$, whence we obtain $\alpha_{pk} + \alpha_{kp} \geq 1$. Therefore, there is no positive integer $k\,(k \neq p, q)$ such that $\alpha_{pk} = \alpha_{kq} = 0$. This means that there is an arrow from p to q in $\tilde{Q}(P)$, and this proves the opposite inclusion.

14.7 QUIVERS OF EXPONENT MATRICES

Let $\mathcal{E} = (\alpha_{ij})$ be a reduced exponent matrix. Set $\mathcal{E}^{(1)} = (\beta_{ij})$, where $\beta_{ij} = \alpha_{ij}$ for $i \neq j$ and $\beta_{ii} = 1$ for $i = 1, \ldots, n$, and $\mathcal{E}^{(2)} = (\gamma_{ij})$, where $\gamma_{ij} = \min\limits_{1 \leq k \leq n} (\beta_{ik} + \beta_{kj})$. Obviously, $[Q] = \mathcal{E}^{(2)} - \mathcal{E}^{(1)}$ is a $(0,1)$-matrix. From theorem 14.3.1 and theorem 14.6.1 we obtain the following statement.

Theorem 14.7.1 *The matrix $[Q] = \mathcal{E}^{(2)} - \mathcal{E}^{(1)}$ is the adjacency matrix of the strongly connected simply laced quiver $Q = Q(\mathcal{E})$.*

Definition. The quiver $Q(\mathcal{E})$ is called the **quiver of a reduced exponent matrix** $\mathcal{E}$.

Definition. A strongly connected simply laced quiver is called **admissible** if it is a quiver of a reduced exponent matrix.

Definition. A reduced exponent matrix $\mathcal{E} = (\alpha_{ij}) \in M_n(\mathbf{Z})$ is called **Gorenstein** if there exists a permutation σ of $\{1, 2, \ldots, n\}$ such that $\alpha_{ik} + \alpha_{k\sigma(i)} = \alpha_{i\sigma(i)}$ for $i, k = 1, \ldots, n$.

The permutation σ is denoted by $\sigma(\mathcal{E})$. Notice that $\sigma(\mathcal{E})$ for a reduced Gorenstein exponent matrix $\mathcal{E}$ has no cycles of length 1.

Recall that a **quasigroup** is a nonempty set Q with a binary algebraic operation (called multiplication) such that the equations $ax = b$ and $ya = b$ have a unique solution x, respectively y, in Q. Obviously, any group is a quasigroup.

Definition. A **Latin square of order** n is a square matrix with rows and columns each of which is a permutation of a set $S = \{s_1, \ldots, s_n\}$. Every Latin square is a Cayley table of a **finite quasigroup**. In particular, the Cayley table of a finite group is a Latin square. As the set S we shall usually take $S = \{0, 1, \ldots, n-1\}$.

Definition. A real non-negative $n \times n$-matrix $P = (p_{ij})$ is **doubly stochastic** if $\sum\limits_{j=1}^{n} p_{ij} = 1$ and $\sum\limits_{i=1}^{n} p_{ij} = 1$ for all $i, j = 1, \ldots, n$.

Example 14.7.1.

The Cayley table of the Klein four-group $(2)\times(2)$ can be written in the following form:

$$K = K(4) = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix}.$$

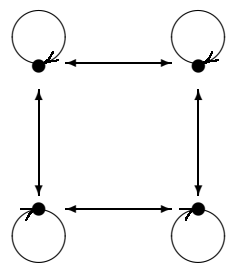
Then $K(4)$ is a reduced Gorenstein exponent matrix with permutation $\sigma = \sigma(K(4)) = (14)(23)$. Obviously,

$$K^{(2)} = \begin{bmatrix} 2 & 2 & 3 & 3 \\ 2 & 2 & 3 & 3 \\ 3 & 3 & 2 & 2 \\ 3 & 3 & 2 & 2 \end{bmatrix}$$

and

$$[Q(K)] = K^{(2)} - K^{(1)} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} = 3 \cdot P_1,$$

where P_1 is a doubly stochastic matrix, and $Q(K)$ is



Definition. A quasigroup Q is called **entropic** if it satisfies the identity $(xu)(vy) = (xv)(uy)$ for all $x, y, u, v \in Q$. (see *Plugfelder, H.O., Quasigroups and loops: Introduction, Berlin: Heldermann, 1990, p. 140*).

Example 14.7.2.
Let $Q(5) = \{0, 1, 2, 3, 4, \}$ be the quasigroup with the following Cayley table

0	0	1	2	3	4
0	0	4	3	2	1
1	1	0	4	3	2
2	2	1	0	4	3
3	3	2	1	0	4
4	4	3	2	1	0

It is clear that $Q(5)$ is an entropic quasigroup. The Cayley table

$$\mathcal{E}(5) = \begin{bmatrix} 0 & 4 & 3 & 2 & 1 \\ 1 & 0 & 4 & 3 & 2 \\ 2 & 1 & 0 & 4 & 3 \\ 3 & 2 & 1 & 0 & 4 \\ 4 & 3 & 2 & 1 & 0 \end{bmatrix}$$

of $Q(5)$ is a reduced Gorenstein exponent matrix with $\sigma(\mathcal{E}(5)) = (12345)$.

Obviously,

$$[Q(\mathcal{E}(5))] = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} = 2P_2,$$

where P_2 is a doubly stochastic matrix.

For the Cayley table

$$\mathcal{E}(n) = \begin{bmatrix} 0 & n-1 & n-2 & \dots & 2 & 1 \\ 1 & 0 & n-1 & \dots & 3 & 2 \\ 2 & 1 & 0 & \dots & 4 & 3 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ n-2 & n-3 & n-4 & \dots & 0 & n-1 \\ n-1 & n-2 & n-3 & \dots & 1 & 0 \end{bmatrix}$$

of the entropic quasigroup $Q(n)$, we have $[Q(\mathcal{E}(n))] = E_n + J_n^-(0) + e_{1n}$, where $J_n^-(0) = e_{21} + \ldots + e_{nn-1}$ is the lower nilpotent Jordan block.

Definition. A finite quasigroup Q defined on the set $S = \{0, 1, \ldots, n-1\}$ is called **Gorenstein** if its Cayley table $C(Q) = (\alpha_{ij})$ has a zero main diagonal and there exists a permutation $\sigma : i \to \sigma(i)$ for $i = 1, \ldots, n$ such that $\alpha_{ik} + \alpha_{k\sigma(i)} = \alpha_{i\sigma(i)}$ for $i = 1, \ldots, n$.

If σ is a cycle, then Q is called a **cyclic Gorenstein quasigroup**. Write $\sigma = \sigma(Q)$.

Proposition 14.7.2. *The quasigroup $Q(n)$ is Gorenstein with permutation $\sigma = (12\dots n)$, i.e., $Q(n)$ is a cyclic Gorenstein quasigroup.*

Proof. This is obvious.

Theorem 14.7.3. *For any permutation $\sigma \in S_n$ without fixed elements there exists a Gorenstein reduced exponent matrix $\mathcal{E}$ order A with permutation $\sigma(\mathcal{E}) = \sigma$.*

Proof. Because σ has no fixed elements, it has no cycles of length 1 and decomposes into a product of non-intersecting cycles $\sigma = \sigma_1 \cdots \sigma_k$, where σ_i has length m_i. Denote by t the least common multiple of the numbers $m_1-1, \dots, m_k-1$.

Consider the matrix

$$\mathcal{E}(m_1,\dots,m_s) = \begin{pmatrix} t_1\mathcal{E}(m_1) & tU_{m_1\times m_2} & tU_{m_1\times m_3} & \dots & tU_{m_1\times m_k} \\ 0 & t_2\mathcal{E}(m_2) & tU_{m_2\times m_3} & \dots & tU_{m_2\times m_k} \\ 0 & 0 & t_3\mathcal{E}(m_3) & \dots & tU_{m_3\times m_k} \\ \dots & \dots & \dots & \ddots & \dots \\ 0 & 0 & 0 & \dots & t_k\mathcal{E}(m_k) \end{pmatrix},$$

where $t_j = \frac{t}{m_j-1}$, $U_{m_i\times m_j}$ is an $m_i \times m_j$ - matrix whose entries equal 1; $\mathcal{E}(m) = (\varepsilon_{ij})$, $\varepsilon_{ij} = \begin{cases} i-j, & \text{if } i \geq j; \\ i-j+m, & \text{if } i < j. \end{cases}$

Let us remark that $\varepsilon_{ij} + \varepsilon_{j\sigma(i)} = \varepsilon_{i\sigma(i)} = m-1$ for all i, j.

Evidently, $\mathcal{E}(m_1,\dots,m_s)$ is a Gorenstein reduced exponent matrix with a permutation $\sigma(\mathcal{E}(m_1,\dots,m_s)) = (123\dots m_1)(m_1+1\dots m_1+m_2)\cdots(m_1+m_2+\cdots+m_{k-1}+1\dots m_1+m_2+\cdots+m_{k-1}+m_k)$.

Since the permutations σ and $\sigma(\mathcal{E}(m_1,\dots,m_s))$ have the same type, these permutations are conjugate, i. e., there exists a permutation τ such that $\sigma = \tau^{-1}\sigma(\mathcal{E}(m_1,\dots,m_s))\tau$.

Consequently, the matrix $P_\tau^T\mathcal{E}(m_1,\dots,m_s)P_\tau$ is the Gorenstein reduced exponent matrix with a permutation σ.

There exist the Gorenstein quasigroups, which are not exponent matrices.

Example 14.7.3. (B.V. Novikov).

The matrix

$$C(\mathcal{L}_{12}) = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 1 & 0 & 5 & 2 & 3 & 4 & 7 & 8 & 9 & 6 & 11 & 10 \\ 2 & 5 & 0 & 4 & 1 & 3 & 8 & 10 & 7 & 11 & 6 & 9 \\ 3 & 2 & 4 & 0 & 5 & 1 & 10 & 6 & 11 & 7 & 9 & 8 \\ 4 & 3 & 1 & 5 & 0 & 2 & 9 & 11 & 6 & 10 & 8 & 7 \\ 5 & 4 & 3 & 1 & 2 & 0 & 11 & 9 & 10 & 8 & 7 & 6 \\ 6 & 7 & 8 & 10 & 9 & 11 & 0 & 2 & 1 & 3 & 4 & 5 \\ 7 & 8 & 10 & 6 & 11 & 9 & 2 & 0 & 5 & 1 & 3 & 4 \\ 8 & 9 & 7 & 11 & 6 & 10 & 1 & 5 & 0 & 4 & 2 & 3 \\ 9 & 6 & 11 & 7 & 10 & 8 & 3 & 1 & 4 & 0 & 5 & 2 \\ 10 & 11 & 6 & 9 & 8 & 7 & 4 & 3 & 2 & 5 & 0 & 1 \\ 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \end{pmatrix}$$

is the Cayley table of a Gorenstein quasigroup $\mathcal{L}_{12}$ with permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 12 & 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

The ring inequalities do not hold, since:

$$\alpha_{17} + \alpha_{79} = 7 < \alpha_{19} = 8.$$

14.8 EXAMPLES

In the book *Tuganbaev A.A., Semidistributive Modules and Rings, Kluwer Academic Publishers, 1998* the following open questions for Noetherian semidistributive ring A were stated (Exercises 11.76):

(1) Is it necessary that A is a direct product of an Artinian ring and semiprime ring?

(2) When is every finitely generated A-module semidistributive?

(3) If A is semiprime, is it hereditary?

We shall give negative answers to questions (1) and (3).

Example 14.8.1 (Negative answer to question 1).

Let $\mathbf{Z}_p$ be a ring of p-integers (p is prime), and let $\mathbf{F}_p = \mathbf{Z}_p/p\mathbf{Z}_p$ be the field of p elements. Consider the $SPSD$-ring A of 2×2-matrices of the following form: $A = \begin{pmatrix} \mathbf{Z}_p & \mathbf{F}_p \\ \mathbf{F}_p & \mathbf{F}_p \end{pmatrix}$.

We describe the multiplication and the addition in A. Denote by e_{11}, e_{12}, e_{21}, e_{22} the matrix units of A: $e_{12}e_{21} = 0$ and $e_{21}e_{12} = 0$. Let $\varphi : \mathbf{Z}_p \to \mathbf{F}_p$ be the canonical epimorphism. If $a \in \mathbf{Z}_p$, then $ae_{11}e_{12} = \varphi(a)e_{12} = e_{12}\varphi(a)$ and $e_{21}ae_{11} = e_{21}\varphi(a) = \varphi(a)e_{21}$. Further, $ae_{11} = e_{11}a$ for $a \in \mathbf{Z}_p$ and $\alpha e_{22} = e_{22}\alpha$ for $\alpha \in \mathbf{F}_p$. The addition is defined elementwise, the multiplication is defined as

multiplication of 2×2-matrices. Obviously, A is an indecomposable Noetherian $SPSD$-ring.

It is easy to see that $R(A) = \begin{pmatrix} p\mathbf{Z}_p & \mathbf{F}_p \\ \mathbf{F}_p & 0 \end{pmatrix}$ and $R(A)^2 = \begin{pmatrix} p^2\mathbf{Z}_p & 0 \\ 0 & 0 \end{pmatrix}$. So, $R(A)/R(A)^2 = \begin{pmatrix} p\mathbf{Z}_p/p^2\mathbf{Z}_p & \mathbf{F}_p \\ \mathbf{F}_p & 0 \end{pmatrix}$ and by the Q-Lemma the quiver $Q(A)$ is the two-pointed quiver with the adjacency matrix $[Q(A)] = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.

This example shows, that there is no analogue to the decomposition theorem for serial Noetherian rings (see theorem 12.3.8) even for Noetherian $SPSD$-rings with two-pointed quiver.

Example 14.8.2 (Negative answer to question 3).

Consider the following ring of 2×2-matrices $A = \begin{pmatrix} \mathbf{Z}_p & p\mathbf{Z}_p \\ p\mathbf{Z}_p & \mathbf{Z}_p \end{pmatrix}$. The Jacobson radical R of A is: $R = \begin{pmatrix} p\mathbf{Z}_p & p\mathbf{Z}_p \\ p\mathbf{Z}_p & \mathbf{Z}_p \end{pmatrix}$. Consider the following right ideal J of A: $J = \begin{pmatrix} p\mathbf{Z}_p & p\mathbf{Z}_p \\ 0 & 0 \end{pmatrix}$. Obviously, $JR = \begin{pmatrix} p^2\mathbf{Z}_p & p^2\mathbf{Z}_p \\ 0 & 0 \end{pmatrix}$. It is clear, that J is indecomposable as a right module and is not projective. It follows that J contains exactly two maximal submodules: $J_1 = \begin{pmatrix} (p^2\mathbf{Z}_p & p\mathbf{Z}_p \\ 0 & 0 \end{pmatrix}$ and $J_2 = \begin{pmatrix} p\mathbf{Z}_p & p^2\mathbf{Z}_p \\ 0 & 0 \end{pmatrix}$, $J_1 \cap J_2 = JR$. Consequently, A is a prime non-hereditary $SPSD$-ring.

14.9 NOTES AND REFERENCES

It is well known that many important classes of rings are naturally characterized by the properties of modules over them. As examples, we mention semisimple Artinian rings, uniserial rings, semiprime hereditary semiperfect rings and semidistributive rings.

There is the following chain of strict inclusions:

semisimple Artinian rings $\subset$ *generalized uniserial rings* $\subset$ $\subset$ *serial rings* $\subset$ *semidistributive rings.*

In this chain the first three classes of rings are semiperfect. The example of the ring of integers $\mathbf{Z}$ shows, that a distributive ring is non-necessarily semiperfect.

The first papers on the theory of semidistributive rings were appeared in the middle of XX century (see *R.L.Blair, Ideal lattice and the structure of rings // Trans. Amer. Math. Soc., 75, N 1, (1953), pp. 136-153; E.A.Behrens, Distributive Darstellbare Ringe I // Math. Z., 73, N 5, (1960), pp. 409-432; W.Menzel, Über der Untergruppenverband einer Abelschen Operatorgruppe. Teil II. Distributive und M.-Verbande von Untergruppen einer Abelschen Opertorgruppe // Math.*

Z., 74, N 1, (1960), pp. 52-65; W.Menzel, Ein Kriterium für Distributivität des Untergruppenverbands einer Abelschen Opertorgruppe // Math. Z., 75, N 3, (1961), pp. 271-276; E.A.Behrens, Distributive Darstellbare Ringe II // Math. Z., 76, N 4, (1961), pp. 367-384).

The paper *W.Stephenson, Modules whose lattice of submodules is distributive // Proc. London Math. Soc., 28, N 2, (1974), pp. 291-310* was the important step in the development of this theory.

Papers of H.H.Brungs, V.Camillo, A.Facchini, R.B.Feinberg, M.Ferrero, K.R.Fuller, J.Gräter, I.Kaplansky, R.Mazurek, A.V.Mikhalev, B.Müller, B.Osofsky, E.Puchylowski, G.Puninskii, G.Törner, A.Tuganbaev, P.Vámos, R.B.Warfield, R.Wisbauer, M.H. Wright were devoted to studying different classes of semidistributive rings.

We note a few monographs, which can help the reader become acquainted better with this area: *P.Cohn, Free Rings and Their Relations, Academic Press, London, 1971; A.A.Tuganbaev, Semidistributive modules and rings, Kluwer Acad. Publ., Dordrecht, 1998; A.A.Tuganbaev, Distributive modules and Related Topics, Gordon and Breach Science Publishers, 1999.*

Theorem 14.1.4 was proved in W.Stephenson's paper (see above). Theorem 14.1.5 first appeared in the paper *V.Camillo, Distributive modules // J. Algebra 36 (1975), pp. 6-26.*

The reduction theorem for $SPSD$-rings and decomposition theorem for semiprime right Noetherian $SPSD$-rings were proved in the paper *V.V.Kirichenko and M.A.Khibina, Semi-perfect semi-distributive rings, In: Infinite Groups and Related Algebraic Topics, Institute of Mathematics NAS Ukraine, 1993, pp. 457-480 (in Russian).*

Quivers and prime quivers of $SPSD$-rings were studied in *V.V.Kirichenko, Semi-perfect semi-distributive rings // Algebras and Representation theory, v. 3, 2000, pp. 81-98.*

Moreover, in this paper, for semihereditary $SPSD$-ring A the existence of a classical ring of fractions $\tilde{A}$ was proved, so that the prime quiver $PQ(A)$ coincides with a quiver $Q(\tilde{A})$. This is false for Noetherian semiperfect piecewise domains, as is shown by the following example

$$A = \begin{pmatrix} \mathcal{O} & \mathcal{O} & \mathcal{O} \\ 0 & \mathcal{O} & \pi\mathcal{O} \\ 0 & 0 & \mathcal{O} \end{pmatrix},$$

where $\mathcal{O}$ is a discrete valuation ring with unique maximal ideal $\mathcal{M} = \pi\mathcal{O} = \mathcal{O}\pi$.

Theorem 14.5.2 was first proved in *A.G.Zavadskij and V.V.Kirichenko, Torsion-free Modules over Prime Rings // Zap. Nauch. Seminar. Leningrad. Otdel. Mat. Steklov. Inst. (LOMI) - 1976. - v. 57. - p. 100-116 (in Russian). English translation in J. of Soviet Math., v. 11, N 4, April 1979, p. 598-612.*

In sections 14.6 and 14.7 we have followed papers *Zh.T.Chernousova, M.A.Dokuchaev, V.V.Kirichenko, M.A.Khibina, S.G.Miroshnichenko,*

V.N.Zhuravlev, Tiled orders over discrete valuation rings, finite Markov chains and partially ordered sets, I // Algebra and Discrete mathematics, N 1, 2002, pp. 32-63 and *Zh.T.Chernousova, M.A.Dokuchaev, V.V.Kirichenko, M.A.Khibina, S.G.Miroshnichenko, V.N.Zhuravlev, Tiled orders over discrete valuation rings, finite Markov chains and partially ordered sets, II // Algebra and Discrete mathematics, N 2, 2003, pp. 47-86.*

For studying the theory of quasigroups we recommend the monographs *H.O.Plugfelder, Quasigroups and loops: Introduction, Berlin: Heldermann, 1990* and *V.D.Belousov, Foundations of quasigroup and loop theory, Moscow, Nauka, 1967 (in Russian).* And for studying Latin squares we recommend a fundamental monograph on this topic *A.D.Keedwell, J.Denes, Latin squares and their applications, New York, Academic Press, 1974.*

Examples 14.8.1 and 14.8.2 are considered in the paper *V.V.Kirichenko, Yu.V.Yaremenko, On semiperfect semidistributive rings // Math. Notes, v. 69, N 1, 2001, pp. 153-156 (in Russian).*

SUGGESTIONS FOR FURTHER READING

1. F.W.Anderson and K.R.Fuller, Rings and Categories of Modules. Second edition, Graduate Texts in Mathematics, Vol. 13, Springer-Verlag, Berlin-Heidelberg-New York, 1992.

2. V.A.Andrunakievich, Yu.M.Ryabukhin, Radicals of Algebras and Structure theory. Nauka, Moscow, 1979.

3. V.I.Arnautov, S.T.Glavatsky, A.V.Mikhalev, Introduction to the theory of topological rings and modules. Monographs and Textbooks in Pure and Applied Mathematics, 197. Marcel Dekker, Inc., New York, 1996.

4. B.N.Arnold, Logic and Boolean Algebra. Prentice-Hall, INC, Englewood Cliffs, New York, 1962.

5. M.F.Atiyah and I.G.Macdonald, Introduction to Commutative Algebra. Addison-Wesley, 1969.

6. M.Auslander, I.Reiten, S.Smalø, Representation Theory of Artin Algebras. Cambridge University Press, 1995.

7. K.I.Beidar, W.S.Martindale, A.V.Mikhalev, Rings with generalized identities. Monographs and Textbooks in Pure and Applied Mathematics, 196. Marcel Dekker, Inc., New York, 1996.

8. Z.I.Borevich, I.R.Shafarevich, Number theory. Acad. Press, 1966.

9. N.Bourbaki, Elements of mathematics. Commutative algebra. Addison-Wesley, 1974.

10. H.Cartan and S.Eilenberg, Homological Algebra. Princeton University Press, Princeton, New York, 1956.

11. P.M.Cohn, Free Rings and Their Relations. Academic Press, London-New York, 1985.

12. C.W.Curtis, I.Reiner, Methods of Representation Theory I,II. John Wiley and Sons, New York, 1990.

13. A.Facchini, Module Theory, Birkhäuser Verlag, Basel, 1998.

14. D.K.Faddeev (ed.), Investigations on Representation Theory. Zap. Nauchn. Sem. LOMI, 1972, v.28.

15. C.Faith, Algebra: Rings, Modules and Categories. I. Springer-Verlag, Berlin-Heidelberg- New York, 1973.

16. C.Faith, Algebra II. Ring Theory. Springer-Verlag, Berlin-Heidelberg- New York, 1976.

17. C.Faith, Algebra: Rings, Modules and Categories I. Moscow, 1977 (in Russian).

18. C.Faith, Algebra: Ring, Modules and Categories II. Moscow, 1979 (in Russian).

19. J.Dauns, Modules and Rings, Cambridge University Press, 1994.

20. N.J.Divinsky, Rings and Radicals. Univ. of Toronto Press, Toronto, 1965.

21. V.Dlab, C.Ringel, Indecomposable representations of graphs and algebras. Memoirs Amer. Math. Soc., v.173, 1976.

22. Yu.A.Drozd, V.V.Kirichenko, Finite Dimensional Algebras (with an Appendix by V.Dlab). Springer-Verlag, Berlin-Heidelberg-New York, 1994.

23. P.Gabriel, A.V.Roiter, Representations of Finite Dimensional Algebras. Springer-Verlag, Berlin-Heidelberg-New York, 1997.

24. B.J.Gardner, Rings and Radicals. CRC Press. Inc., 1996.

25. K.R.Goodearl, R.B.Warfield, Jr, An introduction to Noncommutative Noetherian Rings. London Mathematical Society Student Texts, Vol. 16, Cambridge University Press, 1989.

26. H.Hasse, Vorlesungen über Zahlentheorie. Berlin, 1950.

27. I.N.Herstein, Noncommutative Rings. Carus Mathematical Monographs, No.15, Mathematical Association of America, 1968.

28. N.Jacobson, The Theory of Rings. American Mathematical Society Surveys, Vol. 2, American Mathematical Society, Providence, 1943.

29. N.Jacobson, Structure of Rings. American Mathematical Society Colloquium Publications, Vol. 37, American Mathematical Society, Providence, 1956.

30. N.Jacobson, Lectures in Abstract Algebra, I, II, III. Graduate Texts in Mathematics, Vol. 30, 31, 32, Springer-Verlag, Berlin-Heidelberg-New York, 1975.

31. C.U.Jensen, H.Lenzing, Model Theoretic algebra with Particular Emphasis on Fields, Rings, Modules. v.2, 1989.

32. I.Kaplansky, Commutative Rings. Univ. Chicago Press, Chicago, 1974.

33. I.Kaplansky, Fields and Rings. Univ. Chicago Press, Chicago, 1972.

34. F.Kasch, Modules and Rings. Academic Press, New York, 1982.

35. A.I.Kashu, Functors and torsion in categories of modules. Akademia Nauk Respubliki Moldova, Inst. Math., 1997.

36. I.Kleiner, A sketch of the evolution of (noncommutative) ring theory. Enseing. Math. (2) 33 (1987), No 3-4, p.227-267.

37. T.Y.Lam, A First Course in Noncommutative Rings. Graduate Texts in Mathematics, Vol. 131, Springer-Verlag, Berlin-Heidelberg-New York, 1991.

38. T.Y.Lam, Lectures on Modules and Rings. Graduate Texts in Mathematics, Vol. 189, Springer-Verlag, Berlin-Heidelberg-New York, 1999.

39. J.Lambek, Lectures on Rings and Modules. Blaisdell-Ginn, Waltham-Toronto-London, 1966.

40. S.Lang, Algebra. Addison-Wesley, 1974.

41. S.Lang, Algebraic Number Theory. Addison-Wesley Publishing Company, Reading, Mass., Palo Alto, London, 1964.

42. S.MacLane, Homology. Springer-Verlag, Berlin-Göttingen-Heidelberg, 1963.

43. S.MacLane, Categories for working mathematicians, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1971.

44. J.C.McConnell and J.C.Robson, Noncommutative Noetherian Rings. Wiley-Interscience, New York, 1987.

45. N.H.McCoy, The Theory of Rings. The Macmillian Company, New York, 1965.

46. B.Mitchell, Theory of categories, Academic Press, 1965.

47. D.G.Northcott, A first course of homological algebra, Cambridge University Press, 1973.

48. J.Okninski, Semigroup Algebras. Marcel Dekker, INC, 1991.

49. M.S.Osborne, Basic homological algebra, Springer-Verlag, New York, 2000.

50. B.L.Osofsky, Homological Dimensions of Modules, 1973.

51. D.S.Passman, The Algebraic Structure of Group Rings. John Wiley and Sons, New York-London-Sydney-Toronto, 1977.

52. D.S.Passman, A Course in Ring Theory. Wadsworth and Brooks, Cole Mathematics Series, California, 1991.

53. R.S.Pierce, Associative Algebras. Graduate Texts in Mathematics, Vol. 88, Springer-Verlag, Berlin-Heidelberg-New York, 1982.

54. C.Polcino Milies, S.K.Sehgal, An introduction to group rings. Algebra and Applications, Kluwer Academic Publishers, Dordrecht, 2002.

55. G.Puninski, Serial rings, Kluwer Academic Publishers, Dordrecht, 2001.

56. K.W.Roggenkamp, V. Huber-Dyson, Lattices over Orders, I. Lecture Notes in Math., v. 115, Springer-Verlag, Berlin-Heidelberg-New York, 1970.

57. K.W.Roggenkamp, M.Taylor, Group Rings and Class Groups, Birkhäuser Verlag, Basel, 1992.

58. J.Rotman, An Introduction to Homological Algebra, Academic Press, New York, 1979.

59. L.H.Rowen, Ring Theory, I,II. Academic Press, New York-Boston, 1988.

60. S.K.Sehgal, Topics in Group Rings. M. Dekker, 1978.

61. D.Simson, Linear Representation of Partially Ordered Sets and Vector Space Categories, Algebra, Logic and Appl. v.4, Gordon and Breach Science Publishers, 1992.

62. B.Stenström, Rings of quotients: An introduction to methods of ring theory. Springer-Verlag, 1975.

63. A.A.Tuganbaev, Semidistributive Modules and Rings. Kluwer Academic Publishers, Dordrecht-Boston-London, 1998.

64. B.L.Van der Waerden, Algebra I, II. Springer-Verlag, Berlin-Heidelberg-New York, 1967 - 1971.

65. A.Weil, Basic Number Theory. Springer-Verlag, New York-Heidelberg-Berlin, 1967.

66. E.Weiss, Algebraic Number Theory. International Series in Pure and Applied Mathematics, McGraw-Hill Book Company, New York-San Francisco-Toronto, 1963.

67. R.Wisbauer, Foundations of Module and Ring Theory. Gordon and Breach, Philadelphia, 1991.

68. O.Zariski and P.Samuel, Commutative Algebra, I, II. Graduate Texts in Mathematics, Vol. 28, 29, Springer-Verlag, Berlin-Heidelberg-New York, 1975.

Index

Name Index