

California State University, San Bernardino

CSUSB ScholarWorks

Theses Digitization Project

John M. Pfau Library

2012

Closure operations in commutative rings

Chloette Joy Samsam

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



Part of the [Algebraic Geometry Commons](#)

Recommended Citation

Samsam, Chloette Joy, "Closure operations in commutative rings" (2012). *Theses Digitization Project*. 4179.

<https://scholarworks.lib.csusb.edu/etd-project/4179>

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.

CLOSURE OPERATIONS IN COMMUTATIVE RINGS

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

Chloette Joy Samsam

September 2012

CLOSURE OPERATIONS IN COMMUTATIVE RINGS

A Thesis

Presented to the

Faculty of

California State University,


San Bernardino

by


Chloette Joy Samsam

September 2012


Approved by:

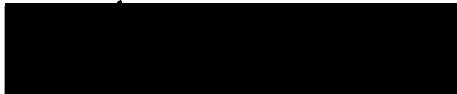

Dr. Laura Wallace, Committee Chair

8/28/12
Date


Dr. J. Paul Vicknair, Committee Member


~~Dr.~~ James Okon, Committee Member


Dr. Peter Williams, Chair,
Department of Mathematics


Dr. Charles Stanton
Graduate Coordinator,
Department of Mathematics

ABSTRACT

A well known concept in mathematics is that of the algebraic closure of a field. The algebraic closure of a field K is the smallest algebraically closed extension field containing K . For example, by the Fundamental Theorem of Algebra, the algebraic closure of the field of real numbers \mathbb{R} is the field of complex numbers \mathbb{C} . By first looking at the algebraic closure of a field we discuss certain properties of algebraic closure that can be extended to the integral closure of a ring and integral closure of ideals in a ring. Analogous to algebraic closure, the integral closure of a ring R is the smallest integrally closed extension of a ring containing R . For example, the ring of integers \mathbb{Z} is integrally closed in the field of rational numbers \mathbb{Q} . Other characterizations and properties of integral closure of a ring and integral closure of ideals provide us with background information to examine the more general notion of closure operations on ideals and discuss other types of closures.

ACKNOWLEDGEMENTS

First of all, I would like to thank my professors at CSUSB. I have learned so much from all of you and I am very appreciative of the work you do. I would like to thank my committee members Dr. Vicknair and Dr. Okon for their advice and help on my thesis. Furthermore, a very special thanks goes out to my advisor, Dr. Wallace. Thank you for all your attention, guidance and patience throughout my graduate career. I have learned many new and interesting concepts from our work together; thank you for sharing your knowledge with me. Secondly, I would like to thank all my friends and everyone at CSUSB who have made these years so memorable. It was an honor working and studying with all of you.

Last but not least, I would like to thank my family. You have always been there to support and encourage me every step of the way. My heartfelt gratitude goes to my parents and brother who have been so generous and loving. I love you! I consider myself blessed to have come this far and I couldn't have accomplished any of this without your love and support.

Table of Contents

Abstract	iii
Acknowledgements	iv
1 Introduction	1
2 Foundational Concepts	3
2.1 Concepts in Ring Theory	3
2.2 Modules	18
3 Algebraic Closure	23
3.1 Field Extensions	23
3.2 Algebraic Extensions	27
4 Integral Closure	31
4.1 Ring/Integral Extensions	31
4.2 Applications of Integral Closure: Dedekind Domains	39
5 Integral Closure of an Ideal	45
5.1 Definitions	45
5.2 Theorems	46
6 Closure Operations	53
6.1 General Closure Operations on Ideals	53
6.2 Corresponding Ring Closures	57
7 Conclusion	61
Bibliography	63

Chapter 1

Introduction

The most familiar and often most popular types of closures in commutative algebra are the algebraic closure of a field and the integral closure of a ring. The algebraic closure of a field is an important topic because of its ties to the Fundamental Theorem of Algebra. This theorem tells us that each polynomial with complex number coefficients has a solution in the complex numbers. The integral closure of a ring is also valuable to the study of mathematics and has come up in different branches of mathematics like number theory and algebraic geometry. It is a widely used concept because of its useful properties and characteristics. However, in the 1930's, the study of the integral closure of a ring was extended to include the ideals of a ring and modernized by Krull and Zariski [Swa89]. Thus, closure operations on ideals was formulated.

The goal of this paper is to survey different types of closures and closure operations on commutative rings and ideals. This paper will give an overview of closure operations, introduce their properties and make comparisons between closure operations of ideals and their ring counterparts.

The general arrangement of this paper is as follows. Some important fundamental concepts from commutative ring theory are first introduced. As well as common notation and basic examples. These theorems and definitions are used widely throughout the paper and are often referred back to. This chapter also includes information and theorems on modules. The next chapters examine algebraic closure and integral closure. These closures explore the concept of viewing elements from their respective fields or rings as roots of polynomials. Included in the chapter on the integral closure of rings is an ap-

plication with Dedekind domains. The main result illustrating the relationship between Dedekind domains and integral closure. As we analyze the structures and properties of these closures, we relate them to their corresponding ideal counterparts, introducing the notion of closure operations on ideals in rings in the subsequent chapters. The properties of the integral closure of an ideal are then generalized to any type of closure operation on an ideal.

Chapter 2

Foundational Concepts

This chapter gives some of the foundational requirements (definitions, theorems, etc.) needed to understand the proofs and theorems written in this paper. The terms and concepts in this section should be familiar to most undergraduate students studying courses in Abstract Algebra.

2.1 Concepts in Ring Theory

We are all familiar with the operations of multiplication and addition on sets of numbers, in fact, we use these operations on the first sets of numbers that we are introduced to like the integers and real numbers. An abstract concept that deals with these operations acting on sets is a ring.

Definition 2.1. A *ring with identity* R is a set with two binary operations, addition and multiplication, such that R is an Abelian group with respect to addition, multiplication is associative and both right and left distributive over addition, and R contains a multiplicative identity element 1_R (or simply 1) such that $1_R r = r = r 1_R$ for all $r \in R$.

If the multiplication in R is commutative, then we say that R is a *commutative ring*. The rings we study in this paper will be commutative rings.

Example (2.1.1). The set of integers, \mathbb{Z} , the set of rational numbers, \mathbb{Q} , and the set of real numbers, \mathbb{R} , are all commutative rings under ordinary addition and multiplication.

The next definition introduces a specific type of ring well-known in many algebra classes; the ring of polynomials.

Definition 2.2. Let R be a commutative ring. The set

$$R[x] = \{a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \mid a_i \in R, n \in \mathbb{N}\}$$

with the operations of polynomial addition and multiplication is called the *ring of polynomials over R* in the indeterminate x . If $a_n \neq 0$, then we say that the degree of the polynomial is n written as $\deg f(x) = n$.

Other specific types of rings include the integers, rational numbers and real numbers. These rings exhibit one special feature that rings in general don't have. They satisfy a property called cancellation. That is, if we let a, b, c be elements in one of these three rings, we can say that if $ab = ac$, then $b = c$. Thus, we present the terms *zero-divisor* and *integral domain* to classify these rings.

Definition 2.3. Let R be a commutative ring. A *zero-divisor* is an element $r \in R$ for which there exists $y \in R$ with $y \neq 0_R$ such that $ry = 0_R$. If R is non-trivial, then 0_R is a zero-divisor in R because $0_R 1_R = 0_R$.

Definition 2.4. Let R be a commutative ring. Then R is said to be an *integral domain* precisely when

- (i) R is not trivial, that is, $1_R \neq 0_R$ and
- (ii) 0_R is the only zero-divisor in R .

Example (2.4.1). A very familiar and basic example of an integral domain is the ring of integers, \mathbb{Z} . In the ring of integers, $1 \neq 0$ and 0 is the only zero-divisor. However, if we take a look at the ring \mathbb{Z}_{10} of residue classes of integers modulo 10, we see that it is not an integral domain because 0, 2, 4, 5, 6, and 8 are zero-divisors.

Example (2.4.2). If R is an integral domain, then the polynomial ring $R[x]$ is also an integral domain. This is shown in Theorem 2.5 below.

Theorem 2.5. *If R is an integral domain, then $R[x]$ is an integral domain.*

Proof. Let R be an integral domain, then $R[x]$ is a commutative ring by definition. We want to show that $R[x]$ has unity and no zero-divisors. The unity of R is 1, so $f(x) = 1$ is the unity of $R[x]$. Let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \neq 0 \text{ for } a_n \neq 0 \text{ and } a_i \in R \text{ and}$$

$$g(x) = b_mx^m + b_{m-1}x^{m-1} + \dots + b_1x + b_0 \neq 0 \text{ for } b_m \neq 0 \text{ and } b_i \in R.$$

Then

$$f(x)g(x) = (a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0)(b_mx^m + b_{m-1}x^{m-1} + \dots + b_1x + b_0).$$

If we show the leading coefficient of this product is not 0, then $f(x)g(x) \neq 0$. The leading coefficient of this product is a_nb_m . Since $a_n \neq 0$ and $b_m \neq 0$, we get $a_nb_m \neq 0$ because $a_n, b_m \in R$ and R is an integral domain. Thus $f(x)g(x) \neq 0$, and so $R[x]$ is an integral domain. \square

Within integral domains we distinguish another set of elements called *fields*. Fields are very important to the notion of algebraic closure (studied in the next chapter) because of their special attributes. We begin with the definition of *unit* which is used to define a field.

Definition 2.6. Let R be a commutative ring. A *unit* of R is an element $r \in R$ for which there exists $u \in R$ such that $ru = 1_R$. When $r \in R$ is a unit of R , then there is exactly one element $u \in R$ with the property that $ru = 1_R$; this element is called the inverse of r , and is denoted r^{-1} .

Definition 2.7. Let R be a commutative ring. Then we say that R is a *field* precisely when

- (i) R is not trivial and
- (ii) every non-zero element of R is a unit.

Example (2.7.1). Some common rings that are fields are the set of rational numbers \mathbb{Q} , the set of real numbers \mathbb{R} and the set of complex numbers \mathbb{C} . They are fields because every non-zero element of these rings is a unit. For $r \in \mathbb{R}$, $r^{-1} = \frac{1}{r}$ and for $a + bi \in \mathbb{C}$,

$$\begin{aligned} (a + bi)^{-1} &= \frac{1}{a + bi} \\ &= \frac{1}{a + bi} \cdot \frac{a - bi}{a - bi} \\ &= \frac{a - bi}{a^2 + b^2} \\ &= \frac{a}{a^2 + b^2} - \frac{bi}{a^2 + b^2}. \end{aligned}$$

Example (2.7.2). Another example is the ring \mathbb{Z}_p where p is prime. For $a \in \mathbb{Z}_p$, $a^{-1} = p - a$. In fact, every finite integral domain is a field (proof below).

Proof. Let $a \in D$ where D is a finite integral domain. Suppose that $a \neq 0$. If $a = 1$, then $a^{-1} = 1$, and so a is a unit. If $a \neq 1$, consider the set $\{a, a^2, \dots\} \subseteq D$. Since D is finite, there is some $a^i = a^j$ for $j < i$. Then $a^{i-j} = 1$ by cancellation, so a is a unit. Thus every non-zero element is a unit, and so D is a field. \square

Example (2.7.3). We can also say that every field is an integral domain since every non-zero element of a field is not a zero-divisor because it is a unit.

The succeeding theorem describes a very popular algorithm used in number theory with the ring of integers. We extend this concept to include polynomials with coefficients from a field. The proof for this theorem can be found in [Gal10].

Theorem 2.8 (Division Algorithm). *Let K be a field and let $f(x), g(x) \in K[x]$ with $g(x) \neq 0$. Then there exists unique polynomials $q(x)$ and $r(x)$ in $K[x]$ such that $f(x) = g(x)q(x) + r(x)$ and either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$.*

The next definition of an *ideal* is very significant to the study of ring theory. Ideals are an important substructure of a ring and are used to help identify characteristics of different types of rings for applications of ring theory. We will use them in our discussion of closure operations.

Definition 2.9. Let R be a commutative ring. A subset I of R is said to be an *ideal* of R precisely when the following conditions are satisfied:

- (i) $I \neq \emptyset$;
- (ii) $a + b \in I$ for all $a, b \in I$; and
- (iii) $ra \in I$ for all $a \in I$ and $r \in R$.

Example (2.9.1). For any ring R , $\{0\}$ and R are ideals of R . The ideal $\{0\}$ is called the trivial ideal.

Example (2.9.2). For any positive integer n , the set $n\mathbb{Z}$ (which can be described as the multiples of n) is an ideal of \mathbb{Z} .

We can think of ideals as elements from a subset of R that “absorbs” elements of R since $rI = \{ra \mid a \in I\}$. Certain ideals, like the ones listed below, require more attention because of their properties.

Definition 2.10. Let P be an ideal in a commutative ring R . We say that P is a *prime ideal* of R precisely when

- (i) $P \subset R$, that is, P is a proper ideal of R , and
- (ii) if $ab \in P$ for some $a, b \in R$, then either $a \in P$ or $b \in P$.

Example (2.10.1). Since prime ideals are proper subsets of a ring, the ring R itself is not considered to be a prime ideal of R . If we look at specific types of rings, like integral domains we see that the trivial ideal, $\{0\}$ is a prime ideal. This is not necessarily true in rings that are not integral domains because elements may be zero-divisors.

Example (2.10.2). The prime ideals of \mathbb{Z} are the ideals $n\mathbb{Z}$ where n is a prime number. For example, let us look at the multiples of 3: $3\mathbb{Z}$. Let ab be a multiple of 3, that is, $ab = 3n$ for $n \in \mathbb{Z}$. This means that $3|ab$. So $3|a$ or $3|b$ by Euclid's Lemma. Thus a and b are also multiples of 3, and hence $a \in 3\mathbb{Z}$ or $b \in 3\mathbb{Z}$.

Definition 2.11. Let R be a commutative ring and let $a \in R$. The set $aR = \{ar | r \in R\}$ is an ideal of R called the *principal ideal* of R generated by a . Principal ideals are also written as (a) and Ra .

Example (2.11.1). The prime ideal $3\mathbb{Z}$ given in Example 2.10.2 is a principal ideal and can also be written as (3) .

In the case of principal ideals, we only deal with one generator. That is, one element that generates the entire ideal. However, ideals can also have multiple generators. Ideals that are generated by a finite amount of elements are called *finitely generated ideals*.

Definition 2.12. Let $H \subseteq R$. We define the *ideal of R generated by H* , denoted by (H) , RH , or HR to be:

$$(H) = RH = HR = \left\{ \sum_{i=1}^n r_i h_i \mid n \in \mathbb{N}, r_i \in R, h_i \in H \right\}.$$

Example (2.12.1). Let us take a look at $(x, 2) \subseteq \mathbb{Z}[x]$. This is the ideal generated by x and 2 in the ring of polynomials with integer coefficients. Every element in this ideal is generated by a linear combination of x and 2. We can write $(x, 2) = \{x \cdot f + 2 \cdot g \mid f, g \in \mathbb{Z}[x]\}$. Basically, this generates the set of polynomials in $\mathbb{Z}[x]$ whose constant term is even. This ideal can also be characterized as a *maximal ideal*.

Definition 2.13. An ideal M of a commutative ring R is said to be a *maximal ideal* if and only if

- (i) $M \subset R$ and
- (ii) there does not exist an ideal I of R with $M \subset I \subset R$.

Example (2.13.1). The prime ideals of \mathbb{Z} are also maximal ideals of \mathbb{Z} because there is no proper subset of \mathbb{Z} that contains a prime ideal and is not equal to a prime ideal.

Example (2.13.2). Another example of a maximal ideal is the ideal generated by x and 2 , $(x, 2)$, which was given in Example 2.12.1. This ideal is maximal in $\mathbb{R}[x]$. We will show why this is true using Theorem 2.16 below.

Now if we let R be a ring and I an ideal of R we can create *factor rings* which are analogous to factor groups in group theory. This gives us important results if I is taken to be a prime or maximal ideal.

Definition 2.14. Let R be a ring, and let A be a subring of R . The set of cosets $\{r + A \mid r \in R\}$, denoted R/A , is a ring under the operations $(s + A) + (t + A) = s + t + A$ and $(s + A)(t + A) = st + A$ if and only if A is an ideal of R .

Example (2.14.1). Let R be the ring of integers \mathbb{Z} and A be the ideal generated by 3 , i.e. $A = (3)$. Then $\mathbb{Z}/(3) = \{0 + (3), 1 + (3), 2 + (3)\}$. The operations of this ring are inherently addition and multiplication modulo 3 .

The proofs for Theorem 2.15 and Theorem 2.16 can also be found in [Gal10].

Theorem 2.15. Let R be a commutative ring with unity, and let A be an ideal of R . Then R/A is an integral domain if and only if A is prime.

Proof. First let R/A be an integral domain. We will show that A is a prime ideal of R . Let $ab \in A$ where $a, b \in R$. Consider $ab + A \in R/A$, $ab + A = A$ since $ab \in A$. Hence $ab + A = (a + A)(b + A) = A = 0 + A$. Since R/A is an integral domain, $a + A = A$ or $b + A = A$. Thus $a \in A$ or $b \in A$, and so A is a prime ideal.

Now let A be a prime ideal of R . We will show that R/A is an integral domain. Let $a + A, b + A \in R/A$ and suppose $(a + A)(b + A) = 0 + A$. Then $(a + A)(b + A) = ab + A = 0 + A = A$. Hence $ab \in A$. Since A is prime, $a \in A$ or $b \in A$. If $a \in A$, then $a + A = 0 + A$. If $b \in A$, then $b + A = 0 + A$. Thus R/A is an integral domain. \square

Example (2.15.1). In \mathbb{Z} , the ideal (3) is a prime ideal. Thus $\mathbb{Z}/(3)$ is an integral domain.

If we restrict the ideal A to be a maximal ideal, our factor ring R/A is a field.

Theorem 2.16. *Let R be a commutative ring with unity and let A be an ideal of R . Then R/A is a field if and only if A is maximal.*

Proof. First, let R/A be a field. We will show that A is a maximal ideal. Suppose $A \subset B \subseteq R$ with $A \neq B$. Since $A \subset B$ and $A \neq B$, there exists a $b \in B$ such that $b \notin A$. Consider $b + A \in R/A$. Since $b \notin A$ we have that $b + A \neq A$. Hence there exists $c + A \in R/A$ such that $(b + A)(c + A) = 1 + A$ since R/A is a field. Thus $bc + A = 1 + A$ and $1 - bc \in A$, but since $A \subset B$, $1 - bc \in B$. We also have that $bc \in B$ because $b \in B$ and B is an ideal. Thus $1 = 1 - bc + bc \in B$ by closure. Therefore, $B = R$, and so A is maximal.

Next, let A be maximal. We will show that R/A is a field. Note that R is a commutative ring with unity, and so R/A is also a commutative ring with unity. Let $0 \neq b + A \in R/A$, so $b + A \neq A$ and $b \notin A$. Consider the set $B = \{br + a \mid r \in R \text{ and } a \in A\}$ hence $A \subset B$ and $A \neq B$ since $b \in B$ but $b \notin A$. Since A is maximal, $B = R$ and $1 \in B$. Thus $1 = br + a$ for $r \in R$ and $a \in A$. Consequently,

$$\begin{aligned} 1 + A &= br + a + A \\ &= br + A \\ &= (b + A)(r + A). \end{aligned}$$

So $(b + A)^{-1} = r + A$. Hence every non-zero element is a unit, and so R/A is a field. \square

Example (2.16.1). Every maximal ideal is a prime ideal; the proof uses Theorem 2.16 and Theorem 2.15.

Proof. Let A be a maximal ideal of a ring R . Then by Theorem 2.16, R/A is a field. But all fields are integral domains so R/A is an integral domain. By Theorem 2.15, if R/A is a integral domain, then A is a prime ideal. \square

If we are given that a factor ring is either an integral domain or field, we can use these theorems to show that an ideal is prime or maximal. For example, we can see

that $\mathbb{Z}[x]/(x, 2)$ is a finite integral domain since

$$\begin{aligned}\mathbb{Z}[x]/(x, 2) &= \{f(x) + (x, 2) \mid f(x) \in \mathbb{Z}[x]\} \\ &= \{0 + (x, 2), 1 + (x, 2)\}.\end{aligned}$$

Thus $\mathbb{Z}[x]/(x, 2)$ is also a field. Since $\mathbb{Z}[x]/(x, 2)$ is a field, $(x, 2)$ is a maximal ideal and hence a prime ideal in $\mathbb{Z}[x]$.

Definition 2.17. An integral domain R is said to be a *principal ideal domain* (or PID for short) precisely when every ideal of R is principal.

Example (2.17.1). We have already seen in Example 2.16.1 that every maximal ideal is a prime ideal. In a principal ideal domain, the converse is true, all prime ideals are maximal ideals.

Proof. Let R be a PID and let A be a prime ideal of R . Suppose $A \subset B \subseteq R$ with $A \neq B$. Since R is a PID, we can write $A = (a)$ and $B = (b)$ for $a \in R$ and $b \notin A$. Then there is an element $r \in R$ such that $a = br$. However, A is prime so either $b \in A$ or $r \in A$, but $b \notin A$, and so $r \in A$. Hence $r = as$ for some $s \in R$, and we have $a = br = bas$ which implies that $bs = 1 \in (b)$. Thus $(b) = B = R$. Therefore A is a maximal ideal. \square

Example (2.17.2). The ring of integers \mathbb{Z} is a principal ideal domain.

Proof. Let I be a non-zero ideal of \mathbb{Z} . Let m be the least positive integer in I , then $(m) \subseteq I$ since $m \in I$. We want to show that $I \subseteq (m)$. Let $x \in I$. By the Division Algorithm for integers we can write $x = mq + r$ for some $m, r \in \mathbb{Z}$ where $0 \leq r < m$. This gives us that $r = x - mq$ which is in I since $x \in I$ and $mq \in I$. We are given that m is the least positive element in I so $r = 0$. Hence $x = mq$. Therefore $x \in (m)$, and so $I \subseteq (m)$. Consequently, \mathbb{Z} is a PID. \square

Another example of a principal ideal domain is the ring of polynomials over K where K is a field.

Theorem 2.18. Let K be a field. Then $K[x]$ is a principal ideal domain.

Proof. Let I be a nonzero ideal of $K[x]$. We want to show that $I = (g(x))$ for some $g(x) \in K[x]$. Let $g(x) \in I$ be of minimum degree. Then $(g(x)) \subseteq I$ since $g(x) \in I$.

We will now show that $I \subseteq (g(x))$. Let $f(x) \in I$. Then $f(x) = g(x)q(x) + r(x)$ where $r(x) = 0$ or $\text{degree of } r < \text{degree of } g$ (by the Division Algorithm Theorem 2.8). We can rewrite this for r so that $r(x) = f(x) - g(x)q(x)$. Since $f(x), g(x) \in I$ and I is an ideal, $f(x) - g(x)q(x) \in I$ which implies that $r(x) \in I$. We assumed that $g(x)$ has minimum degree in I so the only way for the degree of r to be less than the degree of g is if $r(x) = 0$. Therefore, $f(x) = g(x)q(x)$. Hence $I \subseteq (g(x))$. Thus $I = (g(x))$ and $K[x]$ is a PID. \square

Definition 2.19. A *ring homomorphism* ϕ 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 $a, b \in R$

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

A ring homomorphism that is onto is called a *ring epimorphism* and a ring homomorphism that is both one-to-one and onto is called a *ring isomorphism*.

A special ideal related to the image of a homomorphism is the kernel of a homomorphism.

Definition 2.20. Let ϕ be a ring homomorphism from a ring R to a ring S . Then the *kernel* is defined to be

$$\ker \phi = \{r \in R \mid \phi(r) = 0\}$$

Example (2.20.1). Define $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_6$ by $\phi(x) = x \bmod 6$. Then the kernel of ϕ is:

$$\begin{aligned} \ker \phi &= \{r \in R \mid \phi(r) = r \bmod 6 = 0\} \\ &= \{r \in \mathbb{Z} \mid r \bmod 6 = 0\} \\ &= (6) \end{aligned}$$

Theorem 2.21. Let ϕ be a ring homomorphism from R to S . Then $\ker \phi$ is an ideal of R .

Proof. Let $x, y \in \ker \phi$. Then $\phi(x) = 0$ and $\phi(y) = 0$. Since ϕ is a ring homomorphism, $\phi(x - y) = \phi(x) - \phi(y) = 0$. Hence $x - y \in \ker \phi$. Now let $r \in R$. Then $\phi(rx) = \phi(r)\phi(x) = \phi(r) \cdot 0 = 0$, hence $rx \in \ker \phi$. Therefore $\ker \phi$ is an ideal. \square

The theorem below is the First Isomorphism Theorem for Rings and the proof can be found in [Hun74].

Theorem 2.22. *Let ϕ be a ring homomorphism from R to S . Then the mapping from $R/\ker \phi$ to $\phi(R)$, given by $r + \ker \phi \rightarrow \phi(r)$, is an isomorphism. That is, $R/\ker \phi \cong \phi(R)$.*

Now we focus our attention on factoring by first introducing irreducible elements and unique factorization domains.

Definition 2.23. Let R be an integral domain. An element $p \in R$ is said to be an *irreducible element* of R precisely when $p \neq 0$ and p is not a unit of R and whenever $p = ab$ with $a, b \in R$, then either a or b is a unit of R . We say that p is *prime* if $p|ab$ implies $p|a$ or $p|b$.

The definitions for prime and irreducible are very similar but there is a subtle difference that the next examples show. Prime elements are irreducible, but only in a principal ideal domain are irreducible elements prime.

Example (2.23.1). Prime elements are irreducible elements.

Proof. Let p be a prime element and assume $p = ab$ for some $a, b \in R$. Then by definition, $p|a$ or $p|b$. Without loss of generality, assume that $p|a$. Then $a = pr$ for some $r \in R$. Hence $p = ab = prb$ which implies that $rb = 1$, and so b is a unit. Thus, p is irreducible. \square

Example (2.23.2). In a principal ideal domain all irreducible elements are prime elements.

Proof. Let R be a PID and let $x \in R$ be irreducible. We want to show that (x) is maximal, which from Example 2.17.1, will imply that it is prime. Suppose $(x) \subset B \subseteq R$ and $B = (b) \neq (x)$. We have that $b|x$, and so $x = br$ for some $r \in R$. Since x is irreducible b is a unit or r is a unit. If r is a unit, then $(x) = (b)$ which is a contradiction. Hence b is a unit, which means $B = R$. Therefore (x) is maximal which implies that it is prime. \square

Definition 2.24. An integral domain R is a *unique factorization domain* (or UFD for short) if:

- (i) every non-zero, non-unit element of R can be written as $p_1 p_2 \dots p_n$, where p_1, p_2, \dots, p_n are irreducible elements of R and
- (ii) whenever $n, m \in \mathbb{N}$ and $p_1, p_2, \dots, p_n, q_1, q_2, \dots, q_m$ are irreducible elements of R such that

$$p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$$

then $m = n$ and there exists units $u_1, u_2, \dots, u_n \in R$ such that, after renumbering q_i we get $p_i = u_i q_i$ for all $i = 1, \dots, n$.

Example (2.24.1). The Fundamental Theorem of Arithmetic tells us that the ring of integers, \mathbb{Z} , is a UFD.

Example (2.24.2). Any field is a UFD since every nonzero element in a field is a unit.

Other examples of unique factorization domains are given in the theorems below. The proof of the next theorem is found in [Gal10]. Gallian uses an ascending chain condition in the proof to show that every nonzero nonunit in D has at least one irreducible factor. The ascending chain condition for PID's states that in a principal ideal domain, any strictly increasing chain of ideals $I_1 \subset I_2 \subset \dots$ must be finite in length.

Theorem 2.25. *All principal ideal domains are unique factorization domains.*

Proof. Let R be a PID and let $0 \neq a_0 \in R$ be a non-unit. We will show that a_0 is a product of irreducible elements. If a_0 is irreducible, then we are done. Assume that a_0 is not irreducible, and so $a_0 = b_1 a_1$ where b_1, a_1 are not units and $a_1 \neq 0$. If a_1 is not irreducible, then we can write $a_1 = b_2 a_2$ where b_2, a_2 are not units and $a_2 \neq 0$. We can continue this and obtain a sequence of elements b_1, b_2, \dots that are not units in R and a sequence of elements a_1, a_2, \dots that are non-zero with $a_n = b_{n+1} a_{n+1}$ for each n . Hence, $(a_0) \subset (a_1) \subset \dots$ is a strictly increasing chain of ideals which must be finite since R is a PID. So we have $(a_0) \subset (a_1) \subset \dots \subset (a_r)$ where a_r is an irreducible factor of a_0 . Thus every non-zero non-unit in R has at least one irreducible factor.

Now we can write $a_0 = p_1 c_1$ where p_1 is irreducible and c_1 is not a unit. If c_1 is not irreducible, then we can write $c_1 = p_2 c_2$, where p_2 is irreducible and c_2 is not a unit. We can continue this just like before and obtain a strictly increasing sequence $(a_0) \subset (c_1) \subset \dots$ which must be finite because R is a PID. So we have $(a_0) \subset (c_1) \subset \dots \subset (c_s)$ where c_s is irreducible. Then $a_0 = p_1 p_2 \dots p_r c_s$ where each p_i is irreducible. Thus every non-zero non-unit element of a PID is a product of irreducibles.

Finally we need to show that the factorization is unique up to associates and the order in which the factors appear. Suppose that $a \in R$ can be written as $a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$ where p_i and q_i are irreducible elements. We will use induction on r . If $r = 1$, then $a = p_1 = q_1 q_2 \dots q_s$. Since p_1 is irreducible, $s = 1$, and so $p_1 = q_1$. Assume this is

true for products with less than r factors. Since p_1 divides $q_1q_2\cdots q_s$, it must divide q_i for some i . Suppose p_1 divides q_1 . Then $q_1 = up_1$ where $u \in R$ is a unit. Then

$$p_1p_2\cdots p_r = up_1q_2\cdots q_s = p_1(uq_2)\cdots q_s$$

and so by cancellation we get

$$p_2\cdots p_r = (uq_2)\cdots q_s.$$

By the induction hypothesis $p_2\cdots p_r$ and $(uq_2)\cdots q_s$ are identical up to associates and the order in which the factors appear. Therefore, $a = p_1p_2\cdots p_r = q_1q_2\cdots q_s$. So R is a UFD. \square

Corollary 2.26. *Let K be a field. Then $K[x]$ is a unique factorization domain.*

Proof. By Theorem 2.18, $K[x]$ is a PID. By Theorem 2.25, all PID's are UFD's. Thus $K[x]$ is a UFD. \square

Theorem 2.16 showed a connection between maximal ideals and fields. The proceeding theorem and corollary to the theorem relates these two concepts with irreducible polynomials. We will be looking back at this theorem when dealing with algebraic extensions in the next chapter.

Theorem 2.27. *Let F be a field and let $p(x) \in K[x]$. Then $(p(x))$ is a maximal ideal in $F[x]$ if and only if $p(x)$ is irreducible over F .*

Proof. (\Rightarrow) Let $(p(x))$ be a maximal ideal in $K[x]$, and assume $p(x)$ is reducible. Then $(p(x)) \subset K[x]$ and $p(x)$ is not a unit. Since $p(x)$ is reducible we can write $p(x) = f(x)g(x)$. Thus the ideal generated by $p(x)$ is a subset of the ideal generated by $f(x)$. We know that $(p(x))$ is maximal so this means that $(p(x)) = (f(x))$ or $(f(x)) = K[x]$. If $(f(x)) = K[x]$, then $f(x)$ is a unit, so $p(x)$ is irreducible. If $(f(x)) = (p(x))$, then $f(x) = p(x)h(x)$ so $p(x) = f(x)g(x) = p(x)h(x)g(x)$. Thus $h(x)g(x) = 1$, which makes $g(x)$ a unit. If $g(x)$ is a unit, then $p(x)$ is irreducible. Therefore if $(p(x))$ is a maximal ideal in $K[x]$, then $p(x)$ is irreducible.

(\Leftarrow) Let $p(x)$ be irreducible over K . Then $(p(x))$ is a proper ideal of $K[x]$. Assume $(p(x)) \subset (f(x)) \in K[x]$. Then $p(x) = f(x)g(x)$. Since $p(x)$ is irreducible, $f(x)$ is a unit or $g(x)$ is a unit. If $f(x)$ is a unit, then $f(x) = K[x]$ and $(p(x))$ is a maximal ideal of

$K[x]$. If $g(x)$ is a unit, then $p(x) = f(x) \cdot a$ for some $a \in K$. This means $(p(x)) = (f(x))$ and so $(p(x))$ is a maximal ideal. Either way, if $p(x)$ is irreducible over K then $(p(x))$ is maximal. \square

Corollary 2.28. *Let F be a field and $p(x)$ an irreducible polynomial over F . Then $F[x]/(p(x))$ is a field.*

Proof. By Theorem 2.27, $(p(x))$ is maximal. So by Theorem 2.16, $F[x]/(p(x))$ is a field. \square

Theorem 2.29. *Let $f : R \rightarrow S$ be a surjective ring homomorphism with kernel K . If P is a prime ideal in R that contains K , then $f(P)$ is a prime ideal in S .*

Proof. Let P be a prime ideal in R , and let $x, y \in S$ such that $xy \in f(P)$. Then there exists $a, b \in R$ such that $f(a) = x$ and $f(b) = y$ because f is surjective. Thus

$$\begin{aligned} xy &= f(a)f(b) \\ &= f(ab) \in f(P) \text{ because } f \text{ is a homomorphism.} \end{aligned}$$

There also exists a $p \in P$ such that $f(ab) = f(p)$. This means that $f(ab) - f(p) = 0$ so that $f(ab - p) = 0$. So we can say that $ab - p \in K \subseteq P$ hence $ab - p \in P$. Since $p \in P$, $ab - p + p \in P$ because P is an ideal. Hence $ab \in P$. P is prime so $a \in P$ or $b \in P$. Thus $f(a) \in f(P)$ or $f(b) \in f(P)$ which means $x \in f(P)$ or $y \in f(P)$. Therefore, $f(P)$ is prime. \square

As I mentioned above, ideals are important to the study of commutative algebra because they help identify characteristics of certain rings. The last definitions and theorems of this section identify different classes of ideals. The construction of these ideals are used in our study of closure operations.

Definition 2.30. Let I be an ideal of R . The *radical* of I denoted \sqrt{I} is:

$$\sqrt{I} = \{r \in R \mid \text{there exists } n \in \mathbb{N} \text{ with } r^n \in I\}$$

The set of all *nilpotent* elements of R , that is elements $a \in R$ that are of the form $a^n = 0$ where n is a positive integer, is called the *nilradical* of R . In other words, the nilradical is just $\sqrt{0_R}$, or the radical of the zero ideal of R .

Theorem 2.31. *The radical of I , \sqrt{I} , is an ideal of R .*

Proof. $\sqrt{I} \neq \emptyset$ since $I \subseteq \sqrt{I}$ and $I \neq \emptyset$. Now, let $x, y \in \sqrt{I}$. Then there exists positive integers n and m such that $x^n, y^m \in I$. We want to show that $x + y \in \sqrt{I}$.

$$(x + y)^{n+m} = x^{n+m} + a_1 x^{n+m-1} y + \cdots + a_m x^n y^m + \cdots + a_{n+m-1} x y^{n+m-1} + y^{n+m}$$

Since every term on the right hand side has a factor of either $x^n \in I$ or $y^m \in I$, then the sum of those terms is in I . Thus $(x + y)^{n+m} \in I$ so $x + y \in \sqrt{I}$. Next, let $r \in R$.

$$(rx)^n = r^n x^n \in I \text{ since } r^n \in R \text{ and } x^n \in I.$$

So $rx \in \sqrt{I}$. Therefore, \sqrt{I} is an ideal of R . \square

Definition 2.32. Let I and J be ideals of a commutative ring R . We define the *ideal quotient* $(I : J)$ by

$$(I : J) = \{a \in R \mid aJ \subset I\}$$

Example (2.32.1). Let $R = \mathbb{Z}$. Then

$$((12) : (2)) = \{a \in \mathbb{Z} \mid a(2) \subset (12)\} = (6)$$

$$\text{and } ((12) : (5)) = \{a \in \mathbb{Z} \mid a(5) \subset (12)\} = (12)$$

The ideal quotient is an ideal of R (shown below) and $I \subseteq (I : J)$. If $I = 0$, then the ideal quotient $(0 : J) = \{a \in R \mid aJ = 0\} = \{a \in R \mid ab = 0 \text{ for all } b \in J\}$ is called the *annihilator* of J .

Theorem 2.33. *The ideal quotient, $(I : J)$, is an ideal of R .*

Proof. $(I : J) \neq \emptyset$ since $I \subseteq (I : J)$ and $I \neq \emptyset$. Now let $x, y \in (I : J)$. So $xJ \subset I$ and $yJ \subset I$. So $xa_i \in I$ and $ya_i \in I$ for all $a_i \in J$. Hence $(x + y)a_i = xa_i + ya_i \in I$. Thus $(x + y)J \subseteq I$ so $(x + y) \in (I : J)$. Next we will show that the quotient ideal is closed under ring multiplication. Let $r \in R$ and $x \in (I : J)$. Then $xJ \subseteq I$. So $(rx)J = x(rJ) = xJ$ since J is an ideal. Thus $(rx)J \subseteq I$ so $rx \in (I : J)$. Therefore $(I : J)$ is an ideal of R . \square

Definition 2.34. Let I and J be ideals of the commutative ring R . The *product* of I and J , denoted by IJ is defined to be the ideal of R generated by the set $\{ab \mid a \in I, b \in J\}$.

This gives us:

$$IJ = \left\{ \sum_{i=1}^n a_i b_i \mid a_i \in I, b_i \in J, n \in \mathbb{N} \right\}.$$

Lemma 2.35. *Let R and S be commutative rings, $R \subseteq S$ and I is an ideal of R . Then IS is an ideal in S .*

Proof. We will use the definition of ideal (Definition 2.10) to show that IS is an ideal in S . Since I is an ideal in R , $0 \in I$. Hence $0 \in IS$ which means $IS \neq \emptyset$. Now let $x, y \in IS$. Then by definition $x = \sum_{i=1}^n a_i b_i$ for $a_i \in I$, $b_i \in S$ and $n \in \mathbb{N}$ and $y = \sum_{i=n+1}^m a_i b_i$ for $a_i \in I$, $b_i \in S$ and $m \in \mathbb{N}$. Then

$$\begin{aligned} x + y &= \sum_{i=1}^n a_i b_i + \sum_{i=n+1}^m a_i b_i \\ &= \sum_{i=1}^{n+m} a_i b_i \\ &\in IS \end{aligned}$$

Next, we show that IS is closed under ring multiplication. Let $s \in S$ and $x \in IS$. Then

$$\begin{aligned} sx &= s \sum_{i=1}^n a_i b_i \\ &= \sum_{i=1}^n s a_i b_i \\ &= \sum_{i=1}^n a_i (s b_i) \text{ where } s b_i \in S \\ &\in IS \end{aligned}$$

Therefore, IS is an ideal of S . □

Lemma 2.36. *Let R and S be commutative rings, $R \subseteq S$ and I an ideal of R . Then $IS \cap R$ is an ideal of R .*

Proof. Just like in the previous lemma, we use Definition 2.10 to show that $IS \cap R$ is an ideal in R . We know that $0 \in R$ and from the above lemma we know that $0 \in IS$, hence $0 \in IS \cap R$, and so $IS \cap R \neq \emptyset$. Now, let $x, y \in IS \cap R$. Then $x, y \in IS$ and $x, y \in R$. We know that $x + y \in IS$ since IS is an ideal and $x + y \in R$ since R is a ring, thus $x + y \in IS \cap R$. Next, we let $r \in R$ and $x \in IS \cap R$. Then $x = \sum_{i=1}^n a_i b_i$ where $a_i \in I$ and

$b_i \in S$. This gives us

$$\begin{aligned} rx &= r \sum_{i=1}^n a_i b_i \\ &= \sum_{i=1}^n (ra_i) b_i \\ &\in IS. \end{aligned}$$

Since both r and x are elements of R , $rx \in R$, thus $rx \in IS \cap R$. Therefore $IS \cap R$ is an ideal of R . \square

Note that $I \subseteq IS \cap R$ but $IS \cap R$ does not necessarily equal I . For example, if we let $R = \mathbb{Z}$, $S = \mathbb{Q}$ and $I = (2)$. Then $IS \cap R = (2)\mathbb{Q} \cap \mathbb{Z} = \mathbb{Z}$. Hence $I \subseteq IS \cap R$ and $I \neq IS \cap R$.

2.2 Modules

Just like the ideals in a ring, modules can convey important information about the structure of a ring R . For example, an ideal of a ring as well as the quotient R/I are considered to be R -modules. The most basic way of thinking about a module is as a generalized abelian group (which are just modules over the integers \mathbb{Z}).

Definition 2.37. Let R be a ring. An R -module is an additive abelian group, A , together with a function $R \times A \rightarrow A$ (the image of (r, a) being denoted by $r(a)$) such that for all $r, s \in R$ and $a, b \in A$:

- (i) $r(a + b) = ra + rb$
- (ii) $(r + s)a = ra + sa$
- (iii) $r(sa) = (rs)a$
- (iv) $1_R a = a$ for all $a \in A$

Example (2.37.1). The ring R is an R -module.

Example (2.37.2). A module over a field K is a vector space over K .

Example (2.37.3). Every additive Abelian group, G , is a unitary \mathbb{Z} -module, with na ($n \in \mathbb{Z}, a \in G$).

Example (2.37.4). If S is a ring and R is a subring, then S is an R -module with $ra \in S$ ($r \in R, a \in S$) being multiplication in S . Note that R is not an S -module because if $r \in R$ and $a \in S$, then ar might not necessarily be in R since R is a subring of S .

Example (2.37.5). The set of n -tuples made up of real numbers $\mathbb{R}^{\bar{n}} = \{(a_1, \dots, a_n) \mid a_i \in \mathbb{R}\}$ is an \mathbb{R} -module.

To check that this last statement (Example 2.37.5) is true we need all the requirements of Definition 2.37 to be satisfied. So let $r, s \in \mathbb{R}$ and $a, b \in \mathbb{R}^{\bar{n}}$. Then $a = (a_1, a_2, \dots, a_n)$ and $b = (b_1, b_2, \dots, b_n)$ where $a_i, b_i \in \mathbb{R}$.

(i) We first check that the distribution of a ring element over the sum of group elements hold.

$$\begin{aligned}
 r(a + b) &= r[(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n)] \\
 &= r(a_1 + b_1, a_2 + b_2, \dots, a_n + b_n) \\
 &= (r(a_1 + b_1), r(a_2 + b_2), \dots, r(a_n + b_n)) \\
 &= (ra_1 + rb_1, ra_2 + rb_2, \dots, ra_n + rb_n) \\
 &= (ra_1, ra_2, \dots, ra_n) + (rb_1, rb_2, \dots, rb_n) \\
 &= ra + ba.
 \end{aligned}$$

(ii) Next we check that distribution of a group element over the sum of ring elements hold.

$$\begin{aligned}
 (r + s)a &= (r + s)(a_1, a_2, \dots, a_n) \\
 &= ((r + s)a_1, (r + s)a_2, \dots, (r + s)a_n) \\
 &= (ra_1 + sa_1, ra_2 + sa_2, \dots, ra_n + sa_n) \\
 &= (ra_1, ra_2, \dots, ra_n) + (sa_1, sa_2, \dots, sa_n) \\
 &= ra + sa
 \end{aligned}$$

(iii) Now we check the associative property.

$$\begin{aligned}
 r(sa) &= r(sa_1, sa_2, \dots, sa_n) \\
 &= (rsa_1, rsa_2, \dots, rsa_n) \\
 &= rs(a_1, a_2, \dots, a_n) \\
 &= (rs)a
 \end{aligned}$$

(iv) Lastly we check that 1 is the identity element.

$$\begin{aligned} 1_R a &= 1(a_1, a_2, \dots, a_n) \\ &= (a_1, a_2, \dots, a_n) \\ &= a \end{aligned}$$

Definition 2.38. Let R be a ring, A an R -module and B a nonempty subset of A . B is a *submodule* of A , or an R -module of A , provided that B is an additive subgroup of A and $rb \in B$ for all $r \in R$ and $b \in B$ (B is itself an R -module with respect to the operations of A).

A submodule is essentially a subgroup of the original module that is also a module under the same operation.

Theorem 2.39 (The Submodule Criterion). *Let R be a commutative ring and let B be a subset of the R -module A . Then B is a submodule of A if and only if the following conditions hold:*

- (i) $B \neq \emptyset$
- (ii) whenever $b, b' \in B$ and $r, r' \in R$, then $rb + r'b' \in B$.

Proof. (\Rightarrow) Let B be a submodule, then $0 \in B$ so $B \neq \emptyset$. By definition of submodule, B is closed under addition of A and under scalar multiplication by arbitrary elements of R . Thus, whenever $b, b' \in B$ and $r, r' \in R$, then $rb + r'b' \in B$.

(\Leftarrow) Let $B \neq \emptyset$ and whenever $b, b' \in B$ and $r, r' \in R$, then $rb + r'b' \in B$. Let $r' = -r$, then $rb + r'b = rb - rb \in B$. Thus, B is a subgroup of A . Also, $rb + r'b' \in B$ implies $rb \in B$. Therefore, by Definition 2.38, B is a submodule of A . \square

Example (2.39.1). If R is a module over itself, then its submodules are precisely the ideals of R .

Example (2.39.2). Let I be an ideal of R . Then if $a \in A$ and $A \subseteq R$, the principal ideal $Ia = \{ra \mid r \in I\}$ is a submodule of I .

Theorem 2.40 (Quotient Group is an R -module). *Let B be a submodule of a module A over a ring R . Then the quotient group A/B is an R -module with the action of R on A/B given by:*

$$r(a + B) = ra + B \text{ for all } r \in R \text{ and } a \in A.$$

Proof. Let A be an R -module and let B be a submodule of A . We want to show that A/B is an R -module. First we will show that A/B is an additive Abelian group.

(i) Let $x, y \in A/B$. Then $x = a_1 + B$ and $y = a_2 + B$ where $a_i \in A$. Then

$$\begin{aligned} x + y &= (a_1 + B) + (a_2 + B) \\ &= (a_1 + a_2) + B \in A/B \text{ since } a_1 + a_2 \in A. \end{aligned}$$

(ii) Let $x, y, z \in A/B$. Then $x = a_1 + B$, $y = a_2 + B$ and $z = a_3 + B$ for all $a_i \in A$. Then

$$\begin{aligned} (x + y) + z &= (a_1 + B + a_2 + B) + a_3 + B \\ &= (a_1 + a_2) + B + a_3 + B \\ &= (a_1 + a_2) + a_3 + B \\ &= a_1 + (a_2 + a_3) + B \\ &= a_1 + B + (a_2 + a_3) + B \\ &= a_1 + B + (a_2 + B + a_3 + B) \\ &= x + (y + z). \end{aligned}$$

(iii) $0 + B$ is the additive identity.

(iv) $-a + B$ is the additive inverse for $a + B \in A/B$.

Thus, A/B is an additive Abelian group.

Now we will show that A/B is a well-defined Abelian group. That is if $a + B = a' + B$ then $r(a + B) = r(a' + B)$ for all $r \in R$ and $a \in A$. Let $a + B = a' + B$. Then $a - a' \in B$ so $r(a - a') = ra - ra'$ since A is an R -module. So $ra + B = ra' + B$ implies that $r(a + B) = r(a' + B)$. Next, we will check that the four conditions of the definition of module hold. Let $r, s \in R$ and $a + B \in A/B$. Then $r(a + B) = ra + B \in A/B$ since $ra \in A$ and A is an R -module. Let $x - y \in A/B$. Then we can write $x = a_1 + B$ and $y = a_2 + B$, and

$$\begin{aligned} r(x + y) &= r(a_1 + B + a_2 + B) \\ &= r((a_1 + a_2) + B) \\ &= r(a_1 + a_2) + B, \text{ by the definition of } R \text{ on } A/B \\ &= (ra_1 + ra_2) + B, \text{ since } A \text{ is an } R\text{-module} \\ &= ra_1 + B + ra_2 + B \\ &= rx + ry. \end{aligned}$$

Thus the first condition is satisfied. Now

$$\begin{aligned}
 (r + s)x &= (r + s)(a_1 + B) \\
 &= (r + s)a_1 + B, \text{ by the definition of } R \text{ on } A/B \\
 &= (ra_1 + sa_1) + B, \text{ since } A \text{ is an } R\text{-module} \\
 &= ra_1 + B + sa_1 + B \\
 &= rx + sx.
 \end{aligned}$$

Hence the second condition is satisfied. Next

$$\begin{aligned}
 r(sx) &= r(s(a_1 + B)) \\
 &= r(sa_1 + B), \text{ by the definition of } R \text{ on } A/B \text{ and since } A \text{ is an } R\text{-module} \\
 &= rsa_1 + B, \text{ by the definition of } R \text{ on } A/B \text{ and since } A \text{ is an } R\text{-module} \\
 &= (rs)x.
 \end{aligned}$$

Thus the third condition is satisfied. Lastly,

$$\begin{aligned}
 1_R x &= 1_R(a_1 + B) \\
 &= a_1 + B, \text{ by the definition of } R \text{ on } A/B \text{ and } A \text{ is an } R\text{-module} \\
 &= x.
 \end{aligned}$$

Thus the fourth condition is satisfied. Therefore A/B is an R -module. \square

Chapter 3

Algebraic Closure

A familiar concept in mathematics is that of the algebraic closure of a field. The basic idea of algebraic closure is looking at elements of a field as roots of polynomials. An important theorem that deals with roots of polynomials is the Fundamental Theorem of Algebra. This section will introduce definitions and concepts of algebraic closure and use the Fundamental Theorem of Algebra to illustrate how they are used.

3.1 Field Extensions

Before we jump into algebraic closures, we first need to introduce foundational notions about fields and their extensions.

Definition 3.1. A field E is an *extension field* of a field F if F is a subfield of E .

Theorem 3.2 (Fundamental Theorem of Field Theory). *Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Then there is an extension field E of F in which $f(x)$ has a zero.*

Proof. $F[x]$ is a unique factorization domain by Corollary 2.26. So $f(x)$ has an irreducible factor, call it $p(x)$. We will construct an extension field E of F in which $p(x)$ has a zero. Let $E = F[x]/(p(x))$. Then E is a field by Corollary 2.28. Now, let $\phi : F \rightarrow E$ defined by $\phi(a) = a + (p(x))$. We will show that ϕ is a ring isomorphism. First we will show that

addition is preserved. Let $a, b \in F$. Then

$$\begin{aligned}\phi(a+b) &= (a+b) + (p(x)) \\ &= a + (p(x)) + b + (p(x)) \\ &= \phi(a) + \phi(b).\end{aligned}$$

Next we will show that multiplication is preserved:

$$\begin{aligned}\phi(ab) &= (ab) + (p(x)) \\ &= (a + (p(x)))(b + (p(x))) \\ &= \phi(a)\phi(b).\end{aligned}$$

Now, we will show that ϕ is injective. Let $\phi(a) = \phi(b)$, then $a + (p(x)) = b + (p(x))$. Hence $0 = a - b + (p(x))$, and so $a - b \in (p(x))$. This means a and b are in F , and thus $a = b$. Finally, we will show $p(x)$ has a zero in E . Let $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$. Then, in E , $x + (p(x))$ is a zero of $p(x)$:

$$\begin{aligned}p(x + (p(x))) &= a_n(x + (p(x)))^n + \dots + a_1(x + (p(x))) + a_0 \\ &= a_n(x^n + (p(x))) + \dots + a_1(x + (p(x))) + a_0 \\ &= a_n x^n + \dots + a_1 x + a_0 + (p(x)) \\ &= p(x) + (p(x)) \\ &= 0 + (p(x)).\end{aligned}$$

□

Example (3.2.1). Let $f(x) = x^2 + 1 \in \mathbb{Q}[x]$. Let $E = \mathbb{Q}[x]/(x^2 + 1)$ so $f(x) \in E$.

$$\begin{aligned}f(x + (x^2 + 1)) &= (x + (x^2 + 1))^2 + 1 \\ &= x^2 + (x^2 + 1) + 1 \\ &= x^2 + 1 + (x^2 + 1) \\ &= 0 + (x^2 + 1).\end{aligned}$$

Thus $f(x)$ has a zero in E .

Example (3.2.2). Now, let $f(x) = x^5 + 2x^2 + 2x + 2 \in \mathbb{Z}_3[x]$. If we factor $f(x)$ as a product of irreducibles we get $f(x) = (x^2 + 1)(x^3 + 2x + 2)$. By Theorem 3.2, let E be

an extension of \mathbb{Z}_3 . Then $E_1 = \mathbb{Z}_3[x]/(x^2 + 1)$ or $E_2 = \mathbb{Z}_3[x]/(x^3 + 2x + 2)$. Thus, $f(x)$ has a zero in E_1 and E_2 .

Example (3.2.3). Lastly, if we let $f(x) = 2x + 1 \in \mathbb{Z}_4[x]$, Theorem 3.2 does not guarantee that there is an extension field of \mathbb{Z}_4 in which $f(x)$ has a zero since \mathbb{Z}_4 is not a field. In fact, $f(x)$ does not have a zero in any ring containing \mathbb{Z}_4 as a subring. This is because if we let β be a zero in E (an extension of \mathbb{Z}_4), then $0 = 2\beta + 1$. Which then gives us:

$$\begin{aligned} 0 &= 2(2\beta + 1) \\ &= 2(2\beta) + 2 \\ &= (2 \cdot 2)\beta + 2 \\ &= 0 \cdot \beta + 2 \\ &= 2 \end{aligned}$$

But $0 \neq 2$ in \mathbb{Z}_4 . Thus $f(x)$ does not have a zero in any ring containing \mathbb{Z}_4 as a subring.

The following theorem describes a field adjoined with an element from its extension field. We can think of $F[a]$ as a ring of polynomials (as in Definition 2.2) but evaluated at an element a . In part (iii) of the theorem, we use $F(a)$ to describe rational functions evaluated at a .

Theorem 3.3. *If E is an extension field of a field F , $a, a_i \in E$ and $X \subset E$, then*

- (i) *the subring $F[a]$ consists of all elements of the form $f(a)$, where f is a polynomial with coefficients in F ;*
- (ii) *the subring $F[a_1, \dots, a_m]$ consists of all elements of the form $f(a_1, a_2, \dots, a_m)$, where f is a polynomial in m indeterminates with coefficients in F ;*
- (iii) *the subfield $F(a)$ consists of all elements of the form $f(a)/g(a) = f(a)g(a)^{-1}$, where $f, g \in F[x]$ and $g(a) \neq 0$.*

Example (3.3.1). The subring $\mathbb{Q}[\sqrt{2}]$ consists of all elements of the form $f(\sqrt{2})$ where f is a polynomial with coefficients in \mathbb{Q} . We can write it as

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

This is because $(\sqrt{2})^{2n}$ where n is a non-negative integer will always be a multiple of 2 and $(\sqrt{2})^{2m+1}$ where m is a non-negative integer will be a multiple of $\sqrt{2}$.

Example (3.3.2). The subring $\mathbb{Q}[\sqrt{2}, \sqrt{5}]$ consists of all elements of the form $f(\sqrt{2}, \sqrt{5})$ where f is a polynomial in 2 indeterminates with coefficients in \mathbb{Q} . We can write it as

$$\mathbb{Q}[\sqrt{2}, \sqrt{5}] = \mathbb{Q}[\sqrt{2}][\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}[\sqrt{2}]\}.$$

Definition 3.4. Let E be an extension field of F , and let $f(x) \in F[x]$. We say that $f(x)$ *splits in E* if $f(x)$ can be factored as a product of linear factors in $E[x]$. We call E a *splitting field* for $f(x)$ over F if $f(x)$ splits in no proper subfield of E .

Example (3.4.1). Let $f(x) = x^2 + 1 \in \mathbb{Q}[x]$. We can factor $f(x)$ as a product of linear factors in $\mathbb{C}[x]$.

$$f(x) = (x + i)(x - i)$$

Thus, $f(x)$ splits in \mathbb{C} . We cannot say that \mathbb{C} is a splitting field over \mathbb{Q} since there is a proper subfield F of \mathbb{C} such that $(x - i)(x + i) \in F[x]$. That subfield is $\mathbb{Q}(i)$.

Example (3.4.2). Now if we let $f(x) = x^2 + 1 \in \mathbb{R}[x]$, then \mathbb{C} is a splitting field for $f(x)$ over \mathbb{R} .

Theorem 3.5 (Existence of Splitting Fields). *Let F be a field and let $f(x)$ be a non-constant element of $F[x]$. Then there exists a splitting field E for $f(x)$ over F .*

Proof. We will prove this by the principle of mathematical induction on the degree of $f(x)$. Suppose $\deg f(x) = 1$. Then $f(x)$ is linear so $f(x)$ splits in F . Now suppose there exists a splitting field for all polynomials of degree less than the degree of $f(x)$ over F . We will prove there is a splitting field for $f(x)$ over F . By Theorem 3.2 there is an extension field E of F in which $f(x)$ has a zero. Let the zero be a_1 . Then $f(x) = (x - a_1)g(x)$, where $g(x) \in E[x]$ and $\deg g(x) < \deg f(x)$. Since $\deg g(x) < \deg f(x)$, by the induction hypothesis there is an extension field K of E that contains all the zeros of $g(x)$, say a_2, \dots, a_n . Then a splitting field for $f(x)$ over F is $F(a_1, a_2, \dots, a_n)$. Therefore, by the principle of mathematical induction, for any field F , there exists a splitting field E for any polynomial $f(x) \in F[x]$. \square

Example (3.5.1). Let $f(x) = x^4 - x^2 - 2 \in \mathbb{Q}[x]$. If we factor $f(x)$ into a product of linear factors we get $f(x) = (x + \sqrt{2})(x - \sqrt{2})(x + i)(x - i)$. The zeros of $f(x)$ are $\pm\sqrt{2}, \pm i \in \mathbb{C}$. So a splitting field for $f(x)$ over \mathbb{Q} is $\mathbb{Q}(\sqrt{2}, i)$.

Example (3.5.2). Let $f(x) = x^2 + x + 2 \in \mathbb{Z}_3[x]$. If we factor $f(x)$ into a product of linear factors we get $f(x) = (x - (1 + i))(x - (1 + i))$. Thus $\mathbb{Z}_3(i)$ is a splitting field for $f(x)$ over \mathbb{Z}_3 .

3.2 Algebraic Extensions

This section deals with sets of elements of a field F and recognizing these elements as roots of non-zero polynomials with coefficients from a subfield of F . Algebraic extensions are fundamental in the study of algebraic closure.

Definition 3.6. Let E be an extension field of a field F and let $a \in E$. We say a is *algebraic over F* if there exists a non-zero polynomial $f(x) \in F[x]$ such that $f(a) = 0$.

Example (3.6.1). Let $f(x) = 2x - 1 \in \mathbb{Q}[x]$. Then $\frac{1}{2}$ is algebraic over \mathbb{Q} since $f(\frac{1}{2}) = 2(\frac{1}{2}) - 1 = 0$.

Example (3.6.2). Additionally, if we let $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ then $\pm\sqrt{2}$ are algebraic over \mathbb{Q} since $f(\pm\sqrt{2}) = (\pm\sqrt{2})^2 - 2 = 0$.

Definition 3.7. An extension E of F is called an *algebraic extension of F* if every element of E is algebraic over F .

Example (3.7.1). If a is algebraic over a field F , then $F(a)$ is an algebraic extension (see Theorem 3.11). In a previous example we showed that $\sqrt{2}$ is algebraic over \mathbb{Q} , thus $\mathbb{Q}(\sqrt{2})$ is an algebraic extension of \mathbb{Q} .

Definition 3.8. An extension of F of the form $F(a)$, where a is in an extension field of F , is called a *simple extension of F* .

Theorem 3.9 (Characterization of Extensions). Let E be an extension field of the field F , and let $a \in E$. If a is algebraic over F , then

- (i) $F(a) = F[a]$ and
- (ii) $F(a) \cong F[x]/(p(x))$, where $p(x) \in F[x]$ is of minimum degree such that $p(a) = 0$. Moreover, $p(x)$ is irreducible over F .

Proof. Consider the homomorphism $\varphi : F[x] \rightarrow F[a]$ given by $f(x) \rightarrow f(a)$. If a is algebraic over F , then there exists some $f(x) \in F[x]$ such that $f(a) = 0$. Hence $\ker \varphi \neq$

$\{0\}$. Since the kernel of a ring is an ideal (Theorem 2.21) and $F[x]$ is a PID (Theorem 2.18) we can write $\ker \varphi = (p(x))$ where $p(x)$ has minimum degree among all non-zero elements of $\ker \varphi$. Thus $p(a) = 0$ and since $p(x)$ is a polynomial of minimum degree with this property, it is irreducible over F .

By Theorem 2.22, $F[x]/(p(x)) = F[a]$. Since $p(x)$ is irreducible over F , by Theorem 2.27 $(p(x))$ is a maximal ideal in $F[x]$, and so $F[x]/(p(x))$ is a field by Theorem 2.16. $F[a]$ is the smallest subfield containing F and a so $F(a) \subseteq F[a]$, but we also have that $F[a]/(p(x)) \cong F[a] \subseteq F(a)$. Thus $F(a) = F[a]$. \square

Theorem 3.10 (Uniqueness Property). *If a is algebraic over a field F , then there is a unique monic irreducible polynomial $p(x) \in F[x]$ such that $p(a) = 0$.*

Proof. Let $p(x) \in F[x]$ satisfy the conditions of Theorem 3.9. Then by Theorem 3.9, $p(x)$ is irreducible and of minimum degree. Suppose a_n is the leading coefficient of $p(x)$. Let $p_1(x) = \frac{1}{a_n}p(x)$. Then $p_1(x)$ is monic, of minimum degree and satisfies $p_1(a) = 0$. Now, in order to prove uniqueness, assume there is a monic, irreducible polynomial $g(x)$ such that $g(a) = 0$. Using the division algorithm we get

$$g(x) = p_1(x)q(x) + r(x) \text{ where } q(x), r(x) \in F[x] \text{ and } r(x) = 0 \text{ or } \deg r < \deg p_1.$$

This tells us that $r(x) = g(x) - p_1(x)q(x)$. If $r(x) \neq 0$, then

$$\begin{aligned} r(a) &= g(a) - p_1(a)q(a) \\ &= 0 - 0q(a) \\ &= 0. \end{aligned}$$

This is a contradiction since $\deg r < \deg p_1$ and p_1 has minimum degree. Thus $r(x) = 0$, which means $g(x) = p_1(x)q(x)$. We know that $g(x)$ is irreducible, so either $p_1(x)$ is a unit or $q(x)$ is a unit. If $p_1(x)$ is a unit, then $p_1(a) \neq 0$ which is a contradiction, so $q(x)$ is a unit. Since $g(x)$ and $p_1(x)$ are monic polynomials, $q(x) = 1$. Hence $g(x) = p_1(x)$. Therefore $p_1(x)$ is unique. \square

If E is an extension field of F we can think of E as a vector space where scalars are elements of F . If we think about it this way we can introduce concepts familiar to vector spaces like dimension and basis. A vector space that has a dimension n has a basis

consisting of n elements. If an extension field E has dimension n as a vector space over F , we say that E has degree n over F , and E is called a *finite extension* of F .

Theorem 3.11. *If E is a finite extension of F , then E is an algebraic extension of F .*

Proof. Let E be an extension field of F , and suppose that E has degree n over F . We want to show that every element of E is algebraic over F . Let $a \in E$. The set $\{1, a, a^2, \dots, a^n\}$ is linearly dependent over F so there exists elements $c_0, c_1, c_2, \dots, c_n \in F$ such that

$$c_n a^n + c_{n-1} a^{n-1} + \dots + c_1 a + c_0 = 0.$$

If we let $f(x) = c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0$, then $f(a) = 0$. Therefore all $a \in E$ is algebraic over F , hence E is an algebraic extension of F . \square

The next theorem is an important property of algebraic extensions and has connections to integral extensions. The proof can be found in [Hun74].

Theorem 3.12 (Algebraic over Algebraic is Algebraic). *If K is an algebraic extension of E and E is an algebraic extension of F , then K is an algebraic extension of F .*

Example (3.12.1). $\mathbb{Q}[\sqrt{2}]$ is an algebraic extension of \mathbb{Q} and $\mathbb{Q}[\sqrt{2}, \sqrt{5}]$ is an algebraic extension of $\mathbb{Q}[\sqrt{2}]$. Thus $\mathbb{Q}[\sqrt{2}, \sqrt{5}]$ is an algebraic extension of \mathbb{Q} .

Corollary 3.13 (Subfield of Algebraic Elements). *Let E be an extension field of the field F . Then the set of all elements of E that are algebraic over F is a subfield of E .*

The subfield mentioned above has a special name. The elements of E that are algebraic over F make a subfield of E called the algebraic closure of F in E . It is defined in terms of an algebraically closed field in Definition 3.15.

Definition 3.14. A field F is *algebraically closed* if every polynomial in $F[x]$ has a root in F .

Definition 3.15. An *algebraic closure* of a field F is an algebraic extension field E of F that is algebraically closed.

We can also think of the algebraic closure of a field F as the smallest algebraically closed extension field containing F . Now, let us take a look at a familiar theorem and see how the previous definitions are used to classify the complex numbers.

Theorem 3.16 (Fundamental Theorem of Algebra). *Let $f \in \mathbb{C}[x]$ be a polynomial of degree at least 1. Then there exists a complex number $c \in \mathbb{C}$ such that $f(c) = 0$.*

The proof of the Fundamental Theorem of Algebra consists of concepts from the study of analysis. [Hun74] gives a sketch of the proof and assumes that every positive real number has a real positive square root and every polynomial in $\mathbb{R}[x]$ of odd degree has a root in \mathbb{R} . We can also state The Fundamental Theorem of Algebra as follows:

Theorem 3.17. *A polynomial of degree n with complex coefficients has at most n complex roots.*

This theorem tells us that every element of the complex numbers is algebraic over the complex numbers thus making it algebraically closed. Also, the field of complex numbers is the algebraic closure of the field of real numbers as is shown in the next couple of examples below.

Example (3.17.1). \mathbb{C} is algebraically closed because it contains all zeros for any $f(x) \in \mathbb{C}[x]$. To illustrate this further, take the polynomial $4x^2 + 1$ which has roots $\pm \frac{i}{2}$. This polynomial has real number coefficients but its roots are complex numbers.

Example (3.17.2). The algebraic closure of \mathbb{R} is \mathbb{C} and the algebraic closure of \mathbb{Q} is the set of all algebraic numbers, which is described as the set of elements of the complex numbers that are roots of non-zero polynomials with rational coefficients.

Chapter 4

Integral Closure

As defined in the last chapter, an element of E is algebraic over F if it is a zero of a polynomial in $F[x]$. Analogously, an element of S is integral over R if it is a zero of a monic polynomial in $R[x]$. Both algebraic and integral closures deal with having an extension field or ring that contains no proper algebraic or integral extensions within it. For example, if we look at the extension field \mathbb{C} of the real numbers \mathbb{R} , every element of \mathbb{C} is a zero of a polynomial of $\mathbb{R}[x]$ and \mathbb{C} is algebraically closed. So an algebraically closed extension E is the “smallest” extension field of F that contains all the zeros of polynomials in $F[x]$. If the rings R and S are fields then integral closure and algebraic closure are the same.

4.1 Ring/Integral Extensions

Algebraic closure and integral closure share many similarities. One of them is the concept of extensions. Algebraic extensions deal with extension fields and correspondingly, ring/integral extensions deal with extension rings.

Definition 4.1. Let S be a commutative ring with identity and R a subring of S containing 1_S . Then S is said to be an *extension ring of R* .

Example (4.1.1). Extension fields are extension rings, thus the examples of extension fields in the previous chapter are also examples of extension rings.

Example (4.1.2). However, \mathbb{Z} is not an extension ring of the set of even integers E since $1 \notin E$.

Definition 4.2. Let S be an extension ring of R . An element $x \in S$ is said to be *integral over R* if there exists an integer n and elements $r_1, \dots, r_n \in R$ such that

$$x^n + r_1x^{n-1} + \dots + r_{n-1}x + r_n = 0.$$

An element that is integral over a ring is comparable to that of an element that is algebraic over a field because we are essentially looking at elements of a ring as roots of polynomials. But in the case of an integral element, we need the polynomial to be monic. In fact, integral elements are algebraic, but algebraic elements are not necessarily integral.

Example (4.2.1). Let $\frac{1}{\sqrt{3}} \in \mathbb{R}$. Then $\frac{1}{\sqrt{3}}$ is integral over \mathbb{Q} since it is the root of $x^2 - \frac{1}{3} \in \mathbb{Q}[x]$. It is worthy to note that $\frac{1}{\sqrt{3}}$ is not integral over \mathbb{Z} because there does not exist a monic polynomial with integer coefficients in which $\frac{1}{\sqrt{3}}$ is a root.

Example (4.2.2). Similarly, the set of elements in a ring R is integral over R since $r \in R$ is a root of $x - r \in R[x]$.

Definition 4.3. If every element of S is integral over R , then S is said to be an *integral extension* of R .

Example (4.3.1). Every algebraic extension field F of a field K is an integral extension ring and \mathbb{Z} is an integral extension of \mathbb{Z} which will be shown in Example 4.7.1.

The following theorem gives another characterization of integral elements in terms of modules.

Theorem 4.4. Let S be an extension ring of R and $x \in S$. Then the following conditions are equivalent:

- (i) x is integral over R
- (ii) $R[x]$ is a finitely generated R -module
- (iii) there is a subring T of S containing 1_S and $R[x]$ which is finitely generated as an R -module
- (iv) there is an $R[x]$ submodule B of S which is finitely generated as an R -module and whose annihilator in $R[x]$ is zero.

Proof. (i) \Rightarrow (ii) Let x be integral over R . Then there exists $n \in \mathbb{N}_0$ and $r_1, \dots, r_n \in R$ such that

$$x^n + r_1x^{n-1} + \dots + r_{n-1}x + r_n = 0.$$

$R[x]$ is generated by the basis $\{x^i | i \in \mathbb{N}_0\}$ by definition. We want to show $R[x]$ is finitely generated, so we need $x^{n+m} \in R1 + Rx + \dots + Rx^{n-1}$. We have:

$$0 = x^n + r_1x^{n-1} + \dots + r_{n-1}x + r_n$$

hence we can write

$$x^n = -(r_1x^{n-1} + \dots + r_{n-1}x + r_n).$$

We will first show $x^{n+1} \in R1 + Rx + \dots + Rx^{n-1}$:

$$\begin{aligned} x^{n+1} &= x^n x \\ &= -(r_1x^{n-1} + \dots + r_{n-1}x + r_n)x \\ &= -(r_1x^n + \dots + r_{n-1}x^2 + r_nx) \\ &= -(r_1(-r_1x^{n-1} - \dots - r_{n-1}x - r_n) + \dots + r_{n-1}x^2 + r_nx) \\ &= r_1^2x^{n-1} + \dots + r_{n-1}x^2 + (r_1r_{n-1} + r_n)x + r_1r_n \\ &\in R1 + Rx + \dots + Rx^{n-1}. \end{aligned}$$

We can keep doing this m times, and so it will follow by induction that $x^{n+m} \in R1 + Rx + \dots + Rx^{n-1}$. Therefore $R[x]$ is a finitely generated R -module.

(ii) \Rightarrow (iii) Let $R[x]$ be a finitely generated R -module. If we let $T = R[x]$ then T is a subring of S and $1_S \in R[x]$.

(iii) \Rightarrow (iv) Let T , a finitely generated R -module, be a subring of S and $1_S \in T$. Now let $B = T$, $R \subset R[x] \subset T$ so B is an $R[x]$ -module that is finitely generated as an R -module. Now, suppose $uB = 0$ for some $u \in S$. Then since $1_S \in B$ we have that $u = u1_S = 0$. Thus the annihilator of B is 0.

(iv) \Rightarrow (i) Let B be a $R[x]$ -submodule of S and finitely generated as an R -module, and let $(0 : B) = 0$. Then B is generated over R by b_1, b_2, \dots, b_n and since B is an $R[x]$ -module

we know $xb_i \in B$ for $i \in \mathbb{N}$. Thus, there exists $r_{ij} \in R$ such that

$$\begin{aligned} xb_1 &= r_{11}b_1 + r_{12}b_2 + \cdots + r_{1n}b_n \\ xb_2 &= r_{21}b_1 + r_{22}b_2 + \cdots + r_{2n}b_n \\ &\vdots \\ xb_n &= r_{n1}b_1 + r_{n2}b_2 + \cdots + r_{nn}b_n. \end{aligned}$$

Now setting each equation to 0 and combining like terms gives us

$$\begin{aligned} 0 &= (r_{11} - x)b_1 + r_{12}b_2 + \cdots + r_{1n}b_n \\ 0 &= r_{21}b_1 + (r_{22} - x)b_2 + \cdots + r_{2n}b_n \\ &\vdots \\ 0 &= r_{n1}b_1 + r_{n2}b_2 + \cdots + (r_{nn} - x)b_n. \end{aligned}$$

Rewriting these equations in matrix form gives us:

$$\begin{bmatrix} r_{11} - x & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} - x & \cdots & r_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nn} - x \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Let $M = \begin{bmatrix} r_{11} - x & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} - x & \cdots & r_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nn} - x \end{bmatrix}$. Let $d \in R[x]$ be the determinant of M . If

$d \neq 0$, then we would be able to multiply on the right by M^{-1} giving us

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

But b_1, b_2, \dots, b_n are generators so they cannot be 0. Thus $d = 0$. Let f be the polynomial created by the determinant of M . Then $-f$ is a monic polynomial and x is integral over R . \square

Corollary 4.5 (Integral over Integral is Integral). *Let T be an integral extension of S and let S be an integral extension of R . Then T is an integral extension of R .*

This corollary to Theorem 4.4 has a similar structure to that of Theorem 3.12 which states algebraic extensions over algebraic extensions are also algebraic over the original field.

Proof. We are given that $R \subseteq S \subseteq T$, S is integral over R and T is integral over S . Let $t \in T$ be integral over S . Then for $s_i \in S$ we can write

$$t^n + s_{n-1}t^{n-1} + \cdots + s_1t + s_0 = 0.$$

Let $f(x) = x^n + s_{n-1}x^{n-1} + \cdots + s_1x + s_0$. Then $f \in R[s_0, s_1, \dots, s_n]$. By Theorem 4.4, $R[s_0, s_1, \dots, s_{n-1}][t]$ is a finitely generated $R[s_0, s_1, \dots, s_{n-1}]$ -module. Now we want to show that $R[s_0, s_1, \dots, s_{n-1}]$ is a finitely generated R -module. Let $R \subset R[s_0] \subset R[s_0, s_1] \subset \cdots \subset R[s_0, s_1, \dots, s_{n-1}]$. Each s_i is integral over R since S is integral over R . We know that $R[s_0, s_1, \dots, s_i] = R[s_0, s_1, \dots, s_{i-1}][s_i]$ so $R[s_0, s_1, \dots, s_i]$ is a finitely generated module over $R[s_0, s_1, \dots, s_{i-1}]$ by Theorem 4.4. We can keep doing this which will eventually show that $R[s_0, s_1, \dots, s_{n-1}]$ is a finitely generated R -module. Hence $R[s_0, s_1, \dots, s_{n-1}][t] = R[s_0, s_1, \dots, s_{n-1}, t]$ is a finitely generated R -module. Since $R[t] \subset R[s_0, s_1, \dots, s_{n-1}, t]$, t is integral over R by Theorem 4.4. \square

Definition 4.6. Let R be a ring and S an extension ring of R . The set of all elements of S that are integral over R is called the *integral closure of R in S* and is denoted by \bar{R} .

Definition 4.7. If $\bar{R} = R$, then R is said to be *integrally closed* in S .

Example (4.7.1). $\bar{\mathbb{Z}} = \mathbb{Z}$, in other words, the integers are integrally closed in the field of rational numbers. This means that if we look at all the elements in the rational numbers, the only ones that are roots of monic polynomials with integer coefficients are the integers. A short proof is included below.

Proof. First we will show $\mathbb{Z} \subseteq \bar{\mathbb{Z}}$. Let $a \in \mathbb{Z}$, then $x - a \in \mathbb{Z}[x]$. Let $f(x) = x - a$, then $f(a) = a - a = 0$. Hence $a \in \bar{\mathbb{Z}}$.

Next we will show $\bar{\mathbb{Z}} \subseteq \mathbb{Z}$. Let $\frac{c}{d} \in \bar{\mathbb{Z}}$, where $c, d \in \mathbb{Z}$ and $\gcd(c, d) = 1$. Then there exists a monic polynomial $g(x) \in \mathbb{Z}[x]$ such that $g(\frac{c}{d}) = 0$. So

$$\left(\frac{c}{d}\right)^n + a_1 \left(\frac{c}{d}\right)^{n-1} + \cdots + a_{n-1} \left(\frac{c}{d}\right) + a_n = 0.$$

Multiplying both sides by d^n gives us:

$$c^n + a_1 c^{n-1} d + \cdots + a_{n-1} c d^{n-1} + a_n d^n = 0.$$

Then subtracting c^n gives:

$$\begin{aligned} a_1 c^{n-1} d + \cdots + a_{n-1} c d^{n-1} + a_n d^n &= -c^n \\ \Rightarrow d(a_1 c^{n-1} + \cdots + a_{n-1} c d^{n-2} + a_n d^{n-1}) &= -c^n. \end{aligned}$$

Hence d divides c^n . So by Euclid's Lemma, d divides c . But $\gcd(c, d) = 1$, and so $d = 1$. Thus $\frac{c}{d} = \frac{c}{1} = c \in \mathbb{Z}$. Therefore, $\bar{\mathbb{Z}} = \mathbb{Z}$. \square

Note that the integers are not integrally closed in the field of real numbers or the complex numbers. This can be seen when taking into account the monic polynomials $x^2 - 2$ and $x^2 + 1$. Both polynomials have integer coefficients but the roots are not integers. Actually, the integral closure of the ring of integers in the field of complex numbers is called the set of algebraic integers. Those are the complex numbers that are roots of monic polynomials with integer coefficients.

Example (4.7.2). Every UFD is integrally closed. A short proof is provided below.

Proof. Let D be a unique factorization domain. Using the same structure as above we can see that $D \subseteq \bar{D}$. Now we need to show that $\bar{D} \subseteq D$. Let $cd^{-1} \in \bar{D}$ where $c, d \in D$ and assume $c, d \neq 0$. Then $c = p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r}$ and $d = q_1^{m_1} q_2^{m_2} \cdots q_s^{m_s}$ where p_i, q_i are irreducible and $p_i \neq q_j$. Since cd^{-1} is integral over D we can write

$$\begin{aligned} (cd^{-1})^n + a_1 (cd^{-1})^{n-1} + \cdots + a_{n-1} (cd^{-1}) + a_n &= 0 \\ c^n d^{-n} + a_1 c^{n-1} d^{1-n} + \cdots + a_{n-1} c d^{-1} + a_n &= 0. \end{aligned}$$

Multiplying by d^n gives us

$$\begin{aligned} c^n + a_1 c^{n-1} d + \cdots + a_{n-1} c d^{n-1} + a_n d^n &= 0 \\ \Rightarrow a_1 c^{n-1} d + \cdots + a_{n-1} c d^{n-1} + a_n d^n &= -c^n \\ \Rightarrow d(a_1 c^{n-1} + \cdots + a_{n-1} c d^{n-2} + a_n d^{n-1}) &= -c^n \\ \Rightarrow q_1^{m_1} q_2^{m_2} \cdots q_s^{m_s} (a_1 c^{n-1} + \cdots + a_{n-1} c d^{n-2} + a_n d^{n-1}) &= -(p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r})^n. \end{aligned}$$

Since $p_i \neq q_i$, we have $a_1 c^{n-1} + \cdots + a_{n-1} c d^{n-2} + a_n d^{n-1} = (p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r})^n$. Thus $d = q_1^{m_1} q_2^{m_2} \cdots q_s^{m_s} = 1$. Therefore $cd^{-1} = c \in D$ so $\bar{D} \subseteq D$. \square

Theorem 4.8. *Let R be a subring of the commutative ring S and let \bar{R} be the integral closure of R in S . Then \bar{R} is integrally closed in S .*

In other words, let R be a ring and \bar{R} be the integral closure of R . If you want to find the integral closure of the integral closure (\bar{R}) you will just end up with the original closure of R which is \bar{R} . So taking the integral closure of the integral closure two, three, four, up to n -times, will result in the original integral closure of the ring.

Proof. We want to show that $\bar{\bar{R}} = \bar{R}$. Let $\bar{\bar{R}}$ be the integral closure of \bar{R} . We know $R \subseteq \bar{R} \subseteq \bar{\bar{R}}$. By Corollary 4.5 \bar{R} is integral over R and $\bar{\bar{R}}$ is integral over \bar{R} , and so $\bar{\bar{R}}$ is integral over R . Thus $\bar{\bar{R}} = \bar{R}$, so \bar{R} is integrally closed in S . \square

We can also characterize integral closure in terms of other mathematical concepts. The following theorems give us a connection between the integral closure of a ring in terms of ideals.

Theorem 4.9. *Let \bar{R} be the integral closure of R in its quotient field K . Then*

$$\bar{R} = \bigcup \{(I :_K I) \mid I \text{ is a finitely generated ideal of } R\}$$

Proof. First we will show $\bar{R} \subseteq \bigcup \{(I :_K I) \mid I \text{ is a finitely generated ideal of } R\}$. Let $x \in \bar{R}$, we want to show $xI \subseteq I$ for some finitely generated ideal I of R . Let $x \in K$. We can write $x = \frac{a}{b}$ for some $a, b \in R$ and $b \neq 0$. Since x is integral over R , for $a_i \in R$ we have the equation

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

Hence we can write $x^n = -a_1 x^{n-1} - \cdots - a_{n-1} x - a_n$ which is in the finitely generated ideal $J = (1, x, x^2, \dots, x^{n-1})$. Thus $J = (1, \frac{a}{b}, (\frac{a}{b})^2, \dots, (\frac{a}{b})^{n-1})$ and $xJ \subseteq J$. Let $I = b^n J$, then $I = (b^n, ab^{n-1}, a^2 b^{n-2}, \dots, a^{n-1} b)$ which is a finitely generated ideal of R . Therefore $xI = x b^n J \subseteq b^n J = I$, and so $xI \subseteq I$.

Now we will show $\bigcup \{(I :_K I) \mid I \text{ is a finitely generated ideal of } R\} \subseteq \bar{R}$. Let $x \in (I : I)$ for some finitely generated ideal I . Then $xI \subseteq I$ where $I = (a_1, a_2, \dots, a_n)$, $a_i \in R$ and $a_i \neq 0$. Now we can write xI as x multiplied by each of the generators of I

so that for $c_{ij} \in R$, we have the equations

$$\begin{aligned} xa_1 &= c_{11}a_1 + c_{12}a_2 + \cdots + c_{1n}a_n \\ xa_2 &= c_{21}a_1 + c_{22}a_2 + \cdots + c_{2n}a_n \\ &\vdots \\ xa_n &= c_{n1}a_1 + c_{n2}a_2 + \cdots + c_{nn}a_n. \end{aligned}$$

Now setting each equation to 0 and combining like terms gives us

$$\begin{aligned} 0 &= (c_{11} - x)a_1 + c_{12}a_2 + \cdots + c_{1n}a_n \\ 0 &= c_{21}a_1 + (c_{22} - x)a_2 + \cdots + c_{2n}a_n \\ &\vdots \\ 0 &= c_{n1}a_1 + c_{n2}a_2 + \cdots + (c_{nn} - x)a_n. \end{aligned}$$

Rewriting these equations in matrix form gives us:

$$\begin{bmatrix} c_{11} - x & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} - x & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} - x \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Let $A = \begin{bmatrix} c_{11} - x & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} - x & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} - x \end{bmatrix}$. If $\det A \neq 0$ then there exists an A^{-1} so that

when we multiply on the right by A^{-1} we get

$$\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

But $a_1, a_2, \dots, a_n \neq 0$, so $\det A = 0$. Let f be the polynomial created by the determinant of A . Then $-f$ is a monic polynomial and x is integral over R . Thus, $x \in \bar{R}$. \square

4.2 Applications of Integral Closure: Dedekind Domains

The Fundamental Theorem of Arithmetic states that any integer greater than 1 is a prime or a product of primes and this product is unique, except for the order in which the factors appear. This concept can be extended to rings in general and is especially clear in the case of the ring of integers. The ring of integers is a principal ideal domain and every ideal is a unique product of prime ideals. This leads us to the discussion of Dedekind Domains and shows a connection between prime elements of a ring R and prime principal ideals in R . The main result of this section is Theorem 4.16 which portrays Dedekind domains in several ways.

Definition 4.10. A *Dedekind domain* is an integral domain R in which every ideal ($\neq R$) is the product of a finite number of prime ideals

Example (4.10.1). Every principal ideal domain is Dedekind.

Proof. Let R be a PID. Then R is also a UFD by Theorem 2.25. Let A be an ideal of R . Then $A = (a)$. Since R is a UFD, $(a) = (p_1 p_2 \cdots p_n)$ where p_1, p_2, \dots, p_n are irreducible. But in a PID irreducible implies prime so $(a) = (p_1)(p_2) \cdots (p_n)$ where $(p_1), (p_2), \dots, (p_n)$ are prime ideals. Thus R is a Dedekind domain. \square

From this example we can say that \mathbb{Z} is a Dedekind domain since it is a principal ideal domain.

Definition 4.11. Let R be an integral domain with quotient field K . A *fractional ideal* of R is a non-zero R submodule I of K such that $aI \subset R$ for some non-zero $a \in R$.

Since we have introduced this new definition we need to specify between a fractional ideal and *ordinary ideal*. An ordinary ideal is an ideal that is contained in R , whereas a fractional ideal may not be contained in R . We can think of the element $a \in I$ as the element that divides out the “denominators” of the elements in I so that I becomes an ordinary ideal. The element $6 \in \mathbb{Z}$ in Example 4.11.1 below does this exact thing.

Example (4.11.1). Let $R = \mathbb{Z}$ and $K = \mathbb{Q}$. The set of elements $\frac{1}{3}\mathbb{Z}$ is a fractional ideal because $6 \left(\frac{1}{3}\mathbb{Z} \right) \subset \mathbb{Z}$ and $6 \in \mathbb{Z}$.

Example (4.11.2). Every ordinary non-zero ideal I in an integral domain R is a fractional ideal of R , and every fractional ideal of R that is contained in R is an ordinary ideal of R . It is good to note that if I is a fractional ideal of a domain R and $aI \subset R$ ($0 \neq a \in R$), then aI is an ordinary ideal in R and the map $I \rightarrow aI$ given by $x \mapsto ax$ is an R module isomorphism ($a \in R$ “clears the denominator” of I since $I \subseteq K$).

Theorem 4.12. *If R is an integral domain with quotient field K , then the set of all fractional ideals of R forms a commutative monoid, with identity R and multiplication given by Definition 2.34.*

Proof. Let \mathbf{A} be the set of all fractional ideals of R . We want to show that \mathbf{A} is a commutative monoid. First we will show that multiplication is closed in \mathbf{A} . That is, the product of fractional ideals are fractional ideals. Let $A_1, A_2 \in \mathbf{A}$. Since A_1 and A_2 are fractional ideals, there exists $r_1, r_2 \in R$ such that $r_1 A_1 \subset R$ and $r_2 A_2 \subset R$. Then $r_1 r_2 A_1 A_2 = r_1 A_1 r_2 A_2 \subset R$. Thus $A_1 A_2$ is a fractional ideal of R .

Next we will show that multiplication is associative. Let $A_1, A_2, A_3 \in \mathbf{A}$. Then $A_1(A_2 A_3) = A_1 A_2 A_3 = (A_1 A_2) A_3$ since each of the A_i 's are ideals of the ring K and associativity of ideals holds in a ring.

Lastly we show that the identity of \mathbf{A} is R . Since each A_i is an R -module we know that $RA_i \subseteq A_i$ and $A_i \subseteq RA_i$. Thus $RA_i = A_i$. Hence, \mathbf{A} is commutative monoid with identity R . \square

Definition 4.13. A fractional ideal I of an integral domain R is said to be *invertible* if $IJ = R$ for some fractional ideal J of R .

Note that the invertible fractional ideals are precisely those that have inverses in the monoid of all fractional ideals. Some properties of fractional ideals are listed below.

Property (4.13.1). The inverse of an invertible fractional ideal I is unique and is defined to be $I^{-1} = \{a \in K \mid aI \subset R\}$. It is unique because if A and B are inverses of I then $AI = R$ and $BI = R$ so $AI = BI \Rightarrow A = B$. The following property is similar to that of cancellation. Let I, A, B be fractional ideals of R such that $IA = IB$ and I is invertible, then

$$A = RA = (I^{-1}I)A = I^{-1}(IB) = RB = B.$$

Now, if I is an ordinary ideal in R then $R \subset I^{-1}$.

Property (4.13.2). We can also say that every non-zero principal ideal in an integral domain R is invertible. For example, let us look at the principal ideal $(2) \in \mathbb{Z}$. The inverse of this ideal is

$$(2)^{-1} = \{a \in \mathbb{Q} \mid a(2) \subset \mathbb{Z}\} = \frac{1}{2}\mathbb{Z}.$$

Property (4.13.3). Lastly, if K is the quotient field of R and $I = (b), b \neq 0$, let $J = Rc \subset K$ where $c = 1/b$. Then J is a fractional ideal of R such that $IJ = R$.

Lemma 4.14. Let I, I_1, I_2, \dots, I_n be ideals in an integral domain R .

- (i) The ideal $I_1 I_2 \cdots I_n$ is invertible if and only if each I_j is invertible.
- (ii) If $P_1 P_2 \cdots P_m = I = Q_1 Q_2 \cdots Q_n$, where P_i and Q_j are prime ideals in R and every P_i is invertible, then $m = n$ and (after re-indexing) $P_i = Q_i$ for each $i = 1, \dots, m$.

Proof. (i) Let I, I_1, I_2, \dots, I_n be ideals in an integral domain R .

(\Rightarrow) Let $I I_1 I_2 \cdots I_n$ be invertible and let J be a fractional ideal such that $J(I_1 I_2 \cdots I_n) = R$. Then $I_j(J I_1 \cdots I_{j-1} I_{j+1} \cdots I_n) = R$ since R is commutative and associative. Thus I_j is invertible. We can do this for each $I_j, j \in \mathbb{N}$.

(\Leftarrow) Let each $I_j, j \in \mathbb{N}$ be invertible. Then

$$(I_1 \cdots I_n)(I_1^{-1} \cdots I_n^{-1}) = I_1 I_1^{-1} I_2 I_2^{-1} \cdots I_n I_n^{-1} = R$$

Thus $I_1 \cdots I_n$ is invertible.

(ii) We will prove the second part using the principle of mathematical induction. Let $m = 1$. Then $P_1 = I = Q_1 Q_2 \cdots Q_n$. So $Q_i \subseteq P_1$ for some i since P_1 is prime. Suppose $Q_1 \subseteq P_1$. Then $Q_1 \subseteq P_1 = Q_1 Q_2 \cdots Q_n \subseteq Q_1$. Hence $Q_1 = P_1$. Now if $n > 1$, since $P_1 = Q_1$ is invertible, we get $P_1 = P_1 Q_2 \cdots Q_n$ so that $R = Q_2 \cdots Q_n$. This can't happen since $Q_2 \cdots Q_n$ is a proper ideal of R .

If $m > 1$,

Choose a P_i , say P_1 such that P_1 does not properly contain P_i for $i = 2, \dots, m$. Then $Q_1 Q_2 \cdots Q_n = P_1 P_2 \cdots P_m \subset P_1$. Since P_1 is prime there is a $Q_j \subset P_1$ for some $j = 1, 2, \dots, n$, say $Q_1 \subset P_1$. Similarly, because $P_1 P_2 \cdots P_m = Q_1 Q_2 \cdots Q_n \subset Q_1$ and Q_1 is prime, there is a $P_i \subset Q_1$ for some i . Since P_1 does not properly contain P_i , then $P_i = P_1$. Since $P_1 = Q_1$ is invertible this implies that $P_2 P_3 \cdots P_m = Q_2 Q_3 \cdots Q_n$. We can keep going and thus after reindexing we get $P_i = Q_i$ for $i = 1, 2, \dots, m$. \square

In a principal ideal domain, prime ideals are also maximal ideals and we have that every non-zero principal ideal in an integral domain is invertible. Putting these two concepts together show that every non-zero prime ideal in a principal ideal domain is invertible and maximal, which leads to the following theorem.

Theorem 4.15. *If R is a Dedekind Domain, then every non-zero prime ideal of R is invertible and maximal.*

Proof. Let R be a Dedekind domain. Hence R is an integral domain and every ideal of R is a product of primes. We will first show that every invertible prime ideal P is maximal. Let $a \in R, a \notin P$. Assume that $P + Ra \neq R$. Since R is a Dedekind domain we can write every ideal as a product of primes. P is a prime ideal and Ra and $P + Ra$ are ideals. Hence,

$$\begin{aligned} P + Ra &= P_1 P_2 \dots P_m \text{ and} \\ P + Ra^2 &= Q_1 Q_2 \dots Q_n \text{ where } P_i, Q_j \text{ are prime ideals.} \end{aligned}$$

Let $\pi : R \rightarrow R/P$ be the canonical epimorphism. So $\pi(a) = a + P$, $\pi(a^2) = a^2 + P$ and π is a surjective homomorphism. Consider the principal ideals in R/P generated respectively by $\pi(a)$ and $\pi(a^2)$. We have

$$(\pi(a)) = \pi(P_1 \dots P_m) = \pi(P_1) \pi(P_2) \dots \pi(P_m) \text{ and}$$

$$(\pi(a^2)) = \pi(Q_1) \pi(Q_2) \dots \pi(Q_n)$$

Since $\ker \pi = P \subset P_1$ and $P \subset Q_i$ for each i , the ideals $\pi(P_i)$ and $\pi(Q_i)$ are prime by Theorem 2.29.

R/P is an integral domain since P is a prime ideal, and so every non-zero principal ideal in R/P is invertible. Therefore, since $(\pi(a))$ is a principal ideal in R/P , it is invertible; which means $\pi(P_1) \pi(P_2) \dots \pi(P_m)$ is invertible and so each $\pi(P_i)$ is invertible (Lemma 4.14(i)). Similarly, each $\pi(Q_i)$ are invertible since

$$\begin{aligned} \pi(Q_1) \dots \pi(Q_n) &= (\pi(a^2)) \\ &= (\pi(a))^2 \\ &= \pi(P_1)^2 \dots \pi(P_m)^2. \end{aligned}$$

Using Lemma 4.14(ii), we let $n = 2m$ and reindex to get

$$\pi(P_i) = \pi(Q_{2i}) = \pi(Q_{2i-1}), \quad i = 1, 2, \dots, m$$

Thus, $\ker \pi = P \subset P_i$ and $P \subset Q_j$ for all i, j . Hence

$$P_i = \pi^{-1}(\pi(P_i)) = \pi^{-1}(\pi(Q_{2i})) = Q_{2i}$$

and similarly $P_i = Q_{2i-1}$ for $i = 1, 2, \dots, m$.

Now, $P + Ra^2 = Q_1 \dots Q_n = P_1^2 \dots P_m^2 = (P_1 \dots P_m)^2 = (P + Ra)^2$ and $P \subset P + Ra^2 \subset (P + Ra)^2 \subset P^2 + Ra$. If $b = c + ra \in P$ ($c \in P, r \in R$), then $ra \in P$. So $r \in P$ since P is prime and $a \notin P$. Thus $P \subseteq P^2 + Pa \subseteq P$ which implies $P = P^2 + Pa = P(P + Ra)$. Since P is invertible

$$\begin{aligned} R &= P^{-1}P \\ &= P^{-1}P(P + Ra) \\ &= P + Ra \end{aligned}$$

This is a contradiction because we assumed that $R \neq P + Ra$. Therefore, every invertible prime ideal is maximal.

Now suppose P is any non-zero prime ideal in R and c is a non-zero element of P . Then $(c) = P_1 P_2 \dots P_m \subset P$ for P_i prime. Then $P_k \subset P$ for some k since P is prime. Therefore (c) is invertible because it is a principal ideal. Hence, P_k is invertible by Lemma 4.14. By the first part, P_k is maximal so $P_k = P$. Therefore, P is invertible and maximal. \square

Example (4.15.1). Let F be a field. The principal ideals (x_1) and (x_2) in $F[x_1, x_2]$ are prime but not maximal since $(x_1) \subset (x_1, x_2) \subset F[x_1, x_2]$. Thus $F[x_1, x_2]$ is not Dedekind.

Theorem 4.16. *The following conditions on an integral domain R are equivalent:*

- (i) R is a Dedekind domain;
- (ii) Every proper ideal in R is uniquely a product of a finite number of prime ideals;
- (iii) Every non-zero ideal in R is invertible;
- (iv) Every fractional ideal of R is invertible;
- (v) R is integrally closed, every ideal is finitely generated and every non-zero prime ideal is maximal.

This theorem allows us to define a Dedekind domain using different concepts in algebra. It relates Dedekind domains not only to prime ideals but to invertible fractional ideals and integrally closed, finitely generated prime ideals. Part (v) of this theorem supports our claim in the beginning of this section, that the ring of integers, \mathbb{Z} , is a Dedekind domain. This is because the ring of integers is integrally closed and is a principal ideal domain (Example 2.17.2) so every ideal of \mathbb{Z} is finitely generated and every non-zero prime ideal of \mathbb{Z} is maximal (Example 2.17.1). For the proof of this theorem see [Hun74].

Chapter 5

Integral Closure of an Ideal

The integral closure of an ideal is very similar to that of the integral closure of a ring. In fact it seems almost verbatim. We are still dealing with roots of monic polynomials however, a noticable difference is that in the integral closure of an ideal the coefficients of the polynomials are elements of powers of the ideal. But this can also be said of the coefficients of the polynomial in the integral closure of a ring. This is because when we take powers of a ring R , we get back the entire ring R . But when we take powers of an ideal I in a ring R , the powers are subsets of the ideal I . Another difference between integral closure of a ring and integral closure of an ideal in a ring is that integral elements over an ideal stay within the ring R while integral elements over a ring R can be in an extension of the ring R .

5.1 Definitions

We first define what it means for an element to be integral over an ideal in a ring.

Definition 5.1. Let I be an ideal in a ring R . An element $r \in R$ is said to be *integral over I* if there exists an integer n and elements $a_i \in I^i$, $i = 1, 2, \dots, n$, such that

$$r^n + a_1 r^{n-1} + a_2 r^{n-2} + \dots + a_{n-1} r + a_n = 0.$$

Definition 5.2. The set of all elements that are integral over I is called the *integral closure of I* and is denoted \bar{I} .

Example (5.2.1). Consider the ideal $I = (x^2, y^2)$ in the ring $R[x, y]$. The element $xy \in R[x, y]$ is in the integral closure of I because $(xy)^2 + 0(xy) + -x^2y^2 = 0$.

Lemma 5.3. *An ideal I is contained in its integral closure, that is $I \subseteq \bar{I}$.*

Proof. Let $a \in I$, then $x - a \in I[x]$. So for $f(x) = x - a$ we have $f(a) = 0$, hence $a \in \bar{I}$. Thus $I \subseteq \bar{I}$. \square

Definition 5.4. If $I = \bar{I}$, then I is *integrally closed*. If $I \subseteq J$ are ideals, we say J is integral over I if $J \subseteq \bar{I}$.

Example (5.4.1). Radical ideals are integrally closed. See note after Lemma 5.11.

Example (5.4.2). Prime ideals are integrally closed. A short proof is provided below:

Proof. Let P be a prime ideal, we want to show that $P = \bar{P}$. We know $I \subseteq \bar{I}$ for any ideal I as noted above. Hence, $P \subseteq \bar{P}$. Now we need to show $\bar{P} \subseteq P$. Let $b \in \bar{P}$. Then there exists an $f(x) \in P[x]$ such that

$$f(b) = b^n + a_1b^{n-1} + \cdots + a_{n-1}b + a_n = 0 \text{ for } a_i \in P^i.$$

Subtracting a_n from both sides and factoring out a b gives us

$$\begin{aligned} b^n + a_1b^{n-1} + \cdots + a_{n-1}b &= -a_n. \\ b(b^{n-1} + a_1b^{n-2} + \cdots + a_{n-1}) &= -a_n. \end{aligned}$$

Since $a_n \in P$, $b(b^{n-1} + a_1b^{n-2} + \cdots + a_{n-1}) \in P$. Since P is prime either $b \in P$ or $b^{n-1} + a_1b^{n-2} + \cdots + a_{n-1} \in P$. If $b \in P$, then we're done. If $b^{n-1} + a_1b^{n-2} + \cdots + a_{n-1} \in P$, then $b^{n-1} \in P$ because each $a_ib^{n-i-1} \in P$. So $b \in P$. Therefore $P = \bar{P}$. \square

If we consider the ring R to be an ideal of R then the integral closure of the ideal R in the ring R is R , but the integral closure of the ring R may be larger.

5.2 Theorems

The theorem below tells us that the integral closure of an ideal is an ideal in the same way that the integral closure of a ring is a ring and the algebraic closure of a field is a field. Going further down to Theorem 5.9, we see that the integral closure of an

ideal is an integrally closed ideal. The proofs for Theorem 5.8 and 5.9 below follow from Swanson and Huneke's text [SH06]. They use a clever approach via reductions (which is defined below) to simplify this proof.

Definition 5.5. Let $J \subseteq I$ be ideals. J is said to be a *reduction* of I if there exists a non-negative integer n such that $I^{n+1} = JI^n$.

We can think of the last statement as $I \cdot I^n = JI^n$. So simply put, a reduction of an ideal is a subset of that ideal such that the product stays the same. So we are “reducing” the ideal but keeping the product the same. The next lemma uses the idea of reduction and relates it to integral closure.

Lemma 5.6. Let R be a ring. For any element $r \in R$ and ideal $I \subseteq R$, $r \in \bar{I}$ if and only if there exists an integer n such that $(I + (r))^n = I(I + (r))^{n-1}$.

Proof. (\Rightarrow) Let $r \in \bar{I}$. Then we can write

$$r^n + a_1 r^{n-1} + \cdots + a_{n-1} r + a_n = 0 \text{ for some } a_i \in I^i.$$

$$\text{So } -a_1 r^{n-1} - \cdots - a_{n-1} r - a_n = r^n.$$

This shows that $r^n \in I(I + (r))^{n-1}$ and hence $(I + (r))^n = I(I + (r))^{n-1}$. (\Leftarrow) Let $I(I + (r))^{n-1} = (I + (r))^n$ for some n . Then $r^n \in (I + (r))^n = I(I + (r))^{n-1}$. So $r^n \in I(I + (r))^{n-1}$. Thus

$$r^n = xx_n + xx_{n-1}r + xx_{n-2}r^2 + \cdots + xx_1r^{n-1}$$

where $x \in I$ and $x_i \in I^{i-1}$ for $i = 1, 2, \dots, n$. So each $xx_i \in II^{i-1} = I^i$. Now, let $a_i = xx_i$ for $i = 1, 2, \dots, n$. Then

$$r^n = a_1 r^{n-1} + a_2 r^{n-2} + \cdots + a_{n-1} r + a_n \text{ for some } a_i \in I^i.$$

Now, subtracting r^n gives us

$$-r^n + a_1 r^{n-1} + a_2 r^{n-2} + \cdots + a_{n-1} r + a_n = 0 \text{ for some } a_i \in I^i.$$

Thus, $r \in \bar{I}$. □

The following lemma is also used to prove Theorems 5.8 and 5.9. It shows that the reduction property is transitive.

Lemma 5.7. *Let $I \subseteq J \subseteq K$ be ideals in R .*

- (i) *If I is a reduction of J and J is a reduction of K , then I is a reduction of K .*
- (ii) *If I is a reduction of K , then J is a reduction of K .*
- (iii) *If K is finitely generated, $J = I + (r_1, r_2, \dots, r_k)$ and I is a reduction of K , then I is a reduction of J .*

Proof. (i) Let $I \subseteq J$ and $J \subseteq K$ be reductions. Then by Definition 5.5 there are integers n and m such that $IJ^n = J^{n+1}$ and $JK^m = K^{m+1}$. We know that $K^{m+1} = JK^m$, so if we increase the power of K by 1 we get $K^{m+2} = JK^{m+1} = J^2K^m$. We can keep increasing the power of K so that we get $K^{m+n} = J^nK^m$. Hence we can write

$$K^{m+n+1} = J^{n+1}K^m = IJ^nK^m \subseteq IK^{m+n} \subseteq K^{m+n+1}.$$

So actually $K^{m+n+1} = IK^{m+n}$, thus by Definition 5.5 I is a reduction of K .

(ii) Let $I \subseteq K$ be a reduction. Then there exists an integer n such that $K^{n+1} = IK^n \subseteq JK^n \subseteq K^{n+1}$. Thus $JK^n = K^{n+1}$ so by Definition 5.5, J is a reduction of K .

(iii) Let K be finitely generated, $J = I + (r_1, r_2, \dots, r_k)$ and I a reduction of K . Then there exists an integer n such that $IK^n = K^{n+1}$. By part (ii) $I + (r_1, r_2, \dots, r_{i-1})$ is a reduction of K for all $i = 0, 1, \dots, k$. Since $I \subseteq I + (r_1, r_2, \dots, r_k) \subseteq K$, then each $r_i \in K$. So $r_iK^n \in K^{n+1} = IK^n \subseteq (I + (r_1, r_2, \dots, r_{i-1}))K^n$. Hence $r_i \in (I + (r_1, r_2, \dots, r_{i-1}))K^n : K^n$. Following this, $r_iK^n \subseteq (I + (r_1, r_2, \dots, r_{i-1}))K^n$ where $K^n = (a_1, a_2, \dots, a_m)$ since K is finitely generated. We can write r_iK^n as r_i multiplied by the generators of K^n so that for each $x_{ij} \in R$ we have

$$\begin{aligned} r_ia_1 &= x_{11}a_1 + x_{12}a_2 + \dots + x_{1m}a_m \\ r_ia_2 &= x_{21}a_1 + x_{22}a_2 + \dots + x_{2m}a_m \\ &\vdots \\ r_ia_m &= x_{m1}a_1 + x_{m2}a_2 + \dots + x_{mm}a_m. \end{aligned}$$

Now setting each equation to 0 and combining like terms gives us

$$\begin{aligned} 0 &= (x_{11} - r_i)a_1 + x_{12}a_2 + \dots + x_{1m}a_m \\ 0 &= x_{21}a_1 + (x_{22} - r_i)a_2 + \dots + x_{2m}a_m \\ &\vdots \\ 0 &= x_{m1}a_1 + x_{m2}a_2 + \dots + (x_{mm} - r_i)a_m. \end{aligned}$$

Rewriting these equations in matrix form gives us:

$$\begin{bmatrix} x_{11} - r_i & x_{12} & \cdots & x_{1m} \\ x_{21} & x_{22} - r_i & \cdots & x_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mm} - r_i \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Let $A = \begin{bmatrix} x_{11} - r_i & x_{12} & \cdots & x_{1m} \\ x_{21} & x_{22} - r_i & \cdots & x_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mm} - r_i \end{bmatrix}$. If $\det A \neq 0$ then there exists an A^{-1} so

that when we multiply on the right by A^{-1} we get

$$\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

But $a_1, a_2, \dots, a_n \neq 0$, so $\det A = 0$. Let f be the polynomial created by the determinant of A . Then $-f$ is a monic polynomial and r_i is integral over R . Thus, $x \in \overline{I + (r_1, r_2, \dots, r_{i-1})}$. Hence, r_i is integral over $I + (r_1, r_2, \dots, r_{i-1})$ so by Lemma 5.6 $I + (r_1, r_2, \dots, r_{i-1})$ is a reduction of $I + (r_1, r_2, \dots, r_i)$. Therefore by part (i) and induction of k , $I \subseteq I + (r_1, r_2, \dots, r_k) = J$ is a reduction. \square

Theorem 5.8. *The integral closure of an ideal in a ring is an ideal (\bar{I} is an ideal).*

Proof. Let I be an ideal. We first show that \bar{I} is non-empty. Since I is an ideal, $I \neq \emptyset$. So let $a \in I$. Then $a \in \bar{I}$ by Lemma 5.3. Thus $\bar{I} \neq \emptyset$. Next we need to show that \bar{I} is closed under multiplication by elements of R . Let $r \in \bar{I}$ and $t \in R$. Then

$$r^n + a_1 r^{n-1} + \cdots + a_{n-1} r + a_n = 0 \text{ for some } a_i \in I^i.$$

Multiplying by t^n gives us

$$\begin{aligned} t^n r^n + a_1 t^n r^{n-1} + \cdots + a_{n-1} t^n r + a_n t^n &= 0 \\ \text{or } (tr)^n + a_1 t(tr)^{n-1} + \cdots + a_{n-1} t^{n-1}(tr) + a_n t^n &= 0 \end{aligned}$$

We know that $a_i t^i \in \bar{I}^i$ since $a_i \in \bar{I}^i$ and $t^i \in R$. Thus $tr \in \bar{I}$.

Now we need to prove that \bar{I} is closed under addition. Let $r, s \in \bar{I}$. Then we can write

$$r^n + a_1 r^{n-1} + \cdots + a_{n-1} r + a_n = 0 \text{ for some } a_i \in I^i \text{ and}$$

$$s^n + b_1 s^{n-1} + \cdots + b_{n-1} s + b_n = 0 \text{ for some } b_i \in I^i.$$

There exists a finitely generated ideal $I' \subseteq I$ such that $a_i \in (I')^i$. Thus $r \in \bar{I}'$. We can say the same thing about s and by possibly extending I' we get $s \in \bar{I}'$. Now let $J = I' + (r)$ and $K = I' + (r, s) = J + (s)$. We know $I' \subseteq J \subseteq K$, and by Lemma 5.6 I' is a reduction of J and J is a reduction of K . So I' is a reduction of K by Lemma 5.7. I' , J and K are all finitely generated and $I' \subseteq I' + (r + s) \subseteq K$ so by Lemma 5.7, I' is a reduction of $I' + (r + s)$. Thus by Lemma 5.6 $r + s$ is integral over I' . Hence, $r + s \in \bar{I}$. Thus I is an ideal. \square

Theorem 5.9. *For any ideal I , the integral closure of I is integrally closed, in symbols: $\bar{\bar{I}} = \bar{I}$.*

Proof. First, by Lemma 5.3, we know that $\bar{I} \subseteq \bar{\bar{I}}$. Now, let I be an ideal of R and $r \in \bar{\bar{I}}$. Then there exists a finitely generated submodule $J \subseteq \bar{I}$ such that $r \in \bar{J}$. We can write $J = (j_1, j_2, \dots, j_n)$. Similarly there exists a finitely generated ideal $K \subseteq I$ such that each j_i is integral over K . By Lemma 5.7, K is a reduction of $K + J$ and $K + J$ is a reduction of $K + J + (r)$. So K is a reduction of $K + (r)$. Thus r is integral over K by Lemma 5.6 and hence over I . \square

Theorem 5.10. *If $I \subseteq J$, then $\bar{I} \subseteq \bar{J}$.*

Proof. Let $r \in \bar{I}$, then we can write

$$r^n + a_1 r^{n-1} + \cdots + a_{n-1} r + a_n = 0 \text{ for } a_i \in I^i.$$

Since $I^i \subseteq J^i$, then $a_i \in J^i$. Therefore, $r \in \bar{J}$ so $\bar{I} \subseteq \bar{J}$. \square

Lemma 5.11. $I \subseteq \bar{I} \subseteq \sqrt{I}$.

Proof. By Lemma 5.3, we have that $I \subseteq \bar{I}$. Next we will show $\bar{I} \subseteq \sqrt{I}$. Let $b \in \bar{I}$. Then

$$b^n + a_1 b^{n-1} + \cdots + a_{n-1} b + a_n = 0 \text{ for } a_i \in I^i.$$

From this equation we get:

$$-b^n = a_1 b^{n-1} + \cdots + a_{n-1} b + a_n$$

Where $a_1 \in I$, $a_2 \in I^2 \subset I$, ..., $a_n \in I^n \subset I$, so $a_i \in I$ for each i . This means $a_1 b^{n-1} + \cdots + a_{n-1} b + a_n \in I$ because I is ideal. Hence $b^n \in I$, and so $b \in \sqrt{I}$. Therefore $I \subseteq \bar{I} \subseteq \sqrt{I}$. \square

This brings up an interesting notion. We have that if $\sqrt{I} = I$ then $\sqrt{I} = \bar{I}$ because $I \subseteq \bar{I} \subseteq \sqrt{I}$. But we cannot necessarily say that $\sqrt{I} = \bar{I}$ because if $b \in \sqrt{I}$ then $b^n \in I$, but b^n is not necessarily an element of I^n . Thus radical ideals ($\sqrt{I} = I$) are integrally closed, but the radical of I need not be equal to the integral closure of I .

Theorem 5.12. *If I and J are integrally closed, then $I \cap J$ is integrally closed.*

Proof. We want to show that $\overline{I \cap J} = I \cap J$ for $I = \bar{I}$ and $J = \bar{J}$. By Lemma 5.6 we have that $I \cap J \subseteq \overline{I \cap J}$. Now we have to show $\overline{I \cap J} \subseteq I \cap J$. Since $I = \bar{I}$ and $J = \bar{J}$, then $\bar{I} \cap \bar{J} = I \cap J$. Let $b \in \overline{I \cap J}$. Then

$$f(b) = b^n + r_1 b^{n-1} + \cdots + r_{n-1} b + r_n = 0, \text{ for } r_i \in (I \cap J)^i.$$

Since $r_i \in I^i$ and $r_i \in J^i$ then $f(b) \in I[x]$ and $f(b) \in J[x]$. Thus $f(b) \in I[x] \cap J[x]$ so $b \in \bar{I} \cap \bar{J}$. Therefore $\overline{I \cap J} = I \cap J$. \square

This next theorem shows how the integral closure of an ideal is related to the integral closure of a ring. Basically the integral closure of an ideal is the extension of the original ideal into the closure of the ring and then contracted back into the ring.

Theorem 5.13. *$I\bar{R} \cap R = \bar{I}$ for all ideals I of R .*

Proof. First we will show $I\bar{R} \cap R \subseteq \bar{I}$. Let $b \in I\bar{R} \cap R$. Then $b \in I\bar{R}$ and $b \in R$.

Case 1: $b = cd$ for $c \in I$ and $d \in \bar{R}$.

Since $d \in \bar{R}$, d is the root of a monic polynomial with coefficients in R , i.e.

$$d^n + r_1 d^{n-1} + \cdots + r_{n-1} d + r_n = 0.$$

Multiplying by $c^n \in I^n$ gives us

$$\begin{aligned} c^n d^n + r_1 c^n d^{n-1} + \cdots + r_{n-1} c^n d + r_n c^n &= 0 \\ (cd)^n + r_1 c(cd^{n-1}) + \cdots + r_{n-1} c^{n-1}(cd) + r_n c^n &= 0. \end{aligned}$$

Since $r_1c \in I, r_2c^2 \in I^2, \dots, r_nc^n \in I^n$, we have the equation

$$b^n + r_1cb^{n-1} + \dots + r_{n-1}c^{n-1}b + r_nc^n = 0 \text{ for all } r_ic^i \in I^i.$$

Therefore, $b \in \bar{I}$.

Case 2: $b = \sum_{i=1}^n c_id_i$ for $c_i \in I$ and $d_i \in \bar{R}$.

By Theorem 5.8, \bar{I} is an ideal and by the previous case each c_id_i is in \bar{I} , and hence $b \in \bar{I}$. Therefore $I\bar{R} \cap R \subseteq \bar{I}$. Now we will show $\bar{I} \subseteq I\bar{R} \cap R$. Let $b \in \bar{I}$. Then b is a root of a monic polynomial with coefficients $a_i \in I^i$. We can write the equation

$$b^n + a_1b^{n-1} + \dots + a_{n-1}b + a_n = 0.$$

We are given that $b = \sum_{i=1}^n c_id_i$ for $c_i \in I$ and $d_i \in \bar{R}$, so $b \in I$. Thus, $b^n \in I\bar{R}$ and $a_1b^{n-1} + \dots + a_{n-1}b + a_n \in I\bar{R}$ since $a_i \in I$ and $b \in \bar{I} \subseteq R \subseteq \bar{R}$. Hence $b \in I\bar{R}$ so $b \in I\bar{R} \cap R$. Therefore $I\bar{R} \cap R = \bar{I}$ for all ideals I of R . \square

The following theorems list some properties about principal ideals in the integral closure of a ring. Theorem 5.14 is a special case of Theorem 5.13.

Theorem 5.14. $\overline{b\bar{R}} = b\bar{R}$ for all $b \in R$.

Proof. In the previous chapter we saw that $R \subseteq \bar{R}$ and $\bar{\bar{R}} = \bar{R}$. Using this result with Theorem 5.13 gives us $\bar{I} = I\bar{\bar{R}} \cap \bar{R}$ for any ideal I of \bar{R} . If we let $I = b\bar{R}$ then we have $\overline{b\bar{R}} = b\bar{R}\bar{\bar{R}} \cap \bar{R} = b\bar{R} \cap \bar{R} = b\bar{R}$. Thus $\overline{b\bar{R}} = b\bar{R}$. \square

Theorem 5.15. $b\bar{R} \cap R = \overline{bR}$ for all $b \in R$.

Proof. Let $I = bR$. By Theorem 5.13, $\overline{bR} = (bR\bar{R}) \cap R = b\bar{R} \cap R$. \square

Chapter 6

Closure Operations

We have seen many similarities that tie the algebraic closure of a field to the integral closure of a ring and then to the integral closure of an ideal. However, we are now going to concentrate on the operation on ideals in general. We will first define what a closure operation on an ideal is and then explore the properties of closure operations. An interesting fact about closure operations is that the term “closure operation” was first coined by E.H. Moore [Eps11]. He used it to classify operations on subsets of rings and did not use it primarily for ideals.

6.1 General Closure Operations on Ideals

Definition 6.1. Let R be a ring. A *closure operation*, cl , on a set of ideals \mathcal{I} of R is a set map $cl: \mathcal{I} \rightarrow \mathcal{I}$ where $I \mapsto I^{cl}$ and satisfies the following conditions:

- (i) Extension: $I \subseteq I^{cl}$ for all $I \in \mathcal{I}$.
- (ii) Idempotence: $I^{cl} = (I^{cl})^{cl}$ for all $I \in \mathcal{I}$.
- (iii) Order-preservation: If $J \subseteq I$ are ideals of \mathcal{I} , then $J^{cl} \subseteq I^{cl}$.

Four examples are listed below along with short proofs using Definition 6.1 to show they are indeed closure operations.

Example (6.1.1). Identity closure; this mapping sends each ideal to itself.

Proof. Let $I^{cl} = I$ for all ideals $I \in R$. We will check that the three conditions of Definition 6.1 hold.

- (i) Since $I^{cl} = I$ and $I \subseteq I$, we have that $I \subseteq I^{cl}$ for all ideals in R .
- (ii) $I^{cl} = I$ and $(I^{cl})^{cl} = I^{cl} = I$. Thus $I^{cl} = (I^{cl})^{cl}$ for all ideals in R .
- (iii) Let $J \subseteq I$. Since $I^{cl} = I$ and $J^{cl} = J$, we have $J^{cl} \subseteq I^{cl}$. □

Example (6.1.2). Indiscrete closure; this mapping sends each ideal to the unit ideal, R .

Proof. Let $I^{cl} = R$ for all ideals $I \in R$. We will check that the three conditions of Definition 6.1 hold.

- (i) $I \subseteq I^{cl} = R$ for all ideals in R .
- (ii) $I^{cl} = R$ and $(I^{cl})^{cl} = R^{cl} = R$. Thus $I^{cl} = (I^{cl})^{cl}$ for all ideals in R .
- (iii) Let $J \subseteq I$. Since $I^{cl} = J^{cl} = R$ and $R \subseteq R$ we have $J^{cl} \subseteq I^{cl}$. □

Example (6.1.3). The radical $(\sqrt{})$ is a closure operation.

Proof. Let \mathcal{I} be the set of ideals of R with a map where $I \mapsto \sqrt{I}$. We need to check that extension, idempotence and order-preservation hold in order to prove it is a closure operation.

- (i) Extension: Let $f \in I$, then $f^n \in I$ for $n = 1$. Thus $f \in \sqrt{I}$.
- (ii) Idempotence: We want to show that $\sqrt{I} = \sqrt{\sqrt{I}}$.
Note that $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$ since every ideal is contained in its radical extension. So now we just need to show $\sqrt{\sqrt{I}} \subseteq \sqrt{I}$. Let $g \in \sqrt{\sqrt{I}}$. Then there exists $n \in \mathbb{N}$ such that $g^n \in \sqrt{I}$ and there exists $m \in \mathbb{N}$ such that $(g^n)^m \in I$. So $g^{nm} \in I$. Thus $g \in \sqrt{I}$.
- (iii) Order-preservation: Let $J \subseteq I \in \mathcal{I}$. Let $f \in \sqrt{J}$, then $f^n \in J$ for some $n \in \mathbb{N}$. Since $J \subseteq I$, $f^n \in I$ so $f \in \sqrt{I}$.

The radical operation satisfies all conditions and therefore is a closure operation. □

Example (6.1.4). Integral Closure is a closure operation.

Proof. Let \mathcal{I} be the set of ideals of R with the map $I \mapsto \bar{I}$. By Lemma 5.7, $I \subseteq \bar{I}$ so extension holds. By Theorem 5.5, $\bar{\bar{I}} = \bar{I}$, so idempotence holds. Lastly by Theorem 5.6, $I \subseteq J$ implies $\bar{I} \subseteq \bar{J}$, so order-preservation holds. Thus, Integral closure is a closure operation. □

The following theorem gives properties of closure and follows from the definition of closure operation.

Theorem 6.2. *Let R be a ring and cl a closure operation. Let I be an ideal of R .*

- (i) *If $I = I^{cl}$ and $J = J^{cl}$, then $I \cap J = (I \cap J)^{cl}$.*
- (ii) *$(I^{cl} + J^{cl})^{cl} = (I + J)^{cl}$*
- (iii) *$(IJ)^{cl} \subseteq (I^{cl} \cdot J^{cl})^{cl}$*

In part (iii), if we change the containment to equality, that is if $(IJ)^{cl} = (I^{cl} \cdot J^{cl})^{cl}$, then the cl -operation is called a *semi-prime operation*.

Proof. (i) First we will show $(I \cap J)^{cl} \subseteq I \cap J$. We know $I \cap J \subseteq I$ and $I \cap J \subseteq J$. Then $(I \cap J)^{cl} \subseteq I^{cl}$ and $(I \cap J)^{cl} \subseteq J^{cl}$ since closure operations are order-preserving. Now, let $a \in (I \cap J)^{cl}$. So $a \in I^{cl}$ and $a \in J^{cl}$. Hence $a \in I^{cl} \cap J^{cl}$ so $a \in I \cap J$. Next we will show $I \cap J \subseteq (I \cap J)^{cl}$. Let $a \in I \cap J$. By extension $I \cap J \subseteq (I \cap J)^{cl}$. Thus $a \in (I \cap J)^{cl}$. Therefore $I \cap J = (I \cap J)^{cl}$.

(ii) Just as in part (i) we will use subsets to prove this equality. First we will show $(I + J)^{cl} \subseteq (I^{cl} + J^{cl})^{cl}$. By extension $I \subseteq I^{cl}$ and $J \subseteq J^{cl}$. Hence $I + J \subseteq I^{cl} + J^{cl}$. Therefore, by order-preservation $(I + J)^{cl} \subseteq (I^{cl} + J^{cl})^{cl}$. Now we will show $(I^{cl} + J^{cl})^{cl} \subseteq (I + J)^{cl}$. We have that $I \subseteq I + J \subseteq (I + J)^{cl}$ and $J \subseteq I + J \subseteq (I + J)^{cl}$. So by idempotence $(I + J)^{cl} = ((I + J)^{cl})^{cl}$ and by order-preservation $I^{cl} \subseteq ((I + J)^{cl})^{cl} = (I + J)^{cl}$ and $J^{cl} \subseteq ((I + J)^{cl})^{cl} = (I + J)^{cl}$. Hence $I^{cl} + J^{cl} \subseteq (I + J)^{cl} + (I + J)^{cl} = (I + J)^{cl}$. Thus, $(I^{cl} + J^{cl})^{cl} = (I + J)^{cl}$.

(iii) By extension, $I \subseteq I^{cl}$ and $J \subseteq J^{cl}$, so $IJ \subseteq I^{cl} \cdot J^{cl} \subseteq (I^{cl} \cdot J^{cl})^{cl}$. By order-preservation we have $(IJ)^{cl} \subseteq ((I^{cl} \cdot J^{cl})^{cl})^{cl}$ and by idempotence we end up with $(IJ)^{cl} \subseteq (I^{cl} \cdot J^{cl})^{cl}$. \square

We will now look at specific types of closure operations on ideals. Throughout this portion we let R be a commutative integral domain with identity (unless otherwise stated) and K be the quotient field of R . Also $F(R)$ will be the set of non-zero fractional ideals of R . The first definition given is a special type of closure operation taken from [OM92].

Definition 6.3. Let cl be a closure operation for an ideal R . We say that cl is a *star operation on R* is a mapping $I \mapsto I^*$ of $F(R)$ into itself that satisfies the following three properties, for all $0 \neq a \in K$ and $I, J \in F(R)$:

- (i) $(a)^* = (a)$ and $(aI)^* = aI^*$,

- (ii) $I \subset I^*$, and if $I \subset J$, then $I^* \subset J^*$,
- (iii) $(I^*)^* = I^*$.

A very important star operation is the v -operation. Before we get to this definition, let us recall Property 4.13.1 where we defined the inverse of an invertible fractional ideal:

$$I^{-1} = R : I = \{x \in K \mid xI \subset R\},$$

and as in the example for Property 4.13.2 we found that the inverse of the ideal $(2) \in \mathbb{Z}$ is $(2)^{-1} = \frac{1}{2}\mathbb{Z}$. Consequently, we use this terminology in the definition below for v -operation.

Definition 6.4. For any $I \in F(R)$ and denote $(I^{-1})^{-1}$ by I_v . Then the mapping $I \mapsto I_v$ is a star operation on R called the v -operation.

Example (6.4.1). Let $R = \mathbb{Z}$ and $I = (2) = 2\mathbb{Z}$. We know that $(2)^{-1} = \frac{1}{2}\mathbb{Z}$ so

$$((2)^{-1})^{-1} = \left\{x \in \mathbb{Q} \mid x \left(\frac{1}{2}\mathbb{Z}\right) \subset \mathbb{Z}\right\} = 2\mathbb{Z} = (2).$$

First of all we need to show that the v -operation is truly a closure operation. We need to check that extension, idempotence and order-preservation hold.

Proof: The v -operation is a closure operation. Let \mathcal{I} be the set of ideals of R with a mapping from $I \rightarrow I_v$.

- (i) Extension: Let $x \in I$. Then $xI^{-1} \subseteq II^{-1} \subseteq R$. Thus $x \in (I^{-1})^{-1} = I_v$ and so $I \subseteq I_v$.
- (ii) Idempotence: By part (i), $I_v \subseteq (I_v)_v$. Let $x \in (I_v)_v$. Then $x(I_v)^{-1} \subseteq R$. Hence $xI^{-1} \subseteq x \left((I^{-1})^{-1}\right)^{-1} = x(I^{-1})_v = x(I_v)^{-1} \subseteq R$. Thus $x \in I_v$.
- (iii) Order-Preservation: Let $x \in J_v$. Since $J \subseteq I$, then $I^{-1} \subseteq J^{-1}$. This is true because if $x \in I^{-1}$, then $xI \subseteq R$, and since $J \subseteq I$ we have $xJ \subseteq xI$. So $x \in xJ$, and hence $x \in J^{-1}$. Continuing on, we have the $xI^{-1} \subseteq xJ^{-1} \subseteq R$ since $x \in J_v = (J^{-1})^{-1}$. Thus, $x \in I_v$. □

The next step is to show that the v -operation is a star operation.

Proof: The v -operation is a star operation. Let $a \in K$ be non-zero and let $I, J \in F(R)$. Parts (ii) and (iii) of Definition 6.3 are satisfied because the v -operation is a closure operation. Now we need to show that $(a)_v = (a)$ and $(aI)_v = aI_v$. First we will show $(a)_v = (a)$. By part (i) $(a) \subseteq (a)_v$. So now let $x \in (a)_v$. Then $x(a)^{-1} \subseteq R$. So

$x(a)^{-1}(a) \subseteq R(a)$. Since $1 \in (a)^{-1}(a)$, then $x = x \cdot 1 \in (a)$. Thus $(a)_v \subseteq (a)$ and hence $(a)_v = (a)$. Secondly, we will show $(aI)_v = aI_v$. Note that $(aI)^{-1} = a^{-1}I^{-1}$. This is because if $x \in (aI)^{-1}$, then $xaI \subseteq R$. So $xa \in I^{-1}$, and thus $x \in a^{-1}I^{-1}$. Going the other direction, let $x \in a^{-1}I^{-1}$. Then $xa \in I^{-1}$ so $xaI \subseteq R$ and thus $x \in (aI)^{-1}$. From this we can write $((aI)^{-1})^{-1} = (a^{-1}I^{-1})^{-1} = (a^{-1})^{-1}(I^{-1})^{-1} = aI_v$. Therefore, $(aI)_v = aI_v$. \square

The next theorem characterizes the v -operation of I as the intersection of the set of principal fractional ideals that contain I and the corollary after tells us that the v -operation is the largest star operation on R [Eps11].

Theorem 6.5. *For any $I \in F(R)$*

$$I_v = \bigcap \{Rx \mid I \subseteq Rx, x \in K\}$$

Proof. Let $a \in \bigcap \{Rx \mid I \subseteq Rx, x \in K\}$. Then $a \in Rx$ for all $x \in K$ such that $I \subseteq Rx$. Since $I \subseteq Rx$ we have that $x^{-1}I \subseteq R$, and so $x^{-1} \in I^{-1}$. Hence $ax^{-1} \in aI^{-1}$. We also have that $ax^{-1} \in R$ because $a \in Rx$, thus $aI^{-1} \subseteq R$. Therefore, $a \in (I^{-1})^{-1} = I_v$, and so $\bigcap \{Rx \mid I \subseteq Rx, x \in K\} \subseteq I_v$. Next, we will show containment in the other direction. Let $a \in I_v$. Then $aI^{-1} \subseteq R$. Now let $b \in I^{-1}$. Then $abI \subseteq R$, and so $I \subseteq R(ab)^{-1}$. By order-preservation, $I_v \subseteq (R(ab)^{-1})_v = R(ab)^{-1}$ for $(ab)^{-1} \in K$. Therefore $I_v \subseteq \bigcap \{Rx \mid I \subseteq Rx, x \in K\}$. \square

Corollary 6.6. $I \subseteq I^* \subseteq I_v$ for all star operations $*$ on R and all $I \in F(R)$.

Proof. The star operation is a closure operation, so $I \subseteq I^*$ follows from extension. We need to show that $I^* \subseteq I_v$. Let Rx be a principal fractional ideal containing I . Then $I^* \subseteq (Rx)^*$ and $(Rx)^* = Rx$ by the definition of a star operation. Thus $I^* \subseteq \bigcap \{Rx \mid I \subseteq Rx, x \in K\} = I_v$. Thus $I^* \subseteq I_v$. \square

6.2 Corresponding Ring Closures

Along with closure operations of ideals we can define the related closure operations of rings. For instance, we looked at the integral closure of a ring in Chapter 4

before we examined the integral closure of an ideal in a ring which was in Chapter 5. This section provides some definitions and examples of ring closures.

Definition 6.7. Let $I \rightarrow I^{cl}$ be a closure operation on the set of ideals of a ring R and let

$$R^{cl} = \left\{ \frac{c}{b} \mid b \text{ is a regular non-unit in } R \text{ and } c \in (bR)^{cl} \right\}.$$

Then R^{cl} is the ring closure of R .

The example below takes this idea of a ring closure and places it in a more familiar context by using integral closure as the closure operation for the ring.

Example (6.7.1). $\bar{R} = \left\{ \frac{c}{b} \mid b \text{ is a regular non-unit in } R \text{ and } c \in \overline{(bR)} \right\}$.

Proof. Let $\frac{c}{b} \in \bar{R}$. Then we can write

$$\left(\frac{c}{b}\right)^n + a_1 \left(\frac{c}{b}\right)^{n-1} + \cdots + a_{n-1} \left(\frac{c}{b}\right) + a_n = 0 \text{ for } a_i \in R.$$

Multiplying by b^n gives us

$$c^n + a_1 b c^{n-1} + \cdots + a_{n-1} b^{n-1} c + a_n b^n = 0.$$

Since $a_1 b \in bR$, $a_2 b^2 \in (bR)^2, \dots$, and $a_n b^n \in (bR)^n$ we have an equation of integral dependence of c over bR . Thus $c \in \overline{bR}$.

Now we will show containment in the other direction. Let $\frac{c}{b} \in \left\{ \frac{c}{b} \mid b \text{ is a regular non-unit in } R \text{ and } c \in \overline{(bR)} \right\}$. Then we can write

$$c^n + r_1 c^{n-1} + \cdots + r_{n-1} c + r_n = 0 \text{ for } r_i \in (bR)^i.$$

Since $r_i \in (bR)^i$ we can write $r_i = b^i x_i$ where $x_i \in R$ for some i . So rewriting the equation above gives us

$$c^n + b x_1 c^{n-1} + \cdots + b^{n-1} x_{n-1} c + b^n x_n = 0.$$

Now multiplying by $\frac{1}{b^n}$ gives us

$$\left(\frac{c}{b}\right)^n + x_1 \left(\frac{c}{b}\right)^{n-1} + \cdots + x_{n-1} \left(\frac{c}{b}\right) + x_n = 0 \text{ for } x_i \in R.$$

Hence, $\frac{c}{b} \in \bar{R}$. Therefore $\bar{R} = \left\{ \frac{c}{b} \mid b \text{ is a regular non-unit in } R \text{ and } c \in \overline{(bR)} \right\}$. □

Additionally, we can define a star operation on a ring R as follows.

Definition 6.8. For any star operation $*$ on R , we set

$$R^* = \bigcup \{I^* : I^* \mid I \text{ is a finitely generated ideal of } R\}$$

and we shall call R^* the $*$ -integral closure of R .

The $*$ -integral closure of a ring, R^* , is very similar to that of the integral closure of a ring, \bar{R} . First off, R^* is a ring extension of R [OM92], just like \bar{R} . Also, if we recall from Theorem 4.9, which states that the integral closure of a ring can be written as the union of the set of quotient ideals $(I : I)$ where I is a finitely generated ideal of R , we see that it is comparable to the definition above except for the $*$ notation. The theorem below illustrates the relationship between the integral closure of a ring and the $*$ -integral closure.

Theorem 6.9. *The integral closure of a ring, R , is contained in the $*$ -integral closure of R .*

Proof. We want to show $\bar{R} \subseteq R^*$. Let $x \in \bar{R}$. By Theorem 4.9, $x \in \bigcup \{(I : I) \mid I \text{ is a finitely generated ideal of } R\}$. So $xI \subseteq I$ for some finitely generated ideal I . Thus $(xI)^* \subseteq I^*$ by Corollary 6.6. By Definition 6.3, $(xI)^* = xI^*$ so we have $(xI)^* = xI^* \subseteq I^*$. Hence, $x \in I^* : I^*$. Therefore $x \in R^*$ so $\bar{R} \subseteq R^*$. \square

The last theorem of this chapter shows that R^* is an integrally closed ring just as the integral closure of a ring is integrally closed. This theorem provides one more similarity between the integral closure of a ring and the $*$ -integral closure. It is a special case of Theorem 2.8 found in [OM92].

Theorem 6.10. *The $*$ -integral closure of a ring is integrally closed.*

Proof. We want to show $R^* = \overline{R^*}$. We know that $R^* \subseteq \overline{R^*}$ so we just need to show that $\overline{R^*} \subseteq R^*$. Let $x \in \overline{R^*}$. Then there exists $a_1, a_2, \dots, a_n \in R^*$ such that x is integral over $R[a_1, a_2, \dots, a_n]$. Since each $a_i \in R^*$, there exists $a_i \in J_i^* : J_i^*$ where J_i is a finitely generated ideal of R . Let $J = J_1 J_2 \cdots J_n$. Then $a_i J^* \subseteq J^*$ for all $i = 1, 2, \dots, n$. Thus $R[a_1, a_2, \dots, a_n] \subseteq (J^* : J^*)$. Since x is integral over $R[a_1, a_2, \dots, a_n]$, there is a finitely generated ideal I such that $I = (b_1, b_2, \dots, b_m)$ and $xI \subseteq I$. Now, let $H = JI$. Then H is a finitely generated fractional ideal of R and

$$H = JI \subseteq JR[a_1, a_2, \dots, a_n] \subseteq J^* R[a_1, a_2, \dots, a_n] \subseteq J^*.$$

Thus, if $dJ^* \subset R$ for $0 \neq d \in R$, then $dH \subset R$. Additionally, we have

$$JI \subset J^*I \subset (JI)^* \subset H^*.$$

Now, since $xI \subset I$, then $xH = x(JI) = J(xI) \subset JI \subset H^*$. Hence, $xH^* = (xH)^* \subset (H^*)^* = H^*$. Therefore $x \in H^* : H^* \subset R^*$, and so $\overline{R^*} \subseteq R^*$. \square

Chapter 7

Conclusion

The algebraic closure of a field F can be summed up as the smallest algebraically closed extension field containing F . A good example to help ground us with this concept is looking at the algebraic closure of the field of rational numbers \mathbb{Q} . One might think that the complex numbers would be its algebraic closure because we learned that by the Fundamental Theorem of Algebra (Theorem 3.16) the field of complex numbers is algebraically closed. But actually, there is a smaller algebraically closed extension field that contains \mathbb{Q} . It is the set of algebraic numbers. Thus, the algebraic closure of \mathbb{Q} is the set of all algebraic numbers.

Now, the algebraic closure of a field has many resemblances to integral closure of a ring. For one, extension fields are extension rings and integral elements over a field are also algebraic elements. They also have the same transitive property that states an algebraic/integral extension over another algebraic/integral extension is algebraic/integral. However, one thing that separates the integral closure of a ring with the integral closure of a field is its connections to modules and finitely generated ideals as is seen in Theorems 4.4 and 4.9. Additionally, the integral closure of a ring has an ideal counterpart: the integral closure of an ideal in a ring.

After studying the integral closure of an ideal and analyzing some of its properties, we found that it was part of a larger, more general concept of closure operations on ideals. We defined a closure operation on an ideal to be a mapping from an ideal to its closure that satisfies the properties of extension, idempotence and order-preservation. There are also special types of closure operations like star operations and v -operations.

Lastly, closure operations on ideals and their corresponding ring closures have many similar characterizations. Take the case of the integral closure of a ring and the integral closure of an ideal in a ring. By their definitions alone we can see that they share important properties. The core of their definitions both depend on elements from their respective ring or ideal as roots of monic polynomials. Another similarity is that the integral closure of a ring is an integrally closed ring in the same way the integral closure of an ideal is an integrally closed ideal. In the end, we generalized the closure of a ring R to be the set of elements $\frac{c}{b}$ such that b is not a unit in R and c is in the closure of the principal ideal generated by b . The last theorem, Theorem 6.10, ends this survey of closure operations in commutative rings. It associates the information studied about the integral closure of rings to the star operations on ideals.

Bibliography

- [Eps11] Neil Epstein. A guide to closure operations in commutative algebra. arXiv. org Cornell University Library, 2011.
- [Gal10] Joseph A. Gallian. *Contemporary Abstract Algebra*. Brooks/Cole Cengage Learning, Belmont, CA, 2010.
- [Hun74] Thomas W. Hungerford. *Graduate Texts in Mathematics: Algebra*. Springer-Verlag, New York, 1974.
- [OM92] Akira Okabe and Ryuki Matsuda. *Star Operations and Generalized Integral Closures*. Bull. Fac. Sci, Ibaraki Univ., November 1992.
- [SH06] Irena Swanson and Craig Huneke. *Integral Closure of Ideals, Rings, and Modules*. Cambridge University Press, Cambridge, United Kingdom, 2006.
- [Sha00] R.Y. Sharp. *Steps in Commutative Algebra*. Cambridge University Press, Cambridge, United Kingdom, 2000.
- [Swa89] Irena Swanson. Integral closures of ideals and rings. ICTP, Trieste, 1989.