8-2022

Conductors and Rings with Shared Ideals

Sydney Maibach
smaibac@g.clemson.edu

Conductors and Rings with Shared Ideals

A Project
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Master of Science
Mathematical Sciences

---

by
Sydney Marcia Maibach
August 2022

Accepted by:
Dr. Jim Coykendall, Committee Chair
Dr. Michael Burr
Dr. Hui Xue

Abstract

Given an additive subgroup I of a field K, we define the colon ideal $(I : I) = \{\alpha \in K : \alpha I \subseteq I\}$. We then use this to construct collections of rings with shared ideals and explore relationships between these concepts and the complete integral closure.

Acknowledgments

I could not have completed this work without the encouragement and contributions of many others. First, I would like to thank my advisor Dr. James Barker Coykendall for overseeing me and guiding me through this process of researching and writing my project, as well as responding to many emails, sitting through many needed meetings, and giving me great advice. I would also like to thank my other committee members Dr. Hui Xue and Dr. Michael Burr for their participation and input in this process.

I want to thank my undergraduate advisor Dr. Bob Niichel for encouraging me to attend graduate school and giving me the confidence and guidance necessary to succeed as well as the many other faculty at Fairmont State University for all they have done to aid me in this process.

I am very thankful for my family and friends for being patient with me and allowing me to follow the path that I have chosen. With a special thanks to my mother Lori Maibach for her support. Please know that you have my utmost gratitude.

Contents

Chapter 1

Introduction

1.1 Motivation and Background

The motivation behind this project can be understood by looking at two specific examples. We must first introduce some important concepts, all of which will be given a more formal treatment later. Unless otherwise stated, the terminology "ring" refers to an integral domain.

We start by taking any field F and an additive subgroup $A \subseteq F$, and we consider the conductor $(A : A) = \{x \in F | xA \subseteq A\}$. If we have any $x, y \in (A : A)$, then $xA \subseteq A$ and $yA \subseteq A$ so $(x + y)A \subseteq A$. Similarly, if we have $xA \subseteq A$ and $yA \subseteq A$, then $xyA = x(yA) \subseteq xA \subseteq A$. Hence, $(A : A)$ is a domain. Here we are most interested when the quotient field of $(A : A)$ is equal to F.

For example, if F is equal to $\mathbb{Q}(x)$ consider the additive subgroup $x\mathbb{Q}[x]$. Recall that $\mathbb{Q}(x)$ is the field of rational functions with rational coefficients. So anything in $\mathbb{Q}(x)$ is a quotient of two polynomials. Suppose that $\frac{f(x)}{g(x)} \in \mathbb{Q}(x)$, then $\frac{xf(x)}{xg(x)} = \frac{f(x)}{g(x)}$. Here we have determined that the "quotient field" of $A = x\mathbb{Q}[x]$ is all of $F = \mathbb{Q}(x)$. Also, an easy computation shows that $(A : A) = \mathbb{Q}[x]$. It is easy to see that $\mathbb{Q}[x]$ is contained in $(A : A)$ and the other containment is a fairly simple computation since $\mathbb{Q}[x]$ is a UFD (see Definition 1.6.2).

However, there are myriad integral domains of which the subgroup $x\mathbb{Q}[x]$ is also an ideal. In particular $\mathbb{Z} + x\mathbb{Q}[x]$ is the smallest integral domain and $\mathbb{Q}[x]$ is the largest integral domain for which $x\mathbb{Q}[x]$ is an ideal. Notice that there are infinitely many integral domains in between $\mathbb{Z}+x\mathbb{Q}[x]$ and $\mathbb{Q}[x]$ that contain the ideal $x\mathbb{Q}[x]$, for example, $\mathbb{Z}_S + x\mathbb{Q}[x]$ where S is a multiplicatively closed subset of $\mathbb{Z}$ that does not contain 0.

Looking at another example, consider $2\mathbb{Z} \subseteq \mathbb{Z}$. The "quotient field" of $2\mathbb{Z}$ is $\mathbb{Q}$; this is clear because for all $a, b \in \mathbb{Z}$ with $b \neq 0$, $\frac{a}{b} = \frac{2a}{2b} \in \mathbb{Q}$. Note that $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$; we now show $2\mathbb{Z}$ is not an ideal of any overring (a ring between R and its quotient field) of $\mathbb{Z}$.

Suppose that $2\mathbb{Z}$ is an ideal of R a proper overring of $\mathbb{Z}$. Since $\mathbb{Z}$ is a principal ideal domain (PID) any overring is a localization of the form $\mathbb{Z}_S$ where S is a multiplicatively closed subset of $\mathbb{Z}$ not containing 0. Hence, if R is not $\mathbb{Z}$, then there must be an integer $n \in \mathbb{Z}$ such that $\frac{1}{n} \in R$ where $|n| > 1$, that is, n is invertible. Further, note that $(\frac{1}{n})(2)$ has absolute value no more than 1. Hence, $(\frac{1}{n})(2) \notin 2\mathbb{Z}$ which tells us that $2\mathbb{Z}$ is not an ideal of R. Therefore, we have determined that the only ring for which $2\mathbb{Z}$ is an ideal is $\mathbb{Z}$. Notice that in this example we are able to explicitly determine the ring to be $\mathbb{Z}$ where in our previous example we were left with infinitely many integral domains in between $\mathbb{Z} + x\mathbb{Q}[x]$ and $\mathbb{Q}[x]$ that potentially have ideal $x\mathbb{Q}[x]$.

1.2 Overview of Project

The remainder of this project will follow the outline given below. The goal of this chapter and each of its sections are to list important definitions, theorems, and examples. Proofs that provide useful insight for our purposes will be included, but for other results we will merely include a citation to a work containing the proof. In addition, well-known or minor results which will be used later will be presented here. All rings are assumed to be commutative with identity unless otherwise stated.

Chapter 2 is the computational focus of this work and contains foundational results about the relationship between collections of rings with shared ideals and complete integral closure. Important examples and proofs to pave the way to understanding our key results are presented.

Chapter 3 contains more global results that touch on the criteria for $\mathbb{Z} + I$ and $(I :_F I)$ to be distinct as well as relationships between $(I : I)$, $\mathbb{Z} + I$, and complete integral closures.

1.3 Rings and Ideals

This section will introduce definitions of various objects and terms referring to rings and ideals. These concepts will be useful for the main results of this paper.

Definition 1.3.1 ([1]). *A* **ring** *is a nonempty set R together with two binary operations $(+, \cdot)$ such that*

a) $(R, +)$ *is an abelian group.*

b) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *for all* $a, b, c \in R$.

c) $a \cdot (b + c) = a \cdot b + a \cdot c$ *and* $(a + b) \cdot c = a \cdot c + b \cdot c$ *for all* $a, b, c \in R$.

We remark here that if $ab = ba$ for all $a, b \in R$, then we say that R is commutative. Additionally, if there is an element (denoted $1 = 1_R$) such that $1(a) = a(1) = a$ for all $a \in R$ then R is said to have (multiplicative) identity. Unless otherwise specified, our rings will be commutative with identity.

Definition 1.3.2 ([2])**.** *Let* R *be a ring. A subset* $T \subseteq R$ *that is itself a ring is called a* **subring** *of* R*. If* R *has an identity* 1_R *then* $1_R \in T$

Definition 1.3.3 ([1])**.** *A nonempty subset* $I \subseteq R$ *is a* **ideal** *if and only if for all* $a, b \in I$ *and* $r \in R$*,*

a) $a - b \in I$

b) $ra \in I$.

Definition 1.3.4 ([1])**.** *The* **ideal generated by the set X** *is the intersection of all ideals that contain this set:* $\langle X \rangle = \bigcap_{X \subseteq I \subseteq R} I$*. Where the intersection ranges over all ideals containing* X*.*

We remark that $\langle X \rangle$ is equal to the set of all finite R-linear combinations of elements of X; that is, $\langle X \rangle = \{\sum_{k=1}^{n} r_k x_k | r_k \in R, x_k \in X\}$.

Definition 1.3.5 ([1])**.** *Let* I *and* J *be ideals of* R*. We define* $I + J = \{x + y | x \in I, y \in J\}$ *and* $IJ = \{\sum_{i=1}^{m} x_i y_i | x_i \in I, y_i \in J\}$.

Theorem 1.3.1 ([1])**.** *Let* $A_1, A_2, \ldots, A_n, A, B, C$ *be ideals of* R*.*

a) $A_1 + A_2 + \cdots + A_n$ *and* $A_1 A_2 \cdots A_n$ *are ideals of* R*.*

b) $A + (B + C) = (A + B) + C$.

c) $(AB)C = A(BC)$.

d) $B \sum A_i = \sum BA_i$

Now we will define a quotient field. This definition will be vital in understanding later results.

Definition 1.3.6. *The* **field of fractions** *or* **quotient field** *of an integral domain is the smallest field in which it can be embedded.*

Theorem 1.3.2 ([3])**.** *Let* R *be a ring and* $I \subseteq R$ *an ideal. Then the quotient group* R/I *is a ring with multiplication given by* $(a + I)(b + I) = ab + I$ *for all* $a, b \in R$*. What is more, if* R *is commutative, so is* R/I *and if* R *has an identity, then so does* R/I*.*

Proof. We leave most details to the reader, but we will show that multiplication is well-defined. Suppose that $a+I = x+I$ and $b+I = y+I$. This means that $a-x, b-y \in I$. We write $a = x+i$ and $b = y+j$ with $i, j \in I$. Note that $ab = xy+xj+iy+ij$ and since $xj+iy+ij \in I, ab+I = xy+I$ so the multiplication is well-defined. □

Proposition 1.3.1 ([6]). *Let R be finite. Then $\alpha \in R$ is a zero divisor if and only if it is a non-unit.*

Proof. Assume that $\alpha \in R$ is a unit. Then, if $\beta \in R$ such that $\alpha\beta = 0$, note that $\beta = \alpha^{-1}\alpha\beta = 0$. Then if α is a unit, it is not a zero divisor. Notice that this portion of the proof does not depend on R being finite.

Now we can assume that α is not a zero divisor. Then for any $\beta, \gamma \in R$, such that if $\alpha\beta = \alpha\gamma$, then $\alpha(\beta-\gamma) = 0$. Since α is not a zero divisor, then $\beta-\gamma = 0$ implies that $\beta = \gamma$. In other words, the mapping $\alpha : R \to R$ such that $\alpha(\beta) = \alpha\beta$ is injective. Since R is finite, then this mapping must also be surjective, so there is some $\beta \in R$ such that $\alpha\beta = 1$. Then α is a unit. □

We remark that this result depends heavily on the fact that R is finite. For example, if $R = \mathbb{Z}$ then every element other than $-1, 0, +1$, is a non-unit, but none of them are zero divisors.
The following definitions will introduce special types of ideals that will come in handy throughout the paper.

Definition 1.3.7 ([6]). *Let I be an ideal in R. We say that I is a* **principal ideal** *if I is generated by a single element $\alpha \in I$ and we write and we write $I = (\alpha)$.*

Definition 1.3.8 ([6]). *Let P be an ideal in R. We say that P is a* **prime ideal** *if $ab \in P$ for $a, b \in R$ implies that either $a \in P$ or $b \in P$.*

Definition 1.3.9 ([6]). *Let M be an ideal in R. We say that M is a* **maximal ideal** *if the only ideal of R strictly containing M is R itself. In other words, if I is an ideal of R such that $M \subseteq I$, either $I = M$ or $I = R$.*

Definition 1.3.10. *Let R be an integral domain.*
a) Suppose $r \in R$ is nonzero and is not a unit. Then r is called **irreducible** *in R if whenever $r = ab$ with $a, b \in R$, at least one of a or b must be a unit in R. Otherwise r is said to be reducible.*
b) A nonzero element $p \in R$ is called **prime** *in R if the ideal (p) generated by p is a prime ideal. in other words, a nonzero element p is a prime if it is not a unit and whenever $p|ab$ for any $a, b \in R$, then either $p|a$ or $p|b$.*

c) Two elements a and b of R vary by a unit are said to be **associate** *in R (i.e., $a = ub$ for some unit $u \in R$).*

Proposition 1.3.2 ([6])**.** *Let R be an integral domain. Then $(a) = (b)$ if and only if a and b are associates.*

Proof. We will assume that a and b are both nonzero. Note that $(a) = (b)$ if and only if $a \in (b)$ and $b \in (a)$, which is true if and only if $b|a$ and $a|b$. Thus, there exist $x, y \in R$ such that $a = bx$ and $b = ay$. Hence, $a = axy$ and so, $a(1 - xy) = 0$. Since R is an integral domain $a = 0$ or $(1 - xy) = 0$, but since we assumed that $a \neq 0$ then $(1 - xy) = 0$ so $xy = 1$ implying that x and y are units. Hence a and b are associates. □

Proposition 1.3.3 ([6])**.** *Let I be an ideal in R. Then I is maximal if and only if R/I is a field. Furthermore, I is prime if and only if R/I is an integral domain.*

Proof. Assume that I is a maximal ideal of R, that is, the only ideal of R strictly containing I is R. Now for any ideal J of R/I, define J' to be the set of all elements of R whose coset in R/I lies in J. Then J' is an ideal of R (in fact, J' is the kernel of the natural projection map from R to $(R/I)/J$). Now, since J contains the 0 element of R/I, $I \subseteq J'$. Thus, for any ideal J of R/I, either $J' = I$, in which case $J = \{0\}$ or $J' = R$, in which case $J = R/I$. Then any nonzero ideal of R/I is the entirety of R/I. Applying this to any nonzero principal ideal (α) of R/I, we get that

$$(\alpha) = R/I.$$

This implies that $\alpha \in U(R/I)$. Therefore, R/I is a field.

Furthermore, assume that R/I is a field, note that any ideal J of R strictly containing I has an image J' under the natural projection map from R to R/I which is an ideal of R/I. Then since J strictly contains I, $J' \neq \{0\}$. Thus, $J' = R/I$, the only nonzero ideal of the field R/I. Thus, $J = R$. Then the only ideal of R strictly containing I is R, so I is maximal.

Now assume that I is a prime ideal, that is, for $a, b \in R, ab \in I$ if any only if either $a \in I$ or $b \in I$. This is equivalent to saying that $(a + I)(b + I) = 0$ in R/I if any only if either $a + I = 0$ or $b + I = 0$, i.e., R/I is an integral domain. This shows both directions of this implication. □

Theorem 1.3.3 ([1])**.** *Let R be an integral domain and S a subset of R that does not contain* 0 *and is closed under multiplication. The set of equivalence classes $R_S = \{r/s | r \in R \text{ and } s \in S\}$*

(where $r/s = r'/s'$ if and only if $rs' = r's$), with addition given by $(r/s + r'/s' = (rs' + r's)/ss'$ and multiplication given by $(r/s)(r'/s') = (rr')/(ss')$ forms an integral domain.

We remark that R_S is called the localization of R at the set S and if $S = R/\{0\}$, then R_S is called the quotient field of R. In the case that $S = R \setminus P$ where P is a prime ideal R, then R_S is often written R_P and is called the localization of R at the prime ideal P.

Example 1.3.1 ([1])**.** *We now present a few examples of localization.*
a) If R is a field, then its field of fractions is R itself.
b) The field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$. $2\mathbb{Z}$ is not an integral domain, but it is easy to generalize the previous definition; note that its field of fractions is also $\mathbb{Q}$.
c) Consider the polynomial ring $\mathbb{Z}[x]$. Since $\mathbb{Z}$ is an integral domain, so is $\mathbb{Z}[x]$. Then the field of fractions of $\mathbb{Z}[x]$ is the set of rational functions (i.e., functions of the form $p(x)/q(x)$, where $p(x)$ and $q(x)$ are polynomials with integer coefficients and $q(x)$ is not the zero polynomial). Notice that this field contains the field of fractions of $\mathbb{Z}$, namely $\mathbb{Q}$. However, it is interesting to point out that the field of fractions of $\mathbb{Q}[x]$ is the same as the field of fractions of $\mathbb{Z}[x]$.

Definition 1.3.11. *If I, J are ideals in $K[x_1, \cdots, x_n]$, then $(I : J)$ is the set $\{f \in K[x_1, \cdots, x_n] | fg \in I$ for all $g \in J\}$ and is called the* **ideal quotient** *(or colon ideal) of I by J.*

Example 1.3.2. *In $K[x, y, z]$ we have:*

$$\begin{aligned}(xz, yz) : (z) &= \{f \in K[x, y, z] | fz \in \langle xz, yz\rangle\} \\ &= \{f \in K[x, y, z] | fz = Axz + Byz\} \\ &= \{f \in K[x, y, z] | f = Ax + By\} \\ &= \langle x, y\rangle.\end{aligned}$$

Proposition 1.3.4. *If I, J are ideals in $K[x_1, \cdots, x_n]$, then the ideal quotient $(I : J)$ is an ideal in $K[x_1, \cdots, x_n]$ and $(I : J)$ contains I.*

Proof. To show $(I : J)$ contains I, note that because I is an ideal, if $f \in I$, then $fg \in I$ for all $g \in K[x_1, \cdots, x_n]$ and hence, certainly $fg \in I$ for all $g \in J$. To show that $(I : J)$ is an ideal, first note that $0 \in (I : J)$ because $0 \in I$. Let $f_1, f_2 \in (I : J)$. Then $f_1 g, f_2 g$ are in I for all $g \in J$. Since I is an ideal $(f_1 + f_2)g = f_1 g + f_2 g \in I$ for all $g \in J$. Thus $f_1 + f_2 \in (I : J)$. Similarly, if $f \in (I : J)$

and $h \in K[x_1, \cdots, x_n]$, then $fg \in I$ and, since I is an ideal, $hfg \in I$ for all $g \in J$, which means that $hf \in (I : J)$. □

Definition 1.3.11, Example 1.3.2, and Proposition 1.3.4 are all facets of a more general construction. Let A be a ring with subrings R and T and $\emptyset \neq I$, $J \subseteq A$ subsets. We define

$$C = (I :_T I) = \{z \in T | zJ \subseteq I\}$$

and make the following observations that are easy to justify:

1. If I is closed under addition, then so is C.

2. If I, T are R-modules, then so is C.

3. If I, T are R- modules and $I \subseteq J$, then C is a ring.

We will focus on the specific colon ideal defined below.

Definition 1.3.12. *If I is an additive subgroup of a field K, then $(I :_K I)$ is the set $\{\alpha \in K : \alpha I \subseteq I\}$.*

Definition 1.3.13 ([6])**.** *Let R and D be integral domains with $R \subseteq D$. We say that $\alpha \in D$ is* **integral over** *R if α is a root of some monic (that is, leading coefficient is 1) polynomial $f \in R[x]$. Furthermore, the set of all elements of D which are integral over R is called the* **integral closure** *of R in D, denoted $\bar{R}_D$. If $R = \bar{R}_D$, we say that R is* **integrally closed** *in D. If $D = \bar{R}_D$, we say that D is an integral extension of R. When D is not specified, D is assumed to be the field of fractions of R.*

Definition 1.3.14 ([6])**.** *Let R and D be integral domains with $R \subseteq D$. We say that $\alpha \in D$ is* **almost integral** *over R if there exists a nonzero $r \in R$ such that $r\alpha^n \in R$ for every $n \in \mathbb{N}$. Furthermore, if the set of elements in D which are almost integral over R is just R itself, we say that R is* **completely integrally closed** *in D. Again, if D is not specified, it is assumed to be the field of fractions of R.*

The following example illustrates the difference between almost integral and integral over a ring.

Example 1.3.3. *a) Let F be a field and x, y indeterminates. Consider the ring $R = F[x, xy, xy^2.xy^3, xy^4, \cdots]$. The quotient field of this is $F(x, y)$. Notice that $y \notin R$. But y is in the quotient field and $x \in R$ is nonzero and $xy^n \in R$ for all n. So, y is almost integral. We claim that y is not integral over R. If y*

were integral over R, then y is a root of a polynomial $t^n+f_{n-1}(x,y)t^{n-1}+\cdots+f_1(x,y)t+f_0(x,y)=0$ *(where* $f_i(x,y)\in R$*). Plug in y to get* $y^n+f_{n-1}(x,y)y^{n-1}+\cdots+f_1(x,y)y+f_0(x,y)=0$*. Now, plug in 0 for x to obtain* $y^n+f_{n-1}(0,y)y^{n-1}+\cdots+f_1(0,y)y+f_0(0,y)=0$*. As each non-constant monomial of* $f_i(x,y)$ *has a factor of x, we observe that* $f_i(0,y)$ *is in the field F. Hence,* $y^n+a_{n-1}y^{n-1}+\cdots+a_1y+a_0=0$ *(where* $a_i\in F$*) and this is impossible.*

b) Consider $T=\mathbb{Q}+x\mathbb{R}[x]$ *where* $\mathbb{Q}$ *is the rationals and* $\mathbb{R}$ *is the reals. Note that* $\pi=\frac{x\pi}{x}$ *is in the quotient field of T. Also, note* $x\in T$ *and* $x\pi^n\in T$ *for all n. We now show that* π *is not integral over T. Suppose* π *is a root of a monic polynomial* $t^n+f_{n-1}(x)t^{n-1}+\cdots+f_1(x)t+f_0(x)=0$*,* $f_i(x)\in T=\mathbb{Q}+x\mathbb{R}[x]$*. Notice that* $f_i(0)=q_i\in\mathbb{Q}$*. So,* π *is also a root of* $t^n+f_{n-1}(0)t^{n-1}+\cdots+f_1(0)t+f_0(0)=t^n+q_{n-1}t^{n-1}+\cdots+q_1t+q_0=0$ *in particular,* π *is a root of a polynomial with coefficients in* $\mathbb{Q}$*. This is a contradiction since* π *is a transcendental number (it is not the root of any polynomial with rational coefficients).*

We use the term overring of R to mean subring of the quotient ring of R containing R. Overrings of commutative integral domains have been studied rather extensively. We have the following definition.

Definition 1.3.15 ([8])**.** *Let Q be the quotient field of an integral domain R. A* **overring** *S of R is a ring such that* $R\subseteq S\subseteq Q$*.*

Definition 1.3.16. *A valuation domain V is an integral domain with the property that for any nonzero* $a,b\in V$ *either* $a|b$ *or* $b|a$*.*

Examples of valuation domains include any field as well as the localization of $\mathbb{Z}$ at a prime ideal. The following lemma gives us some basic properties of valuation domains.

Lemma 1.3.1 ([4])**.** *A valuation domain V with quotient field K has the following properties.*

a) The ideals of V are totally ordered by inclusion.

b) Any overring T of V is a valuation ring, moreover, if M is the unique maximal ideal of T, then $T=V_{M\bigcap V}$*.*

c) For any nonzero $u\in K$ *either* $u\in V$ *or* $u^{-1}\in V$*.*

d) V is integrally closed.

A proof is found in [4].

The following theorem gives us some background information on what the term "survives" indicates when used in Theorem 1.3.5.

Theorem 1.3.4. *Let $R \subseteq T$ be rings, and u a unit of T, and I a proper ideal in R. Then I survives in $R[u]$ or in $R[u^{-1}]$ i.e., $IV \neq V$.*

Proof. If not, then we obtain two equations:

$$a_0 + a_1 u + \cdots + a_n u^n = 1$$

and

$$b_0 + b_1 u^{-1} + \cdots + b_m u^{-m} = 1$$

with each $a_i, b_j \in I$. We assume that $n \geq m$ and has been chosen as small as possible. First, we multiply the second equation by u^n to get

$$(1 - b_0)u^n = b_1 u^{n-1} + \cdots + b_m u^{n-m}.$$

Now merely multiply the first equation by $1 - b_0$ and substitute to find a similar equation for u with smaller n as follows:

$$(1 - b_0) = (1 - b_0)(a_0 + a_1 u + \cdots + a_{n-1} u^{n-1}) + (1 - b_0)(a_n u^n)$$

and so,

$$(1 - b_0) = (1 - b_0)(a_0 + a_1 u + \cdots + a_{n-1} u^{n-1}) + (b_1 u^{n-1} + \cdots + b_m u^{n-m})(a_n).$$

The equation above contradicts the minimality of n. □

The following theorem gives us an important result concerning the existence of valuation overrings.

Theorem 1.3.5 ([1])**.** *Let R be a domain with quotient field K and $I \subset R$ a proper ideal. Then there is a valuation overring of R (say V) such that I survives in V.*

Proof. We first show that there is a maximal overring of R where I survives. To this end, we consider pairs (R_j, I_j) where R_j is an overring of R and I_j is a proper ideal of R_j containing I. We partially order this set by the relation $(R_a, I_a) \geq (R_b, I_b)$ if and only if $R_b \subseteq R_a$ and $I_b \subseteq I_a$. It is routine to show that every chain has an upper bound, the union of the chain itself. Applying Zorn's Lemma,

we have a maximal element (V, J). We finish by showing that V is a valuation domain. If V is not a valuation domain, then there is an $\alpha \in K$ with neither α nor α^{-1} in V . Note that J must survive in either $V[\alpha]$ or $V[\alpha^{-1}]$. However, this contradicts the maximality of V. Which concludes the proof. □

The following theorem gives us an important characterization of the integral closure of R.

Theorem 1.3.6 ([1])**.** *Let R be an integral domain with quotient field K and integral closure R. Then,*

$$\bar{R} = \bigcap_{R \subseteq V \subseteq K} V$$

where the intersection ranges over all valuation overrings of R.

The next theorem gives important information regarding valuation domains.

Theorem 1.3.7. *Let R be a valuation domain. Then R has the following properties.*

a) R is integrally closed.

b) Every overring of R is a valuation domain.

c) Every overring of R is a localization of R.

d) Every finitely generated ideal of R is principal.

e) All (prime) ideals of R are linearly ordered.

f) If I is any ideal in R, then $\sqrt{I}$ is prime.

1.4 Polynomials

A polynomial ring or polynomial algebra is a ring formed from the set of polynomials in one or more indeterminates or variables with coefficients in another ring, often a field. A polynomial ring in one determinant is denoted $R[x]$. These polynomial rings and their ideals are fundamental in algebraic geometry as well as many other fields.

Definition 1.4.1 ([2])**.** *The* **polynomial ring** $R[x]$ *in the indeterminate x with coefficients from R is the set of all formal sums*

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

with $n \geq 0$ and each $a_i \in R$. If $a_n \neq 0$ then the polynomial is of degree n, $a_n x^n$ is the leading term, and a_n is the leading coefficient.

1.5 Integral Domains and Fields

Here we introduce definitions of various objects and terms pertaining to integral domains and fields. Such concepts will be paramount to the main results of this paper. First, note that every field is an integral domain. Furthermore, rings of polynomials are integral domains if the coefficients come from an integral domain. For example, the ring $\mathbb{Z}[x]$ of all polynomials in one variable with integer coefficients is an integral domain.

Definition 1.5.1 ([3]). *A commutative ring with identity $1 \neq 0$ is called an* **integral domain** *if it has no nonzero zero divisors.*

Proposition 1.5.1 ([2]). *Any finite integral domain is a field.*

Proof. Let R be a finite integral domain and let a be a nonzero element of R. By the cancellation law the map $x \to ax$ is an injective function. Since R is finite, this map is also surjective. In particular, there is some $b \in R$ such that $ab = 1$, i.e., a is a unit in R. Since a was an arbitrary nonzero element, R is a field. □

Definition 1.5.2 ([1]). *A* **field** *F is a set together with two binary operations $+$ and $\cdot$ on F such that $(F, +)$ is an abelian group (call its identity 0) and $(F \setminus \{0\}, \cdot)$ is an abelian group, and the following distributive law holds:*

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c),$$

for all $a, b, c \in F$.

The following proposition is equivalent to the above definition of a field.

Proposition 1.5.2 ([1]). *A field is a commutative ring with identity such that (0) is a maximal ideal.*

Definition 1.5.3 ([1]). *Let $K \subseteq F$ be fields and let $u \in F$. We say that u is* **algebraic** *over K if u is a root of some nonzero polynomial over K. If u is not algebraic, we say that u is* **transcendental**

over K. If every element of F is algebraic over K, we say that F is an algebraic extension of K. If F contains at least one transcendental element, we say that F is transcendental over K.

1.6 Principal Ideal Domains

Now, we will investigate the properties of principal ideal domains.

Definition 1.6.1 ([2])**.** *A* **principal ideal domain** *(PID) is an integral domain in which every ideal is principal.*

Example 1.6.1. *Some examples of PID's may include.*

a) The integers $\mathbb{Z}$ is a PID.

b) If F is a field, then $F[x]$ is a PID.

Proposition 1.6.1. *In a integral domain a nonzero prime element is always irreducible.*

Proof. Suppose (p) is a nonzero prime ideal and $p = ab$. Then $ab = p \in (p)$, so by the definition of a prime ideal, one of a or b, is in (p). Without loss of generality, assume $a \in (p)$, then $a = pr$ for some r. This implies that $p = ab = prb$ so $rb = 1$ and b is a unit. This shows that p is irreducible. □

Note that it is not true in general that an irreducible element is necessarily prime.

Example 1.6.2. *Consider the following example.*

Consider the element 3 in the quadratic integer ring $R = \mathbb{Z}[\sqrt{-5}]$. We can see that 3 is irreducible in R, but 3 is not prime since $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 3^2$ is divisible by 3, but neither $2 + \sqrt{-5}$ nor $2 - \sqrt{-5}$ is divisible by 3 in R.

Note that if R is a principal ideal domain, however, the notations of prime and irreducible elements are the same. These notations coincide in $\mathbb{Z}$ and in $F[x]$ (where F is a field).

Proposition 1.6.2 ([2])**.** *Let R be a principal ideal domain and let a and b be nonzero elements of R. Let d be a generator for the principal ideal generated by a and b. Then*

a) d is a greatest common divisor of a and b.

b) d can be written as a R-linear combination of a and b, i.e., there are elements x and y in R with $d = ax + by$.

c) d is unique up to multiplication by a unit of R.

Proposition 1.6.3 ([2]). *Every nonzero prime ideal in a principal ideal domain is a maximal ideal.*

Proof. Let (p) be a nonzero prime ideal in a principal ideal domain R and let $I = (m)$ be any ideal containing (p). We must show that $I = (p)$ or $I = R$. Now $p \in (m)$ so $p = rm$ for some $r \in R$. Since (p) is a prime ideal and $rm \in (p)$, either r or m must lie in (p). If $m \in (p)$ then $(p) = (m) = I$. If, on the other hand, $r \in (p)$ write $r = ps$. In this case $p = rm = psm$, so $sm = 1$ (since R is an integral domain) and m is a unit so, $I = R$. □

Corollary 1.6.1 ([2]). *If R is any commutative ring such that the polynomial ring $R[x]$ is a principal ideal domain (or Euclidean domain), then R is necessarily a field.*

Proof. Assume that $R[x]$ is a principal ideal domain. Since R is a subring of $R[x]$ then R must be an integral domain (recall that $R[x]$ has and identity if and only if R does). The ideal (x) is a nonzero prime ideal in $R[x]$ because $R[x]/(x)$ is isomorphic to the integral domain R. By the above proposition, (x) is a maximal ideal, hence the quotient R is a field by Proposition 12 in section 7.4 of [2]. □

Proposition 1.6.4 ([2]). *In a principal ideal domain, a nonzero element is a prime if and only if it is irreducible.*

Proof. We have previously shown that prime implies irreducible. Now we much show that if p is irreducible, then p is prime, i.e., the ideal (p) is a prime ideal. If M is any ideal containing (p) then as R is a PID, $M = (m)$ is a principal ideal. Since $p \in (m)$, $p = rm$ for some r. But p is irreducible so by definition either r or m is a unit. This means either $(p) = (m)$ or $(m) = 1$, respectively. Thus, the only ideals containing (p) are (p) and R. Therefore, (p) is a maximal ideal. Since maximal ideals are prime ideals, the proof is complete. □

We will now introduce unique factorization domains and how they relate to prime elements and principal ideal domains.

Definition 1.6.2 ([2]). *A* **unique factorization domain** *(UFD) is an integral domain R in which every nonzero element $r \in R$ which is not a unit has the following two properties:*
a) r can be written as a finite product of irreducible p_i of R (not necessarily distinct): $r = p_1 p_2 \cdots p_n$ and

b) The decomposition in a) is unique up to associates and reordering: namely, if $r = q_1 q_2 \cdots q_m$ is another factorization of r into irreducibles, then $m = n$ and there is some renumbering of the factors so that p_i is associate to q_i for $i = 1, 2, \cdots, n$.

Note that a field F is trivially a unique factorization domain since every nonzero element is a unit, so there are no elements for which Properties a) and b) must be verified.

Proposition 1.6.5 ([2]). *In a unique factorization domain, a nonzero element is a prime if and only if it is irreducible.*

Proof. Let R be a unique factorization domain. Since we have shown that primes of R are irreducible, it remains to prove that each irreducible element is a prime. Let p be irreducible in R and assume that $p|ab$ for some $a, b \in R$. Now we need to show that p divides either a or b. To say that p divides ab is to say $ab = pc$ for some $c \in R$. Writing a and b as a product of irreducibles, we see from this last equation and from the uniqueness of the decomposition into irreducibles or ab that the irreducible element p must be associate to one of the irreducibles occurring either in the factorization of a or in the factorization of b. We can assume that p is associate to one of the irreducibles in the factorization of a, i.e., that a can be written as a product $a = (up)p_2 \cdots p_n$ for u a unit and some (possibly empty set of) irreducibles $p_2, \cdots, p_n$. But then p divides a, since $a = pd$ with $d = up_2 \cdots p_n$, completing the proof. □

Proposition 1.6.6 ([2]). *Let R be a PID, then R is a UFD.*

Proof. We must first show that R is atomic, i.e., every nonzero, non-unit element factors into irreducibles. Then we can show that R is in fact a UFD.

Let $\alpha_1 \in R$ be an arbitrary nonzero, non-unit element of R. If α_1 is irreducible, then it trivially factors into irreducibles. Otherwise, we can factor $\alpha_1 = \alpha_2\beta_2$, where neither α_2 nor β_2 is a unit. If both α_2 and β_2 factor into irreducibles, then so does α_1. without loss of generality, assume that α_2 does not factor into irreducibles. Then we can write $\alpha_2 = \alpha_3\beta_3$, with neither factor a unit. Now, continue factoring in this way to produce a sequence $\alpha_1, \alpha_2, \cdots$ of elements in R such that $(\alpha_1) \subset (\alpha_2) \subset \cdots$, with these inclusions being strict.

Now consider $I = \bigcup_{i=1}^{\infty}(\alpha_i)$. Due to the inclusion relation, I is an ideal in R. Then, since R is a PID, $I = (\alpha)$ for some $\alpha \in R$. So, $\alpha \in (\alpha_n)$ for some $n \in \mathbb{N}$. Also, we know that since $\alpha_n \in (\alpha)$ this

means that $(\alpha_n) = (\alpha)$. Thus, for any $m \geq n$,

$$(\alpha_n) \subseteq (\alpha_m) \subseteq (\alpha)$$

which implies that $(\alpha_n) = (\alpha_m)$, contradicting the strict inclusions. Thus, α_1 must factor into irreducibles, meaning that the sequence of strict ideal inclusions above is finite. This property of ideals is referred to as the ascending chain condition (A.C.C.). Now we show that this factorization is unique as in the definition of a UFD.

Let $\pi \in R$ be an irreducible. Then if I is an ideal containing (π), we have that $I = (\alpha)$ for some $\alpha \in R$ and thus $\alpha|\pi$. Then either α is a unit, in which case $I = R$, or α is an associate of π, in which case $I = (\pi)$. Then (π) is a maximal ideal, so we know that (π) is a prime ideal and π is a prime element.

Now consider two equal factorizations

$$\pi_1 \cdots \pi_m = \tau_1 \cdots \tau_n,$$

with each π_i, τ_i irreducible in R.

Without loss of generality, assume that $m \geq n$. Since π_1 is prime and $\pi_1|\tau_1 \cdots \tau_n$, we have by induction that $\pi_1|\tau_j$ for some j, $1 \leq j \leq n$. So, without loss of generality, assume that $\pi_1|\tau_1$. Then $(\tau_1) \subseteq (\pi_1) \neq R$, so by maximality of (τ_1), we have $(\tau_1) = (\pi_1)$, that is, π_1 and τ_1 are associates. Thus, $\pi_1 = u_1\tau_1$ for some $u_1 \in U(R)$, so

$$u_1\pi_1 \cdots \pi_m = \tau_1 \cdots \tau_n.$$

Note that $u_1\pi_2$ is still irreducible.

Then we can reorder, if necessary, and use induction to reduce this equality, to $u\pi_{n+1} \cdots \pi_m = 1$, with $u \in U(R)$. However, since each π_i is irreducible (and thus a non-unit), we get a contradiction. That is unless $m = n$. Thus, $m = n$ and each π_i is an associate of τ_i, meaning that R is in fact a UFD. □

Chapter 2

Computational Results

In this chapter we explore key examples that provide useful insight to help us understand the main results more clearly.

2.1 Examples

Example 2.1.1. *Let $I = 2\mathbb{Z}$ where the quotient field is $k = \mathbb{Q}$. Then $\mathbb{Z} + I = \mathbb{Z} + 2\mathbb{Z} = \mathbb{Z}$ and $(I :_k I) = (I : I) = (2\mathbb{Z} : 2\mathbb{Z}) = \{\alpha \in \mathbb{Q} | \alpha 2\mathbb{Z} \subseteq 2\mathbb{Z}\} = \mathbb{Z}$.*

Proof. Suppose $\alpha \in (I : I)$. For all $n \in \mathbb{Z}$, $\alpha(2n) = 2k$ for some $k \in \mathbb{Z}$ this implies that $an = k \in \mathbb{Z}$. In particular, if $n = 1$, then $\alpha = k \in \mathbb{Z}$. Therefore $\alpha \in \mathbb{Z}$, so, $(I : I) \subseteq \mathbb{Z}$. Since the other containment is straight forward, $(I : I) = \mathbb{Z}$. □

Example 2.1.2. *Let $R = \mathbb{Z}[x] = \mathbb{Z} + x\mathbb{Z}[x]$ with quotient field $k = \mathbb{Q}(x)$ and $I = x\mathbb{Z}[x]$*
Then, $(I :_k I) = (I : I) = \mathbb{Z}[x]$.

Proof. We claim that $(I : I) = \mathbb{Z}[x]$. We want to show that $\mathbb{Z}[x] \subseteq (I : I)$

Let $f(x) \in \mathbb{Z}[x]$ then $f(x)(x\mathbb{Z}[x]) \subseteq x\mathbb{Z}[x]$. Therefore, by definition of $(I : I)$, $f(x) \in (I : I)$. Hence, $\mathbb{Z}[x] \subseteq (I : I)$. Now we want to show that $(I : I) \subseteq \mathbb{Z}[x]$. Let $\frac{f(x)}{g(x)} \in (I : I)$ such that $f(x), g(x) \in \mathbb{Z}[x]$, and $\gcd(f, g) = 1$. Now, let $g(x) = x^n g'(x), n \geq 0$

Case 1: Let $n > 0$. Then, using $x^n f(x) \in I$ since $n > 0$

$$\begin{aligned}\frac{f(x)}{g(x)}(x^n f(x)) &= \frac{f(x)}{x^n g'(x)}(x^n f(x)) \\ &= \frac{f^2(x)}{g'(x)} \in I\end{aligned}$$

which implies $\frac{f^2(x)}{g'(x)} = xh(x)$. Therefore, $f^2(x) = xh(x)g'(x)$ and $x|f$. However, since $g(x) = x^n g'(x)$ and so $x|g$, which is a contradiction since $\gcd(f, g) = 1$. Therefore, $n = 0$.

Case 2: If $n = 0$ then $g(x) = g'(x)$. So,

$$\frac{f(x)}{g(x)}x = xh(x).$$

This implies that

$$f(x) = g(x)h(x).$$

Therefore,

$$g(x)|f(x).$$

However, since $\gcd(f, g) = 1$ this means that $g(x) = 1$.

Thus,

$$\begin{aligned}\frac{f(x)}{g(x)} &= \frac{f(x)}{1} \\ &= f(x) \in \mathbb{Z}[x].\end{aligned}$$

Hence, $(I : I) \subseteq \mathbb{Z}[x]$. Which, therefore, give us, $(I : I) = \mathbb{Z}[x]$. □

The types of rings that appear in the following example have been studied and are of high interest in the study of factorization.

Example 2.1.3. *Let $R = \mathbb{F}_2[x^3, x^5]$ where $I = (x^3, x^5)$. Then, $(I : I) = \mathbb{F}_2[x^3, x^5, x^7]$.*

Proof. Let $R = \mathbb{F}_2[x^3, x^5]$ and $I = (x^3, x^5) = (x^3, x^5, x^6, x^8, x^9, x^{10}, \cdots)$.

Recall that $(I : I) = \{\alpha(x) \in \mathbb{F}_2(x) | \alpha(x)I \subseteq I\}$.

Write $\alpha(x) = \frac{f(x)}{g(x)}$ such that $f(x), g(x) \in \mathbb{F}_2[x]$ and $\gcd(f, g) = 1$.

Note first that $x^3 \frac{f(x)}{g(x)} \in I$. This implies that,

$$x^3 f(x) \in Ig(x).$$

We can write

$$x^3 \frac{f(x)}{g(x)} = (r_1(x)x^3 + r_2(x)x^5).$$

Thus,

$$x^3 f(x) = (r_1(x)x^3 + r_2(x)x^5)g(x)$$

with $r_1(x), r_2(x) \in R = \mathbb{F}_2[x^3, x^5]$.

Note that as $\gcd(f, g) = 1$ in $\mathbb{F}_2[x]$ this means that $g(x)|x^3$ in $\mathbb{F}_2[x]$. Thus, $g(x) = x^n$ up to a unit which is only the identity in this situation. where $0 \leq n \leq 3$ then dividing through by x^3 we obtain

$$f(x) = (r_1(x) + r_2(x)x^2)x^n$$

and as $\gcd(f, g) = 1$ in $\mathbb{F}_2[x]$, $n = 0$, otherwise $x|f$ and $x|g$. So $\alpha(x) = f(x) \in \mathbb{F}_2[x]$.

Now we must find all

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_kx^k \in \mathbb{F}_2[x]$$

such that $x^3 f, x^5 f \in R = \mathbb{F}_2[x^3, x^5]$.

$$x^3 f = a_0x^3 + a_1x^4 + a_2x^5 + a_3x^6 + a_4x^7 + a_5x^8 \cdots$$

Since $x^3 f, \in R = \mathbb{F}_2[x^3, x^5]$ is implies that $a_1, a_4 = 0$. Similarly,

$$x^5 f = a_0 x^5 + a_1 x^6 + a_2 x^7 + a_3 x^8 \cdots$$

Since $x^5 f, \in R = \mathbb{F}_2[x^3, x^5]$ is implies that $a_2 = 0$.

So,

$$f(x) = a_0 + a_3 x^3 + a_5 x^5 + a_6 x^6 + a_7 x^7 + a_8 x^8 + \cdots \in \mathbb{F}_2[x^3, x^5, x^7].$$

Which concludes the proof. □

The following example will be similar to the previous. However, it allows us to visualize how quickly these types of problems can become large and more difficult to compute.

Example 2.1.4. *Let $R = \mathbb{F}_2[x^9, x^{17}]$ where $I = (x^9, x^{17})$. Then, $(I : I) = \mathbb{F}_2[x^9, x^{17}, x^{127}]$.*

Proof. Let $R = \mathbb{F}_2[x^9, x^{17}]$ and $I = (x^9, x^{17})$.

Write $\alpha(x) = \frac{f(x)}{g(x)}$ such that $f, g \in \mathbb{F}_2[x]$ and $\gcd(f, g) = 1$.

Note first $x^9 \frac{f(x)}{g(x)} \in I$. So,

$$x^9 f(x) = (x^9, x^{17}) g(x) = (r_1(x) x^9 + r_2(x) x^{17}) g(x)$$

with $r_1(x), r_2(x) \in R = \mathbb{F}_2[x^9, x^{17}]$.

Note that as $\gcd(f, g) = 1$ in $\mathbb{F}_2[x]$ than $g(x) | x^9$ in $\mathbb{F}_2[x]$. Thus,

$$g(x) = x^n$$

up to a unit which is only the identity in this situation. Where $0 \leq n \leq 9$, then

$$f(x) = (r_1(x) + r_2(x) x^2) x^n$$

and as $\gcd(f, g) = 1$ in $\mathbb{F}_2[x]$, $n = 0$, otherwise $x | f$ and $x | g$. So $\alpha(x) = f(x) \in \mathbb{F}_2[x]$.

Now we must find all

$$F(x) = a_0 + a_1x + a_2x^2 + \cdots + a_kx^k \in \mathbb{F}_2[x]$$

such that $x^9f, x^{17}f \in R = \mathbb{F}_2[x^9, x^{17}]$.

$$\begin{aligned} x^9f =& a_0x^9 + a_1x^{10} + a_2x^{11} + a_3x^{12} + a_4x^{13} + a_5x^{14} + a_6x^{15} + a_7x^{16} + a_8x^{17} + a_9x^{18} + a_{10}x^{19} + a_{11}x^{20} \\ & + \cdots + a_{114}x^{123} + a_{115}x^{124} + a_{116}x^{125} + a_{117}x^{126} + a_{118}x^{127} + a_{119}x^{128} + \cdots . \end{aligned}$$

Since $x^9f \in R = \mathbb{F}_2[x^9, x^{17}]$ this implies that $a_m = 0$ such that

$$\begin{aligned} m =& \{1, 2, 3, 4, 5, 6, 7, 10, 11, 12, 13, 14, 15, 16, 19, 20, 21, 22, 23, 24, 28, 29, 30, 31, 32, 33, 37, 38, 39, 40, 41, 46, 47, \\ & 48, 49, 55, 56, 57, 58, 64, 65, 66, 67, 73, 74, 75, 82, 83, 84, 91, 92, 100, 101, 109, 118\}. \end{aligned}$$

Similarly,

$$\begin{aligned} x^{17}f =& a_0x^{17} + a_1x^{18} + a_2x^{19} + a_3x^{20} + \cdots + a_{106}x^{123} + a_{107}x^{124} + a_{108}x^{125} + a_{109}x^{126} + a_{110}x^{127} + a_{111}x^{128} \\ & + \cdots , \end{aligned}$$

Since $x^{17}f \in R = \mathbb{F}_2[x^9, x^{17}]$ this implies that $a_j = 0$ where

$$\begin{aligned} j =& \{2, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16, 20, 21, 22, 23, 24, 25, 29, 30, 31, 32, 33, 38, 39, 40, 41, 42, 47, 48, 49, 50, \\ & 56, 57, 58, 59, 65, 66, 67, 74, 75, 76, 83, 84, 92, 93, 101, 110\}. \end{aligned}$$

So,

$$\begin{aligned}f(x) =& a_0 + a_9x^9 + a_{17}x^{17} + a_{18}x^{18} + a_{26}x^{26} + a_{27}x^{27} + a_{34}x^{34} + a_{35}x^{35} + a_{36}x^{36} + a_{43}x^{43} + a_{44}x^{44} + \\ & a_{45}x^{45} + a_{51}x^{51} + a_{52}x^{52} + a_{53}x^{53} + a_{54}x^{54} + a_{60}x^{60} + a_{61}x^{61} + a_{62}x^{62} + a_{63}x^{63} + a_{68}x^{68} + a_{69}x^{69} + \\ & a_{70}x^{70} + a_{71}x^{71} + a_{72}x^{72} + a_{77}x^{77} + a_{78}x^{78} + a_{79}x^{79} + a_{80}x^{80} + a_{81}x^{81} + a_{85}x^{85} + a_{86}x^{86} + a_{87}x^{87} + \\ & a_{88}x^{88} + a_{89}x^{89} + a_{90}x^{90} + a_{94}x^{94} + a_{95}x^{95} + a_{96}x^{96} + a_{97}x^{97} + a_{98}x^{98} + a_{99}x^{99} + a_{102}x^{102} + \\ & a_{103}x^{103} + a_{104}x^{104} + a_{105}x^{105} + a_{106}x^{106} + a_{107}x^{107} + a_{108}x^{108} + a_{111}x^{111} + a_{112}x^{112} + a_{113}x^{113} + \\ & a_{114}x^{114} + a_{115}x^{115} + a_{116}x^{116} + a_{117}x^{117} + a_{119}x^{119} + a_{120}x^{120} + a_{121}x^{121} + a_{122}x^{122} + a_{123}x^{123} + \\ & a_{124}x^{124} + a_{125}x^{125} + a_{126}x^{126} + a_{127}x^{127} + a_{128}x^{128} + \cdots \in \mathbb{F}_2[x^9, x^{17}, x^{127}].\end{aligned}$$

Which concludes the proof. □

2.2 Main Results

This section will cover some main results of this project. However, before we establish Theorem 3.2.1, the theorem that will prove $(I : I) = \mathbb{F}[x^a, x^b, x^{ab-(a+b)}]$, which is a main focus of this project. I would first like to define the Frobenius number.

Definition 2.2.1. *For a given set of relatively prime integers, the* **Frobenius number** *is the greatest integer that cannot be expressed as a positive linear combination (with non-negative integer coefficients) of its elements.*

We can point out that the theorem that follows becomes trickier after we adjoin two variables x^a, x^b. This is because the Frobenius number is not well-understood for three or more variables. While with two variable it is very well-understood as $ab - (a + b)$.

The following lemma will later help guide us through the part of the proof which will show the second containment, $(I : I) \subseteq \hat{R} = \mathbb{F}[x^a, x^b, x^{ab-(a+b)}]$.

Lemma 2.2.1. *If $t + a, t + b \in (a, b)$ and $I = (x^a, x^b)$ then $x^t \in (I : I)$*

Proof. Suppose $t + a, t + b \in (a, b)$ and $I = (x^a, x^b)$. Then, $x^{t+a} \in I$. This implies that $x^t x^a \in I$, since $x^{t+a} = x^t x^a$. Similarly, $x^{t+b} = x^t x^b \in I$. Thus, since $x^a \in I$ and $x^b \in I$, by definition of $(I : I)$, $x^t \in (I : I)$. □

Theorem 2.2.1. *Suppose* $1 < a < b$ *where* $a, b \in \mathbb{N}$ *and* $\gcd(a, b) = 1$. *Let* $R = \mathbb{F}[x^a, x^b]$ *and* $I = (x^a, x^b)$. *Then* $(I : I) = \mathbb{F}[x^a, x^b, x^{ab-(a+b)}]$.

Proof. Let $\hat{R} = \mathbb{F}[x^a, x^b, x^{ab-(a+b)}]$. We first want to prove that $\hat{R} \subseteq (I : I)$. That is, we want to show that $x^{ab-(a+b)} \in (I : I)$.

Let $\alpha \in I$ be a monomial so $\alpha = x^t$ where $t \in (a, b)$ where (a, b) is the monoid generated by a and b. Using this monoid allows us to directly work with the exponents of x. In order to show that $x^{ab-(a+b)} \in (I : I)$ we must show that $(x^t)(x^{ab-(a+b)}) \in I$. Equivalently, we need to show that $t + ab - (a + b) \in (a, b)$.

Let $t = na + mb$ where $n, m \in \mathbb{N}_0$ such that n, m are not both zero. Then,

$$t + ab - (a + b) = na + mb + ab - a - b = ab + (n - 1)a + (m - 1)b.$$

Let $ab + (n-1)a + (m-1)b = S$. Now, we can consider three separate cases depending on n and m.
Case 1: $n \geq 1$ and $m \geq 1$. Then $S \in (a, b)$.

Case 2: $n = 0$ and $m \geq 1$. This implies that $S = ab + (0 - 1)a + (m - 1)b = ab - a + (m - 1)b = a(b - 1) + (m - 1)b \in (a, b)$.

Case 3: $m = 0$ and $n \geq 1$. This implies that $S = ab + (n - 1)a + (0 - 1)b = ab - b + (n - 1)a = b(a - 1) + (n - 1)a \in (a, b)$.
Therefore, $(x^t)(x^{ab-(a+b)}) \in I$ which implies that $x^{ab-(a+b)} \in (I : I)$. Hence, $\hat{R} \subseteq (I : I)$.

Now, we want to show that $(I : I) \subseteq \hat{R}$. Assume that $1 < a < b$, $\gcd(a, b) = 1$, $0 < t \leq ab - (a + b)$. We must show that if $t \leq ab - (a + b)$ then $t \notin (a, b)$. Now, by Lemma 2.2.1 we know that if $t + a, t + b \in (a, b)$ then $x^t \in (I : I)$.
Thus, suppose that $t + a, t + b \in (a, b)$ (by way of contradiction). Then, let $t + a = ma + nb$ and $t + b = pa + qb$ where $m, n, p, q \in \mathbb{N}_0$ such that m and n are not both 0 and p and q are not both 0. This give us that $t = (m - 1)a + nb$ and $t = pa + (q - 1)b$. Now, since $t \notin (a, b)$ this implies that $m = 0$ and $q = 0$. Thus, $t + a = nb$ and $t + b = pa$.
Now,

$$t + b - (t + a) = pa - nb.$$

This would imply that

$$b - a = pa - nb.$$

Which gives us

$$(n+1)b = (p+1)a.$$

Since $\gcd(a, b) = 1$ we have $a|(n+1)$ and $b|(p+1)$.

Recall that $t \leq ab - (a+b)$. So,

$$t + a \leq ab - a - b + a = ab - b$$

and

$$t + b \leq ab - a - b + b = ab - a.$$

Thus, $t + a = nb \leq ab - b$ and $t + b = pa \leq ab - a$. In particular,

$$nb \leq ab - b$$

and

$$pa \leq ab - a.$$

This implies that $n \leq a - 1$ and $p \leq b - 1$. This can be rearranged as $n + 1 \leq a$ and $p + 1 \leq b$.

Since $a|(n+1)$ and $n + 1 \leq a$ we conclude that $n + 1 = a$. Similarly, since $b|(p+1)$ and $p + 1 \leq b$ we conclude that $p + 1 = b$.

Thus,

$$t + a = nb = (a - 1)b.$$

Which implies that

$$t = ab - a - b = ab - (a + b)$$

and

$$t + b = pa = (b - 1)a.$$

Which implies that

$$t = ab - a - b = ab - (a + b).$$

This is a contradiction since $t \leq ab - (a + b)$. Therefore,

$$t + a, t + b \notin (a, b).$$

Hence,

$$x^t x^a, x^t x^b \notin I = (x^a, x^b).$$

So,

$$x^t \notin (I : I).$$

Hence, if $t \leq ab - (a + b)$ then $x^t \notin (I : I)$. Therefore, $(I : I) \subseteq \hat{R}$. Thus we have that $\hat{R} \subseteq (I : I)$ and $(I : I) \subseteq \hat{R}$. Therefore, $(I : I) = \hat{R} = \mathbb{F}[x^a, x^b, x^{ab-(a+b)}]$.

□

Furthermore, if we look at our results from Theorem 3.2.1 this is usually not the complete integral closure. Our result shows that it is always contained in the complete integral closure.

Chapter 3

A More General Setting

The next couple of theorems offers further a more general perspective on the results from Chapter 2. We will start this chapter by letting F be a field and I a nonzero additive subgroup. We will also let K be the quotient field of I, that is, $K = \{\frac{a}{b} | a, b \in I, b \neq 0\}$. We will say that I is dense if $K = F$.

In what follows, if R is an integral domain then $Z \subseteq R$ is the prime subring (that is, $\mathbb{Z}$ if $\text{char}(R) = 0$ and $\mathbb{Z}/p\mathbb{Z}$ if $\text{char}(R) = p$).

Theorem 3.0.1. *Let F be a field and I a dense additive subgroup. Then $(I :_F I)$ and $Z + I$ are distinct if K is not $\mathbb{Q}$ or an algebraic extension of $\mathbb{Z}/p\mathbb{Z}$.*

Proof. Suppose first that F is an algebraic extension of $\mathbb{Q}$ and let $\alpha \in F \backslash \mathbb{Q}$. The extension $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ is a finite algebraic extension. If R is the ring of integers of $\mathbb{Q}(\alpha)$ then we can find a prime $0 \neq p \in \mathbb{Z}$ such that the extension R/P is a proper field extension of $\mathbb{Z}/p\mathbb{Z}$ (where P is a prime ideal of R lying over (p)). The fact that this can be done is related to Chebotarev's Density Theorem (the specific result can be found as Proposition 7.36 in [7]).

Now let Q be a prime ideal of T, the integral closure of $\mathbb{Z}$ in F, containing P (and hence lying over $p\mathbb{Z}$ in $\mathbb{Z}$). Note that the ideal $p\mathbb{Z} + Q$ is a prime ideal of $\mathbb{Z} + Q$, and that the quotient $(\mathbb{Z} + Q)/(p\mathbb{Z} + Q) \cong \mathbb{Z}/p\mathbb{Z}$. Since T/Q is a field extension of R/P, which is a proper extension of $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z} + Q$ cannot be all of T. In this case, we conclude that $\mathbb{Z} + Q \subsetneq (Q :_F Q)$.

Now suppose that K is the prime field ($\mathbb{Q}$ in characteristic 0 or $\mathbb{Z}/p\mathbb{Z}$ in characteristic p) and $x \in F$ is transcendental over K. Consider the extension $K \subset \overline{K}_F \subset F$ where $\overline{K}_F$ is the algebraic closure

of K in F and let S be a transcendence basis of F over $\overline{K}_F$ containing x and $S_1 := S \setminus \{x\}$. In this case, we let $I := x\overline{K}_F(S_1)[x]$ and note that $\mathbb{Z} + I \subsetneq (I :_F I) = F(S_1)[x]$.
Finally, in the case that F is algebraic over $\mathbb{Z}/p\mathbb{Z}$, we note that all subrings of F are fields (it is well known that if $K \subseteq F$ is an algebraic exrension of fields and D is a domain such that $K \subseteq D \subseteq F$ then D is a field). This concludes the proof. □

Now that we have discussed when $(I :_F I)$ and $Z+I$ are distinct we now take a look at when $(I :_F I)$ is contained in the complete integral closure of $\mathbb{Z} + I$.

Theorem 3.0.2. *Let I be a dense ideal in F. Then $(I :_F I)$ is contained in the complete integral closure of $\mathbb{Z} + I$.*

Proof. Let $\alpha \in (I :_F I)$. If $\beta \in I$ is arbitrary, then $\alpha\beta \in I$ and hence $\alpha\beta^n \in I \subset \mathbb{Z} + I$ for all n. Hence α is almost integral over $\mathbb{Z} + I$ and hence is in the complete integral closure of $\mathbb{Z} + I$. □

Example 3.0.1. *We close this chapter with an example following from the previous theorem. Consider the example $\mathbb{F}[x^{2n+1}y^{n(2n+1)}]_{n=0}^{\infty}$ from [5]. This celebrated example showed that the complete integral closure of a domain need not be completely integrally closed. In fact its complete integral closure corresponds to its integral closure ($\mathbb{F}[xy^n]_{n=0}^{\infty}$) which in turn has complete integral closure $\mathbb{F}[x, y]$ (and the process ends here as $\mathbb{F}[x, y]$ is a UFD and is hence completely integrally closed). If we choose the ideal $I = (x^{2n+1}y^{n(2n+1)})_{n=0}^{\infty}$, then the complete integral closure of $Z + I = \mathbb{F}[xy^n]_{n=0}^{\infty}$ and is not completely integrally closed. Also, xy is in the complete integral closure of $Z + I$ but is not in $(I : I)$ since $x(xy) = x^2y$ is not in I.*

Bibliography

[1] Jim Coykendall. Algebra notes. Course NOtes, 2021. `http://jcoyken.people.clemson.edu/gradalgebranotes.pdf`.

[2] David S. Dummit and Richard M. Foote. *Abstract algebra*. Wiley, 3rd ed edition, 2004.

[3] Todd Fenstermacher. On integral closure and its variations. Master's Project, 2017.

[4] Robert W. Gilmer and William J. Heinzer. On the complete integral closure of an integral domain. *Journal of the Australian Mathematical Society*, 6(3):351–361, 1966.

[5] Robert W. Gilmer, Jr. and William J. Heinzer. On the complete integral closure of an integral domain. *J. Austral. Math. Soc.*, 6:351–361, 1966.

[6] Hideyuki Matsumura. *Commutative ring theory*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1986.

[7] Władysł aw Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer-Verlag, Berlin; PWN—Polish Scientific Publishers, Warsaw, second edition, 1990.

[8] J. C. Robson. Localizations of Hereditary Noetherian Rings. *Publications du Département de mathématiques (Lyon)*, 10(1):39–46, 1973.