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 $\sum x_i a y_i$, 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, $\mathcal{I} = \bigcup_{i \in \mathbf{N}} \mathcal{I}_i$ 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 $a \in \bigcup_{i \in \mathbf{N}} \mathcal{I}_i$, 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: