May 2020

Prime Stability in Intermediate Extensions of Integral Domains

Philip de Castro
Clemson University, phisycs26@gmail.com

Prime Stability in Intermediate Extensions of Integral Domains

---

A Thesis
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Master's of Science
Mathematical & Statistical Sciences

---

by
Philip J. de Castro
May 2020

Accepted by:
Dr. James B. Coykendall, Committee Chair
Dr. Sean Sather-Wagstaff
Dr. Matthew Macauley

Abstract

We consider integral domains $R \subset S \subset T$, where T is integral over R. In particular, we study the behavior of an element $p \in R$ which is prime in both R and T and which may or may not be prime in S. If p remains prime in S, we say that p has prime stability. Otherwise, p does not have prime stability. We first consider the case of a quadratic ring of integers, $\mathbb{Z} \subset \mathbb{Z}[\omega]$, with $\mathbb{Z}[\omega]$ a quadratic extension of $\mathbb{Z}$. We proceed to prove results using Legendre, Jacobi, and Kronecker symbols and field discriminants, using both of these tools to determine a criterion for determining the primality of an element in orders of the ring of integers, namely the intermediate extension in the extension $\mathbb{Z} \subset \mathbb{Z}[n\omega] \subset \mathbb{Z}[\omega]$. After this, we consider some conjectures concerning the behavior of prime stability in integral extensions. We then discuss some fundamental definitions and previous work on integral extensions. With all of these tools, we observe some examples which provide support for the conjectures.

Acknowledgments

I would like to thank Dr. Jim Coykendall for all of his guidance and support in this project. From answering the same questions more than once to critiquing my proofs, thank you for your patience and insight.

Sola scriptura. Sola fide. Sola gratia. Solus Christus. Soli Deo gloria.

Table of Contents

Chapter 1

Introduction

1.1 Motivational Example

We are all quite familiar with the algebraic construction of rings in one form or another. Perhaps the most classic, and intuitive, example of a ring comes in the form of the integers, $\mathbb{Z}$. We of course have addition and multiplication in $\mathbb{Z}$ and as a matter of fact, $\mathbb{Z}$ forms a Euclidean domain, which possesses some useful properties.

Definition 1.1.1. Let R be an integral domain. We say that R is a

1. **Euclidean domain** if there is a function $N : R \to \mathbb{N}_0$ such that

   (a) $N(xy) \geq N(x)$, for all nonzero $x, y \in R$

   (b) If $x, y \in R$, with x, y nonzero, then there are $q, r \in R$ such that $y = xq + r$ with $r = 0$ or $N(r) < N(x)$.

   We call this function $N : R \to \mathbb{N}_0$ a **norm function**;

2. **Principal Ideal Domain** (PID) if every ideal of R is principally generated, i.e., for any ideal $I \subseteq R, I = (\alpha)$ for some $\alpha \in R$;

3. **Unique Factorization Domain** (UFD) if every nonzero nonunit of R can be written (uniquely) as a product of primes.

Primes are of particular significance in our discussion here. In the case of the integers, we can define these prime elements in an intuitive way: $p \in \mathbb{Z}$ is prime if $p \neq 0$, $p \neq 1$, and the only integers dividing p are ± 1 and $\pm p$. These primes (in absolute value) are $2, 3, 5, 7, \ldots$ and so on.

We actually have a connection between Eulicdean domains, PIDs, and UFDs.

Theorem 1.1.2. Let R be an integral domain. If R is a Euclidean domain, then it is a PID. If R is a PID, then R is a UFD.

In order to prove this, we need a characterization of UFDs.

Theorem 1.1.3. [9] A ring is a UFD if and only if every nonzero prime ideal contains a principal prime ideal.

We proceed to prove Theorem 1.1.2 and consider the proof from [4].

Proof. First, suppose that R is a Euclidean domain with norm function N and let $I \subseteq R$ be an ideal. Let

$$S = \{N(x) \mid x \in I \setminus \{0\}\}.$$

Indeed, $S \subseteq \mathbb{N} \cup \{0\}$, and so by the Well Ordering Principle, S has a least element. Let $\alpha \in I$ be such that $N(\alpha)$ is this least element of S. We proceed to show that $I = (\alpha)$. Note that as $\alpha \in I$ then certainly $(\alpha) \subseteq I$. Thus, it suffices to show that $I \subseteq (\alpha)$.

To that end, let $\beta \in I$. As R is a Euclidean domain, we may write

$$\beta = q\alpha + r$$

with $r = 0$ or $N(r) < N(\alpha)$. As I is an ideal and $\alpha \in I$, we have that $q\alpha \in I$. Note

$$r = \beta - q\alpha.$$

Since $\beta, q\alpha \in I$ then $r \in I$. We know that $N(\alpha)$ is minimal, which means it is impossible for $N(r)$ to be less than $N(\alpha)$. Thus, $r = 0$. So

$$\beta = q\alpha$$

and $\beta \in (\alpha)$. Ergo, $I = (\alpha)$. Since I is an arbitrary ideal of R, we conclude that every ideal of R is principally generated. Therefore, R is a PID.

Now we suppose that R is a PID and we desire to show that R is a UFD. By Theorem 1.1.3, it suffices to check every nonzero prime ideal of R for a principal prime ideal.

If R has no nonzero prime ideals, then R is a field and is therefore a UFD. (If R is a field, all elements are units and so R has no nonzero primes. Thus, vacuously, R is a UFD.) Now suppose that R has a nonzero prime ideal, call it P. Since R is a PID, we know that $P = (p)$ for some element p. But as $P = (p)$ is a prime ideal, we must have that p is a prime element. Thus, as P is an arbitrary prime ideal, we may conclude that every prime ideal of R contains a nonzero principal prime ideal (in fact, every prime ideal *is* a principal prime ideal) and so by Theorem 1.1.3, R is a UFD. □

The integers are a Euclidean domain and the norm function is standard absolute values. Thus, the integers are a PID and therefore a UFD. So for any $n \in \mathbb{Z}$, with n nonzero, we have that $n = \pm p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ for some powers of primes $p_i, 1 \leq i \leq k$.

We can actually construct larger rings which contain the integers. We do this by throwing whatever we like into the integers and taking all of the possible sums and products with these new elements, which will ensure that we still have a ring. A classic example of this is of course found with the **Gaussian integers**, where we append $i = \sqrt{-1}$. If we adjoin i to the integers, we have

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

This actually accounts for all possible products and sums once we adjoin i to $\mathbb{Z}$. Note that $\mathbb{Z} \subset \mathbb{Z}[i]$ as for any $n \in \mathbb{Z}$,

$$n = n + 0i \in \mathbb{Z}[i].$$

We call $\mathbb{Z}[i]$ a **quadratic extension** of $\mathbb{Z}$ since i is the root of a quadratic polynomial. In particular, $\mathbb{Z}[i]$ is a **quadratic ring of integers**. In order for us to understand and generalize this object, we consider the following definitions.

Definition 1.1.4. Let $R \subseteq T$ be integral domains. We say that $t \in T$ is **integral over** R if t is the root of a monic polynomial $r(x) \in R[x]$. (Recall that a monic polynomial is a polynomial with leading coefficient 1, i.e., $r(x) = x^n + r_{n-1}x^{n-1} + \cdots + r_1 x + r_0$.) If every $t \in T$ is integral over R, then we say that T is **integral over** R or that T is an **integral extension of** R.

Of course, R is integral over itself. After all, for any $r \in R$, r is the root of the monic

polynomial $x - r \in R[x]$.

Definition 1.1.5. Let $R \subseteq T$. The **integral closure of R in T** is

$$\overline{R}_T = \{t \in T \mid t \text{ is integral over } R\}$$

and $\overline{R} = \overline{R}_K$, where K is the quotient field of R, is the **integral closure of R**. If $R = \overline{R}$, then we say that R is **integrally closed**.

We note that it can be shown that $\overline{R}_T, \overline{R}$ are both indeed rings. This is a useful fact as the integral closure of a ring is a powerful extension that allows us to build algebraic structures that find applications in number theory.

Definition 1.1.6. Let $F \subseteq K$ be a field extension. Then the dimension of K over F as a vector space is the **degree of the extension**.

Definition 1.1.7. Consider $\mathbb{Z} \subset \mathbb{Q}$. Let F be a finite extension of degree $n \geq 1$ over $\mathbb{Q}$. Then $R \subseteq F$, where $R := \overline{\mathbb{Z}}_F$, the integral closure of $\mathbb{Z}$ in F, is the **ring of integers** of the extension F.

We can visualize this definition of a ring of integers with the following diagram.

$$\begin{array}{ccc} \overline{\mathbb{Z}}_F & \text{——} & F \\ | & & | \\ \mathbb{Z} & \text{——} & \mathbb{Q} \end{array}$$

Definition 1.1.8. Let R be a ring of integers. Then a subring $A \subseteq R$, such that A and R have the same quotient field, is an **order of R**.

For our motivating example, we consider quadratic rings of integers and orders of integers. Note that a quadratic ring of integers is simply an extension of degree 2. We have the following theorem that describes what every quadratic ring of integers looks like.

Theorem 1.1.9. [3] Let T be a quadratic ring of integers and let d be a square-free integer. Then

$$T = \begin{cases} \mathbb{Z}[\sqrt{d}], & \text{if } d \equiv 2, 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

Furthermore, if S is an order of T, then

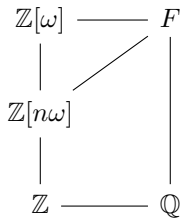
$$S = \begin{cases} \mathbb{Z}[n\sqrt{d}], & \text{if } d \equiv 2,3 \pmod 4 \\ \mathbb{Z}\left[n\left(\frac{1+\sqrt{d}}{2}\right)\right], & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

for $n \in \mathbb{N}$.

For our purposes we define

$$\omega = \begin{cases} \sqrt{d}, & \text{if } d \equiv 2,3 \pmod 4 \\ \frac{1+\sqrt{d}}{2}, & \text{if } d \equiv 1 \pmod 4. \end{cases} \tag{1.1}$$

When we have an order of a ring of integers, we can visualize the relations between all of our rings with the following diagram.



for $n \in \mathbb{N}$. It can be shown that $\mathbb{Z}[n\omega]$ is integrally closed if and only if $n = 1$. So $\mathbb{Z}[n\omega]$ is truly a ring of integers if and only if $n = 1$. When dealing with rings of integers and orders, we can define an invariant called a **discriminant**. But in order for us to define the discriminant, we need to first discuss the **trace**.

Definition 1.1.10. Let F be a finite extension of $\mathbb{Q}$ and $\beta \in F$. The **trace** of β is

$$Tr(\beta) = \sum_{\sigma} \sigma(\beta)$$

where the sum ranges over the distinct embeddings $\sigma : F \to \mathbb{C}$. The **norm** of β is

$$N(\beta) = \prod_{\sigma} \sigma(\beta)$$

where the product ranges over the distinct embeddings $\sigma : F \to \mathbb{C}$.

Definition 1.1.11. For a basis $\{v_1, v_2, \ldots, v_n\}$ of the extension $\mathbb{Q} \subseteq F$ of finite degree, we define

the **discriminant** by

$$D = \det(\mathrm{Tr}(v_i v_j)).$$

For a basis of a quadratic ring of integers given by $\{1, \omega\}$, with ω defined in Equation (1.1), the discriminant is

$$D = \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\omega) \\ \mathrm{Tr}(\omega) & \mathrm{Tr}(\omega^2) \end{pmatrix} = \begin{cases} \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d, & \text{if } d \equiv 2, 3 \pmod 4 \\ \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{pmatrix} = d, & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

For a basis of an order of a quadratic ring of integers with basis $\{1, n\omega\}$, the discriminant is given by

$$D = \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(n\omega) \\ \mathrm{Tr}(n\omega) & \mathrm{Tr}((n\omega)^2) \end{pmatrix} = \begin{cases} \det \begin{pmatrix} 2 & 0 \\ 0 & 2dn^2 \end{pmatrix} = 4dn^2, & \text{if } d \equiv 2, 3 \pmod 4 \\ \det \begin{pmatrix} 2 & n \\ n & n^2 \frac{d+1}{2} \end{pmatrix} = dn^2, & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

We now have sufficient background on quadratic rings of integers to begin asking some questions. We already addressed prime elements in the context of the integers, but now we turn our attention to primes in $\mathbb{Z}[\omega]$. For example, in $\mathbb{Z}[i]$, we want to consider how to factor an element like $25 + 14i$ into primes. Evidently, $25 + 14i \notin \mathbb{Z}$ so if we can still factor this element into primes, we must have that there are "more" primes in $\mathbb{Z}[i]$ than in $\mathbb{Z}$. We thus must consider a more general definition of prime.

Definition 1.1.12. A **unit** is an element $x \in R$ such that there is a $y \in R$ with $xy = 1$.

Definition 1.1.13. Let R be an integral domain. An nonunit $p \in R$ is prime if for $a, b \in R$, $p \mid ab$ implies $p \mid a$ or $p \mid b$.

This is the notion of prime that we study in this endeavor. In particular, we will be observing how primality is affected through integral extensions. In fact, we can generalize the notion of prime even further to **irreducible** and **prime ideals**.

Definition 1.1.14. Let R be an integral domain. A nonunit $\alpha \in R$ is **irreducible** if $\alpha = ab$ implies that either a or b is a unit.

Definition 1.1.15. Let R be an integral domain. A proper ideal $P \subseteq R$ is a **prime ideal** of R if for ideals $A, B \subseteq R$, $AB \subseteq P$ implies $A \subseteq P$ or $B \subseteq P$.

We have a theorem connecting prime ideals to prime elements.

Theorem 1.1.16. Let $p \in R$. p is prime if and only if (p) is a prime ideal of R.

Theorem 1.1.17. Let $x \in R$. x is irreducible if and only if (x) is maximal in the set of proper principal ideals of R. That is, if $(x) \subseteq (\alpha)$ then either $(\alpha) = (x)$ or $(\alpha) = R$.

It can be shown that in integral domains, nonzero prime implies irreducible and in the case of UFDs, irreducibles and nonzero primes are the same thing. Let us focus in on a particular prime element of $\mathbb{Z}$, namely 3, and we consider if it is still prime in $\mathbb{Z}[i]$. To answer this, recall that the Gaussian integers is a Euclidean domain, with norm function $N : \mathbb{Z}[i] \to \mathbb{N}_0$ given by $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$. Therefore, $\mathbb{Z}[i]$ is a UFD. Thus, it suffices to show that 3 is irreducible in $\mathbb{Z}[i]$. To that end, consider the following proposition.

Proposition 1.1.18. Let $N : \mathbb{Z}[i] \to \mathbb{N}_0$ be the norm function for $\mathbb{Z}[i]$. Then $N(a + bi) = 1$ if and only if $a + bi$ is a unit, i.e., $a + bi = -1, 1, -i, i$.

Proof. It is easy to see that $N(-1) = N(1) = (-i) = N(i) = 1$. Now suppose $N(a + bi) = 1$. So $N((a + bi)) = (a + bi)(a - bi) = a^2 + b^2 = 1$. So either $a = \pm 1$ and $b = 0$ or $a = 0$ and $b = \pm 1$. In either case, we have that $a + bi = -1, 1, -i, i$. Conversely, if $a + bi$ is a unit, it must be $-1, 1, -i$, or i. Thus, $N(a + bi) = 1$. □

We can actually generalize this norm function for any quadratic ring of integers.

Definition 1.1.19. Let $\mathbb{Z}[\omega]$ be a quadratic ring of integers with ω defined in Equation (1.1). Then the function $N : \mathbb{Z}[\omega] \to \mathbb{N}_0$ defined by

$$N(a + b\omega) = (a + b\omega)(a + b\overline{\omega}) = a^2 + ab(\omega + \overline{\omega}) + b^2\omega\overline{\omega} = a^2 + ab\mathrm{Tr}(\omega) + b^2\mathrm{N}(\omega),$$

where $\mathrm{Tr}(\cdot)$ and $\mathrm{N}(\cdot)$ are the trace and norm defined in Definition 1.1.10, is the **norm function** for $\mathbb{Z}[\omega]$.

It is worth noting that the norm defined in Definition 1.1.19 should be distinguished from the norm function defined for Euclidean domains. However, in some cases, the norm of Definition 1.1.19 can function as a Euclidean domain norm. We now have the machinery necessary to answer our question about the primeness of 3 in $\mathbb{Z}[i]$.

Proposition 1.1.20. 3 is prime in $\mathbb{Z}[i]$.

Proof. As $\mathbb{Z}[i]$ is a Euclidean domain and hence a UFD, it suffices to show that 3 is irreducible. Towards a contradiction, suppose 3 is not an irreducible in $\mathbb{Z}[i]$. Thus, there are $a+bi, c+di \in \mathbb{Z}[i]$, both nonzero nonunits such that $(a+bi)(c+di) = 3$. Noting the norm of 3, we have

$$N(3+0i) = 9.$$

Thus,

$$N((a+bi)(c+di)) = N(a+bi)N(c+di) = 9.$$

As neither $a+bi$ nor $c+di$ are units, we must have that $N(a+bi) = 3 = N(c+di)$ (after all, the factorizations of 9 are $9 = 3 \cdot 3 = 1 \cdot 9$, and a norm of 1 indicates a unit so we must have the factorization of $3 \cdot 3$). Without loss of generality, consider $N(a+bi) = a^2 + b^2$. We must have

$$a^2 + b^2 = 3.$$

Note that $0^2 = 0, (\pm 1)^2 = 1, (\pm 2)^2 = 4$. Thus, any solution set must have $a < 2$ and $b < 2$. But of course we cannot make $a^2 + b^2 = 3$ for $a, b \in \{0, 1\}$. Thus, $N(a+bi) \neq 3$ and so either $a+bi$ or $c+di$ must be a unit. But this contradicts our assumption that neither $a+bi$ nor $c+di$ are units. Therefore, 3 is irreducible and is thus prime. □

This proof is, in some sense, quite convenient. It relies primarily on the fact that $\mathbb{Z}[i]$ is a UFD. We would like to generalize to the case where a ring of integers is not a UFD.

For example, consider $\mathbb{Z} \subset \mathbb{Z}[\sqrt{-5}]$ and the element 2. Using norm arguments analogous to the proof for Proposition 1.1.20, we can show that 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$. However, 2 is not prime as $2 \mid (1+\sqrt{-5})(1-\sqrt{-5}) = 6$ but $2 \nmid 1+\sqrt{-5}$ and $2 \nmid 1-\sqrt{-5}$. In UFDs, though, irreducible and prime are the same thing. So $\mathbb{Z}[\sqrt{-5}]$ cannot be a UFD.

We need some more number theory magic to construct a more robust way of evaluating the

primeness of an element in a quadratic ring of integers. To do this, we first discuss a generalization of a ring of algebraic integers called **Dedekind domains**. We reference [4] for these definitions.

Definition 1.1.21. Let R be a ring with quotient field K and $I \subset K$ an R-submodule. I is a **fractional ideal** if there is a nonzero $\alpha \in R$ such that $\alpha I \subseteq R$.

A good example of this can be found in $\mathbb{Z} \subseteq \mathbb{Q}$. If we consider the ideal $\frac{5}{2}\mathbb{Z}$, then for $\alpha = 2$ we have $2\left(\frac{5}{2}\mathbb{Z}\right) = 5\mathbb{Z} \subseteq \mathbb{Z}$.

Definition 1.1.22. Let I, J be fractional ideals of a ring R. We define the ideal IJ by

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

Consider, for example, $I = \frac{5}{2}\mathbb{Z}$ and $J = \frac{4}{7}\mathbb{Z}$. Then

$$IJ = \left\{ \sum_{i=1}^{n} \frac{5a_i}{2} \cdot \frac{4b_i}{7} \ \mid \ a_i, b_i \in \mathbb{Z}, n \in \mathbb{N} \right\}.$$

Now consider $I = \frac{5}{2}\mathbb{Z}$ and $J = \frac{2}{5}\mathbb{Z}$, then

$$IJ = \left\{ \sum_{i=1}^{n} \frac{5a_i}{2} \cdot \frac{2b_i}{5} \ \mid \ a_i, b_i \in \mathbb{Z}, n \in \mathbb{N} \right\} = \left\{ \sum_{i=1}^{n} a_i \cdot b_i \ \mid \ a_i, b_i \in \mathbb{N} \right\} = \mathbb{Z}.$$

Evidently, there is something special about this J. It functions as a "multiplicative inverse" of sorts.

Definition 1.1.23. Let I be a fractional ideal of a ring R with quotient field K. Then we define the **inverse of** I by

$$I^{-1} = \{x \in K \ \mid \ xI \subseteq R\}.$$

Indeed, $II^{-1} \subseteq R$ for any fractional ideal I of R. Sometimes, $II^{-1} = R$. When $II^{-1} = R$, we say that I is **invertible**.

We proceed to list some properties of invertible ideals.

Theorem 1.1.24. [9] Let R be an integral domain. If I is an invertible ideal of R, then I is finitely generated.

Theorem 1.1.25. [9] Let R be an integral domain. Let $I \subseteq R$ be invertible. Then there exists an ideal $J \subseteq R$ such that IJ is a principal ideal.

The next theorem actually lays the groundwork for **Dedekind domains**.

Theorem 1.1.26. [4] Let R be an integral domain. The following are equivalent:

1. For all nonzero ideals $I \subseteq R$, I is invertible.
2. For all nonzero fractional ideals I of R, I is invertible.
3. For every proper ideal I of R, I is a unique product of prime ideals.
4. R is a Noetherian ring with $\dim(R) \leq 1$ and is integrally closed.

Any domain R satisfying one, and therefore all, of the above is a **Dedekind domain**.

The third property of Theorem 1.1.26 is typically the most commonly used definition for a Dedekind domain. In [3], we have a useful theorem.

Theorem 1.1.27. [3] Let N be the norm function as defined in Definition 1.1.10. Let $p \in \mathbb{Z}$ be prime and let $\mathfrak{P}$ be a prime ideal of $\mathbb{Z}[\omega]$ with ω defined by Equation (1.1). Then the ideal (p) is affected in $\mathbb{Z}[\omega]$ in one of the following ways:

$$\begin{cases} (p) = (p), \text{ (or } p \text{ is inert and therefore remains prime)} & \Rightarrow N((p)) = p^2 \\ (p) = \mathfrak{P}\overline{\mathfrak{P}} \text{ or } p \text{ splits and therefore is no longer prime} & \Rightarrow N(\mathfrak{P}) = N(\overline{\mathfrak{P}}) = p \\ (p) = \mathfrak{P}^2 \text{ or } p \text{ ramifies and therefore is no longer prime} & \Rightarrow N(\mathfrak{P}) = p. \end{cases}$$

In [7], we have another useful theorem. For our purposes, we note that any Dedekind domain is a Prüfer domain that has the "$1\frac{1}{2}$ generators" property, meaning that any ideal can be generated by two elements, the first of which may be arbitrarily chosen among the nonzero elements of the ideal.

Theorem 1.1.28. [7] Let R be a Prüfer domain with $\dim(R) = 1$. Then every ideal can be generated by $1\frac{1}{2}$ elements. If $\text{rad}(R) \neq 0$ then every finitely generated ideal is principal.

We now introduce a useful tool from number theory. Recall that for an odd prime p and a nonzero integer a relatively prime to p, a is a **quadratic residue** of p if there is a solution to

the congruence relation $x^2 \equiv a \pmod{p}$. Otherwise, a is a **quadratic nonresidue**. For example, consider $p = 7$. Then

$$1^2 = 1 \equiv 1 \pmod{7} \qquad 2^2 = 4 \equiv 4 \pmod{7} \qquad 3^2 = 9 \equiv 2 \pmod{7}$$
$$4^2 = 16 \equiv 2 \pmod{7} \quad 5^2 = 25 \equiv 4 \pmod{7} \quad 6^2 = 36 \equiv 1 \pmod{7}.$$

Thus, $1, 2, 4$ are the quadratic residues of 7 and $3, 5, 6$ are the quadratic nonresidues. Indeed, we can always explicitly find the quadratic residues of a prime, but it can certainly be tedious as p gets large. In order to deal with this difficulty, number theory has a useful tool in examining quadratic residues called the **Legendre symbol**.

Definition 1.1.29. Let a be an integer and p an odd prime. Then the symbol $\left(\frac{a}{p}\right)$ defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue of } p \\ -1, & \text{if } a \text{ is } \textbf{not} \text{ a quadratic residue of } p \text{ (or a quadratic nonresidue)} \\ 0, & \text{if } p \mid a, \end{cases}$$

is the **Legendre symbol**.

Following the example from above we have

$$\left(\frac{1}{7}\right) = 1 \qquad \left(\frac{2}{7}\right) = 1 \qquad \left(\frac{3}{7}\right) = -1$$

$$\left(\frac{4}{7}\right) = 1 \quad \left(\frac{5}{7}\right) = -1 \quad \left(\frac{6}{7}\right) = -1$$

We list some properties of Legendre symbols that are useful to us from [8].

Proposition 1.1.30. Let a, b be integers and p a prime. Then

a) $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$

b) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

c) If $a \equiv b \pmod{p}$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Theorem 1.1.31. (Law of Quadratic Reciprocity) Let p, q be odd primes. Then

a) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

b) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

c) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

Legendre symbols are useful when dealing with odd primes. Now we generalize to $\left(\frac{a}{b}\right)$, for some $a \in \mathbb{Z}$ and b a nonzero odd integer. We use **Jacobi symbols**. The following definition is from [3].

Definition 1.1.32. Let $a, b \in \mathbb{Z}$ with b a nonzero odd integer. Let $b = \pm\prod_i p_i^{\alpha_i}$ be the prime factorization of b. Then we define the symbol $\left(\frac{a}{b}\right)$ by

$$\left(\frac{a}{b}\right) = \prod_i \left(\frac{a}{p_i}\right)^{\alpha_i}$$

as the **Jacobi symbol**. If $b = \pm 1$, we define $\left(\frac{a}{b}\right) = 1$.

There is a significant difference between Legendre symbols and Jacobi symbols that is worth noting. With Legendre symbols, there is no ambiguity whether an integer a is a quadratic residue or nonresidue modulo a prime p. But [3] points out a necessary and sufficient condition for the solvability of

$$x^2 \equiv a \pmod{pq} \tag{1.2}$$

for distinct primes p, q. In particular, for p, q which do not divide a, Equation 1.2 is solvable if and only if $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$, where $\left(\frac{a}{p}\right)$ and $\left(\frac{a}{q}\right)$ are Legendre symbols. However, if the Jacobi symbol $\left(\frac{a}{pq}\right) = -1$, then Equation (1.2) is unsolvable.

[3] notes the following proposition.

Proposition 1.1.33. Let $a, b \geq 0$ and odd. Then

a) $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$

b) $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$

c) $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)(-1)^{\frac{b-1}{2}\cdot\frac{a-1}{2}}$.

We can actually make one more generalization on these symbols. These symbols are defined in terms of odd primes and odd numbers, but we have not accounted for the other half of the integers: the even numbers. To do this, we define another symbol, the **Kronecker symbol**.

Definition 1.1.34. [3] Let $a \in \mathbb{Z}$. Then we define **Kronecker's extension of Jacobi's symbol** by

$$\left(\frac{a}{2}\right) = \begin{cases} 0, & \text{if } a \equiv 0 \pmod 4 \\ 1, & \text{if } a \equiv 1 \pmod 8 \\ -1, & \text{if } a \equiv 5 \pmod 8 \\ \text{undefined}, & \text{for all other } a. \end{cases}$$

Note that we need only consider 2 and not higher powers of two because we use the same definition as Jacobi symbols in Definition 1.1.32 to deal with higher powers.

Using Jacobi and Kronecker symbols and discriminants, we have the following theorem from [3].

Theorem 1.1.35. The rational prime p factors in the quadratic ring of integers $\mathbb{Z}[\omega]$, with ω defined in Equation (1.1), according to the following based on the discriminant of the field, D, and the Kronecker symbol, $\left(\frac{D}{p}\right)$.

$$\begin{cases} (p) = (p) \text{ (i.e., } (p) \text{ remains prime)} \iff \left(\frac{D}{p}\right) = -1; \\ (p) = \mathfrak{P}\overline{\mathfrak{P}} \text{ (i.e., } (p) \textbf{ splits} \text{ into two factors } \mathfrak{P} \neq \overline{\mathfrak{P}}) \iff \left(\frac{D}{p}\right) = 1; \\ (p) = \mathfrak{P}^2 \text{ (i.e., } (p) \textbf{ ramifies)} \iff \left(\frac{D}{p}\right) = 0. \end{cases}$$

We note that this is independent of whether $d \equiv 2, 3 \pmod 4$ or $d \equiv 1 \pmod 4$.

Observe that this theorem is indeed a primality test as p is prime if and only if (p) is a prime ideal. We follow the proof given in [3].

Proof. We first prove the forwards direction for the splitting and ramifying cases. To that end, suppose $(p) = \mathfrak{P}\overline{\mathfrak{P}}$ or $(p) = \mathfrak{P}^2$ (we prove both cases simultaneously). By [7], we have that $\mathfrak{P} = (\pi, p)$ for some π and $p \mid N(\pi)$, where N is the norm function as defined in Definition 1.1.19. We note that if $p \mid \pi$ then $\mathfrak{P} = (p, \pi) = p(1, \pi/p) = (p)$ and so p would not factor, which contradicts our initial assumption. Thus, we may safely assume that $\mathfrak{P} = (p, \pi)$, where $p \mid N(\pi)$, and $p \nmid \pi$.

Suppose p is odd. Then we write $\pi = a + b\sqrt{d}$ if $d \equiv 2, 3 \pmod 4$ or $\pi = \frac{a+b\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$. Either way, we know that $N(\pi) \equiv 0 \pmod p$, by assumption. Note that $p \nmid b$ because if $p \mid b$ then $p \mid a$ which would mean that $p \mid \pi$, which contradicts our assumption. Since p is prime, we

know that every nonzero congruence class has an inverse. Letting $\beta \equiv b^{-1} \pmod{p}$ we have that

$$\begin{aligned}
\beta^2(a^2 - b^2 d) &\equiv \beta^2 \cdot 0 \pmod{p} \\
\beta^2 a^2 - \beta^2 b^2 d &\equiv 0 \pmod{p} \\
\beta^2 a^2 - d &\equiv 0 \pmod{p} \\
\beta^2 a^2 &\equiv d \pmod{p} \\
(\beta a)^2 &\equiv d \pmod{p}.
\end{aligned}$$

Thus, $\left(\frac{d}{p}\right) = 0$ or 1. Therefore, if $d \equiv 2, 3 \pmod{4}$ then $\left(\frac{D}{p}\right) = \left(\frac{4d}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{2}{p}\right)\left(\frac{d}{p}\right) = (-1)^{\frac{p^2-1}{4}}\left(\frac{d}{p}\right)$. Since p is odd, $(-1)^{\frac{p^2-1}{4}} = 1$. Thus, $\left(\frac{D}{p}\right) = \left(\frac{d}{p}\right) = 1$ or 0.

Now we consider the case when $p = 2$. We use Kronecker's symbol for this. Thus, $\left(\frac{D}{p}\right) = -1$ as $D = d \equiv 5 \pmod{8}$. Let $\pi = \frac{a+b\sqrt{d}}{2}$. Then $2 \mid N(\pi) = \frac{a^2-db^2}{4}$. Again, $2 \nmid a$ nor b as then $2 \mid \pi$, which goes against our assumption. We also note that $a \equiv b \pmod{2}$ as $d \neq p^2\alpha$ and since p is prime, $(\alpha, p) = 1$. This would imply that $a^2 - db^2 \equiv 0 \pmod{8}$, which contradicts our assumption that $d \equiv 5 \pmod{8}$. After all, for a, b odd, $a^2 \equiv b^2 \equiv 1 \pmod{8}$. Thus, we must have that $\left(\frac{D}{p}\right) = 1$ or 0.

We may now proceed to prove the backwards direction. We again begin by letting p be odd and suppose $\left(\frac{D}{p}\right) = 0$. Let $\pi = \sqrt{d}$ and define $\mathfrak{P} = (p, \pi)$. Then

$$\mathfrak{P}^2 = (p, \pi)^2 = (p^2, p\pi, \pi^2) = (p^2, p\sqrt{d}, d).$$

But we know that $\left(\frac{D}{p}\right) = \left(\frac{d}{p}\right) = 0$. Thus, $p \mid d$. So

$$\mathfrak{P}^2 = (p^2, p\sqrt{d}, d) = p\left(p, \sqrt{d}, \frac{d}{p}\right).$$

But d is square-free so $\left(p, \frac{d}{p}\right) = (1)$. (After all, d square free means that after dividing d by p, there are no other factors of p left. Thus, d is necessarily relatively prime to p.) Thus,

$$\mathfrak{P}^2 = p\left(p, \sqrt{d}, \frac{d}{p}\right) = p(1) = (p).$$

Now let p still be odd and $\left(\frac{D}{p}\right) = 1$. Thus, we have that there is an $a \in \mathbb{Z}_p$ such that $a^2 \equiv D$

(mod p). Let $\pi = a + \sqrt{d}$ and define

$$\begin{aligned}\mathfrak{P} &= (p, a + \sqrt{d}) = (p, \pi) \\ \overline{\mathfrak{P}} &= (p, a - \sqrt{d}) = (p, \overline{\pi}).\end{aligned}$$

We note that $\mathfrak{P} \neq \overline{\mathfrak{P}}$. After all, if $\mathfrak{P} = \overline{\mathfrak{P}}$ then

$$\begin{aligned}\mathfrak{P} = \overline{\mathfrak{P}} &= \mathfrak{P} + \overline{\mathfrak{P}} \\ &= (p, a + \sqrt{d}, a - \sqrt{d}) \\ &= (p, 2a, a + \sqrt{d}, a - \sqrt{d}) \\ &= (1),\end{aligned}$$

as $(p, a) = 1$ (since $a \in \mathbb{Z}_p$). This contradicts the fact that $(p) = \mathfrak{P}\overline{\mathfrak{P}}$, which is now shown.

$$\begin{aligned}\mathfrak{P}\overline{\mathfrak{P}} &= (p, a + \sqrt{d})(p, a - \sqrt{d}) \\ &= (p^2, pa - p\sqrt{d}, pa + p\sqrt{d}, a^2 - d) \\ &= p\left(p, a - \sqrt{d}, a + \sqrt{d}, \frac{a^2 - d}{p}\right) \\ &= p\left(p, 2a, a - \sqrt{d}, a + \sqrt{d}, \frac{a^2 - d}{p}\right) \\ &= p(1) \\ &= (p).\end{aligned}$$

We now need to show that $\mathfrak{P}, \overline{\mathfrak{P}}$ are both prime ideals. However, the very fact that (p) splits means that its factors $\mathfrak{P}$ and $\overline{\mathfrak{P}}$ are prime by Theorem 1.1.27.

Lastly, we prove the backwards direction for $p = 2$. If $\left(\frac{D}{2}\right) = 1$, then $D \equiv 1 \pmod 8$. We define

$$\begin{aligned}\mathfrak{P} &= \left(2, \frac{1 + \sqrt{d}}{2}\right) \\ \overline{\mathfrak{P}} &= \left(2, \frac{1 - \sqrt{d}}{2}\right).\end{aligned}$$

We again have that $\mathfrak{P} \neq \overline{\mathfrak{P}}$. Following our proof from above, if $\mathfrak{P} = \overline{\mathfrak{P}}$ then

$$\begin{aligned}
\mathfrak{P} = \overline{\mathfrak{P}} &= \mathfrak{P} + \overline{\mathfrak{P}} \\
&= \left(2, \frac{1+\sqrt{d}}{2}, \frac{1-\sqrt{d}}{2}\right) \\
&= \left(2, 1, \frac{1+\sqrt{d}}{2}, \frac{1-\sqrt{d}}{2}\right) \\
&= (1),
\end{aligned}$$

which contradicts the fact that $\mathfrak{P}\overline{\mathfrak{P}} = (p)$. We show this fact.

$$\begin{aligned}
\mathfrak{P}\overline{\mathfrak{P}} &= \left(2, \frac{1+\sqrt{d}}{2}\right)\left(2, \frac{1-\sqrt{d}}{2}\right) \\
&= \left(4, 1-\sqrt{d}, 1+\sqrt{d}, \frac{1-d}{4}\right) \\
&= \left(4, 2, 1-\sqrt{d}, 1+\sqrt{d}, \frac{1-d}{4}\right) \\
&= 2\left(2, 1, \frac{1-\sqrt{d}}{2}, \frac{1+\sqrt{d}}{2}, \frac{1-d}{8}\right) \\
&= 2(1) \\
&= (2).
\end{aligned}$$

So $\mathfrak{P}\overline{\mathfrak{P}} = (2)$ and $\mathfrak{P} \neq \overline{\mathfrak{P}}$. We now check when $\left(\frac{D}{2}\right) = 0$. Thus, $d \equiv 2, 3 \pmod 4$. Let $\pi = 1 + \sqrt{d}$ when $d \equiv 3 \pmod 4$ and $\pi = \sqrt{d}$ when $d \equiv 2 \pmod 4$. First, suppose $d \equiv 3 \pmod 4$. Then we define

$$\mathfrak{P} = (2, 1 + \sqrt{d}).$$

Observe that

$$\begin{aligned}
\mathfrak{P}^2 &= (2, 1+\sqrt{d})^2 \\
&= (4, 2(1+\sqrt{d}), 1 + d + 2\sqrt{d}).
\end{aligned}$$

Note that $d \equiv 3 \pmod 4$ means $d \equiv -1 \pmod 4$. Thus, $d + 1 \equiv 0 \pmod 4$. Thus $d + 1$ is even and

is therefore divisible by 2. So

$$\begin{aligned}(4, 2(1+\sqrt{d}), 1+d+2\sqrt{d}) &= 2\left(2, 1+\sqrt{d}, \frac{1+d}{2}+\sqrt{d}\right) \\ &= 2\left(2, \frac{1-d}{2}, 1+\sqrt{d}, \frac{1+d}{2}+2\sqrt{d}\right).\end{aligned}$$

We know that $d \equiv -1 \pmod 4$ and so $1-d \equiv 2 \pmod 4$. Therefore, $\frac{1-d}{2}$ is odd and $(2, \frac{1-d}{2}) = (1)$. Thus,

$$\mathfrak{P}^2 = 2\left(2, \frac{1-d}{2}, 1+\sqrt{d}, \frac{1+d}{2}+2\sqrt{d}\right) = 2(1) = (2).$$

Now suppose $d \equiv 2 \pmod 4$. Then

$$\begin{aligned}\mathfrak{P}^2 &= (2, \sqrt{d})^2 \\ &= (4, 2\sqrt{d}, d) \\ &= 2\left(2, \sqrt{d}, \frac{d}{2}\right) \\ &= 2(1) \\ &= (2),\end{aligned}$$

as $d \equiv 2 \pmod 4$, we have that $\frac{d}{2} \equiv 1 \pmod 2$. This concludes the proof as the only possibilities were for $\left(\frac{D}{p}\right) = -1, 0, 1$. As $\left(\frac{D}{p}\right) = 0, 1$ implies that p is not prime, we must have that $\left(\frac{D}{p}\right) = -1$ implies that p is prime. This concludes the proof. □

Therefore, this theorem gives us a practical way of checking the primality of an element. We utilize Theorem 1.1.35 with the following proposition to check the primal stability of an element.

Proposition 1.1.36. Let $\mathbb{Z} \subset \mathbb{Z}[n\omega] \subset \mathbb{Z}[\omega]$ be an extension of rings of integers and let $p \in \mathbb{Z}$ be prime in $\mathbb{Z}$ and $\mathbb{Z}[\omega]$. Then p is prime in $\mathbb{Z}[n\omega]$ if and only if $\gcd(n, p) = 1$.

Proof. Let p be prime in $\mathbb{Z}$ and $\mathbb{Z}[\omega]$. Suppose p is prime in $\mathbb{Z}[n\omega]$ and suppose, towards a contradiction, that $\gcd(n, p) \neq 1$. Then there is a $d \in \mathbb{Z}$ such that $d \mid n$ and $d \mid p$. As p is prime, we must have that $d = p$. Thus, $n = pk$ for some integer k. Consider the following element in $\mathbb{Z}[n\omega]$.

$$(n\omega)(n\overline{\omega}) = pk\omega(pk\overline{\omega}) = p^2k^2\omega\overline{\omega}.$$

Certainly $p \mid p^2k^2\omega\overline{\omega}$ but $p \nmid pk\omega = n\omega$ and $p \nmid pk\overline{\omega} = n\overline{\omega}$. So p cannot be prime in $\mathbb{Z}[n\omega]$, which contradicts the assumption that p is prime in all three rings. Thus, $\gcd(n, p) = 1$.

Conversely, suppose $p \in \mathbb{Z} \subset \mathbb{Z}[\omega]$ is prime in both $\mathbb{Z}$ and $\mathbb{Z}[\omega]$ and that $\gcd(p, n) = 1$. Suppose $p \mid (a+b(n\omega))(c+d(n\omega))$ in $\mathbb{Z}[n\omega]$. Since p is prime in $\mathbb{Z}[\omega]$, then without loss of generality, $p \mid (a + b(n\omega)) = (a + (bn)\omega)$. Therefore $p \mid a$ and $p \mid (nb)$. Since $\gcd(p, n) = 1$, we must have $p \mid b$. Thus, $p \mid (a + b(n\omega))$ in $\mathbb{Z}[n\omega]$. □

Theorem 1.1.35 and Proposition 1.1.36 actually fully characterize the prime stability of prime elements in the context of the integers and rings of integers. For example, if we examine the extensions

$$\mathbb{Z} \subset \mathbb{Z}[ni] \subset \mathbb{Z}[i]$$

we already saw that 3 is prime in $\mathbb{Z}$ and $\mathbb{Z}[i]$. Using Theorem 1.1.35 and Proposition 1.1.36, as $i = \sqrt{-1}$ we note that $-1 \equiv 3 \pmod 4$. Thus, the discriminant of $\mathbb{Z}[i]$ is $D = 4(-1) = -4$. Computing the Legendre symbol,

$$\left(\frac{D}{p}\right) = \left(\frac{-4}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1.$$

Thus, 3 remains prime in $\mathbb{Z}[i]$ by Theorem 1.1.35 and if $(n, 3) = 1$, then 3 is also prime in $\mathbb{Z}[ni]$ by Proposition 1.1.36.

As is the way of mathematics, we would like to take this idea of studying how the "primeness" of an element in extensions of the integers to orders and rings of integers and generalize to extensions of integral domains in general. We can formally cast our question of interest in the following way: Let R, S, T be integral domains such that $R \subset S \subset T$ and let $p \in R$ be prime in R and T. We want to know when p is also prime in S. Furthermore, we want to know when p is prime in S for all possible S and when p is not prime in all possible S.

1.2 The Question at Hand

Let $R \subset T$ be integral domains such that $p \in R \subset T$ is prime in both R and T. Let S be an intermediate extension, that is, let $R \subset S \subset T$. We desire to know when p will be prime in S. Furthermore, we also desire to know when p will be prime in all possible intermediate extensions. If

p remains prime in S then we say that p has the property of **prime stability**. In Section 1.1, we saw an in-depth example of prime stability and prime instability depending on what intermediate extension we considered. In Section 3, we present justification for conjectures pertaining to prime stability in intermediate ring extensions, but we briefly introduce the conjectures now.

Definition 1.2.1. Let $R \subseteq T$ be rings. R and T are **adjacent** if there is a ring S such that $R \subseteq S \subseteq T$ then $S = R$ or $S = T$.

Conjecture 1.2.2. Let $R \subset T$ be a proper integral extension of domains such that R and T are not adjacent and let $p \in R$ be prime in both R and T. Then there is a proper intermediate extension S with $R \subsetneq S \subsetneq T$ such that p is prime in S.

Conjecture 1.2.2 is about the mere existence of such an intermediate extension. The assumption that R and T are not adjacent guarantees that there is indeed a ring S such that $R \subset S \subset T$. In the examples that follow in chapter 3, we will see that often as not, this intermediate extension is of the form $S = R[t]$, where $t \in T \setminus pT$.

Conjecture 1.2.3. Let $R \subsetneq S \subsetneq T$ be proper integral extensions of domains and let $p \in R$ be prime in R and T. Suppose that p is not prime in S. Then there exists an S' and injective homomorphisms $\phi : S \to S'$ and $\psi : S' \to T$ such that $\phi(p)$ is prime in S' and $\psi(\phi(p)) = p$. This property may be represented by the following diagram where $\iota_R : R \to S$ is the canonical injection on R and $\iota_S : S \to T$ is the canonical injection on S.

$$\begin{array}{ccccc} R & \xhookrightarrow{\iota_R} & S & \xhookrightarrow{\iota_S} & T \\ & & \downarrow{\scriptstyle \phi} & \nearrow{\scriptstyle \psi} & \\ & & S' & & \end{array}$$

We can think of this conjecture as a sort of "prime washing machine." If given an intermediate extension S where p is not prime we would like to say that all hope is not lost. We can pass S into another integral domain S' that "makes" p prime that will then return p to T, still being prime.

Before presenting the last conjecture, we consider a definition.

Definition 1.2.4. An integral domain T is an *overring* of R if T is a subring of the quotient field of R.

Conjecture 1.2.5. Suppose T is an integral overring of R and $\dim(R) = \dim(T) = 1$. Then if p is prime in R and T then p is prime in S for all $R \subseteq S \subseteq T$.

This would be one of the larger results in this study of prime stability. It appears an obstruction to prime stability occurs when the Krull dimension is greater than one. That is, a number of counterexamples have seemed to depend on the existence of nonzero prime $P \subsetneq Q$ in our domains. To clarify this concept of dimension, we define the Krull dimension of a ring.

Definition 1.2.6. Let R be an integral domain. The **Krull dimension** of R is defined by

$$\dim(R) = \sup\{n \mid P_0 \subsetneq P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_n \subsetneq R, P_i \text{ prime ideal of } R\}$$

In other words, the dimension of R is the supremum of the lengths all possible chains of prime ideals in R.

Thus, the dimension of R is the supremum of all the possible lengths of chains of prime ideals contained in R. So if $\dim(R) = \dim(T) = 1$, then we can only stack the prime ideals two high. (If P is a nonzero prime ideal of an integral domain R, the longest chain possible is $(0) \subsetneq P$.) This seems to be small enough that the primality of p is forced to be preserved irrespective of what intermediate extension we may be considering.

With all of this, we may proceed to consider all necessary preliminary information before working through explicit examples which support the above conjectures.

Chapter 2

Preliminaries

2.1 Definitions

In order to properly frame our discussion about prime stability, we consider integral extensions of integral domains $R \subset S \subset T$ and an element $p \in R$ such that p is prime in both R and T. Recall our definitions of irreducible and prime elements as well as overrings. We examine briefly some examples of irreducibles, primes, and overrings.

Example 2.1.1. Note that $x + 1 \in \mathbb{Z}[x]$ is irreducible. To see this, suppose $x + 1 = f(x)g(x)$ for some $f(x), g(x) \in \mathbb{Z}[x]$. Since the degree of $x + 1$ is 1, we must have that $\deg(f(x)) + \deg(g(x)) = 1$ so either $\deg(f(x)) = 0$ and $\deg(g(x)) = 1$, or vice versa. Without loss of generality, suppose $\deg(f(x)) = 0$. Then $f(x)$ is a constant, say $r \in \mathbb{Z}$. So $x + 1 = rg(x)$. Thus, $r \mid (x + 1)$ and so r must divide the coefficients, namely 1. Thus, $r = \pm 1$ which means that $f(x) = r = \pm 1$ is a unit. Thus, $x + 1$ must be irreducible.

Example 2.1.2. We show that x is prime. To that end, let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m, g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n \in \mathbb{Z}[x]$ such that $x \mid f(x)g(x)$. So the constant term here is a_0b_0 and every other term has at least 1 power of x in it. Thus, as $x \mid f(x)g(x)$ and x divides every other term, then $x \mid a_0b_0$. But a_0, b_0 are constants and so $a_0b_0 = 0$. As $\mathbb{Z}$ is an integral domain, $a_0 = 0$ or $b_0 = 0$. Without loss of generality, $a_0 = 0$. Then $f(x) = a_1x + a_2x^2 + \cdots + a_mx^m = x(a_1 + a_2x + \cdots + a_mx^{m-1})$. Thus, $x \mid f(x)$. Ergo, x is prime.

Example 2.1.3. Finally, we consider the set $S = \mathbb{Z} \setminus 2\mathbb{Z}$. That is, S is the set of odd integers

without zero. Then $\mathbb{Z}_S = \{\frac{a}{b} \mid a \in \mathbb{Z}, b \in S\}$ is an overring of $\mathbb{Z}$ as $\mathbb{Z} \subseteq \mathbb{Z}_S$ and $\mathbb{Z}_S$ is a subring of the quotient field of $\mathbb{Z}$, namely $\mathbb{Q}$.

We now recall the definition of integrality and integral extensions, which leads us to the following lemma and theorem.

Lemma 2.1.4. If $R \subseteq T$ is an integral extension of domains then $U(T) \cap R = U(R)$, where $U(T)$ is the set of units of T and $U(R)$ is the set of units for R.

Theorem 2.1.5. Let $R \subseteq S \subseteq T$ be integral extensions of integral domains and $\pi \in T$ an irreducible element such that $\pi \in R$. Then π is irreducible in S.

Proof. Let $R \subseteq S \subseteq T$ be as above and let $\pi \in R$ be irreducible in T. Indeed, since π is irreducible in T and $\pi \in R$ then π must be irreducible in R (otherwise, $\pi = ab$ for nonunits $a, b \in R$ then $\pi = ab$ in T, a contradiction). Suppose that π is not irreducible in S. So $\pi = xy$ for nonunits $x, y \in S$. But $S \subseteq T$ so $\pi = xy$ in T. But π is irreducible in T. This is a contradiction so π is irreducible in S. $\square$

(Alternatively, if $\pi = xy$ for $x, y \in S$ then as $S \subseteq T$, without loss of generality, $x \in U(T)$. But the extension is integral so $x \in U(S)$. Thus, π is irreducible.)

The above lemma gives us a framework with which to consider our question. This lemma characterizes the irreducibile stability property of irreducible elements through integral extensions. As we saw briefly in the introduction and will see in the following chapter, things tend to get a bit more sticky when we start investigating prime stability. All in all, this is not terribly surprising. In general, primality is a stronger condition that irreducible.

2.2 Previous Results

2.2.1 Same prime ideals: Anderson & Dobbs

In [1], Anderson and Dobbs ask a question related our path of inquiry; they inqure when two commutative rings $R \subset T$ have the same *prime ideals*. In particular, they study necessary and sufficient conditions for two rings to have $\mathrm{Spec}(R) = \mathrm{Spec}(T)$ (note that $\mathrm{Spec}(R)$ is the set of prime ideals of a ring R). Their primary result is Theorem 3.10 where equivalent conditions are given for $\mathrm{Spec}(R) = \mathrm{Spec}(T)$. Interestingly, if $\mathrm{Spec}(R) = \mathrm{Spec}(T)$ then R and T have the same maximal ideals as well, i.e., $\mathrm{Max}(R) = \mathrm{Max}(T)$. Furthermore, R and T have the same radical ideals (recall

that a radical ideal $I \subset R$ is an ideal such that if $a^n \in I$ then $a \in I$ for some $n \in \mathbb{N}$) and if $R \neq T$ then R must be quasilocal (R has a unique maximal ideal). From here, they prove a one-to-one correspondence that guarantees the existence of an extension T with $R \subset T$ for any domain R such that $\text{Spec}(R) = \text{Spec}(T)$ (Theorem 3.25) and Corollary 3.26 provides a necessary and sufficient condition for intermediate extensions. They show that for $R \subset S \subset T$, with $\text{Spec}(R) = \text{Spec}(T)$, $\text{Spec}(S) = \text{Spec}(R)$ if and only if $R/M \subset T/M$ is algebraic, for M the unique maximal ideal of R (remember that R is quasilocal by Theorem 3.10, so this M does indeed exist).

Ultimately, though, this condition of $\text{Spec}(R) = \text{Spec}(T)$ is a quite strong condition and considering Theorem 3.10, makes R and T fairly close to actually just being the same ring. We would like to weaken this requirement and focus primarily on individual prime elements instead of the entire set of prime ideals. It is interesting to note that Anderson and Dobbs comment that the requirement $\text{Spec}(R) = \text{Spec}(T)$ fails in domains that contain a nonzero principal prime. If we consider an individual prime element $p \in R \subset T$, we necessarily have a principal prime and so [1] does not address the behavior of this prime through intermediate extensions.

2.2.2 Same prime ideals, II: Anderson & Dobbs

In [2], Anderson and Dobbs generalize the results from their first paper in [1]. The most noticeable difference is that in [1], they assumed that the two rings R, T with the same prime ideals were comparable. In other words, $R \subset T$. But now in [2], they do not assume that R and T are comparable. Interestingly, many of the results from [1] carry over to the case of incomparable R and T. Interestingly, for R a quasilocal domain and K its quotient field, the set of all subrings $S \subseteq K$ such that $\text{Spec}(R) = \text{Spec}(S)$ forms a complete semilattice. Anderson and Dobbs define a semilattice as a partially ordered set where every nonempty subset has an infimum.

2.2.3 Expanding Prime Ideals: Malcolmson & Okoh

In [10], Malcolmson and Okoh study finitely generated extensions of integral domains $R \subset T$. In particular, they observe the behavior of the set of primes in R that become units in T and are primarily concerned with the finiteness of this set. In order to do this, they introduce two characterizations for domains: GD(1) and GD(2) domains. A GD(1) domain is an integral domain where every nonzero element of R is contained in only finitely many *principal* prime ideals. A GD(2)

domain, on the other hand, is an integral domain where every nonzero element of R is contained in only finitely many prime ideals. They find that the finiteness of the set of primes which become units is deeply connected to GD(1) domains and that GD(1) domains behave similarly to UFDs. This is a related question to ours, but of course the apparent difference is that Malcolmson and Okoh are concerned with how primes *change*. In other words, they are interested in factorizations of primes through a finitely generated extension of an integral domain. Our endeavor in this paper, though, focuses on understanding how a prime may remain prime through integral extensions. Nonetheless, it is interesting to note how much more complicated the case of primes in integral extensions are compared to irreducibles in integral extensions.

2.2.4 Counting Intermediate Rings: Dobbs, Picavet, & Picavet-L'Hermitte

In [6], Dobbs, Picavet, and Picavet-L'Hermitte count intermediate ring extensions in special cases. In particular, they observe ring extensions with Dedekind domains. They prove various results asserting the existence of more than one intermediate extension as well as when there is only one intermediate extension. Again, this is not quite what we are investigating in this thesis. However, the results from this paper may prove to be useful. After all, as we are interested in primes in intermediate extensions, it ostensibly would be useful to know many intermediate extensions we should be worried about.

2.2.5 Ring Extensions that satisfy special properties: Dobbs, Picavet, & Picavet-L'Hermitte

In [5], Dobbs, Picavet, and Picavet-L'Hermitte study ring extensions that satisfy two properties: the finitely many intermediate algebras property (FIP) and the finite chain property (FCP). Recall that an R-algebra is an abelian group A such that A is a module over R and A has "vector multiplication". So for a ring extension $R \subseteq T$, if the set of all R-subalgebras of T is finite then $R \subseteq T$ satisfies FIP. Note that the set of all R-subalgebras of T are essentially the rings S such that $R \subseteq S \subseteq T$. Perhaps more straightforwardly, an extension $R \subseteq T$ satisfies FCP if every chain of R-subalgebras has finite length, ordered under inclusion. Indeed, it should be clear to see that FIP implies FCP, but it can be shown that the converse is false. Dobbs, Picavet, and Picavet-L'Hermitte state that their primary result shows that an extension $R \subseteq T$ is FIP if and only if $R \subseteq \overline{R}$ and

$\overline{R} \subseteq T$ are both FIP, where $\overline{R}$ is the integral closure of R in T. (Similarly for FCP.) This means that their work could be reduced to simply studying integral or integrally closed extensions. They give another necessary and sufficient condition for an extension $F \subseteq T$ having FIP (and therefore FCP): $F \subseteq T$ has FIP (or FCP) if and only if there is a finite maximal chain of rings from R to T.

As for our purposes, this paper speaks to the significance of integral closures and therefore integral extensions. We hope to be able to find analogous results for the case of prime stability.

Chapter 3

Examples of Interest

We consider some examples exhibiting some behavior expressed in Conjectures 1.2.2 and 1.2.5. As for Conjecture 1.2.3, it is more of a follow-up question resulting from examples which exhibit Conjecture 1.2.2.

3.1 An Example with the Same Quotient Field

Example 3.1.1. We begin by considering an example where prime stability fails:

$$\mathbb{Z}[x] \subseteq \mathbb{Z} + x\mathbb{Q}[x] \subseteq \mathbb{Q}[x].$$

Here, we already showed that x is prime in $\mathbb{Z}[x]$ in Example 2.1.2. We actually have an analogous proof for x being prime in $\mathbb{Q}[x]$ and thus x is prime in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$. However, x is not prime in $\mathbb{Z} + x\mathbb{Q}[x]$. Observe that $x \mid x^2$ but $x \nmid (\frac{2}{3}x)$ nor $x \nmid (\frac{3}{2}x)$ as $\frac{2}{3}, \frac{3}{2} \notin \mathbb{Z} + x\mathbb{Q}[x]$.

We note that both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ have the same quotient field, $\mathbb{Q}(x)$. Furthermore, the Krull dimensions of $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ are different: $\dim(\mathbb{Z}[x]) = 2$ while $\dim(\mathbb{Q}[x]) = 1$.

3.2 An Example with Different Quotient Fields

Example 3.2.1. Consider the following field extensions:

$$\mathbb{Z} \subseteq \mathbb{Z}[ni] \subseteq \mathbb{Z}[i].$$

We worked through this example already and found that if $\gcd(n,3) = 1$, then 3 remains prime in the intermediate extension. Note that $\mathbb{Z}$ and $\mathbb{Z}[i]$ have different quotient fields. Namely, the quotient field of $\mathbb{Z}$ is of course $\mathbb{Q}$. On the other hand, the quotient field of $\mathbb{Z}[i]$ is $\mathbb{Q}(i)$. Furthermore, as $\mathbb{Z}[i]$ is an integral extension of $\mathbb{Z}$ ($\mathbb{Z}[i]$ is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(i)$), then as $\dim(\mathbb{Z}) = 1$ then $\dim(\mathbb{Z}[i]) = 1$. So we have a non-example of Conjecture 1.2.5 and an example of Conjecture 1.2.2.

Example 3.2.2. Consider the ring extensions

$$\mathbb{Z} \subseteq \mathbb{Z}[n\sqrt{-14}] \subseteq \mathbb{Z}[\sqrt{-14}].$$

and consider $p = 29$. Using similar norm arguments as in the previous example, we can determine that 29 remains irreducible in each extension. However, these are not UFDs. We thus utilize Theorem 1.1.35 and Proposition 1.1.36 to assert that 29 is prime in $\mathbb{Z}[\sqrt{-14}]$. Note that $-14 \equiv 2 \pmod 4$ and so $D = 4(-14) = -56$. Thus,

$$\left(\frac{-56}{29}\right) = \left(\frac{2}{29}\right) = -1.$$

So 29 remains prime in $\mathbb{Z}[\sqrt{-14}]$ and is therefore prime in $\mathbb{Z}[n\sqrt{-14}]$ for $(n, 29) = 1$.

Note that $\dim(\mathbb{Z}) = 1$. But $\mathbb{Z}[\sqrt{-14}]$ is an integral extension of $\mathbb{Z}$ (after all, $\mathbb{Z}[\sqrt{-14}]$ is the integral closure of $\mathbb{Z}$ in a field extension of $\mathbb{Q}$), and it can be shown that integral extensions of a ring have the same dimension as the ring. So $\dim(\mathbb{Z}[\sqrt{-14}]) = 1$. But $\mathbb{Z}$ and $\mathbb{Z}[\sqrt{-14}]$ have different quotient fields. The quotient field of $\mathbb{Z}$ is $\mathbb{Q}$ and the quotient field of $\mathbb{Z}[\sqrt{-14}]$ is $\mathbb{Q}(\sqrt{-14})$. Once again, since $\mathbb{Z}$ and $\mathbb{Z}[\sqrt{-14}]$ have different quotient fields and 29 does not remain prime in every intermediate extension, this is a non-example of Conjecture 1.2.5 but an example of Conjecture 1.2.2.

3.3 Ring of Algebraic Integers: Prime in All Possible Intermediate Extensions

Example 3.3.1. Consider the extensions

$$\mathbb{Z}[2^m i] \subseteq S \subseteq \mathbb{Z}[i].$$

We have done a couple of examples with Gaussian integers already, and so we know that 3 is prime in $\mathbb{Z}[i]$. As 2^m is relatively prime to 3, for any $m \geq 0$, we know that 3 is also prime in $\mathbb{Z}[2^m i]$. We proceed to consider what S could be. We claim that S will always be of the form

$$S = \mathbb{Z}[2^n i]$$

for $0 \leq n \leq m$. After all, in each case, we can write $2^m i = 2^{m-n} \cdot 2^n i \in \mathbb{Z}[2^n i]$. Evidently, 2^n is always relatively prime to 3. So for all $0 \leq n \leq m$, we have that 3 is prime in $\mathbb{Z}[2^n i]$ and is therefore prime for all possible intermediate extensions. We also note that the dimension of $\mathbb{Z}[2^m i]$ and $\mathbb{Z}[i]$ are both 1, and they have the same quotient field, namely $\mathbb{Q}(i)$. So this is an explicit example of Conjecture 1.2.5.

3.4 Polynomial Rings

Example 3.4.1. As an example in support of Conjecture 1.2.2, consider the extensions

$$\mathbb{F}[x, y^4, y^5, z^4, z^5] \subseteq \mathbb{F}[x, y^4, y^5, z^4, z^5, xy] \subseteq \mathbb{F}[x, y, z],$$

for $\mathbb{F}$ a field. We see that x is of course prime in the "bookends", but $x \mid xy^5$ yet in $\mathbb{F}[x, y^4, y^5, z^4, z^5, xy], xy^5 = (xy)(y^4)$ and x does not divide xy nor y^4. So x cannot be prime in the intermediate extension. However, if we change the intermediate extension to

$$\mathbb{F}[x, y^4, y^5, z^4, z^5] \subseteq \mathbb{F}[x, y, z^4, z^5] \subseteq \mathbb{F}[x, y, z]$$

we will find that x is indeed prime in the intermediate extension.

To that end, recall that R is an integral domain if and only if $R[x]$ is an integral domain. Naturally, as $\mathbb{F}$ is a field, it is an integral domain. Therefore, $\mathbb{F}[x, y, z^4, z^5]$ is an integral domain. Furthermore, recall that the ideal (0) is prime in an integral domain R. After all, if for two ideals $A, B \subseteq R$, we have that $AB \in (0)$, that means that for all $ab \in AB$, $ab \in (0)$. So $ab = 0$. But R is an integral domain, so $a = 0$ or $b = 0$. Thus, either $A \subseteq (0)$ or $B \subseteq (0)$. We can use these two facts to show x is prime in the following way: construct a ring homomorphism ϕ such that $(x) = \ker(\phi)$ and apply the following theorem.

Theorem 3.4.2. Let R be an integral domain and $P \subseteq R$ an ideal. P is prime if and only if R/P is an integral domain.

We proceed to show that $(x) = \ker(\phi)$ for some ring homomorphism ϕ. To that end, consider $\phi : \mathbb{F}[x, y, z^4, z^5] \to \mathbb{F}[y, z^4, z^5]$ given by

$$\phi(a) = a, a \in \mathbb{F} \qquad \phi(x) = 0$$

$$\phi(y) = y \qquad \phi(z^4) = z^4$$

$$\phi(z^5) = z^5$$

It is clear that $(x) \subseteq \ker(\phi)$. Thus it suffices to show that $\ker(\phi) \subseteq (x)$. To proceed, we make the following observation. We see that $\mathbb{F}[x, y, z^4, z^5] = \mathbb{F}[y, z^4, z^5][x]$. In other words, elements in $\mathbb{F}[x, y, z^4, z^5]$ can be though as polynomials in x with coefficients in $\mathbb{F}[y, z^4, z^5]$.

Now let $f \in \ker(\phi)$. Thus, f is of the form

$$f = \alpha_0(y, z^4, z^5) + \alpha_1(y, z^4, z^5)x + \cdots + \alpha_n(y, z^4, z^5)x^n,$$

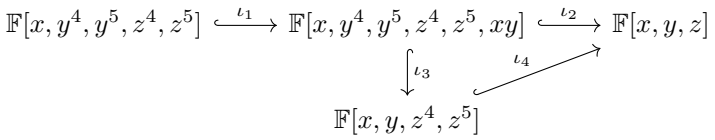
where $\alpha_i(y, z^4, z^5) \in \mathbb{F}[y, z^4, z^5]$. Applying ϕ to f,

$$\begin{aligned}
\phi(f) &= \phi(\alpha_0(y, z^4, z^5)) + \alpha_1(y, z^4, z^5)x + \cdots + \alpha_n(y, z^4, z^5)x^n \\
&= \phi(\alpha_0(y, z^4, z^5)) + \phi(\alpha_1(y, z^4, z^5))\phi(x) + \cdots + \phi(\alpha_n(y, z^4, z^5))\phi(x^n) \\
&= \phi(\alpha_0(y, z^4, z^5)) \\
&= 0.
\end{aligned}$$

This implies $\alpha_0(y, z^4, z^5) = 0$. So $f \in (x)$. Therefore, $\ker(\phi) = (x)$. Note that $\mathbb{F}[x, y, z^4, z^5]/(x) \cong \mathbb{F}[y, z^4, z^5]$, which is an integral domain. After all $\mathbb{F}[z^4, z^5]$ is a subring of $\mathbb{F}[z]$, which is an integral domain. Therefore, $\mathbb{F}[z^4, z^5]$ is an integral domain and therefore $\mathbb{F}[z^4, z^5][y] = \mathbb{F}[y, z^4, z^5]$ is also an integral domain. Indeed because $\mathbb{F}[x, y, z^4, z^5]/(x) \cong \mathbb{F}[y, z^4, z^5]$, then $\mathbb{F}[x, y, z^4, z^5]/(x)$ is also an integral domain. Ergo, we conclude that (x) is a prime ideal and therefore x itself is prime in $\mathbb{F}[y, z^4, z^5]$.

We also briefly note that this is a trivial example of Conjecture 1.2.3. We consider the

following diagram.



We let $\iota_i, 1 \leq i \leq 4$ be the canonical injections. Indeed, we saw that x is not prime in $\mathbb{F}[x, y^4, y^5, z^4, z^5, xy]$ but $\iota_3(x) = x$ is prime in $\mathbb{F}[x, y, z^4, z^5]$ and $\iota_4(\iota_3(x)) = \iota_4(x) = x$ is prime in $\mathbb{F}[x, y, z]$.

Chapter 4

Conclusion

Moving forward, we of course intend on evaluating the validity of our conjectures. It appears that Conjectures 1.2.2 and 1.2.5 are the most likely to be true. Working through examples such as we have covered do a tremendous amount in illuminating interesting behavior as well as provide frameworks for proofs. We saw in the introduction the development of some machinery from number theory for us to fully characterize the primal stability of quadratic rings of integers. It would be interesting to see this result extended to other types of rings of integers in a continued effort to get a handle on the depth of this problem. In Conjecture 1.2.3 we could have a unique result and it may be productive to try some other machinery to potentially prove this conjecture. Irrespective of the validity of the conjectures, some rich mathematics underlie our question of how primality is affected as we step up into extensions of integral domains. Even remaining in of rings of integers, or generalizing to integral or almost integral extensions, there are some interesting paths to take. For example, given a particular order in a quadratic extension of rings of integers, what is the behavior of primes and irreducibles, specifically how many primes remain prime? Primes have been the central focus of number theory and algebra for centuries and we hope to be able to contribute some more interesting results to shed light on a seemingly endless field of study.

Bibliography

[1] D. Anderson and D. Dobbs. Pairs of rings with the same prime ideals. *Canadian Journal of Mathematics*, Vol. XXXII, 1980.

[2] D. Anderson and D. Dobbs. Pairs of rings with the same prime ideals, ii. *Canadian Journal of Mathematics*, Vol. XL, 1988.

[3] H. Cohn. *Advanced Number Theory.* Dover Publications, Inc., 1980.

[4] James Coykendall. Theory of factorization, 2020.

[5] D. Dobbs, G. Picavet, and M. Picavet-L'Hermitte. Characterizing the ring extensions that satisfy fip or fcp. *Journal of Algebra*, 2012.

[6] D. Dobbs, G. Picavet, and M. Picavet-L'Hermitte. On the number of intermediate rings when a decomposed extension lies atop a ramified extension. *Palestine Journal of Mathematics*, 2018.

[7] R.C. Heitmann and L.S. Levy. 1 1/2 and 2 generator ideals in prufer domains. *The Rocky Mountain Journal of Mathematics*, Vol. 5, No. 3, 1975.

[8] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory.* Springer, 1990.

[9] I. Kaplansky. *Commutative Rings.* Allyn and Bacon, Inc., 1970.

[10] P. Malcolmson and F. Okoh. Exapnsions of prime ideals. *Rocky Mountain Journal of Mathematics*, 2005.