RAMIFICATION AND INFINITE EXTENSIONS OF DEDEKIND DOMAINS

A Dissertation
Submitted to the Graduate Faculty
of the
North Dakota State University
of Agriculture and Applied Science

By

Carl Stanley Hashbarger

In Partial Fulfillment of the Requirements
for the Degree of
DOCTOR OF PHILOSOPHY

Major Department:
Mathematics

April 2010

Fargo, North Dakota

North Dakota State University
Graduate School

Title

RAMIFICATION AND INFINITE EXTENSIONS OF DEDEKIND DOMAINS

By

CARL HASHBARGER

The Supervisory Committee certifies that this ***disquisition*** complies with North Dakota State University's regulations and meets the accepted standards for the degree of

DOCTOR OF PHILOSOPHY

ABSTRACT

Hashbarger, Carl Stanley, Ph.D., Department of Mathematics, College of Science and Mathematics, North Dakota State University, April 2010. Ramification and Infinite Extensions of Dedekind Domains. Major Professor: Dr. James Coykendall.

This dissertation presents methods for determining the behavior of prime ideals in an integral extension of a Dedekind domain. One tool used to determine this behavior is an algorithm that computes which prime ideals ramify in a finite separable extension. Other results about factorization of prime ideals are improved and applied to finite extensions. By considering a set of finite extensions whose union is an infinite extension, it is possible to predict ideal factorization in the infinite extension as well. Among other things, this ideal factorization determines whether a given infinite extension is almost Dedekind. These methods and results yield some interesting facts when they are demonstrated on a pair of classical rings of algebraic number theory.

ACKNOWLEDGMENTS

The one person without whom this project would not exist is my advisor, Dr. Jim Coykendall. I would like to thank Dr. Coykendall for his untiring and unending advice, help, and support. He was always willing to lend his seemingly infinite supply of energy and savvy to this project, even after business hours or on holidays. I am very grateful that I found an advisor that gives so much to his students.

I would also like to thank Chris Spicer for finding the mistakes in my *LaTeX* code and having the patience to assist me in fixing them.

TABLE OF CONTENTS

ABSTRACT iii

ACKNOWLEDGMENTS iv

1. CHAPTER 1. BACKGROUND 1

   1.1. Dedekind Domains 1

   1.2. Almost Dedekind Domains 16

   1.3. The Discriminant 17

   1.4. Extensions of Dedekind Domains 21

2. CHAPTER 2. IDEAL FACTORIZATION VIA POLYNOMIALS 27

   2.1. An Ideal Factorization Theorem 27

   2.2. The Condition $\mathfrak{p}R + \mathfrak{C} = R$ 37

3. CHAPTER 3. RAMIFIED PRIMES AND THE DERIVATIVE 41

   3.1. The Ramified Prime Theorem 41

   3.2. The Ramified Prime Algorithm 41

4. CHAPTER 4. INFINITE EXTENSIONS OF $\mathbb{Z}$ 45

   4.1. The integral closure of $\mathbb{Z}$ in $\mathbb{Q}\left(\sqrt{d}, \sqrt[3]{d}, \sqrt[4]{d}, \ldots, \sqrt[N]{d}, \ldots\right)$ 45

   4.2. The integral closure of $\mathbb{Z}$ in $\mathbb{Q}\left(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \ldots, \sqrt{p_N}, \ldots\right)$ 52

REFERENCES 67

APPENDIX A. MATHEMATICA RAMIFIED PRIME ALGORITHM ... 68

CHAPTER 1. BACKGROUND

Much of this paper is dedicated to ideal factorization methods and applications. The basics of ideal factorization arise in the Fundamental Theorem of Arithmetic, which states that every integer can be factored uniquely into a product of prime integers. Of course, if every element in a ring can be factored uniquely into prime elements, then every ideal of that ring can be factored uniquely into prime ideals. The converse is not true in general. This lends itself to a sensible generalization of the Fundamental Theorem of Arithmetic, the ability to factor any ideal (uniquely) of a given ring into a product of prime ideals. We begin by introducing a class of rings called Dedekind domains that are defined by this property.

1.1. Dedekind Domains

Dedekind domains have many equivalent definitions in the literature; we will shortly state a list of equivalent characterizations that was adapted from [2]. The definition that is most important in the context of this paper, however, is the following:

Definition 1.1.1. *An integral domain is a Dedekind domain if every proper ideal factors (uniquely) into a finite product of prime ideals.*

In the context of this definition, a Dedekind domain is the ideal analogue of a unique factorization domain. We will primarily be looking at interesting ways to predict ideal factorizations in extensions of Dedekind domains. As we will see in Theorem 1.4.9, there are large classes of extensions of Dedekind domains that are Dedekind. Ideals of any such extension would once again factor uniquely into products of prime ideals. There will be many instances, therefore, in which we will take advantage of the rich structure of Dedekind domains, in part the aforementioned list of alternate characterizations. We will set the stage by looking at integral extensions and fractional ideals.

Definition 1.1.2. *Let S be a ring and let R be a subring of S. An element $s \in S$ is said to be integral over R if there exists a monic polynomial $f(x)$ with coefficients in R such that $f(s) = 0$. The extension S is said to be integral if every element of S is integral over R.*

Integral extensions of Dedekind domains have many useful properties that will be discussed in the course of this paper. The following lemma shows that an extension of a ring by a single integral element is a finitely generated.

Lemma 1.1.3. *Let S be a ring and let R be a subring of S. Let $s \in S$ such that s is integral over R. Then $R[s]$ is a finitely generated R-module.*

Proof. Since s is integral over R, there exists a monic polynomial f over R of degree n such that $f(s) = 0$. We show $R[s] \subseteq R+sR+s^2R+\cdots+s^{n-1}R$. Let $t \in R[s]$. Let m be the least integer such that t has a representation $t = r_0+r_1s+r_2s^2+\cdots+r_ms^m$ where each $r_i \in R$ and $r_m \neq 0$. Assume $m \geq n$, say $m = n + k$ where k is a nonnegative integer. Notice that $f(s) = 0$ implies $s^m - s^k f(s) = s^m$ where $s^m - s^k f(s)$ is a polynomial of degree less than m. Therefore, $t = r_0+r_1s+r_2s^2+\cdots+r_m(s^m-s^k f(s))$ is a representation of t where the highest power of s is $m-1$, contradicting our choice of m. So $m < n$ and $R[s] \subseteq R + sR + s^2R + \cdots + s^{n-1}R$, as desired.

□

It is fairly straightforward that an extension adjoining finitely many integral elements will also be finitely generated. The following lemma is essentially a converse of the previous lemma.

Lemma 1.1.4. *Let S be an integral domain and let R be a subring of S. If S is finitely generated as an R-module, then every element of S is integral over R.*

Proof. Let $s \in S$. We need to show that s is the root of a monic polynomial with

coefficients in R. Let $\{s_1, s_2, \ldots, s_n\}$ be a set of generators for S over R. Then $ss_i \in S$ for each i so we have

$$ss_i = r_{i1}s_1 + r_{i2}s_2 + \cdots + r_{in}s_n$$

Also, we can subtract ss_i, which results in the homogeneous equations

$$0 = r_{i1}s_1 + r_{i2}s_2 + \cdots + (r_{ii} - s)s_i + r_{i,i+1}s_{i+1} + \cdots + r_{in}s_n$$

Let M be the matrix with entries r_{ij} if $i \neq j$ and $r_{ij} - s$ if $i = j$. Let M_i be the matrix formed by replacing column i of M with the zero vector. Cramer's rule states that if $\det(M) \neq 0$, then $s_i = \frac{\det(M_i)}{\det(M)} = 0$ for each i, but this is a contradiction because $S \neq 0$. So $\det(M) = 0$. Let N be the matrix with entries r_{ij} if $i \neq j$ and $r_{ij} - x$ if $i = j$. Then $f(x) = \det(N)$ is a polynomial with leading coefficient either 1 or -1. Let c be the leading coefficient of $f(x)$. Then $cf(x)$ is a monic polynomial with coefficients in R and we have

$$cf(s) = c\det(M) = 0$$

This shows that s is integral over R, as desired.

□

Let R be a ring. A common way to build integral extensions of R is to choose a ring S that contains R as a subring, then consider the set of all elements of S that are integral over R.

Definition 1.1.5. *Let S be a ring and let R be a subring of S. The integral closure of R in S is the set of all elements of S that are integral over R. If R contains all of the elements of S that are integral over R, we say R is integrally closed in S. In*

the special case where R is an integral domain, Q is the quotient field of R, and R is integrally closed in Q, we say that R is integrally closed.

Any integral extension generated in this way is integrally closed, as the next theorem shows.

Theorem 1.1.6. *Let S be a ring and let R be a subring of S. Let T be the integral closure of R in S. Then T is integrally closed in S.*

Proof. Let $s \in S$ be integral over T. Then there exist elements $t_0, t_1, \ldots, t_{n-1}$ of T such that $s^n + t_{n-1}s^{n-1} + t_{n-2}s^{n-2} + \cdots + t_1 s + t_0 = 0$. Because t_0 is integral over R, $R[t_0]$ is finitely generated over R by Lemma 1.1.3. Similarly, for each i such that $0 \leq i \leq n-1$, t_i is integral over $R[t_0, t_1, \ldots, t_{i-1}]$, so $R[t_0, t_1, \ldots, t_i]$ is finitely generated over $R[t_0, t_1, \ldots, t_{i-1}]$. We have already seen that s is integral over any ring that contains $t_0, t_1, \ldots, t_{n-1}$. In particular s is integral over $R[t_0, t_1, \ldots, t_{n-1}]$. Once again, we invoke Lemma 1.1.3 which shows that $R[t_0, t_1, \ldots, t_{n-1}, s]$ is finitely generated over $R[t_0, t_1, \ldots, t_{n-1}]$. Since there are finitely many finitely generated extensions between R and $R[t_0, t_1, \ldots, t_{n-1}, s]$, $R[t_0, t_1, \ldots, t_{n-1}, s]$ is finitely generated over R. Hence by Lemma 1.1.4, s is integral over R. This shows that $s \in T$, as desired.

□

Let D be an integral domain with quotient field Q. Then D is a subring of any extension field K of Q as well as Q itself. Therefore, it makes sense to discuss the integral closure of D in K, call it R. If K is a finite separable extension of Q, then there is an element $\gamma \in K$ such that $Q(\gamma) = K$. See [2] for details. Such an extension can often be associated to a polynomial that has γ as one of its roots, as in the following definition.

Definition 1.1.7. *The polynomial $f(x)$ is said to be a minimal polynomial for K over Q if $f(x)$ is irreducible as an element of $Q[x]$ and $K \cong Q[x]/f(x) \cong Q(\gamma)$.*

One characterization of Dedekind domains involves a special class of module called the fractional ideals.

Definition 1.1.8. *Let D be an integral domain with quotient field Q. A fractional ideal of D is a nonzero D-submodule I of Q such that $aI \subseteq D$ for some nonzero $a \in D$.*

Definition 1.1.9. *Let D be an integral domain. Let I be a fractional ideal of D. Then I is said to be invertible if there exists a fractional ideal J such that $IJ = R$. In this case, we call J the inverse of I.*

It is straightforward that the inverse of a fractional ideal is unique. Notice that the ideal $I^{-1} := \{a \in Q \mid aI \subseteq D\}$. Is a fractional ideal of D. If I is invertible, then I^{-1} is the inverse of I. For another example of an invertible fractional ideal, let $a \neq 0$ be any element of the quotient field of the integral domain D. Then aD is a fractional ideal with inverse $\frac{1}{a}D$. In particular, this shows that any principal ideal of D is invertible. The following lemma shows that invertible is a stronger condition for ideals than finitely generated:

Lemma 1.1.10. *Let D be an integral domain. Then any invertible fractional ideal I of D is finitely generated over D.*

Proof. Let J be the fractional ideal of D such that $IJ = D$. Then there exists $a_i \in I$ and $b_i \in J$ such that $a_1b_1 + a_2b_2 + \cdots + a_nb_n = 1$. Let $c \in I$ be arbitrary. Then $ca_1b_1 + ca_2b_2 + \cdots + ca_nb_n = c$. Because each element $cb_i \in IJ = D$, we can take $\{a_1, a_2, \ldots, a_n\}$ to be a generating set for I.

□

Definition 1.1.11. *A principal ideal domain D is said to be a discrete valuation domain if D contains a unique nonzero prime ideal or if D is a field.*

A useful property of discrete valuation domains is that the ideals are totally ordered by inclusion. To see this, let V be a discrete valuation domain with unique prime ideal (p). Notice that the only nonunits in V are of the form $p^k u$ where u is a unit in V. Hence the only nonzero proper ideals of V are of the form (p^k). So the total ordering on the nonzero proper ideals of V is defined by $(p^i) \supseteq (p^j)$ where $1 \leq i \leq j$. Of course, all ideals of V contain (0) and are contained in V, which completes the total ordering. The following lemma from [2] gives us a nice way to show that a given domain is a discrete valuation domain.

Lemma 1.1.12. *Let D be a Noetherian integrally closed domain such that D has a unique nonzero prime ideal P. Then D is a discrete valuation domain.*

Proof. Let Q be the quotient field of D. For any ideal I, define the fractional ideal $I^{-1} := \{a \in Q \mid aI \subseteq D\}$. Clearly $D \subseteq I^{-1}$ always holds. We show that $D \subsetneq P^{-1}$. Let $\mathcal{A}$ be the set of all ideals J in D such that $D \subsetneq J^{-1}$. Let $b \neq 0$ be an element of P. Any such element is a nonunit, or else $P = D$, a contradiction. Since the fractional ideal $(b)^{-1}$ contains the element b^{-1}, we have $D \subsetneq (b)^{-1}$. So $(b) \in \mathcal{A}$ and $\mathcal{A}$ is nonempty. Because D is Noetherian, $\mathcal{A}$ contains a maximal element, say M. Notice that M is not the zero ideal because $b \in M$. We show M is a prime ideal of D. Let $r \in D$ and $s \in D$ such that $rs \in M$ and $r \notin M$. Since $M \in \mathcal{A}$, there exists an element $t \in M^{-1} \setminus D$. Since $t \in M^{-1}$ and $rs \in M$, $trs \in D$. This means that $st(rD + M) \subseteq D$, which implies $st \in (rD + M)^{-1}$. If $st \notin D$, then $D \subsetneq (rD + M)^{-1}$ implies $(rD + M) \in \mathcal{A}$. This is a contradiction of the maximality of M because $M \subsetneq (rD + M)$. So assume $st \in D$. Then $t(sD + M) \subseteq D$, which shows that $t \in (sD + M)^{-1}$. Because $t \notin D$, $D \subsetneq (sD + M)^{-1}$ so $(sD + M) \in \mathcal{A}$. So we have $(sD + M) \subseteq M \subseteq (sD + M)$, that is $M = sD + M$ and $s \in M$. This proves that M is a nonzero prime ideal of D, so $P = M \subsetneq D$. Thus $P \in \mathcal{A}$, and $D \subsetneq P^{-1}$. For any fractional ideal I of D, define the set $\mathcal{F}(I) := \{a \in Q \mid aI \subseteq I\}$. We show

that $\mathcal{F}(I) \subseteq D$. Because I is a fractional ideal, there exists $c \in I$ such that $cI \subseteq D$. Then $c\mathcal{F}(I) \subseteq D$, so $c\mathcal{F}(I)$ is an ideal of D. Since the mapping $\mathcal{F}(I) \to c\mathcal{F}(I)$ is a D-module isomorphism, $\mathcal{F}(I)$ is module isomorphic to an ideal of D. If we combine this with the fact that D is Noetherian, we see that $\mathcal{F}(I)$ is finitely generated. By Lemma 1.1.4 every element of $\mathcal{F}(I)$ is integral over D. Since D is integrally closed, $\mathcal{F}(I) \subseteq D$, as claimed. Notice that PP^{-1} is an ideal of D that contains P. Since P is the unique prime ideal of D, P is maximal and we have $P = PP^{-1}$ or $D = PP^{-1}$. Suppose $P = PP^{-1}$. Then for any element $a \in P^{-1}$, $aP \subseteq P$, so by definition $P^{-1} \subseteq \mathcal{F}(P)$. We have already seen that $D \subsetneq P^{-1}$ and that $\mathcal{F}(P) \subseteq D$, so we have $D \subsetneq P^{-1} \subseteq \mathcal{F}(P) \subseteq D$, a contradiction. Therefore, $D = PP^{-1}$, and by definition P is invertible. We show $\bigcap_{n=1}^{\infty} P^n = 0$. Suppose not, then $\bigcap_{n=1}^{\infty} P^n$ is a fractional ideal of D. If $a \in P^{-1}$, then $aP \subseteq D$, so $a\bigcap_{n=1}^{\infty} P^n \subseteq aP\bigcap_{n=1}^{\infty} P^n \subseteq D\bigcap_{n=1}^{\infty} P^n = \bigcap_{n=1}^{\infty} P^n$. This shows that $P^{-1} \subseteq \mathcal{F}\left(\bigcap_{n=1}^{\infty} P^n\right)$. As we have seen, $D \subsetneq P^{-1} \subseteq \mathcal{F}\left(\bigcap_{n=1}^{\infty} P^n\right) \subseteq D$, contradicting $\bigcap_{n=1}^{\infty} P^n \neq 0$. Since $\bigcap_{n=1}^{\infty} P^n = 0$, there exists $a \in P \setminus P^2$. Notice that $a \in P$ implies $aP^{-1} \subseteq D$. Suppose $aP^{-1} \subseteq P$. Then $a \in aD = aP^{-1}P \subseteq P^2$, a contradiction. Recall that P is the unique maximal ideal of D. Therefore, the only ideal not contained in P is D, so $aP^{-1} = D$. Thus $aD = aP^{-1}P = DP = P$, which shows that P is principally generated. Let I be an ideal of D. Every proper ideal is contained in some maximal ideal. In this case the only choice is P, so $I \subseteq P$. Let k be the least integer such that $I \subseteq P^k$ but $I \nsubseteq P^{k+1}$. Let $b \in I \setminus P^{k+1}$. Also, $b \in P^k = a^k D$ implies $a^k w = b$ for some $w \in D$. Suppose $w \in P$. Then $b \in P^{k+1}$, a contradiction. So $w \notin P$, which means that w is not contained in a maximal ideal. In particular, w is a unit. So we have $I \subseteq P^k = a^k D = a^k wD = bD \subseteq I$, which shows that $a^k D = I$ hence I is principally generated. Thus every ideal of D is principal and by assumption D has a unique nonzero prime ideal, which proves our result.

□

We now prove a few preparatory lemmata before giving the characterization theorem for Dedekind domains. Similar results are found in [2].

Lemma 1.1.13. *Let R be a ring and I an ideal of R. Let P be a prime ideal of R that contains I. Then the mapping $P \mapsto P/I$ defines a one-to-one correspondence between the prime ideals in R that contain I and the prime ideals of R/I.*

Proof. Elementary ring theory states that $R/P \cong (R/I)/(P/I)$. Since P is prime, R/P is an integral domain, which implies $(R/I)/(P/I)$ is an integral domain. Thus P/I is prime in R/I. This shows that $P \mapsto P/I$ maps prime ideals to prime ideals. Also, if J is a prime ideal of R such that $I \subseteq J$ and $(R/I)/(J/I) \cong (R/I)/(P/I)$, then $R/P \cong R/J$ so $P \cong J$. This shows that $P \mapsto P/I$ is one-to-one. Now let Q be a prime ideal in R/I, and let $f : R \to R/I$ be the canonical homomorphism. We show that $f^{-1}(Q)$ is a prime ideal of R that contains I. We know that $Q \subsetneq R/I$ implies $f^{-1}(Q) \subsetneq R$. Let $a \in R$ and $b \in R$ such that $ab \in f^{-1}(Q)$. Then $f(ab) \in Q$ implies $f(a)f(b) \in Q$ implies $f(a) \in Q$ or $f(b) \in Q$. Hence $a \in f^{-1}(Q)$ or $b \in f^{-1}(Q)$. In any case, $f^{-1}(Q)$ is prime. Notice that $0 \in Q$, so $f^{-1}(Q)$ contains the kernel of f, which is I. Thus $f^{-1}(Q)$ is a prime ideal of R that maps to Q under $P \mapsto P/I$. This shows that $P \mapsto P/I$ is surjective, and we have our result.

□

Lemma 1.1.14. *Let D be an integral domain, and let I be an ideal of D. Suppose I has the prime ideal factorizations $I = P_1P_2 \dots P_m$ and $I = Q_1Q_2 \dots Q_n$ where P_i is invertible for each i. Then $m = n$, and after reindexing we have $P_i = Q_i$ for each i.*

Proof. We induct on m. If $m = 1$, then we have $P_1 = I = Q_1Q_2 \dots Q_n$. Suppose $n > 1$. Since P_1 is prime, we know that $P_1 \supseteq Q_i$ for some i. Since also $P_1 \subseteq Q_1Q_2 \dots Q_n \subseteq Q_i$, we know that $P_1 = Q_i$. Hence $D = P_1^{-1}P_1 = Q_1Q_2 \dots Q_{i-1}Q_{i+1} \dots Q_n$. This contradicts The fact that the ideals Q_j for $i \neq j$ are proper. Therefore, $n = 1$ and

$P_1 = I = Q_1$. Assume that our result holds for all $k < m$. Let $P_1P_2 \dots P_m = Q_1Q_2 \dots Q_n$. Reindex so that P_1 is an ideal that does not strictly contain any P_i. Because P_1 is prime and $P_1 \supseteq P_1P_2 \dots P_m = Q_1Q_2 \dots Q_n$, $P_1 \supseteq Q_i$ for some i. Reindex so that $P_1 \supseteq Q_1$. Since Q_1 is prime and $Q_1 \supseteq Q_1Q_2 \dots Q_n = P_1P_2 \dots P_m$, Q_1 similarly contains some P_i. So we have $P_i \subseteq Q_1 \subseteq P_1$. Because of our choice for P_1, the containment cannot be strict, hence $P_i = Q_1 = P_1$. Multiplying by P_1^{-1} gives $P_2P_3 \dots P_m = Q_2Q_3 \dots Q_n$. By our induction hypothesis, $m = n$ and after reindexing $Q_i = P_i$, so we have our result.

□

Lemma 1.1.15. *Let D be a Dedekind domain. Then every invertible prime ideal P of D is maximal.*

Proof. Suppose P is an invertible prime ideal that is not maximal. Then there exists $d \in D \setminus P$ such that $P + dD \neq D$. Because D is Dedekind, there exists a prime ideal factorization $P + dD = P_1P_2 \dots P_n$. Similarly, we have $P + d^2D = Q_1Q_2 \dots Q_m$. Let $\bar{*}$ be the image of $*$ under the canonical mapping $D \to D/P$. Then $\bar{d}\bar{D} = \bar{P} + \bar{d}\bar{D} = \bar{P}_1\bar{P}_2 \dots \bar{P}_n$ and $\bar{d}^2\bar{D} = \bar{P} + \bar{d}^2\bar{D} = \bar{Q}_1\bar{Q}_2 \dots \bar{Q}_m$. Notice that P_i and Q_i are prime ideals containing P. Thus by Lemma 1.1.13 we know that the images $\bar{P}_i$ and $\bar{Q}_i$ are prime ideals in $\bar{D}$. Since P is prime in D, D/P is an integral domain. This means that principal ideals in D/P such as $\bar{d}^2\bar{D}$ are invertible. Therefore, $\bar{Q}_1\bar{Q}_2 \dots \bar{Q}_m$ is invertible, hence each $\bar{Q}_i$ is invertible with inverse $\bar{Q}_1\bar{Q}_2 \dots \bar{Q}_{i-1}\bar{Q}_{i+1} \dots \bar{Q}_m(\bar{Q}_1\bar{Q}_2 \dots \bar{Q}_m)^{-1}$. So we can apply Lemma 1.1.14 to the factorizations $\bar{P}_1^2\bar{P}_2^2 \dots \bar{P}_n^2 = \bar{d}^2\bar{D} = \bar{Q}_1\bar{Q}_2 \dots \bar{Q}_m$. Consequently, $m = 2n$ and we can reorder so $\bar{Q}_{2j-1} = \bar{Q}_{2j} = \bar{P}_j$ for all $1 \leq j \leq n$. If we let ϕ denote the isomorphism in Lemma 1.1.13, then we have $\phi^{-1}\left(\bar{Q}_{2j-1}\right) = \phi^{-1}\left(\bar{Q}_{2j}\right) = \phi^{-1}\left(\bar{P}_j\right)$, which implies that $Q_{2j-1} = Q_{2j} = P_j$. As a result, $(P + dD)^2 = P + d^2D$ and we have $P \subseteq P + d^2D = (P + dD)^2 \subseteq P^2 + dD$. So we can write any element of P in

the form $a+rd$ where $a \in P^2$ and $r \in D$. Since $a \in P$ and $a+rd \in P$, $rd \in P$. Since also $d \notin P$, we know $r \in P$. Hence $P \subseteq P^2 + dP \subseteq P$, and we have $P = P^2 + dP$. Because P is invertible $D = P^{-1}P = P^{-1}(P^2 + dP) = P + dD$, which contradicts our assumption. Therefore, every invertible prime ideal is maximal, and we have our result.

□

Lemma 1.1.16. *Let D be a Dedekind domain. Then every nonzero prime ideal P of D is invertible.*

Proof. Let p be a nonzero element of P. Then there exists the prime ideal factorization $(p) = P_1P_2 \dots P_n$. Because P is prime and $P_1P_2 \dots P_n = (p) \subseteq P$, $P_k \subseteq P$ for some k. The fractional ideal $P_1P_2 \dots P_{k-1}P_{k+1} \dots P_n \frac{1}{p} D$ multiplied by P_k gives D, so P_k is invertible. By Lemma 1.1.15, P_k is maximal. Combining this with $P_k \subseteq P$ gives $P_k = P$. This means P is invertible, as desired.

□

The following lemma allows us to apply properties of the local ring $D_\mathfrak{p}$ to D.

Lemma 1.1.17. *Let D be an integral domain. Let $\mathfrak{p}$ be a prime ideal of D. Let $H = D \setminus \mathfrak{p}$. Let $D_\mathfrak{p}$ denote the localization of D at the prime ideal $\mathfrak{p}$. Let Q be the quotient field of D, and let $Q(\gamma)$ be a finite extension of Q. Let R be the integral closure of D in $Q(\gamma)$. Let L be the integral closure of $D_\mathfrak{p}$ in $Q(\gamma)$. Define the ring $R_H := \left\{ \frac{x}{y} \in Q(\gamma) \mid x \in R, y \in H \right\}$. Then $L = R_H$.*

Proof. We show $R_H \subseteq L$. Since $D \subseteq D_\mathfrak{p}$, The integral closure of D is certainly contained in the integral closure of $D_\mathfrak{p}$. This justifies that $R \subseteq L$. Also, by definition $D_\mathfrak{p}$ contains $\frac{1}{y}$ for all $y \in H$. Therefore, L contains these elements as well, which justifies that $R_H \subseteq L$. We show $L \subseteq R_H$. Let $l \in L$. Then l is the root of a monic polynomial with coefficients in $D_\mathfrak{p}$, say $l^n + \frac{a_{n-1}}{b_{n-1}} l^{n-1} + \frac{a_{n-2}}{b_{n-2}} l^{n-2} + \dots + \frac{a_1}{b_1} l + \frac{a_0}{b_0} = 0$ where

$a_i \in D$ and $b_i \in H$. Let $\beta = b_{n-1}b_{n-2}\dots b_1 b_0$. Multiplying the above equation by β gives $(\beta l)^n + c_{n-1}(\beta l)^{n-1} + c_{n-2}(\beta l)^{n-2} + \cdots + c_1(\beta l) + c_0 = 0$ where $c_i = \frac{a_i \beta^{n-i}}{b_i} \in D$. This proves that βl is integral over D; that is, $\beta l \in R$. From above $b_i \in H$, so $\beta \in H$. Therefore, $\beta^{-1} \in R_H$ which implies $\beta l \beta^{-1} = l \in R_H$. Hence $L \subseteq R_H$, and we have our result.

□

One of the characterizations of Dedekind domains involves Krull dimension, which we will define here.

Definition 1.1.18. *Let D be a ring. The Krull dimension of D is the supremum of the set of all k such that $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_k$ and each P_i is a prime ideal of D.*

For example, a field has Krull dimension 0. An integral domain that is not a field has Krull dimension at least 1, because there is some nonzero prime ideal that contains the zero ideal, which is prime. If we combine the results of Lemma 1.1.15 and Lemma 1.1.16, we see that every nonzero prime ideal of a Dedekind domain is maximal. This implies that Dedekind domains have Krull dimension at most 1. Therefore, the following corollary is valid for Dedekind domains.

Corollary 1.1.19. *Let D be an integral domain of Krull dimension at most 1, $\mathfrak{p}$ a prime ideal of D, $H = D \setminus \mathfrak{p}$, Q the quotient field of D, $Q(\gamma)$ a finite extension of Q, R the integral closure of D in $Q(\gamma)$, L the integral closure of $D_\mathfrak{p}$ in $Q(\gamma)$, and $R_H := \left\{ \frac{x}{y} \in Q(\gamma) \mid x \in R, y \in H \right\}$. Then there exists a prime factorization $\mathfrak{p}R = P_1^{k_1} P_2^{k_2} \dots P_m^{k_m}$ if and only if there exists a corresponding prime factorization $\mathfrak{p}L = (\mathfrak{P}_1)^{k_1}(\mathfrak{P}_2)^{k_2} \dots (\mathfrak{P}_m)^{k_m}$.*

Proof. Because of Lemma 1.1.17, we know that $L = R_H$, so it suffices to replace L with R_H. Consider the homomorphism $\sigma : R \to R_H$ defined by $\sigma(r) = \frac{r}{1}$. It is a well known result that σ is injective, so σ embeds R in R_H. We show that if P_i is a prime

ideal of R that contains $\mathfrak{p}R$, then P_iR_H is a prime ideal of R_H that contains $\mathfrak{p}R_H$. First notice that $\mathfrak{p}R_H \subseteq P_iR_H$ follows from the fact that $\mathfrak{p} \subseteq P_i$. We show $P_i \cap H = \emptyset$. Assume otherwise; then there exists some $a \in P_i \cap H$. Recall $a \in H$ implies $a \notin \mathfrak{p}$. Since $\mathfrak{p} \subseteq P_i$ and $\mathfrak{p}$ is maximal in D, we have $P_iR \supseteq (aD + \mathfrak{p})R = DR = R$. This contradicts the fact that P_i is a (proper) prime ideal of R. So we know that $P_i \cap H = \emptyset$. Suppose that $P_iR_H = R_H$. Then $\sigma^{-1}(P_iR_H) = R$, so there exists $\frac{b}{h} \in P_iR_H$ such that $\frac{b}{h} = \sigma(1) = \frac{1}{1}$. Therefore, there is some $h_1 \in H$ such that $bh_1 = hh_1$, hence $bh_1 \in P_i \cap H$. This contradicts $P_i \cap H = \emptyset$. So $P_iR_H \subsetneq R_H$. Assume that $\frac{r_1}{h_1} \in R_H$ and $\frac{r_2}{h_2} \in R_H$ such that $\frac{r_1}{h_1}\frac{r_2}{h_2} = \frac{b_1}{h_3} \in P_iR_H$. Then there is some $h_4 \in H$ such that $h_4h_3r_1r_2 = h_4h_1h_2b_1$. Notice $h_4h_3r_1r_2 \in P_i$ but $h_4h_3 \notin P_i$, so $r_1r_2 \in P_i$. Because P_i is prime, either $r_1 \in P_i$ or $r_2 \in P_i$. This implies that $\frac{r_1}{h_1} \in P_iR_H$ or $\frac{r_2}{h_2} \in P_iR_H$, which justifies that P_iR_H is prime. Suppose $\mathfrak{p}R = P_1^{k_1}P_2^{k_2}\dots P_m^{k_m}$. Then we have $\mathfrak{p}R_H = \mathfrak{p}RR_H = P_1^{k_1}P_2^{k_2}\dots P_m^{k_m}R_H = (P_1R_H)^{k_1}(P_2R_H)^{k_2}\dots(P_mR_H)^{k_m}$. Thus we have proven the only if condition of the theorem where $\mathfrak{P}_i = P_iR_H$. We show that if $\mathfrak{P}_i$ is a prime ideal of R_H containing $\mathfrak{p}R_H$, then $\sigma^{-1}(\mathfrak{P}_i)$ is a prime ideal of R containing $\mathfrak{p}R$. Since $\mathfrak{p}R_H \subseteq \mathfrak{P}_i$, $\mathfrak{p}R = \sigma^{-1}(\mathfrak{p}R_H) \subseteq \sigma^{-1}(\mathfrak{P}_i)$. We show that $\sigma^{-1}(\mathfrak{P}_i)$ is a prime ideal of R. Let $c_1 \in R$ and $c_2 \in R$ such that $c_1c_2 \in \sigma^{-1}(\mathfrak{P}_i)$. Then $\sigma(c_1c_2) = \sigma(c_1)\sigma(c_2) \in \mathfrak{P}_i$. Since $\mathfrak{P}_i$ is prime, either $\sigma(c_1) \in \mathfrak{P}_i$ or $\sigma(c_2) \in \mathfrak{P}_i$. Therefore, without loss of generality, $c_1 = \sigma^{-1}(\sigma(c_1)) \in \sigma^{-1}(\mathfrak{P}_i)$. This shows that $\sigma^{-1}(\mathfrak{P}_i)$ is prime in R. Assume that $\mathfrak{p}R_H = (\mathfrak{P}_1)^{k_1}(\mathfrak{P}_2)^{k_2}\dots(\mathfrak{P}_m)^{k_m}$ is a prime factorization for $\mathfrak{p}R_H$. Then $\mathfrak{p}R = \sigma^{-1}(\mathfrak{p}R_H) = \sigma^{-1}((\mathfrak{P}_1)^{k_1}(\mathfrak{P}_2)^{k_2}\dots(\mathfrak{P}_m)^{k_m}) = \sigma^{-1}(\mathfrak{P}_1)^{k_1}\sigma^{-1}(\mathfrak{P}_2)^{k_2}\dots\sigma^{-1}(\mathfrak{P}_m)^{k_m}$. As we have seen, $\sigma^{-1}(\mathfrak{P}_i)$ is prime, so we let $\sigma^{-1}(\mathfrak{P}_i) = P_i$ and we have our result.

□

We are ready to state the characterization theorem for Dedekind domains. More characterizations appear in the literature, but the following list contains six that are

best suited to the purposes of this paper.

Theorem 1.1.20. *Let D be an integral domain. The following are equivalent:*

1) D is a Dedekind domain.

2) Every proper ideal of D factors uniquely into a finite product of prime ideals.

3) Every nonzero ideal of D is invertible.

4) Every fractional ideal of D is invertible.

5) D is Noetherian, integrally closed, and has Krull dimension at most 1.

6) D is Noetherian and for every nonzero prime ideal $\mathfrak{p}$ of D, the localization $D_{\mathfrak{p}}$ is a discrete valuation domain.

Proof. 1) $\implies$ 2) :

Suppose that every proper ideal of D factors into a finite product of prime ideals. By Lemma 1.1.16, those prime ideals must be invertible. By Lemma 1.1.14, any such factorization must be unique, which proves our result.

2) $\implies$ 3) :

Let I be a nonzero ideal. Then we have the prime ideal factorization $I = P_1 P_2 \dots P_n$ where each P_i is a nonzero prime. By Lemma 1.1.16, each P_i is invertible, hence $I^{-1} = P_1^{-1} P_2^{-1} \dots P_n^{-1}$ as desired.

3) $\implies$ 4) :

Suppose every nonzero ideal of D is invertible. Let I be a fractional ideal of D and $a \in D$ a nonzero element such that $aI \subseteq D$. Then aI is a nonzero ideal of D, hence by assumption there exists a nonzero ideal J of D such that $aIJ = D$. Then $I(aJ) = D$ implies that I is invertible with inverse aJ, and we have our result.

4) $\implies$ 5) :

Suppose every fractional ideal of D is invertible. Since ideals of D are fractional ideals of D, every ideal is invertible hence finitely generated by Lemma 1.1.10. This shows that D is Noetherian. Let Q be the quotient field of D, and let $c \in Q$ be

integral over D. By Lemma 1.1.3, we know that $D[c]$ is a finitely generated D-module, say $D[c] \subseteq D + c_1D + c_2D + \cdots + c_nD$ where each $c_i \in Q$. Because $c_i \in Q$, there exists b_i such that $b_ic_i \in D$. Thus if we let $b = b_1b_2 \ldots b_n$, then $bD[c] \subseteq bD + bc_1D + bc_2D + \cdots + bc_nD \subseteq D$ because each $bc_i \in D$. So we know that $D[c]$ is a fractional ideal of D, which means $D[c]$ is invertible by assumption. So let J be the fractional ideal of D such that $JD[c] = D$. Because D and $D[c]$ share the same identity element, we have $D[c] = (D[c])D = (D[c])((D[c])J = (D[c])J = D$. Thus $D[c] = D$, which implies that $c \in D$ and D is integrally closed. Suppose there exists a nonzero prime ideal P and maximal ideal M such that $P \subsetneq M$. Both P and M are invertible by assumption with inverses P^{-1} and M^{-1}, respectively. Also, $M^{-1}P$ is an ideal of D because $M^{-1}P \subseteq M^{-1}M = D$. Because $M^{-1}PM = P$ and P is prime, either $M \subseteq P$ or $M^{-1}P \subseteq P$. Since $M \subseteq P$ contradicts our supposition that $P \subsetneq M$, we continue under the assumption that $M^{-1}P \subseteq P$. Under this assumption $R = MM^{-1} \subseteq M^{-1} = M^{-1}R = M^{-1}PP^{-1} \subseteq PP^{-1} = R$, which implies $R = M^{-1}$. Hence $R = MM^{-1} = MR = M$, which contradicts the maximality of M. So we cannot have a nonzero prime ideal P and a maximal ideal M such that $P \subsetneq M$. This proves that the Krull dimension of D is at most 1.

5) $\Longrightarrow$ 6) :

We prove that $D_\mathfrak{p}$ satisfies the hypotheses of Lemma 1.1.12. To see why $D_\mathfrak{p}$ is integrally closed, apply Lemma 1.1.17. Since the integral closure of D is D, the integral closure of $D_\mathfrak{p}$ is again $D_\mathfrak{p}$. By assumption, D is Noetherian. Notice that any ideal of $D_\mathfrak{p}$ is of the form $ID_\mathfrak{p}$ where I is an ideal of D. This is because localization either turns an element of I into a unit or does not, and this determines what happens to I in $D_\mathfrak{p}$. If localization turns an element of I into a unit (that is, $I \cap D \setminus \mathfrak{p} \neq 0$), then locally $ID_\mathfrak{p} = DD_\mathfrak{p} = D_\mathfrak{p}$. If localization does not turn an element of I into a unit, then the ideal retains its structure in $D_\mathfrak{p}$. In either case, the property of

finite generation of ideals is preserved under localization, and this shows that $D_{\mathfrak{p}}$ is Noetherian. By assumption, D has Krull dimension 1, so the only nonzero prime ideal contained in $\mathfrak{p}$ is $\mathfrak{p}$ itself. As we have seen in the proof of Corollary 1.1.19, prime ideals of D contained in $\mathfrak{p}$ correspond to prime ideals of $D_{\mathfrak{p}}$. Since there is a unique nonzero prime ideal contained in $\mathfrak{p}$, there is a unique nonzero prime ideal of $D_{\mathfrak{p}}$, namely $\mathfrak{p}D_{\mathfrak{p}}$. Therefore $D_{\mathfrak{p}}$ is a discrete valuation domain by Lemma 1.1.12.

6) $\Longrightarrow$ 1) :

Let I be an ideal of D. Recall that for any ideal I of D, $I^{-1} := \{a \in Q \mid aI \subseteq D\}$ is a fractional ideal of D such that $D \subseteq I^{-1}$. The product $II^{-1} \subseteq D$, and hence is an ideal of D. Suppose $II^{-1} \subsetneq D$. Then there exists a maximal ideal M such that $II^{-1} \subseteq M \subsetneq D$. By assumption, the ideal ID_M is principal in D_M, say $ID_M = \frac{a}{s}D_M$ where $a \in I$ and $s \in D \setminus M$. By assumption, D is Noetherian. Hence I is finitely generated, say $I = (b_1, b_2, \ldots, b_n)$. For each i such that $1 \leq i \leq n$, $\frac{b_i}{1} \in ID_M$. Therefore, $\frac{b_i}{1} = \frac{a}{s}\frac{d_i}{s_i}$ for some $d_i \in D$ and $s_i \in D \setminus M$. So $b_i s s_i = a d_i$. Let $c = s s_1 s_2 \ldots s_n$. Then $cb_i \in aD$, hence $\frac{c}{a}b_i \in D$. Thus, if $t_1 b_1 + t_2 b_2 + \cdots + t_n b_n$ is any element of I, then $\frac{c}{a}(t_1 b_1 + t_2 b_2 + \cdots + t_n b_n) = \frac{c}{a}t_1 b_1 + \frac{c}{a}t_2 b_2 + \cdots + \frac{c}{a}t_n b_n \in D$. This means that $\frac{c}{a} \in I^{-1}$, which implies $c = a\frac{c}{a} \in II^{-1} \subseteq M$. Notice that c is a product of elements of the multiplicatively closed set $D \setminus M$, so $c \in D \setminus M$, a contradiction. Therefore, $II^{-1} = D$ and I is invertible. We define the ideal $\mathcal{M}(I)$ for every ideal $I \subseteq D$. If $I \subsetneq D$, let $\mathcal{M}(I)$ be a maximal ideal containing I. If $I = D$, then let $\mathcal{M}(I) = D$. Because of the relations $I\mathcal{M}(I)^{-1} \subseteq \mathcal{M}(I)\mathcal{M}(I)^{-1} = D$, we know that the fractional ideal $I\mathcal{M}(I)^{-1}$ is, in fact, an ideal of D. Also, $D \subseteq \mathcal{M}(I)^{-1}$ implies $I = ID \subseteq I\mathcal{M}(I)^{-1}$. Notice that $\mathcal{M}(I) = \mathcal{M}(I)II^{-1} = I(\mathcal{M}(I)I^{-1}) \subseteq (I\mathcal{M}(I)^{-1})(\mathcal{M}(I)I^{-1}) = II^{-1}\mathcal{M}(I)\mathcal{M}(I)^{-1} = D$, where equality holds if and only if $I = D$. Therefore, $I = I\mathcal{M}(I)^{-1}$ if and only if $I = D$. So let $I \subsetneq D$. Define the ideal $I_0 = I$, and for every nonnegative integer n

let $I_{n+1} = I_n \mathcal{M}(I_n)^{-1}$. Consider the chain of ideals

$$I \subseteq I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \ldots$$

We have seen that $I_{n+1} = I_n$ if and only if $I_n = D$. This means that every "$\subseteq$" in the chain is actually a "$\subsetneq$" unless there is some m for which $I_m = D$, after which every "$\subseteq$" is actually "=". Because D is Noetherian, every ascending chain of ideals must stabilize, so there exists some minimal integer m such that $I_m = I_{m+1} = I_m \mathcal{M}(I_m)^{-1}$. As mentioned, this implies $I_m = D$, so the above chain of ideals is of the form

$$I \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_{m-1} \subsetneq D = D = \ldots$$

This means that for each i such that $0 \leq i \leq m-1$, $I_i \subsetneq I_i \mathcal{M}(I_i)^{-1}$. This implies that $I_i \subsetneq D$, hence $\mathcal{M}(I_i)$ is a maximal ideal containing I_i. Because $D = I_m = I_{m-1}\mathcal{M}(I_{m-1})^{-1}$, we multiply by $\mathcal{M}(I_{m-1})$ to get $\mathcal{M}(I_{m-1}) = D\mathcal{M}(I_{m-1}) = I_{m-1}$. If we also recall how each ideal I_i was defined, we get

$$I_{m-1} = I_{m-2}\mathcal{M}(I_{m-2})^{-1} = \cdots = I\mathcal{M}(I)^{-1}\mathcal{M}(I_1)^{-1}\mathcal{M}(I_2)^{-1}\ldots\mathcal{M}(I_{m-2})^{-1}$$

Multiplying both sides by $\mathcal{M}(I)\mathcal{M}(I_1)\mathcal{M}(I_2)\ldots\mathcal{M}(I_{m-2})$ and replacing I_{m-1} with $\mathcal{M}(I_{m-1})$ results in

$$\mathcal{M}(I)\mathcal{M}(I_1)\mathcal{M}(I_2)\ldots\mathcal{M}(I_{m-1}) = I$$

Thus I factors into a product of prime ideals, as desired.

□

1.2. Almost Dedekind Domains

Property 6) in Theorem 1.1.20 has a straightforward generalization if we remove the Noetherian condition.

Definition 1.2.1. *An integral domain D is said to be an almost Dedekind domain if for every nonzero prime ideal $\mathfrak{p}$ of D, the localization $D_{\mathfrak{p}}$ is a discrete valuation domain.*

Theorem 1.1.20 clearly shows that Dedekind implies almost Dedekind. On the other hand, there are many examples of almost Dedekind domains that are not Dedekind in the literature. A thorough collection of construction techniques and papers with interesting examples of almost Dedekind domains is given in [8]. We will state a result of [4] that will be a useful tool in determining whether a ring is almost Dedekind.

Theorem 1.2.2. *Let D_0 be an almost Dedekind domain with quotient field K_0. Let $\{K_n\}$ be a set of fields such that each K_n is a finite separable extension of K_0. Let $K := \bigcup_{n=0}^{\infty} K_n$ Let D_n be the integral closure of D_0 in K_n for all $n \geq 0$. Then $D := \bigcup_{n=0}^{\infty} D_n$ is the integral closure of D_0 in K. Choose a maximal ideal P of D. Define $P_n = P \cap D_n$ for each $n \geq 0$. Then P_n is a factor of $P_0 D_n$, say to the e_n power. Also, D is almost Dedekind if and only if the set $\{e_n\}$ is bounded for every maximal ideal P of D.*

Proof. See [4] for details.

□

1.3. The Discriminant

We define the discriminant of a monic polynomial. The discriminant of a monic polynomial gives useful information about the associated field extension, as we will see later.

Definition 1.3.1. *Let Q be a field, and let $f(x) \in Q[x]$ be a monic separable polynomial of degree n with roots $r_1, r_2, \ldots, r_n$. Then the discriminant of $f(x)$ is*

given by the product

$$d(f(x)) := \prod_{i>j}^{n} (r_i - r_j)^2$$

It is straightforward from the definition yet worth noting that the discriminant $d(f(x)) = 0$ if and only if $f(x)$ has a repeated root in some splitting field. When $f(x)$ is a minimal polynomial for a finite separable extension of a field, there is another characterization of the situation where $d(f(x)) = 0$. This characterization appears in [7] as follows.

Theorem 1.3.2. *Let D be a Dedekind domain, Q the quotient field of D, γ an element of the algebraic closure of D, $Q(\gamma)$ a finite separable extension of Q, R the integral closure of D in $Q(\gamma)$, and $f(x)$ a minimal polynomial for $Q(\gamma)$ over Q of degree n. Then $d(f(x)) \neq 0$ if and only if $\{1, \gamma, \gamma^2, \ldots, \gamma^{n-1}\}$ is a basis for $Q(\gamma)$ over Q.*

Proof. See [7] for details.

□

We will give a few alternate characterizations of the discriminant. One of the characterizations involves the formal derivative of a monic polynomial and the other involves the trace, both of which are defined below.

Definition 1.3.3. *Let $f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_2x^2 + a_1x + a_0$. Then the formal derivative of $f(x)$, denoted $f'(x)$, is given by $f'(x) = nx^{n-1} + (n-1)a_{n-1}x^{n-2} + (n-2)a_{n-2}x^{n-3} + \cdots + 2a_2x + a_1$*

Definition 1.3.4. *Let Q be a field and let K be a finite separable field extension of Q of degree n. Let $r_1 \in K$. Then there exists a minimal polynomial of degree n for r_1 over Q, say $f(x)$. Suppose the roots of $f(x)$ in some field extension are given by $r_1, r_2, \ldots, r_n$. The trace of r_1 is the function $Tr : K \to Q$ defined by $Tr(r_1) = r_1 + r_2 + \cdots + r_n$.*

Theorem 1.3.5. *Let Q be a field, $f(x) \in Q[x]$ a monic separable polynomial of degree n, and $r_1, r_2, \ldots, r_n$ the roots of $f(x)$. Suppose $f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_2x^2 + a_1x + a_0$ where each $a_i \in Q$. Define $b_{m-1} = ma_m$ for all m such that $1 \leq m \leq n-1$ and $b_{n-1} = n$. Thus $f'(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_2x^2 + b_1x + b_0$. Let $\gamma \in \{r_1, r_2, \ldots, r_n\}$. Define the matrix*

$$M := \begin{bmatrix} Tr(1) & Tr(\gamma) & \ldots & Tr(\gamma^{n-2}) & Tr(\gamma^{n-1}) \\ Tr(\gamma) & Tr(\gamma^2) & \ldots & Tr(\gamma^{n-1}) & Tr(\gamma^n) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ Tr(\gamma^{n-1}) & Tr(\gamma^n) & \ldots & Tr(\gamma^{2n-3}) & Tr(\gamma^{2n-2}) \end{bmatrix}$$

In addition, define the matrix

$$N := \begin{bmatrix} 1 & a_{n-1} & a_{n-2} & \ldots & a_1 & a_0 & 0 & 0 & \ldots & 0 \\ 0 & 1 & a_{n-1} & \ldots & a_2 & a_1 & a_0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & 0 & 1 & a_{n-1} & a_{n-2} & a_{n-3} & a_{n-4} & \ldots & a_0 \\ b_{n-1} & b_{n-2} & \ldots & b_1 & b_0 & 0 & 0 & 0 & \ldots & 0 \\ 0 & b_{n-1} & b_{n-2} & \ldots & b_1 & b_0 & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & b_{n-1} & b_{n-2} & b_{n-3} & \ldots & b_1 & b_0 \end{bmatrix}$$

Then $d(f(x)) = \det(M) = (-1)^{\frac{n(n-1)}{2}} \det(N)$

Proof. The proof is computational; see [1].

□

The discriminant can be defined on any set of elements in an extension field.

This definition coincides with the polynomial definition of a discriminant in the case where the field extension is generated by a minimal polynomial. However, because not every field extension is generated in this way, it will be necessary in some cases to use the following definition from [7].

Definition 1.3.6. *Let D be a Dedekind domain, Q the quotient field of D, γ an element of the algebraic closure of D, $Q(\gamma)$ a finite separable extension of Q of degree n, R the integral closure of D in $Q(\gamma)$, and $\{\sigma_i\}$ the set of n distinct embeddings of $Q(\gamma)$ in a given algebraic closure of Q. Let $Y = \{y_1, y_2, \ldots, y_n\}$ be a subset of $Q(\gamma)$. Then the discriminant of Y is given by $d_{Q(\gamma)/Q}(Y) = \det(\sigma_i y_j)^2$.*

The discriminant gives important information about the module generated by Y, as in the following result from [7].

Theorem 1.3.7. *Let D be a Dedekind domain, Q the quotient field of D, γ an element of the algebraic closure of D, $Q(\gamma)$ a finite separable extension of Q of degree n, R the integral closure of D in $Q(\gamma)$, and $\{\sigma_i\}$ the set of n distinct embeddings of $Q(\gamma)$ in a given algebraic closure of Q. Let $Y = \{y_1, y_2, \ldots, y_n\}$ and $W = \{w_1, w_2, \ldots, w_n\}$ be subsets of $Q(\gamma)$. Then there exists a matrix X such that $Y = XW$ and $d_{Q(\gamma)/Q}(Y) = \det(X)^2 d_{Q(\gamma)/Q}(W)$. Then Y and W generate the same module if and only if $\det(X)$ is a unit in D.*

Proof. See [7].

□

The previous theorem shows that whenever the discriminants of $D[\gamma]$ and R differ by a factor of a unit, $D[\gamma] = R$. For a demonstration of the consequences of the relationship $D[\gamma] = R$, see Example 2.2.1.

1.4. Extensions of Dedekind Domains

This section is devoted to extensions of Dedekind domains, more specifically the integral closure of a Dedekind domain in a finite separable extension of the quotient field. We will continue working with such extensions for much of the rest of the paper, so for ease of notation we define them as Dedekind D - R constructions.

Definition 1.4.1. *Let D be a Dedekind domain, Q the quotient field of D, γ an element of the algebraic closure of Q, $Q(\gamma)$ a finite separable extension of Q of degree n, and R the integral closure of D in $Q(\gamma)$. Then R is said to be a Dedekind D - R construction. Whenever we speak of Dedekind D - R constructions, D, Q, γ, R, and n will be as in this definition. The diagram below gives the layout of the situation.*

$$\begin{array}{ccc} R & \rightarrow & Q(\gamma) \\ \uparrow & & \uparrow \\ D & \rightarrow & Q \end{array}$$

At the end of this section, we will have prove an important classical result of algebraic number theory, that any Dedekind D - R construction is Dedekind. For now, we discuss the most familiar class of Dedekind D - R constructions, the algebraic rings of integers.

Definition 1.4.2. *Let $\mathbb{F}$ be an extension of $\mathbb{Q}$ created by adjoining the roots of a monic polynomial with coefficients in $\mathbb{Z}$. An algebraic ring of integers is the integral closure of $\mathbb{Z}$ in $\mathbb{F}$.*

As mentioned, any algebraic ring of integers is a Dedekind D - R construction. We know that $\mathbb{Z}$ is a Dedekind domain, and since $\mathbb{Q}$ is of characteristic 0, every extension of $\mathbb{Q}$ is separable [2]. This leads us to our first example of a Dedekind D - R construction.

Example 1.4.3. *Let* $\mathbb{F}$ *be* $\mathbb{Q}$ *adjoined with the roots of the polynomial* $x^2 + 5$*, so* $\mathbb{F} = \mathbb{Q}(\sqrt{-5})$*. The integral closure of* $\mathbb{Z}$ *in* $\mathbb{F}$ *is an algebraic ring of integers; it can be shown using an argument in the spirit of Theorem* 4.2.10 *that this ring is* $\mathbb{Z}[\sqrt{-5}]$

Let $\mathfrak{p}$ be a prime ideal of the Dedekind domain D. In the existing literature, much work has been done to predict the behavior $\mathfrak{p}R$ in a Dedekind D - R construction. One question that is often asked is whether $\mathfrak{p}R$ factors as a product of two or more ideals of R, and if so, how. Depending on the answer to this question, $\mathfrak{p}$ is classified as a ramified, split, or inert prime, as in the definition below.

Definition 1.4.4. *Let* $\mathfrak{p}$ *be a prime ideal in the Dedekind domain* D*. Let* R *be a be a Dedekind* D - R *construction. Consider the ideal* $\mathfrak{p}R$*. Since* R *is a Dedekind domain,* $\mathfrak{p}R$ *factors uniquely as a product of prime ideals in* R*, say* $\mathfrak{p}R = P_1^{e_1} P_2^{e_2} \dots P_k^{e_k}$*. If* $k = 1$ *and* $e_1 = 1$ *then we say* $\mathfrak{p}R$ *is inert. If* $k > 1$ *and* $e_i = 1$ *for all* $1 \leq i \leq k$ *then we say* $\mathfrak{p}R$ *is split. If* $e_i > 1$ *for some* $1 \leq i \leq k$ *then we say* $\mathfrak{p}R$ *is ramified.*

We return to Example 1.4.3 to illustrate inert, split, and ramified:

Example 1.4.5. *Recall that the integral closure of* $\mathbb{Z}$ *in* $\mathbb{Q}(\sqrt{-5})$ *is* $\mathbb{Z}[\sqrt{-5}]$*. Then* 2 *and* 5 *are ramified primes because* $(2) = (2, \sqrt{-5} + 1)^2$ *and* $(5) = (\sqrt{-5})^2$*. The primes* 3 *and* 7 *are split because* $(3) = (3, \sqrt{-5}+1)(3, \sqrt{-5}+2)$ *and* $(7) = (7, \sqrt{-5}+3)(7, \sqrt{-5}+4)$*. For an example of an inert prime, consider* 11 *because* (11) *is a prime ideal in* $\mathbb{Z}[\sqrt{-5}]$*.*

We set about proving that Dedekind D - R constructions are Dedekind, first by proving a series of lemmata. The first lemma is from [5], and it has many important consequences above and beyond the discussion of this section.

Lemma 1.4.6. *Let* R *be a Dedekind* D - R *construction. Let* $f(t)$ *be a minimal polynomial for* $Q(\gamma)$ *over* Q*, and let* $d(f(t))$ *be the discriminant of* $f(t)$*. Let* $E :=$

$D[t]/f(t)$. *Then* $d(f)R \subseteq E \subseteq D[\gamma]$. *In addition,* R *is finitely generated as a* D*-module.*

Proof. Let $E := D[t]/f(t)$. Then a basis for E over D is given by $\{1, \gamma, \gamma^2, \ldots, \gamma^{n-1}\}$. Notice that the quotient field K of E is given by $K = Q[t]/f(t)$. A basis for K over Q is again given by $\{1, \gamma, \gamma^2, \ldots, \gamma^{n-1}\}$. Define the trace $Tr : K \to Q$ as the function that maps each element of K to the sum of its conjugate elements. If $\alpha \in R$, then $Tr(\alpha) \in D$. This is because $f(t) = (t - \gamma_1)(t - \gamma_2)\ldots(t - \gamma_n)$ where γ_i is a conjugate of γ. The coefficient of t^{n-1}, which must be an element of D, is $-(\gamma_1 + \gamma_2 + \cdots + \gamma_n)$. Also notice that Tr is linear over elements of Q. Define the matrix

$$M := \begin{bmatrix} Tr(1) & Tr(\gamma) & \ldots & Tr(\gamma^{n-2}) & Tr(\gamma^{n-1}) \\ Tr(\gamma) & Tr(\gamma^2) & \ldots & Tr(\gamma^{n-1}) & Tr(\gamma^n) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ Tr(\gamma^{n-1}) & Tr(\gamma^n) & \ldots & Tr(\gamma^{2n-3}) & Tr(\gamma^{2n-2}) \end{bmatrix}$$

Theorem 1.3.5 states that $\det(M) = d(f)$. Let $b \in R$. Since $R \subseteq K$, b can be represented in the form $b = q_0 + q_1\gamma + q_2\gamma^2 + \cdots + q_{n-1}\gamma^{n-1}$ where $q_i \in Q$ for $1 \leq i \leq n-1$. For $0 \leq j \leq n-1$, $b\gamma^j$ is a product of elements of R, hence $b\gamma^j \in R$ and consequently $Tr(b\gamma^j) \in D$. So define $d_j := Tr(b\gamma^j)$. Since Tr is linear and $b\gamma^j$ has the representation $b\gamma^j = q_0\gamma^j + q_1\gamma^{j+1} + \cdots + q_{n-1}\gamma^{j+n-1}$, d_j has the representation $d_j = q_0Tr(\gamma^j) + q_1Tr(\gamma^{j+1}) + \cdots + q_{n-1}Tr(\gamma^{j+n-1})$. This defines a linear equation for each j such that $0 \leq j \leq n-1$. For ease of notation define the vectors:

$$\vec{d} = \begin{bmatrix} d_0 \\ d_1 \\ \vdots \\ d_{n-1} \end{bmatrix} \qquad \vec{q} = \begin{bmatrix} q_0 \\ q_1 \\ \vdots \\ q_{n-1} \end{bmatrix}$$

With these definitions the aforementioned linear equations are represented by

the system:

$$M\overrightarrow{q} = \overrightarrow{d}$$

By Theorem 1.3.2, we know that $d(f) \neq 0$. This yields $0 \neq d(f) = \det(M)$. Therefore, we can apply Cramer's rule to the previous system. For $1 \leq k \leq n$ define M_k as the matrix formed by replacing column k of M with $\overrightarrow{d}$. Then by Cramer's rule we have $q_{k-1} = \frac{\det(M_k)}{d(f)}$. Since the entries of M_k are in D, $q_{k-1}d(f) = \det(M_k) \in D$. Hence $bd(f) = q_0 d(f) + q_1 d(f)\gamma + q_2 d(f)\gamma^2 + \cdots + q_{n-1}d(f)\gamma^{n-1}$. Because the coefficients of the γ^k terms are all elements of D, $bd(f) \in E$. Thus $d(f)R \subseteq E \subseteq D[\gamma]$, which gives us our first result. For the second result, notice that division by $d(f)$ gives $R \subseteq \frac{1}{d(f(t))}E$. Therefore, any element $r \in R$ has the representation $r = c_0\frac{1}{d(f(t))} + c_1\frac{\gamma}{d(f(t))} + c_2\frac{\gamma^2}{d(f(t))} + \cdots + c_{n-1}\frac{\gamma^{n-1}}{d(f(t))}$ where each $c_i \in D$. So R is finitely generated as a D-module, and we have our second result.

□

Lemma 1.4.7. *Let R be a Dedekind D - R construction. Let P be a prime ideal of R. Then $D \cap P$ is a prime ideal of D.*

Proof. Since $D \subset R$, there exists an injective homomorphism $\phi : D \to R$. By passing to equivalence classes, we can define a mapping $\psi : D/(D \cap P) \to R/P$ Notice that $\phi(D \cap P) \subseteq P$. Therefore, the kernel of ψ is the set of all elements of D that map into P under ϕ. This is precisely $D \cap P$, so the kernel of ψ is 0. This means ψ is also injective. This proves that $D/D \cap P$ is a subring of R/P. Since P is a prime ideal, R/P is an integral domain. Hence there are no zero divisors in $D/(D \cap P)$, proving that $D \cap P$ is a prime ideal of D.

□

Lemma 1.4.8. *Let R be a Dedekind D - R construction. Let P_1 and P_2 be prime ideals of R such that $P_1 \subseteq P_2$ and $D \cap P_1 = D \cap P_2$. Then $P_1 = P_2$.*

Proof. Let $a \in P_2 \setminus P_1$. Let $m(x) = x^k + b_{k-1}x^{k-1} + b_{k-2}x^{k-2} + \cdots + b_1x + b_0$ be a polynomial with $b_i \in D$ such that $m(a) = 0$. Suppose $b_i \in P_1 \cap D$ for all $0 \leq i \leq k-1$. Then since $m(a) - a^k \in P_1$, $a^k \in P_1$. Because P_1 is prime, $a \in P_1$, which contradicts our supposition that each $b_i \in P_1 \cap D$. So there exists a minimal j such that $b_j \notin P_1 \cap D$. Thus $b_0, b_1, \ldots, b_{j-1}$ are all elements of $P_1 \cap D$. Then $b_0 + b_1a + b_2a^2 \cdots + b_{j-1}a^{j-1} = c \in P_1$ and $m(a) \in P_1$, so $m(a) - c = a^j(a^{k-j} + a^{k-j-1}b_{k-1} + a^{k-j-2}b_{k-2} + \cdots + + ab_{j+1} + b_j) \in P_1$. We know $a \notin P_1$ hence $a^j \notin P_1$, which implies $a^{k-j} + a^{k-j-1}b_{k-1} + a^{k-j-2}b_{k-2} + \cdots + ab_{j+1} + b_j \in P_1 \subseteq P_2$. Because also $a \in P_2$ we know $a^{k-j} + a^{k-j-1}b_{k-1} + a^{k-j-2}b_{k-2} + \cdots + ab_{j+1} \in P_2$, so $b_j \in P_2 \cap D = P_1 \cap D$. This contradicts our choice of b_j and hence our assumption that there is an $a \in P_2 \setminus P_1$. So $P_1 = P_2$, and we have our result.

□

Theorem 1.4.9. *Let R be a Dedekind D - R construction. Then R is a Dedekind domain.*

Proof. We saw in Lemma 1.4.6 that R is finitely generated as a D-module. Since also D is Noetherian, R is Noetherian. By Theorem 1.1.6, we know that R is integrally closed. We show that the Krull dimension of R is 1. Let $P_1 \subsetneq P_2$ be prime ideals of R. Lemma 1.4.8 shows that $D \cap P_1 \subsetneq D \cap P_2$. Lemma 1.4.7 asserts that $D \cap P_1$ and $D \cap P_2$ are both prime ideals of D. By Theorem 1.1.20 D has Krull dimension 1, so $D \cap P_1 = 0$. Hence $D \cap P_1 = 0 = D \cap 0$ and $0 \subseteq P_1$, which by Lemma 1.4.8 shows that $0 = P_1$. But then $P_1 \subsetneq P_2$ implies $P_1 = 0$, which proves that the Krull dimension of R is 1. Since we also R is Noetherian and integrally closed, by Theorem 1.1.20 R is Dedekind.

□

Corollary 1.4.10. *Every algebraic ring of integers is Dedekind.*

Proof. See Theorem 1.4.9 along with the comments following Definition 1.4.2.

□

CHAPTER 2. IDEAL FACTORIZATION VIA POLYNOMIALS

2.1. An Ideal Factorization Theorem

We are ready to refine the theory that will be used to determine ideal factorizations in Dedekind D - R constructions. Directly computing the prime factorization of a given ideal can be quite difficult. However, for a given ideal in an appropriately chosen Dedekind domain, there often exists a much simpler polynomial factorization that corresponds to the ideal factorization. Many of the works in the references section also determine ideal factorizations by computing the factorizations of corresponding polynomials; see [3], [4], [1], [5], and [6]. The methods in this paper are most similar to those in [5]. Essentially, the idea is to compute ideal factorizations in $D[\gamma]$ and pass those factorizations on to R.

We begin by defining the conductor ideal, an ideal of great importance in making connections between $D[\gamma]$ and R.

Definition 2.1.1. *Let R be a Dedekind D - R construction. Then the conductor ideal, denoted $\mathfrak{C}$, is defined as*

$$\mathfrak{C} := \{x \in D[\gamma] \mid xR \subseteq D[\gamma]\}$$

We give a series of lemmata that will assist us in proving the ideal factorization theorem.

Lemma 2.1.2. *Let R be a Dedekind D - R construction. The set $\mathfrak{C}$ is an ideal of both $D[\gamma]$ and R. In addition, $\mathfrak{C}D[\gamma] = \mathfrak{C}R$.*

Proof. If $a \in R$, $b \in R$ and $x \in \mathfrak{C}$, then certainly $xab \in D[\gamma]$. So $\mathfrak{C}$ is an ideal of both $D[\gamma]$ and R. Also, since $x \in \mathfrak{C}R$ implies $x \in D[\gamma]$ and $x \in \mathfrak{C}R$ implies $x \in \mathfrak{C}$, we have

the relationship $\mathfrak{C}R \subseteq \mathfrak{C}D[\gamma] \subseteq \mathfrak{C}R$. Hence the subsets above are equalities, and we have our result.

□

Lemma 2.1.3. *Let R be a Dedekind D - R construction. Let $T \in \{D[\gamma], R\}$. Define $\mathfrak{G}(T) := \{I \subseteq T \mid I$ is a nonzero ideal of T and $IT + \mathfrak{C}T = T\}$. Then the mapping $\tau : \mathfrak{G}(D[\gamma]) \to \mathfrak{G}(R)$ defined by $\tau(I) = IR$ is an isomorphism of commutative multiplicative monoids.*

Proof. The fact that $\mathfrak{G}(D[\gamma])$ and $\mathfrak{G}(R)$ are commutative multiplicative monoids follows if we define the binary operation to be ideal multiplication with identity element $D[\gamma]$. We show that τ is an isomorphism. Let $I \in \mathfrak{G}(D[\gamma])$. Then $R = RD[\gamma] = R(D[\gamma]I + D[\gamma]\mathfrak{C}) = RI + R\mathfrak{C} = \tau(I) + R\mathfrak{C}$. This shows that the image of τ is contained in $\mathfrak{G}(R)$. We know τ is a homomorphism because for $I \in D[\gamma]$ and $J \in D[\gamma]$ we have $\tau(IJ) = RIJ = RIRJ = \tau(I)\tau(J)$. We next show that τ is injective. Let $I \in \mathfrak{G}(D[\gamma])$. Then $I = I + IR\mathfrak{C} = I + IR \cap \mathfrak{C}R = IR \cap (I + \mathfrak{C}R) = IR \cap (I + \mathfrak{C}D[\gamma]) = IR \cap D[\gamma]$. The equality $IR \cap (I + \mathfrak{C}R) = IR \cap (I + \mathfrak{C}D[\gamma])$ is due to Lemma 2.1.2. The equality $I + IR\mathfrak{C} = I + IR \cap \mathfrak{C}R$ holds because $IR\mathfrak{C} = IR \cap \mathfrak{C}R$. To see this, let $x \in IR \cap \mathfrak{C}R$. Since $ID[\gamma] + \mathfrak{C}D[\gamma] = D[\gamma]$, there exist $a \in IR$ and $b \in \mathfrak{C}R$ such that $a + b = 1$. Thus $x = xa + xb \in IR\mathfrak{C}$. We have shown that $IR \cap \mathfrak{C}R \subseteq IR\mathfrak{C}$. The reverse containment is always true, so we have $IR\mathfrak{C} = IR \cap \mathfrak{C}R$ as desired. Hence, if $I \in \mathfrak{G}(D[\gamma])$ and $J \in \mathfrak{G}(D[\gamma])$ such that $\tau(I) = RI = RJ = \tau(J)$, then $I = RI \cap D[\gamma] = RJ \cap D[\gamma] = J$. This proves that τ is injective. We show τ is surjective. Let $J \in \mathfrak{G}(R)$ and let $I = RJ \cap D[\gamma]$. Then $R = RJ + R\mathfrak{C}$ implies $D[\gamma] = R \cap D[\gamma] = RJ \cap D[\gamma] + R\mathfrak{C} \cap D[\gamma] = RJ \cap D[\gamma] + \mathfrak{C}D[\gamma]$. So $I \in \mathfrak{G}(D[\gamma])$. In addition, $\tau(I) = RI = (RJ + R\mathfrak{C})RI = RJI + R\mathfrak{C}I = RJI + D[\gamma]\mathfrak{C}I = RJI + D[\gamma]\mathfrak{C} \cap I = RJI + (D[\gamma]\mathfrak{C} \cap D[\gamma]) \cap RJ = RJI + D[\gamma]\mathfrak{C} \cap RJ = RJI + R\mathfrak{C} \cap RJ = RJI + R\mathfrak{C}J = RJ(I + R\mathfrak{C}) = RJ(I + D[\gamma]\mathfrak{C}) = RJD[\gamma] = RJ$. So τ is surjective.

Since τ is surjective and injective, we have our result.

□

Lemma 2.1.4. *Let R be a Dedekind D - R construction. Let $I \in \mathfrak{G}(R)$. Then $R/I \cong D[\gamma]/(D[\gamma] \cap I)$.*

Proof. Consider the map $\mu : D[\gamma] \to R/I$ defined by $\mu(a) = a + I$ for $a \in D[\gamma]$. We need to show that μ is a surjective homomorphism with kernel $D[\gamma] \cap I$. The fact the μ is a well-defined homomorphism follows because μ is a residue class mapping. All of the elements $a \in D[\gamma]$ such that $a \in I$ are precisely the elements such that $a + I = 0$. Therefore, the kernel of μ is $D[\gamma] \cap I$. Now we show μ is surjective. Let $r \in R$. Because of Lemma 2.1.2 and the equation $RI + R\mathfrak{C} = R$, we have $RI + D[\gamma]\mathfrak{C} = R$. So there exists $b \in I$ and $c \in D[\gamma]\mathfrak{C}$ such that $b + c = r$. Then since $c \in D[\gamma]$ such that $c = r - b$ we have $\mu(c) = r - b + I = r + I$. This justifies that μ is surjective and by the ring isomorphism theorem $R/I \cong D[\gamma]/(D[\gamma] \cap I)$.

□

Lemma 2.1.5. *Let R be a Dedekind D - R construction. Let $J \in \mathfrak{G}(D[\gamma])$. Then B is a maximal ideal of $D[\gamma]$ containing J if and only if RB is a maximal ideal of R containing RJ.*

Proof. By Lemma 2.1.3, we know that $RJ \in \mathfrak{G}(R)$. Let M be a maximal ideal of R that contains RJ. Notice that because M contains RJ, we have $R = RJ + R\mathfrak{C} \subseteq M + R\mathfrak{C} \subseteq R$. All of the subsets are actually equalities, so $M \in \mathfrak{G}(R)$. We claim that $B = M \cap D[\gamma]$ is a maximal ideal of $D[\gamma]$ containing J such that $RB = M$. The relation $RJ \subseteq M$ implies $J \subseteq RJ \cap D[\gamma] \subseteq M \cap D[\gamma] = B$. In particular, we have $J \subseteq B$. Because M is a maximal ideal, R/M is a field. Also, by Lemma 2.1.4 we have $R/M \cong D[\gamma]/B$, so $D[\gamma]/B$ is also a field. Hence B is a maximal ideal of $D[\gamma]$. The properties $J \subseteq B$ and $J \in \mathfrak{G}(D[\gamma])$ justify that $D[\gamma] = D[\gamma]J + D[\gamma]\mathfrak{C} \subseteq B + D[\gamma]\mathfrak{C} \subseteq$

$D[\gamma]$. All subsets must be equalities, so $B \in \mathfrak{G}(D[\gamma])$. Thus by Lemma 2.1.3, we have $RB = M$ which proves our claim, and thereby we have the "only if" condition of the lemma. For the "if" condition, let B be a maximal ideal of $D[\gamma]$ containing J. We have already seen that $J \subseteq B$ and $J \in \mathfrak{G}(D[\gamma])$ implies $B \in \mathfrak{G}(D[\gamma])$. By Lemma 2.1.3, we know that $RB \cap D[\gamma] = B$. So we can apply Lemma 2.1.4 to conclude that RB is a maximal ideal of R. Since also $J \subseteq B$ implies $RJ \subseteq RB$, we have our result.

□

Lemma 2.1.6. *Let D be an integral domain and let $\mathfrak{p}$ be a maximal ideal of D. Let H be a multiplicatively closed set such that $1 \in H \subseteq D \setminus \mathfrak{p}$, and let $D_H := \left\{\frac{d}{s} \mid d \in D, s \in H\right\}$. Then $D_H/\mathfrak{p}D_H \cong D/\mathfrak{p}$.*

Proof. Define the map $\phi : D \to D_H/\mathfrak{p}D_H$ by $\phi(d) = \frac{d}{1} + \mathfrak{p}D_H$ for any $d \in D$. We know that ϕ is a well-defined homomorphism because the maps $d \mapsto \frac{d}{1}$ and $\frac{d}{1} \mapsto \frac{d}{1} + \mathfrak{p}D_H$ are well-defined homomorphisms. Any element $\frac{d}{1} \in D_H$ is also an element of $\mathfrak{p}D_H$ if and only if $d \in \mathfrak{p}$, so the kernel of ϕ is $\mathfrak{p}$. We show that ϕ is surjective. To see this, let $\frac{d}{s} + \mathfrak{p}D_H \in D_H/\mathfrak{p}D_H$ where $d \in D$ and $s \in H$. We will find $c \in D$ such that $\phi(c) = \frac{d}{s} + \mathfrak{p}D_H$. Consider the element $s + \mathfrak{p}D \in D/\mathfrak{p}$. Notice that $s \in H \subseteq D \setminus \mathfrak{p}$, so $s \notin \mathfrak{p}$. Because also $D/\mathfrak{p}$ is a field, $s + \mathfrak{p}D$ has an inverse in $D/\mathfrak{p}$. Since the canonical map $D \to D/\mathfrak{p}$ is surjective, we can find $t \in D$ such that the image of t under the canonical map is the inverse of $s + \mathfrak{p}D$. Thus $st + \mathfrak{p}D = 1 + \mathfrak{p}D$. We claim $c = td$ is an element of D such that $\phi(c) = \frac{d}{s} + \mathfrak{p}D_H$. By our choice of t, $1 - ts \in \mathfrak{p}$ hence $d(1 - ts) \in \mathfrak{p}$. Notice that $\frac{d}{s} - \frac{td}{1} = \frac{d-tds}{s} = \frac{d(1-ts)}{s}$, so $\frac{d}{s} - \frac{td}{1} \in \mathfrak{p}D_H$. Therefore, $\phi(td) = \frac{td}{1} + \mathfrak{p}D_H = \frac{d}{s} + \mathfrak{p}D_H$. Because ϕ is a surjective homomorphism with kernel $\mathfrak{p}$, the ring isomorphism theorem proves that $D_H/\mathfrak{p}D_H \cong D/\mathfrak{p}$, as desired.

□

Lemma 2.1.7. *Let R be a Dedekind D - R construction and $\mathfrak{p}$ a nonzero prime ideal of D. Suppose that $\mathfrak{p}R = P_1^{k_1} P_2^{k_2} \dots P_m^{k_m}$. Let $H = D \setminus \mathfrak{p}$ and define the*

set $R_H := \left\{\frac{r}{s} \mid r \in R, s \in H\right\}$. *Let* $[Q(\gamma) : Q] = n$ *and* $[R/P_i : D/\mathfrak{p}] = z_i$. *Then* $z_1k_1 + z_2k_2 + \cdots + z_mk_m = n$.

Proof. As shown in Corollary 1.1.19, $\mathfrak{p}R_H = (P_1R_H)^{k_1}(P_2R_H)^{k_2}\ldots(P_mR_H)^{k_m}$. In Lemma 2.1.6, we showed that $D_\mathfrak{p}/\mathfrak{p}D_\mathfrak{p} \cong D/\mathfrak{p}$. Lemma 2.1.6 shows that $R_H/P_iR_H \cong R/P_i$ as well as long as we verify the hypothesis $H \subseteq R \setminus P_i$. To see this, suppose $h \in H \cap P_i$. Then $h \in D \cap P_i = \mathfrak{p}$, a contradiction of the definition of H. Thus $h \in H$ implies $h \notin P_i$, and $H \subseteq R \setminus P_i$ holds. The isomorphisms $D_\mathfrak{p}/\mathfrak{p}D_\mathfrak{p} \cong D/\mathfrak{p}$ and $R_H/P_iR_H \cong R/P_i$ show that $[R_H/P_iR_H : D_\mathfrak{p}/\mathfrak{p}D_\mathfrak{p}] = z_i$, so it suffices to prove this lemma for the rings R_H and $D_\mathfrak{p}$. We note that R_H is finitely generated as a $D_\mathfrak{p}$ module. To see this, replace D with $D_\mathfrak{p}$ and R with R_H in Lemma 1.4.6. As a result, $R_H = r_1D_\mathfrak{p} + r_2D_\mathfrak{p} + \cdots + r_nD_\mathfrak{p}$ where $r_i \in R_H$ for each i. We show that R_H has a finite free $D_\mathfrak{p}$-module basis by induction on n. If $n = 1$, the result is obvious. Assume that R_H has a finite free $D_\mathfrak{p}$-module basis for all $n \leq z$. Now let $n = z + 1$; that is, $R_H = r_1D_\mathfrak{p} + r_2D_\mathfrak{p} + \cdots + r_{z+1}D_\mathfrak{p}$. For all $r \in R_H$, define the annihilator $Ann(r) = \{d \in D_\mathfrak{p} \mid dr = 0\}$. It is a well-known fact that $Ann(r)$ is a proper ideal of $D_\mathfrak{p}$. Let $S = \{Ann(r) \mid r$ is one of a set of $z + 1$ generators of $R_H\}$. Because the ideals of a discrete valuation domain are totally ordered with respect to containment, S has a maximal element, say $Ann(x_1)$. By definition, x_1 is part of a set of $z + 1$ generators for R_H, say $R_H = x_1D_\mathfrak{p} + x_2D_\mathfrak{p} + x_3D_\mathfrak{p} + \cdots + x_{z+1}D_\mathfrak{p}$. Let $\{d_1, d_2, \ldots, d_{z+1}\}$ be a subset of $D_\mathfrak{p}$ such that $x_1d_1 + x_2d_2 + \cdots + x_{z+1}d_{z+1} = 0$. We show that $d_1x_1 = 0$. Assume not; then $d_1 \notin Ann(x_1)$. Every ideal of the discrete valuation domain $D_\mathfrak{p}$ is principal, so we can write $Ann(x_1) = (t)$ where $t \in D_\mathfrak{p}$. Because $D_\mathfrak{p}$ is a valuation domain, either d_1 divides t or t divides d_1. If t divides d_1, then $d_1 = ta$ where $a \in D_\mathfrak{p}$. As a result, $d_1x_1 = tax_1 = 0$, a contradiction. So we can write $t = d_1b$ for $b \in D_\mathfrak{p}$. Therefore, $(d_1) \supsetneq (t)$. The total ordering of the ideals of $D_\mathfrak{p}$ implies that we can find a permutation σ on the set $\{1.2, \ldots, z + 1\}$ such that

$(d_{\sigma(1)}) \supseteq (d_{\sigma(2)}) \supseteq \cdots \supseteq (d_{\sigma(z+1)})$. Thus for all i such that $2 \leq i \leq z+1$, we can write $d_{\sigma(i)} = y_i d_{\sigma(1)}$ for some $y_i \in D_{\mathfrak{p}}$. Let $c = x_{\sigma(1)} + y_2 x_{\sigma(2)} + y_3 x_{\sigma(3)} + \cdots + y_{z+1} x_{\sigma(z+1)}$. Notice that the set $T = \left\{c, x_{\sigma(2)}, x_{\sigma(3)}, \ldots, x_{\sigma(z+1)}\right\}$ generates R_H. This is due to the fact that the elements of T generate $\{x_1, x_2, \ldots, x_{z+1}\}$, which generates R_H by assumption. Clearly T generates $x_{\sigma(j)}$ for $j \geq 2$. To see why T generates $x_{\sigma(1)}$, appeal to the equation $c - y_2 x_{\sigma(2)} - y_3 x_{\sigma(3)} - \cdots - y_{z+1} x_{\sigma(z+1)} = x_{\sigma(1)}$. So T generates R_H as claimed. Also, we have $d_{\sigma(1)} c = x_1 d_1 + x_2 d_2 + \cdots + x_{z+1} d_{z+1} = 0$. Therefore, $Ann(c) \supseteq (d_{\sigma(1)}) \supseteq (d_1) \supsetneq Ann(x_1)$. This is a contradiction of the definition of $Ann(x_1)$. Hence $d_1 x_1 = 0$. Since we have shown that $x_1 d_1 + x_2 d_2 + \cdots + x_{z+1} d_{z+1} = 0$ implies $d_1 x_1 = 0$, we know that $R_H = x_1 D_{\mathfrak{p}} \oplus (x_2 D_{\mathfrak{p}} + x_3 D_{\mathfrak{p}} + \cdots + x_{z+1} D_{\mathfrak{p}})$. Our induction hypothesis states that $M = x_2 D_{\mathfrak{p}} + x_3 D_{\mathfrak{p}} + \cdots + x_{z+1} D_{\mathfrak{p}}$ has a finite free basis over $D_{\mathfrak{p}}$, hence so does $x_1 D_{\mathfrak{p}} \oplus M = R_H$. So we have the representation $R_H = v_1 D_{\mathfrak{p}} \oplus v_2 D_{\mathfrak{p}} \oplus \cdots \oplus v_u D_{\mathfrak{p}}$ where $v_i \in R_H$ and u is some positive integer. Let N be the set of nonzero elements of $D_{\mathfrak{p}}$. Define the set $(R_H)_N = \left\{\frac{x}{y} \mid x \in R_H, y \in N\right\}$. We show $(R_H)_N = Q(\gamma)$. Apply Lemma 1.1.17, replacing $\mathfrak{p}$ with (0) and H with $N = D_{\mathfrak{p}} \setminus (0)$. We see that $(R_H)_N$ is the integral closure of Q in $Q(\gamma)$, hence $(R_H)_N = Q(\gamma)$ as claimed. The previous two claims combine to give $Q(\gamma) = (R_H)_N = (v_1 D_{\mathfrak{p}} \oplus v_2 D_{\mathfrak{p}} \oplus \cdots \oplus v_u D_{\mathfrak{p}})_N = v_1 Q \oplus v_2 Q \oplus \cdots \oplus v_u Q$. This means that $\{v_1, v_2, \ldots, v_u\}$ is a basis for $Q(\gamma)$ over Q, which implies $u = n$. Choose i such that $1 \leq i \leq m$. We will show $\left[R_H / R_H P_i^{k_i} : D_{\mathfrak{p}} / \mathfrak{p} D_{\mathfrak{p}}\right] = z_i k_i$. Notice that there are no ideals of R_H that properly contain $R_H P_i^{j+1}$ and are properly contained in $R_H P_i^j$. Therefore, $R_H P_i^j / R_H P_i^{j+1}$ is a one dimensional vector space over $R_H / R_H P_i$. Hence $\left[R_H P_i^j / R_H P_i^{j+1} : D_{\mathfrak{p}} / \mathfrak{p} D_{\mathfrak{p}}\right] = \left[R_H P_i^j / R_H P_i^{j+1} : R_H / R_H P_i\right] \left[R_H / R_H P_i : D_{\mathfrak{p}} / \mathfrak{p} D_{\mathfrak{p}}\right] = z_i$ for any positive integer j. Because of the relationship $D_{\mathfrak{p}} / \mathfrak{p} D_{\mathfrak{p}} \subseteq R_H / \mathfrak{p} R_H \subseteq R_H / R_H P_i^{k_i}$, we can think of $R_H / R_H P_i^{k_i}$ as a vector space over $D_{\mathfrak{p}} / \mathfrak{p} D_{\mathfrak{p}}$. Thus, we can construct the decreasing chain of subspaces $R_H / R_H P_i^{k_i} \supsetneq R_H P_i / R_H P_i^{k_i} \supsetneq$

$R_H P_i^2/R_H P_i^{k_i} \supsetneq \cdots \supsetneq R_H P_i^{k_i}/R_H P_i^{k_i}$. The corresponding factor spaces are isomorphic to $R_H/R_H P_i, R_H P_i/R_H P_i^2, \ldots, R_H P_i^{k_i-1}/R_H P_i^{k_i}$. So the dimension

$$\left[R_H/R_H P_i^{k_i} : D_\mathfrak{p}/\mathfrak{p}D_\mathfrak{p}\right] = \sum_{j=1}^{k_i} \left[R_H P_i^{j-1}/R_H P_i^j : D_\mathfrak{p}/\mathfrak{p}D_\mathfrak{p}\right] = k_i z_i$$

By the Chinese Remainder Theorem, $R_H/\mathfrak{p}R_H \cong R_H/R_H P_1^{k_1} \oplus R_H/R_H P_2^{k_2} \oplus \cdots \oplus R_H/R_H P_m^{k_m}$. Combining this with the previous claim gives

$$[R_H/\mathfrak{p}R_H : D_\mathfrak{p}/\mathfrak{p}D_\mathfrak{p}] = k_1 z_1 + k_2 z_2 + \cdots + k_m z_m$$

We have already seen that $R_H = v_1 D_\mathfrak{p} \oplus v_2 D_\mathfrak{p} \oplus \cdots \oplus v_n D_\mathfrak{p}$. Because $\mathfrak{p}D_\mathfrak{p}$ is principal, we have $\mathfrak{p}R_H = v_1\mathfrak{p}D_\mathfrak{p} \oplus v_2\mathfrak{p}D_\mathfrak{p} \oplus \cdots \oplus v_n\mathfrak{p}D_\mathfrak{p}$ and $R_H/\mathfrak{p}R_H \cong v_1 D_\mathfrak{p}/v_1\mathfrak{p}D_\mathfrak{p} \oplus v_2 D_\mathfrak{p}/v_2\mathfrak{p}D_\mathfrak{p} \oplus \cdots \oplus v_n D_\mathfrak{p}/v_n\mathfrak{p}D_\mathfrak{p}$. The vector spaces $v_i D_\mathfrak{p}/v_i\mathfrak{p}D_\mathfrak{p}$ are one dimensional over $D_\mathfrak{p}/\mathfrak{p}D_\mathfrak{p}$, so we have $[R_H/\mathfrak{p}R_H : D_\mathfrak{p}/\mathfrak{p}D_\mathfrak{p}] = n$. Therefore, $k_1 z_1 + k_2 z_2 + \cdots + k_m z_m = [R_H/\mathfrak{p}R_H : D_\mathfrak{p}/\mathfrak{p}D_\mathfrak{p}] = n$, which gives the desired result.

□

We now prove the main theorem of this section.

Theorem 2.1.8. *Let R be a Dedekind D - R construction. Let $f(t) \in D[t]$ be a minimal polynomial for γ, so the degree of $f(t)$ is n. Let $\mathfrak{p}$ be a nonzero prime ideal in D such that $\mathfrak{p}R + \mathfrak{C} = R$. Let $\bar{*}$ denote the image of $*$ under the canonical map that reduces coefficients of polynomials in $D[t]$ modulo $\mathfrak{p}$. Let $\bar{f}(t) = f_1(t)^{k_1} f_2(t)^{k_2} \ldots f_m(t)^{k_m}$ be the factorization of $\bar{f}(t)$ into distinct irreducibles f_i in $\bar{D}[t]$. Then in R we have the factorization $\mathfrak{p}R = P_1^{k_1} P_2^{k_2} \ldots P_m^{k_m}$ where $P_i = f_i(\gamma)R + \mathfrak{p}R$.*

Proof. We proceed by showing that $D[\gamma]/\mathfrak{p} \cong \bar{D}[t]/\bar{f}(t)$. We do this by showing that the mapping $\phi : D[\gamma] \to \bar{D}[t]/\bar{f}(t)$ defined by $\phi(g(\gamma)) = \bar{g}(t) + \bar{f}(t)\bar{D}[t]$ is a surjective homomorphism with kernel $\mathfrak{p}$. First, we justify that ϕ is well-defined. Let $g_1(t), g_2(t)$

be polynomials in $D[t]$ such that $g_1(\gamma) = g_2(\gamma)$. Then γ is a root of $g_1(t) - g_2(t)$. Since $f(t)$ is the minimal polynomial for γ, we know that $g_1(t) - g_2(t) = f(t)h(t)$ for some polynomial $h(t) \in D[t]$. Reducing modulo $\mathfrak{p}$ yields $\bar{g_1}(t) - \bar{g_2}(t) = \bar{f}(t)\bar{h}(t)$. Reducing modulo $\bar{f}(t)$ yields $\bar{g_1}(t) \equiv \bar{g_2}(t) \bmod \bar{f}(t)$. This shows that ϕ is well-defined. To see why ϕ is a homomorphism, let $g(\gamma), h(\gamma) \in D[\gamma]$. Then $\phi(g(\gamma)h(\gamma)) = \bar{g}(t)\bar{h}(t) + \bar{f}(t)\bar{D}[t] = (\bar{g}(t) + \bar{f}(t)\bar{D}[t])(\bar{h}(t) + \bar{f}(t)\bar{D}[t]) = \phi(g(\gamma))\phi(h(\gamma))$. To see why the kernel of ϕ is $\mathfrak{p}$, suppose $g(\gamma)$ is in the kernel of ϕ. Then $\bar{g}(t) = \bar{f}(t)\bar{h}(t)$. This means that $g(t) = f(t)h(t) + m(t)$ where $m(t)$ is in $\mathfrak{p}$. Plugging γ in for t yields $g(\gamma) = m(\gamma)$ because by assumption $f(\gamma) = 0$. But then $g(\gamma)$ is also in $\mathfrak{p}$. This proves that the kernel of ϕ is contained in $\mathfrak{p}$. The fact that $\mathfrak{p}$ is contained in the kernel of ϕ follows directly from the fact that ϕ reduces the coefficients of the polynomials modulo $\mathfrak{p}$. So we know that the kernel of ϕ is $\mathfrak{p}$. Lastly, we show that ϕ is surjective. This is true because the canonical map $\bar{g}(t) \mapsto \bar{g}(t) + \bar{f}(t)\bar{D}[t]$ is surjective. Similarly, the map $g(t) \mapsto \bar{g}(t)$ is surjective. Thus we choose $g(t)$ such that $g(t) \mapsto \bar{g}(t) + \bar{f}(t)\bar{D}[t]$ under the composition of these canonical maps and we get $\phi(g(\gamma)) = \bar{g}(t) + \bar{f}(t)\bar{D}[t]$. This justifies that ϕ is surjective. By the ring isomorphism theorem, we have $D[\gamma]/\mathfrak{p} \cong \bar{D}[t]/\bar{f}(t)$. In fact, we know the isomorphism between these rings is given by $\psi(g(\gamma) + \mathfrak{p}D[\gamma]) = \bar{g}(t) + \bar{f}(t)\bar{D}[t]$. Since D is a Dedekind domain and $\mathfrak{p}$ is a nonzero prime, $\mathfrak{p}$ is maximal. This means $D/\mathfrak{p}$ is a field, hence $\bar{D}[t]$ is a principal ideal domain. Therefore, the prime ideals containing $\bar{f}(t)$ in $\bar{D}[t]$ are precisely the ideals generated by the irreducible divisors of $\bar{f}(t)$, namely the polynomials $f_i(t)$ where $1 \leq i \leq m$. Consequently, the only nonzero prime ideals of $\bar{D}[t]/\bar{f}(t)$ are those generated by $f_i(t) + \bar{f}(t)\bar{D}[t]$. Because the ideals $f_i(t) + \bar{f}(t)\bar{D}[t]$ are principally generated by an irreducible element, they are, in fact, maximal. Also, because ψ is an isomorphism, all maximal ideals of $D[\gamma]/\mathfrak{p}$ are generated by the elements $\psi^{-1}(f_i(t) + \bar{f}(t)\bar{D}[t]) = f_i(\gamma) + \mathfrak{p}D[\gamma]$. Thus, the maximal ideals in $D[\gamma]$

containing $\mathfrak{p}$ are of the form $f_i(\gamma)D[\gamma] + \mathfrak{p}D[\gamma]$. By Lemma 2.1.5, the maximal ideals in R containing $\mathfrak{p}R$ are similarly given by $P_i = f_i(\gamma)R + \mathfrak{p}R$.

Because R is a Dedekind domain, $\mathfrak{p}R$ factors uniquely into a product of powers of the maximal ideals that contain $\mathfrak{p}R$. So we have $\mathfrak{p}R = P_1^{j_1}P_2^{j_2}\dots P_m^{j_m}$. We need to show that $j_i = k_i$ for all $1 \leq i \leq m$. First we show $j_i \leq k_i$. Notice that $P_1^{k_1}P_2^{k_2}\dots P_m^{k_m} = (f_1(\gamma)R + \mathfrak{p}R)^{k_1}(f_2(\gamma)R + \mathfrak{p}R)^{k_2}\dots(f_m(\gamma)R + \mathfrak{p}R)^{k_m} \subseteq f_1(\gamma)^{k_1}f_2(\gamma)^{k_2}\dots f_m(\gamma)^{k_m}R + \mathfrak{p}R = \bar{f}(\gamma) + \mathfrak{p}R = \mathfrak{p}R = P_1^{j_1}P_2^{j_2}\dots P_m^{j_m}$. This means $P_i^{k_i} \subseteq P_i^{j_i}$ for each i, which justifies $j_i \leq k_i$. Next, we need to show that $deg(f_i) = [R/P_i : D/\mathfrak{p}]$ for each i. Consider the mapping $\zeta : (D/\mathfrak{p})[x] \to R/P_i$ defined by $\zeta(g(x)) = g(\gamma) + P_i$. Note that this definition makes sense because $g(\gamma) \in (D/\mathfrak{p})[\gamma] \subseteq R$. We will show that ζ is a surjective homomorphism of vector spaces over $D/\mathfrak{p}$, the kernel of which is the ideal (f_i). By the ring isomorphism theorem we will have $(D/\mathfrak{p})[x]/(f_i) \cong R/P_i$, which gives the desired result. The reason why ζ is well-defined is because the maps $g(x) \mapsto g(\gamma)$ and $g(\gamma) \mapsto g(\gamma)+P_i$ are well-defined. We know ζ is a homomorphism because $\zeta(g_1(x)g_2(x)) = g_1(\gamma)g_2(\gamma) + P_i = (g_1(\gamma) + P_i)(g_2(\gamma) + P_i) = \zeta(g_1(x))\zeta(g_2(x))$. To see that ζ is a vector space homomorphism, notice that for $c \in D/\mathfrak{p}$, we have $c\zeta(g(x)) = c(g(\gamma) + P_i) = cg(\gamma) + P_i = \zeta(cg(x))$. The surjectivity of ζ is guaranteed by the following argument: Recall that $\mathfrak{p}R + \mathfrak{C} = R$. This means that there exist $\alpha \in \mathfrak{C}$ and $\beta \in \mathfrak{p}R$ such that $\alpha + \beta = 1 \in R$. Let $r \in R$ be arbitrary. Then $r = \alpha r + \beta r$. Notice by definition of $\mathfrak{C}$ that $\alpha r \in D[\gamma]$, so let $\alpha r = h(\gamma) \in D[\gamma]$. Then $\zeta(\bar{h}(x)) = \bar{h}(\gamma) + P_i = \bar{\alpha}\bar{r} + P_i = \bar{r} - \bar{\beta}\bar{r} + P_i = \bar{r} + P_i$. The last equality holds because $\beta r \in \mathfrak{p}R$. All that is left is to justify that every element of R/P_i is of the form $\bar{r} + P_i$. This is because $\mathfrak{p}R \subseteq P_i$. So ζ is onto. We now determine the kernel of ζ. Clearly the kernel of ζ is a proper ideal of $(D/\mathfrak{p})[x]$. Because $P_i = f_i(\gamma)R + \mathfrak{p}R$, certainly $f_i(\gamma) \in P_i$, which implies that $f_i(x)(D/\mathfrak{p})[x]$ is contained in the kernel of ζ. Also, since $f_i(x)$ is irreducible by assumption and $(D/\mathfrak{p})[x]$ is a principal

ideal domain, $f_i(x)(D/\mathfrak{p})[x]$ is in fact maximal, contradicting that $f_i(x)(D/\mathfrak{p})[x]$ is properly contained in the kernel of ζ. Thus the kernel of ζ is $f_i(x)(D/\mathfrak{p})[x]$. We have justified that $(D/\mathfrak{p})[x]/(f_i)$ and R/P_i are isomorphic as vector spaces over $D/\mathfrak{p}$. Therefore, $deg(f_i) = dim((D/\mathfrak{p})[x]/(f_i)) = dim(R/P_i) = [R/P_i : D/\mathfrak{p}]$. From Lemma 2.1.7 we know that $j_1 [R/P_1 : D/\mathfrak{p}] + j_2 [R/P_2 : D/\mathfrak{p}] + \cdots + j_m [R/P_m : D/\mathfrak{p}] = n$. Combining the last few results, we have $n = deg(f) = deg(f_1)k_1 + deg(f_2)k_2 + \cdots + deg(f_m)k_m = [R/P_1 : D/\mathfrak{p}]\, k_1 + [R/P_2 : D/\mathfrak{p}]\, k_2 + \cdots + [R/P_m : D/\mathfrak{p}]\, k_m \geq [R/P_1 : D/\mathfrak{p}]\, j_1 + [R/P_2 : D/\mathfrak{p}]\, j_2 + \cdots + [R/P_m : D/\mathfrak{p}]\, j_m = n$. Consequently, the inequality is an equality and we have

$$\sum_{b=1}^{m} [R/P_b : D/\mathfrak{p}]\, k_b = \sum_{b=1}^{m} [R/P_b : D/\mathfrak{p}]\, j_b$$

Combining this statement with $1 \leq j_i \leq k_i$ gives $j_i = k_i$ as desired.

□

The following example illustrates Theorem 2.1.8. This example is especially interesting because $D/\mathfrak{p}$ has infinite cardinality. In algebraic number theory, it is often assumed that $D/\mathfrak{p}$ has finite cardinality. The following example demonstrates why this is not necessary.

Example 2.1.9. *Let A be the integral closure of $\mathbb{Q}[x]$ in $\mathbb{Q}(x)(\alpha)$ where α is a root of the polynomial $f(t) = t^3 - xt + x$. Notice that $f(t)$ is irreducible by Eisenstein's Criterion. We will determine the factorizations of a few prime ideals from $\mathbb{Q}[x]$ in A. In the following section, we will discuss ways of satisfying or avoiding the hypothesis $\mathfrak{p}A + \mathfrak{C} = A$. For now, we simply consider the connection between the polynomial factorizations and the ideal factorizations. Let $\mathfrak{q} = (x-8)\mathbb{Q}[x]$. Then $f(t) = t^3 - xt + x \equiv t^3 - 8t + 8 \equiv (t-2)(t^2+2t-4) \pmod{\mathfrak{q}}$. This suggests that $\mathfrak{q}A = (x-8, \alpha-2)(x-8, \alpha^2+2\alpha-4)A$. Let $\mathfrak{m} = (x-2)\mathbb{Q}[x]$. Then $f(t) =$*

$t^3-xt+x \equiv t^3-2t+2 \pmod{\mathfrak{m}}$, *which is irreducible. This suggests that* $\mathfrak{m}A$ *is prime. Let* $\mathfrak{n} = (-4x+27)\mathbb{Q}[x]$. *For ease of computation, we will factor the polynomial* $4f(t) = g(t) = 4t^3 - 4xt + 4x$. *There is no harm in doing this because* $g(t)$ *is a unit multiple of* $f(t)$. *We factor* $g(t)$ *to get* $4t^3-4xt+4x \equiv 4t^3-27t+27 \equiv (t+3)(2t-3)^2 \pmod{\mathfrak{n}}$. *So we suspect that* $\mathfrak{n}A = (-4x+27, \alpha+3)(-4x+27, 2\alpha-3)^2 A$. *All three of the above suggested factorizations turn out to be true; see Example* 2.2.4 *for details.*

We conclude this section with a discussion on obstructions to applying Theorem 2.1.8 when D is not Dedekind. Let $D = \mathbb{Q}[x, y]$. Notice that $\mathbb{Q}[x, y]$ has prime ideals that are not maximal, for example $x\mathbb{Q}[x, y]$ and $y\mathbb{Q}[x, y]$. Theorem 2.1.8 relies on the fact that $D/\mathfrak{p}$ is a field, which would not be true if $\mathfrak{p}$ were not maximal. So we attempt to apply Theorem 2.1.8 in the case where $\mathfrak{p}$ is maximal. This will still create problems. Let R be the integral closure of $\mathbb{Q}[x, y]$ in $\mathbb{Q}(x, y, \sqrt{x})$. The ring R is not Dedekind because yR and $\sqrt{x}R$ are prime ideals that are not maximal. As a result, ideals of R do not necessarily factor uniquely into a product of prime ideals. For example, Theorem 2.1.8 would seem to indicate that $(x, y)R = (\sqrt{x}, y)(\sqrt{x}, y)R$, which is clearly false. It is likely that $(x, y)R$ does not have a unique factorization into prime ideals, which would only add emphasis to the point that we cannot expect to apply Theorem 2.1.8 in this case.

2.2. The Condition $\mathfrak{p}R + \mathfrak{C} = R$

The condition $\mathfrak{p}R + \mathfrak{C} = R$ arises as a stumbling block in many attempts to factor ideals in a Dedekind D - R construction. It deserves mention that there are situations where it is impossible to work around the condition $\mathfrak{p}R + \mathfrak{C} = R$; see [3] for an example. The methods of [6] tackle this problem because they do not rely on $\mathfrak{p}R + \mathfrak{C} = R$. For the purposes of this paper, we will either ensure that $\mathfrak{p}R + \mathfrak{C} = R$ holds or work around the situations where it does not hold as in [5]. This will suffice because for the Dedekind D - R constructions that we are interested in either $\mathfrak{p}$

satisfies $\mathfrak{p}R + \mathfrak{C} = R$ or $\mathfrak{p}R$ has a straightforward factorization.

One way to ensure that $\mathfrak{p}R + \mathfrak{C} = R$ holds is to choose γ such that $R = D[\gamma]$. If such a γ exists, then a basis for R over D is given by powers of γ. In this case, we say that R has a power basis over D. Notice that $D[\gamma] = R$ implies $\mathfrak{C} = R$, hence $\mathfrak{p}R + \mathfrak{C} = R$ for all primes $\mathfrak{p} \in D$. We use this fact to justify our statements in Example 1.4.5.

Example 2.2.1. *Return to the situation of Example* 1.4.5 *where* $D = \mathbb{Z}$ *and* $R = \mathbb{Z}\left[\sqrt{-5}\right]$. *The comments in the previous paragraph and Theorem* 2.1.8 *show that the factorization of* $\mathfrak{p}\mathbb{Z}\left[\sqrt{-5}\right]$ *is determined by the factorization of* $f(t) = t^2 + 5$ *as an element of* $(\mathbb{Z}/\mathfrak{p})\left[\sqrt{-5}\right]$. *If* $\mathfrak{p} = 5\mathbb{Z}$, *then* $\bar{f}(t) = t^2$. *This implies that* $(5) = (\sqrt{-5})^2$ *as an ideal of* $\mathbb{Z}\left[\sqrt{-5}\right]$. *When* $\mathfrak{p} = 2\mathbb{Z}$, *then* $\bar{f}(t) = t^2 + 1 \equiv (t+1)^2 \pmod 2$. *Thus* $(2) = (2, \sqrt{-5}+1)^2$ *in* $\mathbb{Z}\left[\sqrt{-5}\right]$. *For* $\mathfrak{p} = 3\mathbb{Z}$, $\bar{f}(t) = t^2 + 2 \equiv (t+1)(t+2) \pmod 3$. *Thus* $(3) = (3, \sqrt{-5}+1)(3, \sqrt{-5}+2)$ *in* $\mathbb{Z}\left[\sqrt{-5}\right]$. *Similarly, with* $\mathfrak{p} = 7\mathbb{Z}$, $\bar{f}(t) = t^2+5 \equiv (t+3)(t+4) \pmod 7$, *which justifies* $(7) = (7, \sqrt{-5}+3)(7, \sqrt{-5}+4)$. *We omit the computations required to show that* $t^2 + 5$ *is irreducible modulo 11. However, assuming that this is true, we obtain that* (11) *remains prime in* $\mathbb{Z}\left[\sqrt{-5}\right]$.

The following lemmata will help us detect primes that satisfy the condition $\mathfrak{p}R + \mathfrak{C} = R$ even when R does not have a power basis over D.

Lemma 2.2.2. *Let* R *be a Dedekind* D *-* R *construction and* $\mathfrak{p}$ *a nonzero prime ideal of* D. *Let* $d \in D \setminus \mathfrak{p}$ *such that* $dR \subseteq \mathfrak{C}$. *Then* $\mathfrak{p}$ *satisfies* $\mathfrak{p}R + \mathfrak{C} = R$.

Proof. The assumption that D is a Dedekind domain implies $\mathfrak{p}D$ is maximal. Since dD is a nonzero ideal that is not contained in $\mathfrak{p}D$, we have $\mathfrak{p}D \subsetneq \mathfrak{p}D + dD$, which implies $\mathfrak{p}D + dD = D$. Since $D \subseteq R$ this relationship also takes place in R; that is, $\mathfrak{p}DR + dDR = DR = R$ where the last equality is valid because D and R share the same element 1. Consequently, $R \supseteq \mathfrak{p}R + \mathfrak{C} \supseteq \mathfrak{p}R + dR = R$. All subsets must be equalities, so we have our result.

□

Lemma 2.2.3. *Let R be a Dedekind D - R construction, $f(t) \in D[t]$ a minimal polynomial for γ, and $\mathfrak{p}$ a nonzero prime ideal of D. Let $d(f)$ denote the discriminant of the polynomial $f(t)$. If $d(f)$ is not in $\mathfrak{p}$, then $\mathfrak{p}$ satisfies $\mathfrak{p}R + \mathfrak{C} = R$.*

Proof. By Lemma 1.4.6, $d(f)R \subseteq E \subseteq D[\gamma]$. This implies by definition of $\mathfrak{C}$ that $d(f)R \subseteq \mathfrak{C}$. By Lemma 2.2.2, we have our result.

□

Example 2.2.4. *Return to Example 2.1.9 where A is the integral closure of $\mathbb{Q}[x]$ in $\mathbb{Q}(x)(\alpha)$ such that α is a root of the polynomial $f(t) = t^3 - xt + x$. Let $\mathfrak{q} = (x-8)\mathbb{Q}[x]$, $\mathfrak{m} = (x-2)\mathbb{Q}[x]$, and $\mathfrak{n} = (-4x+27)\mathbb{Q}[x]$ as before. By computing $det(N)$ as in Theorem 1.3.5, we find that the discriminant of $f(x)$ is a unit multiple of $x^2(-4x+27)$. Hence $d(f) \notin \mathfrak{q}$ and $d(f) \notin \mathfrak{m}$. By Lemma 2.2.3, $\mathfrak{q}A + \mathfrak{C} = A$, which justifies the suggested factorization $\mathfrak{q}A = (x-8, \alpha-2)(x-8, \alpha^2+2\alpha-4)A$ from Example 2.1.9. Since $\mathfrak{m}A + \mathfrak{C} = A$, we also know that $\mathfrak{m}$ is prime as conjectured in Example 2.1.9. On the other hand, $d(f) \in \mathfrak{n}$. Therefore, Lemma 2.2.3 fails for $\mathfrak{n}$. We work around this by showing directly that $\mathfrak{n}A = P_1P_2^2$ where $P_1 = (-4x+27, \alpha+3)A$ and $P_2 = (-4x+27, 2\alpha-3)$. By multiplying we see that the generators of $P_1P_2^2$ are $(-4x+27)^3, (-4x+27)^2(2\alpha-3), (-4x+27)^2(\alpha+3), (-4x+27)(2\alpha-3)^2, (-4x+27)(\alpha+3)(2\alpha-3)$, and $(\alpha+3)(2\alpha-3)^2$. We show that all generators are multiples of $-4x+27$. This is obvious for all generators except for the last, so we justify that the last generator is a multiple of $-4x+27$. Because α is a root of $f(x)$, $4\alpha^3 - 4x\alpha + 4x = 0$. Hence $(-4x+27)(1-\alpha) = 4\alpha^3 - 4x\alpha + 4x + (-4x+27)(1-\alpha) = 4\alpha^3 - 27\alpha + 27 = (\alpha+3)(2\alpha-3)^2$, so all generators are multiples of $-4x+27$. We have justified the containment $\mathfrak{n}A \supseteq P_1P_2^2$. For the reverse containment, we show that $-4x+27 \in P_1P_2^2$. Notice that $(-4x+27)(27-18\alpha) = (-4x+27)(2\alpha-3)^2 - 2(-4x+27)(\alpha+3)(2\alpha-3) \in P_1P_2^2$. In addition, $(-4x+27)9 = (-4x+27)(27-18\alpha) - 18(-4x+27)(1-\alpha) \in P_1P_2^2$.*

Since 9 *is a unit in* A, $(-4x + 27) \in P_1 P_2^2$. *This justifies the second containment in the equality* $\mathfrak{n}A = P_1 P_2^2$, *as desired.*

CHAPTER 3. RAMIFIED PRIMES AND THE DERIVATIVE

3.1. The Ramified Prime Theorem

The following theorem, which is essentially a corollary to Theorem 2.1.8, gives a simplified way to determine ramified primes in an integral extension of a Dedekind domain.

Theorem 3.1.1. *Let R be a Dedekind D - R construction, $f(t) \in D[t]$ a minimal polynomial for γ, and $\mathfrak{p}$ a nonzero prime ideal of D. Then $\mathfrak{p}$ is ramified in R if and only if $\bar{f}(r) = 0$ and $\bar{f}'(r) = 0$ for some $r \in D/\mathfrak{p}$.*

Proof. Both f and f' have the same root modulo $\mathfrak{p}$ if and only if f has a repeated root modulo $\mathfrak{p}$. By Theorem 2.1.8, f has a repeated root modulo $\mathfrak{p}$ if and only if $\mathfrak{p}R = P_1^{k_1} P_2^{k_2} \dots P_m^{k_m}$ where $k_i > 1$ for some $1 \leq i \leq m$. Hence $\mathfrak{p}$ ramifies in R, and we have our result.

□

3.2. The Ramified Prime Algorithm

Theorem 3.1.1 allows us to use linear algebra to determine ramified primes such that $\mathfrak{p}R + \mathfrak{C} = R$. Our claim is that some linear combination of polynomials of the form $t^i f(t)$ and $t^j f'(t)$ is equal to a nonzero constant, say $a_0 f(t) + a_1 t f(t) + \dots + a_m t^m f(t) + b_0 f'(t) + b_1 t f'(t) + \dots + b_v t^v f'(t) = c$. Then if there exists a root $r \in D/\mathfrak{p}$ such that $\bar{f}(r) = 0$ and $\bar{f}'(r) = 0$, $\bar{c} = 0$. That is, $c \in \mathfrak{p}$. So c is contained in any ramified prime $\mathfrak{p}$ such that $\mathfrak{p}R + \mathfrak{C} = R$. We outline an algorithm that computes c. Define the polynomials $s_0 = f(t)$, $s_1 = f'(t)$, and $s_2(t) = nf(t) - tf'(t)$. Notice that $s_2(t)$ is a linear combination of $f(t)$ and $f'(t)$, and that $deg(s_2(t)) < deg(f(t))$. If $s_2(0) = s_2(t)$ (that is, if $s_2(t)$ is a constant function) then let $s_2(t) = c$ and we are done. Otherwise, continue the process recursively. Let $s_\alpha(t) = d_\alpha s_\beta(t) + y_\alpha t^{z_\alpha} s_\delta(t)$

be the definition of s_α from the previous step where $z_\alpha \in \mathbb{Z}$, $d_\alpha \in D$, and $y_\alpha \in D$ are such that $deg(s_\alpha(t)) \leq deg(s_\beta(t))$.

If $deg(s_\alpha(t)) < deg(s_\delta(t))$, then choose $z_{\alpha+1} \in \mathbb{Z}$, $d_{\alpha+1} \in D$, and $y_{\alpha+1} \in D$ such that $s_{\alpha+1}(t) = d_{\alpha+1}s_\delta(t) + y_{\alpha+1}t^{z_{\alpha+1}}s_\alpha(t)$ and $deg(s_{\alpha+1}(t)) < deg(s_\delta(t))$.

If $deg(s_\alpha(t)) \geq deg(s_\delta(t))$, then choose $z_{\alpha+1} \in \mathbb{Z}$, $d_{\alpha+1} \in D$, and $y_{\alpha+1} \in D$ such that $s_{\alpha+1}(t) = d_{\alpha+1}s_\alpha(t) + y_{\alpha+1}t^{z_{\alpha+1}}s_\delta(t)$ and $deg(s_{\alpha+1}(t)) < deg(s_\alpha(t))$.

In either definition of $s_{\alpha+1}(t)$, if $s_{\alpha+1}(0) = s_{\alpha+1}(t)$ then let $s_{\alpha+1}(t) = c$ and we are done. Otherwise repeat the process again. We show that the process terminates. Suppose not. Then there exists $k \in \mathbb{Z}$ such that for all $\alpha \geq 0$, $0 < deg(s_k(t)) \leq deg(s_\alpha(t))$. Assume $s_{k+1}(t) = d_{k+1}s_k(t) + y_{k+1}t^{z_{k+1}}s_\beta(t)$ for some nonnegative integer β. Then $deg(s_{k+1}(t)) < deg(s_k(t))$, a contradiction of the definition of k. So $s_{k+1}(t) = d_{k+1}s_\beta(t) + y_{k+1}t^{z_{k+1}}s_k(t)$ and $deg(s_{k+1}(t)) < deg(s_\beta(t))$. Assume $s_{k+2}(t) = d_{k+2}s_k(t) + y_{k+2}t^{z_{k+2}}s_{k+1}(t)$. Then $deg(s_{k+2}(t)) < deg(s_k(t))$, once again contradicting the definition of k. So we have $s_{k+2}(t) = d_{k+2}s_{k+1}(t) + y_{k+2}t^{z_{k+2}}s_k(t)$, which implies $deg(s_{k+2}(t)) < deg(s_{k+1}(t)) < deg(s_\beta(t))$. Appeal to induction. Let $j \geq 1$, and suppose that $s_{k+j-1}(t) = d_{k+j-1}s_{k+j-2}(t) + y_{k+j-1}t^{z_{k+j-1}}s_k(t)$. Suppose also that $deg(s_{k+j-1}(t)) < deg(s_{k+j-2}(t)) < \cdots < deg(s_{k+1}(t)) < deg(s_\beta(t))$. Assume $s_{k+j}(t) = d_{k+j}s_k(t) + y_{k+j}t^{z_{k+j}}s_{k+j-1}(t)$. This contradicts the definition of k, so $s_{k+j}(t) = d_{k+j}s_{k+j-1}(t) + y_{k+j}t^{z_{k+j}}s_k(t)$. Thus $deg(s_{k+j}(t)) < deg(s_{k+j-1}(t)) < \cdots < deg(s_{k+1}(t)) < deg(s_\beta(t))$. By induction, we can find such a chain of inequalities for any $j \geq 1$. So let $j = deg(s_\beta(t))$. Then the chain of inequalities shows that $deg(s_{k+i}(t)) \leq j - i$ for all positive integers i. In particular, $deg(s_{k+j}(t)) \leq j - j = 0 < deg(s_k(t))$, contradicting our choice of k. In any case, the process must terminate.

So let k be a positive integer such that $s_k(t) = s_k(0)$. Suppose r is a root of $f'(t)$ and $f(t)$ as elements of $(D/\mathfrak{p})[t]$. Then $s_k(r) = s_k(0) = s_k(t) \in \mathfrak{p}$. Therefore, by Theorem 3.1.1, all ramified primes $\mathfrak{p}$ such that $R = R\mathfrak{p} + \mathfrak{C}$ contain $s_k(t)$. An

interesting corollary to this fact is that there are only finitely many ramified primes in any finite separable integral extension of a Dedekind domain D.

Corollary 3.2.1. *Let R be a Dedekind D - R construction and $f(t) \in D[t]$ a minimal polynomial for γ. Then there are only finitely many primes of D that ramify in R.*

Proof. By the preceding comments, it suffices to show that there are only finitely many prime ideals of D that contain $s_k(t)$. To see this, notice that any such prime ideal must appear in the prime factorization of the ideal generated by $s_k(t)$. Therefore, there are only finitely many ramified primes $\mathfrak{p}$ such that $R = R\mathfrak{p} + \mathfrak{C}$. On the other hand, any prime $\mathfrak{p}$ such that $R \neq R\mathfrak{p} + \mathfrak{C}$ contains the discriminant of $f(t)$ by Lemma 2.2.3. By the previous argument, only finitely many prime ideals of D contain the discriminant of $f(t)$, so there are only finitely many ramified primes that such that $R \neq R\mathfrak{p} + \mathfrak{C}$. Hence there are only finitely many ramified primes in D.

□

Example 3.2.2. *Let B be the integral closure of $\mathbb{Z}$ in the ring $\mathbb{Q}(\omega)$ where ω is a root of the polynomial $f(t) = t^3 - 6t^2 + 4t + 2$. We use the algorithm described above to find the ramified primes of B. Notice that $f(t)$ is irreducible over $\mathbb{Z}$ by Eisenstein's Criterion. We calculate the polynomial $s_2(t) = 3f(t) - tf'(t) = -6t^2 + 8t + 6$. Since $deg(s_2(t)) \geq deg(f'(t))$, the algorithm states that $s_3(t) = -s_2(t) - 2f'(t) = 16t - 14$. Because $deg(s_3(t)) < deg(f'(t))$, the algorithm gives $s_4(t) = -16f'(t) + 3ts_3(t) = 150t - 64$. Since $deg(s_4(t)) \geq deg(s_3(t))$, we know that $s_5(t) = 8s_4(t) - 75s_3(t) = 538$. Hence $s_5(t) = s_5(0)$, and primes that divide $538 = 2(269)$ are candidates for ramification. Recall that theoretically, these might not be the only ramified primes because the algorithm might miss ramified primes that divide the discriminant of $f(t)$. A quick computer computation shows that the discriminant of $f(t)$ is $2^2(269)$, so 2 and 269 are, in fact, the only candidates for ramification. We show that 2 is ramified by showing that the ideal $(2, \omega)^3 B = (8, 4\omega, 2\omega^2, \omega^3)B =$*

$(8, 4\omega, 2\omega^2, 6\omega^2 - 4\omega - 2)B = 2B$. *All equalities are clear except for the last. The containment* $(8, 4\omega, 2\omega^2, 6\omega^2 - 4\omega - 2)B \subseteq 2B$ *is clear because each generator of* $(8, 4\omega, 2\omega^2, 6\omega^2 - 4\omega - 2)B$ *is a multiple of* 2. *Also, because* $2 = -(6\omega^2 - 4\omega - 2) + 3(2\omega^2) - (4\omega) \in (8, 4\omega, 2\omega^2, 6\omega^2 - 4\omega - 2)B$, *we have the containment* $(8, 4\omega, 2\omega^2, 6\omega^2 - 4\omega - 2)B \supseteq 2B$. *Thus* $(8, 4\omega, 2\omega^2, 6\omega^2 - 4\omega - 2)B = 2B$ *as claimed and* 2 *ramifies in* B. *We show that* 269 *is ramified. A computational computer program shows that* $t^3 - 6t^2 + 4t + 2 \equiv (t + 63)(t + 100)^2 \pmod{269}$. *So we claim that* $(269, \omega + 63)(269, \omega + 100)^2 B = (269^3, 269^2(\omega + 63), 269^2(\omega + 100), 269(\omega^2 + 163\omega + 6300), 269(\omega^2 + 200\omega + 10000), \omega^3 + 263\omega^2 + 22600\omega + 630000) = 269B$. *The last equality is the only nontrivial equality. Let* I *be the ideal on the left side of the last equality. The only generator that is not clearly divisible by* 269 *is* $\omega^3 + 263\omega^2 + 22600\omega + 630000$. *However,* $\omega^3 + 263\omega^2 + 22600\omega + 630000 = \omega^3 - 6\omega^2 + 4\omega + 2 + 269\omega^2 + 22596\omega + 629998 = 269\omega^2 + 22596\omega + 629998$ *because* $f(\omega) = 0$. *Since* 269 *divides each of these terms,* 269 *divides* $\omega^3 + 263\omega^2 + 22600\omega + 630000$ *and hence every generator of* I *is divisible by* 269. *This justifies the containment* $I \subseteq 269B$. *To show the other containment, we will show that* $269 \in I$. *We have seen that* $269\omega^2 + 22596\omega + 629998 \in I$. *Hence* $269\omega^2 + 22596\omega + 629998 - 269(\omega^2 + 163\omega + 6300) = -269(3958 + 79\omega) \in I$. *Also,* $269(\omega^2 + 200\omega + 10000) - 269(\omega^2 + 163\omega + 6300) = 269(37\omega + 3700) \in I$. *So* $37(-269(3958 + 79\omega)) + 79(269(37\omega + 3700)) = 39234726 \in I$. *This is significant because the greatest common divisor of* 39234726 *and* 269^3 *is* 269, *which implies that* $269 \in I$. *So* $I \supseteq 269B$. *Combining this with the other containment shows that* $(269, \omega + 63)(269, \omega + 100)^2 B = 269B$, *hence* 269 *ramifies.*

See the appendix for a Mathematica implementation of the algorithm that computes and factors $s_k(t)$ in the case where $D = \mathbb{Z}$.

CHAPTER 4. INFINITE EXTENSIONS OF $\mathbb{Z}$

If S is an algebraic ring of integers and $p \in \mathbb{Z}$ is prime, Theorem 2.1.8 gives us a way to determine the ideal factorization of pS. On the other hand, if R is an arbitrary integral extension of $\mathbb{Z}$, R need not be Dedekind; indeed, in this case R may not even be Noetherian. However, we can still use Theorem 2.1.8 to analyze the algebraic rings of integers S such that $\mathbb{Z} \subseteq S \subseteq R$ to find information about the primes of R that lie over (p), as the following examples demonstrate.

4.1. The integral closure of $\mathbb{Z}$ in $\mathbb{Q}\left(\sqrt{d}, \sqrt[3]{d}, \sqrt[4]{d}, \ldots, \sqrt[N]{d}, \ldots\right)$

Let d be an integer such that $d \neq 0$ and $d \neq 1$. Let R be the integral closure of $\mathbb{Z}$ in $\mathbb{Q}\left(\sqrt{d}, \sqrt[3]{d}, \sqrt[4]{d}, \ldots, \sqrt[N]{d}, \ldots\right)$. Let p be a prime element in $\mathbb{Z}$. In this section we will show that for any integer n, we can find a subring of R in which (p) factors uniquely into a product of greater than n prime ideals. We start with a few lemmata:

Lemma 4.1.1. *Let $d \in \mathbb{Z}$ such that $d \neq 1$ and $d \neq 0$. Let $p \in \mathbb{Z}$ be a prime such that p does not divide d. Let $q \in \mathbb{Z}$ be prime such that q does not divide $p-1$. Then for any $w \in \mathbb{Z}$ such that $w \geq 1$, there is an integer r such that $r^{q^w} \equiv d \pmod{p}$.*

Proof. Suppose p is odd. Let g be a generator for $(\mathbb{Z}/p\mathbb{Z})^*$, the multiplicative group of integers modulo p. Let k be the unique integer such that $1 \leq k \leq p-1$ and $g^k \equiv d \pmod{p}$. Since q does not divide $p-1$, $p-1$ has a multiplicative inverse modulo q^w; call this inverse u. Notice that $k - ku(p-1) \equiv 0 \pmod{q^w}$. Thus, there exists and integer b such that $k - ku(p-1) = bq^w$. Also notice that the order of $(\mathbb{Z}/p\mathbb{Z})^*$ is $(p-1)$ so $g^{p-1} \equiv 1 \pmod{p}$. So we have $\left(g^b\right)^{q^w} \equiv g^{bq^w} \equiv g^{k-ku(p-1)} \equiv g^k g^{-ku(p-1)} \equiv g^k \left(g^{p-1}\right)^{-ku} \equiv g^k \equiv d \pmod{p}$. Therefore, $g^b \pmod{p}$ is the required integer and Lemma 4.1.1 is proven for the case where p is odd.

Suppose $p = 2$. By hypothesis p does not divide d. Then for any odd prime q and $w \geq 1$, $1^{q^w} \equiv 1 \equiv d \pmod{p}$, hence 1 is the required integer.

□

Lemma 4.1.2. *Let d, p, and q be as in Lemma 4.1.1. Then $x^{q^n} - d$ factors into at least $n+1$ terms modulo p for all integers $n \geq 1$.*

Proof. We proceed by induction on n. From Lemma 4.1.1 we know that $x^q - d$ is not irreducible, so the statement holds for $n = 1$. Suppose $x^{q^n} - d$ factors into polynomials $f_1(x) f_2(x) \ldots f_m(x)$ modulo p where $m > n$. Then notice that $x^{q^{n+1}} - d \equiv (x^q)^{q^n} - d \equiv f_1(x^q) f_2(x^q) \ldots f_m(x^q) \pmod{p}$ where the degree of $f_i(x^q)$ for $1 \leq i \leq m$ is greater than 1. By Lemma 4.1.1 there exists an $r \in \mathbb{Z}$ such that $r^{q^{n+1}} \equiv d \pmod{p}$. Thus $f_1(r^q) f_2(r^q) \ldots f_m(r^q) \equiv r^{q^{n+1}} - d \equiv 0 \pmod{p}$. Therefore, $f_i(r^q) \equiv 0 \pmod{p}$ for some $1 \leq i \leq m$. Since the degree of $f_i(x^q)$ is greater than 1, we now know that $f_i(x^q)$ is not irreducible. Therefore, $x^{q^{n+1}} - d$ factors into at least $m+1 > n+1$ terms. By induction, we have Lemma 4.1.2.

□

Lemma 4.1.3. *Let d, p, and q be as in Lemma 4.1.1. In addition, let $q \neq p$. Let $T_0 = \mathbb{Z}$, and for every $n \geq 1$ define T_n to be the integral closure of $\mathbb{Z}$ in $\mathbb{Q}\left(\sqrt[q^n]{d}\right)$. Then (p) factors uniquely into a product of at least $n+1$ prime ideals in T_n.*

Proof. First we notice that a minimal polynomial for $\sqrt[q^n]{d}$ is $f(x) = x^{q^n} - d$. Put the coefficients of $f(x)$ and $f'(x)$ into the matrix N as defined in Theorem 1.3.5. Basic linear algebra shows that the determinant of N is $(q^n)^{q^n}(-d)^{q^n-1}$. Since p does not divide q and p does not divide d, p does not divide $\det(N)$. Hence by Theorem 1.3.5, p does not divide the discriminant of $f(x)$. So we can apply Lemma 2.2.3, which shows that (p) satisfies the hypotheses of Theorem 2.1.8. This means that $f(x) \pmod{p}$ and pT_n factor into the same number of terms. By Lemma 4.1.2, $f(x)$ factors into at least $n+1$ terms modulo p, and our result follows.

□

The rings T_n in Lemma 4.1.3 are interesting in their own right. Clearly $T_n \subseteq$

T_{n+1} for every n. So we know that the union $T := \bigcup_{n=1}^{\infty} T_n$ is a ring which corresponds to the integral closure of $\mathbb{Z}$ in $\bigcup_{n=1}^{\infty} \mathbb{Q}\left(\sqrt[n]{d}\right)$. As the following example illustrates, some prime ideals of T may be finitely generated, while others may not be.

Example 4.1.4. *Let $C_0 = \mathbb{Z}$, and for every $n \geq 1$ define C_n to be the integral closure of $\mathbb{Z}$ in $\mathbb{Q}\left(\sqrt[2^n]{2}\right)$. Let $C := \bigcup_{n=1}^{\infty} C_n$. The ideal I of C generated by the set $\left\{\sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \ldots, \sqrt[2^n]{2}, \ldots,\right\}$ is clearly not finitely generated. Hence any prime ideal of C that contains I is also not finitely generated. On the other hand, C contains an infinite class of prime elements, hence infinitely many distinct principally (finitely) generated prime ideals. Proving this fact will require a lemma:*

Lemma 4.1.5. *Let p be a prime such that $p \equiv 5 \pmod 8$. Then $x^{2^n} - 2$ is irreducible as a polynomial in $(\mathbb{Z}/p\mathbb{Z})[x]$.*

Proof. We accept without proof the following facts from elementary number theory. See [7] for details:

1) There does not exist $a \in \mathbb{Z}/p\mathbb{Z}$ such that $a^2 \equiv 2 \pmod p$.

2) There exists $a \in \mathbb{Z}/p\mathbb{Z}$ such that $a^2 \equiv -1 \pmod p$.

Because of 1), we know that $x^2 - 2$ is irreducible in $(\mathbb{Z}/p\mathbb{Z})[x]$. Proceed by induction. Suppose that $x^{2^m} - 2$ is irreducible in $(\mathbb{Z}/p\mathbb{Z})[x]$ for all $1 \leq m \leq n$, and let $\alpha = \sqrt[2^n]{2}$ be a root of $x^{2^n} - 2$. Then $[(\mathbb{Z}/p\mathbb{Z})[\alpha] : \mathbb{Z}/p\mathbb{Z}] = 2^n$. Notice that the field extension $(\mathbb{Z}/p\mathbb{Z})[\sqrt{\alpha}]$ is quadratic over $(\mathbb{Z}/p\mathbb{Z})[\alpha]$, hence $[(\mathbb{Z}/p\mathbb{Z})[\sqrt{\alpha}] : (\mathbb{Z}/p\mathbb{Z})[\alpha]] \leq 2$. This means that $[(\mathbb{Z}/p\mathbb{Z})[\sqrt{\alpha}] : (\mathbb{Z}/p\mathbb{Z})[\alpha]] = 2$ if and only if $(\mathbb{Z}/p\mathbb{Z})[\sqrt{\alpha}] \supsetneq (\mathbb{Z}/p\mathbb{Z})[\alpha]$ if and only if $\sqrt{\alpha} \notin (\mathbb{Z}/p\mathbb{Z})[\alpha]$. Suppose that this is not the case; then $\sqrt{\alpha} \in (\mathbb{Z}/p\mathbb{Z})[\alpha]$. Notice that $(\mathbb{Z}/p\mathbb{Z})[\alpha] = (\mathbb{Z}/p\mathbb{Z})[\alpha^2][\alpha]$. Thus there exist $b \in (\mathbb{Z}/p\mathbb{Z})[\alpha^2]$ and $c \in (\mathbb{Z}/p\mathbb{Z})[\alpha^2]$ such that $\sqrt{\alpha} = b + c\alpha$. Then $\alpha = b^2 + c^2\alpha^2 + 2bc\alpha$. By matching coefficients we see that $b^2 + c^2\alpha^2 = 0$ and $2bc = 1$. Hence $c = \frac{1}{2b}$, and we substitute into the first equation to get $b^2 + \frac{1}{4b^2}\alpha^2 = 0$ which implies $-4b^4 = \alpha^2$.

Let a be as in 2) above. Then $(2ab^2)^2 = \alpha^2$. Since $a \in \mathbb{Z}/p\mathbb{Z}$, $2ab^2 \in (\mathbb{Z}/p\mathbb{Z})[\alpha^2]$ is a square root of α^2. Therefore, $[(\mathbb{Z}/p\mathbb{Z})[\alpha] : (\mathbb{Z}/p\mathbb{Z})[\alpha^2]] = 1$. This leads to the contradiction $2^n = [(\mathbb{Z}/p\mathbb{Z})[\alpha] : \mathbb{Z}/p\mathbb{Z}] = [(\mathbb{Z}/p\mathbb{Z})[\alpha] : (\mathbb{Z}/p\mathbb{Z})[\alpha^2]][(\mathbb{Z}/p\mathbb{Z})[\alpha^2] : \mathbb{Z}/p\mathbb{Z}] = [(\mathbb{Z}/p\mathbb{Z})[\alpha^2] : \mathbb{Z}/p\mathbb{Z}] \leq 2^{n-1}$, where the last inequality follows because α^2 is a root of a polynomial with degree 2^{n-1}. Because of this contradiction, we have $\sqrt{\alpha} \notin (\mathbb{Z}/p\mathbb{Z})[\alpha]$ which implies that $[(\mathbb{Z}/p\mathbb{Z})[\sqrt{\alpha}] : (\mathbb{Z}/p\mathbb{Z})[\alpha]] = 2$. Therefore, $[(\mathbb{Z}/p\mathbb{Z})[\sqrt{\alpha}] : \mathbb{Z}/p\mathbb{Z}] = [(\mathbb{Z}/p\mathbb{Z})[\sqrt{\alpha}] : (\mathbb{Z}/p\mathbb{Z})[\alpha]][(\mathbb{Z}/p\mathbb{Z})[\alpha] : \mathbb{Z}/p\mathbb{Z}] = 2^{n+1}$. This proves that any polynomial of degree 2^{n+1} over $(\mathbb{Z}/p\mathbb{Z})[x]$ that has $\sqrt{\alpha}$ as a root is irreducible. Consequently, $x^{2^{n+1}} - 2$ is irreducible in $(\mathbb{Z}/p\mathbb{Z})[x]$, and by induction we have our result.

□

Armed with Lemma 4.1.5, *we will show that if* p *is a prime in* $\mathbb{Z}$ *such that* $p \equiv 5 \pmod 8$, *then* pC *is prime. It suffices to show that* pC_n *is prime for any* $n \geq 0$. *To see this, notice that for any* $a \in C$ *and* $b \in C$ *such that* $ab \in pC$, *there exists some* n *such that* $a \in C_n$, $b \in C_n$, *and* $ab \in pC_n$. *If* pC_n *is prime, then without loss of generality* $a \in pC_n$. *Hence* $a \in pC$, *which implies* pC *is prime.*

Lemma 4.1.6. *Let* $p \in \mathbb{Z}$ *be prime such that* $p \equiv 5 \pmod 8$. *Then the ideal* pC_n *is prime for every* $n \geq 0$.

Proof. The minimal polynomial for $\sqrt[2^n]{2}$ is $f(x) = x^{2^n} - 2$. The discriminant of $f(x)$ is a unit multiple of a power of 2 (see the proof of Lemma 4.1.3). In particular, the discriminant of $f(x)$ is not divisible by p, so we apply Lemma 2.2.3 and Theorem 2.1.8 to show that the factorization of pC_n corresponds to the factorization of $f(x)$ modulo p . Since $f(x)$ is irreducible modulo p by Lemma 4.1.5, pC_n is prime and we have our result.

□

Theorem 4.1.7. *The ideal pC is prime for every prime $p \equiv 5 \pmod 8$.*

Proof. Use Lemma 4.1.6 along with the comments preceding it.

□

Computations indicate that if $p \equiv 3 \pmod 8$, then prime ideals of C_n lying over pC_n split for finitely many values of n. This provides support for the following conjecture.

Conjecture 4.1.8. *The ideal pC can be factored uniquely into a finite product of prime ideals for every prime $p \equiv 3 \pmod 8$.*

Besides showing that prime ideals in T may or may not be finitely generated, Example 4.1.4 shows that prime ideals from $\mathbb{Z}$ may be inert in T. This is because we chose the roots of d that are contained in T carefully. On the other hand, the ring R contains every root of d. Hence every prime ideal of R will fragment into an arbitrarily long product of ideals, as the following theorem guarantees.

Theorem 4.1.9. *Let (p) be a prime ideal in $\mathbb{Z}$. Then for every positive integer n there is a subring of R in which (p) factors uniquely into a product of at least n prime ideals. Furthermore, if p divides d, each distinct prime ideal appears at least n times in the factorization of (p).*

Proof. Case 1: p divides d

Assume p divides d. Let a be the integer such that p^a divides d, but no higher power of p divides d. For each integer $k > 1$, define the subring S_k of R as the integral closure of $\mathbb{Z}$ in $\mathbb{Q}\left(\sqrt{d}, \sqrt[3]{d}, \sqrt[4]{d}, \ldots, \sqrt[k]{d}\right)$. Also define the ideal I_k of S_k as $I_k := \left(p^a, \sqrt[k]{d}\right)$. We proceed by showing $(I_k)^k = (p^a)$. The generators of $(I_k)^k$ are p^{ak}, $p^{a(k-1)}\sqrt[k]{d}$, $p^{a(k-2)}\sqrt[k]{d^2}$, $\ldots$, $p^a\sqrt[k]{d^{k-1}}$, d. Since p^a divides each of the generators, $(p^a) \supseteq (I_k)^k$. For the other containment, notice that $\gcd(p^{ak}, d) = p^a$. Thus, we can

find integers b and c such that $bp^{ak} + cd = p^a$. This proves that $(p^a) \subseteq (I_k)^k$, and we have $(I_k)^k = (p^a)$. So for any integer $n > 1$, choose $k = an$ to get $(I_{an})^{an} = (p^a)$. This leads to $(p)^a = (p^a) = (I_{an})^{an}$ which gives $(p) = (I_{an})^n$. Recall that S_{an} is a Dedekind domain; this means that (I_{an}) factors uniquely into a product of prime ideals in S_{an}. Each of these prime ideals appears n times in the factorization of (p), which proves case 1 as well as the second conclusion of the theorem.

Case2: p does not divide d

This case was proven in Lemma 4.1.3, since the ring T_n is a subring of R in which (p) factors uniquely into at least $n + 1$ prime ideals.

□

Corollary 4.1.10. *The ring R is not almost Dedekind.*

Proof. As we saw in Theorem 4.1.9, arbitrarily high powers of prime ideals of S_k appear in the factorization of pS_k as k grows to infinity. Therefore, Theorem 1.2.2 shows that R is not almost Dedekind.

□

Notice that a similar argument shows that the ring C in Example 4.1.4 is not almost Dedekind.

Example 4.1.11. *In Example* 4.1.4, *we saw an extension of $\mathbb{Z}$ where some primes remained inert, but others factored into arbitrarily long products. In this example, we will adjoin all roots of* 2, *which will guarantee the splitting or ramification of all primes from $\mathbb{Z}$ by Theorem* 4.1.9. *Let $d = 2$ so that S_k is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots, \sqrt[k]{2}\right)$ and $R = \bigcup_{k=1}^{\infty} S_k$. We show how we can apply the theory of this section to determine the factorization of* 5 *in S_k. Notice that* 3 *is a generator for $(\mathbb{Z}/5\mathbb{Z})^*$ such that $3^3 \equiv 2 \pmod 5$. Since the multiplicative inverse for* 4 (mod 11) *is* 3, $3 - 3(3)(4) = -3(11) \equiv 0 \pmod{11}$. *Thus* $3^{-3(11)} \equiv 3^{3-3(3)(4)} \equiv 3^3(3^4)^{-3(3)} \equiv 2$

(mod 5). *Therefore,* $3^{-3} \equiv 2^{-1} \equiv 3 \pmod 5$ *is a root of the polynomial* $x^{11} - 2 \pmod 5$. *This proves that* $x - 3$ *is a factor of* $x^{11} - 2 \pmod 5$. *Similar computations show that* $x - 2$ *is a factor of* $x^{121} - 2 \pmod 5$. *So we divide to get* $x^{11} - 2 \equiv (x-3)f_2(x)f_3(x) \pmod 5$ *where* $f_2(x) = x^5 + x^4 + x^3 + 2x^2 + x + 2$ *and* $f_3(x) = x^5 + 2x^4 + x^3 + 2x^2 + 3x + 2$ *are irreducible factors of* $x^{11} - 2 \pmod 5$. *Substituting* x^{11} *in for* x *reveals that* $x^{121} - 2 \equiv (x^{11} - 3)f_2(x^{11})f_3(x^{11})$. *We have mentioned that* $x - 2$ *is a factor of* $x^{121} - 2 \pmod 5$, *so* $(x^{11} - 3)$, $f_2(x^{11})$, *and* $f_3(x^{11})$ *cannot all be irreducible. Therefore, there are at least four factors of* $x^{121} - 2 \pmod 5$. *A computer program can verify that there are actually five factors, say* $x^{121} - 2 \equiv (x-2)g_2(x)g_3(x)g_4(x)g_5(x) \pmod 5$ *where each* $g_i(x)$ *is an irreducible polynomial in* $(\mathbb{Z}/5\mathbb{Z})[x]$. *Repeating this process shows that* $(x^{11})^n - 2 \pmod 5$ *factors into at least* $n + 1$ *terms for all* $n \geq 1$. *There are corresponding factorizations of ideals, for example* $5S_{11} = \left(5, \sqrt[11]{2} - 3\right)\left(5, f_2\left(\sqrt[11]{2}\right)\right)\left(5, f_3\left(\sqrt[11]{2}\right)\right) S_{11}$ *and* $5S_{121} = \left(5, \sqrt[121]{2} - 2\right)\left(5, g_2\left(\sqrt[121]{2}\right)\right)\left(5, g_3\left(\sqrt[121]{2}\right)\right)\left(5, g_4\left(\sqrt[121]{2}\right)\right)\left(5, g_5\left(\sqrt[121]{2}\right)\right) S_{121}$. *Let* T_k *be the integral closure of* $\mathbb{Z}$ *in* $\mathbb{Q}\left(\sqrt[11^k]{2}\right)$. *The ideals in the above factorizations of* $5S_{11}$ *and* $5S_{121}$ *are prime in* T_1 *and* T_2, *respectively, but notice that this does not guarantee that they are prime in* S_{11} *and* S_{121}. *However, we do know that the prime factorizations of* $5S_{11}$ *and* $5S_{121}$ *are of length at least three and five, respectively. This demonstrates the power of the first part of Theorem* 4.1.9, *which states that ideal factorizations of* $5S_k$ *increase in length as* k *increases. To see the second part of Theorem* 4.1.9 *in action, we look at the factorization of* $2S_k$. *It is easy to verify that for every* $k \geq 1$ *the ideal* $I_k := \left(\sqrt[k]{2}\right)$ *has the property* $I_k^k S_k = 2S_k$. *Each* I_k *is a proper ideal, hence each factors into prime ideals. So prime ideals appear to a power greater than or equal to* k *in the factorization of* $2S_k$. *As we have seen in Theorem* 1.2.2, *this shows that* S *is not almost Dedekind.*

4.2. The integral closure of $\mathbb{Z}$ in $\mathbb{Q}\left(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \ldots, \sqrt{p_N}, \ldots\right)$

Let $\{p_i\}$ be the set of odd primes of $\mathbb{Z}$. We will be looking at the extent to which primes from $\mathbb{Z}$ fragment in a ring that contains the square root of every element of $\mathbb{Z}$, the integral closure of $\mathbb{Z}$ in $\mathbb{Q}\left(\sqrt{2}, \sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \ldots, \sqrt{p_N}, \ldots\right)$. We again build up to the main results by considering first some finite extensions of $\mathbb{Z}$.

Lemma 4.2.1. *Let p_1 and p_2 be distinct primes in $\mathbb{Z}$. A minimal polynomial for the extension $\mathbb{Q}\left(\sqrt{p_1}, \sqrt{p_2}\right)$ over $\mathbb{Q}$ is $f(x) = x^4 - 2(p_1 + p_2)x^2 + (p_1 - p_2)^2$. The discriminant of $f(x)$ is $4^6 p_1^2 p_2^2 (p_1 - p_2)^2$.*

Proof. The roots of $f(x)$ are $\sqrt{p_1} + \sqrt{p_2}, \sqrt{p_1} - \sqrt{p_2}, -\sqrt{p_1} + \sqrt{p_2}$, and $-\sqrt{p_1} - \sqrt{p_2}$. We show $\mathbb{Q}\left(\sqrt{p_1}, \sqrt{p_2}\right) = \mathbb{Q}\left(\sqrt{p_1} + \sqrt{p_2}\right) = \mathbb{Q}[x]/f(x)$. It suffices to prove that $\mathbb{Q}\left(\sqrt{p_1}, \sqrt{p_2}\right) \subseteq \mathbb{Q}\left(\sqrt{p_1} + \sqrt{p_2}\right)$ because the containments $\mathbb{Q}\left(\sqrt{p_1}, \sqrt{p_2}\right) \supseteq \mathbb{Q}[x]/f(x) \supseteq \mathbb{Q}\left(\sqrt{p_1} + \sqrt{p_2}\right)$ are obvious. Notice that $\sqrt{p_1 p_2} \in \mathbb{Q}\left(\sqrt{p_1} + \sqrt{p_2}\right)$ due to the fact that $(\sqrt{p_1} + \sqrt{p_2})^2 = p_1 + 2\sqrt{p_1 p_2} + p_2$. Hence $\sqrt{p_1} = \frac{\sqrt{p_1 p_2} - p_1}{p_2 - p_1}(\sqrt{p_1} + \sqrt{p_2}) \in \mathbb{Q}\left(\sqrt{p_1} + \sqrt{p_2}\right)$. Similarly, $\sqrt{p_2} \in \mathbb{Q}\left(\sqrt{p_1} + \sqrt{p_2}\right)$, which proves $\mathbb{Q}\left(\sqrt{p_1}, \sqrt{p_2}\right) \subseteq \mathbb{Q}\left(\sqrt{p_1} + \sqrt{p_2}\right)$. We know that $\mathbb{Q}\left(\sqrt{p_1}, \sqrt{p_2}\right)$ is a degree 4 extension, and $f(x)$ is a degree 4 polynomial, so $f(x)$ must be irreducible and therefore must the minimal polynomial for $\mathbb{Q}\left(\sqrt{p_1}, \sqrt{p_2}\right)$ over $\mathbb{Q}$. Let r_1, r_2, r_3, r_4 be the roots of $f(x)$. The discriminant of $f(x)$ is the product $\prod_{i>j}(r_i - r_j)^2$. A straightforward computation shows that the discriminant of $f(x)$ is $4^6 p_1^2 p_2^2 (p_1 - p_2)^2$.

□

The following lemma shows that the minimal polynomial in the previous lemma factors as an element of $\mathbb{F}[x]$ where $\mathbb{F}$ is any finite field.

Lemma 4.2.2. *Let $\mathbb{F}$ be a finite field. Let a and b be elements of $\mathbb{F}$. The polynomial $f(x) = x^4 + ax^2 + b^2$ is not irreducible in $\mathbb{F}[x]$.*

Proof. Suppose $\mathbb{F}$ has characteristic 2. Assume that there does not exist $h \in \mathbb{F}$ such that $h^2 = a$. Then $a \neq 0$. Since $\mathbb{F}$ is a finite field, the set of all nonzero elements of $\mathbb{F}$ is a cyclic group under multiplication. Hence every nonzero element of $\mathbb{F}$ is the power of some generating element $g \in \mathbb{F}$. Because the order of $\mathbb{F}$ is even, the order of the multiplicative group is odd hence $g^t = 1$ for some odd integer t. Suppose $a = g^z$ for some integer z. We also have $a = g^z g^t = g^{z+t}$ and since t is odd, either z or $z + t$ is even. In either case we have $g^{2m} = a$ for some integer m, which gives $(g^m)^2 = a$, a contradiction. Therefore, we can assume that there exists $h \in \mathbb{F}$ such that $h^2 = a$. Then we have $x^4 + ax^2 + b^2 = (x^2 + hx + b)^2$ as desired. Now consider the case where $\mathbb{F}$ does not have characteristic 2. Suppose $2b - a = c^2$ for some $c \in \mathbb{F}$. Then we have $(x^2 + cx + b)(x^2 - cx + b) = x^4 + (2b - c^2)x^2 + b^2 = x^4 + ax^2 + b^2$, which proves the lemma. So we continue under the assumption that there is no $c \in \mathbb{F}$ such that $2b - a = c^2$. Suppose $-2b - a = d^2$ for some $d \in \mathbb{F}$. Then we have $(x^2 + dx - b)(x^2 - dx - b) = x^4 + (-2b - d^2)x^2 + b^2 = x^4 + ax^2 + b^2$, which similarly proves the lemma. So we also have the assumption that there is no $d \in \mathbb{F}$ such that $-2b - a = d^2$. Notice that in particular, we have shown that $2b - a$ and $-2b - a$ are nonzero. As we have seen, there exists a generating element $g \in \mathbb{F}$ such that any nonzero element of $\mathbb{F}$ is some power of g. So write $2b - a = g^i$ and $-2b - a = g^j$. If i is even, then $\frac{i}{2}$ is an integer and we have $(g^{\frac{i}{2}})^2 = g^i = 2b - a$, which is a contradiction. So i is odd, and by a similar argument j is odd implying that $i + j$ is even. So $-4b^2 + a^2 = (2b - a)(-2b + a) = g^i g^j = g^{i+j} = g^{2k}$ for some integer k. Thus $(g^k)^2 = -4b^2 + a^2$. Because $2 \neq 0$, $(x^2 + \frac{a+g^k}{2})(x^2 + \frac{a-g^k}{2}) = x^4 + ax^2 + \frac{a^2-g^{2k}}{4} = x^4 + ax^2 + \frac{a^2-(-4b^2+a^2)}{4} = x^4 + ax^2 + b^2$ as desired. This completes the proof.

□

Theorem 4.2.3. *Let p, p_1, and p_2 be distinct prime elements of $\mathbb{Z}$ such that $p \neq 2$ and p does not divide $p_1 - p_2$. Let R be the integral closure of $\mathbb{Z}$ in $\mathbb{Q}\left(\sqrt{p_1}, \sqrt{p_2}\right)$.*

Then p is not inert in R.

Proof. Lemma 4.2.1 states that $f(x) = x^4 - 2(p_1 + p_2)x^2 + (p_1 - p_2)^2$ is a minimal polynomial for $\mathbb{Q}\left(\sqrt{p_1}, \sqrt{p_2}\right)$ over $\mathbb{Q}$. In addition, Lemma 4.2.1 guarantees that p does not divide the discriminant of $f(x)$, since p does not divide $2, p_1, p_2$, or $p_1 - p_2$. By Lemma 2.2.3, we know that the ideal generated by p satisfies the hypotheses of Theorem 2.1.8. Therefore, the factorization of pR into prime ideals mirrors the prime factorization of $f(x)$ as an element of $(\mathbb{Z}/p\mathbb{Z})[x]$. By Lemma 4.2.2, we have our result. □

Let $K = \mathbb{Q}\left(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \ldots, \sqrt{p_N}, \ldots\right)$ and B the integral closure of $\mathbb{Z}$ in K. It should be noted that given any odd prime p, we can always find p_1 and p_2 that satisfy the hypotheses of Theorem 4.2.3. Theorem 4.2.3 states that any such p is not inert in the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(p_1, p_2)$. For the case $p = 2$, notice that $2 = (\sqrt{p_1} + \sqrt{p_1 - 2})(\sqrt{p_1} - \sqrt{p_1 - 2})$. So if $\sqrt{p_1 - 2}$ is an integer, then 2 is not inert in the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(p_1)$. In either case, pB factors into a product of ideals. Notice this may not be a unique factorization into prime ideals because B need not be Dedekind. Regardless, this factorization shows that pB is not prime. In fact, adjoining square roots of as few as two distinct primes can cause all primes from $\mathbb{Z}$ to split or ramify.

Example 4.2.4. *No prime is inert in the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{3}, \sqrt{7})$. All odd primes except for 3 and 7 satisfy the hypotheses of Theorem 4.2.3. The primes 3 and 7 are not inert because $\sqrt{3}^2 = 3$ and $\sqrt{7}^2 = 7$. Finally, $2 = (\sqrt{3}+1)(\sqrt{3}-1)$, so 2 is also not inert.*

On the other hand, there exists a prime p that divides $p_1 - p_2$ and remains inert in the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$. Notice that in this case, p does not satisfy the hypotheses of Theorem 4.2.3.

Example 4.2.5. *The prime* 5 *is inert in the integral closure of* $\mathbb{Z}$ *in* $\mathbb{Q}(\sqrt{3}, \sqrt{13})$. *We will show in Theorem* 4.2.10 *that this integral closure is* $\mathbb{Z}[\sqrt{3}, \frac{1+\sqrt{13}}{2}]$. *Accepting this as fact for now, we see that* 5 *is inert in* $\mathbb{Z}[\sqrt{3}]$ *because the minimal polynomial* $x^2 - 3$ *is irreducible in* $(\mathbb{Z}/5\mathbb{Z})[x]$. *To show that* 5 *is inert in* $\mathbb{Z}[\sqrt{3}, \frac{1+\sqrt{13}}{2}]$, *we need to verify that* $x^2 - x - 3$ *is irreducible in* $(\mathbb{Z}[\sqrt{3}]/5\mathbb{Z}[\sqrt{3}])[x]$. *Assume not; then* $x^2 - x - 3 = (x + a + b\sqrt{3})(x + c + d\sqrt{3})$ *where* a, b, c, d *are elements of* $\mathbb{Z}/5\mathbb{Z}$. *It is straightforward to verify that* $x^2 - x - 3$ *is irreducible in* $(\mathbb{Z}/5\mathbb{Z})[x]$, *so assume that* b *and* d *are not both* 0. *Since* $x^2 - x - 3 = (x + a + b\sqrt{3})(x + c + d\sqrt{3}) = x^2 + [a + c + (b + d)\sqrt{3}]x + ac + 3bd + (ad + bc)\sqrt{3}$, *matching coefficients reveals that* $[a + c + (b + d)\sqrt{3}] = -1$ *and* $ac + 3bd + (ad + bc)\sqrt{3} = -3$. *Matching coefficients again leads to the equations* $a + c = -1, b + d = 0, ac + 3bd = -3$, *and* $ad + bc = 0$. *Hence by substitution,* $0 = ad - d(-1 - a) = d(2a + 1)$. *Since this operation is taking place in the field* $\mathbb{Z}/5\mathbb{Z}$, *either* $d = 0$ *or* $2a - 1 = 0$. *However, as we have seen* $d = 0$ *implies* $b = 0$, *which is a contradiction. So* $2a - 1 = 0$ *and because the multiplicative inverse of* 2 *in* $\mathbb{Z}/5\mathbb{Z}$ *is* 3, $a = 3$. *Substituting again gives* $c = -4$, *implying that* $-12 - 3b^2 = -3$. *The last equation is true if and only if* $b^2 \equiv 2 \pmod 5$, *which is a contradiction. So* $x^2 - x - 3$ *is irreducible in* $(\mathbb{Z}[\sqrt{3}]/5\mathbb{Z}[\sqrt{3}])[x]$, *hence* 5 *is inert in* $\mathbb{Z}[\sqrt{3}, \frac{1+\sqrt{13}}{2}]$.

The previous two examples show that only for carefully chosen p_1, p_2, and p does p remain inert in the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$. An interesting follow-up question is whether or not for every integer $N \geq 1$ there exists a set of primes $\{p_i\}_{i=0}^{N}$ such that p_0 remains inert in the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_N})$. As far as we know, this is an open question. Theorem 4.2.3 and the arguments in the examples above show that if the answer to the question is yes and all p_i are odd, then $p_1 \equiv p_2 \equiv \cdots \equiv p_N \pmod{p_0}$.

We define notation that will assist in proving the next few results. Let $\{p_i\}$ be

the set of all odd primes. For technical reasons, we assume that $p_1 = 3$, although some of our results will hold regardless. Let $K_0 = \mathbb{Q}$ and $K_{N+1} = K_N\left(\sqrt{p_{N+1}}\right)$ for all nonnegative integers N. Then we have $K = \mathbb{Q}\left(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \ldots, \sqrt{p_N}, \ldots\right) = \bigcup_{N=1}^{\infty} K_N$. Let $B_0 = \mathbb{Z}$, B_N the integral closure of $\mathbb{Z}$ in K_N, and $B = \bigcup_{N=1}^{\infty} B_N$. Because of the containments $B_i \subseteq B_j$ for all $i \leq j$, B is the integral closure of $\mathbb{Z}$ in K (this coincides with our previous definition of B). Let q be an odd prime in $\mathbb{Z}$ and $\mathfrak{q}_0$ the ideal generated by q in $\mathbb{Z}$. Let V_0 be the localization of $\mathbb{Z}$ at $\mathfrak{q}_0$. Choose a prime ideal $\mathfrak{q}_1$ that lies over $\mathfrak{q}_0$ in B_1. Define V_1 to be the localization of B_1 at $\mathfrak{q}_1$. Inductively choose a prime ideal $\mathfrak{q}_N$ that lies over $\mathfrak{q}_{N-1}$ in B_N. Define V_N to be the localization of B_N at $\mathfrak{q}_N$. Continuing in this manner, we define V_N for all nonnegative integers N. Let $V = \bigcup_{N=1}^{\infty} V_N$. As before, we have $V_i \subseteq V_j$ for all $i \leq j$. For all $N \geq 1$, define C_N to be the integral closure of V_{N-1} in K_N.

Lemma 4.2.6. *The maximal ideal of V_N is generated by a single element of B_N.*

Proof. Recall that Theorem 1.1.20 guarantees that V_N is a discrete valuation domain, hence the maximal ideal $\mathfrak{q}_N V_N$ is principally generated. If $\mathfrak{q}_N V_N = vV_N$ for some $v \in V_N$, then $v = \frac{r}{s}$ where $r \in B_N$ and $s \in B_N \setminus \mathfrak{q}_N$. Since $\frac{1}{s}$ is a unit in V_N, we have $\mathfrak{q}_N V_N = vV_N = \frac{1}{s} rV_N = rV_N$, as desired.

□

Lemma 4.2.6 allows us to choose an element $y_N \in B_N$ for each nonnegative integer N such that $y_N V_N = \mathfrak{q}_N V_N$. This allows us to make connections between the factorizations of elements of B_N and the factorizations of ideals of B_N, as we will see in the following results:

Lemma 4.2.7. *Let $0 \leq M < N$ be integers. Then $y_N^{2^k} V_N = y_M V_N$ where k is the number of elements in the set $\{M \leq j \leq N-1 \mid \mathfrak{q}_j$ ramifies in $B_{j+1}\}$.*

Proof. We will look at the prime factorization of the ideal $\mathfrak{q}_j B_{j+1}$ for each $M \leq j \leq N$. By Lemma 2.1.7, $\mathfrak{q}_j B_{j+1}$ factors into at most $[K_{j+1} : K_j] = 2$ prime ideals. If $\mathfrak{q}_j$ remains prime, then $\mathfrak{q}_j B_{j+1}$ is the unique prime ideal of B_{j+1} lying over $\mathfrak{q}_j$ in B_{j+1}. This means that our choice of $\mathfrak{q}_{j+1}$ is forced to be $\mathfrak{q}_j B_{j+1}$. By Corollary 1.1.19, $\mathfrak{q}_j V_{j+1} = \mathfrak{q}_{j+1} V_{j+1}$. If $\mathfrak{q}_j$ splits in B_{j+1}, then we have $\mathfrak{q}_j B_{j+1} = \mathfrak{a}\mathfrak{b}$ where $\mathfrak{a}$ and $\mathfrak{b}$ are distinct prime ideals of B_{j+1} that lie over $\mathfrak{q}_j$. Without loss of generality choose $\mathfrak{a} = \mathfrak{q}_{j+1}$. By Corollary 1.1.19, $\mathfrak{q}_j V_{j+1} = \mathfrak{q}_{j+1}\mathfrak{b} V_{j+1} = \mathfrak{q}_{j+1} V_{j+1}$, where the last equality follows from the fact that $\mathfrak{b}$ contains units in V_{j+1}. Notice that in either case, $\mathfrak{q}_j V_{j+1} = \mathfrak{q}_{j+1} V_{j+1}$ which means that $\mathfrak{q}_j V_{j+1}$ is the unique prime ideal of V_{j+1} Therefore, $y_j V_j V_{j+1} = y_j V_{j+1} = y_{j+1} V_{j+1}$. Suppose $\mathfrak{q}_j$ ramifies in B_{j+1}. then the prime factorization $\mathfrak{q}_j B_{j+1} = \mathfrak{c}^2$ implies that $\mathfrak{c}$ is the unique prime ideal of B_{j+1} lying over $\mathfrak{q}_j$. Hence $\mathfrak{c} = \mathfrak{q}_{j+1}$ and we have $\mathfrak{q}_j B_{j+1} = \mathfrak{q}_{j+1}^2$. Appealing again to Corollary 1.1.19, the factorization $\mathfrak{q}_j V_{j+1} = \mathfrak{q}_{j+1}^2 V_{j+1}$ holds. Therefore, in this case, $y_j V_j V_{j+1} = y_j V_{j+1} = y_{j+1}^2 V_{j+1}$. Because each V_j shares the same identity element, the factorizations of $y_j V_{j+1}$ take place in V_N as well. So if $\mathfrak{q}_j$ ramifies in B_{j+1}, then $y_j V_N = y_j V_{j+1} V_N = y_{j+1}^2 V_{j+1} V_N = y_{j+1}^2 V_N$. If $\mathfrak{q}_j$ does not ramify in B_{j+1}, $y_j V_N = y_j V_{j+1} V_N = y_{j+1} V_{j+1} V_N = y_{j+1} V_N$. So let $\{j_1, j_2, \ldots, j_k\}$ be the set of integers $M \leq j_i \leq N-1$ such that $\mathfrak{q}_{j_i}$ ramifies in B_{j_i+1}. Then $y_M V_N = y_{j_1} V_N = y_{j_1+1}^2 V_N = y_{j_2}^2 V_N = y_{j_2+1}^4 V_N = y_{j_3}^4 V_N = \cdots = y_{j_k}^{2^{k-1}} V_N = y_{j_k+1}^{2^k} V_N = y_N^{2^k} V_N$, as desired.

□

Corollary 4.2.8. *Let $0 \leq M < N$ be integers. Then $\mathfrak{q}_j$ ramifies in B_{j+1} for some $M \leq j \leq N-1$ if and only if there exist $s \in B_N$, $t \in B_N \setminus \mathfrak{q}_N$, and $r \in B_N \setminus \mathfrak{q}_N$ such that $y_M t = s^2 r$.*

Proof. ($\Longrightarrow$)

Suppose $\mathfrak{q}_j$ ramifies in B_{j+1} for some $M \leq j \leq N-1$. Then we have $k \geq 1$ in Lemma 4.2.7. Thus $y_M V_N = y_N^{2^k} V_N$. This means there exists a unit of V_N, say v, such

that $y_M v = y_N^{2k}$. Because v is a unit in V_N, we can write $v = \frac{t}{r}$ where $t \in B_N \setminus \mathfrak{q}_N$ and $r \in B_N \setminus \mathfrak{q}_N$. Hence $y_M \frac{t}{r} = y_N^{2k}$ implies $y_M t = y_N^{2k} r$, and we have our result if we let $s = y_N^k$.

($\Longleftarrow$)

Suppose that for all j such that $M \leq j \leq N-1$, $\mathfrak{q}_j$ does not ramify in B_{j+1}. Then according to Lemma 4.2.7, $y_M V_N = y_N V_N$ and hence $y_M V_N$ is the unique prime (maximal) ideal of V_N. Suppose that there exist $s \in B_N$, $t \in B_N \setminus \mathfrak{q}_N$, and $r \in B_N \setminus \mathfrak{q}_N$ such that $y_M t = s^2 r$. Then $y_M \in \mathfrak{q}_N$ implies $y_M t \in \mathfrak{q}_N$ and hence $s^2 r \in \mathfrak{q}_N$. Since $r \notin \mathfrak{q}_N$, we have $s^2 \in \mathfrak{q}_N$. Because $\mathfrak{q}_N$ is prime, $s \in \mathfrak{q}_N$. Since t and r are units in V_N, $y_M V_N = y_M t V_N = s^2 r V_N = s^2 V_N \subsetneq s V_N \subsetneq V_N$. This is a contradiction of the primality and maximality of $y_M V_N$, and we have our result.

□

Theorem 4.2.9. *The ideal q_N ramifies in B_{N+1} for precisely one nonnegative integer N. In fact, q_N ramifies in B_{N+1} if and only if $p_{N+1} = q$.*

Proof. Notice that the polynomial $f(t) = t^2 - p_{N+1}$ is a minimal polynomial for K_N over K_{N+1}. Recall that C_{N+1} is the integral closure of V_N in K_{N+1}. Because of our result in Corollary 1.1.19, it suffices to prove that q_N ramifies in C_{N+1} for precisely one nonnegative integer N. As mentioned in the proof of Lemma 1.4.6, any element $v \in C_{N+1}$ has the representation $v = a + b\gamma$ where $a \in K_N$, $b \in K_N$, and $\gamma \in K_{N+1}$ such that $f(\gamma) = 0$. So we let $\gamma = \sqrt{p_{N+1}}$ to get $v = a + b\sqrt{p_{N+1}}$. Because v is integral over V_N and $[K_{N+1} : K_N] = 2$, v is the root of a monic quadratic polynomial with coefficients in V_N. Any element of the form $a + b\sqrt{p_{N+1}}$ is a root of the polynomial $g(t) = t^2 - 2at + a^2 - p_{N+1}b^2$. Because $-2 \notin \mathfrak{q}_0$ and $\mathfrak{q}_N$ lies over $\mathfrak{q}_0$, -2 is not in $\mathfrak{q}_N$, which is the maximal ideal of V_N. Therefore, -2 is a unit in V_N. Since $-2a$ is a coefficient of $g(t)$, $-2a \in V_N$, which implies $a \in V_N$. Also notice $a^2 - p_{N+1}b^2$ is a coefficient of $g(t)$, and hence is and element of V_N. Let $b = \frac{u}{w}$ where $u \in V_N$

and $w \in V_N$ such that u and w have no prime factors in common. We can do this because V_N is a principal ideal domain by Theorem 1.1.20. In particular, this means w does not divide u. Then $w^2a^2 - w^2p_{N+1}b^2 = w^2a^2 - p_{N+1}u^2$ is an element of V_N that is divisible by w^2. Since w^2a^2 is also divisible by w^2, $p_{N+1}u^2$ is divisible by w^2. However, we have already made the case that u^2 and w^2 have no prime factors in common. So w^2 divides p_{N+1}, say $p_{N+1} = w^2y$ where $y \in V_N$. Returning to our original representation $a+b\sqrt{p_{N+1}}$, we multiply by p_{N+1} to get $ap_{N+1}+bp_{N+1}\sqrt{p_{N+1}} = ap_{N+1} + yu^2\sqrt{p_{N+1}} \in V_N\left[\sqrt{p_{N+1}}\right]$. So $p_{N+1}C_{N+1} \subseteq V_N\left[\sqrt{p_{N+1}}\right]$.

Suppose $p_{N+1} \in \mathfrak{q}_N$. We assert that this occurs if and only if p_{N+1} and q are associates (unit multiples) in $\mathbb{Z}$. Recall that $\mathfrak{q}_N$ lies over precisely one prime ideal from $\mathbb{Z}$, namely $\mathfrak{q}_0$. Thus $\mathfrak{q}_N \cap \mathbb{Z} = \mathfrak{q}_0$, which implies that $\mathfrak{q}_N$ contains a prime element from $\mathbb{Z}$ if and only if that prime element is in $\mathfrak{q}_0$. So q is, in fact, the only prime element from $\mathbb{Z}$ in $\mathfrak{q}_N$. Thus $p_{N+1} \in \mathfrak{q}_N$ if and only if p_{N+1} is an associate of q, which proves our assertion. To see why $\mathfrak{q}_N$ ramifies in C_{N+1} when p_{N+1} and q are associates, appeal to Corollary 4.2.8 with $y_M = q, t = 1, r = 1$, and $s = \sqrt{q}$. We have shown that $p_{N+1} \in \mathfrak{q}_N$ implies $\mathfrak{q}_N$ ramifies in C_{N+1}.

Suppose $p_{N+1} \notin \mathfrak{q}_N$. We have seen that this occurs if and only if p_{N+1} and q are not associates. To complete the theorem, we show that $\mathfrak{q}_N$ does not ramify in C_{N+1}. By Lemma 2.2.2 along with the fact that $p_{N+1}C \subseteq V_N\left[\sqrt{p_{N+1}}\right]$, $\mathfrak{q}_N$ satisfies the hypotheses of Theorem 2.1.8. Let $\bar{p}_{N+1}$ be the image of p_{N+1} under the canonical mapping $V_N \to V_N/\mathfrak{q}_N$. Consider the polynomials $f(t) = t^2 - \bar{p}_{N+1}$ and $f'(t) = 2t$ as elements of $(V_N/\mathfrak{q}_N)[t]$. By Theorem 3.1.1, $\mathfrak{q}_N$ ramifies in C_{N+1} if and only if both polynomials have a common root, say $r \in V_N/\mathfrak{q}_N$. If such a root exists, then $r^2 - \bar{p}_{N+1} = 0$ and $2r = 0$. Because 2 is a unit in $V_N/\mathfrak{q}_N$, $2r = 0$ implies $r = 0$. Substituting into the first equation gives $-\bar{p}_{N+1} = 0$. This implies that the characteristic of $V_N/\mathfrak{q}_N$ is p_{N+1}, which contradicts $p_{N+1} \notin \mathfrak{q}_N$. Therefore, there is

no common root for $f(t)$ and $f'(t)$. Theorem 3.1.1 states that $\mathfrak{q}_N$ does not ramify in C_{N+1}, and we have our result.

□

Theorem 4.2.9 guarantees that as N gets arbitrarily large, prime ideals of B_N lying over odd primes from $\mathbb{Z}$ ramify exactly once. We turn our attention to prime ideals lying over 2. We will make a statement similar to the one in Theorem 4.2.9. However, we will prove the statement in a different way.

As before, let $p_1 = 3$, $\{p_i\}_{i=1}^{N}$ be the set of all odd primes, $K_0 = \mathbb{Q}$, $K_{N+1} = K_N\left(\sqrt{p_{N+1}}\right)$, $K = \mathbb{Q}\left(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \ldots, \sqrt{p_N}, \ldots\right)$, $B_0 = \mathbb{Z}$, B_N the integral closure of $\mathbb{Z}$ in K_N, and B the integral closure of $\mathbb{Z}$ in K.

At this point the notation will differ a little from before. We are looking at prime ideals that lie over 2, so let $\mathfrak{m}_0$ the ideal generated by 2 in $\mathbb{Z}$. Choose a prime ideal $\mathfrak{m}_1$ that lies over $\mathfrak{m}_0$ in B_1. Inductively choose a prime ideal $\mathfrak{m}_N$ that lies over $\mathfrak{m}_{N-1}$ in B_N.

Since $p_1 = 3$, $K_1 = \mathbb{Q}\left(\sqrt{3}\right)$. We note that $B_1 = \mathbb{Z}\left[\sqrt{3}\right]$. See [5] for details.

Theorem 4.2.10. *For all $N \geq 2$ such that p_N is equivalent to 3 modulo 4, $B_N = B_{N-1}\left[\frac{\sqrt{3}+\sqrt{p_N}}{2}\right]$. For all $N \geq 2$ such that p_N is equivalent to 1 modulo 4, $B_N = B_{N-1}\left[\frac{1+\sqrt{p_N}}{2}\right]$.*

Proof. Suppose $p_N \equiv 3 \pmod 4$. A minimal polynomial for $\frac{\sqrt{3}+\sqrt{p_N}}{2}$ over B_{N-1} is given by $f(x) = x^2 - \sqrt{3}x - \frac{p_N-3}{4}$. Also, $\frac{\sqrt{3}+\sqrt{p_N}}{2} \in K_N$, so $\frac{\sqrt{3}+\sqrt{p_N}}{2} \in B_N$. This proves that $B_{N-1}\left[\frac{\sqrt{3}+\sqrt{p_N}}{2}\right] \subseteq B_N$. The roots of $f(x)$ are $\frac{\sqrt{3}\pm\sqrt{p_N}}{2}$. Therefore, the discriminant of $f(x)$ is given by $\left(\frac{\sqrt{3}+\sqrt{p_N}}{2} - \frac{\sqrt{3}-\sqrt{p_N}}{2}\right)^2 = \left(\frac{-2\sqrt{p_N}}{2}\right)^2 = p_N$. As we have seen in Theorem 4.2.9, a prime ideal of B_{i-1} lying over an odd prime $q \in \mathbb{Z}$ ramifies in B_i if and only if q is an associate of p_i. So let $q = p_N$. Then there does not exist $0 \leq i \leq N-2$ such that a prime ideal lying over p_N in B_{i-1} ramifies in B_i. Therefore by Corollary 4.2.8, p_N is square-free; that is, any square that divides p_N is

a unit in B_{N-1}. By Theorem 1.3.7, we know that there exists $z \in B_{N-1}$ such that $p_N = d(f(x)) = d_{K_N/K_{N-1}}(B_{N-1}\left[\frac{\sqrt{3}+\sqrt{p_N}}{2}\right]) = z^2 d_{K_N/K_{N-1}}(B_N)$. Because z^2 divides p_N, z is a unit and hence Theorem 1.3.7 implies that $B_{N-1}\left[\frac{\sqrt{3}+\sqrt{p_N}}{2}\right] = B_N$.

Suppose $p_N \equiv 1 \pmod 4$. If we replace $f(x)$ with $x^2 - x + \frac{1-p_N}{4}$ and replace $\frac{\sqrt{3}+\sqrt{p_N}}{2}$ with $\frac{1+\sqrt{p_N}}{2}$ in the proof of the previous case, then the discriminant of $f(x)$ is once again p_N and the required result holds.

□

Let $\gamma = \frac{\sqrt{3}+\sqrt{p_N}}{2}$ if $p_N \equiv 3 \pmod 4$ or $\gamma = \frac{1+\sqrt{p_N}}{2}$ if $p_N \equiv 1 \pmod 4$. Theorem 4.2.10 asserts that $B_N = B_{N-1}[\gamma]$ has a power basis over B_{N-1}. Hence all primes $\mathfrak{p}$ of B_{N-1} satisfy $\mathfrak{p}B_N + \mathfrak{C} = B_N$ as mentioned in the comments preceding Example 2.2.1. So for any prime ideal $\mathfrak{p}$ of B_{N-1}, we can apply Theorem 2.1.8 and predict the factorization of $\mathfrak{p}B_N$ by factoring polynomials.

Lemma 4.2.11. *Let $N \geq 1$ be an integer and $\mathfrak{m}_N$ a prime ideal that lies over 2 in B_N. Then $\mathfrak{m}_N$ contains $\sqrt{3}+1$. In addition, the derivatives of the polynomials $f(x) = x^2 - \sqrt{3}x - \frac{p_N-3}{4}$ and $g(x) = x^2 - x + \frac{1-p_N}{4}$ do not have roots in $(B_N/\mathfrak{m}_N B_N)[x]$ for any $N \geq 1$.*

Proof. First we show that $\mathfrak{m}_N$ contains $\sqrt{3}+1$. This is because $\sqrt{3}+1 \in B_1 \subseteq B_N$, $(\sqrt{3}+1)(\sqrt{3}-1) = 2$, and $\mathfrak{m}_N$ is a prime ideal that contains 2. Now we prove the second conclusion of the lemma. Notice that $2 \equiv 0 \pmod{\mathfrak{m}_N}$. Then $f'(x) \equiv -\sqrt{3} \equiv 1 \pmod{\mathfrak{m}_N}$. Also, $g'(x) \equiv 1 \pmod{\mathfrak{m}_N}$. Therefore, neither $f'(x)$ nor $g'(x)$ has a root in $(B_N/\mathfrak{m}_N B_N)[x]$, which proves our result.

□

Theorem 4.2.12. *The ideal $\mathfrak{m}_N$ does not ramify in B_{N+1} for any $N \geq 1$.*

Proof. Let N be an integer such that $N \geq 1$. By Theorem 4.2.10 and the comments following it, either $f(x) = x^2 - \sqrt{3}x - \frac{p_N-3}{4}$ or $g(x) = x^2 - x + \frac{1-p_N}{4}$ is a minimal

polynomial for K_{N+1} over K_N. By Theorem 3.1.1, $\mathfrak{m}_N$ ramifies in B_{N+1} if and only if the minimal polynomial for K_{N+1} over K_N and its derivative have a common root in $(B_N/\mathfrak{m}_N B_N)[x]$. We have seen in Lemma 4.2.11 that this is not possible, so $\mathfrak{m}_N$ does not ramify in B_{N+1}.

□

Notice that $2B_1 = (\sqrt{3}+1)^2 B_1$, so there exists a value of N for which $\mathfrak{m}_N$ ramifies in B_{N+1}, namely $N = 0$. Theorem 4.2.12 justifies that there are no other values of N that have this property, which suggests the following theorem when combined with Theorem 4.2.9.

Theorem 4.2.13. *The ring B is almost Dedekind.*

Proof. By Theorem 4.2.9, prime ideals of B_{N-1} lying over odd primes of $\mathbb{Z}$ ramify in B_N for precisely one value of $N \geq 1$. By Theorem 4.2.12 and the comments that follow it, prime ideals of B_{N-1} lying over 2 ramify in B_N for precisely one value of $N \geq 1$. In any case, the number of ramifications is bounded, so we apply Theorem 1.2.2 to get the required result.

□

Corollary 4.2.14. *The integral closure of $\mathbb{Z}$ in $\mathbb{Q}\left(\sqrt{2}, \sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \ldots, \sqrt{p_N}, \ldots\right)$ is almost Dedekind.*

Proof. By Theorem 4.2.13, B is almost Dedekind. The integral closure of $\mathbb{Z}$ in $K(\sqrt{2})$ is the same as the integral closure of B in $K(\sqrt{2})$. This is a finite separable extension of B, so there is still a bound on the ramifications of the primes from $\mathbb{Z}$, and by Theorem 1.2.2 we have our result.

□

Corllary 4.2.14 shows that adding the square roots of all integers to an integrally closed ring containing $\mathbb{Z}$ preserves the almost Dedekind property. We will show that

the Dedekind property is not preserved by this operation. In fact, we will show that adjoining any infinite set of square roots destroys the Dedekind property. We set about proving this fact by first stating a helpful theorem.

Theorem 4.2.15. *Let D be a Dedekind domain and I a nonzero ideal of D. Then finitely many prime ideals of D contain I.*

Proof. It suffices to show that a prime ideal $\mathfrak{p}$ of D contains I if and only if $\mathfrak{p}$ appears in the ideal factorization of I, since finitely many prime ideals appear in an ideal factorization of a Dedekind domain. It is straightforward that if $\mathfrak{p}$ appears in the factorization of I, then $\mathfrak{p}$ contains I. We prove the converse. Suppose the prime factorization of I is given by $I = P_1P_2 \dots P_n$. Assume $\mathfrak{p}$ is a prime ideal of D such that $\mathfrak{p} \supseteq I = P_1P_2 \dots P_n$. Since $\mathfrak{p}$ is prime, $P_i \subseteq \mathfrak{p}$ for some i such that $1 \leq i \leq n$. Since I is nonzero, P_i is nonzero. Because D has Krull dimension 1 by Theorem 1.1.20, P_i is maximal hence $\mathfrak{p} = P_i$. So $\mathfrak{p}$ appears in the prime factorization of I, and we have our result.

□

The following classification of the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_N})$ is a good intermediate step in understanding the situation where infinitely many square roots are adjoined to $\mathbb{Q}$.

Theorem 4.2.16. *Let $\{a_i\}_{i=1}^N$ be a set of primes equivalent to 3 (mod 4), $\{b_i\}_{i=1}^M$ a set of primes equivalent to 1 (mod 4), $F = \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_N}, \sqrt{b_1}, \dots, \sqrt{b_M})$, and E the integral closure of $\mathbb{Z}$ in F. Define $\gamma_1 = \sqrt{a_1}$, $\gamma_i = \frac{\sqrt{a_1}+\sqrt{a_i}}{2}$ if $2 \leq i \leq N$, and $\gamma_i = \frac{1+\sqrt{b_i}}{2}$ if $N+1 \leq i \leq N+M$. Then $E = \mathbb{Z}[\gamma_1, \gamma_2, \dots, \gamma_{N+M}]$.*

Proof. Let E_1 be the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{a_1})$. We show $E_1 = \mathbb{Z}[\sqrt{a_1}]$. Because $E_1 \subseteq \mathbb{Q}(\sqrt{a_1})$, any element of E_1 is of the form $c_1 + c_2\sqrt{a_1}$ where $c_1 \in \mathbb{Q}$ and $c_2 \in \mathbb{Q}$. Such an element is a root of the polynomial $t^2 - 2c_1t + c_1^2 - a_1c_2^2$. Since every element

of E_1 is integral over $\mathbb{Z}$, $-2c_1$ and $c_1^2 - a_1c_2^2$ are elements of $\mathbb{Z}$. Suppose $c_1 \notin \mathbb{Z}$. Then $-2c_1 \in \mathbb{Z}$ implies $c_1 = \frac{r}{2}$ where $r \in \mathbb{Z}$ and 2 does not divide r. Let $c_2 = \frac{u}{w}$ where u and w are integers with no common prime factors. Because $c_1^2 - a_1c_2^2 = \frac{r^2}{4} - a_1c_2^2 \in \mathbb{Z}$, $r^2 - 4a_1c_2^2 \in \mathbb{Z}$ so $-4a_1c_2^2 = \frac{-4a_1u^2}{w^2} \in \mathbb{Z}$. This means all prime factors of w must appear in the prime factorization of $-4a_1u^2$. Since w is relatively prime to u and a_1 is not a square, either w is a unit or w is a unit multiple of 2. Assume w is a unit multiple of 2. Then $c_1^2 - a_1c_2^2 = \frac{r^2}{4} - \frac{a_1u^2}{4} \in \mathbb{Z}$. This implies $r^2 - a_1u^2 \equiv 0 \pmod 4$. Since r and u are odd, $r^2 \equiv u^2 \equiv 1 \pmod 4$. This leads to the contradiction $2 \equiv r^2 - a_1u^2 \equiv 0 \pmod 4$. So w must be a unit and c_2 is an integer, which contradicts $\frac{r^2}{4} - a_1c_2^2 \in \mathbb{Z}$. Hence $c_1 \in \mathbb{Z}$. Since any element of E_1 is of the form $c_1 + c_2\sqrt{a_1}$ where c_1 and c_2 are integers, $E_1 = \mathbb{Z}[\sqrt{a_1}]$. *Let* $E_i = \mathbb{Z}[\gamma_1, \gamma_2, \ldots, \gamma_i]$. Suppose $i < N$. We show that the integral closure of E_i in $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{i+1}})$ is E_{i+1}. A minimal polynomial for γ_{i+1} over E_i is given by $f(x) = x^2 - \sqrt{a_1}x - \frac{a_{i+1}-3}{4}$. As noted in Theorem 4.2.10, a_{i+1} is square-free in E_i. The discriminant of $f(x)$ is given by $\left(\frac{\sqrt{a_1}+\sqrt{a_{i+1}}}{2} - \frac{\sqrt{a_1}-\sqrt{a_{i+1}}}{2}\right)^2 = \left(\frac{-2\sqrt{a_{i+1}}}{2}\right)^2 = a_{i+1}$. Hence by Theorem 1.3.7, $E_i[\gamma_{i+1}] = E_{i+1}$ is the integral closure of E_i in $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{i+1}}$. Suppose $N \leq i < M$. We show that the integral closure of E_i in $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_N}, \sqrt{b_1}, \ldots, \sqrt{b_{i+1}})$ is E_{i+1}. This is because the above argument holds if we replace $f(x)$ with $x^2 - x + \frac{1-b_{N+i+1}}{4}$. Hence the integral closure of E_{N+M-1} in F is E. Since the integral closure of E_{N+M-1} in F corresponds with the integral closure of $\mathbb{Z}$ in F, we have our result.

□

We have seen that only finitely many prime ideals contain any nonzero ideal in a Dedekind domain. Therefore, no Dedekind domain can satisfy the conclusion of the following theorem.

Theorem 4.2.17. *Let* $\{p_i\}$ *be an infinite set of odd prime integers. If* $p_i \equiv 3 \mod 4$ *for some* i, *reorder the set so that* $p_1 \equiv 3 \pmod 4$. *Let* $K_0 = \mathbb{Q}$, $K_i = K_{i-1}(\sqrt{p_i})$,

and $K = \bigcup_{i=0}^{\infty} K_i$. *Let* $B_0 = \mathbb{Z}$, B_i *the integral closure of* $\mathbb{Z}$ *in* K_i, *and* $B = \bigcup_{i=0}^{\infty} B_i$. *Let* q *be an odd prime element of* $\mathbb{Z}$, $\mathfrak{q}_0$ *the ideal generated by* q, *and* $\mathfrak{q}_i$ *a prime ideal of* B_i *lying over* $\mathfrak{q}_0$. *Then infinitely many prime ideals of* B *contain* $\mathfrak{q}_0 B$.

Proof. We first show that $\mathfrak{q}_i$ splits in B_{i+1} for infinitely many i. We have already seen that ramification occurs for finitely many i. Therefore, it suffices to show that $\mathfrak{q}_i$ is inert in B_{i+1} for finitely many i. By Theorem 4.2.16, we know that the minimal polynomial for B_{i+1} over B_i where $i \geq 1$ is either $f_i(x) = x^2 - \sqrt{p_1}x - \frac{p_{i+1}-3}{4}$ or $g_i(x) = x^2 - x + \frac{1-p_{i+1}}{4}$. By Theorem 2.1.8, $\mathfrak{q}_i$ is inert in B_{i+1} if and only if the minimal polynomial for B_{i+1} over B_i is irreducible in $(B_i/\mathfrak{q}_i)[x]$. Notice that there are only q possible distinct equivalence classes for $\frac{p_{i+1}-3}{4}$ and $\frac{1-p_{i+1}}{4}$ in $B_i/\mathfrak{q}_i$. This is because $q \in \mathfrak{q}_i$, hence each equivalence class has a representative in $\mathbb{Z}/q\mathbb{Z}$. So there are at most $2q$ distinct polynomials $f_i(x)$ and $g_i(x)$ when considered as elements of $(B_i/\mathfrak{q}_i)[x]$. Also, if the minimal polynomial for B_{i+1} over B_i is irreducible in $(B_i/\mathfrak{q}_i)[x]$, then it is not irreducible in $(B_j/\mathfrak{q}_j)[x]$ for any $j \geq i$. This is because the roots of the minimal polynomial are added to the extension B_{i+1} and $B_{i+1} \subseteq B_j$. So there are at most $2q$ values of i such that $\mathfrak{q}_i$ is inert in B_{i+1}. This shows that $\mathfrak{q}_i$ splits in B_{i+1} for infinitely many i. We use this fact to show that infinitely many distinct prime ideals of B contain $\mathfrak{q}_0 B$. Suppose not; then there exists an integer m such that precisely m distinct prime ideals of B contain $\mathfrak{q}_0 B$. We have seen that there exists n such that the number of indices $i < n$ where $\mathfrak{q}_i$ splits in B_{i+1} is greater than m. Hence there are greater than m prime ideals of B_n that contain $\mathfrak{q}_0 B_n$. Each of these prime ideals is contained in a distinct prime ideal of B, which in turn must contain $\mathfrak{q}_0 B$. This contradicts our assumption that precisely m distinct prime ideals of B contain $\mathfrak{q}_0 B$. So infinitely many prime ideals of B contain $\mathfrak{q}_0 B$, and we have our result.

□

REFERENCES

[1] H. Cohen, *A Course in Computational Algebraic Number Theory*, 2nd ed., Springer-Verlag, Berlin, Heidelberg, and New York, 1995, pp. 118–120, 163–165.

[2] T. Hungerford, *Algebra*, Springer Science+Business Media, Inc., New York, 1974, pp. 261–288, 394–407.

[3] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd ed., Springer-Verlag, Berlin, Heidelberg, and New York, 2004.

[4] R. Gilmer, *Multiplicative Ideal Theory*, Queen's Papers in Pure and Applied Mathematics, vol. 90, Kingston, 1992, pp. 509–511.

[5] M.Pohst and H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Paperback ed., Cambridge University Press, Cambridge, 1997.

[6] I. Del Corso, *Factorization of Prime Ideal Extensions in Dedekind Domains*, J. Symbolic Computation **19** (1995), 435–439.

[7] S. Lang, *Algebraic Number Theory*, 2nd ed., Springer-Verlag, New York, 1994, pp. 64 – 66, 76–79.

[8] K. A. Loper, *Almost Dedekind domains which are not Dedekind*, Multiplicative Ideal Theory in Commutative Algebra; A Tribute to the Work of Robert Gilmer, New York, 2006, pp. 279 – 292.

APPENDIX A. MATHEMATICA RAMIFIED PRIME ALGORITHM

This appendix contains the Mathematica code referred to and described in the comments following Theorem 3.1.1. The input should be an irreducible polynomial over the integers in the variable x, say $f(x)$. The algorithm computes an integer labelled $s[x]$ that is a linear combination of polynomials of the form $x^i f(x)$ and $x^j f'(x)$. The output is the prime factorization of $s[x]$.

```
f[x_] := input

For[{g[x] = f[x], h[x] = f'[x],
  r[x] = h[x]*x^(Exponent[g[x], x] - Exponent[h[x], x]), s[x] = h[x],
  lc[poly_] := Coefficient[poly, x, Exponent[poly, x]]},
 Exponent[s[x], x] > 0,
{s[x] = Simplify[(lcm/lc[g[x]]) g[x] - (lcm/lc[r[x]]) r[x]],
  If[Exponent[h[x], x] > Exponent[s[x], x], {g[x] = h[x],
    h[x] = s[x]}, g[x] = s[x]],
  r[x] = h[x]*x^(Exponent[g[x], x] - Exponent[h[x], x])},
 lcm = LCM[lc[g[x]], lc[r[x]]]]

output = FactorInteger[s[x]]
```