Factorization of Ideals

William M. Faucette

University of West Georgia

Summer 2021

1. The Fundamental Theorem of Arithmetic
2. What is a Unique Factorization Domain?
3. Prime Elements and Irreducible Elements
4. Prime Elements Are Irreducible
5. When are Irreducible Elements Always Prime?
6. A Ring That is Not a UFD
7. Generalized Notion of Factoring
8. Associated Prime Ideals
9. Primary Decomposition
10. Noetherian Rings
11. A Pause for History
12. Existence of Primary Decompositions
13. Uniqueness Theorems
14. Intersections and Products of Ideals
15. Integral Elements and Integral Closure

The Fundamental Theorem of Arithmetic

One of the most fundamental results of the natural numbers is the Fundamental Theorem of Arithmetic:

Theorem (Fundamental Theorem of Arithmetic)

Every integer greater than 1 can be written in the form

$$p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$$

where $n_i \geq 0$ and the p_i's are distinct primes. The factorization is unique, except possibly for the order of the factors.

The Fundamental Theorem of Arithmetic

There is a straightforward generalization of this theorem to a property possessed by large class of commutative rings.

These rings are called **unique factorization domains**.

What is a Unique Factorization Domain?

Definition

A **unique factorization domain (UFD)** is an integral domain in which every non-zero non-unit element can be written as a product of prime elements (or irreducible elements), uniquely up to order and units.

Recall that an integral domain is a nontrivial commutative ring in which the product of any two nonzero elements is nonzero.

What is a Unique Factorization Domain?

Examples of integral domains include the ring of integers, $\mathbb{Z}$, the ring of polynomials in one variable over a field k, $k[X]$, and the ring of polynomials in n variables over a field, $k[X_1, \ldots, X_n]$.

These examples are some pretty important rings.

What is a Unique Factorization Domain?

In order to make sense of this definition, we need to define two terms. First, we need to know what a prime element is. Second, we need to know what an irreducible element is.

These are both generalizations of the notion of prime numbers in the set of natural numbers.

Prime Elements and Irreducible Elements

In the ring of integers or in the ring of polynomials with coefficients in some field, there are two distinct properties which can serve as definitions of a prime number.

1. If p is prime, then p divides ab implies p divides a or p divides b.
2. If p is prime, then $p = ab$ implies that either a or b is a unit.

However, in a general integral domain, these two properties are not equivalent.

So, we will define two terms to refer to elements with the two properties.

Prime Elements and Irreducible Elements

Prime elements in a commutative ring correspond to prime numbers in the set of natural numbers and to irreducible polynomials in polynomial rings.

Definition

An element p in a commutative ring R is a **prime element** or is **prime** if p is nonzero, not a unit, and whenever p divides the product ab for a, $b \in R$, then either p divides a or p divides b.

Prime Elements and Irreducible Elements

On the other hand, there are **irreducible elements**.

Definition

An element a in an integral domain R is an **irreducible element** or is **irreducible** if there is no way to factor a in R into two factors that are nonunits. That is, if $a = bc$ with $b, c \in R$, then b or c is a unit in R.

Notice that irreducible elements are only defined for integral domains, whereas prime elements are defined for all commutative rings.

Prime Elements and Irreducible Elements

In the ring of natural numbers and in polynomial rings, these two terms are equivalent. Every prime element is irreducible and irreducible element is prime.

In general, they are not equivalent. The equivalence of these two terms is the determining factor (pardon the pun) in whether a ring is a UFD.

Prime Elements Are Irreducible

We do have the following theorem:

Theorem

In an integral domain R, every prime element is irreducible.

Prime Elements Are Irreducible

Proof.

Let $p \in R$ be a prime element and suppose $p = ab$ for some elements a, $b \in R$. To show p is irreducible, we must show that a or b is a unit.

Since p is prime and p divides ab (which after all is p itself), p divides a or p divides b.

If p divides a, then p divides a and a divides $p = ab$, so b is a unit.

If p divides b, then p divides b and b divides $p = ab$, so a is a unit.

This shows p is irreducible. □

When are Irreducible Elements Always Prime?

So, the question of whether an integral domain is a unique factorization domain boils down to this: Is every irreducible element a prime element?

A Ring That is Not a UFD

Example

This should actually be called a nonexample. Look at the number 6 in the integral domain

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}.$$

In this ring, $6 = 2 \cdot 3$ and 2 and 3 are prime.

However, $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, and $1 \pm \sqrt{-5}$ are also prime.

So in this integral domain we do not have unique factorization into primes.

Generalized Notion of Factoring

Since the Fundamental Theorem of Arithmetic—the ability to factor natural numbers into a product of primes—is rather important, we need some way to generalize this to rings that do not have unique factorization of elements.

Generalized Notion of Factoring

Prussian mathematician Ernst Kummer (1810–1893) then asked the following question:

Is it possible to take a ring in which one doesn't have unique factorization and introduce "ideal prime numbers" outside the given number system in order to recover unique factorization?

That is, can we find a somewhat larger ring in which unique factorization is possible?

Generalized Notion of Factoring

To make a very long story very short, Kummer, Leopold Kronecker (1823–1891), and Richard Dedekind (1831–1916), introduced the notions of an ideal and a prime ideal in a ring.

So, instead of factoring elements, we ask if we can factor ideals uniquely into a product of prime ideals.

Primary Ideals

We need a concept for ideals analogous to a power of a prime for natural numbers.

Definition

An ideal $\mathfrak{q}$ in a commutative ring R is a **primary ideal** if whenever $ab \in \mathfrak{q}$, either $a \in \mathfrak{q}$ or some power of b is in $\mathfrak{q}$. That is, either $a \in \mathfrak{q}$ or $b^n \in \mathfrak{q}$ for some natural number n.

This can be restated as follows: An ideal $\mathfrak{q}$ in a commutative ring R is a primary ideal if every zero-divisor in the quotient ring $R/\mathfrak{q}$ is nilpotent.

Primary Ideals

Example

In the ring of integers, the primary ideals are the principal ideals (p^n) for $n \in \mathbb{N}$.

If $ab \in (p^n)$, then p must divide ab n times.

If $p^n \nmid a$, then p must divide b. So, if $a \notin (p^n)$, then $p \mid b$. In this case, $b^n \in (p^n)$.

If $p^n \nmid b$, then p must divide a. So, if $b \notin (p^n)$, then $p \mid a$. In this case, $a^n \in (p^n)$.

Associated Prime Ideals

Definition

Let $\mathfrak{a}$ be an ideal in a commutative ring R. The **radical** of $\mathfrak{a}$ is the set of elements of R which have some power in $\mathfrak{a}$. That is

$$\operatorname{rad}(\mathfrak{a}) = \{x \in R \mid x^n \in \mathfrak{a} \text{ for some } n \in \mathbb{N}\}.$$

The radical of an ideal is also an ideal in R.

The radical of a primary ideal $\mathfrak{q}$ is a prime ideal $\mathfrak{p}$. We say $\mathfrak{q}$ is **$\mathfrak{p}$-primary**. The prime ideal $\mathfrak{p}$ is the **prime ideal associated to** $\mathfrak{q}$.

Primary Decomposition

We are going to investigate the representation of an ideal not as a product, but as an intersection of primary ideals.

Definition

A **primary decomposition** of an ideal $\mathfrak{a}$ in R is an expression of $\mathfrak{a}$ as a finite intersection of primary ideals, say

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i .$$

Primary Decomposition

Definition

A primary decomposition is **minimal** if

1. the associated primes of the primary ideals are all distinct and
2. no primary ideal in the decomposition contains the intersection of the remaining primary decomposition.

If an ideal has a primary decomposition, then it always has a minimal primary decomposition.

Noetherian Rings

Not every ring has the property that every ideal has a primary decomposition, but a large category of very important rings has this property.

These are the Noetherian rings. This class of rings is named after one of the few women mathematicians of her age, Emmy Noether (1882–1935).

A Pause for History

Emmy Noether, born in the Bavarian town of Erlangen in the German Empire, originally planned to teach French and English after passing the required examinations, but instead studied mathematics at the University of Erlangen, where her father, mathematician Max Noether, lectured.

After completing her doctorate in 1907 under the supervision of Paul Gordan, she worked at the Mathematical Institute of Erlangen without pay for seven years. At the time, women were largely excluded from academic positions.

In 1915, she was invited by David Hilbert and Felix Klein to join the mathematics department at the University of Göttingen, a world-renowned center of mathematical research. The philosophical faculty objected, however, and she spent four years lecturing under Hilbert's name.

Noetherian Rings

Definition

A commutative ring R is called **Noetherian** or is a **Noetherian ring** if it satisfies any of the following equivalent properties:

1. Every ideal in R is finitely generated.
2. Every ascending chain of ideals is stationary.
3. Every nonempty set of ideals contains a maximal element.

Noetherian Rings

Many important rings are Noetherian rings and the Noetherian property is exactly the finiteness condition that makes many important theorems work.

Examples

1. Any field, including the rational numbers, the real numbers, and the complex numbers
2. Any principal ideal domain, which includes the ring of integers and the ring of polynomials in one variable
3. The ring of polynomials in finitely many variables over a field
4. Any finitely generated algebra over a field

Existence of Primary Decompositions

Theorem

In a Noetherian ring R, every ideal has a primary decomposition.

First Uniqueness Theorem

Theorem (First Uniqueness Theorem)

Let $\mathfrak{a}$ be a decomposable ideal and let $\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{q}_i$ be a minimal primary decomposition of $\mathfrak{a}$. Let $\mathfrak{p}_i = \operatorname{rad}(q_i)$ $(1 \leq i \leq n)$. Then $\mathfrak{p}_i$ are precisely the prime ideals which occur in the set of ideals $\operatorname{rad}(a : x)$ for $x \in A$, and hence are independent of the particular decomposition or $\mathfrak{a}$.

This says the prime ideals associated to an ideal $\mathfrak{a}$ do not depend on the primary decomposition.

Isolated Set of Prime Ideals

Definition

A set Σ of prime ideals belong to $\mathfrak{a}$ is said to be **isolated** if it satisfies the following condition:

If $\mathfrak{p}'$ is a prime ideal belonging to $\mathfrak{a}$ and $\mathfrak{p}' \subseteq \mathfrak{p}$ for some $\mathfrak{p} \in \Sigma$, then $\mathfrak{p}' \in \Sigma$.

Second Uniqueness Theorem

Theorem (Second Uniqueness Theorem)

Let $\mathfrak{a}$ *be a decomposable ideal and let* $\mathfrak{a} = \cap_{i=1}^{n}\mathfrak{q}_i$ *be a minimal primary decomposition of* $\mathfrak{a}$*. Let* $\{\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_m}\}$ *be an isolated set of prime ideals of* $\mathfrak{a}$*. Then* $\mathfrak{q}_{i_1} \cap \cdots \cap \mathfrak{q}_{i_m}$.

Corollary

The isolated primary components (i.e, the primary components $\mathfrak{q}_i$ *corresponding to minimal prime ideals* $\mathfrak{p}_i$*) are uniquely determined by* $\mathfrak{a}$*.*

This says the primary components belonging to the minimal prime ideals of $\mathfrak{a}$ are independent of the decomposition.

Intersections and Products of Ideals

We would like some way of relating intersections of ideals with products of ideals.

If $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals in a ring R, we have

$$\begin{aligned}(\mathfrak{a}+\mathfrak{b})(\mathfrak{a}\cap\mathfrak{b}) &= \mathfrak{a}(\mathfrak{a}\cap\mathfrak{b})+\mathfrak{b}(\mathfrak{a}\cap\mathfrak{b})\\ &\subseteq \mathfrak{a}\mathfrak{b}\subseteq\mathfrak{a}\cap\mathfrak{b}.\end{aligned}$$

So, if two ideals have the property that $\mathfrak{a}+\mathfrak{b}=(1)$, then

$$\mathfrak{a}\cap\mathfrak{b}=\mathfrak{a}\mathfrak{b}.$$

Intersections and Products of Ideals

Two ideals $\mathfrak{a}$, $\mathfrak{b}$ are **coprime** (or **comaximal**) if $\mathfrak{a} + \mathfrak{b} = (1)$.

So, for coprime ideals $\mathfrak{a}$, $\mathfrak{b}$, we have

$$\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}.$$

Intersections and Products of Ideals

An integral domain has **dimension 1** if every nonzero prime ideal is maximal.

Examples are the integers and the ring of polynomials in one variable over a field.

Intersections and Products of Ideals

In an integral domain A of dimension 1, for any two nonzero prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are coprime. That is,

$$\mathfrak{p}_1 + \mathfrak{p}_2 = A.$$

For nonzero prime ideals in an integral domain A of dimension 1,

$$\mathfrak{p}_1 \cap \mathfrak{p}_2 = \mathfrak{p}_1 \mathfrak{p}_2.$$

Intersections and Products of Ideals

If $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are primary ideals with associated prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ which are coprime, then $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are also coprime.

For primary ideals in this instance

$$\mathfrak{q}_1 \cap \mathfrak{q}_2 = \mathfrak{q}_1 \mathfrak{q}_2.$$

So, if the associated prime ideals are coprime, so are their primary ideals.

This property allows us to convert intersections of primary ideals into products of primary ideals.

Intersections and Products of Ideals

Proposition

Let A be a Noetherian domain of dimension 1. Then every non-zero ideal $\mathfrak{a}$ in A can be uniquely expressed as a product of primary ideals whose radicals are all distinct.

Integral Elements and Integral Closures

Let A be a subring of a ring B. An element $x \in B$ is **integral** over A is x is a root of a monic polynomial with coefficients in A, that is, if x satisfies an equation of the form

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0,$$

with $a_1, \ldots, a_n$ in A.

The set of all elements in B integral over A is the **integral closure** of A in B.

The integral closure of A in B is a subring of B containing A.

Integral Elements and Integral Closure

If A is an integral domain with field of fractions K, we say A is **integrally closed** if it is integrally closed in K.

The domain of integers $\mathbb{Z}$ is integrally closed. This means every rational root of a monic polynomial with integer coefficients is itself an integer.

The truly frightening part of this is that you learned this in MATH 1113.

A Reminder of Precalculus

Theorem (The Rational Zeroes Theorem)

Any rational root of a polynomial with integer coefficients must be of the form p/q where p is a factor of the constant term and q is a factor of the leading coefficient.

If the polynomial is monic, the leading coefficient is 1, so $q = \pm 1$. This means the rational root p/q is an integer.

So, any rational number that is a root of a monic polynomial with integer coefficients must be an integer. This says $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$.

Dedekind Domains

Definition (Dedekind Domain)

A Dedekind domain in an integrally closed, Noetherian integral domain of dimension 1.

Dedekind Domains

Theorem

In a Dedekind domain, every primary ideal is the power of a prime ideal.

This means that in a Dedekind domain, every ideal can be factored as a product of prime ideals. That is what we're looking for.

Integers in a Number Field

A **number field** is a finite extension field of the rational numbers.

An element in a number field is an **(algebraic) integer** if it is a root of a monic polynomial with integer coefficients.

Integers in a Number Field

Theorem

If K is a number field and $\mathcal{O}_K$ is the ring of algebraic integers in K, then $\mathcal{O}_K$ is a Dedekind domain.

In particular, this means in any ring of algebraic integers, we can factor every ideal uniquely into a product of prime ideals, up to order of factors.

This generalizes the Fundamental Theorem of Arithmetic.

A Note of Thanks

Thank you for attending.