

**INTRODUCTORY  
LECTURES ON  
RINGS AND MODULES:  
SUPPLEMENT**

**John A. Beachy**

Northern Illinois University

1999

*PRELIMINARY VERSION*

This chapter is a supplement to the book

**Introductory Lectures on Rings and Modules,**  
by John A. Beachy.

ISBN 0-521-64340-6, Copyright 1999

Cambridge University Press  
Edinburgh Building  
Shaftesbury Road  
Cambridge CB2 2RU

Copyright 1999 by John A. Beachy

Permission is granted to copy this document in electronic form, or to print it for personal use, under these conditions:

- it must be reproduced in whole;
- it must not be modified in any way;
- it must not be used as part of another publication.

Formatted May 18, 1999, at which time the original was available at:

[http://www.math.niu.edu/~beachy/rings\\_modules/](http://www.math.niu.edu/~beachy/rings_modules/)

# Contents

<b>PREFACE</b>	<b>iv</b>
<b>5 COMMUTATIVE RINGS</b>	<b>239</b>
5.1 Primary decomposition	240
5.2 Noetherian rings	245
5.3 Dedekind domains	249
5.4 Integral extensions	254
<b>BIBLIOGRAPHY</b>	<b>261</b>
<b>INDEX</b>	<b>262</b>

# Preface

The text *Introductory Lectures on Rings and Modules* grew out of the first-year graduate course that I have taught at Northern Illinois University. In keeping with the noncommutative focus of the text, I included a chapter on group representations in place of the chapter on commutative rings that is in our course syllabus. Since a course at that level should lay some foundation for later work in commutative algebra, I felt that I should make my class notes available as a supplement to the text.

I believe that the material I have chosen to include in this chapter is rather standard. It is not as extensive as that in other texts, but I hope that it will serve as a starting point for students interested in algebra. Those interested in further exploration of the field will find David Eisenbud's book *Commutative Algebra with a View toward Algebraic Geometry* to be a fascinating point of entry.

One of the advantages of electronic publishing is the ability to make changes quickly, I would appreciate receiving corrections and suggestions from anyone who uses this material.

John A. Beachy  
DeKalb, Illinois  
May, 1999

---

## Chapter 5

---

# COMMUTATIVE RINGS

---

The history of commutative algebra begins in the nineteenth century with work in number theory, algebraic geometry, and invariant theory. We will discuss just a bit of that history, and refer the reader to Chapter 1 of [3] for a more detailed account.

Gauss showed that the ring  $\mathbf{Z}[i]$  is a unique factorization domain, and used this fact to prove results about ordinary integers. He also showed that  $\mathbf{Z}[\omega]$  is a unique factorization domain, where  $\omega$  is a root of the polynomial  $x^2 + x + 1$ , and used this fact to give a proof of Fermat's last theorem for the exponent 3 (see Chapter 9 of [2] for his proof, and for some historical notes). The search for a proof of Fermat's last theorem led to questions of unique factorization in the rings  $\mathbf{Z}[\xi]$ , where  $\xi$  is a root of unity. It was eventually realized that this method of proof could not be extended beyond a certain point, since it cannot be assumed that unique factorization holds. In fact, it fails in the ring  $\mathbf{Z}[e^{2\pi i/23}]$ .

In this chapter we return to the question of unique factorization in commutative rings. Unique factorization of elements into products of irreducible elements is impossible even in such relatively nice rings as  $\mathbf{Z}[\sqrt{-5}]$ . Dedekind introduced the notion of an ideal in order to recover some semblance of unique factorization. He proved that in certain important subrings of the complex

numbers, at least it is true that every ideal can be written uniquely as a product of prime ideals. We will study these rings in the last two sections of the chapter, under the general heading of Dedekind domains. (Note that the last two sections do not depend on the first two, and can be read independently.)

A parallel development along somewhat different lines occurred for ideals in polynomial rings in several indeterminates. Lasker and Macauley gave a decomposition theorem for such ideals, showing that every ideal is an intersection of finitely many primary ideals. This was extended to all commutative Noetherian rings in 1921 by Emmy Noether, in a very influential paper. The primary motivation for the development of this theory comes from algebraic geometry. We will prove the Lasker-Noether primary decomposition theorem in the first section of the chapter. A part of the general theory of Noetherian rings is outlined in the second section of the chapter.

Invariant theory grew out of an interest in the geometric properties of plane curves that remain invariant under certain classes of transformations. The general problem was eventually stated in the following way: if an appropriate group  $G$  acts as automorphisms of a polynomial ring  $R = F[x_1, \dots, x_n]$  (where  $F$  is a field), what is the subring  $R^G$  of elements left fixed by  $G$ ? For example, if  $G$  is the symmetric group  $S_n$ , then  $R^G$  is the ring of symmetric functions, which can be shown to be generated (as an  $F$ -algebra) by the elementary symmetric functions  $f_1 = x_1 + \dots + x_n$ ,  $f_2 = \sum_{1 \leq i < j \leq n} x_i x_j$ ,  $\dots$ ,  $f_n = \prod_{i=1}^n x_i$ .

Hilbert solved the fundamental problem of invariant theory, by showing that the ring of invariants is finitely generated in a broad range of interesting cases. We have already given a proof of the Hilbert basis theorem (see Theorem 2.4.10), which was the first step in his proof of the finiteness of invariants. It was Emmy Noether who recognized the general importance of the ascending chain condition, and so the basis theorem is usually stated in the following way: if  $R$  is a Noetherian ring, then so is the polynomial ring  $R[x]$ .

Although in this chapter we make the underlying assumption that all rings under consideration are commutative (with identity element), we will often restate this in the hypotheses of the major results.

## 5.1 Primary decomposition

Let  $F$  be a field, and first consider the ring  $F[x]$  of polynomials in one indeterminate. Since this ring is a principal ideal domain, each ideal is a product of prime ideals. Unfortunately, although the ring  $F[x, y]$  of polynomials in two indeterminates is a unique factorization domain, the ideal structure is not so simple. For an example that illustrates this particular difficulty, consider the ideal  $(x^2, y)$  generated by the elements  $x^2$  and  $y$ . In  $F[x, y]/(y) \cong F[x]$ , the only prime ideal that contains  $(x^2, y)/(y)$  is  $(x, y)/(y)$ . It follows that in  $F[x, y]$

the only prime ideal that contains  $(x^2, y)$  is  $(x, y)$ . Since  $(x, y)^2 = (x^2, xy, y^2)$ , which is properly contained in  $(x^2, y)$ , it is impossible to express  $(x^2, y)$  as a product of prime ideals.

To obtain an appropriate generalization of unique factorization of ideals in polynomial rings, it is necessary to replace products of ideals with intersections of ideals, and to replace powers of prime ideals with ‘primary’ ideals. The primary decomposition theorem does not depend on having unique factorization of elements, but simply on having the ascending chain condition on ideals, so it remains true for all Noetherian rings.

**Proposition 5.1.1** *Let  $R$  be a commutative ring. The set of all nilpotent elements of  $R$  forms an ideal of  $R$ .*

*Proof.* If  $a, b \in R$  with  $a^m = 0$  and  $b^n = 0$ , then

$$(a+b)^{m+n-1} = a^{m+n-1} + \dots + \binom{m+n-1}{m} a^m b^{n-1} + \binom{m+n-1}{m-1} a^{m-1} b^n + \dots + b^{m+n-1},$$

and each term in this expansion of  $(a+b)^{m+n-1}$  is zero because it contains either the factor  $a^m$  or the factor  $b^n$ . For any  $r \in R$ , we have  $(ra)^n = r^n a^n = 0$ , completing the proof that the set of nilpotent elements is an ideal of  $R$ .  $\square$

**Definition 5.1.2** *Let  $R$  be a commutative ring. The nil radical of  $R$  is defined to be the ideal*

$$N(R) = \{x \in R \mid x^n = 0 \text{ for some } n \in \mathbf{Z}^+\}.$$

**Theorem 5.1.3** *Let  $R$  be a commutative ring.*

- (a) *The nil radical of  $R/N(R)$  is zero.*
- (b) *The nil radical of  $R$  is the intersection of all prime ideals of  $R$ .*

*Proof.* (a) If  $a \in R$  and  $a + N(R)$  is nilpotent in  $R/N(R)$ , then  $a^n \in N(R)$  for some  $n$ , so  $(a^n)^m = 0$  for some  $m$ , and thus  $a \in N(R)$ , showing that  $a + N(R)$  is the zero coset.

(b) If  $a \in N(R)$ , then  $a^n = 0$  for some  $n$ , so  $a^n$  belongs to each prime ideal of  $R$ . This implies that  $a$  belongs to each prime ideal of  $R$ .

Conversely, suppose that  $a \notin N(R)$ . Then  $a^m \neq 0$  for all  $m \in \mathbf{Z}^+$ , and so by Zorn’s lemma there exists an ideal  $P$  maximal with respect to the property that  $a^m \notin P$  for all  $m$ . If  $I, J$  are ideals of  $R$  which properly contain  $P$ , then there exist  $n, k$  with  $a^n \in I$  and  $a^k \in J$ . Thus  $IJ \subseteq P$  would lead to a contradiction, showing that  $P$  is a prime ideal. This implies that  $a$  is not in the intersection of all prime ideals of  $R$ .  $\square$

The ideal  $N(R)$  is also called the *prime radical* of  $R$ . This terminology is justified by the above theorem. This definition can be extended to noncommutative rings, where the prime radical of  $R$  is defined to be the intersection of all prime ideals of  $R$ .

**Definition 5.1.4** *Let  $R$  be a commutative ring, and let  $I$  be an ideal of  $R$ . The ideal*

$$\sqrt{I} = \{x \in R \mid x^n \in I \text{ for some } n \in \mathbf{Z}^+\}$$

*is called the radical of  $I$ .*

We note that if  $I$  is an ideal of  $R$ , then  $\sqrt{I}$  is the inverse image in  $R$  of the nil radical of  $R/I$ , which shows that  $\sqrt{I}$  is an ideal. It also follows that  $\sqrt{I}$  is the intersection of all prime ideals of  $R$  that contain  $I$ .

In any principal ideal domain, our next definitions both reduce to the statement that the ideal in question is generated by a power of an irreducible element. But even for the polynomial ring in two indeterminates over a field or the ring of polynomials with integer coefficients the two concepts are distinct.

**Definition 5.1.5** *Let  $I$  be an ideal of the commutative ring  $R$ .*

(a) *We say that  $I$  is a primary ideal if for all elements  $a, b \in R$  we have the following condition:  $ab \in I$  implies  $a \in I$  or  $b^n \in I$ , for some  $n \in \mathbf{Z}^+$ .*

(b) *We say that  $I$  is an irreducible ideal if  $I = J \cap K$  implies  $I = J$  or  $I = K$ , for all ideals  $J, K$  of  $R$  with  $I \subseteq J$  and  $I \subseteq K$ .*

Let  $D$  be a principal ideal domain, let  $p$  be an irreducible element  $D$ , and let  $Q = p^n D$ . If  $a, b \in D$  with  $ab \in Q$ , then  $p^n \mid ab$ , so either  $p \mid a$  or  $p \mid b$ . If  $a \notin I$ , then  $p \nmid a$  implies  $p^n \mid b$ , and hence  $b \in Q$ . This shows that  $Q$  is a primary ideal.

Note that if  $I, Q$  are ideals of  $R$  with  $I \subseteq Q$ , then  $Q$  is a primary ideal of  $R$  if and only if  $Q/I$  is a primary ideal of  $R/I$ . If  $F$  is any field, we can apply this observation to  $R = F[x, y]$ ,  $Q = (x^2, y)$ , and  $I = (y)$  to show that  $(x^2, y)$  is a primary ideal of  $F[x, y]$ . This provides an example of a primary ideal that is not a power of a prime ideal.

**Proposition 5.1.6** *Let  $R$  be a commutative Noetherian ring. Then every irreducible ideal of  $R$  is a primary ideal.*

*Proof.* For an ideal  $I$  of  $R$  the conditions to be an irreducible ideal or a primary ideal are easily translated to the factor ring  $R/I$ , and so without loss of generality we may assume that  $I$  is the zero ideal.

If  $(0)$  is not a primary ideal, then there exist  $a, b \in R$  with  $ab = 0$ ,  $a \neq 0$ , and  $b^n \neq 0$  for all  $n \in \mathbf{Z}^+$ . The ideals  $\text{Ann}(b) \subseteq \text{Ann}(b^2) \subseteq \dots$  form an ascending chain, which must terminate since  $R$  is Noetherian. If  $\text{Ann}(b^m) = \text{Ann}(b^{m+1})$ , then consider the ideals  $Ra$  and  $Rb^m$ . If  $x \in Ra \cap Rb^m$ , then we have  $x = r_1a$  and  $r_2b^m$  for some  $r_1, r_2 \in R$ . But then  $(r_2b^m)b = (r_1a)b = r_1(ab) = 0$ , which implies that  $r_2 \in \text{Ann}(b^m) = \text{Ann}(b^{m+1})$ , so  $x = r_2b^m = 0$ . Thus  $Ra \cap Rb^m = (0)$ , showing that  $(0)$  is not an irreducible ideal.  $\square$

**Proposition 5.1.7** *Let  $R$  be a commutative ring. If  $I$  is an ideal of  $R$  such that  $\sqrt{I}$  is a maximal ideal of  $R$ , then  $I$  is a primary ideal of  $R$ .*

*Proof.* Let  $a, b \in R$  with  $ab \in I$ . If  $b^n \in I$  for some  $n$ , we are done. If not, then  $b \notin \sqrt{I}$ , and so  $b$  is invertible modulo  $\sqrt{I}$  since  $R/\sqrt{I}$  is a field. Since  $\sqrt{I}/I$  is the Jacobson radical of  $R/I$ , it follows that  $b$  is invertible module  $I$ , and therefore  $ab \in I$  implies  $a \in I$ .  $\square$

**Proposition 5.1.8** *Let  $R$  be a commutative ring. If  $I$  is a primary ideal of  $R$ , then  $\sqrt{I}$  is a prime ideal of  $R$ .*

*Proof.* Suppose that  $ab \in \sqrt{I}$ , with  $a \notin \sqrt{I}$ . Then  $a^n b^n = (ab)^n \in I$  for some positive integer  $n$ , but  $a^n \notin I$  since  $a \notin \sqrt{I}$ , so  $(b^n)^m \in I$  for some positive integer  $m$ , since  $I$  is a primary ideal. It follows that  $b \in \sqrt{I}$ , showing that  $\sqrt{I}$  is a prime ideal.  $\square$

**Lemma 5.1.9** *Let  $R$  be a commutative ring. If  $\{Q_i\}_{i=1}^n$  is a collection of primary ideals of  $R$  such that  $\sqrt{Q_i} = P$  for  $1 \leq i \leq n$ , then  $\bigcap_{i=1}^n Q_i$  is a primary ideal of  $R$  with  $\sqrt{\bigcap_{i=1}^n Q_i} = P$ .*

*Proof.* We first observe that  $\sqrt{\bigcap_{i=1}^n Q_i} \subseteq \bigcap_{i=1}^n \sqrt{Q_i}$ , since  $\bigcap_{i=1}^n Q_i \subseteq Q_i$ , for  $1 \leq i \leq n$ . On the other hand, if  $a \in \bigcap_{i=1}^n \sqrt{Q_i}$ , then for each  $i$  there exists  $m_i$  with  $a^{m_i} \in Q_i$ , so  $a^k \in \bigcap_{i=1}^n Q_i$ , for  $k = \max\{m_1, \dots, m_n\}$ . Thus  $a \in \sqrt{\bigcap_{i=1}^n Q_i}$ , showing that  $\sqrt{\bigcap_{i=1}^n Q_i} = \bigcap_{i=1}^n \sqrt{Q_i} = P$ .

Now suppose that  $ab \in \bigcap_{i=1}^n Q_i$ , with  $a \notin \bigcap_{i=1}^n Q_i$ . Then  $a \notin Q_j$  for some  $j$ , so  $b \in \sqrt{Q_j} = P = \sqrt{\bigcap_{i=1}^n Q_i}$ . Thus  $b^k \in \bigcap_{i=1}^n Q_i$ , for some positive integer  $k$ , showing that  $\bigcap_{i=1}^n Q_i$  is a primary ideal.  $\square$

**Definition 5.1.10** *Let  $Q$  be a primary ideal of the commutative ring  $R$ . We say that  $\sqrt{Q}$  is the associated prime ideal of  $Q$ . If  $P = \sqrt{Q}$ , then we say that  $Q$  belongs to the prime ideal  $P$  and that  $Q$  is primary for  $P$ .*

**Lemma 5.1.11** *Let  $I$  be a proper ideal of the commutative ring  $R$ . Assume that  $I = \bigcap_{i=1}^n Q_i$ , where each ideal  $Q_i$  is primary, no  $Q_i$  contains the intersection of the other primary ideals, and the ideals  $Q_i$  have distinct associated primes. Then a prime ideal  $P$  of  $R$  is the associated prime of  $Q_i$ , for some  $i$ , if and only if there exists an element  $a \in R \setminus I$  such that  $\{r \in R \mid ra \in I\}$  is primary for  $P$ .*

*Proof.* We can assume, without loss of generality, that  $I = (0)$ .

First suppose that  $P$  is a prime ideal with  $P = \sqrt{Q_j}$  for some  $1 \leq j < n$ . We need to find a nonzero element  $a \in R$  such that  $\text{Ann}(a) = \{r \in R \mid ra = 0\}$  is primary for  $P$ . Since by assumption  $Q_j$  does not contain  $\bigcap_{i \neq j} Q_i$ , there exists a nonzero element  $a \in \bigcap_{i \neq j} Q_i$ , with  $a \notin Q_j$ . Note that

$$Q_j a \subseteq Q_j \cdot \bigcap_{i \neq j} Q_i \subseteq \bigcap_{i=1}^n Q_i = (0) ,$$

and so  $Q_j \subseteq \text{Ann}(a)$ . We have  $\text{Ann}(a) \subseteq P$ , since if  $ra = 0$  for  $r \in R$ , then  $ra \in Q_j$  implies  $a^k \in Q_j$  for some  $k$ , and hence  $a \in P$  since  $P$  is prime. It follows that

$$P = \sqrt{Q_j} \subseteq \sqrt{\text{Ann}(a)} \subseteq \sqrt{P} = P .$$

Finally, we show that  $\text{Ann}(a)$  is a primary ideal. Suppose that  $x, y \in R$  with  $xy \in \text{Ann}(a)$ , but  $x \notin \text{Ann}(a)$ . Then  $xa \neq 0$ , so  $xa \notin \bigcap_{i=1}^n Q_i$ , and therefore  $xa \notin Q_j$  since we already have  $xa \in \bigcap_{i \neq j} Q_i$ . Because  $xy \in \text{Ann}(a)$ , we have  $(xa)y = 0 \in Q_j$ , and it follows that for some  $k$  we have  $y^k \in Q_j \subseteq \text{Ann}(a)$ .

Conversely, suppose that  $a$  is a nonzero element of  $R$  such that  $\text{Ann}(a)$  is primary for the prime ideal  $P$ . Since  $a \neq 0$ , but  $\bigcap_{i=1}^n Q_i = (0)$ , we must have  $a \notin Q_j$  for some  $j$ . By renumbering, if necessary, assume that  $a \notin Q_j$  for  $1 \leq j \leq m \leq n$ , and  $a \in Q_j$  for  $m < j$ . If  $r \in \sqrt{\bigcap_{j=1}^m Q_j}$ , then there exists  $k$  with  $r^k a \in \bigcap_{j=1}^m Q_j$ , so in fact  $r^k a \in \bigcap_{i=1}^n Q_i = (0)$ , and thus  $r \in P$ . Therefore  $\prod_{j=1}^m \sqrt{Q_j} \subseteq P$ , and since  $P$  is prime, we must have  $\sqrt{Q_j} \subseteq P$  for some  $j$ . But then  $P \subseteq \sqrt{Q_j}$ , since  $r \in P$  implies  $r^k a = 0 \in Q_j$  for some  $k$ , and so  $r \in \sqrt{Q_j}$  since  $a \notin Q_j$ . This shows that  $P$  is the associated prime of  $Q_j$ , completing the proof.  $\square$

**Theorem 5.1.12 (Lasker-Noether Decomposition Theorem)** *Let  $R$  be a commutative, Noetherian ring, and let  $I$  be an ideal of  $R$ .*

*There exist primary ideals  $\{Q_i\}_{i=1}^n$  with  $I = \bigcap_{i=1}^n Q_i$ , such that no  $Q_i$  contains the intersection of the other primary ideals, and the ideals  $Q_i$  have distinct associated primes.*

*Furthermore, in any such representation of  $I$  as an intersection of primary ideals, there must be  $n$  ideals, and the set of their associated prime ideals must be the same.*

*Proof.* If  $R$  contains an ideal that cannot be written as a finite intersection of irreducible ideals, then there is a maximal such ideal, since  $R$  is Noetherian. This ideal cannot be irreducible, so it can be expressed as the intersection of two larger ideals. By assumption each of these is a finite intersection of irreducible ideals, a contradiction. This shows that each ideal of  $R$  can be written as the intersection of finitely many irreducible ideals,

Assume that  $I = Q_1 \cap Q_2 \cap \cdots \cap Q_m$ , where each ideal  $Q_i$  is irreducible, and hence primary. If some  $Q_i$  contains the intersection of the others, it can be omitted. If  $Q_i$  and  $Q_j$  have the same associated prime ideal, then we can replace  $Q_i$  and  $Q_j$  with  $Q_i \cap Q_j$ , which is primary and has the same associated prime ideal.

The preceding lemma shows that the associated prime ideals of  $I$  are completely determined by  $I$ , and not by the choice of the ideals  $Q_1, \dots, Q_m$ . This completes the uniqueness part of the proof. and each of these is a primary ideal.  $\square$

### EXERCISES: SECTION 5.1

1. Let  $I, J$  be ideals of the commutative ring  $R$ . Show that  $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ .
2. Let  $I, J$  be ideals of the commutative ring  $R$ . Show that if  $\sqrt{I} + \sqrt{J} = R$ , then  $I + J = R$ .
3. Prove the note in the text that if  $I, Q$  are ideals of  $R$  with  $I \subseteq Q$ , then  $Q$  is a primary ideal of  $R$  if and only if  $Q/I$  is a primary ideal of  $R/I$ .
4. Let  $R$  be a commutative Noetherian ring, let  $P$  be a prime ideal of  $R$ , and suppose that  $Q$  is an ideal that is primary for  $P$ . Prove that if  $I, J$  are ideals of  $R$  with  $IJ \subseteq Q$ , and  $I$  is not contained in  $Q$ , then  $J$  is contained in  $Q$ .
5. Let  $F$  be a field, and consider the ideal  $I = (x^2, xy)$  of  $F[x, y]$ .
  - (a) Show that  $I$  is not a primary ideal.
  - (b) Show that  $I = (x) \cap (x^2, y)$ .
  - (c) Show that  $(x^2, ax + y)$  is a primary ideal, for any  $a \in F$ , and show that  $I = (x) \cap (x^2, ax + y)$ , so that  $I$  can be represented in infinitely many ways as an intersection of primary ideals.
6. Let  $P$  be a maximal ideal of the commutative ring  $R$ . Show that if  $Q$  is any ideal of  $R$  such that  $P^n \subseteq Q \subseteq P$  for some positive integer  $n$ , then  $Q$  is  $P$ -primary.

## 5.2 Noetherian rings

We have shown that if  $R$  is any left Noetherian ring, then the ring  $R[x]$  of polynomials with coefficients in  $R$  is again left Noetherian. This implies that if  $R$  is any commutative Noetherian ring, then the polynomial ring  $R[x_1, x_2, \dots, x_n]$  is again Noetherian. The next example provides another large class of Noetherian rings.

### Example 5.2.1

Let  $R$  be any commutative ring. We define the ring  $R[[x]]$  of all *formal power series* over  $R$  as the set of all sequences  $a = (a_0, a_1, a_2, \dots)$ , with componentwise addition and a multiplication given by defining

$$(a_0, a_1, a_2, \dots) \cdot (b_0, b_1, b_2, \dots) = (c_0, c_1, c_2, \dots),$$

where  $c_i = \sum_{j+k=i} a_j b_k$ . It can be checked easily that  $R[[x]]$  is a ring, that  $R$  can be identified with elements of the form  $(a_0, 0, 0, \dots)$ , and that the polynomial ring  $R[x]$  can be identified with the subset of all sequences with only finitely many nonzero terms.

**Theorem 5.2.1 (Cohen)** *Let  $R$  be a commutative ring. Then  $R$  is Noetherian if and only if every prime ideal of  $R$  is finitely generated.*

*Proof.* If  $R$  is Noetherian, then every ideal of  $R$  is finitely generated.

Conversely, suppose that  $R$  is not Noetherian, so that the set  $\mathcal{N}$  of all ideals of  $R$  that are not finitely generated is nonempty. If  $\{I_\alpha\}$  is an ascending chain of ideals in  $\mathcal{N}$ , then its union must be in  $\mathcal{N}$ , since otherwise the generators of the union would be a finite set of generators for some ideal in the chain. Applying Zorn's lemma yields a maximal element  $I$  in  $\mathcal{N}$ , and  $I$  cannot be a prime ideal, since by assumption every prime ideal is finitely generated. Thus there exist  $a, b \in R \setminus I$  with  $ab \in I$ , and so  $I + Rb$  and  $\{r \in R \mid rb \in I\}$  are ideals which properly contain  $I$ , and therefore must be finitely generated.

Assume that  $a_1, a_2, \dots, a_m$  generate  $\{r \in R \mid rb \in I\}$ , and that  $b, b_1, \dots, b_n$  generate  $I + Rb$ . We can assume that  $b_1, \dots, b_n \in I$ . For any  $x \in I$ , we first consider  $x$  as an element of  $I + Rb$ , and write  $x = rb + r_1 b_1 + \dots + r_n b_n$ . But then  $rb \in I$ , so  $r = s_1 a_1 + \dots + s_m a_m$ , and substituting for  $rb$  in the expression for  $x$  shows that  $a_1 b, \dots, a_m b, b_1, \dots, b_n$  generate  $I$ . This contradicts our assumption, and so  $R$  must be Noetherian.  $\square$

**Corollary 5.2.2** *If  $R$  is a commutative Noetherian ring, then so is the ring  $R[[x]]$  of all formal power series over  $R$ .*

*Proof.* Define a ring homomorphism  $\phi : R[[x]] \rightarrow R$  by  $\phi(\sum_{i=0}^{\infty} a_i x^i) = a_0$ , for all  $\sum_{i=0}^{\infty} a_i x^i \in R[[x]]$ . If  $P$  is any prime ideal of  $R[[x]]$ , then  $\phi(P)$  is a finitely generated ideal of  $R$ , with generators  $a_{10}, \dots, a_{m0}$ . Thus, for  $1 \leq k \leq m$ , there exist elements  $f_k = \sum_{i=0}^{\infty} a_{ki} x^i \in P$  for which the constant term of  $f_k$  is  $a_{k0}$ .

*Case 1.* If  $x \in P$ , then  $a_{k0} = f_k - x(\sum_{i=1}^{\infty} a_{ki} x^{i-1})$  belongs to  $P$ . For any  $f = \sum_{i=0}^{\infty} a_i x^i \in P$  we have  $f = \sum_{k=1}^m r_k a_{k0} + x(\sum_{i=1}^{\infty} a_i x^{i-1})$ , showing that  $P$  is generated by  $x, a_{10}, \dots, a_{m0}$ .

*Case 2.* If  $x \notin P$ , then  $P$  is generated by  $f_1, \dots, f_m$ . To see this, let  $f = \sum_{i=0}^{\infty} a_i x^i \in P$ . Then  $a_0 = \sum_{k=1}^m r_{k0} a_{k0}$ , for some  $r_{k1}, \dots, r_{km} \in R$ , and so  $f - \sum_{k=1}^m r_{k0} f_k = g_1 x$  for some  $g_1 \in R[[x]]$ . Since  $g_1 x \in P$ ,  $x \notin P$ , and  $P$  is prime, it follows that  $g_1 \in P$ . It is possible to extend this argument inductively to obtain  $f - \sum_{k=1}^m (\sum_{i=1}^j r_{ki} x^i) f_k = g_j x^j$  for some  $g_j \in R[[x]]$ . Finally,  $f = \sum_{k=1}^m h_k f_k$  for  $h_k = \sum_{i=0}^{\infty} r_{ki} x^i$ .  $\square$

**Theorem 5.2.3** *Let  $R$  be a commutative Noetherian ring. Then the nil radical of  $R$  is nilpotent. That is, there exists  $m \in \mathbf{Z}^+$  such that  $N(R)^m = (0)$ .*

*Proof.* The proof that  $N(R)$  is an ideal (see Proposition 5.1.1) actually shows that if  $a^n = 0$  and  $b^m = 0$ , then  $(ra + sb)^{n+m} = 0$  for any  $r, s \in R$ . An inductive argument shows that if  $a_1, \dots, a_k$  are the generators of  $N(R)$ , with  $a_i^{m_i} = 0$ , then  $N(R)^m = (0)$  for  $m = m_1 + \dots + m_k$ .  $\square$

**Corollary 5.2.4** *If  $Q$  is a primary ideal of the commutative Noetherian ring  $R$ , then there exists a positive integer  $m$  such that  $(\sqrt{Q})^m \subseteq Q$ .*

**Lemma 5.2.5** *Let  $J$  be an ideal of the commutative Noetherian ring  $R$ , and let  $I = \bigcap_{n=1}^{\infty} J^n$ . Then  $J I = I$ .*

*Proof.* Suppose that  $J I$  is properly contained in  $I$ . By assumption  $R$  is Noetherian, so we can write  $J I$  as an intersection  $J I = Q_1 \cap \dots \cap Q_m$  of primary ideals  $Q_k$ , for  $1 \leq k \leq m$ . Since  $J I \subset I$ , for some index  $k$  there must exist  $b \in I \setminus Q_k$ . For any  $a \in J$ , we have  $ab \in J I \subseteq Q_k$ , and so  $a^n \in Q_k$  for some  $n$  since  $Q_k$  is a primary ideal. This shows that  $J \subseteq \sqrt{Q_k}$ , and it follows from Corollary 5.2.3 that  $J^n \subseteq Q_k$  for some  $n$ . By the definition of  $I$  we have  $I \subseteq Q_k$ , contradicting our assumption that  $J I \neq I$ .  $\square$

The proof of the next theorem makes use of Lemma 3.2.8 (Nakayama's lemma). We review its proof in this context. Let  $J$  be the Jacobson radical of  $R$ , and let  $I$  be any nonzero ideal of  $R$ . The set of ideals properly contained in  $I$  has a maximal element  $I'$ , since  $R$  is Noetherian. Then  $I/I'$  is a simple  $R$ -module, so it is annihilated by  $J(R)$ , which is the intersection of annihilators of simple  $R$ -modules. It follows that  $J I \subseteq I' \neq I$ .

**Theorem 5.2.6 (Krull)** *Let  $R$  be a commutative Noetherian ring. Then the intersection of powers of the Jacobson radical is zero. That is,*

$$\bigcap_{n=1}^{\infty} (J(R))^n = (0) ,$$

where  $J(R)$  is the Jacobson radical of  $R$ .

*Proof.* Let  $J(R) = J$ , and  $I = \bigcap_{n=1}^{\infty} J^n$ . If  $I \neq (0)$ , then since  $I$  is finitely generated it follows from Nakayama's lemma that  $J I \neq I$ . This contradicts the preceding lemma, and so we conclude that  $I = (0)$ .  $\square$

We now state several results whose proofs are beyond the scope of this brief introduction to Noetherian rings. Recall that in a principal ideal domain every nonzero prime ideal is maximal, so that the only proper chains of prime ideals have the form  $P \supset (0)$ . This result was extended by Krull to Noetherian rings, and is known as the principal ideal theorem: If  $R$  is a Noetherian ring,  $aR$  is a proper principal ideal of  $R$ , and  $P$  is any prime ideal minimal over  $aR$ , then  $P$  contains no chains of primes longer than  $P \supset P_1$ .

We say that a chain  $P_0 \supset P_1 \supset \cdots \supset P_m$  of prime ideals has length  $m$ . An induction argument can be used to generalize the principal ideal theorem, and this important result is usually called Krull's generalized principal ideal theorem. We will investigate some of its consequences for the study of polynomial rings.

**Theorem 5.2.7 (Generalized principal ideal theorem)** *Let  $I$  be a proper ideal of the Noetherian ring  $R$ . If  $I$  is generated by  $m$  elements, and  $P$  is any prime ideal minimal over  $I$ , then any chain of primes  $P \supset P_1 \supset \cdots$  has length at most  $m$ .*

*Proof.* See Section 7.17 of [5] on Krull dimension.  $\square$

One important consequence of the generalized principal ideal theorem is that any Noetherian ring satisfies the descending chain condition for prime ideals. There may or may not be a uniform bound on the lengths of chains of prime ideals of a Noetherian ring. If  $R$  is Noetherian, and has a chain of prime ideals of length  $n$ , but none longer, then we say that  $R$  has *Krull dimension* equal to  $n$ .

A field  $F$  is said to be *algebraically closed* if every monic polynomial of positive degree with coefficients in  $F$  has a root in  $F$ . As a second consequence of the generalized principal ideal theorem, we can compute the Krull dimension of the polynomial ring  $R = F[x_1, x_2, \dots, x_n]$ , where  $F$  is algebraically closed. It can be shown that any maximal ideal of  $R$  is generated by  $n$  elements  $x_1 - a_1,$

$x_2 - a_2, \dots, x_n - a_n$ . It follows that any chain of prime ideals of  $R$  has length at most  $n$ . Of course, there is a chain of length  $n$ , given by

$$(x_1, x_2, \dots, x_n) \supset (x_2, \dots, x_n) \supset \dots \supset (x_n) \supset (0) .$$

Thus  $R$  has Krull dimension  $n$ .

We end the section with an important theorem due to Hilbert.

**Lemma 5.2.8** *Let  $F$  be an algebraically closed field, and let  $f, f_1, \dots, f_m$  be elements of the polynomial ring  $F[x_1, \dots, x_n]$ . If the system*

$$f(x_1, \dots, x_n) \neq 0$$

$$f_1(x_1, \dots, x_n) = \dots = f_m(x_1, \dots, x_n) = 0$$

*has a solution in some extension field of  $F$ , then it must have a solution in  $F$ .*

**Theorem 5.2.9 (Hilbert's Nullstellensatz)** *Let  $F$  be an algebraically closed field, and let  $I$  be any ideal of the polynomial ring  $F[x_1, \dots, x_n]$ . Then  $\sqrt{I}$  consists of all elements  $f \in F[x_1, \dots, x_n]$  such that  $f(a_1, a_2, \dots, a_n) = 0$  for all  $(a_1, a_2, \dots, a_n)$  such that  $g(a_1, a_2, \dots, a_n) = 0$  for all  $g \in I$ .*

*Proof.* For proofs of the Nullstellensatz and the preceding lemma, see Section 7.12 of [5].  $\square$

## EXERCISES: SECTION 5.2

1. Let  $R$  be a commutative Noetherian ring. Prove that if every prime ideal of  $R$  is maximal, then  $R$  is Artinian.
2. Let  $D$  be a Noetherian integral domain. Show that if  $S$  is any multiplicative set in  $D$ , then  $D_S$  is Noetherian.
3. Let  $I$  be an ideal of a Noetherian ring  $R$ , let  $M$  be a finitely generated  $R$ -module, and let  $N = \bigcap_{n=1}^{\infty} I^n M$ . Show that  $IN = N$ .
4. Let  $R$  be a Noetherian ring, and let  $M$  be a finitely generated  $R$  module. A submodule  $Q$  of  $M$  is said to be a *primary submodule* if for all  $a \in R$  and all  $x \in M$ , we have the following condition: if  $ax \in Q$  but  $x \notin Q$ , then  $a^n M \subseteq Q$  for some positive integer  $n$ . Prove that any submodule of  $M$  can be written as a finite intersection of primary submodules of  $M$ .

### 5.3 Dedekind domains

In this section we investigate a new approach to unique factorization, using ideals rather than elements. If  $D$  is a principal ideal domain, then any nonzero ideal  $I$  of  $D$  has the form  $I = aD$  for some nonzero  $a \in D$  with  $a = p_1 p_2 \cdots p_n$  for irreducible elements  $p_1, p_2, \dots, p_n$  of  $D$ . It follows that  $I$  is a product of prime ideals, since  $aD = \prod_{i=1}^n p_i D$ . We use this condition as our definition of a Dedekind domain.

**Definition 5.3.1** *An integral domain  $D$  is called a Dedekind domain if each proper ideal of  $D$  can be written as a product of a finite number of prime ideals of  $D$ .*

We will show in Theorem 5.3.4 that a Dedekind domain has some of the properties of a principal ideal domain. Specifically, a Dedekind domain must be Noetherian, and any nonzero prime ideal of a Dedekind domain must be maximal. This shows that a unique factorization domain can fail to be a Dedekind domain, since, for example, the unique factorization domain  $\mathbf{Q}[x, y]$  contains the nonzero prime ideals  $(x) \subset (x, y)$ .

We will prove a number of facts about Dedekind domains by using the notion of an ‘inverse’ of an ideal. This necessitates the introduction of the following concept.

**Definition 5.3.2** *Let  $D$  be an integral domain with quotient field  $F$ . A fractional ideal of  $D$  is a nonzero  $D$ -submodule  $I$  of  $F$  such that there exists  $0 \neq d \in D$  with  $dI \subseteq D$ .*

*If  $I$  is a fractional ideal of  $D$ , we define*

$$I^{-1} = \{q \in F \mid qI \subseteq D\},$$

*and say that  $I$  is invertible if  $I^{-1} \cdot I = D$ .*

The preceding definition relies on the following observation. If  $D$  is an integral domain with quotient field  $F$ , then it is not difficult to check the if  $I_1, I_2$  are fractional ideals of  $D$ , then so are  $I_1 + I_2$ ,  $I_1 \cap I_2$ , and  $I_1 I_2$ , where

$$I_1 I_2 = \left\{ \sum_{i=1}^n u_i v_i \mid u_i \in I_1 \text{ and } v_i \in I_2 \right\}.$$

#### Example 5.3.1

In the field of rational numbers  $\mathbf{Q}$ , the set  $\frac{1}{2}\mathbf{Z}$  of all multiples of  $1/2$  is a fractional ideal of  $\mathbf{Z}$ . In fact it is an invertible fractional ideal, with inverse  $2\mathbf{Z}$ .

More generally, if  $D$  is an integral domain with quotient field  $F$ , let  $I$  be any nonzero finitely generated  $D$ -submodule of  $F$ . If  $d$  is the product of the denominators of the generators of  $I$ , then  $dI \subseteq D$ , showing that  $I$  is a fractional ideal. If  $I$  is generated by a single element  $q \in F$ , then  $q^{-1}D \cdot qD = D$ , so in this case  $I$  is invertible.

**Lemma 5.3.3** *Let  $D$  be an integral domain with quotient field  $F$ , and let  $I$  be an ideal of  $D$  that is invertible when considered as a fractional ideal. The following conditions hold.*

(a) *The ideal  $I$  is finitely generated.*

(b) *If  $I$  is a product of prime ideals, then this product is unique (up to order).*

*Proof.* (a) Let  $I$  be any invertible fractional ideal. Since  $I^{-1} \cdot I = D$ , there exist elements  $u_i \in I^{-1}$ ,  $v_i \in I$ , for  $1 \leq i \leq n$ , with  $\sum_{i=1}^n u_i v_i = 1$ . For any element  $x \in I$  we have  $x = \sum_{i=1}^n (u_i x) v_i$ , and since  $u_i x \in D$ , this shows that  $v_1, \dots, v_n$  are generators for  $I$ .

(b) Assume that  $I = P_1 P_2 \cdots P_n = Q_1 Q_2 \cdots Q_m$  for prime ideals  $P_1, \dots, P_n$  and  $Q_1, \dots, Q_m$ . Since  $I^{-1} \cdot I = D$ , we have  $(I^{-1} P_2 \cdots P_n) P_1 = D$ , etc., showing that each of the prime ideals  $P_i$  and  $Q_j$  is invertible. Since  $P_1$  is prime and  $P_1 \supseteq Q_1 Q_2 \cdots Q_m$ , it follows that  $P_1$  contains one of the primes  $Q_j$ , and (after renumbering if necessary) we can assume that  $P_1 \supseteq Q_1$ . Now  $P_1^{-1} Q_1$  is an ideal of  $D$  since  $P_1^{-1} Q_1 \subseteq P_1^{-1} P_1 = D$ , so  $P_1 (P_1^{-1} Q_1) = Q_1$  implies that either  $P_1 \subseteq Q_1$  or  $P_1^{-1} \subseteq Q_1$ . The second case is impossible since it implies that  $P_1^{-1} \subseteq D$ , and so we conclude that  $P_1 = Q_1$ .

Multiplying  $I$  by  $P_1^{-1}$ , we obtain  $P_2 \cdots P_n = Q_2 \cdots Q_m$ . (In case  $n = 1$ , we have  $D = Q_2 \cdots Q_m$ , which is impossible.) An induction argument now completes the proof.  $\square$

**Theorem 5.3.4** *The following conditions hold for any Dedekind domain  $D$ .*

(a) *Every nonzero ideal of  $D$  is invertible.*

(b) *Every proper ideal of  $D$  can be written uniquely (up to order) as a product of a finite number of prime ideals of  $D$ ;*

(c)  *$D$  is a Noetherian domain.*

(d) *Every nonzero prime ideal of  $D$  is maximal.*

*Proof.* (a) Since every nonzero ideal of  $D$  is a product of finitely many prime ideals, it suffices to prove that every nonzero prime ideal is invertible. Let  $P$  be a nonzero prime ideal of  $D$ , and let  $p$  be a nonzero element of  $P$ . Then  $pD = P_1P_2 \cdots P_n$  for prime ideals  $P_1, \dots, P_n$ , and each of these prime ideals is invertible since  $pD$  is invertible. Since  $P$  is prime and  $P_1P_2 \cdots P_n \subseteq P$ , we must have  $P_i \subseteq P$  for some  $i$ . If we can show that  $P_i$  is maximal, then we must have  $P_i = P$ , and hence  $P$  is invertible.

To complete the proof, we will show that any invertible prime ideal of  $D$  is maximal. Let  $Q$  be an invertible prime ideal of  $D$ , and let  $a \in D \setminus Q$ . Our strategy is to show that  $aQ + Q^2 = Q$ , and then since  $Q$  is invertible we obtain  $aD + Q = D$ , showing that  $aD + Q$  is invertible is an invertible element of  $D/Q$ , and therefore  $D/Q$  is a field.

To prove the claim that  $aQ + Q^2 = Q$ , we first observe that  $D/Q$  must be a Dedekind domain. This follows from the fact that every nonzero ideal of  $D/Q$  has the form  $I/Q$  for an ideal  $I$  of  $D$  with  $I \supset Q$ , and the representation of  $I$  as a product  $I = P_1 \cdots P_n$  of prime ideals of  $D$  yields a representation of  $I/Q$  as a product  $I/Q = (P_1/Q) \cdots (P_n/Q)$  of prime ideals of  $D/Q$ . Let  $I = aD + Q = P_1 \cdots P_n$  and  $J = a^2D + Q = Q_1 \cdots Q_m$  be representations of these two ideals as products of prime ideals of  $D$ . In  $D/Q$  we have  $I^2/Q = J/Q$ , and since  $J/Q$  is a principal ideal of  $D/Q$ , it is invertible, so the preceding lemma shows that the prime factorizations of  $I^2/Q$  and  $J/Q$  in  $D/Q$  must be the same (up to order). The one-to-one correspondence between prime ideals of  $D/Q$  and  $D$  shows that we must have  $P_1^2 \cdots P_n^2 = Q_1 \cdots Q_m$ , and so  $I^2 = J$ . Thus  $Q \subset I^2 = a^2D + aQ + Q^2 \subseteq aD + Q^2$ , so for any element  $x \in Q$  we have  $x = ad + y$ , for some  $a, d \in D$  and  $y \in Q^2$ . Then  $ad = x - y \in Q$ , so  $d \in Q$  since  $a \notin Q$ , and in fact we have  $Q \subseteq aQ + Q^2 \subseteq Q$ . This verifies the claim, and completes the proof of part (a).

The proofs of (b) and (c) follow from the preceding lemma, and we have actually proved (d) in the course of proving part (a).  $\square$

Before giving several characterizations of Dedekind domains, we need additional information about fractional ideals. In a principal ideal domain, every nonzero ideal is a free module on one generator. We can generalize this to Dedekind domains by showing that every nonzero ideal is projective, and finitely generated. In fact, every ideal can be generated by at most two elements. (See the exercises.)

**Proposition 5.3.5** *Let  $D$  be an integral domain. A fractional ideal  $I$  of  $D$  is invertible if and only if it is projective as a  $D$ -module.*

*Proof.* First assume that  $I$  is an invertible fractional ideal of  $D$ . There exist  $u_i \in I^{-1}$  and  $v_i \in I$ , for  $1 \leq i \leq n$ , with  $1 = \sum_{i=1}^n u_i v_i$ , and so for any  $x \in I$  we have  $x = \sum_{i=1}^n (u_i x) v_i$ , with  $u_i x \in D$ . Therefore we can define

$D$ -homomorphisms  $f : D^n \rightarrow I$  by  $f(d_1, \dots, d_n) = \sum_{i=1}^n d_i v_i$  and  $g : I \rightarrow D^n$  by  $g(x) = (xv_1, \dots, xv_n)$ . Since  $fg = 1_I$ , it follows that  $I$  is isomorphic to a direct summand of a free module.

Conversely, assume that  $I$  is projective, with a  $D$ -homomorphism  $f : M \rightarrow I$  from a free  $D$ -module  $M$  onto  $I$ , and a splitting  $D$ -homomorphism  $g : I \rightarrow M$ . Let  $\pi_\alpha : M \rightarrow D$  be the projection of  $M$  onto the component indexed by  $\alpha$ , and let  $f_\alpha : D \rightarrow I$  be the component of  $f$  indexed by  $\alpha$ . If for each component we let  $f_\alpha(1) = v_\alpha$ , then for any nonzero  $q \in I$ , the element  $g(q)$  has only finitely many nonzero components, and

$$q = fg(q) = \sum_{\alpha \in J} f_\alpha(\pi_\alpha g(q)) = \sum_{\alpha \in J} \pi_\alpha g(q) f_\alpha(1) = \sum_{\alpha \in J} \pi_\alpha g(q) \cdot v_\alpha.$$

Now consider  $\pi_\alpha g : I \rightarrow D$ . There exists  $0 \neq d \in D$  with  $dI \subseteq D$ , so for any  $q \in I$  we have the equation

$$dv_\alpha(\pi_\alpha g(q)) = \pi_\alpha g(dv_\alpha q) = dq(\pi_\alpha g(v_\alpha))$$

in  $D$ . This leads to the equation

$$\pi_\alpha g(q) = (v_\alpha^{-1}q)(\pi_\alpha g(v_\alpha))$$

in the quotient field of  $D$ , which shows that  $v_\alpha^{-1}\pi_\alpha g(v_\alpha) \in I^{-1}$ , and also shows that  $v_\alpha^{-1}q \in D$  since  $\pi_\alpha g(q) \in D$  and  $\pi_\alpha g(v_\alpha) \in D$ . We now have

$$q = \sum_{\alpha \in J} f_\alpha(\pi_\alpha g(q)) = \sum_{\alpha \in J} \pi_\alpha g(q) \cdot v_\alpha = \sum_{\alpha \in J} (v_\alpha^{-1}q)(\pi_\alpha g(v_\alpha)) \cdot v_\alpha,$$

and cancelling  $q$  yields the following sum, which is taken over the nonzero components of  $g(q)$ .

$$1 = \sum_{i=1}^n (v_i^{-1}\pi_i g(v_i)) \cdot v_i$$

Since  $v_i^{-1}\pi_i g(v_i) \in I^{-1}$  and  $v_i \in I$  for  $1 \leq i \leq n$ , we have shown that  $I$  is invertible.  $\square$

**Theorem 5.3.6** *The following conditions are equivalent for an integral domain  $D$ :*

- (1)  $D$  is a Dedekind domain;
- (2) every nonzero ideal of  $D$  is invertible;
- (3) every fractional ideal of  $D$  is invertible;
- (4) every nonzero ideal of  $D$  is projective as a  $D$ -module.

*Proof.* (1)  $\Rightarrow$  (2) This follows from Theorem 5.3.4.

(2)  $\Rightarrow$  (4) This was shown in Proposition 5.3.5.

(4)  $\Rightarrow$  (3) Let  $I$  be a fractional ideal of  $D$ , with  $dI \subseteq D$  for  $0 \neq d \in D$ . Then  $I$  is isomorphic to the ideal  $dI$  via the  $D$ -homomorphism  $f(q) = dq$ , for all  $q \in I$ ,

and so  $I$  is projective since  $dI$  is projective. It follows from Proposition 5.3.5 that  $I$  is invertible.

(3)  $\Rightarrow$  (2) This implication is clear.

(2)  $\Rightarrow$  (1) Assume that there exists a nonzero ideal of  $D$  that cannot be written as a finite product of prime ideals of  $D$ . Since every nonzero ideal of  $D$  is invertible, every nonzero ideal of  $D$  is finitely generated, and so  $D$  is Noetherian. Therefore, since the set of nonzero ideals that cannot be expressed as a finite product of prime ideals is nonempty, it must have a maximal element  $I$ . The ideal  $I$  cannot itself be prime, so it cannot be maximal, and thus there exists a maximal ideal  $P$  of  $D$  with  $I \subset P \subset D$ . Using the assumption that every nonzero ideal of  $D$  is invertible, we have  $IP^{-1} \subseteq D$  since  $I \subset P$ . Furthermore, there exist  $u_i \in P^{-1}$  and  $v_i \in P$ , for  $1 \leq i \leq n$ , such that  $\sum_{i=1}^n u_i v_i = 1$ . It follows from this identity that  $I \subseteq IP^{-1}$  and  $I = (IP^{-1})P$ . If  $I = IP^{-1}$ , then  $P^{-1} = D$ , contradicting the fact that  $P$  is a proper ideal, so the choice of  $I$  implies that  $IP^{-1}$  can be expressed as a finite product of prime ideals. We conclude that  $I = (IP^{-1})P$  is a finite product of prime ideals, a contradiction. This completes the proof.  $\square$

If  $D$  is a Dedekind domain, then for any proper nonzero ideal  $I$  of  $D$  we have  $I^{-1}I = D$ , and so  $I^{-1}$  must be strictly larger than  $D$ . The same result holds more generally, and we will need it in the next section to give an additional characterization of Dedekind domains.

**Proposition 5.3.7** *Let  $D$  be an integral domain with quotient field  $F$ . Assume that  $D$  is Noetherian and that every nonzero prime ideal of  $D$  is maximal. Then for any proper nonzero ideal  $I$  of  $D$  there exists  $q \in F \setminus D$  with  $qI \subseteq D$ .*

*Proof.* Let  $I$  be a proper nonzero ideal of  $D$ . If  $I$  is a principal ideal, say  $I = aD$ , then  $a^{-1} \in F \setminus D$  and  $a^{-1}I \subseteq D$ . If  $I$  is not principal, let  $a$  be any nonzero element of  $D$ , and let  $P$  be a maximal ideal of  $D$  with  $I \subseteq P$ . Using an argument similar to that in Theorem 5.3.6, it can be shown that any nonzero ideal of a Noetherian domain contains a product of nonzero prime ideals. (If the condition fails, choose a maximal such ideal. It cannot be prime, hence contains a product of larger ideals, each of which contains a product of primes, and this contradicts the assumption.) Thus there exist nonzero prime ideals  $P_1, P_2, \dots, P_n$  of  $D$  with  $P_1 P_2 \cdots P_n \subseteq aD$ , and one of these ideals must be contained in  $P$ , say  $P_1 \subseteq P$ , since  $P$  is prime. By assumption, every nonzero prime ideal of  $D$  is maximal, so it follows that  $P_1 = P$ . We thus have

$$PP_2 \cdots P_n \subseteq aD \subset I \subseteq P \subset D,$$

and by omitting unnecessary prime ideals, we can assume that  $P_2 \cdots P_n$  is not contained in  $aD$ . If we choose an element  $b \in P_2 \cdots P_n \setminus aD$ , then  $a^{-1}b \notin D$ ,

since  $b \notin aD$ . We have

$$a^{-1}bI \subseteq a^{-1}bP \subseteq a^{-1}PP_2 \cdots P_n \subseteq a^{-1}aD = D,$$

and this completes the proof.  $\square$

### EXERCISES: SECTION 5.3

1. Show that if  $D$  is a Dedekind domain, then  $D/I$  is Artinian for all nonzero ideals  $I$  of  $D$ .
2. Let  $D$  be any integral domain. Show that the set of invertible fractional ideals of  $D$  forms a group.
3. Let  $D$  be an integral domain. Show that  $D$  is a Dedekind domain if and only if every divisible  $D$ -module is injective.
4. Let  $D$  be an integral domain. Prove that  $D$  is a Dedekind domain if and only if for each nonzero ideal  $I$  of  $D$  and each  $0 \neq a \in I$  there exists  $b \in I$  such that  $I = aD + bD$ .

## 5.4 Integral extensions

We recall that an extension field  $F \supseteq K$  in which each element is a root of a nonzero polynomial with coefficients in  $K$  is said to be algebraic over  $K$ . There is a similar concept for ring extensions  $T \supseteq R$ , which reduces to the familiar one for fields.

**Definition 5.4.1** *Let  $R$  be a subring of the commutative ring  $T$ .*

(a) *An element  $u \in T$  is said to be integral over  $R$  if there exists a monic polynomial  $f(x) \in R[x]$  such that  $f(u) = 0$ .*

(b) *The ring  $T$  is said to be an integral extension of  $R$  if each element of  $T$  is integral over  $R$ .*

**Proposition 5.4.2** *Let  $R$  be a subring of the commutative ring  $T$ . The following conditions are equivalent for an element  $u \in T$ :*

- (1)  *$u$  is integral over  $R$ ;*
- (2) *the subring  $R[u]$  generated by  $R$  and  $u$  is finitely generated as an  $R$ -module;*
- (3) *there exists a subring  $R'$  with  $R \subseteq R' \subseteq T$  such that  $R[u] \subseteq R'$  and  $R'$  is finitely generated as an  $R$ -module;*
- (4) *there exists a faithful  $R[u]$ -submodule of  $T$  that is finitely generated as an  $R$ -module.*

*Proof.* (1)  $\Rightarrow$  (2) Let  $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  be a monic polynomial in  $R[x]$  with  $f(u) = 0$ . Then  $u^n = -a_{n-1}u^{n-1} - \dots - a_1u - a_0$ , and an inductive argument shows that  $\sum_{i=0}^{n-1} Ru^i$  contains  $u^m$  for all  $m \geq 0$ , so  $R[u]$  is generated as an  $R$ -module by  $\{1, u, \dots, u^{n-1}\}$ .

(2)  $\Rightarrow$  (3) We can simply let  $R' = R[u]$ .

(3)  $\Rightarrow$  (4) We can simply take  $R'$  to be the required  $R[u]$ -module.

(3)  $\Rightarrow$  (1) Assume that  $M$  is a faithful  $R[u]$ -submodule of  $T$ , with  $M = \sum_{i=1}^n Rt_i$  for  $t_1, \dots, t_n \in T$ . Since  $ut_i \in M$ , for  $1 \leq i \leq n$  we have  $ut_i = \sum_{j=1}^n a_{ij}t_j$ , with  $a_{ij} \in R$ . The coefficients  $a_{ij}$  define a matrix  $A = [a_{ij}]$ , and if we let  $x$  be the column vector with entries  $t_1, \dots, t_n$ , then in matrix form we have the equation

$$uIx = Ax,$$

where  $I$  is the  $n \times n$  identity matrix.

Let  $d = \det(uI - A)$ . Multiplying the matrix equation  $(uI - A)x = 0$  by the adjoint of the matrix  $uI - A$ , we obtain  $dIx = 0$ , so  $dt_i = 0$  for  $1 \leq i \leq n$ . Since  $M$  is a faithful  $R[u]$ -module and  $dM = (0)$ , it follows that  $d = 0$ . Expanding  $\det(uI - A)$  yields an expression of the form  $u^n + b_{n-1}u^{n-1} + \dots + b_1u + b_0$ , which must equal zero, and this produces the necessary monic polynomial in  $R[x]$  that has  $u$  as a root.  $\square$

**Corollary 5.4.3** *Let  $R$  be a subring of the commutative ring  $T$ . If  $T$  is finitely generated as a module over  $R$ , then  $T$  is an integral extension of  $R$ .*

We can now provide numerous examples of integral ring extensions. The rings of Gaussian integers  $\mathbf{Z}[i]$  is an integral extensions of  $\mathbf{Z}$ , as is  $\mathbf{Z}[\sqrt{-5}]$  (the example of a non-UFD), since both are finitely generated as modules over  $\mathbf{Z}$ .

Let  $R$  be a subring of  $T$  such that  $T$  is finitely generated as a module over  $R$ , say  $T = \sum_{i=1}^n Rt_i$ . Then it is clear that  $T[x] = \sum_{i=1}^n R[x]t_i$ , and so the polynomial ring  $T[x]$  is an integral extension of  $R[x]$ .

As a final example, we note that any polynomial ring  $R[x]$  is an integral extension of the subring  $R[x^n]$  generated by  $x^n$ . To see this, we only need to note that  $R[x]$  is generated as an  $R[x^n]$ -module by the set  $\{1, x, \dots, x^{n-1}\}$ .

**Corollary 5.4.4** *Let  $R$  be a subring of the commutative ring  $T$ . Then*

$$\widehat{R} = \{u \in T \mid u \text{ is integral over } R\}$$

*is a subring of  $T$ .*

*Proof.* Let  $u, v \in \widehat{R}$ , with  $f(u) = 0$  and  $g(v) = 0$  for monic polynomials in  $R[x]$  of degrees  $n$  and  $m$ , respectively. As in the proof of Proposition 5.4.2,

the subring  $R[u, v]$  is generated as an  $R$ -module by  $\{u^i v^j\}$ , for  $0 \leq i < n$  and  $0 \leq j < m$ . Since  $u - v$  and  $uv$  belong to  $R[u, v]$ , it follows that both belong to  $\widehat{R}$ . This implies that  $\widehat{R}$  is a subring of  $T$ .  $\square$

**Definition 5.4.5** *Let  $R$  be a subring of the commutative ring  $T$ .*

(a) *The subring  $\widehat{R}$  of all elements integral over  $R$  is called the integral closure of  $R$  in  $T$ .*

(b) *If  $\widehat{R} = R$ , then we say that  $R$  is integrally closed in  $T$ . If  $D$  is an integral domain that is integrally closed in its quotient field, then we simply say that  $D$  is integrally closed.*

#### Example 5.4.1

We will show that any principal ideal domain is integrally closed in its quotient field. If  $D$  is a principal ideal domain with quotient field  $Q$ , then each nonzero element of  $Q$  can be expressed in the form  $a/b$ , where  $a, b$  are nonzero elements of  $D$  and  $\gcd(a, b) = 1$ . If  $a/b$  is a root of the monic polynomial  $x^n + c_{n-1}x^{n-1} + \dots + c_1x + c_0$ , then  $a^n + c_{n-1}a^{n-1}b + \dots + c_1ab^{n-1} + c_0b^n = 0$ , which implies that  $b$  is a divisor of  $a^n$ . This is impossible unless  $b$  is a unit, in which case  $a/b \in D$ .

The previous example shows that we cannot find an integral extension  $R$  of  $\mathbf{Z}$  with  $\mathbf{Z} \subset R \subset \mathbf{Q}$ . The examples given previously of integral extensions of  $\mathbf{Z}$  were subrings of  $\mathbf{R}$  or  $\mathbf{C}$ .

The next proposition shows that  $\mathbf{Q}$  is not an integral extension of any subring.

**Proposition 5.4.6** *Let  $R$  be a subring of the integral domain  $D$ , and assume that  $D$  is an integral extension of  $R$ . Then  $D$  is a field if and only if  $R$  is a field.*

*Proof.* First assume that  $R$  is a field. Let  $u$  be a nonzero element of  $D$ , and let  $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  be a monic polynomial in  $R[x]$  of minimal degree in the set of polynomials having  $u$  as a root. Then  $u^n + a_{n-1}u^{n-1} + \dots + a_1u + a_0 = 0$ , and if  $a_0 = 0$  then we can cancel  $u$  to obtain a monic polynomial of lower degree with  $u$  as a root. Thus we must have  $a_0 \neq 0$ , and therefore the equation  $u(u^{n-1} + a_{n-1}u^{n-2} + \dots + a_1) = -a_0$  shows that  $u$  is invertible in  $D$  if and only if  $a_0$  is invertible in  $R$ . Since  $R$  is assumed to be a field, it follows that  $D$  is a field.

Conversely, assume that  $D$  is a field and  $a$  is a nonzero element of  $R$ . Then  $a^{-1}$  exists in  $D$ , and since  $D$  is integral over  $R$  there exists a monic polynomial  $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  in  $R[x]$  with  $f(a^{-1}) = 0$ . Since  $(a^{-1})^n + a_{n-1}(a^{-1})^{n-1} + \dots + a_1a^{-1} + a_0 = 0$ , we can multiply by  $a^n$  to obtain  $1 + a_{n-1}a + \dots + a_1a^{n-1} + a_0a^n = 0$ . This shows that  $a^{-1} = -a_{n-1} - \dots - a_0a^{n-1}$  in fact belongs to  $R$ , and so  $R$  is a field.  $\square$

**Corollary 5.4.7** *Let  $R$  be a subring of the commutative ring  $T$ , and assume that  $T$  is an integral extension of  $R$ . If  $Q$  is a prime ideal of  $T$ , then  $Q$  is a maximal ideal of  $T$  if and only if  $Q \cap R$  is a maximal ideal of  $R$ .*

*Proof.* Let  $Q$  be any prime ideal of  $T$ , and let  $P = Q \cap R$ . The composition of the inclusion  $R \rightarrow T$  and natural projection  $T \rightarrow T/Q$  is a ring homomorphism with kernel  $Q \cap R = P$ , and so there is an induced ring homomorphism  $R/P \rightarrow T/Q$  that is one-to-one, and we can identify  $R/P$  with its image in  $T/Q$ . Since  $T$  is an integral extension of  $R$ , by simply reducing coefficients modulo  $P$  it is easy to see that each element of  $T/Q$  is a root of a monic polynomial with coefficients in  $R/P$ . By the preceding proposition,  $T/Q$  is a field if and only if  $R/P$  is a field, so  $Q$  is maximal if and only if  $P$  is maximal.  $\square$

**Proposition 5.4.8** *Let  $R$  be a subring of the integral domain  $D$ , and assume that  $D$  is an integral extension of  $R$ . If  $S$  is any multiplicative set of  $R$ , then  $D_S$  is an integral extension of  $R_S$ .*

*Proof.* Let  $\frac{u}{s}$  be a nonzero element of  $D_S$ , with  $u \in D$  and  $s \in S$ . Since  $D$  is an integral extension of  $R$ , there exists a polynomial  $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  in  $R[x]$  with  $f(u) = 0$ . It follows that  $g(\frac{u}{s}) = 0$  for the polynomial

$$g(x) = x^n + \frac{a_{n-1}}{s}x^{n-1} + \dots + \frac{a_1}{s^{n-1}}x + \frac{a_0}{s^n}$$

in  $R_S[x]$ .  $\square$

**Theorem 5.4.9** *Let  $R$  be a subring of the integral domain  $D$ , and assume that  $D$  is an integral extension of  $R$ .*

(a) **(Incomparability)** *Let  $Q, Q'$  be prime ideals of  $D$  such that  $Q \subseteq Q'$ . Then  $Q \neq Q'$  implies  $Q \cap R \neq Q' \cap R$ .*

(b) **(Lying-over)** *For each prime ideal  $P$  of  $R$  there exists a prime ideal  $Q$  of  $D$  such that  $Q \cap R = P$ .*

(c) **(Going up)** *If  $P \subseteq P'$  are prime ideals of  $R$ , and  $Q$  is a prime ideal of  $D$  with  $Q \cap R = P$ , then there exists a prime ideal  $Q'$  of  $D$  such that  $Q \subseteq Q'$  and  $Q' \cap R = P'$ .*

*Proof.* (a) Let  $Q, Q'$  be prime ideals of  $D$  such that  $Q \subseteq Q'$ , and let  $Q \cap R = P$ . Then  $R/P$  is isomorphic to a subring of  $D/Q$ , so  $P$  is a prime ideal of  $R$ , and therefore  $S = R \setminus P$  is a multiplicative set in both  $R$  and  $D$ . By Proposition 5.4.8, the localization  $D_S$  of  $D$  at  $S$  is an integral extension of the localization  $R_S$  of  $R$  at  $S$ . It can easily be checked that  $Q_S \cap R_S = P_S$ , and so Corollary 5.4.7 implies that  $Q_S$  is a maximal ideal of  $D_S$  since  $P_S$  is a maximal ideal of  $R_S$ . If  $Q' \cap R = Q \cap R = P$ , then  $Q' \cap S = \emptyset$ , and so it follows from Theorem 1.3.11 that  $Q'_S$  is a prime ideal of  $D_S$  with  $Q_S \subseteq Q'_S$ . The maximality of  $Q_S$  implies that  $Q_S = Q'_S$ , and therefore  $Q = Q'$ .

(b) Let  $P$  be a prime ideal of  $R$ , and let  $S$  be the multiplicative set  $R \setminus P$ . We again consider the localizations  $R_S \subseteq D_S$ . We can choose a maximal ideal of  $D_S$ , which must have the form  $Q_S$  for some maximal ideal  $Q$  of  $D$ . As in part (a), since  $D_S$  is integral over  $R_S$ , the ideal  $Q_S \cap R_S$  must be maximal in  $R_S$ , so  $Q_S \cap R_S = P_S$  since  $P_S$  is the only maximal ideal of  $R_S$ . Now consider the following diagram, in which the vertical mappings are all one-to-one.

$$\begin{array}{ccccc} R & \longrightarrow & D & \longrightarrow & D/Q \\ \downarrow & & \downarrow & & \downarrow \\ R_S & \longrightarrow & D_S & \longrightarrow & D_S/Q_S \end{array}$$

The kernel of the bottom row is  $P_S$ , since  $Q_S \cap R_S = P_S$ . It can be checked that the kernel of the top row is  $P$ , and so  $Q \cap R = P$ .

(c) Let  $P \subseteq P'$  be prime ideals of  $R$ , and let  $Q$  be a prime ideal of  $D$  with  $Q \cap R = P$ . The canonical mapping from  $R/P$  into  $D/Q$  is one-to-one since  $Q \cap R = P$ , and so we can identify  $R/P$  with its image in  $D/Q$ . Since  $D/Q$  is an integral extension of  $R/P$ , it follows from part (b) that we can find a prime ideal  $Q'/Q$  of  $D/Q$  lying over the prime ideal  $P'/P$  of  $R/P$ . Consider the following diagram, in which the vertical mappings are all onto.

$$\begin{array}{ccccc} R & \longrightarrow & D & \longrightarrow & D/Q' \\ \downarrow & & \downarrow & & \downarrow \\ R/P & \longrightarrow & D/Q & \longrightarrow & (D/Q)/(Q'/Q) \end{array}$$

Since  $(Q'/Q) \cap (R/P) = (P'/P)$ , the kernel of the bottom row is  $P'/P$ , and it follows that the kernel of the top row is  $P'$ , showing that  $Q' \cap R = P'$ , as required.  $\square$

In the setting of the previous theorem, if we assume in addition that  $R$  is an integrally closed domain, then a further condition holds, known as 'going down'. We state the result without proof: Let  $R$  be a subring of the integral domain

$D$ , assume that  $D$  is an integral extension of  $R$ , and that  $R$  is an integrally closed domain. If  $P' \subseteq P$  are prime ideals of  $R$ , and  $Q$  is a prime ideal of  $D$  with  $Q \cap R = P$ , then there exists a prime ideal  $Q'$  of  $D$  such that  $Q' \subseteq Q$  and  $Q' \cap R = P'$ .

We can now give an additional characterization of Dedekind domains.

**Theorem 5.4.10** *The following conditions are equivalent for an integral domain  $D$ :*

- (1)  $D$  is a Dedekind domain;
- (2)  $D$  is Noetherian, integrally closed in its quotient field, and each nonzero prime ideal of  $D$  is maximal.

*Proof.* First assume that  $D$  is a Dedekind domain with quotient field  $F$ . Then Theorem 5.3.4 shows that  $D$  is Noetherian, and that each nonzero prime ideal of  $D$  is maximal. To show that  $D$  is integrally closed in  $F$ , let  $u \in F$  be an element integral over  $D$ , and assume that  $u$  is a root of a monic polynomial  $f(x)$  in  $D[x]$  of degree  $n$ . Let  $I$  be the  $D$ -submodule of  $F$  generated by  $\{1, u, \dots, u^{n-1}\}$ . It follows from the relation given by  $f(x)$  that  $I$  contains all powers of  $u$ , and therefore  $I^2 \subseteq I$ . Since  $I$  is a finitely generated  $D$ -submodule of  $F$ , it is a fractional ideal, which must be invertible since  $D$  is a Dedekind domain. This implies that  $I \subseteq D$ , and so  $u \in D$ .

Conversely, assume that  $D$  is Noetherian, integrally closed, and each nonzero prime ideal of  $D$  is maximal. Let  $I$  be any ideal of  $D$ , and suppose that  $I^{-1}I$  is properly contained in  $D$ . Then  $I^{-1}I$  is an ideal of  $D$ , and it follows from Proposition 5.3.7 that there exists  $u \in F \setminus D$  with  $u(I^{-1}I) \subseteq D$ . For any element  $q \in I^{-1}$ , and any  $a \in I$ , we have  $(uq)a = u(qa) \in u(I^{-1}I) \subseteq D$ , and this shows that  $uq \in I^{-1}$ , so  $uI^{-1} \subseteq I^{-1}$ . Because  $D$  is Noetherian, the ideal  $I$  is finitely generated, and if we let  $d$  be the product of these generators, then  $dI^{-1} \subseteq D$ , showing that  $I^{-1}$  is a fractional ideal. Furthermore,  $dI^{-1}$  is an ideal of  $D$ , so it is finitely generated, say  $dI^{-1} = \sum_{i=1}^n Da_i$ . It can be checked that  $I^{-1} = \sum_{i=1}^n Da_i d^{-1}$ . Thus  $I^{-1}$  is a faithful  $D[u]$ -submodule of  $F$  that is finitely generated as a  $D$ -module, and so  $u$  is integral over  $D$ . Since  $D$  is assumed to be integrally closed, this implies that  $u \in D$ , contradicting the choice of  $u$ . We conclude that  $I^{-1}I$  is *not* properly contained in  $D$ , so  $I^{-1}I = D$ , and thus  $I$  is invertible.  $\square$

The next theorem implies that unique factorization of ideals holds in the rings that are of interest in number theory. We state the theorem, with a reference to a proof that used Theorem 5.4.10. In the theorem,  $\widehat{D}$  is an integral extension of  $D$ , and so it follows from Theorem 5.4.9 that every nonzero prime ideal of  $\widehat{D}$  is maximal. It is not too difficult to prove that  $\widehat{D}$  is integrally closed, so the hardest part of the proof lies in showing that  $\widehat{D}$  is a Noetherian ring.

**Theorem 5.4.11** *Let  $D$  be an integral domain with quotient field  $Q$ , and let  $F$  be a finite extension field of  $Q$ . If  $\tilde{D}$  is the set of all elements of  $F$  that are integral over  $D$ , then  $\tilde{D}$  is a Dedekind domain.*

*Proof.* See the proof of Theorem 10.7 of [5].  $\square$

Let  $p$  be a prime, and let  $\rho$  be a primitive  $p$ th root of unity. If  $\mathbf{Z}[\rho]$  denotes the subring of  $\mathbf{C}$  generated by  $\rho$ , then it can be shown that  $\mathbf{Z}[\rho]$  is the integral closure of  $\mathbf{Z}$  in  $\mathbf{Q}(\rho)$ , the splitting field over  $\mathbf{Q}$  of  $x^p - 1$ . It follows that  $\mathbf{Z}[\rho]$  is a Dedekind domain.

#### EXERCISES: SECTION 5.4

1. Show that  $\mathbf{Z}[x]$  is an integrally closed domain.
2. Suppose that the ring  $T$  is an integral extension of  $T'$ , and  $T'$  is an integral extension of  $R$ . Show that  $T$  is an integral extension of  $R$ .
3. Let  $T$  be an integral extension of  $R$ . Show that the polynomial ring  $T[x]$  is an integral extension of  $R[x]$ .
4. Prove that any unique factorization domain is integrally closed.
5. Let  $D$  be an integral domain. Prove that  $D$  is a Dedekind domain if and only if  $D$  is Noetherian, integrally closed in its quotient field, and  $D/I$  is Artinian for all nonzero ideals  $I$  of  $D$ .
6. Let  $T$  be an integral extension of  $R$ . Prove that  $J(R) = R \cap J(T)$ .



# Bibliography

- [1] Auslander, M., and D. A. Buchsbaum, *Groups, Rings, Modules*, Harper and Row, New York, 1974.
- [2] Beachy, J. A., and W. D. Blair, *Abstract Algebra*, 2<sup>nd</sup> Ed., Waveland Press, Prospect Heights, Ill., 1996.
- [3] Eisenbud, D., *Commutative Algebra with a View toward Algebraic Geometry*, Graduate Texts in Mathematics, Vol. 150, Springer-Verlag, New York, 1995.
- [4] Jacobson, N., *Basic Algebra I*, 2<sup>nd</sup> Ed., W. H. Freeman & Company Publishers, San Francisco, 1985.
- [5] Jacobson, N., *Basic Algebra II*, 2<sup>nd</sup> Ed., W. H. Freeman & Company Publishers, San Francisco, 1989.
- [6] Lang, S., *Algebra*, 3<sup>rd</sup> Ed., Addison-Wesley Publishing Co., Inc., Reading, Mass., 1993.
- [7] Matsumura, H., *Commutative Ring Theory*, Cambridge University Press, Cambridge, 1986.
- [8] Sharp, R. Y., *Steps in Commutative Algebra*, London Mathematical Society Student Texts, Vol. 19, Cambridge University Press, Cambridge, 1990.
- [9] Van der Waerden, B. L., *Algebra*, Springer-Verlag, New York, 1991.
- [10] Walker, Elbert A. *Introduction to Abstract Algebra*, Random House, New York, 1987.

**INDEX**

algebraically closed field, 248  
associated prime ideal, 243  
closure, integral, 257  
Dedekind, 239  
Dedekind domain, 250  
dimension, Krull, 248  
domain, Dedekind, 250  
element, integral, 255  
extension, integral, 255  
field, algebraically closed, 248  
fractional ideal, 250  
going down theorem, 259  
going up theorem, 258  
Hilbert, 249  
ideal, fractional, 250  
ideal, irreducible, 242  
ideal, primary, 242  
incomparability theorem, 258  
integral closure, 257  
integral element, 255  
integral extension ring, 255  
integrally closed, 257  
invertible fractional ideal, 250  
irreducible ideal, 242  
Krull, 248  
Krull, 248  
Krull dimension, 248  
Lasker, 240  
lying over theorem, 258  
Macauley, 240  
nil radical, 241  
Noether, 240  
power series, ring of, 246  
primary ideal, 242  
primary submodule, 249  
prime ideal, associated to  $\mathcal{Q}$ , 243  
prime radical, 242  
principal ideal theorem, generalized, 248  
principal ideal theorem, 248  
radical, nil, 241  
radical, of an ideal, 242  
radical, prime, 242  
ring, of power series, 246  
submodule, primary, 249  
theorem, generalized principal ideal, 248

theorem, going down, 259  
theorem, going up, 258  
theorem, incomparability, 258  
theorem, lying over, 258  
theorem, principal ideal, 248