Primary decomposition of ideals in a ring

Sola Oyinsan

Follow this and additional works at: https://scholarworks.lib.csusb.edu/etd-project

Part of the Algebraic Geometry Commons

Recommended Citation

This Thesis is brought to you for free and open access by the John M. Pfau Library at CSUSB ScholarWorks. It has been accepted for inclusion in Theses Digitization Project by an authorized administrator of CSUSB ScholarWorks. For more information, please contact scholarworks@csusb.edu.
PRIMARY DECOMPOSITION OF IDEALS IN A RING

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment
of the Requirements for the Degree

Master of Arts

in

Mathematics

by

Sola Oyinsan

June 2007
PRIMARY DECOMPOSITION OF IDEALS IN A RING

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

by

Sola Oyinsan

June 2007

Approved by:

Laura Wallace, Committee Chair

Jim Okon, Committee Member

Davida Fischman, Committee Member

Peter Williams, Chair,
Department of Mathematics

6/8/07

Joseph Chavez
Graduate Coordinator,
Department of Mathematics
Abstract

The concept of unique factorization was first recognized in the 1840s, but even then, it was still fairly believed to be automatic. The error of this assumption was exposed largely through attempts to prove Fermat’s last theorem. Once mathematicians discovered that this property did not always hold, it was only natural for them to try to search for the strongest available alternative. Thus began the attempt to generalize unique factorization. Using the ascending chain condition on principal ideals, we will show the conditions under which a ring is a unique factorization domain. We will also generalize the properties of unique factorization of elements to the primary decomposition of ideals in a ring, thus generalizing of the Fundamental Theorem of Arithmetic.
ACKNOWLEDGEMENTS

First of all, I would like to thank God for not only giving me the ability, but also the means to be able to pursue such an endeavor. I would also like to thank Dr. Laura Wallace for her advising and for the many hours I’ve spent in her office during this long process. I could not have done this without her. Thank you to Dr. Davida Fischman for inspiring me to enroll in the Masters program, and for all her help and support while I was a Math student. She has been very instrumental in the development of my skills in mathematics. Thank you to Dr. Jim Okon for giving me this idea, directing me to the right people, and for reading my paper. I would like to extend my gratitude to the entire math department here at CSUSB. You have made my experience here at Cal State pleasant and memorable.

Thanks to my family for their patience with me while I worked on this project. Thanks to my church family for all your encouragement and support. Finally thank you to my fellow students Dolores Chavez, Maria Chaparro, and Daniela Sandoval for the countless hours we spent studying together and getting through these classes. We did it!
# Table of Contents

Abstract iii

Acknowledgements iv

1 INTRODUCTION 1

2 UNIQUE FACTORIZATION IN AN INTEGRAL DOMAIN 3
   2.1 Rings, Ideals, and Ring Homomorphisms ...................... 3
   2.2 Prime and Irreducible Elements .............................. 9
   2.3 Unique Factorization of Elements in a Domain .................. 11
   2.4 The Ascending Chain Condition on Principal Ideals .......... 12
   2.5 Principal Ideal Domains ........................................ 13
   2.6 Unique Factorization in $D[x]$ .................................. 15
   2.7 Unique Factorization in $\mathbb{Z}[\sqrt{d}]$ ................... 21

3 PRIMARY DECOMPOSITION OF IDEALS IN A RING 25
   3.1 Prime and Primary Ideals ....................................... 25
   3.2 Primary Decomposition ........................................... 31
   3.3 Noetherian Rings .................................................. 32

4 PRIMARY DECOMPOSITION AND UNIQUENESS 40
   4.1 First Uniqueness Theorem ...................................... 40
   4.2 Extended and Contracted Ideals ................................. 42
   4.3 Extended and Contracted Ideals in Rings of Fractions ........ 44
   4.4 Second Uniqueness Theorem ..................................... 46

5 An Application of Unique Factorization 49

6 Conclusion 54

Bibliography 55
Chapter 1

INTRODUCTION

According to the Fundamental Theorem of Arithmetic, every integer may be uniquely expressed as a product of primes. But does this property of unique factorization hold for an arbitrary ring? This question arose in the early to mid 1800s when it was largely assumed that the decomposition of an element into irreducible components is unique. The answer to this question is the subject of this paper.

After Z, Q, R, and C, one of the very first rings of interest was \( \mathbb{Z}[\sqrt{-1}] \), introduced by Gauss in his paper on Biquadratic Residues in 1828. Gauss showed that in this ring, any element can be factored uniquely into a product of primes, as is the case of the integers. Number theorists soon after appreciated the usefulness of adjoining the solutions of polynomial equations to Z and they found that in many ways, these enlarged rings behaved just like Z. Euler, Gauss, Dirichlet, and Kummer all used this idea to prove special cases of Fermat's Last Theorem (the insolubility in the integers of the equation \( x^p + y^p = z^p \) for \( p \geq 3 \)). Their proofs involved factoring the expression \( x^p + y^p = z^p \) in the enlarged ring \( \mathbb{Z}[\omega_n] \), where \( \omega_n \) is an \( n \)th root of unity. The equation \( x^p + y^p \) becomes \( (x + y)(x + ay) \cdots (x + a^{p-1}y) \). Thus this factorization takes place in the ring \( \mathbb{Z}[\alpha] = \{a_0 + a_1 \alpha + \cdots + a_{p-1} \alpha^{p-1} | a_i \in \mathbb{Z} \} \). When \( \mathbb{Z}[\alpha] \) has unique factorization, it is profitable to compare the factorization of \( x^p + y^p \) as \( (x + y)(x + ay) \cdots (x + a^{p-1}y) \) to the factorization of \( z^p \). However, the problem with this method is that the ring \( \mathbb{Z}[\alpha] \) with \( \alpha \in \mathbb{C} \) does not always have unique factorization.

This was the case when Lame, in 1839 stirred excitement in the mathematics community by announcing that he had solved the general case of Fermat's Last Theorem.
Lame assumed that unique factorization holds in these enlarged rings. But this is not always the case as can be seen in the ring $\mathbb{Z}[\sqrt{-5}]$ where $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

As it became clear that unique factorization did not always hold, the search for some generalized form of this property began. Many of the objects that we now associate with commutative algebra are a direct result of this search. In his attempt to generalize unique factorization, Dedekind introduced the concept of an ideal and also defined a ring. Kronecker, in his generalization, introduced the polynomial ring $k[x]$ where $k$ is a field and a similar concept of an ideal which he called a modular system or module. In 1905, Lasker further generalized unique factorization into primary decomposition. However in his proofs, he used many complicated arguments from elimination theory. In her paper in 1921, Emmy Noether developed the general theory of primary decomposition from the ascending chain condition alone. In this way, she enormously simplified the theory and made it more elegant.

Our objective is to show some of the properties of rings that tell us when elements will factor uniquely into a product of irreducible (or prime) elements. We will show that if a ring satisfies the ascending chain condition on principal ideals, then any element that is not zero or a unit may be factored into a product of irreducible elements. We will see that these factors are unique only under certain conditions. Some of the examples we have chosen are the rings of the form $\mathbb{Z}[\sqrt{d}]$ where $d$ is a negative integer and $D[x]$, where $D$ is an integral domain. We will further generalize this to the factorization of elements in a ring into primary decomposition of an ideal. However, just as in the case of unique factorization, primary decomposition does not hold for an arbitrary ring. One important result of this generalization that we will see is that in a special class of rings called Noetherian rings, every ideal has a primary decomposition.

Over the centuries, many other proposed proofs of Fermat’s Last Theorem did not hold up under scrutiny. However, recent discoveries tying Fermat’s Last Theorem to modern mathematical theories gave hope that these theories might eventually lead to a proof. In June 1993, excitement again spread through the mathematics community with the announcement that Andrew Wiles of Princeton University had proved Fermat’s Last Theorem. But again, his proof did not hold up under scrutiny. This proof was later revised by Andrew Wiles and Richard Taylor in September of 1994. There is a consensus among the mathematics community that the revised proof is indeed valid.
Chapter 2

UNIQUE FACTORIZATION IN AN INTEGRAL DOMAIN

The integers have the property that every nonzero integer \( \neq \pm 1 \) can be uniquely factored into a product of primes. However, this is not true for all rings. The classical example is the ring \( \mathbb{Z}[\sqrt{-5}] \), where 6 has two different factorizations into irreducible components, \( 2 \cdot 3 \) and \( (1 + \sqrt{-5})(1 - \sqrt{-5}) \). We will later see that these factors are indeed irreducible in \( \mathbb{Z}[\sqrt{-5}] \). In this chapter we will be looking at certain characteristics of rings that will tell us when unique factorization will hold. We will also see some classes of rings, namely principal ideal domains and euclidean domains that have unique factorization. Some of the examples of rings that we will consider are the rings \( \mathbb{Z}[\sqrt{d}] \) where \( d \) is a negative integer and polynomial rings such as \( \mathbb{Z}[x] \).

2.1 Rings, Ideals, and Ring Homomorphisms

The integers are our analogue for understanding unique factorization. One consequence of the search for a generalized form of unique factorization is that the integers and some properties of numbers were placed into a more general setting. In this section, we will look at some of these properties of numbers in a more abstract setting. Also included in this section are some definitions that will serve as tools for illustrating other properties that we will later discuss regarding unique factorization.

Definition 2.1. A ring \( R \) is a nonempty set with two binary operations, addition (de-
noted \( a + b \) and multiplication (denoted \( ab \)), such that for all \( a, b, c \in R \),

i) \( a + b = b + a \).

ii) \( (a + b) + c = a + (b + c) \).

iii) There is an additive identity 0; that is, there is an element 0 \( \in R \) such that \( a + 0 = a \) for all \( a \in R \).

iv) There is an element \( -a \) in \( R \) such that \( a + (-a) = 0 \) for all \( a \in R \).

v) \( a(bc) = (ab)c \).

vi) \( a(b + c) = ab + ac \) and \( (b + c)a = ba + ca \).

A ring \( R \) is a commutative ring if for every \( a, b \in R \), \( ab = ba \). The integers \( \mathbb{Z} \) would qualify as a commutative ring. Some rings have an element called a multiplicative identity or unity. A unity is a nonzero element \( e \) such that for every \( a \in R \), \( ae = ea = a \).

In the integers, \( 1 \) is a unity. A unit is a nonzero element that has a multiplicative inverse; that is \( a \in R \) is a unit if there is a nonzero \( b \in R \) such that \( ab = ba = e \). The only elements in the integers that are units are 1 and \( -1 \).

**Definition 2.2.** A **field** is a commutative ring with unity in which every nonzero element is a unit.

Some familiar fields are the rationals \( \mathbb{Q} \) and the complex numbers \( \mathbb{C} \). Unless otherwise stated, all rings will be commutative with unity.

**Definition 2.3.** An ideal of a ring \( R \) is a subset \( I \) of \( R \) such that:

i) \( 0 \in I \);

ii) \( a, b \in I \) imply \( a - b \in I \);

iii) \( a \in I \) and \( r \in R \) imply \( ra \in I \).

**Example 2.4.** The set \( I = \{2\} = \{2k : k \in \mathbb{Z}\} \) of all even integers is an ideal of \( \mathbb{Z} \):
\[ 2 \cdot 0 = 0 \in I; \text{ for any } a, b \in I, \ a = 2k \text{ and } b = 2l \text{ for } k, l \in \mathbb{Z} \text{ and } a - b = 2k - 2l = 2(k - l) \in I; \text{ and finally, for any } r \in \mathbb{Z}, \ ar = 2kr \in I. \text{ Because } I \text{ satisfies (i), (ii) and (iii), we conclude that } I \text{ is indeed an ideal in } \mathbb{Z}. \]
Definition 2.5. An ideal $P$ in a ring $R$ is said to be prime if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$.

Definition 2.6. An ideal $Q$ of a ring $R$ is said to be primary if $Q \neq R$ and $ab \in Q$ implies $a \in Q$ or $b^n \in Q$ for some positive integer $n$.

Dedekind was the first to introduce the notion of an ideal of a ring. An ideal is a general way of representing a number or an element of a ring. A prime ideal in some sense, generalizes a prime number while a primary ideal is the corresponding generalization of the power of a prime number. It is clear that a prime ideal is primary.

Definition 2.7. An integral domain $D$ (or domain for short) is a commutative ring with unity and no zero divisors, that is for any $a, b \in D$, $ab = 0$ implies that $a = 0$ or $b = 0$.

A ring is not the most appropriate abstraction of the integers because some important properties that the integers have are left out of the definition of a ring. An integral domain is more appropriate because integral domains admit some properties that are not true for all rings. One of such properties is cancellation, which we will introduce here:

Lemma 2.8. Let $a$, $b$, and $c$ belong to an integral domain $D$. If $a \neq 0$ and $ab = ac$, then $b = c$. This property is called cancellation.

Proof. From $ab = ac$, we have $a(b - c) = 0$. Since $a \neq 0$, we must have $b - c = 0$ so that $b = c$. \qedsymbol

Example 2.9. The ring of integers $\mathbb{Z}$ is an integral domain.

Example 2.10. The ring of Gaussian integers $\mathbb{Z}[i] := \{a + bi | a, b \in \mathbb{Z}\}$ is a subring of the complex numbers $\mathbb{C}$ and is therefore an integral domain.

Example 2.11. The ring $\mathbb{Z}[x]$ of polynomials with integer coefficients is an integral domain; for if $f = a_0 + a_1 x^1 + \cdots + a_n x^n$ and $g = b_0 + b_1 x^1 + \cdots + b_m x^m$ with $f$ and $g$ nonzero, then among the coefficients of $f$ and $g$, there is some $a_k \neq 0$ and $b_l \neq 0$. Choose $a_k$ and $b_l$ to be the leading coefficients of $f$ and $g$ respectively. If $fg = 0$, then the coefficient $a_k b_l = 0$ in the product $fg$, which we cannot have since $\mathbb{Z}$ is a domain.
Given a ring $R$ and an ideal $I$ of $R$, another interesting type of ring that can be constructed is the ring $R/I = \{ r + I : r \in R \}$. $R/I$ is called a quotient ring and the elements of $R/I$ are cosets. Quotient rings are important because their structure is usually less complicated than that of $R$ and by examining a quotient ring $R/I$, we can often deduce certain properties of the ring $R$ itself. Given two elements $r + I$, $s + I \in R/I$, addition and multiplication are defined as follows: $(r + I) + (s + I) = (r + s) + I$ and $(r + I)(s + I) = rs + I$.

Lemma 2.12. Let $I$ be an ideal of a ring $R$. Then $I$ is prime if and only if $R/I$ is a domain.

Proof. Let $I$ be a prime ideal. If $0 = (a + I)(b + I) = (ab + I)$, then $ab \in I$. Since $I$ is prime, either $a \in I$ or $b \in I$. That is either $a + I = 0$ or $b + I = 0$. Hence $R/I$ is a domain.

Conversely, Let $R/I$ be a domain and $ab \in I$. This implies $0 = ab + I = (a + I)(b + I)$.

Since $R/I$ is a domain, then $a + I = 0$ or $b + I = 0$. It follows that $a \in I$ or $b \in I$. Hence $I$ is prime. □

One way to discover information about a ring is to examine its interaction with other rings by way of homomorphisms. Homomorphic images of a ring tell us some important properties of the original ring. The utility of a particular homomorphism lies in its ability to preserve the ring properties we want while losing some inessential ones. In this way, we have replaced the ring $R$ by a ring which is less complicated and therefore easier to study, but in the process, we have preserved enough information to answer questions we have about $R$.

Definition 2.13. A ring homomorphism $\phi$ from a ring $R$ to a ring $S$ is a mapping from $R$ to $S$ that preserves the two ring operations; that is for all $a, b \in R$,

$$\phi(a + b) = \phi(a) + \phi(b) \text{ and } \phi(ab) = \phi(a)\phi(b).$$

Definition 2.14. Let $\phi$ be a map from a ring $R$ to a ring $\tilde{R}$. $\phi$ is a ring isomorphism if it satisfies the following properties:

i) $\phi$ is a ring homomorphism;

ii) $\phi$ is one to one: that is for $a, b \in R$, $\phi(a) = \phi(b)$ implies $a = b$;
iii) \( \phi \) is onto: that is for any \( \bar{a} \in \bar{R} \), there is some \( a \in R \) such that \( \phi(a) = \bar{a} \).

If such an isomorphism exists, then \( R \) and \( \bar{R} \) are said to be isomorphic, and we write \( R \cong \bar{R} \). When two rings are isomorphic, they are algebraically identical. Whatever is true for one ring algebraically is true for the other. Although an isomorphism is a special case of a homomorphism, the two concepts are entirely different. Isomorphisms allow us to look at a group in an alternative way. Homomorphisms are strictly investigative tools.

The next three theorems are a result of utilizing ring homomorphisms. We will frequently refer to them and direct the reader to the appropriate reference for their proofs.

**Theorem 2.15. Correspondence Theorem for Rings:** If \( I \) is a proper ideal of a ring \( R \), then there is a bijection from the family of all intermediate ideals \( J \), where \( I \subseteq J \subseteq R \) to the family of all ideals in \( R/I \), given by

\[
J \mapsto \pi(J) = J/I = \{a + I : a \in J\},
\]

where \( \pi : R \to R/I \) is the natural map [5].

The Correspondence Theorem is usually used to say that every ideal of the quotient ring \( R/I \) has the form \( J/I \) for some unique ideal \( J \) with \( I \subseteq J \subseteq R \).

**Definition 2.16.** Let \( \phi \) be a homomorphism from a ring \( R \) onto a ring \( S \). Then the **kernel** of \( \phi \), denoted \( \text{Ker}(\phi) \) is the set \( \{r \in R | \phi(r) = 0\} \).

**Theorem 2.17. First Isomorphism Theorem for Rings:** Let \( \phi \) be a ring homomorphism from a ring \( R \) to a ring \( S \). Then the mapping from \( R/\text{Ker}(\phi) \) to \( R \) given by \( r + \text{Ker}(\phi) \to \phi(r) \), is an isomorphism; that is, \( R/\text{Ker}(\phi) \cong \phi(R) \) [3].

**Theorem 2.18. Third Isomorphism Theorem for Rings:** Let \( R \) be a ring and \( I \) and \( J \) be ideals of \( R \) with \( I \subseteq J \). Then \( J/I \) is an ideal of \( R/I \) and \( R/J \cong R/I \) [3].

The procedure by which the rational numbers \( \mathbb{Q} \) are constructed from the integers \( \mathbb{Z} \) extends easily to any ring \( R \) that is an integral domain and produces the **field of fractions** of \( R \), denoted \( \text{Frac}(R) = \{r/s : r, s \in R, s \neq 0\} \). This construction consists of
taking all ordered pairs \((a, s)\), where \(a, s \in R\) and \(s \neq 0\) and setting up an equivalence relation between such pairs as:

\[(a, s) \equiv (b, t) \iff at - bs = 0.\]

This works only if \(R\) is a domain because the verification that the relation is transitive involves cancellation. For instance, we want to be able to show that if \((a, s) \equiv (b, t)\) and \((b, t) \equiv (c, w)\) then \((a, s) \equiv (c, w)\). We verify transitivity as follows: From the hypothesis, we have \(at - bs = 0\) and \(bu - tc = 0\), so that \(at = bs\) and \(bu = tc\). Hence we have

\[at + bu - bs - tc = 0.\]

Multiplying both sides by \(uc\) we get

\[atuc + buuc - bsuc - tcuc = 0.\]

and by cancellation we get

\[au + uc - cs - uc = au - cs = 0.\]

It follows that \((as) \equiv (cu)\).

Let \(R\) be a ring. A \textit{multiplicatively closed subset} of \(R\) is a subset \(S\) of \(R\) such that \(1 \in S\) and \(S\) is closed under multiplication. We define the relation \(\equiv\) on \(R \times S\) as follows:

\[(a, s) \equiv (b, t) \iff (at - bs)u = 0 \text{ for some } u \in S.\]

If we just had \(at - bs = 0\), then the transitive law would fail when \(S\) has zero-divisors[4]. The equivalence class of \((a, s)\) is denoted \(a/s\) and \(S^{-1}R\) denotes the set of equivalence classes. A ring structure is put on \(S^{-1}R\) by defining addition and multiplication of the fractions \(a/s\) in the same way as in elementary algebra: that is

\[(a/s) + (b/t) = (at + bs)/st,\]

\[(a/s)(b/t) = ab/st.\]

The set \(S^{-1}R\) satisfies the axioms of a commutative ring with identity [1].

The canonical mapping \(f: R \to S^{-1}R\) defined by \(f(x) = x/1\) is a ring homomorphism; for \(f(x + y) = (x + y)/1 = x/1 + y/1 = f(x) + f(y)\), \(f(xy) = xy/1 = \)
(x/1)(y/1) = f(x)f(y) and f(1) = 1/1 as expected. The ring $S^{-1}R$ is called the ring of fractions or localisation of $R$ with respect to $S$. If $R$ is a domain and $S = R - \{0\}$, then $S^{-1}R$ is called the field of fractions of $R$. We will often refer to homomorphisms from a ring $R$ to a ring of fractions $S^{-1}R$ when investigating some ring properties.

2.2 Prime and Irreducible Elements

Factorization in the integers is unique only if the factors are prime. In this section we will look at prime numbers more generally. The concept of a prime element turns out to be crucial to unique factorization. Let us begin with the following definitions:

**Definition 2.19.** A nonzero element $p$ of an integral domain $D$ is prime if $p$ is not a unit and $p | bc$ implies $p | b$ or $p | c$.

**Definition 2.20.** A nonzero element $q$ of an integral domain $D$ is irreducible if $q$ is not a unit and whenever $b, c \in D$ with $q = bc$ then $b$ is a unit or $c$ is a unit.

**Definition 2.21.** Elements $a$ and $b$ of an integral domain $D$ are associates if $a = ub$ where $u$ is a unit in $D$.

In $\mathbb{Z}$, the irreducible elements are precisely the prime elements. Here, we have defined a prime element and an irreducible element separately. This distinction might appear confusing. That is because in $\mathbb{Z}$, the notion of prime and irreducible are equivalent. Usually, our definition of irreducible is given for a prime number while our definition of a prime is stated as a property of primes attributed to Euclid. However, it is necessary to make this distinction as this equivalence does not hold in an arbitrary domain. In fact, this relationship between prime and irreducible will be a very important part of our discussion. Many of those attempting to prove Fermat’s Last Theorem were not aware of this, and it proved to be a fundamental flaw in their reasoning.

**Theorem 2.22.** In an integral domain $D$, a prime element is irreducible.

**Proof.** Suppose $a \in D$ is prime and $a = bc$ with $b, c \in D$. By the definition of a prime, $a | b$ or $a | c$. Say $a | b$ so that $ax = b$, $x \in D$. Then $b \cdot 1 = b = ax = (bc)x = b(cx)$, and by cancellation, $1 = cx$. Hence $c$ is unit, and $a$ is irreducible. \qed
We will later illustrate in Example 2.28 that the converse of the previous theorem is false; that is, an irreducible element is not always prime. The distinction between prime and irreducible is best illustrated in integral domains of the form \( \mathbb{Z}[\sqrt{d}] = \{ a + b\sqrt{d} \mid a, b \in \mathbb{Z} \} \) and \( d < 0 \). In order to analyze these rings, we need a convenient way of determining their units and irreducibles. To this end, we define a function \( N \), called the *norm*, from \( \mathbb{Z}[\sqrt{d}] \) into the non-negative integers, defined by \( N(a + b\sqrt{d}) = a^2 - db^2 \). We will now prove the following three properties regarding \( N \):

**Proposition 2.23.** Let \( x, y \in \mathbb{Z}[\sqrt{d}] \) and \( N(a + b\sqrt{d}) = a^2 - db^2 \):

i) \( N(x) = 0 \) if and only if \( x = 0 \).

ii) \( N(xy) = N(x)N(y) \) for all \( x, y \).

iii) \( N(x) = 1 \) if and only if \( x \) is a unit.

**Proof.** Let \( x = a + b\sqrt{d} \) and \( y = \bar{a} + \bar{b}\sqrt{d} \).

i) Let \( a + b\sqrt{d} = 0 \). Then \( a = b = 0 \). So \( N(a + b\sqrt{d}) = a^2 - db^2 = 0 \). Conversely, if \( N(a + b\sqrt{d}) = 0 \), then \( a^2 - db^2 = 0 \). So \( a^2 = db^2 \leq 0 \). Since \( d < 0 \), \( a = b = 0 \).

ii) \( N(xy) = N((a\bar{a} + b\bar{b}d) + (\bar{a}b + a\bar{b}\sqrt{d})) \)

\[
= (a\bar{a} + b\bar{b}d)^2 - d(a\bar{b} + \bar{a}b)^2 \\
= a^2\bar{a}^2 + 2a\bar{a}b\bar{b}d + b^2\bar{b}^2d^2 - d(a\bar{a}b\bar{b} + \bar{a}b\bar{a}d + \bar{a}^2b^2) \\
= a^2\bar{a}^2 + b^2\bar{b}^2d^2 - d(a^2\bar{b}^2 + a\bar{a}b\bar{b}) \\
= (a^2 - db^2)(\bar{a}^2 - d\bar{b}^2) \\
= N(a + b\sqrt{d})N(\bar{a} + \bar{b}\sqrt{d}) \\
= N(x)N(y).
\]

iii) If \( xy = 1 \), then \( 1 = N(1) = N(xy) = N(x)N(y) \). Hence \( N(x) = 1 = N(y) \).

Conversely, if \( N(x) = 1 \) where \( x = a + b\sqrt{d} \), then

\[
1 = N(a + b\sqrt{d}) = a^2 - db^2 = (a + b\sqrt{d})(a - b\sqrt{d}).
\]

Hence \( a + b\sqrt{d} \) is a unit.

\(\square\)
2.3 Unique Factorization of Elements in a Domain

Here, we will look at unique factorization property itself more generally. We will see examples of rings other than the integers that have this property. We will also give an example of a ring that does not have unique factorization.

**Definition 2.24.** An integral domain $D$ is a **unique factorization domain (or UFD)** if the following two conditions hold:

i) Every nonzero element of $D$ that is not a unit can be written as a product of irreducibles.

ii) The factorization into irreducibles is unique up to associates and the order in which the factors appear.

**Example 2.25.** The ring of integers $\mathbb{Z}$ is a UFD by the Fundamental Theorem of Arithmetic.

**Example 2.26.** The polynomial ring $\mathbb{Z}[x]$ is a UFD. A proof of the general case of this example is in section 2.6.

**Example 2.27.** The ring $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. We have already seen that in this domain, $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 + \sqrt{-5})$. But now, we must show that each of $2, 3, 1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$ and that $2$ is not an associate of $1 + \sqrt{-5}$ or $1 - \sqrt{-5}$. Suppose $2$ is not irreducible. Then $2 = xy$, $x, y \in \mathbb{Z}[\sqrt{-5}]$ and $x, y$ are not units. We must have $N(2) = N(xy) = N(x)N(y) = 4$. Since $x$ and $y$ are not units, $N(x) \neq 1$ and $N(y) \neq 1$. So $N(x) = 2$ and $N(y) = 2$. Now with $x = a + b\sqrt{-5}, N(x) = a^2 + 5b^2 = 2$ implying $b^2 = 0$ and $a^2 = 2$, which is a contradiction to $a \in \mathbb{Z}$. So $2$ is irreducible in $\mathbb{Z}[\sqrt{-5}]$. Using a similar argument, it is easy to see that $3$ is also irreducible. For if $N(3) = N(x)N(y) = 9$, then $a^2 + 5b^2 = 3$, so $a^2 = 3$, a contradiction. Now suppose $1 + \sqrt{-5}$ is not irreducible. Then $1 + \sqrt{-5} = xy$, and $x, y$ are not units. $N(1 + \sqrt{-5}) = 1^2 + 1^2 \cdot 5 = 6 = N(x)N(y)$. Without loss of generality we may assume that $N(x) = 2$ and $N(y) = 3$. This implies $a^2 + 5b^2 = 2$ or $a^2 + 5b^2 = 3$. This is not possible since $a^2$ and $b^2$ are non-negative integers. So we see that $1 + \sqrt{-5}$ is irreducible. The argument for $1 - \sqrt{-5}$ is analogous. Finally, if $2$ is an associate of $1 + \sqrt{-5}$, Then for some unit $u$, $2u = 1 + \sqrt{-5}$. This implies $N(1 + \sqrt{-5}) = 6 = N(2u) = 4$, which is
a contradiction. So 2 is not an associate of $1 + \sqrt{-5}$. The argument that 2 is not an associate of $1 - \sqrt{-5}$ is similar. This concludes the assertion that $\mathbb{Z} [\sqrt{-5}]$ is not a UFD.

**Example 2.28.** We will now exhibit an irreducible element in $\mathbb{Z} [\sqrt{-5}]$ that is not prime. We have already seen that 2 is irreducible and that $2 | (1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$. If $2 | (1 + \sqrt{-5})$, then there are integers $a$ and $b$ such that $2(a + b\sqrt{-5}) = (1 + \sqrt{-5})$. Thus $2a + 2b\sqrt{-5} = 1 + \sqrt{-5}$. So $2a = 1$ and $a = 1/2$, which we cannot have. The argument that $2 \nmid (1 - \sqrt{-5})$ is similar. Therefore, 2 is not prime.

### 2.4 The Ascending Chain Condition on Principal Ideals

In general, which integral domains are UFDs? The first part of the definition of a UFD requires that every nonzero element that is not a unit be written as a product of irreducibles. For example, suppose $a \in D$ is not zero or a unit. If $a$ is not irreducible, then $a = bc$ where $b$ is not zero or a unit and $c$ is not zero or a unit. If $b$ and $c$ are irreducible, then we are done. If either one is not irreducible, then we repeat this process with those elements. If this process is finite, then we will have a factorization into irreducibles (but it may not be unique). Therefore we need a way of saying that if this process stops, then we will have an irreducible factorization of $a$. The following definitions and theorems will help us to illustrate this.

**Definition 2.29.** A **principal ideal** $I$ is an ideal generated by one element, i.e. $I = (a) = \{ax | x \in D\}$, $a \in D$.

**Definition 2.30.** **Ascending chain condition on principal ideals:** Let $D$ be an integral domain. If every increasing sequence of principal ideals of $D$, $(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_i) \subseteq \cdots$ terminates, that is if there exists $n$ such that $i \geq n$ implies $(a_n) = (a_i)$, then we will say that $D$ satisfies the ascending chain condition (or ACC) on principal ideals.

**Theorem 2.31.** If a domain $D$ satisfies the ascending chain condition on principal ideals, then any element of $D$ may be factored into a product of irreducibles.

**Proof.** Suppose $D$ satisfies the ascending chain condition on principal ideals and $a \in D$ admits no factorization into a product of irreducible elements (and $a$ is nonzero or
a unit). As $a$ is not irreducible (otherwise the singleton $a$ would be its irreducible
factorization), it can be factored as $bc$ with neither $b$ nor $c$ a unit. Clearly not both $b$
and $c$ can have factorizations into irreducibles, or putting them together would result
in an irreducible factorization of $a$. Say $b$ admits no factorization into irreducibles. We
have $(a) = (bc) \subset (b)$ and since $a = bc$ and $c$ is not a unit, $b \notin (a)$. Setting $a_1 = a$
and $a_2 = b$ and repeating this argument inductively, we have a nonterminating, strictly
increasing sequence of principal ideals $(a_1) \subset (a_2) \subset \cdots$, violating the hypothesis. Thus
$a$ can be factored into a product of irreducibles. □

2.5 Principal Ideal Domains

One particular class of domains that are UFDs are principal ideal domains. In
this section, we will show that any principal ideal domain is a UFD.

**Definition 2.32.** A principal ideal domain (or PID) is an integral domain in which
every ideal is principal.

**Example 2.33.** $\mathbb{Z}$ is a PID: Let $I$ be an ideal of $\mathbb{Z}$. If $I = \{0\}$, then $I = (0)$. If $I \neq \{0\}$,
then by the Well Ordering Principle, there is a number $a \neq 0 \in I$ that is smallest in
absolute value. We will show that $I = (a)$. Since $a \in I$ and $I$ is an ideal, then $(a) \subseteq I$.
Now let $b \neq 0 \in I$. By the division algorithm for $\mathbb{Z}$, we may write $b = aq + r$, where
$|r| < |a|$. Since $a \in I$ is least in absolute value, we must have $r = 0$ and $b = aq$.
Therefore $I \subseteq (a)$ and $I = (a)$.

**Example 2.34.** $k[x]$, where $k$ is a field, is a PID: The justification that $k[x]$ is an integral
domain is analogous to that of example 2.11. Now, let $I$ be an ideal of $k[x]$. If $I = \{0\}$,
then $I = (0)$. If $I \neq \{0\}$, then among the elements of $I$, let $g(x)$ be one of minimal
degree. We will show that $I = g(x)$. Since $g(x) \in I$ and $I$ is an ideal, then $(g(x)) \subseteq I$.
Now let $f(x) \in I$. Then by the division algorithm, we may write $f(x) = g(x)q(x) + r(x)$,
where $r(x) = 0$ or the deg $r(x) \leq$ deg $g(x)$ (deg denotes the degree of a polynomial).
Since $r(x) = f(x) - g(x)q(x) \in I$, the minimality of deg $g(x)$ implies that deg $r(x) \neq$ deg
$g(x)$. So $r(x) = 0$ and $f(x) \in g(x)$. Therefore, $I \subseteq (g(x))$.

**Lemma 2.35.** Let $I_1 \subset I_2 \subset \cdots$ be a chain of strictly increasing ideals of a ring $R$ and
let $I = \cup I_i$. Then $I$ is an ideal.
Proof.  

i) $0 \in I_i$ for all $i$ so $0 \in I$ and $I$ is not empty.

ii) Let $a \in I$ and $r \in R$. Since $a \in I$, then $a \in I_j$ for some $j$. This implies $ar \in I_j$ so that $ar$ is in $I$.

iii) Let $a, b$ be in $I$. Then $a \in I_i$ for some $i$ and $b \in I_j$ for some $j$. Since the chain is strictly increasing, then we may assume that $j \geq i$ and therefore, $I_i \subset I_j$. Hence, $a - b \in I_j$, so $a - b \in I$.

By (i), (ii), and (iii), we conclude that $I$ is an ideal.

\[ \square \]

Theorem 2.36. Every PID satisfies the ascending chain condition

Proof. Let $(a_1) \subset (a_2) \subset \cdots$ be a chain of strictly increasing ideals of a PID $D$, and let $I$ be the union of all the ideals in this chain. By Lemma 2.35, $I$ is an ideal. Since $D$ is a PID, $(a) = I$ for some $a \in D$. Because $a \in I$ and $I = \cup (a_n)$, $a$ belongs to some ideal in the chain, say $a \in (a_k)$. Since $a$ is the generator of $I$, we have $(a_i) \subset I = (a) \subset (a_k)$ for $i \geq k$. Hence the chain stops at $(a_k)$.

It follows directly from Theorems 2.31 and 2.36 that any element of a PID that is not zero or a unit can be factored into a product of irreducibles. But are these factorization unique? We will now address this question.

Theorem 2.37. Let $D$ be a domain in which every $a \in D$ that is not zero or a unit is a product of irreducibles. Then $D$ is a UFD if and only if irreducible elements of $D$ are prime (in the language of ideals, the ideal $(p)$ is prime for every irreducible $p$).

Proof. Assume $D$ is a UFD and let $p$ be irreducible in $D$. Let $a, b \in D$ and $p \mid ab$. Then there exists $r \in D$ such that $ab = pr$. We now factor $a, b$ and $r$ into their irreducible components. By unique factorization in $D$, the left side of the equation must involve an associate of $p$, say $q$. Now $q$ arose as a factor of $a$ or $b$, implying that $q \mid a$ or $q \mid b$. Thus $p \mid a$ or $p \mid b$. So $p$ is prime.

The proof of the converse in merely an adaptation of the Fundamental Theorem of Arithmetic. Let us assume that $p_1 \cdots p_n = q_1 \cdots q_m$ where $p_i$ and $q_i$ are irreducible. We prove by induction on $\max\{n, m\} \geq 1$ that $n = m$ and the $q$'s can be reindexed so that $q_i$ and $p_i$ are associates. For the base step, $\max\{n, m\} = 1$ has $p_1 = q_1$ and the result is obviously true. For the inductive step, Let $p_1 \cdots p_n = q_1 \cdots q_m$. By hypothesis
that \( p_1 \) is prime, \( p_1 \mid q_j \) for some \( j \). So \( p_1 u = q_j \) for some unit \( u \in D \) since \( q_j \) is irreducible. Canceling \( p_1 \) from both sides, we get \( p_2 \cdots p_n = uq_1 \cdots q_m \). By our hypothesis, \( m - 1 = n - 1 \), so \( m = n \), and after reindexing, \( q_i \) and \( p_i \) are associates for all \( i \).

\textit{Theorem 2.38.} In a PID, an element is irreducible if and only if it is prime.

\textit{Proof.} We have already seen in Theorem 2.22 that in an integral domain, any prime element is irreducible. For the converse, Let \( a \in D \), where \( D \) is a PID and \( a \) irreducible. Suppose \( a \mid bc \), \( b, c \in D \). We need to show that \( a \mid b \) or \( a \mid c \). Consider the ideal \( I = \{ ax + by \mid x, y \in D \} \). Now \( I \) is principal, so we may write \( I = (d) \) for some \( d \in D \). Clearly, \( a \in I \) so that \( a = dr \) for some \( r \in D \). Because \( a \) is irreducible, \( d \) is a unit or \( r \) is a unit. If \( d \) is a unit, then \( I = D \) and we may write \( 1 = ax + by \). Thus \( c = acx + bcy \). Now, \( a \mid acx \) and since \( a \mid bc \), \( a \mid bcy \). So \( a \mid acx + bcy = c(ax + by) \) and \( a \mid c \). If \( r \) is a unit, then \( a \) and \( d \) are associates and \( (a) = (d) = I \). Because \( b \in I \), \( b = as \) for some \( s \in D \). Thus \( a \mid b \).

\textit{Theorem 2.39.} Every PID is a UFD.

\textit{Proof.} This follows immediately from Theorems 2.37 and 2.38.

In the next section, we will see that the converse of Theorem 2.39 is false, that is not every UFD is a PID. In chapter 3, we will establish a necessary and sufficient for a UFD to be a PID.

\subsection*{2.6 Unique Factorization in \( D[x] \)}

The goal of this section is to show that for any UFD \( D \), the polynomial ring \( D[x] \) is a UFD. Before we can do this, we will need to define the \textit{content} of a polynomial and a \textit{primitive} polynomial. We will also need to know some properties of divisibility in integral domains.

\textit{Definition 2.40.} An element \( d \) of a ring \( R \) is a \textit{greatest common divisor} (or \textit{gcd} for short) of elements \( a, b \in R \) if

\begin{itemize}
  \item[i)] \( d \) is a common divisor of \( a \) and \( b \);
\end{itemize}
ii) if $\tilde{d}$ is a common divisor of $a$ and $b$, then $\tilde{d}|d$.

**Lemma 2.41.** If $R$ is a UFD, then the gcd of any finite set of elements $a_1, \cdots, a_n$ in $R$ exists.

**Proof.** It is sufficient to show that the gcd of any two elements exists; the general follows by induction on the number of elements. Because $R$ is a UFD, there are units $u$, $v$ and irreducibles $p_1, p_2 \cdots p_t$ in $D$ such that $a = up_1^{e_1}p_2^{e_2} \cdots p_t^{e_t}$ and $b = vp_1^{f_1}p_2^{f_2} \cdots p_t^{f_t}$ where $e_i \geq 0$ and $f_i \geq 0$ for all $i$. It is easy to see that if $c | a$, then $c = wp_1^{g_1}p_2^{g_2} \cdots p_t^{g_t}$ where $w$ is a unit and $0 \leq g_i \leq e_i$ for all $i$. And thus $c$ is a common divisor of $a$ and $b$ if and only if $g_i \leq m_i$ for all $i$ with $m_i = \min\{e_i, f_i\}$. It is also clear that $d = p_1^{m_1}p_2^{m_2} \cdots p_t^{m_t}$ is a gcd of $a$ and $b$. □

**Definition 2.42.** If $D$ is a UFD, and $f(x) = a_0 + a_1x^1 + \cdots + a_nx^n \in D[x]$ we define the **content** or $f(x)$, denoted $c(f)$, to be the greatest common divisor (or gcd) of $a_0, \cdots, a_n$.

**Definition 2.43.** Elements $a_1, a_2, \cdots, a_n$ of a UFD $D$ are **relatively prime** if their gcd is a unit, that is every common divisor of $a_1, a_2, \cdots, a_n$ is a unit.

**Definition 2.44.** A polynomial $f(x) = a_0 + a_1x^1 + \cdots + a_nx^n \in D[x]$ where $D$ is a UFD is called **primitive** if its coefficients are relatively prime.

**Lemma 2.45.** (Gauss) If $D$ is a UFD and $f(x), g(x) \in D[x]$ are primitive, then their product $f(x)g(x)$ is also primitive.

**Proof.** Let $\pi: D \rightarrow D/(p)$ be the natural map $\pi: a \mapsto a + (p)$ where $p$ is irreducible and let $\tilde{\pi}: D[x] \rightarrow (D/(p))[x]$ be the function which replaces the coefficients $c$ of a polynomial by $\pi(c)$. A routine calculation will show that $\tilde{\pi}$ is a ring homomorphism. Suppose a polynomial $h(x) \in D[x]$ is not primitive. Then there is some nonzero, nonunit element $d \in D$ that divides all the coefficients of $h$. Since $D$ is a UFD, $d$ has some irreducible factor, say $p$. It follows that all the coefficients of $\tilde{\pi}(h)$ are zero in $D/(p)$, that is $\tilde{\pi}(h) = 0$ in $(D/(p))[x]$. Thus if a product $f(x)g(x)$ is not primitive, then there is some irreducible $p$ with $0 = \tilde{\pi}(fg) = \tilde{\pi}(f)\tilde{\pi}(g)$ in $(D/(p))[x]$. Since $(p)$ is a prime ideal, then $D/(p)$ is a domain by the Lemma 2.12, and thus $(D/(p))[x]$ is also a domain. But neither $\tilde{\pi}(f)$ nor $\tilde{\pi}(g)$ is zero in $(D/(p))[x]$ because $f$ and $g$ are primitive and this contradicts $(D/(p))[x]$ being a domain. □
Lemma 2.46. Let $D$ be a UFD and let $Q = \text{Frac}(D)$ be its fractional field. Then $a/b \in Q$ has an expression in lowest terms.

Proof. We wish to show that there are elements $\tilde{a}, \tilde{b} \in D$ such that $a/b = \tilde{a}/\tilde{b}$ in $Q$ and the gcd of $\tilde{a}$ and $\tilde{b}$ is a unit. Because $D$ is a UFD, there are units $u, v$ and irreducibles $p_1, p_2, \ldots, p_t$ in $D$ such that $a = u p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ and $b = v p_1^{f_1} p_2^{f_2} \cdots p_t^{f_t}$ where $e_i \geq 0$ and $f_i \geq 0$ for all $i$. It is easy to see that if $c \mid a$, then $c = u p_1^{g_1} p_2^{g_2} \cdots p_t^{g_t}$ where $u$ is a unit and $0 \leq g_i \leq e_i$ for all $i$. And thus $c$ is a common divisor of $a$ and $b$ if and only if $g_i \leq m_i$ for all $i$ with $m_i = \min\{e_i, f_i\}$. It is also clear that $d = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$ is a gcd of $a$ and $b$.

Now let $a/d = \tilde{a}$ and $b/d = \tilde{b}$; $a/b = \tilde{a}/\tilde{b}$. To see that $a$ and $b$ are relatively prime, suppose $\tilde{c} \mid \tilde{a}$ and $\tilde{c} \mid \tilde{b}$, where $\tilde{c}$ is not a unit or zero. Then $\tilde{c} \mid a/d$ and $\tilde{c} \mid b/d$ and there are nonzero elements $x, y \in D$ with $\tilde{c}x = a/d$ and $\tilde{c}y = a/d$. Hence $\tilde{c}xd = a$ and $\tilde{c}yd = b$. So have $\tilde{c}d$ as a common divisor of $a$ and $b$ which contradicts $d$ being a gcd.

Lemma 2.47. Let $D$ be a UFD. If $a, b, c \in D$ with $a$ and $b$ relatively prime, then $a \mid bc$ implies that $a \mid c$.

Proof. Let $a = u p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ and $b = v p_1^{f_1} p_2^{f_2} \cdots p_t^{f_t}$ be the factorization of $a$ and $b$ into irreducibles, with $a$ and $b$ relatively prime. This implies that possibly after renumbering, we may write $b = v p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ and $a = u p_{n+1}^{e_{n+1}} p_{n+2}^{e_{n+2}} \cdots p_t^{e_t}$. Let $c = w q_1^{d_1} q_2^{d_2} \cdots q_m^{d_m}$, where the $w$ is a unit, be the factorization of $c$ into a product of irreducibles. Now,

$$bc = vw p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} q_1^{d_1} q_2^{d_2} \cdots q_m^{d_m}$$

and since $a$ is a divisor of $bc$, then

$$a = vw p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n} q_1^{g_1} q_2^{g_2} \cdots q_m^{g_m}$$

with $0 \leq f_i \leq e_i$ and $0 \leq g_i \leq d_i$. However $a$ and $b$ are relatively prime so that $f_i = 0$ for all $i$ and $a = vw q_1^{f_1} q_2^{f_2} \cdots q_m^{f_m}$. It follows that $a \mid c$.

Lemma 2.48. If $D$ is a UFD, then every irreducible $p(x) \in D[x]$ is primitive.

Proof. Suppose $p(x)$ is irreducible but not primitive. If $\deg(p) = 0$, then it is primitive. So assume $\deg(p) > 0$. Since $p(x)$ is not primitive, there is an irreducible $q \in D$ with $p(x) = qg(x)$; and $\deg(q) = 0$. Since $p(x)$ is irreducible, its only factors are units and
associates, so \( q \) must be an associate of \( p(x) \). Hence \( \deg(g) = \deg(p) \) and since \( p(x) \) and \( q \) are associates, then \( g(x) \) is a unit. But the only units of \( D[x] \) have degree 0. Therefore, \( \deg(g) = 0 \), a contradiction. We conclude that \( p(x) \) is primitive. \( \square \)

**Proposition 2.49.** Let \( D \) be a UFD and \( Q = \text{Frac}(D) \).

i) If \( f(x) \in D[x] \) is nonzero, then there is a factorization \( f(x) = c(f)f^*(x) \) where \( c(f) \in D \) is the content of \( f(x) \) and \( f^*(x) \in D[x] \) is primitive. This factorization is said to be unique in the sense that if \( f(x) = dg^*(x) \), where \( d \in D \) is nonzero and \( g^*(x) \in D[x] \), then \( c(f) \) and \( d \) are associates in \( D \) and \( f^*(x) \) and \( g^*(x) \) are associates in \( D[x] \).

ii) If \( f(x), g(x) \in D[x] \), then \( c(fg) \) and \( c(f)c(g) \) are associates and \( (fg)^* \) and \( f^*g^* \) are associates.

iii) Let \( g^*(x), f^*(x) \in D[x] \). If \( g^*(x) \) is primitive and \( g^*(x) \mid bf(x) \), where \( b \in D \) and \( b \neq 0 \), then \( g^*(x) \mid f(x) \).

**Proof.** (i) If \( f(x) \in Q[x] \), then \( f^*(x) = f(x)/c(f) \) is primitive since \( c(f) \) is a gcd of all the coefficients of \( f(x) \).

To prove uniqueness, suppose that \( f(x) \in D[x] \) and \( c(f)f^*(x) = dg^*(x) \) with \( d \in D \) and \( g^*(x) \in D[x] \) primitive. Then Lemma 2.46 allows us to write \( d/c(f) \) in lowest terms; \( d/c(f) = u/v \) where \( u \) and \( v \) are relatively prime elements of \( D \). The equation \( uf^*(x) = vg^*(x) \) holds in \( D[x] \). Equating like coefficients, \( v \) is a common divisor of each of the coefficients of \( vg^*(x) \). Since \( u \) and \( v \) are relatively prime, Lemma 2.47 gives \( v \) as a common divisor of the coefficients of \( g^*(x) \). But \( g^*(x) \) is primitive so that \( v \) is a unit. A similar argument shows that \( u \) is a unit. Therefore \( c(f) = u/v \) is a unit in \( D \), call it \( w \), and \( d = wc(f) \); that is \( d \) and \( c(f) \) are associates and \( g^*(x) = u/vf^*(x) \) so that \( f^*(x) \) and \( g^*(x) \) are associates.

(ii) There are two factorizations of \( f(x)g(x) \) in \( D[x] \):

\[
 f(x)g(x) = c(fg)(f(x)g(x))^*
\]

and

\[
 f(x)g(x) = c(f)f^*(x)c(g)^*(x) = c(f)c(g)f^*(x)g^*(x).
\]
Since the product of two primitive polynomials is primitive (Lemma 2.45), each of these is a factorization as in part (i), and the uniqueness assertion gives $c(fg)$ an associate of $c(f)c(g)$ and $(fg)^*$ an associate of $f^*g^*$.

(iii) Since $bf = hg^*$, we have $bc(f)f^* = c(h)h^*g^* = c(h)(hg)^*$. By uniqueness (part(i), $f^*$ and $(hg)^*$ are associates, and so $g^* | f^*$. But $f = c(f)f^*$ and so $g^* | f$. □

**Theorem 2.50.** (Gauss) If $D$ is a UFD, then $D[x]$ is also a UFD.

**Proof.** We show first by induction on the degree of $f(x)$, denoted $\deg(f)$ that every $f(x) \in D[x]$ that is neither zero nor a unit is a product of irreducibles. If $\deg(f) = 0$, then $f(x)$ is a constant and lies in $D$ and we are done. If $\deg(f) > 0$, then $f(x) = c(f)f^*(x)$ where $c(f) \in D$ and $f^*(x)$ is primitive by Proposition 2.49i. Now, $c(f)$ is either a unit or a product of irreducibles by the base step. If $f^*(x)$ is irreducible then we are done. Otherwise, $f^*(x) = g(x)h(x)$ where neither $g$ nor $h$ is a unit. Since $f^*(x)$ is primitive, then neither $g$ nor $h$ is a constant. Therefore, each has degree less than $\deg(f^*) = \deg(f)$ and so each is product of irreducibles.

To prove uniqueness, we now apply Theorem 2.37: that is $D[x]$ is a UFD if $(p(x))$ is a prime ideal for every irreducible $p(x) \in D[x]$; that is if $p \mid fg$, then $p \mid f$ or $p \mid g$. Let us assume that $p \nmid f$.

Case(i): Suppose $\deg(p) = 0$. Write $f(x) = c(f)f^*(x)$ and $g(x) = c(g)g^*(x)$ where $c(f), c(g) \in D$ and $f^*(x), g^*(x)$ are primitive. Proposition 2.49ii says that $c(f)c(g)$ is an associate of $c(fg)$. However, if $p \mid f(x)g(x)$, then $p$ divides each of the coefficients of $fg$; that is $p$ is a common divisor of all of the coefficients of $fg$ and hence $p \mid c(fg) = c(f)c(g)$ in $D$ which is a UFD. But Theorem 2.37 says that $(p)$ is a prime ideal in $D$ and so $p \mid c(f)$ or $p \mid c(g)$. If $p \mid c(f)$ then $c \mid c(f)f^*(x) = f(x)$, a contradiction. Therefore, $p \mid c(g)$ and thus $p \mid g(x)$ as desired.

Case(ii) Suppose $\deg(p) \geq 0$. Let $(p, f) = \{s(x)p(x) + t(x)f(x) : s(x), t(x) \in D[x]\}$. Of course, $(p, f)$ is an ideal containing $p(x)$ and $f(x)$. Choose $m(x)$ in $(p, f)$ of minimal degree. If $Q = \text{Frac}(D)$ is the fraction field of of $D$, then the division algorithm in $Q[x]$ gives the polynomial $\bar{q}(x), \bar{r}(x) \in Q[x]$ with $f(x) = m(x)\bar{q}(x) + \bar{r}(x)$ where either $\bar{r}(x) = 0$ or $\deg(\bar{r}) \leq \deg(m)$. Clearing the denominators, there are polynomials $q(x), r(x) \in D[x]$ and a constant $b \in D$ with $bf(x) = q(x)m(x) + r(x)$, where $r(x) = 0$
or \( \deg(r) \leq \deg(m) \). Since \( m \in (p, f) \), there are polynomials \( s(x), t(x) \in D[x] \) with 
\[
m(x) = s(x)p(x) + t(x)f(x);
\]

hence \( r = bf - qm \in (p, f) \). Since \( m \) has minimal degree in \((p, f)\), we must have \( r = 0 \); that is \( bf(x) = m(x)q(x) \) so \( bf(x) = c(m)m^*(x)q(x) \). But \( m^*(x) \) is primitive and \( m^*(x) \mid bf(x) \), so \( m^*(x) \mid f(x) \) by Proposition 2.49iii. A similar argument, replacing \( f(x) \) by \( p(x) \) gives \( m^*(x) \mid p(x) \). Since \( p(x) \) is irreducible, its only factors are units and associates. If \( m^*(x) \) were an associate of \( p(x) \), then \( p(x) \mid f(x) \) (because \( p(x) \mid m^*(x) \mid f(x) \)), contrary to the hypothesis. Hence \( m^*(x) \) must be a unit; that is \( m(x) = c(m) \in D \), and so \((p, f)\) contains the nonzero constant \( c(m) \). Now 
\[
c(m) = sp + tf
\]
and so
\[
c(m)g(x) = s(x)p(x)g(x) + t(x)f(x)g(x).
\]

Since \( p(x) \mid f(x)g(x) \), we have \( p(x) \mid c(m)g(x) \). But \( p(x) \) is primitive because it is irreducible by Lemma 2.48 and so by Lemma 2.49iii, \( p(x) \mid g(x) \).

**Corollary 2.51.** If \( D \) is a UFD, then \( D[x_1, \ldots, x_n] \) is also a UFD.

**Proof.** The proof is by induction on \( n \geq 1 \). For the base step, \( D[x_1] \) is a UFD by the previous theorem. For the inductive step, \( D[x_1, \ldots, x_n] = R[x_{n+1}] \), where \( R = R[x_1, \ldots, x_n] \). By induction, \( R \) is a UFD, and by the previous theorem so is \( R[x_{n+1}] \).

**Example 2.52.** We will now show that the converse of Theorem 2.39 is false; that is not every UFD is a PID. The polynomial ring \( \mathbb{Z}[x] \) is a UFD, but the set \( I \) of polynomials with even constants is an ideal that is not principal: For \( 0 \) is even, so \( 0 \in I \). If \( f(x), g(x) \in I \), then \( f(x) - g(x) \in I \), since the sum or difference of any two even integers is even, hence the difference of their constant terms is even. Finally for any \( f(x) \in I \) and \( g(x) \in \mathbb{Z}[x] \), the constant term of \( fg \) is also even because the product of an even integer with any other integer is even. So \( I \) is an ideal. To see that \( I \) is not principal, suppose \( I = (d(x)) \) for some \( d(x) \in \mathbb{Z}[x] \). The constant 2 \in I so that there is \( f(x) \in \mathbb{Z}[x] \) with \( 2 = f(x)d(x) \). So \( \deg(2) = \deg(f(x)) + \deg(d(x)) \), so that \( \deg(d(x)) = 0 \) and \( d(x) \) is a constant. The only candidates for \( d(x) \) are \( \pm 2 \). Now, \( x \in I \) so we must have \( x = \pm 2h(x) \) for some \( h(x) \in \mathbb{Z}[x] \), which is not possible. Hence, there is no such \( d(x) \) and \( I \) is not principal.
2.7 Unique Factorization in $\mathbb{Z}[\sqrt{d}]$

In this section, we will show that for any $d \in \mathbb{Z}, d < 0$, the domain $\mathbb{Z}[\sqrt{d}]$ is a UFD if and only if $d = -1$ or $d = -2$. But first, we will introduce another class of domains that are UFDs, called euclidean domains.

Definition 2.53. An integral domain $D$ is a euclidean domain (or ED) if there is a function $d$ (called the measure) from the nonzero elements of $D$ to the nonnegative integers such that

i) $d(a) \leq d(ab)$ for all nonzero $a, b \in D$, and

ii) if $a, b \in D$, $b \neq 0$, then there exists elements $q, r \in D$ such that $a = bq + r$, where $r = 0$ or $d(r) < d(b)$.

Example 2.54. The ring $\mathbb{Z}[i] = \{a + bi \mid a, d \in \mathbb{Z}\}$ is a ED: We let $d(a + bi) = a^2 + b^2 = N(a + bi)$. First, we need to show $d(x) < d(xy)$ for all $x, y \in \mathbb{Z}[i]$. Let $x = a + bi$ and $y = \bar{a} + \bar{b}i$. Now $d(xy) = d(x)d(y) \geq d(x)$ since $d(x)$ and $d(y)$ are non-negative integers. Secondly, if $x, y \in \mathbb{Z}[i]$ and $y \neq 0$, then $xy^{-1} \in \mathbb{Q}[i]$, the field of fractions of $\mathbb{Z}[i]$. Say $xy^{-1} = s + ti, s, t \in \mathbb{Q}$. Let $m$ be the integer nearest $s$ and $n$ be the integer nearest $t$. These may not be uniquely determined, but that is irrelevant, as we will see. So $|m - s| \leq 1/2$ and $|n - t| \leq 1/2$. Then

$$xy^{-1} = s + ti$$

$$= (m - m + s) + (n - n + t)i$$

$$= (m - ni) + (s - m) + (t - n)i.$$

We have $x = (m + ni)y + [(s - m) + (t - ni)]y$. We claim that the division condition is satisfied with $q = m + ni$ and $r = [(s - m) + (t - n)i]y$. Clearly, $q \in \mathbb{Z}[i]$ since $m, n \in \mathbb{Z}$. Since $r = x - qy, x, y \in \mathbb{Z}[i]$, so $r \in \mathbb{Z}[i]$.

Finally,

$$d(r) = d[(s - m) + (t - n)i]d(y)$$

$$= [(s - m)^2 + (t - n)^2]d(y)$$

$$\leq (1/4 + 1/4)d(y) < d(y).$$

It follows that $\mathbb{Z}[i]$ is a ED.
Example 2.55. The ring \( \mathbb{Z} [\sqrt{-2}] = \{ a + b \sqrt{-2} \mid a, d \in \mathbb{Z} \} \) is an ED: We let \( d(a + b \sqrt{-2}) = a^2 + 2b^2 = N(a + b \sqrt{-2}) \). First, we need to show \( d(x) < d(xy) \) for all \( x, y \in \mathbb{Z}[\sqrt{-2}] \).

Let \( x = a + b \sqrt{-2} \) and \( y = \bar{a} + \bar{b} \sqrt{-2} \). Now \( d(xy) = d(x)d(y) \geq d(x) \) since \( d(x) \) and \( d(y) \) are non-negative integers. If \( x, y \in \mathbb{Z}[\sqrt{-2}] \) and \( y \neq 0 \), then \( xy^{-1} \in \mathbb{Q}[\sqrt{-2}] \), the field of fractions of \( \mathbb{Z}[\sqrt{-2}] \). Say \( xy^{-1} = s + t \sqrt{-2} \), \( s, t \in \mathbb{Q} \). Let \( m \) be the integer nearest \( s \) and \( n \) be the integer nearest \( t \). These may not be uniquely determined, but that is irrelevant, as we will see. So \( | m - s | \leq 1/2 \) and \( | n - t | \leq 1/2 \). Then

\[
xy^{-1} = s + t \sqrt{-2}
\]

\[
= (m - m + s) + (n - n + t) \sqrt{-2}
\]

\[
= (m - n \sqrt{-2}) + (s - m) + (t - n) \sqrt{-2}.
\]

So

\[
x = (m + n \sqrt{-2}) y + [(s - m) + (t - n) \sqrt{-2}] y.
\]

We claim that the division condition is satisfied with \( q = m + n \sqrt{-2} \) and

\[
r = [(s - m) + (t - n) \sqrt{-2}] y
\]

Clearly, \( q \in \mathbb{Z}[\sqrt{-2}] \) since \( m, n \in \mathbb{Z} \). Since \( r = x - qy \), with \( x, q, y \in \mathbb{Z}[\sqrt{-2}] \), so that \( r \in \mathbb{Z}[\sqrt{-2}] \).

Finally,

\[
d(r) = d((s - m) + (t - n) \sqrt{-2}) d(y)
\]

\[
= [(s - m)^2 + 2(t - n)^2] d(y)
\]

\[
\leq (1/4 + 2/4) d(y) < d(y).
\]

We conclude that \( \mathbb{Z}[\sqrt{-2}] \) is an ED.

Theorem 2.56. Every ED is a PID.

Proof. Let \( D \) be an ED and \( I \) a nonzero ideal of \( D \). Let \( a \neq 0 \in I \) such that \( d(a) \) is minimum (by the well-ordering principle). We will show that \( I = (a) \). If \( b \in I \), then there are elements \( q, r \in D \) such that \( b = aq + r \) and \( r = 0 \) or \( d(r) < d(a) \). But \( r = b - aq \in I \), so that \( d(r) \) cannot be less than \( d(a) \). So \( r \) must be zero and \( b = aq \). Thus \( b \in (a) \), as desired and every ideal is principal. \( \square \)
It follows immediately from Theorems 2.56 and 2.39 that \( \mathbb{Z}[i] \) and \( \mathbb{Z}[\sqrt{-2}] \) are UFDs. However, the converse of Theorem 41 is false, although this is not easy to verify. The first example of a PID that is not a ED was given by T. Motzkin in 1949 [5]. Motzkin showed that

\[ D = \{ a + ba : a, b \in \mathbb{Z} \} \]

where \( a = \frac{1}{2}(1 + \sqrt{-19}) \) is a PID, but not a ED.

Notice that if we apply the same argument to \( \mathbb{Z}[\sqrt{-3}] \), with \( d(a + b\sqrt{-3}) = a^2 + 3b^2 \), as we did to \( \mathbb{Z}[\sqrt{-2}] \), then the argument seems to be the same if we simply replace \( \sqrt{-2} \) with \( \sqrt{-3} \). However, the last part of the equation then becomes

\[ d(r) = [(s - m)^2 + 3(t - n)^2]d(y) \]

which is

\[ \leq (1/4 + 3/4)d(y) = d(y). \]

So we lose the inequality at the end. But this is to be expected. As we will see, \( \mathbb{Z}[\sqrt{-3}] \) is not a UFD so it cannot be a ED.

**Lemma 2.57.** If \( \mathbb{Z}[\sqrt{d}] \) is a UFD, then 2 is not irreducible in \( \mathbb{Z}[\sqrt{d}] \).

**Proof.** Assume \( \mathbb{Z}[\sqrt{d}] \) is a UFD. So \( d \) or \( d-1 \) is an integer multiple of 2, hence \( 2 | d(d-1) \).

Now \( (d + \sqrt{d})(d - \sqrt{d}) = d^2 - d = d(d-1) \) So \( 2 | (d + \sqrt{d})(d - \sqrt{d}) \). If \( 2 | d + \sqrt{d} \), then there is some \( x = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}] \) such that

\[ 2x = d + \sqrt{d} = 2(a + b\sqrt{d}) = 2a + 2b\sqrt{d} \]

This implies \( 2b = 1 \), hence \( b = 1/2 \), which is a contradiction to \( b \in \mathbb{Z} \). So \( 2 \nmid d + \sqrt{d} \).

Similarly, \( 2 \nmid d - \sqrt{d} \). Hence 2 is not a prime. Since prime and irreducible are equivalent in a UFD, 2 is not irreducible. \( \square \)

**Theorem 2.58.** If \( d < 0 \), then \( \mathbb{Z}[\sqrt{d}] \) is a UFD if and only if \( d = -1 \) or \( d = -2 \).

**Proof.** We will show that if \( d \leq -3 \), then 2 is irreducible in \( \mathbb{Z}[\sqrt{d}] \), and then use the previous lemma. We have already seen that \( \mathbb{Z}[i] \) and \( \mathbb{Z}[\sqrt{-2}] \) are UFD’s. We will now consider \( d \leq -3 \). Suppose 2 is not irreducible in \( \mathbb{Z}[\sqrt{d}] \). Then there exists \( x, y \in \mathbb{Z}[\sqrt{d}] \) such that \( 2 = xy \), and \( x \) is not a unit and \( y \) is not a unit. So \( N(x) > 1 \), \( N(y) > 1 \)
and \( N(2) = 4 = N(xy) = N(x)N(y) \). This implies \( N(x) = 2 \) and \( N(y) = 2 \). Now \( x = a + b\sqrt{d} \) for some \( a, b \in \mathbb{Z} \). So \( N(x) = a^2 + db^2 = 2 \). If \( d \leq -3 \), and \( b \neq 0 \) then \( a^2 + db^2 \geq 0 + 3.1 > 2 \). If \( b = 0 \), then \( a^2 = 2 \) which we cannot have since \( a \) is an integer. Thus we conclude that \( 2 \) is irreducible and \( \mathbb{Z}[\sqrt{d}] \) is not a UFD by Lemma 2.57. \( \square \)
Chapter 3

PRIMARY DECOMPOSITION OF IDEALS IN A RING

In the previous chapter, we looked at the factorization of an element into a product of other irreducibles elements. In this chapter, we will look at the decomposition of an ideal into an intersection of primary ideals. Primary decomposition is a generalization of unique factorization. Dedekind was one of those who sought conditions under which a ring has unique factorization of an ideal into prime ideals. He made his findings available in a famous supplement to later editions (after 1871) to Dirichlet’s book on Number Theory. However, it is not always possible to factorize ideals multiplicatively, so Lasker, in [1905] showed how to generalize unique factorization into primary decomposition. Both Dedekind and Lasker’s theories were thoroughly reformulated and axiomatized by Emmy Noether in the 1920’s using the ascending chain condition. One of the main results of this chapter is to show that in a Noetherian ring, every ideal has a primary decomposition [2].

3.1 Prime and Primary Ideals

In chapter 2, we defined a prime and a primary ideal. In his study of unique factorization, Dedekind was the first to introduce the notion of an ideal of a ring. His idea was to represent an element \( r \) of a ring \( R \) by the ideal \( (r) \) of its multiples. Arbitrary ideals would then be regarded as ideal elements. The ideal \( (r) \) determines the element
If only up to multiples by units u of R. Since prime factorization is unique only up to unit multiples, it turns out that this is just the right generalization [2]. Instead of looking at elements as products of other elements, we will be looking at ideals as intersections of other ideals. For example, in \( \mathbb{Z} \), \( 12 = 2^2 \cdot 3 \) and so \( (12) = (2^2) \cap (3) \). Indeed, it is clear that \( (12) \subseteq (2^2) \cap (3) \). Since \( 2^2 \) and 3 are relatively prime, \( 1 = 2^2m + 3n \), \( m, n \in \mathbb{Z} \). If \( x \in (2^2) \cap (3) \), then \( x = 2^2a \) and \( x = 3b \) for some \( a, b \in \mathbb{Z} \). Now \( x = 2^2mx + 3nx = 2^2m \cdot 3b + 3n2^2a = 2^2 \cdot 3(mb + na) = 12(mb + na) \in (12) \).

**Example 3.1.** In \( \mathbb{Z} \), the only primary ideals are \( (0) \) and \( (p^n) \) where \( p \) is prime: It can be easily verified that \( (0) \) and \( (p^n) \) are primary. If \( I \) is an ideal of \( \mathbb{Z} \), then \( I = (a) \) for some \( a \in \mathbb{Z} \) since \( \mathbb{Z} \) is a PID. If \( a \neq p^n \), then the prime factorization of \( a \) is \( a = up_1p_2 \cdots p_n \) with some \( i, j \) such that \( p_i \neq p_j \). Without loss of generality, assume \( p_1 \neq p_n \). Now \( a = up_1p_2 \cdots p_n \in (a) \) but \( up_1p_2 \cdots p_{n-1} \notin (a) \). If \( p_n^m \not\in (a) \) for some positive integer \( m \), then \( p_n^m = ab \) for some \( b \neq 0 \in R \) This implies that \( a \) is some power of \( p_n \), which contradicts our hypothesis. Thus \( (a) = I \) is not primary.

A primary ideal in some sense generalizes a prime number while a primary ideal is the corresponding generalization of the power of a prime. From the previous example, we see that in \( \mathbb{Z} \), the only primary ideals are \( (0) \) and \( (p^n) \) where \( p \) is prime. But this is misleading because generally, primary ideals are not that easy to identify. In fact, we will see in examples 3.20 and 3.21 show that there are primary ideals that are not powers of prime ideals and there are also powers of prime ideals that are not primary ideals. In this section, we will introduce another type of prime ideal called a maximal ideal along with some concepts that will help us to determine when an ideal is primary.

**Definition 3.2.** An ideal \( M \) of a ring \( R \) is **maximal** if \( M \neq R \) and if there is an ideal \( I \subseteq R \) such that \( M \subset I \), then \( I = R \).

**Proposition 3.3.** An ideal \( I \) of a ring \( R \) is maximal if and only if \( R/I \) is a field.

**Proof.** Here, we apply the Correspondence Theorem for Rings, Now \( R/I \) is a field if and only if \( R/I \) has no ideals other than \( \{0\} \) and \( R/I \) itself [5]. We will now show that these are the only ideals of \( R/I \). If \( I \) is maximal, then \( R/I \) has only one proper ideal \( I/I \). And conversely, if the only proper ideal of \( R/I \) is \( I/I \), then \( I \) is maximal because there are no intermediate ideal of \( R \) containing \( I \) other than \( I \) and \( R \) itself. Since these are the only ideals of \( R/I \), then \( R/I \) is a field. \( \square \)
Corollary 3.4. Let $M$ be a maximal ideal in a ring $R$. Then $M$ is a prime ideal.

Proof. By Proposition 3.3, $R/I$ is a field. Since every field is a domain, $M$ is prime by Lemma 2.12.

Proposition 3.5. Every ring $R \neq 0$ has at least one maximal ideal.

Proof. Let $\Sigma$ be the set of all proper ideals of $R$. We will use Zorn’s Lemma to show that $\Sigma$ has a maximal element. First, we order $\Sigma$ by inclusion. $\Sigma$ is not empty since $0 \in \Sigma$. Now we will use Zorn’s Lemma to show that every chain in $\Sigma$ has an upper bound in $\Sigma$. Let $(I_\alpha)$ be a chain of ideals in $\Sigma$ so that for each pair of indices $\alpha, \beta$ we have either $I_\alpha \subseteq I_\beta$ or $I_\beta \subseteq I_\alpha$. Let $I = \bigcup \alpha I_\alpha$. By Lemma 2.35, $I$ is an ideal. $I \neq R$ since $1 \notin I_\alpha$ for all $\alpha$. So $I \in \Sigma$ is an upper bound for the chain. Hence $\Sigma$ has a maximal element.

Corollary 3.6. If $I \neq R$ is an ideal of $R$, then there is a maximal ideal of $R$ containing $I$.

Proof. By Proposition 3.5, the quotient ring $R/I$ has a maximal ideal. By the Correspondence Theorem for Rings, this maximal ideal is of the form $M/I$, where $M$ is a maximal ideal containing $I$.

Corollary 3.7. Let $R$ be a ring and $a \in I$, where $I$ is an ideal of $R$. If $a$ is not a unit, then $a \in M$ for some maximal ideal $M$ in $R$.

Proof. The ideal $(a)$ is contained in some maximal ideal $M$ (Corollary 3.6) so that $a \in M$.

Definition 3.8. Let $I$ be an ideal of $R$. Then the radical of $I$, denoted $r(I)$ is the set \[ \{ x \in R : x^n \in I \} \].

Proposition 3.9. The radical $r(I)$ of an ideal $I$ is an ideal.

Proof. Let $a, b \in r(I)$. Then for some $n, m \in \mathbb{Z}$, $a^n \in I$ and $b^m \in I$. We will now use the binomial expansion to show that $(a - b)^{n+m-1} \in I$.

\[
(a - b)^{n+m-1} = \sum_{i=0}^{n+m-1} \binom{n+m-1}{i} a^i (-b)^{n+m-1-i}
\]
For each \( i \), either \( i \geq n \) or \( n + m - 1 - i \geq m \). This tells us that for each expression \( a^i(-b)^{n+m-1-i} \), either the exponent of \( a \) will be large enough to make that power of \( a \) be in \( I \) or the exponent of \( -b \) will be large enough so that that power of \( -b \) is in \( I \). Because each expression is in \( I \), the entire sum is in \( I \) and therefore, \((a-b)^{n+m-1} \in I \). Finally, for any \( a \in r(I) \) and \( t \in R \), \( a^n \in I \). Now, \((ta)^n = t^n a^n \in I \) so that \( ta \in r(I) \). It follows that \( r(I) \) is an ideal.

**Proposition 3.10.** Let \( I \) and \( J \) be ideals of a ring \( R \).

i) If \( I \subseteq J \) then \( r(I) \subseteq r(J) \)

ii) \( r(I \cap J) = r(I) \cap r(J) \).

**Proof.** (i) Let \( x \in r(I) \). Then \( x^n \in I \subseteq J \) so that \( x^n \in J \). Hence \( x \in r(J) \).

(ii) \( I \cap J \subseteq I \). By the part (i), \( r(I \cap J) \subseteq r(I) \). Similarly, \( r(I \cap J) \subseteq r(J) \). So \( r(I \cap J) \subseteq r(I) \cap r(J) \). Now let \( a \in r(I) \cap r(J) \). This implies \( a^n \in I \) and \( a^m \in J \). So \( a^{m+n} \in I \), \( a^{m+n} \in J \) and \( a^{m+n} \in I \cap J \). Thus \( a \in r(I \cap J) \). It follows that \( r(I \cap J) = r(I) \cap r(J) \).

**Definition 3.11.** An element \( a \) of a ring \( R \) is **nilpotent** if \( a^n = 0 \) for some positive integer \( n \).

**Definition 3.12.** The set of all nilpotent elements of a ring \( R \) is called the **nilradical** of \( R \).

**Proposition 3.13.** The nilradical of \( R \) is the intersection of all the prime ideals of \( R \).

**Proof.** Let \( R \) denote the intersection of all the prime ideals of \( R \). If \( a \in R \) is nilpotent, and if \( P \) is a prime ideal, then \( a^n = 0 \in P \) for some \( n > 0 \), and therefore, \( a \in P \) since \( P \) is prime. So \( a \in R \). Conversely, suppose that \( a \) is not nilpotent. Let \( \Sigma \) be the set of ideals \( I \) with the property

\[
 n > 0 \Rightarrow a^n \notin I. \]

Then \( \Sigma \neq \emptyset \) because \( a \notin (0) \) and so that \( (0) \in \Sigma \). As in Proposition 3.5, we apply Zorn’s Lemma to the set \( \Sigma \) ordered by inclusion. Accordingly, \( \Sigma \) has a maximal element. Let \( M \) be a maximal element in \( \Sigma \). We will show that \( M \) is a prime ideal. Let \( x, y \notin M \).
The ideals $M + (x)$, and $M + (y)$ strictly contain $M$, and therefore do not belong to $\Sigma$. Therefore

$$a^m \in M + (x), \ a^n \in M + (y)$$

for some $m, n$. It follows that $a^{m+n} \in M + (xy)$, so that the ideal $M + (xy) \notin \Sigma$. Therefore, $xy \notin M$ (otherwise, $M + xy = M$). Hence, we have a prime ideal $M$ such that $a \notin M$, and as a result, $a \notin \mathfrak{R}$.

Proposition 3.14. Let $Q$ be an ideal of a ring $R$. Then $Q$ is primary if and only if $R/Q \neq 0$ and every zero divisor in $R/Q$ is nilpotent.

Proof. Let $Q$ be a primary ideal in a ring $R$ and let $a = x + Q \neq Q$ be a zero divisor in the quotient ring $R/Q$. Now $Q$ is primary so that $Q \neq R$ and $R/Q \neq (0)$. Since $x + Q$ is a zero divisor, there is a nonzero element $b = y + Q \in R/Q$ such that $ba = yx + Q = Q$. This implies $yx \in Q$. Now, $y \notin Q$ because $y + Q$ is nonzero. Since $Q$ is primary, we have that $x^n \in Q$ so that $(x + Q)^n = a^n = Q$. Hence $a$ is nilpotent. Conversely, Let $xy \in Q$ and $x \notin Q$. Now, $xy + Q = Q$ implies that $y + Q$ is a zero divisor in $R/Q$ and by hypothesis, is nilpotent. So $(y + Q)^n = y^n + Q = Q$. It follows that $y^n \in Q$, and $Q$ is primary.

Proposition 3.15. If $Q$ is a primary ideal, then $r(Q)$ is prime.

Proof. Let $xy \in r(Q)$. Then $(xy)^m \in Q$ for some $m > 0$. Therefore, either $x^m \in Q$ or $y^{mn} \in Q$ for some $n > 0$. It follows that either $x \in r(Q)$ or $y \in r(Q)$.

Definition 3.16. If $P = r(Q)$, where $Q$ is a primary ideal, then $Q$ is said to be P-primary.

Proposition 3.17. If $Q_i$ are P-primary for $1 \leq i \leq n$, then $Q = \bigcap_{i=1}^{n} Q_i$ is P-primary.

Proof. $r(Q) = r(\bigcap_{i=1}^{n} Q_i) = \bigcap_{i=1}^{n} r(Q_i) = P$ (Proposition 3.10), since all the $Q_i$ are P-primary. Now, let $xy \in Q$, $y \notin Q$. Then for some $i$, we have $xy \in Q_i$ and $y \notin Q_i$. Since $Q_i$ is P-primary, $x^n \in Q_i$ and $x \in P$.

We will later see in example 3.21 that the converse of Proposition 3.15 is false; that is if $r(I) = P$ is prime, then $I$ is not necessarily primary. However, we do have the following result:
Proposition 3.18. If \( r(Q) \) is maximal, then \( Q \) is primary. In particular, the powers of a maximal ideal are primary.

Proof. Let \( r(Q) = M \) where \( M \) is a maximal ideal in \( R \). We will show that \( R/Q \neq 0 \) and that every zero divisor in \( R/Q \) is nilpotent and then use Proposition 3.14. \( R/Q \neq 0 \) since \( Q \neq R \). By the Correspondence Theorem for Rings (Theorem 2.15), we have \( M/Q \) is an ideal of \( R/Q \). We claim that \( M/Q \) is the nilradical (the set of all nilpotent elements) of \( R/Q \): If \( x + Q \in M/Q \), then \( x \in M \) and \( x^n \in Q \). So \((x + Q)^n = x^n + Q = Q \), the zero element of \( R/Q \). Thus \( x + Q \) is nilpotent. Conversely, if \( y + Q \in R/Q \) is nilpotent, then \((y + Q)^n = y^n + Q = Q \). So \( y^n \in Q \) and \( y \in M \) so that \( y + Q \in M/Q \). This proves that \( M/Q \) is the nilradical of \( R/Q \). By Proposition 3.13, \( M/Q \) is the intersection of all the prime ideals of \( R/Q \). So \( \cap P_i/Q = M/Q \) where \( P_i/Q \) is prime. Also by hypothesis, \( M \) is maximal, so that \( M/Q \) is maximal (Correspondence Theorem for Rings). Now \( M/Q \subseteq P_i/Q \) for all \( i \) since \( M/Q \) is in the intersection. But \( M/Q \) is maximal so that \( P_i/Q \subseteq M/Q \) and \( P_i/Q = M/Q \) for all \( i \) (since \( P_i \) is prime, \( P_i/Q \) is a proper ideal). Hence \( R/Q \) has only one prime ideal, namely \( M/Q \). By Corollary 3.6, if \( x \in R/Q \) is not a unit, then \( x \in M/Q \). Hence we have that every element of \( R/Q \) is either a unit or nilpotent and thus every zero divisor of \( R/Q \) is nilpotent.

Corollary 3.19. Let \( Q \) be a primary ideal of a ring \( R \) with \( r(Q) = M \) where \( M \) is a maximal ideal. If \( I \) is an ideal of \( R \) and \( Q \subseteq I \subseteq M \), then \( I \) is primary and \( r(I) = M \).

Proof. \( Q \subseteq I \subseteq M \) implies \( r(Q) \subseteq r(I) \subseteq r(M) \) by Proposition 3.10. So \( M \subseteq r(I) \subseteq M \) and \( r(I) = M \). By Proposition 3.18, \( I \) is primary.

Example 3.20. A primary ideal is not necessarily the power of a prime ideal: Let \( R = k[x,y], Q = (x,y^2) \). Then the quotient ring

\[
R/Q = k[x,y]/(x,y^2) \cong k[y]/(y^2) : 
\]

The elements of the quotient ring \( R/Q \) are of the form \( f(x,y) + (x,y^2) \) where \( f(x,y) \in k[x,y] \). Now any term of \( f(x,y) \) that is a multiple of \( x \) or \( y^2 \) will be absorbed into the ideal \((x,y^2)\) so that any \( f(x,y) + (x,y^2) \) reduces to \( ay + b + (x,y^2) \), with \( a,b \in k \). Similarly, any \( f(y) + (y^2) \) of \( k[y]/(y^2) \) reduces to \( ay + b + (y^2) \). The zero divisors of \( k[y]/(y^2) \) are all multiples of \( y \) and are therefore nilpotent. So \( Q \) is primary by Proposition 3.14 and
$r(Q) = P = (x, y)$. We have $P^2 \subset Q \subset P$. Indeed, we will show that $Q \neq I^k$ where $I$ is a prime ideal. If $Q = I^k$ then $P^2 \subset I^k \subset P$, and therefore $r(P^2) \subseteq r(I^k) \subseteq r(P)$ so that $P \subseteq I \subseteq P$. Thus $P^2 \subset P^k \subset P$, a contradiction because no such $k$ exists. So $Q$ is not the power of a prime.

Example 3.21. We will now construct a ring in which the power of a prime ideal is not primary, although its radical is prime. Let $R = k[x, y, z]/(xy - z^2)$, and let $\bar{x}, \bar{y}, \bar{z}$ denote the images of $x, y, z$ respectively in $R$. Then $P = (\bar{x}, \bar{y})$ is prime by Lemma 2.12 since

$$R/P = k[x, y, z]/(xy - z^2) / (x, z)/(xy - z^2) \cong k[x, y, z]/(x, z) \cong k[y],$$

a domain. To see that the above rings are isomorphic using the third isomorphism theorem for rings (Theorem 2.18), for any ring $R$ and any ideals $I, J \subseteq R$ with $I \subseteq J$, $R/I \cong R/J$ so that $k[x, y, z]/(xy - z^2)/(x, z) \cong k[x, y, z]/(x, z)$. For any $f(x, y, z) + (x, z) \in k[x, y, z]/(x, z)$, $f(x, y, z) + (x, z) = f(y) + (x, z)$ where $f(y)$ is the sum of terms of $f(x, y, z)$ in only the $y$ variable with possible constant terms. If we define $\phi : k[x, y, z]/(x, y) \to k[y]$ by $\phi(f(x, y, z) + (x, z)) = f(y)$, it is easily verifiable that that $\phi$ is an isomorphism: first we will show that $\phi$ is injective. If $\phi(f(y) + (x, z)) = \phi(g(y) + (x, z))$, then $f(y) = g(y)$ and clearly $f(y) + (x, z) = g(y) + (x, z)$, so that $\phi$ is injective. For any $h(y) \in k[y]$, $h(y) + (x, z) \in k[x, y, z]/(x, z)$ and $\phi(h(y) + (x, z)) = h(y)$ so that $\phi$ is surjective. An elementary calculation will show that $\phi$ is a homomorphism, and therefore an isomorphism. Since $k[y]$ is an integral domain, then $(x, z)/(xy - z^2) = (\bar{x}, \bar{z})$ is prime. We have $\bar{x}\bar{y} = xy + (xy - z^2)$ and $\bar{z}^2 = z^2 + (xy - z^2)$. Thus $\bar{x}\bar{y} - \bar{z}^2 = xy - z^2 + (xy - z^2)$ which is zero in $R/P$. Therefore, $\bar{x}\bar{y} = \bar{z}^2$. Finally, $\bar{x}\bar{y} = \bar{z}^2 \in P^2$ but $\bar{x} \notin P^2$ and $\bar{y} \notin r(P^2) = P$. Hence $P^2$ is not primary but it is the power of a prime.

3.2 Primary Decomposition

Definition 3.22. A primary decomposition of an ideal $I$ in a ring $R$ is an expression of $I$ as a finite intersection of primary ideals, say $I = \bigcap_{i=1}^{n} Q_i$.

Definition 3.23. A primary decomposition is said to be minimal if:

i) the $r(Q_i)$ are all distinct and;
If a primary decomposition \( I = \bigcap_{i=1}^{n} Q_i \) is not minimal, that is if \( r(Q_j) = r(Q_k) = P \), for \( j \neq k \) then we may achieve (i) by replacing \( Q_j \) and \( Q_k \) by \( Q' = Q_j \cap Q_k \) which is \( P \)-primary by Proposition 3.17. Repeating this process, we get will arrive at a primary decomposition in which all \( r(Q_i) \) are distinct. If \( \bigcap_{j \neq k} Q_j \subseteq Q_i \), we may simply omit \( Q_i \). Repeating this process, we will achieve (ii).

**Example 3.24.** In \( \mathbb{Z} \), we have already seen that \((12) = (2^2) \cap (3)\), and since \((2^2), (3)\) are primary, this is a primary decomposition. It is easy to see that this decomposition is minimal.

**Example 3.25.** In \( k[x, y] \), \( I = (x^2, xy) = (x) \cap (x, y)^2 \cap (x^2, y) \). Now, \( (x) \) is prime and therefore, primary. The ideal \( (x, y) \) is maximal, and by Proposition 3.18, \((x, y)^2\) is primary. Also \((x, y)^2 \subseteq (x^2, y) \subseteq (x, y)\) so that by Proposition 3.19, \((x^2, y)\) is primary. Thus we have a primary decomposition of \( I \). We will now minimize this decomposition: \( r(x, y)^2 = r(x^2, y) = (x, y) \), so we may replace \((x^2, y)\) and \((x, y)^2\) by \((x, y)^2 \cap (x^2, y) = (x, y)^2\). Thus \( I = (x) \cap (x^2, y) \) is now a minimal primary decomposition.

**Example 3.26.** Let \( R \) be the polynomial ring \( k[x, y, z] \). Let \( P_1 = (x, y), P_2 = (x, z) \) and \( M = (x, y, z) \). Now, \( P_1 \) and \( P_2 \) are prime and \( M \) is maximal \([1]\). Let \( I = P_1 P_2 = (x^2, xy, xz, yz) \). We will verify that \( I = P_1 \cap P_2 \cap M^2 \) is a reduced primary decomposition of \( I \). Now, \((x, z) \cap (x, y, z)^2 \subseteq (x, y)\) since \( z^2 \in (x, z) \cap (x, y, z)^2 \) but \( z^2 \notin (x, y)\); \((x, y, z)^2 \cap (x, y) \subseteq (x, z)\) since \( y^2 \in (x, y) \cap (x, y, z)^2 \) but \( y^2 \notin (x, z)\); \((x, y) \cap (x, z) \subseteq (x, y, z)^2\) since \( x \in (x, y) \cap (x, z) \) but \( x \notin (x, y, z)^2\); \( r(x, y) = (x, y), r(x, z) = (x, z)\), \( r(x, y, z)^2 = (x, y, z)\) and clearly they are all distinct. Thus we have a minimal primary decomposition of \( I \).

### 3.3 Noetherian Rings

As stated earlier, primary decomposition does not exist in general. In this section, we show that in a certain class of rings called **Noetherian rings**, every ideal has a primary decomposition. These rings are named after Emmy Noether, who inaugurated the use of chain conditions in Algebra \([2]\).
Theorem 3.27. The following conditions are equivalent for a commutative ring $R$:

i) $R$ satisfies the ascending chain condition (ACC) on all ideals.

ii) $R$ satisfies the maximum condition: Every nonempty family $\mathcal{R}$ of ideals in $R$ has a maximal element; that is there is some $I_n \in \mathcal{R}$ for which there is no $I \in \mathcal{R}$ with $I_n \subset I$.

iii) Every ideal is finitely generated, that is every ideal is generated by a finite number of elements of $R$.

Proof. (i)$\Rightarrow$(ii): Let $\mathcal{I}$ be a family of ideals of $R$ and assume that $\mathcal{I}$ has no maximal element. Now, choose $I_1 \in \mathcal{I}$. Since $I_1$ is not a maximal element there is $I_2 \in \mathcal{I}$ such that $I_1 \subset I_2$. Now $I_2$ is not maximal in $\mathcal{I}$ so there is $I_3 \in \mathcal{I}$ such that $I_2 \subset I_3$. Continuing this way, we may construct an ascending chain of ideals that is not stationary. So $\mathcal{I}$ must have a maximal element.

(ii)$\Rightarrow$(iii): Let $I$ be an ideal of $R$ and define $\mathcal{F}$ to be the family of finitely generated ideals contained in $I$. Now $\mathcal{F}$ is nonempty since $\{0\} \in \mathcal{F}$. By hypothesis, $\mathcal{F}$ has a maximal element, say $M$. Now, $M \subseteq I$ since $M \in \mathcal{F}$. If $M \subset I$, then there is a nonzero element $a \in I$ such that $a \notin M$. The ideal $J = \{M + (a)\} \subseteq I$ is finitely generated. So $J \in \mathcal{F}$. But $M \subseteq J$ which contradicts the maximality of $M$. So $M = I$ and $I$ is finitely generated.

(iii)$\Rightarrow$(i): Assume that every ideal is finitely generated and let $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \cdots$ be an ascending chain of ideals of $R$. Then $J = \bigcup_{n \geq 1} I_n$ is an ideal of $R$. By hypothesis, there are elements $a_i \in J$ such that $J = (a_1, a_2, \cdots, a_n)$. Now, $a_i \in J \Rightarrow a_i \in I_{n_i}$ for some $n_i$. If $N$ is the largest $n_i$, then $I_{n_i} \subseteq I_N$ for all $i$; hence $a_i \in I_N$ for all $i$ and $J = (a_1, \cdots, a_n) \subseteq I_N$ and $I_N \subseteq J$. So $J = I_N$. It follows that if $n > N$, then $J = I_N \subseteq I_n \subseteq J$. Therefore, the chain stops and $R$ satisfies ACC. $\square$

Definition 3.28. A commutative $R$ is said to be Noetherian if it satisfies any of the three equivalent conditions of Theorem 3.27.

Example 3.29. The ring of integers $\mathbb{Z}$ is Noetherian since every ideal is principal.

Lemma 3.30. (I.S. Cohen) If all the prime ideals of a ring $R$ are finitely generated, then $R$ is Noetherian.
Proof. Let $\Sigma$ be the set of ideals of $R$ that are not finitely generated. If $\Sigma \neq \emptyset$ then by Zorn’s Lemma, $\Sigma$ contains a maximal element $I$. Then $I$ is not a prime ideal and there are elements $x, y \in R$ with $x \notin I$, $y \notin I$ but $xy \in I$. Now $I + Ry$ is bigger than $I$, and is therefore finitely generated. So we may choose $a_1, \ldots, a_n \in I$ such that $(a_1, \ldots, a_n, y) = I + Ry$. Moreover, $I : y = \{ a \in R | ay \in I \}$ contains $x$ and is thus bigger than $I$, so that it is finitely generated by $\{ b_1 \cdots b_m \}$. Finally, $I = \{ a_1, \ldots, a_n, b_1y \cdots b_my \}$ since all that generators are also in $I$. Hence $I \notin \Sigma$ because it is finitely generated, but this is a contradiction. Therefore, $\Sigma = \emptyset$ and $R$ is Noetherian. \hfill \Box

**Theorem 3.31.** Let $R$ be a Noetherian ring and $I$ an ideal of $R$. Then the quotient ring $R/I$ is Noetherian.

**Proof.** If $\bar{I}$ is an ideal of $R/I$, then the Correspondence Theorem for Rings provides the ideal $J$ in $R$ with $\bar{I} = J/I$. Since $R$ is Noetherian, the ideal $J$ is finitely generated. Therefore, $J = (a_1, \ldots, a_n)$, and $\bar{I} = J/I$ is also finitely generated by the cosets $a_1 + I, \ldots, a_n + I$. \hfill \Box

**Theorem 3.32.** *(Hilbert Basis Theorem)* If $R$ is Noetherian, then the polynomial ring $R[x]$ is Noetherian.

**Proof.** Assume that the ideal $I$ of $R[x]$ is not finitely generated. Clearly $I \neq \{ 0 \}$. We define $f_0(x)$ to be a polynomial of minimal degree in $I$ and define, inductively, $f_{n+1}(x)$ to be a polynomial of minimal degree in $I - (f_0, \ldots, f_n)$. It is also clear that

$$\deg(f_0) \leq \deg(f_1) \leq \deg(f_2) \leq \cdots.$$ 

Let $a_n$ denote the leading coefficient of $f_n(x)$. Since $R$ is Noetherian, there is an integer $m$ such that $a_{m+1} \in (a_0, \ldots, a_m)$, otherwise we will have an increasing chain of ideals $(a_0) \subseteq (a_0, a_1) \subseteq (a_0, a_1, a_2) \subseteq \cdots$ that is not stationary. This implies that there are elements $r_i \in R$ with $a_{m+1} = r_0a_0 + r_1a_1 + \cdots + r_ma_m$. We define

$$f^*(x) = f_{m+1}(x) - \sum_{i=0}^{m} x^{d_{m+1} - d_i} r_i f_i(x),$$

where $d_i = \deg(f_i)$. Now $\sum_{i=0}^{m} x^{d_{m+1} - d_i} r_i f_i(x) \in (f_0, \ldots, f_m)$ since $f_i(x) \in (f_0, \ldots, f_m)$. If $f^*(x) \in (f_0, \ldots, f_m)$, then $f_{m+1}(x) - \sum_{i=0}^{m} x^{d_{m+1} - d_i} r_i f_i(x) + \sum_{i=0}^{m} x^{d_{m+1} - d_i} r_i f_i(x) =$
\[ f_{m+1}(x) \in (f_0, \ldots, f_m) \] which we cannot have since \( f_{m+1} \in I - (f_0, \ldots, f_m). \) Thus \( f^* \in I - (f_0(x), \ldots, f_m(x)). \) It suffices to show that \( \deg(f^*(x)) < \deg(f_{m+1}), \) for this contradicts \( f_{m+1} \) having minimal degree among the polynomials in \( I \) but not in \( (f_0, \ldots, f_m). \) If \( f_i(x) = a_i x^{d_i} + \text{lower terms}, \) then

\[ f^*(x) = f_{m+1}(x) - \sum_{i=0}^{m} x^{d_{m+1} - d_i} r_i f_i(x) \]

\[ = a_{m+1} x^{d_{m+1}} + \text{lower terms} - \sum_{i=0}^{m} x^{d_{m+1} - d_i} r_i (a_i x^{d_i} + \text{lower terms}). \]

The leading coefficient being subtracted off is \( \sum_{i=0}^{m} r_i a_i x^{d_{m+1}} = a_{m+1} x^{d_{m+1}}. \)

\[ \square \]

**Corollary 3.33.** If \( R \) is Noetherian, so is \( R[x_1, x_2, \ldots, x_n]. \)

*Proof.* \( R[x] \) is Noetherian so that \((R[x_1])[x_2] = R[x_1, x_2] \) is Noetherian by Theorem 3.32. Repeating this inductively, we will arrive at the desired result. \( \square \)

**Example 3.34.** The polynomial ring \( k[x_1, x_2, \ldots, x_n] \) is Noetherian since any field \( k \) is Noetherian.

**Example 3.35.** The polynomial ring \( k[x_1, x_2, \ldots] \) in an infinite number of indeterminates does not satisfy ACC since the sequence \( (x_1) \subset (x_1, x_2) \subset \cdots \) is not stationary. Hence \( k[x_1, x_2, \ldots] \) is not Noetherian.

In chapter 2, we saw that one of the requirements for a ring \( R \) to be a UFD is that \( R \) must satisfy ACC on principal ideals. We will now demonstrate that a UFD does not need to be Noetherian. It is sufficient that it satisfy ACC only on principal ideals. The next two examples illustrate that there are UFD’s that are not Noetherian and there are certainly Noetherian rings that are not UFDs.

**Example 3.36.** Although the polynomial ring \( R = k[x_1, x_2, \ldots] \) in an infinite number of indeterminates is not Noetherian, it is a UFD. We will verify this as follows: Regard \( R \) as the union of the ascending chain \( k[x_1] \subset k[x_1, x_2] \subset \cdots \subset k[x_1, x_2, \ldots, x_n] \subset \cdots. \) So \( R = \bigcup_{i=1}^{\infty} R_i, \) where \( R_i = k[x_1, \ldots, x_i]. \) Now let \( f \in R \) where \( f \) is neither zero nor a unit. Since \( f \) is in \( R, \) \( f \) is in \( R_i \) for some \( i. \) In fact, there is some \( k \) such that \( f \in R_i \) for all \( i \geq k \) since the chain is ascending. Select \( k \) such that \( f \in R_k, \) but \( f \notin R_{k-1}. \) By Corollary 2.51 \( R_k \) is UFD so that \( f \) may be factored into a product of irreducibles...
say, \( f = u g_1 \cdots g_m \) with each \( g_j \) irreducible in \( R_k \). If for some \( j > k \), some \( g_j \) is not irreducible, then let \( g_j = h_1 \cdots h_l \) be the irreducible factorization of \( g_j \) (now \( l > 1 \) or \( g_j \) would be irreducible). Since all the \( R_i \) are integral domains, \( h_i \) cannot introduce any new indeterminates into the factorization of \( g_j \), so that each \( h_i \) is an irreducible element of \( R_k \). Thus in \( R_k \) we have two distinct irreducible factorizations of \( g_j = g_j \) and \( g_j = h_1 \cdots h_l \), which is a contradiction. So \( g_j \) is irreducible for all \( R_i \). Since each \( R_i \) is a UFD, then \( f = g_1 \cdots g_m \) is a unique irreducible factorization in each \( R_i \) so that \( f \) may be factored uniquely into a product of irreducibles in \( R \).

**Example 3.37.** The polynomial ring \( \mathbb{Z}[\sqrt{d}] \), where \( d \in \mathbb{Z}, d < 0 \) is Noetherian: Define \( \phi : \mathbb{Z}[x] \rightarrow \mathbb{Z}[\sqrt{d}] \) by the evaluation map \( \phi(f) = f(\sqrt{d}) \). Our technique is to show that \( \text{Ker} \phi \) is the ideal \( < x^2 - d > \) and then use the First Isomorphism Theorem to show that \( \mathbb{Z}[x]/(x^2 + d) \cong \mathbb{Z}[\sqrt{d}] \), which is Noetherian by Theorem 3.31. But first we will show that \( \phi \) is indeed a homomorphism. Let \( f \in \mathbb{Z}[x], f = 1 \). Then \( \phi(f) = f(\sqrt{d}) = 1 \).

For \( g \in \mathbb{Z}[x] \), from elementary Algebra, we know that \( (f + g)\sqrt{d} = f(\sqrt{d}) + g(\sqrt{d}) \) and \( (fg)\sqrt{d} = f(\sqrt{d})g(\sqrt{d}) \). Therefore, \( \phi(f + g) = \phi(f) + \phi(g) \) and \( \phi(fg) = \phi(f)\phi(g) \). Hence \( \phi \) is a ring homomorphism. Next, we will show that \( \text{Ker} \phi = (x^2 - d) \). Let \( f \in (x^2 - d) \). Then \( f = (x^2 - d)g(x) \) for some \( g(x) \in \mathbb{Z}[x] \). Now \( f(d) = ((\sqrt{d})^2 - d)g(\sqrt{d}) = 0 \). This implies \( g(\sqrt{d}) = 0 \). If we look at \( g \) as an element in \( \mathbb{R}[x] \), then \( x - \sqrt{d} \) is a factor of \( g \). Since \( \sqrt{d} \) is a complex root, then \( -\sqrt{d} \) is also a root of \( g \), which makes \( x + \sqrt{d} \) also a factor of \( g \). From this, we get \( g = (x - \sqrt{d})(x + \sqrt{d})h = (x^2 - d)h \) for some \( h \in \mathbb{R}[x] \). We chose \( g \) as an element of \( \mathbb{Z}[x] \) so that the coefficients of \( g \) are integers. Since \( g = (x^2 - d)h \), if follows that \( h \) must also have integer coefficients, so that \( h \in \mathbb{Z}[x] \). So \( g \in (x^2 - d) \) as desired. Therefore \( \text{Ker} \phi = (x^2 - d) \). By the First Isomorphism Theorem, \( \mathbb{Z}[x]/(x^2 + d) \cong \text{Im} (\mathbb{Z}[x]) \) (it remains to show that \( \text{Im} (\mathbb{Z}[x]) = \mathbb{Z}[\sqrt{d}] \)). For any element \( y \in \mathbb{Z}[\sqrt{d}], y = a + b\sqrt{d}, a, b \in \mathbb{Z} \) and if we choose \( f \in \mathbb{Z}[x] \) to be the polynomial \( a + bx \), then \( \phi(f) = a + b\sqrt{d} \). So \( \phi \) is onto and \( \text{Im} (\mathbb{Z}[x]) = \mathbb{Z}[\sqrt{d}] \). Hence \( \mathbb{Z}[x]/(x^2 + d) \cong \mathbb{Z}[\sqrt{d}] \). Finally by Theorem 3.31, \( \mathbb{Z}[x]/(x^2 + d) \) is Noetherian so that \( \mathbb{Z}[\sqrt{d}] \) is also Noetherian. In particular, \( \mathbb{Z}[\sqrt{-5}] \) is not a UFD but it is Noetherian.

**Proposition 3.38.** A UFD \( R \) is a PID if and only if every prime ideal of \( R \) is maximal.

**Proof.** Let \( R \) be a PID and let \( I \neq (0) \) be a prime ideal in \( R \), which implies that \( I = (p) \)
for some prime $p \in R$. Suppose $(p)$ is not maximal. Then there is some proper ideal $J = (a) \subset R$ such that $(p) \subset (a)$. Hence $p \in (a)$ and $p = ab$ for some $b \in R$. Now $a$ cannot be a unit since $J$ is a proper ideal, and since $p$ is prime, $b$ must be a unit. So $a$ and $p$ are associates and $(a) = (p)$, a contradiction. So $I$ is maximal.

Conversely, suppose every prime ideal $P$ in $R$ is maximal. Let $a \in P$, $a \neq 0$. Factor $a$ into its irreducible components: $a = u p_1 \cdots p_n$. For some $i$, $p_i \in P$ because $P$ is prime. So $(p_i) \subseteq P$. Since $R$ is a UFD, the irreducible elements generate prime ideals so that $(p_i)$ is prime and therefore maximal. Thus $P \subseteq (p_i)$ and $(p_i) = P$. This shows that every prime ideal of $R$ is principal. Now, let $J$ be any ideal of $R$. By Lemma 3.30 $J$ is finitely generated say $I = (a_1, \ldots, a_n)$. By Lemma 2.41 $a_1, \ldots, a_n$ has a gcd, say $d$. It is clear that $(a_1, \ldots, a_n) \subseteq (d)$. Let $K \subseteq R$ be the ideal $(a_1/d, \ldots, a_n/d)$. It is easy to verify that all the elements $a_1/d, \ldots, a_n/d$ are relatively prime and thus their only common divisors are units. From this, we get that $K \not\subseteq (p)$ for any prime ideal $(p)$. Thus, $K$ is not contained in any maximal ideal, and therefore, $K = R = (1)$. Finally, $1 \in (a_1/d, \ldots, a_n/d)$ which implies $1 = x_1 a_1/d + \cdots + x_n a_n/d$ and multiplying by $d$, we get $d = x_1 a_1 + \cdots + x_n a_n$ so that $d \in (a_1, \ldots, a_n)$ and therefore, $(d) = (a_1, \ldots, a_n)$ and $I$ is principal.

We have not proved that a gcd of elements $a_1, \ldots, a_n$ may be expressed as a linear combination of them. Indeed, in the ring $k[x, y]$, the gcd of $x$ and $y$ is 1, but 1 cannot be expressed as a linear combination of $x$ and $y[5]$.

Our next objective is to prove that in a Noetherian ring, every ideal has a primary decomposition, but before we can get to this result, we will need the following theorem, definitions and lemma:

**Definition 3.39.** An ideal $I$ is said to be **irreducible** if $I = J \cap K \Rightarrow I = J$ or $I = K$.

**Theorem 3.40.** In a Noetherian ring $R$, every ideal is a finite intersection of irreducible ideals.

**Proof.** Suppose the theorem is false. Then the set of ideals of $R$ for which the theorem is false is non empty and by the Noetherian property, has a maximal element $M$. Since $M$ is not irreducible, we have $M = I \cap J$ where $M \subset I$ and $M \subset J$. Because $M$ is maximal, each of $I$ and $J$ are a finite intersection of irreducible ideals. If we let
I = I_1 \cap I_2 \cdots \cap I_n and J = J_1 \cap J_2 \cdots \cap J_m, with each I_i and J_j irreducible, then
M = I \cap J = I_1 \cap_2 \cdots \cap I_n \cap J = J_1 \cap J_2 \cdots \cap J_m, which is a finite intersection of irreducible ideals, a contradiction. Thus we conclude that every ideal of R is a finite intersection of irreducible ideals.

We wish to show that in a Noetherian ring, every irreducible is primary, which will then lead to our final result in this section. We will need the following lemmas regarding quotient rings.

**Lemma 3.41.** Let R be a ring and I an ideal of R. If I/I is irreducible in R/I, then I is irreducible in R.

*Proof.* Suppose I is not irreducible in R. Then we have I = J \cap K with I \subset J and I \subset K. Now J/I and K/I are ideals of R/I (Correspondence Theorem for Rings). Since I = J \cap K, then I/I = J/I \cap K/I. But I/I \subset J/I and I/I \subset K/I which implies that I/I is not irreducible. \qed

**Lemma 3.42.** Let R be a ring and I an ideal of R. If I/I is primary, then I is primary.

*Proof.* Suppose I is not primary. Then there are a, b \in R with ab \in I but a \notin I and b^n \notin I. So we have ab + I \in I/I and a + I \notin I/I and b^n \notin I/I. This implies that I/I is not primary. \qed

**Definition 3.43.** Let A be a subset of a ring R. The annihilator of A denoted Ann(A) = \{r \in R : ra = 0 for all a \in A\}.

**Lemma 3.44.** Ann(A) is an ideal.

*Proof.* 0 \cdot a = 0 for all a \in A So 0 \in Ann(A). For b \in Ann(A) (ba = 0 for all a \in A) and r \in R, rba = r \cdot 0 = 0 so that br \in Ann(A). For b, c \in Ann(A), (b - c)a = ba - ca = 0. So b - c \in Ann(A). It follows that Ann(A) is an ideal. \qed

**Theorem 3.45.** In a Noetherian ring, every irreducible ideal is primary.

*Proof.* Let R be a Noetherian ring and I an irreducible ideal. Let x, y \in R/I, and xy = 0, y \neq 0 (in this case, 0 = I/I). Now, consider the chain of ideals Ann(x) \subseteq Ann(x^2) \subseteq \cdots. By ACC, this chain is stationary, so there exists an n such that
Ann(x^n) = Ann(x^{n+1}) = \cdots. It follows that (x^n) \cap (y) = 0; for if a \in (y) then a = ys and ax = ysx = 0 since xy = 0. If a is also in (x^n), then a = bx^n and 0 = ax = bx^n x = bx^{n+1}. Hence b \in Ann(x^{n+1}) = Ann(x^n) implies bx^n = 0. So a = 0. Since 0 is irreducible and 0 = (x^n) \cap (y) and (y) \neq 0, then (x^n) = 0. This implies x^n = 0. So 0 is primary. By Lemma 3.42, I is primary.\qed

**Theorem 3.46.** In a Noetherian ring, every ideal has a primary decomposition.

**Proof.** This follows immediately from Theorems 3.40 and 3.45.\qed

It follows that every ideal of \(\mathbb{Z}, \mathbb{Z}[x]\) and \(k[x]\) have a primary decomposition. We will see examples of primary decomposition of ideals when we talk about uniqueness in the next section.
Chapter 4

PRIMARY DECOMPOSITION AND UNIQUENESS

4.1 First Uniqueness Theorem

The primary components in a primary decomposition are in general not unique. For example, in \( k[x, y] \), \((x^2, xy) = (x) \cap (x, y)^2 = (x) \cap (x^2, y)\). We will later see that these are two distinct minimal primary decompositions. However, primary decomposition has some properties that are unique. One of such properties involves the set of the radicals of the primary components. Another involves the minimal components of the decomposition. In this chapter, we will prove the First and Second Uniqueness Theorems for primary decomposition. We precede the First Uniqueness Theorem with the following definitions and lemmas:

**Definition 4.1.** Let \( I \) be an ideal of a ring \( R \) and let \( x \in R \). Then \((I : x) = \{y \in R: xy \in I\}\).

**Proposition 4.2.** Let \( J \) be a subset of a ring \( R \) with \( J = (I : x) \). Then \( J \) is an ideal of \( R \).

**Proof.**

i) \( 0 \cdot x = 0 \in I \) so that \( 0 \in J \).

ii) Let \( y \in J \). This implies \( yx \in I \). For \( r \in R \), \( ryx \in I \) so that \( ry \in J \).

iii) For \( a, b \in J \), \( ax \in I \) and \( bx \in I \) so that \( ax - bx = (a - b)x \in I \). Therefore, \( a - b \in J \).
It follows that $J$ is an ideal.

It is clear that $Q \subseteq (Q : x)$: for if $y \in Q$, of course $yx \in Q$ so that $y \in (Q : x)$.

**Proposition 4.3.** Let $Q$ be a $P$-primary ideal of a ring $R$ and $x \in R$:

i) If $x \in Q$, then $(Q : x) = R$;

ii) If $x \notin Q$, then $(Q : x)$ is $P$-primary and $r(Q : x) = P$.

**Proof.**

i) Let $x \in Q$. If $y \in R$, then $yx \in Q$, and $y \in (Q : x)$. So $R \subseteq (Q : x)$. Clearly $(Q : x) \subseteq R$. Therefore $(Q : x) = R$.

ii) Assume $x \notin Q$. If $y \in (Q : x)$, then $yx \in Q$. Since $x \notin Q$ and $Q$ is primary, $y^n \in Q$. Thus $y \in r(Q) = P$. So $(Q : x) \subseteq P$. Now let $z \in Q$. Then $zx \in Q$ so that $z \in (Q : x)$. So $Q \subseteq (Q : x) \subseteq P$. When we apply the radical, we get $P = r(Q) \subseteq r(Q : x) \subseteq r(P) = P$. So we have $r(Q : x) = P$. To see that $(Q : x)$ is primary, let $yz \in (Q : x)$ with $y^n \notin (Q : x)$ for any positive integer $n$. Then $y \notin P$. Now $xyz \in Q$ implies that $xz \in Q$ or $y^n \in Q$. But $y^n \notin Q$ by hypothesis so $xz \in Q$. So $z \in (Q : x)$. It follows that $(Q : x)$ is primary.

**Lemma 4.4.** Let $I_1, \ldots, I_n$ be ideals of a ring $R$ and let $P$ be a prime ideal of $R$.

i) If $\bigcap_{i=1}^n I_i \subseteq P$, then $I_i \subseteq P$ for some $i$.

ii) If $\bigcap_{i=1}^n I_i = P$, then $I_i = P$ for some $i$.

**Proof.**

i) Suppose $I_i \nsubseteq P$ for all $i$. Then there exists $x_i \in I_i$, $x_i \notin P$ for $1 \leq i \leq n$. Therefore, $x_1x_2 \cdots x_n \in I_1I_2 \cdots I_n \subseteq \bigcap I_i$. But since $P$ is prime, and $x_i \notin P$ for all $i$, then $x_1x_2 \cdots x_n \notin P$. Hence $\bigcap I_i \nsubseteq P$.

ii) If $P = \bigcap I_i$, then $P \subseteq I_i$ for all $i$, and from part(i), $I_i \subseteq P$ for some $i$. Hence $P = I_i$ for some $i$.

**Theorem 4.5.** (First Uniqueness Theorem) Let $I$ be a decomposable ideal and let $I = \bigcap_{i=1}^n Q_i$ be a minimal primary decomposition of $I$. Let $P_i = r(Q_i)$, $1 \leq i \leq n$. Then the $P_i$ are precisely the prime ideals that occur in the set of ideals $r(I : x)$, $x \in R$ and thus, are independent of the particular decomposition.
Proof. For any $x \in R$, we have $(I : x) = (\cap Q_i : x) = \cap (Q_i : x)$ (if $a \in (\cap Q_i : x)$, then $ax \in \cap Q_i$ and $ax \in Q_i$ for all $i$. So $a \in (\cap (Q_i : x)$). Conversely, if $a \in (\cap (Q_i : x)$, then $ax \in (Q_i : x)$ for all $i$ and $ax \in Q_i$ for all $i$. So $a \in (\cap Q_i : x)$. It follows that $(\cap Q_i : x) = \cap (Q_i : x))$. Hence $r(I : x) = r(\cap Q_i : x) = \cap_{i=1}^n r(Q_i : x)$ by Proposition 3.10. By Proposition 4.3, if $x \in Q_j$, then $r(Q_j : x) = R$ and if $x \notin Q_j$ then $r(Q_j : x) = P_j$. So $\cap_{i=1}^n r(Q_i : x) = \cap_{x \notin Q_j} P_j$. Now, suppose $r(I : x)$ is prime. Since $r(I : x) = \cap_{x \notin Q_j} P_j$, then by Proposition 4.4ii, $r(I : x) = P_j$ for some $j$. Hence every prime ideal $r(I : x)$ is one of the $P_j$.

Conversely, for each $i$, there exists $x_i \notin Q_i$, $x_i \in \cap_{j=1}^n Q_j$ since the decomposition is minimal. Hence $r(I : x_i) = \cap_{j=1}^n r(Q_j : x_i) = P_i$, since all the other $r(P_j, j \neq i) = R$ by Proposition 4.3i. □

Example 4.6. In $k[x, y]$, $I = (x^2, xy) = (x) \cap (x, y)^2 = (x) \cap (x^2, y)$. Now, $(x)$ is prime and therefore, primary. The ideal $(x, y)$ is maximal, and by Proposition 3.18, $(x, y)^2$ is primary. So $(x, y)^2 \subseteq (x^2, y) \subseteq (x, y)$ so that by Proposition 3.19, $(x^2, y)$ is primary and $r(x, y)^2 = r(x^2, y) = (x, y)$. We will now verify that each decomposition is minimal: for $(x) \cap (x, y)^2$, $r((x)) = (x) \neq r((x, y)^2) = (x, y)$ and we have $(x) \not\subseteq (x, y)^2$ since $x \notin (x, y)^2$ and $(x, y)^2 \not\subseteq (x)$ since $y^2 \notin (x)$. Therefore the primary decomposition $I = (x^2, xy) = (x) \cap (x, y)^2$ is minimal. The verification that $I = (x^2, xy) = (x) \cap (x^2, y)$ is minimal is similar. Observe that the radicals of the ideals in each decomposition are the same.

Although the components of a primary decomposition are not independent of the decomposition, it turns out that some of the components are uniquely determined, namely the minimal components. Our proof of this result uses some facts about extended and contracted ideals, multiplicatively closed subsets and rings of fractions. The next section gives a brief introduction to extended and contracted ideals.

4.2 Extended and Contracted Ideals

Let $f: R \rightarrow \tilde{R}$ be a ring homomorphism. If $I$ is an ideal in $R$, then the set $f(I)$ is not necessarily an ideal in $\tilde{R}$. For example, let $f: \mathbb{Z} \rightarrow \mathbb{Q}$ be the natural homomorphism $f(x) = x/1$ and let $I$ be the ideal generated by 2; $f(2) = 2/1$ and $2/1 \cdot 1/3 = 2/3 \notin f(I)$.
because there is no \( y \in I \) such that \( f(y) = 2/3 \). So \( f(I) \) is not an ideal. However, we have the following definition:

**Definition 4.7.** Let \( f: R \to \tilde{R} \) be a ring homomorphism. We define the extension, \( I^e \) of \( I \) to be the ideal \( \tilde{R}f(I) \), generated by \( f(I) \) in \( \tilde{R} \).

Explicitly, \( I^e \) is the set of sums \( \sum y_if(x_i) \) where \( x_i \in I, y_i \in \tilde{R}[1] \). On the contrary if \( \tilde{I} \) is an ideal of \( \tilde{R} \), then \( f^{-1}(\tilde{I}) \) is always an ideal of \( R \), and thus we have the following proposition:

**Proposition 4.8.** Let \( f: R \to \tilde{R} \) be a ring homomorphism and \( \tilde{I} \) an ideal of \( \tilde{R} \). Then \( f^{-1}(\tilde{I}) \) is an ideal of \( R \).

**Proof.** Let \( f^{-1}(\tilde{I}) = I \). First we wish to show that for \( x \in I \) and \( t \in R \), \( xt \in I \). If \( x \in I \), then there is some \( y \in \tilde{I} \) such that \( f^{-1}(y) = x \). Now \( f(xt) = f(x)f(t) = yf(t) \). Since \( \tilde{I} \) is an ideal, \( yf(t) \in \tilde{I} \) and \( f^{-1}(yf(t)) = xt \). So \( xt \in I \). Secondly, we will show that for \( c, d \in I \), \( c - d \in I \). Since \( c, d \in I \), then there is some \( u, v \in \tilde{I} \) such that \( f^{-1}(u) = c \) and \( f^{-1}(v) = d \). Now \( c - d \in R \) so that \( f(c - d) = f(c) - f(d) = u - v \); \( u - v \in \tilde{I} \) and \( f^{-1}(u - v) = c - d \in I \). Finally, \( 0 \in I \) since \( 0 \in \tilde{I} \) and \( f^{-1}(0) = 0 \). It follows that \( I \) is an ideal. \( \square \)

**Definition 4.9.** The ideal in the proposition 4.8, \( f^{-1}(\tilde{I}) \), is called the contraction of \( \tilde{I} \) and is denoted \( \tilde{I}^c \).

**Proposition 4.10.** Let \( f: R \to \tilde{R} \) be a ring homomorphism, \( \tilde{I} \) an ideal of \( \tilde{R} \) and \( I \) an ideal of \( R \):

i) \( I \subseteq I^e \).

ii) \( \tilde{I}^e \subseteq \tilde{I} \).

iii) \( I^e = I^e \).

iv) \( \tilde{I}^e = \tilde{I}^e \).

**Proof.** i) Let \( a \in I \). Then \( f(a) \in f(I) \subseteq I^e \) and \( f(f^{-1}(a)) = a \in I^e \) as desired.
ii) Let \( a \in (\overline{I}^{\text{ee}}) = \overline{R}f(\overline{I}^c) \). This implies that \( a = f(b)\overline{b} \) where \( b \in \overline{I}^c \) and \( \overline{b} \in \overline{R} \). Now \( b \in \overline{I} \) implies that there is some \( \bar{c} \in \overline{I} \) such that \( f^{-1}(\bar{c}) = b \). Substituting for \( b \), we get

\[
a = \overline{b}f(b) = f(f^{-1}(\bar{c}))\overline{b} = \overline{b}\bar{c}
\]

Since \( \bar{c} \in \overline{I} \) and \( \overline{I} \) is an ideal of \( \overline{R} \), \( \overline{b}\bar{c} \in \overline{I} \). So \( a \in \overline{I} \) as desired.

iii) Extending both sides of (i), we get \( I^e \subseteq I^{\text{ee}} \). In part (ii) if we let \( \overline{I} = I^e \), then \( I^{\text{ee}} \subseteq I^e \), so that \( I^{\text{ee}} = I^e \).

iv) Similarly, contracting both sides of part (ii), we get \( \overline{I}^{\text{ec}} \subseteq \overline{I}^c \) and in part (i), if we let \( \overline{I}^c = I \), we get \( \overline{I}^c \subseteq \overline{I}^{\text{ec}} \). It follows that \( \overline{I}^{\text{ec}} = \overline{I}^c \).

\[\square\]

4.3 Extended and Contracted Ideals in Rings of Fractions

We will now combine the concepts of the last two sections by looking at various properties about extended and contracted ideals in rings of fractions.

**Proposition 4.11.** Let \( R \) be a ring and \( S \) be a multiplicatively closed subset of \( R \) and define \( f: R \to S^{-1}R \) to be the natural homomorphism defined by \( f(r) = r/1 \). If \( I \) is an ideal in \( R \), its extension \( I^e \) in \( S^{-1}R \) is \( S^{-1}I \)

**Proof.** We have defined the \( I^e \) to the the ideal \( f(I) \). Any \( x \in I^e \) is of the form \( \sum r_i/s_i \), where \( r_i \in I \) and \( s_i \in S \). If we bring the fraction \( x \) to a common denominator, then it is easy to see that \( x \in S^{-1}I \). Conversely, if \( y \in S^{-1}I \), then \( y = r/s \), \( r \in I \) and \( s \in S \), which is of the form \( \sum r_i/s_i \). So \( y \in I^e \).

\[\square\]

**Proposition 4.12.** Let \( B \) be an ideal in \( S^{-1}R \). Then \( B \) is an extended ideal; that is \( B = I^e \) for some \( I \in R \).
Proof. Our technique here is to let $I = B^c$, which is an ideal $S^{-1}R$ by Proposition 4.8. For any $x/s \in B$, $s/1 \cdot x/s = x/1 \in B$. Therefore $x \in B^c$ and $x/s \in B^{ce}$ so that $B \subseteq B^{ce}$. By Proposition 4.10, $B^{ce} \subseteq B$ and $B = (B^{ce})^e = I^e$. □

Proposition 4.13. If $I$ is an ideal of $R$, then $I^{ec} = \bigcup_{s \in S}(I : s)$.

Proof. Let $x \in I^{ec} = (S^{-1}I)^c$. Then $x/1 \in S^{-1}I$ and $x/1 = a/s$ for some $a \in I$ and $s \in S$ so that $(xs - a)t = 0$ for some $t \in S$. From this we get $xst = at \in I$. So $x \in \bigcup_{s \in S}(I : s)$. For the reverse inclusion, suppose $x \in \bigcup_{s \in S}(I : s)$. Then, $xs \in I$ and $xs/1 \in I^e$. For $1/s \in S^{-1}R$, $(1/s) \cdot (xs/1) = x/1 \in I^e$ and $x \in I^{ec}$. □

Proposition 4.14. Let $I$ and $J$ be ideals of a ring $R$ and let $S$ be a a multiplicatively closed subset of $R$:

1) Then $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$.

2) $r(S^{-1}I) = S^{-1}r(I)$.

Proof. 1) Since $I \cap J \subseteq I$ then $S^{-1}(I \cap J) \subseteq S^{-1}I$. Similarly $S^{-1}(I \cap J) \subseteq S^{-1}J$. Therefore, we have $S^{-1}(I \cap J) \subseteq S^{-1}I \cap S^{-1}J$. Conversely, let $a/s \in S^{-1}I \cap S^{-1}J$. Then $a \in I$ and $a \in J$ so that $a \in I \cap J$ and $a/s \in S^{-1}(I \cap J)$ and $S^{-1}I \cap S^{-1}J \subseteq S^{-1}(I \cap J)$.

2) Let $a/s \in r(S^{-1}I)$. Then $(a/s)^n = a^n/s^n \in S^{-1}I$, so that $a^n \in I$ and $a \in r(I)$. Since $a \in r(I)$, $a/s \in S^{-1}r(I)$. Conversely, if $a/s \in S^{-1}r(I)$, then $a^n \in I$ and $s^n \in S$ by multiplicative closure. So $(a/s)^n \in S^{-1}I$. Hence $a/s \in r(S^{-1}I)$. □

Proposition 4.15. Let $S$ be a multiplicatively closet subset of $R$, and let $Q$ be a $P$-primary ideal.

1) If $S \cap P \neq \emptyset$, then $S^{-1}Q = S^{-1}R$.

2) If $S \cap P = \emptyset$, then $S^{-1}Q$ is $S^{-1}P$-primary and its contraction in $R$ is $Q$.

Proof. 1) If $s \in S \cap P$, then $s^n \in S \cap Q$ (because $Q$ is $P$-primary and $s^n \in S$ by multiplicative closure). Now, $s^n/1 \in S^{-1}Q$ and $1/s^n \in S^{-1}R$ so that $(s^n/1) \cdot (1/s^n) = 1/1$ and therefore $s^n/1$ is a unit of $S^{-1}R$. Hence $S^{-1}Q = S^{-1}R$.

2) If $S \cap P = \emptyset$, then for $s \in S$ and $a \in R$, $as \in Q$ implies $a \in Q$ (since $as \in Q$ implies $a \in Q$ or $s^n \in Q$, but $s^n \in S$, so $s^n \notin Q$ and $a \in Q$). Also, by Proposition
Proposition 4.13. \( Q^c = \bigcup_{s \in S} (Q : s) = \{ y \in R : ys \in Q \} \). So \( \bigcup_{s \in S} (Q : s) \) consists precisely of the elements of \( Q \) so that \( Q^c = Q \). Indeed, \( Q \subseteq Q^c \) from Proposition 4.10i and if \( x \in Q^c = \bigcup_{s \in S} (Q : s) \), then \( xs \in Q \) and from above, \( x \in Q \). From Proposition 4.14, we also get \( r(Q^c) = r(S^{-1}Q) = S^{-1}r(Q) = S^{-1}P \). The verification that \( S^{-1}Q \) is primary is as follows: \( Q^c = S^{-1}Q \). Let \( Q \) be primary and let \( x, y \in S^{-1}R \). Then \( x = a/b \) and \( y = c/d \) for some \( a, b, c, d \in R \), \( c, d \in S \). If \( a/b \cdot c/d \in S^{-1}Q \) then \( ac \in Q \), so that \( a \in Q \) or \( c^n \in Q \) and \( bd \in S \). Now \( d/1 \in S^{-1}R \) and since \( S^{-1}Q \) is an ideal, \( a/bd \cdot d/1 = a/b \in S^{-1}Q \). Similarly, if \( c^n \in Q \), \( c^n/b \cdot d/b^{n-1} = c^n/b^n = (c/c)^n \in S^{-1}Q \). Hence \( S^{-1}Q \) is primary.

For any ideal \( I \) and any multiplicatively closed subset \( S \subseteq R \), we will denote the contraction in \( R \) of the ideal \( S^{-1}I \) as \( S(I) \).

**Proposition 4.16.** Let \( S \) be a multiplicatively closed subset of \( R \) and let \( I \) be a decomposable ideal. Let \( I = \bigcap_{i=1}^{n} Q_i \) be a minimal primary decomposition of \( I \). Let \( P_i = r(Q_i) \) and suppose the \( Q_i \) are numbered so that \( S \) meets \( P_{m+1}, \ldots, P_n \) but not \( P_1, \ldots, P_m \). Then \( S^{-1}I = \bigcap_{i=1}^{m} S^{-1}Q_i \) and \( S(I) = \bigcap_{i=1}^{m} Q_i \) and these are minimal primary decompositions.

**Proof.** \( S^{-1}I = \bigcap_{i=1}^{n} S^{-1}Q_i = \bigcap_{i=1}^{m} S^{-1}Q_i \) (by Propositions 4.14 and 4.15) and \( S^{-1}Q_i \) is \( S^{-1}P_i \)-primary for \( i = 1, \ldots, m \). Since the \( P_i \) are distinct, so are the \( S^{-1}P_i \), \( 1 \leq i \leq m \). Hence we have a minimal primary decomposition. Contracting both sides, we get \( S(I) = (S^{-1}I)^c = \bigcap_{i=1}^{m}(S^{-1}Q_i)^c = \bigcap_{i=1}^{m} Q_i \) by Proposition 4.15ii. \( \square \)

### 4.4 Second Uniqueness Theorem

**Definition 4.17.** A set \( \Sigma \) of prime ideals belonging \( I \) is said to be isolated if it satisfies the following conditions: If \( P' \) is a prime ideal belonging to \( I \) and \( P' \subseteq P \) for some \( P \in \Sigma \), then \( P' \in \Sigma \).

**Proposition 4.18.** Let \( \Sigma \) be an isolated set of prime ideals belonging to \( I \) in a ring \( R \), and let \( S = R - \bigcup_{P \in \Sigma} P \). Then \( S \) is multiplicatively closed and for any prime ideal \( P' \) belonging to \( I \), we have \( P' \in \Sigma \Rightarrow P' \cap S = \emptyset \). 

\[ P' \notin \Sigma \Rightarrow P' \notin \bigcap_{P \in \Sigma} P \Rightarrow P' \cap S \neq \emptyset. \]

**Proof.** Let \( 1 \notin P \) for any prime ideal \( P \in \Sigma \), so that \( 1 \in S = R - \bigcup_{P \in \Sigma} P \). Let \( a, b \in S \) which implies \( a, b \notin P \) for all \( P \in \Sigma \). If \( ab \in \bigcup_{P \in \Sigma} P \), then \( ab \notin P \) for some \( P \in \Sigma \). Since \( P \) is prime, we get \( a \in P \) or \( b \in P \), a contradiction. Therefore, we must have \( ab \notin P \) for all \( P \in \Sigma \). Hence \( ab \notin \bigcup_{P \in \Sigma} P \). We must have \( ab \in S \). So \( S \) is multiplicatively closed. It is obvious that if \( P' \in \Sigma \), then \( P' \cap S = \emptyset \) since \( P' \subseteq \bigcup_{P \in \Sigma} P \) and \( S = R - \bigcup_{P \in \Sigma} P \). Finally, \( P' \notin \Sigma \) implies \( P' \notin \bigcap_{P \in \Sigma} P \) by Lemma 4.4. Hence \( P' \cap S \neq \emptyset \). \( \square \)

**Definition 4.19.** Let \( \Sigma \) be a set of prime ideals of a ring \( R \). Then \( P \) is **minimal** in \( \Sigma \) if \( P \in \Sigma \) and if there is no prime ideal \( P' \in \Sigma \) such that \( P' \subset P \).

**Theorem 4.20.** Let \( I \) be a decomposable ideal, let \( I = \bigcap_{i=1}^{n} Q_i \) be a minimal primary decomposition of \( I \), and let \( \{P_{i_1}, \ldots, P_{i_m}\} \) be an isolated set of prime ideals of \( I \). Then \( Q_{i_1} \cap \cdots \cap Q_{i_m} \) is independent of the decomposition.

In particular:

**Corollary 4.21.** The isolated primary components (i.e., the primary components \( Q_i \) corresponding to minimal prime ideals \( P_i \)) are uniquely determined.

**Proof.** Let \( I = \bigcap_{i=1}^{n} Q_i = \bigcap_{j=1}^{m} \tilde{Q}_j \) be two minimal primary decompositions of \( I \), \( \{P_{i_1}, \ldots, P_{i_t}\} \) be an isolated set of prime ideals belonging to \( I \), and \( S = R - P_{i_1} \cup \cdots \cup P_{i_t} \). Since the \( P_{i_k} \) are uniquely determined, there are \( Q_i \) and \( \tilde{Q}_j \) such that \( r(Q_i) = r(\tilde{Q}_j) = P_{i_k} \). We may reindex so that \( r(Q_{i_k}) = r(\tilde{Q}_{j_k}) = P_{i_k} \). By Proposition 4.18, \( S \) is multiplicatively closed and \( S(I) = Q_{i_1} \cap \cdots \cap Q_{i_t} = \tilde{Q}_{j_1} \cap \cdots \cap \tilde{Q}_{j_t} \) by Proposition 4.16 as desired.

For the proof of the corollary, for any minimal prime \( P_k \) belonging to \( I \), the set \( \{P_k\} \) containing just the ideal \( P_k \) is an isolated set. By the theorem, \( Q_k \) is independent of the decomposition. \( \square \)

**Example 4.22.** In \( k[x,y] \), \( I = (x^2, xy) = (x) \cap (x,y)^2 = (x) \cap (x^2, y) \) are reduced primary decompositions (Example 4.6). The set \( \{r(x) = (x)\} \) is isolated so that the ideal \( (x) \) is independent of any particular decomposition of \( I \).

**Example 4.23.** In the polynomial ring \( k[x,y,z] \), with \( P_1 = (x,y) \), \( P_2 = (x,z) \), \( M = (x,y,z) \) and \( I = P_1P_2 = (x^2, xy, xz, yz) \), we have seen that \( I = P_1 \cap P_2 \cap M^2 \) is a reduced...
primary decomposition (Example 3.26). The set \{(x, y), (x, z)\} is an isolated set so that 
\(P_1 \cap P_2\) is independent of any particular decomposition of \(I\) and the minimal primary 
components are \((x, y)\) and \((x, z)\).
Chapter 5

An Application of Unique Factorization

Sicherman dice [3]: Let us consider an ordinary pair of dice with faces labeled 1 through 6. The only way to roll a sum of 2 is to roll a 1 on each die. Since there are $6 \times 6$ different ways to combine the faces of the dice, the probability of rolling a sum of 2 is $1/36$. The probability of a sum of 3 is $2/36$; the probability of a sum of four is $3/36$ and so on. Other than 1 through 6, is there an alternative way to label the faces of a pair of dice so that the probability of rolling any particular sum is exactly the same as ordinary dice? This is the question that we will seek to answer in this section.

In the 1978 issue of Scientific American, Martin Gardner gave an alternative way of labeling the face of the dice which would yield the same probability of obtaining any particular sums as with ordinary dice. If we were to label the face of one cube with the integers 1,2,2,3,3,4 and the other with 1,3,4,5,6,8, (called the Sicherman dice) the probabilities of sums are indeed identical (that is 1/36 for 2, 2/36 for 3, and so on). We will derive the Sicherman dice and then use unique factorization in $\mathbb{Z}[x]$ to show that these are the only possible such labels besides 1 through 6.

First of all, let us observe how we may obtain a sum of say, 5 with an ordinary pair of dice. The possibilities are as follows: (1,4), (2,3), (3,2), and (4,1). Thus there are 4 possibilities. Let let us now observe the product of two polynomials having the labels
of the ordinary dice as exponents:

\[(x^6 + x^5 + x^4 + x^3 + x^2 + x)(x^6 + x^5 + x^4 + x^3 + x^2 + x).\]

If we look at the coefficient of \(x^5\) in the product, we will notice that it is 4 and we pick up the term \(x^5\) in precisely the following ways: \(x^4 \cdot x^1, x^3 \cdot x^2, x^2 \cdot x^3,\) and \(x^1 \cdot x^4\). Notice that there is a correspondence between the pairs of labels whose sum is 5 and the pairs of terms whose product is \(x^5\). This correspondence holds for all sums and all dice. Now let \(a_1, a_2, a_3, a_4, a_5, a_6\) and \(b_1, b_2, b_3, b_4, b_5, b_6\) be any two possible positive integer labels for a pair of dice, with the restriction that the possibility of rolling any particular sum be the same as that of ordinary dice. Utilizing our observation about dice labels and the product of polynomials, we have

\[(x^6 + x^5 + x^4 + x^3 + x^2 + x)(x^6 + x^5 + x^4 + x^3 + x^2 + x) = (x^{a_1} + x^{a_2} + x^{a_3} + x^{a_4} + x^{a_5} + x^{a_6})(x^{b_1} + x^{b_2} + x^{b_3} + x^{b_4} + x^{b_5} + x^{b_6}).\]

Solving the equation for \(a\)'s and \(b\)'s will give us our desired dice labels. Now we will utilize unique factorization in \(\mathbb{Z}[x]\). The polynomial \((x^6 + x^5 + x^4 + x^3 + x^2 + x)\) factors uniquely into irreducible components as

\[x(x + 1)(x^2 + x + 1)(x^2 - x + 1)\]

so that

\[(x^6 + x^5 + x^4 + x^3 + x^2 + x)(x^6 + x^5 + x^4 + x^3 + x^2 + x)\]

has the following irreducible factorization:

\[x^2(x + 1)^2(x^2 + x + 1)^2(x^2 - x + 1)^2.\]

By Theorem 3.32 we know that these factors are the only possible irreducible factors of \(P(x) = x^{a_1} + x^{a_2} + x^{a_3} + x^{a_4} + x^{a_5} + x^{a_6}\). Thus we have

\[P(x) = x^9(x + 1)^7(x^2 + x + 1)^4(x^2 - x + 1)^u,\]

where \(0 \leq q, r, t, u \leq 2\). To further restrict our possibilities for \(q, r, t,\) and \(u\), we evaluate \(P(1)\):

\[P(1) = (1^{a_1} + 1^{a_2} + 1^{a_3} + 1^{a_4} + 1^{a_5} + 1^{a_6}) = 6 = 1^22^33^11^u.\]
So \( r = 1 \) and \( t = 1 \). Similarly, evaluating \( P(0) \) yields

\[
P(0) = 0^q \cdot 1 \cdot 1^u
\]

so that \( q \neq 0 \). On the other hand, if \( q = 2 \), \( P(x) \) becomes

\[
x^2(x + 1)(x^2 + x + 1)(x^2 - x + 1)^u = (x^5 + 2x^4 + 2x^3 + x^2)(x^2 - x + 1)^u.
\]

Observing this equation, we can see that regardless of our choice of \( u \), the smallest degree that \( x \) can have is 2. Since the degree on \( x \) corresponds to the number on the face of a die, the smallest possible sum that one could roll with two dice would be 3. This results in a violation of our assumption because there is no way to get a sum of two. Thus the only remaining possibility is that \( q = 1 \). We now have \( q = r = t = 1 \) and \( u = 0, 1, 2 \). Let us consider each of these possibilities for \( u \).

1. When \( u = 0 \), \( P(x) = x(x + 1)(x^2 + x + 1) = x^4 + x^3 + x^2 + x^2 + x \), so the die labels are 4, 3, 3, 2, 2, 1 which is a Sicherman die.

2. When \( u = 1 \), \( P(x) = x(x + 1)(x^2 + x + 1)(x^2 - x + 1) = x^6 + x^5 + x^4 + x^3 + x^2 + x \), so the die labels are 6, 5, 4, 3, 2, 1, which is an ordinary die.

3. When \( u = 2 \), \( P(x) = x(x + 1)(x^2 + x + 1)(x^2 - x + 1)^2 = x^8 + x^6 + x^5 + x^4 + x^3 + x \), so the die labels are 8, 6, 5, 4, 3, 1, which is the other Sicherman die.

This proves that the Sicherman die give the same probabilities as ordinary dice and that they are the only other pair of dice that do so.

We will now consider the question of rolling \( n \) (\( n > 2 \)) ordinary dice with each labeled 1 through 6. Again we will show that the only possible labels are 1 through 6 and the Sicherman labels. The manner in which we represent a pair of dice is analogous to the way in which we represent \( n \) dice:

\[
(x^6 + x^5 + x^4 + x^3 + x^2 + x)(x^6 + x^5 + x^4 + x^3 + x^2 + x) \cdots (x^6 + x^5 + x^4 + x^3 + x^2 + x)
\]

\[
= (x^{a_1} + x^{a_2} + x^{a_3} + x^{a_4} + x^{a_5} + x^{a_6})(x^{a_2} + x^{a_3} + x^{a_4} + x^{a_5} + x^{a_6})
\]

\[
\cdots (x^{a_1} + x^{a_2} + x^{a_3} + x^{a_4} + x^{a_5} + x^{a_6})
\]
Again the polynomial \((x^6 + x^5 + x^4 + x^3 + x^2 + x)\) factors uniquely into irreducible components as
\[
x(x + 1)(x^2 + x + 1)(x^2 - x + 1)
\]
so that left hand side of the equation has the following irreducible factorization:
\[
x^2(x + 1)^n(x^2 + x + 1)^n(x^2 - x + 1)^n.
\]
By Theorem 3.32, these are the only possible factors for \(P(x) = (x^{a_1} + x^{a_2} + x^{a_3} + x^{a_4} + x^{a_5} + x^{a_6})\). Thus \(P(x)\) is of the form
\[
x^2(x + 1)^r(x^2 + x + 1)^t(x^2 - x + 1)^u
\]
where \(0 \leq q, r, t, y \leq n\). The justification that \(r = t = 1\) is the same as that of having a pair of dice. What about \(q\)? Again, evaluating \(P(0)\) in two ways as before shows that \(q \neq 0\). Also as before, if \(q \geq 2\), the smallest possible sum we could get is \(n + 1\) so that there is no way to get a sum of \(n\) which corresponds to rolling all 1s with ordinary dice. So we have now reduced our possibilities to \(q = r = t = 1\) and \(u = 0, 1, 2, \cdots, n\). We already know that \(u = 0, 1, 2\) yields the Sicherman dice and the ordinary die. What about \(u > 2\)? In general,
\[
x(x + 1)(x^2 + x + 1)(x^2 - x + 1)^u = (x^4 + 2x^3 + 2x^2 + x)(x^2 - x + 1)^u
\]
\[
= (x^4 + 2x^3 + 2x^2 + x)(x^{2u} - ux^{2u-1} + \cdots)
\]
\[
= x^{2u+4} + (2 - u)x^{2u+3} + \cdots
\]
Thus \(P(x)\) has \((2 - u)x^{2u+3}\) as one of its terms. When \(u > 2\), the coefficient of this term will be negative. Since the coefficient of \(2u - 3\) represents the number of faces of the die with the label \(2u - 3\), this number cannot be negative. Thus, \(u \leq 2\). We have again showed that the only possibilities besides the ordinary pair of dice are the Sicherman dice.

Does this result mean that a pair of Sicherman dice may always be substituted for a pair of ordinary dice? Although the probability of rolling a particular sum is the same with either the Sicherman dice or regular dice is the same, the probability of rolling doubles is severely affected. With regular dice, the probability of rolling a double is \(6/36 = 1/6\). With the Sicherman dice, the probability of rolling a double is \(4/36 = 1/9\).
Thus if a game like monopoly were played with a pair of Sicherman dice, the probability of landing on various properties would be different. For instance, since getting out of jail requires rolling doubles, you might find yourself serving longer jail terms if playing with Sicherman dice. Once in jail, there is also no way to land in Virginia by rolling a pair of 2s with Sicherman dice. However, the probability of landing on St. James with a pair of 3s is twice as likely with Sicherman dice since there are two ways to roll a pair of 3s.
Chapter 6

Conclusion

I was first introduced to this topic on seeing a simple example of an element of a ring which did not factor uniquely into a product of irreducibles: in $\mathbb{Z}[\sqrt{-5}], 6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 + \sqrt{-5})$. I wanted to know why some rings maintained this property while others did not. I did not expect this apparently simple question to be so rich in its history and to have had such a profound contribution in the field of commutative algebra. We have seen how the concept of unique factorization led to the development of many of the objects we now associate with commutative algebra. Emmy Noether made this theory more elegant by introducing chain conditions. In conclusion, a ring is a unique factorization domain if it satisfies the ascending chain condition on principal ideals and if every irreducible element is prime. Dedekind, Lasker, and others helped to develop the theory of primary decomposition. Thus they provided a generalization of the Fundamental Theorem of Arithmetic.
Bibliography


