UNIVERSITY OF CALIFORNIA
RIVERSIDE

Some Results on Factorization in Integral Domains

A Dissertation submitted in partial satisfaction
of the requirements for the degree of

Doctor of Philosophy

in

Mathematics

by

Jack Robert Bennett

August 2011

Dissertation Committee:

Professor David Rush, Chairperson
Professor Vyjayanthi Chari
Professor Mei-Chu Chang

The Dissertation of Jack Robert Bennett is approved:

Committee Chairperson

University of California, Riverside

Acknowledgments

Throughout my education, I have been fortunate to have been surrounded by amazing teachers and extraordinary researchers. Their ability to communicate and do mathematics have made this dissertation possible.

First, I would like to thank my adviser Dr. David E. Rush. The guidance he has provided me with as my adviser and his expertise as a mathematician have made this work and other joint work possible. He has done an excellent job providing me with new and exciting problems to work on and he was always willing to listen to any new ideas that I might have and provide me with the resources I needed to carry them out. I could not have come this far without him.

I would like to extend my appreciation to my other committee members, Dr. Mei-Chu Chang, whose course in algebraic number theory has had an influence on this work, and Dr. Vyjayanthi Chari, for her advice and guidance throughout my years as a graduate student mentor. I would also like to thank Dr. Albert Stralka, for all his support throughout my years as a graduate student.

Aside from being surrounded by great professors, I have amazing family and friends who have encouraged me to pursue my dreams and who have made it possible for me to pursue my dreams. Without their love and support, this dissertation would not have been possible. To begin, I would like to thank my wife Jeni. Over the past six years, she has given me unwavering support and encouragement. During the times when I was not sure if I would make it through the qualifiers, or when my research was not going as smoothly as I hoped, she encouraged me to work hard and give it my all, and she assured me that everything would work out for the best. Aside from her encouragement, she sacrificed many of our weekends together and ate many meals alone so I could study for the qualifiers and pursue new directions in my research. She is an amazing wife and mother, my best friend, and in many ways, this dissertation is as much hers as it is mine. Thank you Jeni for being the wonderful person you are.

Next, I would like to thank my parents and Jeni's parents. From the time I was born, my parents have been there for me in every way possible. They were at every baseball game, every school event, and they worked hard and sacrificed much to see that I got a good education. They are always there to listen and support me in all my dreams. Thank you Mom and Dad for all your love and support. When I married Jeni, I became a part of another great family. I would like to

thank Jeni's parents for all of the love and support they have shown me as well. There have been many days when "Ma" or "Pa" would help watch our son so I could do my work. It is our (Jeni and I) hope that we can provide Jack (and our future children) with all of the love and support that our parents have given us. Finally, I would like to thank the rest of my family and friends for all of their love and encouragement. You all have helped make this possible.

To my family, who made this possible.

ABSTRACT OF THE DISSERTATION

Some Results on Factorization in Integral Domains

by

Jack Robert Bennett

Doctor of Philosophy, Graduate Program in Mathematics
University of California, Riverside, August 2011
Professor David Rush, Chairperson

In this dissertation, we study three recent generalizations of unique factorization; the almost Schreier property, the inside factorial property, and the IDPF property. Let R be an integral domain and let p be a nonzero element of R. Then, p is said to be *almost primal* if whenever $p \mid xy$, there exists an integer $k \geq 1$ and $p_1,\ p_2 \in R$ such that $p^k = p_1 p_2$ with $p_1 \mid x^k$ and $p_2 \mid y^k$. R is said to be *almost Schreier* if every nonzero element of R is almost primal. Given an M-graded domain $R = \bigoplus_{m \in M} R_m$, where M is a torsion-free, commutative, cancellative monoid, we classify when R is almost Schreier under the assumption that $R \subseteq \widetilde{R}$ is a root extension. We then specialize to the case of commutative semigroup rings and show that if $R[M] \subseteq \widetilde{R[M]}$ is a root extension, then $R[M]$ is almost Schreier if and only if R is an almost Schreier domain and M is an almost Schreier monoid.

Let $D_n(a)$ denote the set of non-associate irreducible divisors of a^n. R is said to be *IDPF*, if for every nonzero, nonunit element a of R, the ascending chain $D_1(a) \subseteq D_2(a) \subseteq \cdots$ stabilizes on a finite set. Also, a monoid H is *inside factorial* if there exists a divisor homomorphism $\phi : D \to H$ from a factorial monoid D such that for any $x \in H$ there is an $n \in \mathbb{N}$ with $x^n \in \phi(D)$. R is *inside factorial* if its multiplicative monoid $R - \{0\}$ is inside factorial. Continuing our investigation of semigroup rings, we prove that no proper numerical semigroup ring $R[S]$ of characteristic zero is IDPF. Let R be an order in any quadratic integer ring and let n be the least positive integer in $[R :_R \widetilde{R}]$. We tie the IDPF, inside factorial, and the almost Schreier properties together by proving that $R[X]$ is IDPF if and only if $R[X]$ is almost Schreier if and only if $R[X]$ is inside factorial if and only if every prime divisor of n also divides $\delta_{\mathbb{Q}(\sqrt{d})}$, the discriminant of $\mathbb{Q}(\sqrt{d})$.

Contents

Chapter 1

Introduction

1.1 Preliminaries and Motivation

Fermat's Last Theorem, which states that $x^n + y^n = z^n$ has no positive integer solutions when $n > 2$, has inspired the creation of many branches of mathematics. Historically, mathematicians tried to prove Fermat's Last Theorem by extending the arithmetic of $\mathbb{Z}$ to the slightly larger domain $\mathbb{Z}[\zeta]$, where ζ is a primitive nth root of 1 and $n > 2$ is prime [1]. By doing this, they could factor $x^n + y^n$ in $\mathbb{Z}[\zeta]$ as

$$x^n + y^n = \prod_{i=0}^{n-1} \left(x + \zeta^i y\right)$$

and compare this factorization with the factorization of z^n in $\mathbb{Z}[\zeta]$ ([13, Edwards]). This method proved to be effective provided that nonzero, nonunit elements in $\mathbb{Z}[\zeta]$ had unique factorization into irreducibles; that is, that $\mathbb{Z}[\zeta]$ is a unique factorization domain (UFD). The discovery that not all algebraic number rings, such as $\mathbb{Z}[\zeta]$, are UFDs sparked the search for some useful generalization of unique factorization. This led Dedekind to the creation of ideals, that is to say the "ideal" elements of the domain, and the discovery that every nonzero, nonunit ideal in an algebraic number ring factors uniquely into prime ideals. It was in this setting that the study of factorization in integral domains arose.

It wasn't too long before mathematicians began to generalize certain properties of UFDs. For example, a UFD has the property that every nonzero, nonunit element has a factorization into a product of a finite number of irreducibles (atoms). A general integral domain R with this

[1] Fermat's Last Theorem had already been reduced to the case when $n > 2$ is prime.

property is called atomic. Examples of atomic domains abound. As mentioned, any UFD is atomic. More generally, any integral domain satisfying the ascending chain condition on principal ideals (ACCP) is atomic [3]. It should be noted that one usually proves that an integral domain is atomic by showing that it satisfies the ACCP. However, there are atomic integral domains that do not satisfy the ACCP [17]. There are also many examples of integral domains that are not atomic. For example, any domain that has an element with an infinite number of prime divisors is not atomic. In particular, the ring of entire functions is not atomic [10]. Atomicity is usually the minimal condition one requires of an integral domain when studying factorization [2].

Another important property of a UFD R is that every nonzero element of R has only a finite number of irreducible divisors, up to associates. A general integral domain with this property is called an irreducible divisors finite (IDF) domain. There are many examples of IDF domains. As mentioned, UFDs are IDF domains. More generally, Krull domains are IDF [18, Proposition 1]. Thus, all algebraic number rings are IDF. What is surprising is how easy it is to produce an integral domain that has a single element with an infinite number of irreducible divisors that are not just unit multiples of one another. The subring

$$\mathbb{R} + X\mathbb{C}[X] = \left\{ \sum_{j=0}^{n} a_i X^i : a_i \in \mathbb{C}, a_0 \in \mathbb{R}, n \in \mathbb{N} \right\}$$

consisting of all polynomials of the UFD $\mathbb{C}[X]$, with constant term in $\mathbb{R}$, is not IDF [3, Example 4.1]. Indeed, the set $\{(r+i)X : r \in \mathbb{R}\}$ forms an infinite set of non-associate irreducible divisors of X^2.

One interesting property of a UFD is that every nonzero element has only finitely many divisors, up to associates, and hence only finitely many factorizations, up to associates. A general integral domain with this property is called a finite factorization domain (FFD). There are many examples of FFDs. As mentioned, any UFD is a FFD. Any Krull domain is an FFD. More generally, a locally finite intersection of FFDs is again an FFD [4, Theorem 2.2]. There are a couple of important theorems on FFDs that are used repeatedly throughout this dissertation. The first is a theorem that links the notion of a FFD with the notions of IDF and atomicity [4, Theorem 1], and states that an integral domain R is an FFD if and only if R is an atomic IDF domain. Another

[2] There are times when one will not assume atomicity when studying factorization. For example, if a domain is Schreier and atomic, it is a UFD. So, one does not assume the integral domain is atomic when studying the Schreier property.

important property of FFDs is that it behaves well with respect to polynomial extensions. That is, [3, Theorem 5.3] states that an integral domain R is an FFD if and only if $R[X]$ is an FFD.

Three factorization properties will be the central objects of study in this dissertation; the IDPF, almost Schreier, and inside factorial properties. In their 2006 paper, *A Class of Integral Domains Between Factorial Domains and IDF Domains* [21], Malcolmson and Okoh discuss a notion of factorization that is a stronger condition on an integral domain than the IDF property, but weaker than the unique factorization property. Given a nonzero, nonunit element a in an integral domain R, let $D_n(a)$ denote the set of non-associate irreducible divisors of a^n. The domain R is said to be *irreducible divisors of powers finite (IDPF)* if for each nonzero, nonunit element $a \in R$, the union $\bigcup_{n=1}^{\infty} D_n(a)$ is finite, up to associates. There are many important examples of IDPF domains. Clearly, any UFD is IDPF. More generally, Krull domains are IDPF [21, Corollary 3.3]. Thus, any algebraic number ring is IDPF. Recall that a ring extension T of R is a *root extension* if for each $t \in T$, there is a natural number n such that $t^n \in R$. One of the main theorems on IDPF domains that we will use repeatedly throughout this paper states that if R is a Noetherian domain with integral closure $\widetilde{R}$ and nonzero conductor ideal $[R :_R \widetilde{R}]$, then R is IDPF if and only if $U(\widetilde{R})/U(R)$ is a finite group and $R \subseteq \widetilde{R}$ is a root extension [14, Theorem 2.8]. This theorem allows us to determine, with relative ease, which Noetherian domains are IDPF. For example, let K be a field of characteristic zero. Then, the cuspidal algebra

$$K[X^2, X^3] = \{f(x) \in K[X] : \text{the coefficient of the linear term is } 0\} \cong K[X, Y]/\left(Y^2 - X^3\right),$$

is not IDPF [21, Proposition 4.1]. Indeed, $\widetilde{K[X^2, X^3]} = K[X]$ and $X^2 \in [K[X^2, X^3] : K[X]]$. Now, $K[X^2, X^3] \subseteq K[X]$ is not a root extension, whence $K[X^2, X^3]$ is not IDPF.

Another factorization property that will be studied in this dissertation is the almost Schreier property. A nonzero element p of an integral domain R is said to be *primal* if whenever $p \mid xy$, there exist $p_1,\ p_2 \in R$ such that $p = p_1 p_2$ with $p_1 \mid x$ and $p_2 \mid y$. In their 2010 paper [11], Dumitrescu and Khalid introduce the notion for a nonzero element p of an integral domain R to be almost primal. That is to say, $p \in R - \{0\}$ is *almost primal* if whenever $p \mid xy$, there exists an integer $k \geq 1$ and $p_1,\ p_2 \in R$ such that $p^k = p_1 p_2$ with $p_1 \mid x^k$ and $p_2 \mid y^k$. They define R to be *almost Schreier* if every nonzero element of R is almost primal. Unlike FFDs, the almost Schreier property does not behave well with respect to polynomial ring extensions. For example,

the domain $D = \mathbb{C}[[X^2, X^3]]$, consisting of all formal power series in $\mathbb{C}[[X]]$ with zero linear term, is almost Schreier, but the polynomial ring $D[Y]$ is not [11, Example 4.2]. However, if R is an integrally closed almost Schreier domain, then $R[X]$ is almost Schreier [11, Theorem 4.4].

1.2 Outline of the Dissertation

In Chapter 2, we investigate when graded domains are almost Schreier and inside factorial. Let $R = \bigoplus_{m \in M} R_m$ be an M-graded domain, where M is a torsion-free, commutative, cancellative monoid. In Section 2.2, we give a classification of when graded domains are almost Schreier, under the assumption that $R \subseteq \widetilde{R}$ is a root extension (see Theorem 10). As a corollary, we give a classification of the commutative semigroup rings $R[M]$ that are almost Schreier, under the assumption that $R[M] \subseteq \widetilde{R[M]}$ is a root extension (see Corollary 14). In Section 2.3, we give a classification of when graded domains are inside factorial, via the almost primal property (see Theorem 15). As a corollary, we offer a new proof of the well known result due to Krause ([20, Theorem 3.2]) as to when commutative semigroup rings are inside factorial (see Corollary 16).

In Chapter 3, we continue to explore commutative semigroup rings, but this time in relation to the IDPF property. Our main result in this chapter states that given an atomic (IDPF) domain R of characteristic zero and a proper numerical semigroup S, $R[S]$ will never be IDPF, even though they are all FFDs (see Theorem 25). We also determine when numerical semigroup rings $R[S]$ of characteristic $q > 0$ are IDPF (see Theorem 26).

In Chapter 4, we study the orders R of the quadratic integer rings such that $R[X]$ is IDPF. Let n be the least positive integer in $[R :_R \widetilde{R}]$. We show that $R[X]$ is IDPF if and only if every prime divisor p of n also divides $\delta_{\mathbb{Q}(\sqrt{d})}$, the discriminant of $\mathbb{Q}(\sqrt{d})$, and R is IDPF (see Theorem 35). In Section 4.5, we explore when certain orders R of the ring of integers in cyclotomic field extensions are such that $R[X]$ is IDPF. In particular, we will see that for orders R in the ring of integers in cyclotomic field extensions, we lose the number theoretic criterion that we have for the ring of integers in quadratic field extensions, for determining precisely when $R[X]$ is IDPF.

In Chapter 5, we tie all of these factorization properties together (see Corollary 42) by showing that for a well known class of rings, the factorization properties that we have been studying are all equivalent. In particular, we show that given an order R of the quadratic integer rings, the following are equivalent:

1. $R[X]$ is IDPF

2. $R[X]$ is almost Schreier

3. $R[X]$ is inside factorial

4. $R[X] \subseteq \widetilde{R[X]}$ is a root extension

5. Every prime divisor of n also divides $\delta_{\mathbb{Q}(\sqrt{d})}$, where n is the least positive integer in $[R :_R \widetilde{R}]$.

In Chapter 6, we discuss what we have done and outline some ideas for future work. For the reader's convenience, we provide an appendix consisting of the main definitions used throughout this dissertation (see Appendix A).

Chapter 2

The Inside Factorial and Almost Schreier Properties in Graded Domains

2.1 Introduction

Let $R = \bigoplus_{m \in M} R_m$ be an M-graded domain, where M is a torsion-free, cancellative, commutative monoid, and let S denote the set of nonzero homogeneous elements of R. One often likes to know if the M-graded domain R has a property $\mathcal{P}$ if and only if the homogeneous elements of R have the same property. For example, it is well known that the M-graded domain R is a UFD if and only if R is a graded UFD (that is, M is a factorial monoid) and R_S is a UFD ([1, Theorem 4.4]).

Recall that a nonzero element of an integral domain R is said to be *primal* if whenever $a \mid b_1 b_2$ in R, there exist $a_1,\ a_2 \in R$ such that $a = a_1 a_2$ with $a_i \mid b_i$ in R, for $i = 1,\ 2$. The integral domain R is said to be *pre-Schreier* if every nonzero element a of R is primal. If R is an integrally closed pre-Schreier domain, then R is said to be *Schreier*. Finally, we call a graded domain $R = \bigoplus_{m \in M} R_m$ *gr-pre-Schreier* if whenever $s \mid xy$, where $s,\ x,\ y \in S$, there exist $s_1,\ s_2 \in S$ such that $s = s_1 s_2$ with $s_1 \mid x$ and $s_2 \mid y$. In their paper [7, Theorem 2.1], Brookfield and Rush determine when an M-graded domain is pre-Schreier.

Theorem A [7]: Let $R = \bigoplus_{m \in M} R_m$ be an M-graded domain, where M is a torsion-free, commutative, cancellative monoid. Let S denote the set of nonzero homogeneous elements. Then, the following are equivalent:

1. R is pre-Schreier
2. The homogeneous elements of R are primal
3. R is gr-pre-Schreier and $I = (s) :_R (x)$ is a homogeneous ideal for each $s \in S$ and $x \in R$.

So, we have seen a couple of examples of when an M-graded domain $R = \bigoplus_{m \in M} R_m$ has a property $\mathcal{P}$ if and only if the homogeneous elements of R have the property $\mathcal{P}$.

In their 2010 paper [11], Dumitrescu and Khalid investigate a generalization of the pre-Schreier property.

Definition 1 A nonzero element a of an integral domain R is said to be *almost primal* if whenever $a \mid b_1 b_2$, there exists an integer $k \geq 1$ and $a_1,\ a_2 \in R$ such that $a^k = a_1 a_2$ with $a_i \mid b_i^k$ for $i = 1,\ 2$. R is said to be *almost Schreier* if every nonzero element of R is almost primal.

We will also need the following three definitions:

Definition 2 Let $R = \bigoplus_{m \in M} R_m$ be an M-graded domain. We say that R is *gr-almost-Schreier* if whenever $s \mid xy$, where $s,\ x,\ y \in S$, there exists an integer $k \geq 1$ such that $s^k = s_1 s_2$ with $s_1 \mid x^k$ and $s_2 \mid y^k$.

Definition 3 Let $R \subseteq T$ be an extension of rings. Then, we say that $R \subseteq T$ is a *root extension* if for each $t \in T$, there exists an integer $k \geq 1$ such that $t^k \in R$.

Definition 4 Let $x \in \bigoplus_{m \in M} R_m$ be an M-graded integral domain. Let $x = x_1 + x_2 + \cdots + x_n$ be the unique representation of x as a sum of homogeneous elements. Then, the *content of* x is $C(x) = (x_1, \ldots, x_n)$.

In Section 2.2, we prove an analog of Brookfield and Rush's result for when graded domains are pre-Schreier.

Theorem B [5]: Let $R = \bigoplus_{m \in M} R_m$ be an M-graded domain and suppose $R \subseteq \widetilde{R}$ is a root extension, where $\widetilde{R}$ denotes the integral closure of R. Let S denote the set of nonzero homogeneous elements of R. Then the following conditions are equivalent:

1. R is almost Schreier
2. the homogeneous elements of R are almost primal
3. R is gr-almost-Schreier and whenever $y \in (s) :_R (x)$, where $x,\ y \in R$ and $s \in S$, there exists an integer $k \geq 1$ such that $C(y^k) \subseteq (s^k) :_R C(x^k)$.

We then specialize to the case of semigroup rings and prove that if $R[M] \subseteq \widetilde{R[M]}$ is a root extension, where the monoid M is a torsion-free, commutative, cancellative monoid, then $R[M]$ is almost Schreier if and only if R is an almost Schreier domain and M is an almost Schreier monoid.

In Section 2.3, we explore when graded domains are inside factorial. We need the following definitions:

Definition 5 A monoid homomorphism $\phi : D \to H$ is called a *divisor homomorphism* if for any $a,\ b \in D$, $\phi(a) \mid \phi(b)$ in H implies $a \mid b$ in D.

Definition 6 A monoid H is called *inside factorial* if there exists a divisor homomorphism $\phi : D \to H$ from a factorial monoid D such that for every $x \in H$ there exists some $n \in \mathbb{N}$ such that $x^n \in \phi(D)$. An integral domain R is called *inside factorial* if its multiplicative monoid $R^* = R - \{0\}$ is inside factorial.

In particular, we classify when an M-graded domain $R = \bigoplus_{m \in M} R_m$ is inside factorial in terms of the almost primal property, where M is a torsion-free, commutative, cancellative monoid. As a corollary, we offer a new proof of the well known result due to Krause ([20, Theorem 3.2]), which states that given a monoid domain $R[M]$ with trivial invertible elements, $R[M]$ is inside factorial if and only if R is an inside factorial domain, M is an inside factorial monoid, and $R[M] \subseteq \widetilde{R[M]}$ is a root extension.

2.2 Graded Domains and the Almost Schreier Property

Let $R = \bigoplus_{m\in M} R_m$ be an M-graded domain, where M is a torsion-free, cancellative, commutative monoid and let S denote the set of non-zero homogeneous elements of R. Consider the following condition:

(†): For any nonempty finite subsets $Y_1,\ Y_2 \subseteq M$ and $x \in M$ such that $x \mid Y_1Y_2$, there are $z_1,\ z_2 \in M$ and an integer $k \geq 1$ such that $x^k = z_1z_2$ with $z_1 \mid Y_1^k$ and $z_2 \mid Y_2^k$.

We have the following lemma:

Lemma 7 *If M is a cancellative monoid which is almost Schreier, then M satisfies (†).*

Proof. See [5]. ■

Let (††) denote the following property:

(††): If $x,\ y \in R$, $s \in S$ and $y \in (s) :_R (x)$, then $C(y^k) \subseteq (s^k) :_R C(x^k)$ for some positive integer k.

The following lemmas are from [5]. We give the proofs here.

Lemma 8 *Suppose $R = \bigoplus_{m\in M} R_m$ is an M-graded domain, where M is a cancellative, torsionless, commutative monoid. If R is almost Schreier, then R satisfies (††).*

Proof. Let $y \in (s) :_R (x)$. Then, $xy \in (s)$ and hence $xy = sz$, for some $z \in R$. So, $s \mid xy$. Thus, $s^k = s_1s_2$ with $s_1 \mid x^k$ and $s_2 \mid y^k$. Now, write $y^k = s_2y'$, where $y' \in R$. Then, $y^k \in (s_2)$, a homogeneous ideal. Thus, $C(y^k) \subseteq (s_2)$. Now, s_1 divides every member of $C(x^k)$. Let $x^k = x_1+x_2+\cdots+x_n$, where $x_i \in R_{\alpha_i}$ and $\alpha_i = \alpha_j$ if and only if $i = j$. Then, $s_1 \mid x_i$ for all i. Thus, $x_i = s_1x_i'$, where $x_i' \in R$, for all i. Hence, $s_2x_i = s^kx_i'$ and thus, $s_2 \in (s^k) :_R (x_i)$ for all i.

So, $s_2 \in \bigcap_{i=1}^{n} ((s^k) :_R (x_i)) = (s^k) :_R (x_1,\ x_2,\ \ldots, x_n) = (s^k) :_R C(x^k)$. Thus,
$(s_2) \subseteq (s^k) :_R C(x^k)$. So, $C(y^k) \subseteq (s^k) :_R C(x^k)$. ■

Lemma 9 *Suppose $R = \bigoplus_{m\in M} R_m$ is an M-graded domain, where M is a cancellative, torsionless, commutative monoid. Let S denote the set of non-zero homogeneous elements of R. Suppose R is graded almost Schreier, R satisfies (††) and $R \subseteq \widetilde{R}$ is a root extension. Then, every $s \in S$ is almost primal in R.*

Proof. Let $s \mid xy$. Then, $xy = sr$, for some $r \in R$. Thus, $y \in (s) :_R (x)$. So, by (††),
$C(y^k) \subseteq (s^k) :_R C(x^k)$ for some integer $k \geq 1$. Thus, $C(x^k)C(y^k) \subseteq (s^k)$. So, s^k divides every

member of $C(x^k)C(y^k)$. Let $x = x_1 + x_2 + \cdots + x_n,\ x_i \in R_{\alpha_i},\ \alpha_i = \alpha_j$ if and only if $i = j$, and $y = y_1 + y_2 + \cdots + y_m,\ y_j \in R_{\beta_j},\ \beta_i = \beta_j$ if and only if $i = j$. Now, $x^k = \sum x'_i$ and $y^k = \sum y'_j$, where each monomial x'_i is of the form $x_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}$, where $\sum l_i = k$, and each monomial y'_j is of the form $y_1^{b_1}y_2^{b_2}\cdots y_m^{b_m}$, where $\sum b_j = k$. By Lemma 7, there exists an integer $t \geq 1$ and $s_1,\ s_2 \in S$ such that $s^{kt} = s_1s_2$ with $s_1 \mid x_i'^t$ and $s_2 \mid y_j'^t$ for every i and j. Now, by [24, Corollary 3.3], $s_1 \mid x_1'^{t_1}x_2'^{t_2}\cdots x_n'^{t^n}$, where $\sum t_i = t$, in $\widetilde{R}$. Also, by [24, Corollary 3.3], $s_2 \mid y_1'^{a_1}y_2'^{a_2}\cdots y_m'^{a_m}$, where $\sum a_j = t$. So, s_1 divides each element of $C(x^{kt})$ and s_2 divides each element of $C(y^{kt})$ in $\widetilde{R}$. Thus, $s^{kt} = s_1s_2,\ s_1 \mid x^{kt}$, and $s_2 \mid y^{kt}$ in $\widetilde{R}$. As $R \subseteq \widetilde{R}$ is a root extension, there exists an integer $w \geq 1$ such that $s^{ktw} = s_1^w s_2^w$ and $s_1^w \mid x^{ktw}$ and $s_2^w \mid y^{ktw}$ in R. ■

We would like to determine when graded domains are almost Schreier. We have the following theorem.

Theorem 10 *Let $R = \bigoplus_{m\in M} R_m$ be an M-graded domain, where M is a cancellative, torsionless, commutative monoid. Let S denote the set of non-zero homogeneous elements of R. Suppose $R \subseteq \widetilde{R}$ is a root extension. Then, the following conditions are equivalent:*

1. *R is almost Schreier*
2. *Every element $s \in S$ is almost primal in R*
3. *R is gr-almost-Schreier and R satisfies (††).*

Proof.

(1) ⇒ (2): As R is almost Schreier, every element in the saturated multiplicative set S is almost primal in R.

(2) ⇒ (1): R_S is a GCD-Domain [1, Proposition 2.1], and is hence almost Schreier [11, Proposition 2.2(a)]. As every $s \in S$ is almost primal in R, it follows that R is almost Schreier [11, Theorem 4.3].

(1) ⇒ (3): As R is almost Schreier, R is gr-almost-Schreier. The fact that R satisfies (††) follows from Lemma 8.

(3) ⇒ (2): This follows from Lemma 9. ■

We will now specialize to commutative semigroup rings. Given a domain R and a torsion-free, cancellative, commutative monoid M, one often likes to know if the semigroup ring $R[M]$ satisfies a property $\mathcal{P}$ if and only if the domain R and the monoid M satisfy the property $\mathcal{P}$. For the almost Schreier property, we will show that if $R[M] \subseteq \widetilde{R[M]}$ is a root extension, then $R[M]$ is almost Schreier if and only if R is an almost Schreier domain and M is an almost Schreier monoid. To do this, we need the following definition and lemmas (from [5]).

Definition 11 A commutative monoid ring $R[M]$ is said to have *trivial invertible elements* if $M \cap -M = \{0\}$.

Lemma 12 *Let R be an almost Schreier domain, M a torsion-free, commutative cancellative, almost Schreier monoid, and $R[M] \subseteq \widetilde{R[M]}$ a root extension. Suppose $R[M]$ has trivial invertible elements. Then, $R[M]$ is gr-almost- Schreier and satisfies (††).*

Proof. Suppose $r_1X^{\alpha_1} \mid r_2X^{\alpha_2}r_3X^{\alpha_3}$ in $R[M]$. Then, $r_1 \mid r_2r_3$ in R and $\alpha_1 \leq \alpha_2 + \alpha_3$ in M. Since R is almost Schreier, there exists an integer $k_1 \geq 1$ and $w_2,\ w_3$ in R such that $r_1^{k_1} = w_2w_3$ with $w_2 \mid r_2^{k_1}$ and $w_3 \mid r_3^{k_1}$ in R. Also, $\alpha_1 \leq \alpha_2 + \alpha_3$ implies that there exists an integer $k_2 \geq 1$ and $\beta_2,\ \beta_3 \in M$ such that $k_2\alpha_1 = \beta_2 + \beta_3$ and $\beta_2 \leq k_2\alpha_2$ and $\beta_3 \leq k_2\alpha_3$. Let $k = \text{lcm}(k_1,\ k_2)$. Then, $r_1^k = w_2^{k_2}w_3^{k_2}$, with $w_2^{k_2} \mid r_2^k$ and $w_3^{k_2} \mid r_3^k$. Also, $k\alpha_1 = k_1\beta_2 + k_1\beta_3$ with $k_1\beta_2 \leq k\alpha_2$ and $k_1\beta_3 \leq k\alpha_3$. So,

$$(r_1X^{\alpha_1})^k = \left(w_2^{k_2}X^{k_1\beta_2}\right)\left(w_3^{k_2}X^{k_1\beta_3}\right)$$

with $w_2^{k_2}X^{k_1\beta_2} \mid (r_2X^{\alpha_2})^k$ and $w_3^{k_2}X^{k_1\beta_3} \mid (r_3X^{\alpha_3})^k$. So, $R[M]$ is gr-almost-Schreier.

It remains to show that $R[M]$ satisfies (††). We first show that $\widetilde{R}$ and $\widetilde{M}$ are almost Schreier. For, let K be the quotient field of R, and suppose $r \in K$ is integral over R. Then, $r \in \widetilde{R} \subseteq \widetilde{R[M]}$. So, $r^k \in R[M]$, for some positive integer k, and hence $r^k \in R$. So, $R \subseteq \widetilde{R}$ is a root extension. As R is almost Schreier, it follows that $\widetilde{R}$ is almost Schreier [11, Proposition 2.2(d)]. Also, let $\alpha \in \widetilde{M}$. Then, $X^\alpha \in \widetilde{R[M]}$. Thus, there exists an integer $k \geq 1$ such that $X^{\alpha k} \in R[M]$. So, $\alpha k \in M$. So, $M \subseteq \widetilde{M}$ is a root extension. As M is almost Schreier, it follows that $\widetilde{M}$ is almost Schreier [11, Proposition 2.2(d)].

We now show $R[M]$ satisfies (††). Let $g \in (rX^\alpha) :_{R[M]} (f)$, where $f,\ g \in R[M]$ and rX^α is a homogeneous element of $R[M]$. So, $rX^\alpha \mid fg$ in $R[M]$, and hence in $\widetilde{R[M]}$. So, rX^α divides every element of $C(fg)$ in $\widetilde{R[M]}$. As $\widetilde{R[M]}$ is integrally closed, $(C(fg))_v = (C(f)C(g))_v$ [2, Theorem

3.5(1)]. So, rX^{α} divides every element of $C(f)C(g)$ in $\widetilde{R[M]}$. Let $f = r_1X^{\alpha_1} + \cdots + r_nX^{\alpha_n}$, $\alpha_1 < \cdots < \alpha_n$, and $g = s_1X^{\beta_1} + \cdots + s_mX^{\beta_m}$, $\beta_1 < \cdots < \beta_m$. Then, $r \mid r_is_j$ for all i and j in $\widetilde{R}$. As $\widetilde{R}$ is almost Schreier, Lemma 7 implies that there exists a positive integer $k_1 \geq 1$ and $z,\ w \in \widetilde{R}$ such that

$$r^{k_1} = zw \text{ with } z \mid r_i^{k_1} \text{ and } w \mid s_j^{k_1},$$

for all i and j. Also, $X^{\alpha} \mid X^{\alpha_i}X^{\beta_j}$, for all i and j. So, $\alpha \leq \alpha_i + \beta_j$ for all i and j. As $\widetilde{M}$ is almost Schreier, Lemma 7 implies that there exists an integer $k_2 \geq 1$ and $\gamma_1,\ \gamma_2 \in \widetilde{M}$ such that

$$k_2\alpha = \gamma_1 + \gamma_2 \text{ with } \gamma_1 \leq k_2\alpha_i \text{ and } \gamma_2 \leq k_2\beta_j$$

for all i and j. Now, let $k = \operatorname{lcm}(k_1,\ k_2)$. Then,

$$r^k = z^{k_2}w^{k_2},\ \text{with } z^{k_2} \mid r_i^k,\ \text{and } w^{k_2} \mid s_j^k,$$

for all i and j. Also,

$$k\alpha = k_1\gamma_1 + k_1\gamma_2,\ \text{with } k_1\gamma_1 \leq k\alpha_i,\ \text{and } k_1\gamma_2 \leq k\beta_j,$$

for all i and j. Thus,

$$(rX^{\alpha})^k = \left(z^{k_2}X^{k_1\gamma_1}\right)\left(w^{k_2}X^{k_1\gamma_2}\right) \text{ with } z^{k_2}X^{k_1\gamma_1} \mid (r_iX^{\alpha_i})^k \text{ and } w^{k_2}X^{k_1\gamma_2} \mid \left(s_jX^{\beta_j}\right)^k,$$

in $\widetilde{R[M]}$.

As $\widetilde{R[M]}$ is integrally closed, $z^{k_2}X^{k_1\gamma_1} \mid (r_1X^{\alpha_1})^{l_1} \cdots (r_nX^{\alpha_n})^{l_n}$, where $\sum l_i = k$, in $\widetilde{R[M]}$ [24, Corollary 3.3]. Also, $w^{k_2}X^{k_1\gamma_2} \mid \left(s_1X^{\beta_1}\right)^{b_1} \cdots \left(s_mX^{\beta_m}\right)^{b_m}$, where $\sum b_j = k$ in $\widetilde{R[M]}$ [24, Corollary 3.3]. So,

$$r^kX^{\alpha k} = \left(z^{k_2}X^{k_1\gamma_1}\right)\left(w^{k_2}X^{k_1\gamma_2}\right) \text{ with } z^{k_2}X^{k_1\gamma_1} \mid f^k \text{ and } w^{k_2}X^{k_1\gamma_2} \mid g^k,$$

in $\widetilde{R[M]}$. Since $R[M] \subseteq \widetilde{R[M]}$ is a root extension, there exists an integer $T \geq 1$ such that

$$(rX^{\alpha})^{kT} = \left(z^{k_2T}X^{k_1\gamma_1T}\right)\left(w^{k_2T}X^{k_1\gamma_2T}\right) \text{ with } z^{k_2T}X^{k_1\gamma_1T} \mid f^{kT} \text{ and } w^{k_2T}X^{k_1\gamma_2T} \mid g^{kT},$$

in $R[M]$. So, $z^{k_2T}X^{k_1\gamma_1T}$ divides every element of $C(f^{kT})$ in $R[M]$ and $w^{k_2T}X^{k_1\gamma_2T}$ divides every element of $C(g^{kT})$ in $R[M]$. Thus,

$$(rX^{\alpha})^{kT} = \left(z^{k_2T}X^{k_1\gamma_1T}\right)\left(w^{k_2T}X^{k_1\gamma_2T}\right)$$

divides every element of $C(f^{kT})C(g^{kT})$ in $R[M]$. So,

$$C(f^{kT})C(g^{kT}) \subseteq \left((rX^{\alpha})^{kT}\right),$$

and hence

$$C(g^{kT}) \subseteq \left((rX^{\alpha})^{kT}\right) :_{R[M]} C(f^{kT}).$$

So, $R[M]$ satisfies (††). ■

Lemma 13 *Let $R[M]$ be a semigroup ring with trivial invertible elements. If $R[M]$ is almost-Schreier, then R is an almost Schreier domain and M is an almost Schreier monoid.*

Proof. Let $r \mid xy$ in R. Then, there exists an integer $k \geq 1$ and $r_1,\ r_2 \in R[M]$ such that $r^k = r_1r_2$, $r_1 \mid x^k,\ \ r_2 \mid y^k$. Since the degree of r is 0, it follows that the degree of r_1 and r_2 is 0 since $R[M]$ is a semigroup ring with trivial invertible elements. Thus, $r_1,\ r_2 \in R$. So, R is almost Schreier. Now, suppose $\alpha \leq \alpha_1 + \alpha_2$. Then, $X^{\alpha} \mid X^{\alpha_1}X^{\alpha_2}$. As $R[M]$ is graded almost Schreier, there exists an integer $k \geq 1$, and $f_1,\ f_2 \in R[M]$ such that $f_1 \mid X^{\alpha_1 k}$ and $f_2 \mid X^{\alpha_2 k}$. By [15, Theorem 11.1], f_1 and f_2 are monomials. So, $f_1 = uX^{\beta_1}$ and $f_2 = u^{-1}X^{\beta_2}$. Thus, $X^{\alpha k} = uX^{\beta_1}u^{-1}X^{\beta_2},\ \ uX^{\beta_1} \mid X^{\alpha_1 k}$ and $u^{-1}X^{\beta_2} \mid X^{\alpha_2 k}$. So, $\alpha k = \beta_1 + \beta_2$ and $\beta_1 \leq \alpha_1 k$ and $\beta_2 \leq \alpha_2 k$. So, M is almost Schreier. ■

Corollary 14 *Suppose $R[M] \subseteq \widetilde{R[M]}$ is a root extension and $R[M]$ has trivial invertible elements. Then, $R[M]$ is almost Schreier if and only if R is an almost Schreier domain and M is an almost Schreier monoid.*

Proof. Suppose $R[M]$ is almost Schreier. Since $R[M]$ has trivial invertible elements, it follows from Lemma 13 that R is an almost Schreier domain and M is an almost Schreier monoid. Conversely,

suppose R is an almost Schreier domain and M is an almost Schreier monoid. As $R[M] \subseteq \widetilde{R[M]}$ is a root extension, Lemma 12 implies that $R[M]$ is graded almost Schreier and $R[M]$ satisfies (††). Thus, by (1) $\Leftrightarrow$ (3) of Theorem 10, $R[M]$ is almost Schreier. ■

2.3 When Graded Domains are Inside Factorial

In this section, we answer the question as to when graded domains are inside factorial. As a corollary, we offer a new proof of the well known result due to Krause [20, Theorem 3.2], which states that, given a monoid ring $R[M]$, where M is a torsion-free, commutative, cancellative monoid and $R[M]$ has trivial invertible elements, $R[M]$ is an inside factorial domain if and only if R is an inside factorial domain, M is an inside factorial monoid, and $R[M] \subseteq \widetilde{R[M]}$ is a root extension.

Recall that a *Krull domain* is a locally finite intersection of valuation rings $\{V_\lambda\}$ which are rank one discrete. A *generalized Krull domain* is a locally finite intersection of rank one valuation rings $\{V_\lambda\}$ and a *rational generalized Krull domain* is a generalized Krull domain such that the value group of each valuation ring V_λ is order isomorphic to an additive subgroup of $\mathbb{Q}$.

Theorem 15 *Let $R = \bigoplus_{m \in M} R_m$ be an M-graded domain, where M is a cancellative, torsionless, commutative monoid. Let S denote the set of non-zero homogeneous elements of R. Then, the following conditions are equivalent:*

1. *R is inside factorial*
2. *Every element $s \in S$ is almost primal in R, $R \subseteq \widetilde{R}$ is a root extension, and $\widetilde{R}$ is a rational generalized Krull domain.*
3. *R is gr-almost-Schreier, R satisfies (††), $R \subseteq \widetilde{R}$ is a root extension, and $\widetilde{R}$ is a rational generalized Krull domain.*

Proof.

(1) $\Rightarrow$ (2): As R is inside factorial, $R \subseteq \widetilde{R}$ is a root extension and $\widetilde{R}$ is a rational generalized Krull domain [8, Theorem 7(a)]. Also, R inside factorial implies that R is almost Schreier [11, Proposition 2.2(e)]. In particular, the homogeneous elements of R are almost primal in R.

(2) $\Rightarrow$ (1): R_S is a GCD-domain [1, Proposition 2.1] and hence almost Schreier [11, Proposition 2.2(a)]. Since every element of S is almost primal in R, R is almost Schreier [11, Theorem 4.3]. But, $R \subseteq \widetilde{R}$ is a root extension. So, $\widetilde{R}$ is almost Schreier [11, Proposition 2.2(d)]. Thus, $Cl_t(\widetilde{R})$ is torsion [11, Theorem 3.1]. As $Cl_t(\widetilde{R})$ is torsion, $R \subseteq \widetilde{R}$ is a root extension, and $\widetilde{R}$ is a rational generalized Krull domain, it follows that R is inside factorial [8, Theorem 7(a)].

(1) $\Rightarrow$ (3): R inside factorial implies that $R \subseteq \widetilde{R}$ is a root extension and $\widetilde{R}$ is a rational generalized Krull domain [8, Theorem 7(a)]. Now, R inside factorial implies that R is almost Schreier [11, Proposition 2.2(e)] and hence R is gr-almost-Schreier. Lemma 8 implies that R satisfies (††).

(3) $\Rightarrow$ (2): This follows from Lemma 9. ■

We are now ready to specialize to semigroup rings and offer a new proof of [20, Theorem 3.2], as a corollary of Theorem 15.

Corollary 16 *Let M be a cancellative, torsion-free, commutative monoid, with trivial invertible elements. Then, $R[M]$ is inside factorial if and only if R is an almost Schreier domain, M is an almost Schreier monoid, $R[M] \subseteq \widetilde{R[M]}$ is a root extension, and $\widetilde{R[M]}$ is a rational generalized Krull domain.*

Proof. Suppose $R[M]$ is inside factorial. Then, $R[M] \subseteq \widetilde{R[M]}$ is a root extension and $\widetilde{R[M]}$ is a rational generalized Krull domain [8, Theorem 7(a)]. As $R[M]$ is inside factorial, $R[M]$ is almost Schreier [11, Proposition 2.2(e)]. By Lemma 13, R is an almost Schreier domain and M is an almost Schreier monoid.

Conversely, suppose that R is an almost Schreier domain, M is an almost Schreier monoid, $R[M] \subseteq \widetilde{R[M]}$ is a root extension, and $\widetilde{R[M]}$ is a rational generalized Krull domain. By Lemma 12, it follows that $R[M]$ is gr-almost-Schreier and that $R[M]$ satisfies (††). By (1) $\Leftrightarrow$ (3), $R[M]$ is inside factorial. ■

2.4 Conclusion

We have seen for an M-graded domain R with $R \subseteq \widetilde{R}$ a root extension, where $\widetilde{R}$ denotes the integral closure of R, that R is almost Schreier if and only if each nonzero homogeneous element of R is almost primal if and only if R is gr-almost-Schreier and whenever $y \in (s) :_R (x)$, where $s \neq 0$ is homogeneous and $x,\ y \in R$, then $C(y^k) \subseteq (s^k) :_R C(x^k)$, for some integer $k \geq 1$ (Theorem 10).

Question 17 *We wonder if an M-graded domain R, where M is a torsion-free, commutative, cancellative monoid, is almost Schreier implies $R \subseteq \widetilde{R}$ is a root extension?*

We were unable to determine if this is the case or not. In Chapter 5, we classify the orders R of the quadratic integer rings such that $R[X]$ is almost Schreier and we link this up with two other factorization properties; namely, the IDPF property and the inside factorial property. As a corollary to Theorem 10, we have found that if $R[M] \subseteq \widetilde{R[M]}$ is a root extension, then $R[M]$ is almost Schreier if and only if R is an almost Schreier domain and M is an almost Schreier monoid (Corollary 14). We have also given a classification of the M-graded domains that are inside factorial via the almost primal property (Theorem 15). As a corollary, we offered a new proof to the well known result of Krause ([20, Theorem 3.2]) which classifies when commutative semigroup rings are inside factorial (Corollary 16).

In the next chapter, we continue our investigation of commutative semigroup rings and determine when a particular class of commutative semigroup rings, the numerical semigroup rings, have the IDPF property (Theorem 25, Theorem 26).

Chapter 3

Numerical Semigroup Rings and the IDPF Property

3.1 Introduction

Factorization in commutative semigroup rings is not as nice as one would hope. For example, let K be a field. It is well known that $K[X;\langle 2,3\rangle]$ is not a UFD, or an HFD for that matter, since the element X^6 has two factorizations, into irreducibles, in $K[X;\langle 2,3\rangle]$; namely, $X^6 = X^2X^2X^2 = X^3X^3$. Recall the following factorization property:

Definition 18 Let R be an integral domain and let $a \in R$ be a nonzero, nonunit element. Let $D_n(a)$ denote the set of non-associate irreducible divisors of a^n. Then, R is said to be *irreducible divisors of powers finite (IDPF)* if for every nonzero, nonunit $a \in R$, the set $D(a) = \bigcup_{n=1}^{\infty} D_n(a)$ is finite.

In 2006, Malcolmson and Okoh showed that $K[X;\langle 2,3\rangle]$ is not even IDPF [21, Proposition 4.1]. More generally, they showed that for any integral domain R of characteristic zero, the cuspidal algebra $R[X;\langle 2,p+2\rangle]$ is not IDPF for any odd prime p or $p = 1$ [21, Proposition 4.1]. Before we state the main result of this chapter, let's recall a few definitions.

Definition 19 A *numerical semigroup* S is a submonoid of $\mathbb{N} = \{0,1,2,\dots\}$ with $\mathbb{Z}$ as the group generated by S.

Definition 20 For a numerical semigroup S, the *Frobenius number of* S, denoted $g = g(S)$, is the largest element of $\mathbb{Z}$ not in S. The *multiplicity* of S, denoted e, is the smallest positive integer in S.

In 1884, Sylvester proved that the Frobenius number of a numerical semigroup with two relatively prime generators n_1 and n_2, is given by $g(\langle n_1, n_2\rangle) = (n_1 - 1)(n_2 - 1) - 1$. Interestingly, there is no known closed formula for the Frobenius number of a numerical semigroup S with three or more generators. However, it is well known that given a positive integer a, there exists a numerical semigroup S such that $g(S) = a$. In this paper, we extend Malcolmson and Okoh's result. We show that given any atomic integral domain R of characteristic zero and any proper numerical semigroup S, it follows that $R[X; S] = R[S]$ is not IDPF. From the results of Etingof, Malcolmson, and Okoh in [14], we can deduce some special cases of our theorem. For example, since the integral closure of $R[S]$ is $R[X]$ and $X^{g(S)+1} \in [R[S] : R[X]]$, if R is Noetherian, one sees by [14, Theorem 2.8] that $R[S]$ is not IDPF, since $R[S] \subseteq R[X]$ is not a root extension. They also show that if K is a field of characteristic zero, then any K-subalgebra R of $K[X]$ that is IDPF is isomorphic to $K[X]$ [14, Theorem 2.11]. So, this result shows that $K[X; S]$ is never IDPF, when K is a field of characteristic zero (this also follows from [14, Theorem 2.8]). So, our result extends the non-IDPF status of the numerical semigroup rings $R[S]$, when R is atomic and not Noetherian. For example, if R has characteristic zero and satisfies the ascending chain condition on principal ideals (that is, R satisfies the ACCP), then $R[S]$ is not IDPF, since if R satisfies the ACCP, then R is atomic [3].

Interestingly, given a numerical semigroup S with Frobenius number $g(S) = p^m$, for p a prime and m a positive integer, the condition that R is atomic can be dropped (Lemma 21). This gives Malcolmson and Okoh's result on the cuspidal algebra as a corollary, since the Frobenius number of the numerical semigroup $\langle 2, p + 2\rangle$,where p is an odd prime, is $g(\langle 2, p + 2\rangle) = p$.

In section 3.3, we settle the case when R has positive characteristic q. Namely, we show that if R is an atomic integral domain of characteristic $q > 0$, and S is a numerical semigroup, then $R[S]$ is IDPF if and only if $R[X]$ is IDPF.

3.2 Proper Numerical Semigroup Rings of Characteristic Zero and IDPF

Before we can prove our main result, we first prove a lemma for the case when the numerical semigroup S has a Frobenius number that is a power of a prime number. Notice that we need not assume that our integral domain R is atomic.

Lemma 21 *Let S be a proper numerical semigroup with Frobenius number $g = p^m$ and let R be an integral domain of characteristic zero. Then, $R[S]$ is not IDPF.*

Proof. To show that $R[S]$ is not IDPF, we produce an element $f(X)$ of $R[S]$ such that $D_s(f(X)) \neq D_{s+1}(f(X))$ for any positive integer s. This shows that $D(f(X)) = \bigcup_{s=1}^{\infty} D_s(f(X))$ is infinite, whence $R[S]$ is not IDPF. Let $f(X) = X^e(X^g - 1)$, where e is the multiplicity of S and g is the Frobenius number of S. Notice that

$$(f(X))^n = X^{ne}(X^g - 1)^n = X^{(n-1)e}X^e(X^g - 1)^n.$$

Let $f_n(X) = X^e(X^g - 1)^n$. We should note that

$$f_n(X) = X^e \sum_{j=0}^{n} \binom{n}{j} (-1)^{n-j} X^{gj} = \sum_{j=0}^{n} \binom{n}{j} (-1)^{n-j} X^{gj+e}$$

belongs to $R[S]$. This follows because when $j = 0$, we get $\pm X^e \in R[S]$, since e is the multiplicity of S, and for $j \geq 1$, $X^{gj+e} \in R[S]$, since g is the Frobenius number of S. To prove that $R[S]$ is not IDPF, it is enough to show that $f_n(X)$ is irreducible for every positive integer n, since $f_j(X)$ and $f_i(X)$ are non-associate when $i \neq j$. So, by way of contradiction, suppose that $f_n(X) = FG$, for some n, where F and G are nonzero, nonunits in $R[S]$. Let K denote the quotient field of R and $\overline{K}$ denote the algebraic closure of K. Since the characteristic of R is zero, we note that K contains $\mathbb{Q}$. Now, in $\overline{K}[X]$,

$$F = X^{l_1} \prod_{i=0}^{g-1} (X - \zeta^i)^{e_i},$$

and

$$G = X^{l_2} \prod_{i=0}^{g-1} (X - \zeta^i)^{d_i},$$

where $l_1,\ l_2,\ e_i,\ d_i$ are nonnegative integers with $l_1 + l_2 = e$, $e_i + d_i = n$, and $\zeta = e^{\frac{2\pi i}{g}}$.

Consider $F = X^{l_1}\prod_{i=0}^{g-1}(X-\zeta^i)^{e_i}$. Then, either $l_1 = 0$ or $l_1 > 0$. Suppose first that $l_1 = 0$, so that $F = \prod_{i=0}^{g-1}(X-\zeta^i)^{e_i}$. Now, since S is a proper numerical semigroup, $1 \notin S$. Thus, the X-coefficient of F must be 0. Now, we get the X-coefficient of F by choosing one term in the product

$$F = (X-\zeta^0)\cdots(X-\zeta^0)(X-\zeta^1)\cdots(X-\zeta^1)\cdots(X-\zeta^{g-1})\cdots(X-\zeta^{g-1}), \tag{3.1}$$

where the factor $X-\zeta^j$ occurs e_j times, taking the product of the remaining constant terms from each factor, and taking a sum over all possible ways of doing this. There are $\binom{e_j}{1}$ ways we can choose the binomial $X-\zeta^j$ in (3.1), for each $0 \le j \le g-1$. Choosing the factor $X-\zeta^j$ and taking a product of the remaining constant terms, we obtain $\prod_{i\neq j}(-\zeta^i)^{e_i}(-\zeta^j)^{e_j-1}$. Taking a sum over all the possibilities, we obtain

$$\begin{aligned} X-\text{coefficient} &= \sum_{j=0}^{g-1} e_j \prod_{i\neq j}(-\zeta^i)^{e_i}(-\zeta^j)^{e_j-1} \\ &= \prod_{i=0}^{g-1}(-\zeta^i)^{e_i-1}\sum_{j=0}^{g-1} e_j \prod_{i\neq j}(-\zeta^i). \end{aligned}$$

But, the X-coefficient $= 0$. So, we get by cancellation that

$$0 = \sum_{j=0}^{g-1} e_j \prod_{i\neq j}(-\zeta^i).$$

Thus,

$$0 = \sum_{j=0}^{g-1} e_j \prod_{i\neq j}(\zeta^i).$$

Now, if $g = p^m$, where p is an odd prime, we get

$$\begin{aligned}\prod_{i\neq j}\zeta^i &= \zeta^{0+1+\cdots+j-1+j+1+\cdots g-1}\\ &= \zeta^{\frac{(g-1)g}{2}-j}\\ &= \zeta^{-j},\end{aligned}$$

since g odd implies 2 divides $g-1$, and $\zeta^g = 1$. Thus,

$$\begin{aligned}0 &= \sum_{j=0}^{g-1} e_j\zeta^{-j}\\ &= \sum_{j=0}^{g-1} e_j(\zeta^{-1})^j\\ &= \sum_{j=0}^{g-1} e_j(\zeta^{g-1})^j.\end{aligned}$$

Since $g-1$ and g are relatively prime, we can apply the $\mathbb{Q}$-automorphism $\zeta \mapsto \zeta^{g-1}$ to $0 = \sum_{j=0}^{g-1} e_j\left(\zeta^{g-1}\right)^j$. Doing so, we obtain,

$$\begin{aligned}0 &= \sum_{j=0}^{g-1} e_j(\zeta^{(g-1)^2})^j\\ &= \sum_{j=0}^{g-1} e_j(\zeta^{(g^2-2g+1)j})\\ &= \sum_{j=0}^{g-1} e_j\zeta^j,\end{aligned}$$

since $\zeta^{g^2} = \zeta^{-2g} = 1$.

Now, if $g = 2^m$, we get

$$\begin{aligned}\prod_{i\neq j}\zeta^i &= \zeta^{0+1+\cdots+j-1+j+1+\cdots+g-1}\\ &= \zeta^{\frac{(g-1)g}{2}-j}\\ &= \zeta^{\frac{(2^m-1)2^m}{2}-j}\\ &= \zeta^{-2^{m-1}}\zeta^{-j}\\ &= (\zeta^{-1})^{2^{m-1}+j}\\ &= (\zeta^{2^m-1})^{2^{m-1}+j}.\end{aligned}$$

So, we have

$$0 = \sum_{j=0}^{g-1} e_j(\zeta^{2^m-1})^{2^{m-1}+j}.$$

Applying the $\mathbb{Q}$-automorphism $\zeta \mapsto \zeta^{2^m-1}$, we obtain

$$\begin{aligned}0 &= \sum_{j=0}^{g-1} e_j\left(\zeta^{(2^m-1)^2}\right)^{2^{m-1}+j}\\ &= \sum_{j=0}^{g-1} e_j\left(\zeta^{2^{2m}-2^{m+1}+1}\right)^{2^{m-1}+j}\\ &= \sum_{j=0}^{g-1} e_j\zeta^{2^{m-1}+j}\\ &= \sum_{j=0}^{g-1} e_j\zeta^{2^{m-1}}\zeta^{j}\\ &= \sum_{j=0}^{g-1} e_j(-1)\zeta^{j},\end{aligned}$$

since $\zeta^{2^{m-1}} = -1$. Thus,

$$0 = \sum_{j=0}^{g-1} e_j\zeta^{j},$$

when $g = 2^m$. So, whether $g = p^m$ has $p = 2$ or p an odd prime, we obtain from the fact that the X-coefficient must be zero, the relation

$$0 = \sum_{j=0}^{g-1} e_j \zeta^j.$$

Now, $[\mathbb{Q}(\zeta_g) : \mathbb{Q}] = \phi(g)$. So, the set $\{\zeta^0, \ldots, \zeta^{\phi(g)-1}\}$ forms a basis for $\mathbb{Q}(\zeta_g)$ over $\mathbb{Q}$. We want to express the ζ^i in $0 = \sum_{j=0}^{g-1} e_j \zeta^j$ in terms of the basis elements $\{\zeta^0, \ldots, \zeta^{\phi(g)-1}\}$ of $\mathbb{Q}(\zeta_g)$ over $\mathbb{Q}$, and use the linear independence of $\{\zeta^0, \ldots, \zeta^{\phi(g)-1}\}$ over $\mathbb{Q}$ to obtain a relation among the e_i, and in turn use this relation to get a reduction of F. The minimal polynomial for ζ over $\mathbb{Q}$ is

$$\Phi_g(X) = \sum_{0 \le k \le p-1} X^{kp^{m-1}},$$

which has $\deg \Phi_g(X) = (p-1)p^{m-1} = \phi(g)$. Since $\Phi_g(X)$ is the minimal polynomial for ζ over $\mathbb{Q}$, we have $0 = \Phi_g(\zeta) = \sum_{0 \le k \le p-1} \zeta^{kp^{m-1}}$. Solving for $\zeta^{\phi(g)}$, we obtain

$$\zeta^{\phi(g)} = - \sum_{0 \le k \le p-2} \zeta^{kp^{m-1}}. \tag{3.2}$$

To express the remaining ζ^i, $\phi(g) + 1 \le i \le p^m - 1 = g$, in terms of the basis elements $\{\zeta^0, \ldots, \zeta^{\phi(g)-1}\}$ of $\mathbb{Q}(\zeta_g)$ over $\mathbb{Q}$, we need only multiply (3.2) by ζ^j, for $1 \le j \le g - \phi(g) - 1 = p^m - (p-1)p^{m-1} - 1$. Doing so, we obtain

$$\begin{aligned}
\zeta^{\phi(g)+1} &= - \sum_{0 \le k \le p-2} \zeta^{kp^{m-1}+1} \\
\zeta^{\phi(g)+2} &= - \sum_{0 \le k \le p-2} \zeta^{kp^{m-1}+2} \\
&\vdots \quad \vdots \\
\zeta^{g-1} &= - \sum_{0 \le k \le p-2} \zeta^{kp^{m-1}+p^m-(p-1)p^{m-1}-1}.
\end{aligned}$$

Substituting $\zeta^{\phi(g)+1}, \ldots, \zeta^{g-1}$ into $0 = \sum_{j=0}^{g-1} e_j \zeta^j$, we obtain

$$\begin{aligned}
0 &= e_0\zeta^0 + e_1\zeta^1 + \cdots + e_{\phi(g)-1}\zeta^{\phi(g)-1} + e_{\phi(g)}\zeta^{\phi(g)} + \cdots + e_{p^m-1}\zeta^{p^m-1} \\
&= e_0\zeta^0 + e_1\zeta^1 + \cdots + e_{\phi(g)-1}\zeta^{\phi(g)-1} \\
&\quad + e_{\phi(g)}\left(-\sum_{0\le k\le p-2}\zeta^{kp^{m-1}}\right) + \cdots + e_{p^m-1}\left(-\sum_{0\le k\le p-2}\zeta^{kp^{m-1}+p^{m-1}-1}\right) \\
&= e_0\zeta^0 + e_1\zeta^1 + \cdots + e_{\phi(g)-1}\zeta^{\phi(g)-1} + e_{\phi(g)}\left(-\zeta^0 - \zeta^{p^{m-1}} - \zeta^{2p^{m-1}} - \cdots - \zeta^{(p-2)p^{m-1}+1}\right) \\
&\quad + e_{\phi(g)+1}\left(-\zeta^1 - \zeta^{p^{m-1}+1} - \zeta^{2p^{m-1}+1} - \cdots - \zeta^{(p-2)p^{m-1}+1}\right) \\
&\quad + \cdots + e^{p^m-1}\left(-\zeta^{p^{m-1}-1} - \zeta^{2p^{m-1}-1} - \cdots - \zeta^{(p-1)p^{m-1}-1}\right) \\
&= (e_0 - e_{\phi(g)})\zeta^0 + (e_1 - e_{\phi(g)+1})\zeta^1 + \cdots + (e_{p^{m-1}-1} - e_{g-1})\zeta^{p^{m-1}-1} \\
&\quad + (e_{p^{m-1}} - e_{\phi(g)})\zeta^{p^{m-1}} + (e_{p^{m-1}+1} - e_{\phi(g)+1})\zeta^{p^{m-1}+1} + \cdots + (e_{2p^{m-1}-1} - e_{g-1})\zeta^{2p^{m-1}-1} \\
&\qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\
&\quad + (e_{(p-2)p^{m-1}} - e_{\phi(g)})\zeta^{(p-2)p^{m-1}} + (e_{(p-2)p^{m-1}+1} - e_{\phi(g)+1})\zeta^{(p-2)p^{m-1}+1} \\
&\quad + \cdots + (e_{(p-2)p^{m-1}+p^{m-1}-1} - e_{g-1})\zeta^{\phi(g)-1}.
\end{aligned}$$

Using the linear independence of $\{\zeta^0, \ldots \zeta^{\phi(g)-1}\}$ over $\mathbb{Q}$, we obtain

$$e_0 = e_{\phi(g)},\ e_{p^{m-1}} = e_{\phi(g)},\ \ldots, e_{(p-2)p^{m-1}} = e_{\phi(g)}$$

$$e_1 = e_{\phi(g)+1},\ e_{p^{m-1}+1} = e_{\phi(g)+1},\ \ldots, e_{(p-2)p^{m-1}+1} = e_{\phi(g)+1}$$

$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

$$e_{p^{m-1}-1} = e_{g-1},\ e_{2p^{m-1}-1} = e_{g-1},\ \ldots, e_{(p-2)p^{m-1}+p^{m-1}-1} = e_{g-1}.$$

Thus,

$$\begin{aligned} F &= \Big[(X-\zeta^0)(X-\zeta^{p^{m-1}})(X-\zeta^{2p^{m-1}})\cdots(X-\zeta^{(p-1)p^{m-1}})\Big]^{e_0} \\ &\quad \Big[(X-\zeta^1)(X-\zeta^{p^{m-1}+1})\cdots(X-\zeta^{(p-1)p^{m-1}+1})\Big]^{e_1} \\ &\qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ &\quad \Big[(X-\zeta^{p^{m-1}-1})(X-\zeta^{p^{m-1}-1+p^{m-1}})\cdots(X-\zeta^{(p-1)p^{m-1}+p^{m-1}-1})\Big]^{e_{p^{m-1}-1}} \end{aligned}$$

Consider the first term in F, namely $(X-\zeta^0)(X-\zeta^{p^{m-1}})(X-\zeta^{2p^{m-1}})\cdots(X-\zeta^{(p-1)p^{m-1}})$. The constants in the linear factors are the p^{m-1} roots of unity, starting at ζ^0. Thus,

$$(X-\zeta^0)(X-\zeta^{p^{m-1}})(X-\zeta^{2p^{m-1}})\cdots(X-\zeta^{(p-1)p^{m-1}}) = X^p-\zeta^0. \tag{3.3}$$

So, the X^j-coefficient of

$$(X-\zeta^0)(X-\zeta^{p^{m-1}})(X-\zeta^{2p^{m-1}})\cdots(X-\zeta^{(p-1)p^{m-1}}) = 0, \text{ for } 1\le j\le p-1.$$

As far as the other factors of F are concerned, say

$$(X-\zeta^i)(X-\zeta^{p^{m-1}+i})\cdots(X-\zeta^{(p-1)p^{m-1}+i}), \tag{3.4}$$

we get that the X^j-coefficient of (3.4) is

$$\begin{aligned} & X^j-\text{coefficient} \\ = \ & \zeta^{i(p-j)}\Big(X^j-\text{coefficient of } (X-\zeta^0)(X-\zeta^{p^{m-1}})(X-\zeta^{2p^{m-1}})\cdots(X-\zeta^{(p-1)p^{m-1}})\Big) \\ = \ & \zeta^{i(p-j)}0 \\ = \ & 0. \end{aligned}$$

For, to get the X^j-coefficient of (3.4), we take the product of the constant terms of all but j of the binomials and sum over all possible ways of doing this, namely $\binom{p}{j}$. Each term in the sum

has a common factor of $\zeta^{i(p-j)}$. Taking this factor out, we get the X^j-coefficient of (3.3), which is zero, for $1 \leq j \leq p-1$. Thus, we get that F reduces as follows:

$$F = \left(X^p - \zeta^0\right)^{e_0} \left(X^p - \zeta^p\right)^{e_1} \cdots \left(X^p - \zeta^{p(p^{m-1}-1)}\right)^{e_{p^{m-1}-1}}.$$

Since $g = p^m$, the X^p-coefficient of F must be 0. As before, we get that

$$0 = \sum_{j=0}^{e_{p^{m-1}-1}} e_j \zeta^{pj}.$$

But, ζ^p is a primitive p^{m-1} root of unity. So, the elements $\left\{\zeta^0, \zeta^p, \zeta^{2p}, \ldots, \zeta^{p(\phi(p^{m-1})-1)}\right\}$ form a basis for $\mathbb{Q}(\zeta^p)$ over $\mathbb{Q}$. Now, ζ^p is a zero of

$$\Phi_{p^{m-1}}(X) = \sum_{0 \leq k \leq p-2} X^{kp^{m-2}},$$

the minimal polynomial of the primitive p^{m-1} root of unity ζ^p. Again, we want to use the linear independence of $\left\{\zeta^0, \zeta^p, \ldots, \zeta^{p(\phi(p^{m-1})-1)}\right\}$ over $\mathbb{Q}$, to find a relation among the e_j and reduce F further. We use $\Phi_{p^{m-1}}(X)$ to find an expression of $\zeta^{p(\phi(p^{m-1}))}$ in terms of the basis elements $\left\{\zeta^0, \zeta^p, \ldots, \zeta^{p(\phi(p^{m-1})-1)}\right\}$ over $\mathbb{Q}$. We get

$$0 = \Phi_{p^{m-1}}\left(\zeta^p\right) = \sum_{0 \leq k \leq p-1} \left(\zeta^p\right)^{kp^{m-2}}.$$

Solving for $\zeta^{p\phi(p^{m-1})}$, we obtain

$$\zeta^{p\phi(p^{m-1})} = -\left(\sum_{0 \leq k \leq p-2} \zeta^{kp^{m-1}}\right). \tag{3.5}$$

To find the other $\zeta^{p(\phi(p^{m-1})+i)}$, $1 \leq i \leq p^{m-2}-1$, in terms of the basis elements $\left\{\zeta^0, \zeta^p, \ldots, \zeta^{p(\phi(p^{m-1})-1)}\right\}$ over $\mathbb{Q}$, we multiply (3.5) by ζ^{jp}, for $1 \leq j \leq p^{m-2}-1$. Doing so, we obtain

$$\begin{aligned}
\zeta^{p(\phi(p^{m-1})+1)} &= -\left(\sum_{0\le k\le p-2}\zeta^{kp^{m-1}+p}\right)\\
&\vdots \qquad \vdots\\
\zeta^{p(\phi(p^{m-1})+p^{m-2}-1)} &= -\left(\sum_{0\le k\le p-2}\zeta^{kp^{m-1}+p(p^{m-2}-1)}\right)
\end{aligned}$$

We now substitute the above equations into $\sum_{j=0}^{e_{p^{m-1}}-1} e_j\zeta^{pj}=0$, and use the linear independence of $\left\{\zeta^0,\zeta^p,\ldots,\zeta^{p(\phi(p^{m-1})-1)}\right\}$ over $\mathbb{Q}$ to get a relation among the e_i. We get

$$\begin{aligned}
0 &= \sum_{j=0}^{e_{p^{m-1}}-1} e_j\zeta^{pj}\\
&= e_0\zeta^0+e_1\zeta^p+e_2\zeta^{2p}+\cdots+e_{\phi(p^{m-1}-1)}\zeta^{p(\phi(p^{m-1})-1)}\\
&\quad +e_{\phi(p^{m-1})}\zeta^{p\phi(p^{m-1})}+e_{\phi(p^{m-1}+1)}\zeta^{p(\phi(p^{m-1}+1))}+\cdots+e_{\phi(p^{m-1})+p^{m-2}-1}\zeta^{p(\phi(p^{m-1})+p^{m-2}-1)}\\
&= e_0\zeta^0+e_1\zeta^p+e_{2p}\zeta^{2p}+\cdots+e_{\phi(p^{m-1})-1}\zeta^{p(\phi(p^{m-1})-1)}\\
&\quad +e_{\phi(p^{m-1})}\left(-\sum_{0\le k\le p-2}\zeta^{kp^{m-1}}\right)+e_{\phi(p^{m-1})+1}\left(-\sum_{0\le k\le p-2}\zeta^{kp^{m-1}+p}\right)\\
&\quad +\cdots+e_{\phi(p^{m-1})+p^{m-2}-1}\left(-\sum_{0\le k\le p-2}\zeta^{kp^{m-1}+p(p^{m-2}-1)}\right)\\
&= e_0\zeta^0+e_1\zeta^p+e_2\zeta^{2p}+\cdots+e_{\phi(p^{m-1}-1)}\zeta^{p(\phi(p^{m-1})-1)}\\
&\quad +e_{\phi(p^{m-1})}\left(-\zeta^0-\zeta^{p^{m-1}}-\zeta^{2p^{m-1}}-\cdots-\zeta^{(p-2)p^{m-1}}\right)\\
&\quad +e_{\phi(p^{m-1})+1}\left(-\zeta^p-\zeta^{2p^{m-1}+p}-\cdots-\zeta^{(p-2)p^{m-1}+p}\right)\\
&\quad +\cdots+e_{\phi(p^{m-1})+p^{m-2}-1}\left(-\zeta^{p(p^{m-2}-1)}-\zeta^{p^{m-1}+p(p^{m-2}-1)}-\cdots-\zeta^{(p-2)p^{m-1}+p(p^{m-2}-1)}\right)
\end{aligned}$$

$$
\begin{aligned}
= \quad & \left(e_0 - e_{\phi(p^{m-1})}\right)\zeta^0 + \left(e_1 - e_{\phi(p^{m-1})+1}\right)\zeta^p + \cdots + \left(e_{p^{m-2}-1} - e_{p^{m-1}-1}\right)\zeta^{p(p^{m-2}-1)} \\
& + \left(e_{p^{m-2}} - e_{\phi(p^{m-1})}\right)\zeta^{p^{m-1}} + \left(e_{p^{m-2}+1} - e_{\phi(p^{m-1})+1}\right)\zeta^{p(p^{m-2}+1)} + \cdots \\
& + \left(e_{2p^{m-2}-1} - e_{p^{m-1}-1}\right)\zeta^{2p(p^{m-2}-1)} \\
& \qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\
& + \left(e_{(p-2)p^{m-2}} - e_{\phi(p^{m-1})}\right)\zeta^{(p-2)p^{m-1}} + \left(e_{(p-2)p^{m-2}+1} - e_{\phi(p^{m-1})+1}\right)\zeta^{p((p-2)p^{m-2}+1)} + \cdots \\
& + \left(e_{(p-2)p^{m-2}+p^{m-2}-1} - e_{p^{m-1}-1}\right)\zeta^{p(\phi(p^{m-1})-1)}
\end{aligned}
$$

Using the linear independence of $\left\{\zeta^0, \zeta^p, \ldots, \zeta^{p(\phi(p^{m-1})-1)}\right\}$ over $\mathbb{Q}$, we get

$$
\begin{gathered}
e_0 = e_{\phi(p^{m-1})},\ e_{p^{m-2}} = e_{\phi(p^{m-1})}, \ldots, e_{(p-2)p^{m-2}} = e_{\phi(p^{m-1})} \\
e_1 = e_{\phi(p^{m-1})+1},\ e_{p^{m-2}+1} = e_{\phi(p^{m-1})+1}, \ldots, e_{(p-2)p^{m-2}+1} = e_{\phi(p^{m-1})+1} \\
\vdots \qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\
e_{p^{m-2}-1} = e_{p^{m-1}-1},\ e_{2p^{m-2}-1} = e_{p^{m-1}-1},\ \ldots, e_{(p-2)p^{m-2}+p^{m-2}-1} = e_{p^{m-1}-1}
\end{gathered}
$$

Thus, we get that

$$
\begin{aligned}
F \quad = \quad & \left[\left(X^p - \zeta^0\right)\left(X^p - \zeta^{p(p^{m-2})}\right)\cdots\left(X^p - \zeta^{p\phi(p^{m-1})}\right)\right]^{e_0} \\
& \left[\left(X^p - \zeta^p\right)\left(X^p - \zeta^{p(p^{m-2}+1)}\right)\cdots\left(X^p - \zeta^{p(\phi(p^{m-1})+1)}\right)\right]^{e_1} \\
& \qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\
& \left[\left(X^p - \zeta^{p(p^{m-2}-1)}\right)\left(X^p - \zeta^{p(2p^{m-2}-1)}\right)\cdots\left(X^p - \zeta^{p(p^{m-1}-1)}\right)\right]^{e_{p^{m-2}-1}}.
\end{aligned}
$$

Since the constants in the linear factors of the first term in F are the p^{m-2} roots of unity, we get

$$
\left(X^p - \zeta^0\right)\left(X^p - \zeta^{p(p^{m-2})}\right)\cdots\left(X^p - \zeta^{p\phi(p^{m-1})}\right) = X^{p^2} - \zeta^0.
$$

As before, F reduces to

$$F = \left(X^{p^2} - \zeta^0\right)^{e_0} \left(X^{p^2} - \zeta^{p^2}\right)^{e_1} \cdots \left(X^{p^2} - \zeta^{p^2(p^{m-2}-1)}\right)^{e_{p^{m-2}-1}}.$$

But, $g = p^m$ implies that $p^2 \notin S$. Thus, the X^{p^2}-coefficient must be zero. Continuing in this manner, we arrive at

$$F = \left(X^{p^{m-1}} - \zeta^0\right)^{e_0} \left(X^{p^{m-1}} - \zeta^{p^{m-1}}\right)^{e_1} \cdots \left(X^{p^{m-1}} - \zeta^{p^{m-1}(p-1)}\right)^{e_{p-1}}.$$

Now, $g = p^m$. Thus, $p^{m-1} \notin S$. So, the $X^{p^{m-1}}$-coefficient must be zero. That is,

$$0 = \sum_{j=0}^{p-1} e_j \zeta^{p^{m-1}j}.$$

But, $\zeta^{p^{m-1}}$ is a $p = p^{m-(m-1)}$th root of unity. So, $\{\zeta^{p^{m-1}}, \ldots, \zeta^{(p-1)p^{m-1}}\}$ forms a basis for $\mathbb{Q}(\zeta^{p^{m-1}})$ over $\mathbb{Q}$. Thus,

$$0 = \sum_{j=0}^{p-1} e_j \left(\zeta^{p^{m-1}j}\right) = \sum_{j=1}^{p-1} (e_j - e_0)\zeta^{p^{m-1}j}.$$

The latter equality holds since

$$\begin{aligned}
\sum_{j=1}^{p-1}(e_j - e_0)\zeta^{p^{m-1}j} &= (e_1 - e_0)\zeta^{p^{m-1}} + (e_2 - e_0)\zeta^{2p^{m-1}} + \cdots + (e_{p-1} - e_0)\zeta^{(p-1)p^{m-1}} \\
&= e_1\zeta^{p^{m-1}} + e_2\zeta^{2p^{m-1}} + \cdots + e_{p-1}\zeta^{(p-1)p^{m-1}} \\
&\quad -e_0\left(\zeta^{p^{m-1}} + \cdots + \zeta^{(p-1)p^{m-1}}\right) \\
&= e_1\zeta^{p^{m-1}} + e_2\zeta^{2p^{m-1}} + \cdots + e_{p-1}\zeta^{(p-1)p^{m-1}} - e_0(-1) \\
&= e_0\zeta^0 + e_1\zeta^{p^{m-1}} + e_2\zeta^{2p^{m-1}} + \cdots + e_{p-1}\zeta^{(p-1)p^{m-1}} \\
&= \sum_{j=0}^{p-1} e_j \left(\zeta^{p^{m-1}j}\right).
\end{aligned}$$

By the linear independence of $\left\{\zeta^{p^{m-1}}, \ldots, \zeta^{(p-1)p^{m-1}}\right\}$ over $\mathbb{Q}$, we get that $e_j = e_0$ for all $j = 1, \ldots, p-1$. Thus, $F = (X^{p^m} - 1)^{e_0}$. But, $g = p^m$ implies that the X^{p^m}-coefficient must be zero. The only way this can happen is if $e_0 = 0$. But, then we get $F = 1$, a contradiction to our assumption that F is not a unit. Since the assumption that $l_1 = 0$ in $F = X^{l_1} \prod_{j=0}^{g-1} \left(X - \zeta^j\right)^{e_j}$ led

to a contradiction, it must be that $l_1 > 0$. In this case, we get that the X^{l_1}-coefficient is not zero, since the constant term of $\prod_{j=0}^{g-1} \left(X - \zeta^j\right)^{e_j}$ is not zero. Thus, $l_1 \geq e$, since e is the multiplicity of S. From $l_1 + l_2 = e$, we get $l_1 = e$ and $l_2 = 0$. If $l_2 = 0$, then $G = \prod_{j=0}^{g-1} \left(X - \zeta^j\right)^{d_j}$. Applying the same techniques to G, we get that $G = 1$. This is a contradiction to the assumption that G is not a unit. Thus, $f_n(X)$ is irreducible in $R[S]$ for all n, whence $R[S]$ is not IDPF. ■

So, we have seen that given a proper numerical semigroup S with Frobenius number $g(S) = p^m$, where p is prime and m is a positive integer, and given any integral domain R of characteristic zero, the numerical semigroup ring $R[S]$ is not IDPF. We wish to know what happens if the Frobenius number of S is not a power of a prime; that is, if $g(S)$ has more than one distinct prime factor. To answer this, we must first recall the following definitions and results.

Definition 22 Let R be an integral domain. Then, R is called *atomic* if every nonzero, nonunit of R has a factorization into a finite product of irreducibles (atoms).

Definition 23 Let R be an integral domain. Then, R is said to be *irreducible divisors finite (IDF)* if every nonzero element has a finite number of irreducible divisors, up to associates.

Definition 24 An integral domain R is said to be a *finite factorization domain (FFD)* if each nonzero nonunit of R has only a finite number of non-associate divisors.

An equivalent condition that R be an FFD is that R is atomic and IDF [3, Theorem 5.1]. We also recall that R is an FFD if and only if $R[X]$ is an FFD [3, Proposition 5.3]. We are now ready to prove the main result of this section.

Theorem 25 *Let R be an atomic domain of characteristic zero and let S be a proper numerical semigroup. Then, $R[S]$ is not IDPF.*

Proof. We can assume R is IDPF, for if R is not IDPF, then $R[S]$ is not IDPF. This is because if R is not IDPF, there is a nonzero element a in R with $D^R(a)$ infinite. But each element in $D^R(a)$ is an element in $D^{R[S]}(a)$ and $U(R[S]) = U(R)$, where $U(R[S])$ and $U(R)$ denote the unit groups of $R[S]$ and R respectively. So, no two elements of $D^R(a)$ are associated in $R[S]$. Thus, $D^{R[S]}(a)$ is infinite, whence $R[S]$ is not IDPF. So, we assume that R is IDPF. If $g(S) = 1$, then $S = \langle 2, 3\rangle$ and this case has been proven [21, Proposition 4.1]. We induct on the number of district prime

factors in the Frobenius number $g(S)$. If $g(S) = p_1^{\alpha_1}$, then this is Lemma 21. Suppose the result holds for any numerical semigroup ring $R[S]$ where S has a Frobenius number with r distinct prime factors. Let S be a numerical semigroup with Frobenius number $g(S) = p_1^{\alpha_1} \cdots p_r^{\alpha_r} p_{r+1}^{\alpha_{r+1}}$. Construct the set $\widetilde{S} = \left\{x \in \mathbb{Z} : p_{r+1}^{\alpha_{r+1}} x \in S\right\}$. We claim that $\widetilde{S}$ is a numerical semigroup. For, $0 \in \widetilde{S}$ since $p_{r+1}^{\alpha_{r+1}} \cdot 0 = 0 \in S$. Suppose that $x_1,\ x_2 \in \widetilde{S}$. Then,

$$p_{r+1}^{\alpha_{r+1}}(x_1 + x_2) = p_{r+1}^{\alpha_{r+1}} x_1 + p_{r+1}^{\alpha_{r+1}} x_2,$$

and $p_{r+1}^{\alpha_{r+1}} x_1,\ p_{r+1}^{\alpha_{r+1}} x_2 \in S$. Since S is a numerical semigroup, it follows that $p_{r+1}^{\alpha_{r+1}}(x_1 + x_2) \in S$. Thus, $x_1 + x_2 \in \widetilde{S}$. So, $\widetilde{S}$ is a numerical semigroup.

Notice that $S \subseteq \widetilde{S}$ and hence $R[S] \subseteq R[\widetilde{S}]$. We claim that $g(\widetilde{S}) = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. For, $(p_1^{\alpha_1} \cdots p_r^{\alpha_r}) p_{r+1}^{\alpha_{r+1}} \notin S$ implies $p_1^{\alpha_1} \cdots p_r^{\alpha_r} \notin \widetilde{S}$. Also, $(p_1^{\alpha_1} \cdots p_r^{\alpha_r} + m) p_{r+1}^{\alpha_{r+1}} = p_1^{\alpha_1} \cdots p_r^{\alpha_r} p_{r+1}^{\alpha_{r+1}} + m p_{r+1}^{\alpha_{r+1}} \in S$ for every $m \geq 1$, since $g(S) = p_1^{\alpha_1} \cdots p_r^{\alpha_r} p_{r+1}^{\alpha_{r+1}}$. So, $p_1^{\alpha_1} \cdots p_r^{\alpha_r} + m \in \widetilde{S}$ for every $m \geq 1$. Thus, $g(\widetilde{S}) = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Now, $\left[R[S] : R[\widetilde{S}]\right] \neq \{0\}$, since $X^{g(S)+1} f(X) \in R[S]$ for any $f(X) \in R[\widetilde{S}]$. Since $R[S] \subseteq R[\widetilde{S}]$, $\left[R[S] : R[\widetilde{S}]\right] \neq \{0\}$, and by the induction hypothesis $R[\widetilde{S}]$ is not IDPF, it follows from [14, Theorem 2.3] that $R[S]$ is not atomic or that $R[S]$ is not IDPF. Since R is atomic and IDPF, R is an FFD and hence $R[X]$ is an FFD [3, Proposition 5.3]. So, $R[S] \subseteq R[X]$ is an FFD. For, if not, some $f \in R[S]$ has an infinite number of non-associate divisors in $R[S]$ and hence in $R[X]$, since $U(R[X]) = U(R[S])$. This contradicts the fact that $R[X]$ is an FFD. Thus, $R[S]$ is an FFD which implies that $R[S]$ is atomic [4, Theorem 1]. Since $R[S]$ is atomic, it must be that $R[S]$ is not IDPF. ■

So, we have seen that given an atomic domain R of characteristic zero and a proper numerical semigroup, it follows that $R[S]$ is never IDPF. In the next section, we explore the case when R has positive characteristic.

3.3 Numerical Semigroup Rings R[S] of Positive Characteristic

It turns out that when the characteristic of the atomic domain R is positive, say R has characteristic $q > 0$, it follows that $R[S]$ is IDPF if and only if $R[X]$ is IDPF, for any numerical semigroup S.

Theorem 26 *Let R be an atomic integral domain with characteristic $q > 0$, q a prime. Let S be a numerical semigroup. Then $R[S]$ is IDPF if and only if $R[X]$ is IDPF.*

Proof. Suppose that $R[S]$ is IDPF. Then, R is IDPF. For, if not, there is a nonzero $a \in R$ with $D^R(a)$ infinite. But, the irreducible divisors of a in R are also irreducible in $R[S]$. Since $U(R[S]) = U(R)$, where $U(R[S])$ and $U(R)$ denote the unit groups of $R[S]$ and R respectively, it follows that every $y \in D^R(a)$ belongs to $D^{R[S]}(a)$. Thus, $D^{R[S]}(a)$ is infinite, whence $R[S]$ is not IDPF, a contradiction. So, R is IDPF. But, R IDPF implies that R is IDF by definition. Since R is atomic by hypothesis, it follows that R is an FFD [3, Theorem 5.1]. Now, R is an FFD if and only if $R[X]$ is an FFD [3, Proposition 5.3]. We claim that $R[S]$ is an FFD. For, if not, there is an $f \in R[S]$ with an infinite number of non-associated divisors in $R[S]$. But, $U(R[X]) = U(R[S])$. So, f has an infinite number of non-associated divisors in $R[X]$. So, $R[X]$ is not an FFD, a contradiction. Thus, $R[S]$ is an FFD. So, by [3, Theorem 5.1], $R[S]$ is atomic. Note that $[R[S] : R[X]] \neq \{0\}$, since $X^{g(S)+1} f(X) \in R[X]$ for all $f(X) \in R[X]$. We want to show that $R[X]$ is IDPF. Suppose not. Then, by [14, Theorem 2.3], $R[S]$ is not atomic, or $R[S]$ is not IDPF. But, we have shown that $R[S]$ is atomic. Thus, $R[S]$ is not IDPF. So, if $R[S]$ is IDPF, then $R[X]$ is IDPF.

Conversely, suppose $R[X]$ is IDPF. Then, R is IDPF by the same reasoning as above. Again, R IDPF implies that R is IDF, by definition. By hypothesis, R is atomic. Thus, R is an FFD [3, Theorem 5.1]. But, R is an FFD if and only if $R[X]$ is an FFD [3, Proposition 5.3]. Since $R[X]$ is an FFD, $R[X]$ is atomic [3, Theorem 5.1]. Now, $U(R[X]) = U(R[S])$ and this implies that the factor group $U(R[X])/U(R[S]) = 1$. By [14, Theorem 2.1], to show that $R[S]$ is IDPF, it is enough to show that $R[S] \subseteq R[X]$ is a root extension. So, let $f(X) \in R[X]$. Write $f(X) = a_0 + a_1 X + \cdots + a_n X^n$. Choose a positive integer r so that $q^r > g(S)$. Then,

$$\begin{aligned}
(f(X))^{q^r} &= (a_0 + (a_1 X + \cdots + a_n X^n))^{q^r} \\
&= \sum_{j=0}^{q^r} \binom{q^r}{j} a_0^{q^r - j} (a_1 X + \cdots + a_n X^n)^j \\
&= a_0^{q^r} + (a_1 X + \cdots + a_n X^n)^{q^r} \\
&= a_0^{q^r} + X^{q^r} \left(a_1 + \cdots + a_n X^{n-1}\right),
\end{aligned}$$

since the characteristic of R is q and $\binom{q^r}{j}$ is divisible by q for $1 \leq j \leq q^r - 1$. Since $q^r > g(S)$, it follows that $(f(X))^{q^r} \in R[S]$. So, $R[S] \subseteq R[X]$ is a root extension. Thus, if $R[X]$ is IDPF, it follows that $R[S]$ is IDPF. ■

3.4 Conclusion

We have shown that for an atomic integral domain R of characteristic $q > 0$, $R[S]$ is IDPF if and only if $R[X]$ is IDPF, where S is any numerical semigroup. Further, we have shown that for an atomic domain R of characteristic zero, and a proper numerical semigroup S, $R[S]$ is never IDPF. At this point, two questions arise naturally. The first question comes from the observation that the condition that R is atomic in Lemma 21 was never used. We only needed this assumption for the inductive step.

Question 27 *Can the condition that R is atomic be removed from Theorem 25?*

In general, we do not know the answer to Question 27. Atomicity was not assumed in Lemma 21 . Further, one can apply the techniques in the proof of Lemma 21 to show that if $g(S) = 2p$, where p is an odd prime, then $R[S]$ is not IDPF, regardless of the atomicity of R. It seems if you can write down a formula for the irreducible polynomial of ζ_g, where g is the Frobenius number of S, then the techniques of Lemma 21 show that the condition that R is atomic can be dropped. The trouble of course is that in general, we don't know a formula for the irreducible polynomial of ζ_g. It seems reasonable, however, to conjecture that we can drop the condition that R is atomic in Theorem 25, but we are not sure. The second question removes the condition that S be a proper numerical semigroup.

Question 28 *What conditions on an atomic integral domain R are the necessary and sufficient for $R[X]$ to be IDPF?*

In 2009, Malcolmson and Okoh prove that if $n = 2^k$ for some positive integer k, then $\mathbb{Z}[ni][X]$ is IDPF [22, Theorem 1.10]. They also show that if n is a positive integer such that $\mathbb{Z}[ni]$ is IDPF and n is not a power of 2, then $\mathbb{Z}[ni][X]$ is not IDPF [22, Theorem 2.2]. Let $\omega = \dfrac{-1+\sqrt{d}}{2}$ if $d \equiv 1 \bmod 4$ and $\omega = \sqrt{d}$ if $d \equiv 2, 3 \bmod 4$, where d is a square free integer. In the next chapter (Chapter 4, Theorem 35), we generalize Malcolmson and Okoh's results by classifying the

orders R of the quadratic integer rings $\mathbb{Z}[\omega]$ such that $R[X]$ is IDPF. We also look at certain orders R in cyclotomic extensions $\mathbb{Q}(\zeta)$, where ζ is a primitive mth root of unity, and give a necessary condition for R to have the property that $R[X]$ is IDPF. We show this condition is sufficient if ζ is a p^mth root of unity, and fails to be sufficient otherwise.

Chapter 4

The Case When $R[S] = R[X]$

4.1 Introduction

In the last chapter, we showed that if R is an atomic domain of characteristic zero and S is a proper numerical semigroup, then the semigroup ring $R[S]$ is never IDPF. In this chapter, we look at the case when the numerical semigroup S is $\mathbb{N}$. We classify the orders R of the quadratic integer rings with the property that $R[X]$ is IDPF, via the discriminant $\delta_{\mathbb{Q}(\sqrt{d})}$ of $\mathbb{Q}(\sqrt{d})$. In particular, we prove that given a positive integer n, with prime factorization $n = p_1^{l_1} \cdots p_r^{l_r}$, $\mathbb{Z}[n\omega][X]$ is IDPF if and only if $\mathbb{Z}[n\omega]$ is IDPF and $p_i | \delta_{\mathbb{Q}(\sqrt{d})}$ for every $1 \leq i \leq r$. This generalizes Malcolmson and Okoh's classification of the orders R of the Gaussian integers such that $R[X]$ is IDPF [22]. We then pass to the ring of integers in cyclotomic field extensions $\mathbb{Q}(\zeta)$, where ζ is a primitive root of unity. Given the order $R = \mathbb{Z}[n\zeta] = \text{span}_{\mathbb{Z}}\{1, n\zeta, \ldots, n\zeta^{\phi(n)-1}\}$, where ζ is a primitive mth root of unity, we show that if $R[X]$ is IDPF, then $p_i | \delta_{\mathbb{Q}(\zeta)}$, for every i, where $n = p_1^{l_1} \cdots p_r^{l_r}$. In contrast to the case for orders in quadratic integer rings, we then look at the case where ζ is a 15th root of unity to show that the above condition is no longer sufficient. However, if ζ is a p^mth root of unity, where p is prime, then the condition is sufficient.

4.2 Background

Before we classify the orders R of the quadratic integer rings with the property that $R[X]$ is IDPF, we must state a few known results. Let $\widetilde{R}$ denote the integral closure of R. The equivalence of IDPF and inside factorial for an order R in an algebraic number ring is given by Chapman,

Halter-Koch, and Krause in [8] and states that R is inside factorial if and only if $R \subseteq \widetilde{R}$ is a root extension if and only if R is IDPF. They also give the following classification of the IDPF, and hence inside factorial, orders of the quadratic integer rings, via the discriminant $\delta_{\mathbb{Q}(\sqrt{d})}$ of $\mathbb{Q}(\sqrt{d})$, and the Legendre symbol $\left(\frac{d}{p}\right)$, where $d \neq 1$ is a square-free integer [8, Example 3]. Let

$$\omega = \begin{cases} \frac{-1+\sqrt{d}}{2} & \text{if } d \equiv 1 \mod 4 \\ \sqrt{d} & \text{if } d \equiv 2,\ 3 \mod 4 \end{cases},$$

and let n be a positive integer. Then, the order $\mathbb{Z}[n\omega]$ is IDPF if and only if $\mathbb{Z}[n\omega]$ is inside factorial if and only if $\left(\frac{\delta_{Q(\sqrt{d})}}{p}\right) \neq 1$, for every prime p dividing n. Let n be a positive integer with prime factorization $n = p_1^{l_1} \cdots p_r^{l_r}$. In this chapter, we prove that $\mathbb{Z}[n\omega][X]$ is IDPF if and only if $\mathbb{Z}[n\omega]$ is IDPF and $p_i | \delta_{\mathbb{Q}(\sqrt{d})}$ for every $1 \leq i \leq r$.

4.3 The Orders R of $\mathbb{Z}[\omega]$ such that the Polynomial Ring R[X] is IDPF

Being orders in the quadratic integer rings $\mathbb{Z}[\omega]$, the subrings of the form $\mathbb{Z}[n\omega]$ are Noetherian. This is because $\mathbb{Z}[n\omega]$ is a finitely generated $\mathbb{Z}$-module. Thus, $\mathbb{Z}[n\omega][X]$ is Noetherian. Furthermore, the integral closure of $\mathbb{Z}[n\omega][X]$ is $\mathbb{Z}[\omega][X]$ and $n \in [\mathbb{Z}[n\omega][X] : \mathbb{Z}[\omega][X]]$. So, by [14, Theorem 2.8], to show that the subring $\mathbb{Z}[n\omega][X]$ of $\mathbb{Z}[\omega][X]$ is IDPF, we need only show that $U(\mathbb{Z}[\omega][X])/U(\mathbb{Z}[n\omega][X])$ is finite and $\mathbb{Z}[n\omega][X] \subseteq \mathbb{Z}[\omega][X]$ is a root extension. We first show that $U(\mathbb{Z}[\omega][X])/U(\mathbb{Z}[n\omega][X])$ is finite. Now, $U(\mathbb{Z}[\omega][X])/U(\mathbb{Z}[n\omega][X]) = U(\mathbb{Z}[\omega])/U(\mathbb{Z}[n\omega])$. As already observed, $\mathbb{Z}[n\omega]$ is Noetherian. Also, $\widetilde{\mathbb{Z}[n\omega]} = \mathbb{Z}[\omega]$ and $n \in [\mathbb{Z}[n\omega] : \mathbb{Z}[\omega]]$. Since $\mathbb{Z}[n\omega][X]$ is not IDPF if $\mathbb{Z}[n\omega]$ is not IDPF, we may assume that $\mathbb{Z}[n\omega]$ is IDPF. Thus, $U(\mathbb{Z}[\omega])/U(\mathbb{Z}[n\omega])$ is finite [14, Theorem 2.8], and so it follows that $U(\mathbb{Z}[\omega][X])/U(\mathbb{Z}[n\omega][X])$ is finite. We must now find the positive integers n that admit root extensions from $\mathbb{Z}[\omega][X]$ into $\mathbb{Z}[n\omega][X]$.

Lemma 29 *If $n = p^k$ and $p | \delta_{\mathbb{Q}(\sqrt{d})}$, then $\mathbb{Z}[n\omega][X] \subseteq \mathbb{Z}[\omega][X]$ is a root extension.*

Proof. Let $h \in \mathbb{Z}[\omega][X]$. Then, $h = f + g\omega$, where $f,\ g \in \mathbb{Z}[X]$. We claim that $h^{p^k} \in \mathbb{Z}[p^k\omega][X]$. Throughout the proof, let W_{p^k} denote the ω-part of $(f + g\omega)^{p^k}$ and let $\widetilde{W_{p^k}}$ denote the greatest

common divisor of the coefficients of the polynomial of the ω-part of $(f+g\omega)^{p^k}$. We induct on k. Suppose that $k=1$. There are two cases to consider; namely, $d \equiv 1 \mod 4$ and $d \equiv 2,\ 3 \mod 4$. Suppose first that $d \equiv 1 \mod 4$. Then,

$$\begin{aligned}(f+g\omega)^p &= \sum_{j=0}^{p} \binom{p}{j} f^{p-j} g^j \omega^j \\ &= \sum_{j=0}^{p} \binom{p}{j} f^{p-j} g^j (a_j + b_j \omega) \\ &= \sum_{j=0}^{p} \binom{p}{j} f^{p-j} g^j a_j + \sum_{j=0}^{p} \binom{p}{j} f^{p-j} g^j b_j \omega\end{aligned}$$

So,

$$W_p = \sum_{j=0}^{p} \binom{p}{j} f^{p-j} g^j b_j.$$

Now, $\binom{p}{j}$ is divisible by p for $0 < j < p$. If $j = 0$, we get a strictly real part; that is, $j = 0$ implies $b_0 = 0$. If $j = p$, we get $g^p b_p$, where b_p denotes the ω-part of ω^p. So, we show that $p | b_p$. Since $d \equiv 1 \mod 4$, we have that

$$\omega = \left(\frac{-1+\sqrt{d}}{2} \right).$$

Thus,

$$\begin{aligned}\left(\frac{-1+\sqrt{d}}{2} \right)^p &= \sum_{\text{j even}} \binom{p}{j} (-1)^{p-j} \left(\frac{1}{2} \right)^p \sqrt{d}^j + \sum_{\text{j odd}} \binom{p}{j} (-1)^{p-j} \left(\frac{1}{2} \right)^p d^{\frac{j-1}{2}} \\ &\quad + \sum_{\text{j odd}} \binom{p}{j} (-1)^{p-j} \left(\frac{1}{2} \right)^{p-1} d^{\frac{j-1}{2}} \left(\frac{-1+\sqrt{d}}{2} \right).\end{aligned}$$

So,

$$2^{p-1} b_p = \sum_{\text{j odd}} \binom{p}{j} d^{\frac{j-1}{2}}.$$

Taking both sides $\mod p$, using Fermat's Little Theorem, the hypothesis that $p | \delta_{\mathbb{Q}(\sqrt{d})} = d$, and $\binom{p}{1} = p$, we get $b_p \equiv_p 0$. So, if $d \equiv 1 \mod 4$, the result holds.

Now, consider the case when $d \equiv 2,\ 3 \mod 4$. In this case, we have

$$\left(f + g\sqrt{d}\right)^p = \sum_{\text{j even}} \binom{p}{j} f^{p-j} g^j \sqrt{d}^j + \sum_{\text{j odd}} \binom{p}{j} f^{p-j} g^j d^{\frac{j-1}{2}} \sqrt{d}.$$

So,

$$W_p = \sum_{\text{j odd}} \binom{p}{j} f^{p-j} g^j d^{\frac{j-1}{2}}.$$

Now, $\binom{p}{j}$ is divisible by p for $0 < j < p$. If $j = p$, we have $g^p d^{\frac{p-1}{2}}$. But, $p|\delta_{\mathbb{Q}(\sqrt{d})} = 4d$. If $p \neq 2$, then $p|d$ and thus $\widetilde{W_p} \equiv 0 \mod p$. If $p = 2$, $j = p$ is not an option and $\widetilde{W_p} \equiv 0 \mod p$. Thus, ω-part of $\left(f + g\sqrt{d}\right)^p$ is divisible by p. In either case, we see that the ω-part of $(f + g\omega)^p$ is divisible by p. So, the result holds for $k = 1$. Suppose the result holds for k. We prove that the result holds for $k + 1$. Now,

$$(f + g\omega)^{p^{k+1}} = \left((f + g\omega)^{p^k}\right)^p.$$

By the induction hypothesis, the ω-part of $(f + g\omega)^{p^k}$ is divisible by p^k. Thus, there are $\widetilde{f},\ \widetilde{g} \in \mathbb{Z}[X]$ such that

$$(f + g\omega)^{p^k} = \widetilde{f} + p^k \widetilde{g}\omega.$$

So, we have

$$\begin{aligned}
(f + g\omega)^{p^{k+1}} &= \left((f + g\omega)^{p^k}\right)^p \\
&= \left(\widetilde{f} + p^k \widetilde{g}\omega\right)^p \\
&= \sum_{j=0}^{p} \binom{p}{j} \widetilde{f}^{p-j} \left(p^{kj}\right) \widetilde{g}^j \omega^j \\
&= \sum_{j=0}^{p} \binom{p}{j} \widetilde{f}^{p-j} \left(p^{kj}\right) \widetilde{g}^j (a_j + b_j\omega) \\
&= \sum_{j=0}^{p} \binom{p}{j} \widetilde{f}^{p-j} \left(p^{kj}\right) \widetilde{g}^j a_j + \sum_{j=0}^{p} \binom{p}{j} \widetilde{f}^{p-j} \left(p^{kj}\right) \widetilde{g}^j b_j\omega
\end{aligned}$$

Now, $\binom{p}{j}$ is divisible by p for $0 < j < p$. So, $\binom{p}{j} p^{kj}$ is divisible by p^{k+1} for $0 < j < p$. If $j = 0$, we get a strictly real part; that is, if $j = 0$, then $b_0 = 0$. If $j = p$, then p^{kp} is divisible by p^{k+1}. Thus, the ω-part of $(f + g\omega)^{p^{k+1}}$ is divisible by p^{k+1}. Therefore, if $n = p^k$ and $p|\delta_{\mathbb{Q}(\sqrt{d})}$, it follows

that $\mathbb{Z}[n\omega][X] \subseteq \mathbb{Z}[\omega][X]$ is a root extension. ■

Proposition 30 *Let n be a positive integer for which $\mathbb{Z}[n\omega]$ is IDPF. If $n = p_1^{l_1} \cdots p_r^{l_r}$, where $p_i | \delta_{\mathbb{Q}(\sqrt{d})}$, for all $1 \leq i \leq r$, then $\mathbb{Z}[n\omega][X]$ is IDPF.*

Proof. As discussed in the introduction, we need only show that if $n = p_1^{l_1} \cdots p_r^{l_r}$, where $p_i | \delta_{\mathbb{Q}(\sqrt{d})}$, for all $1 \leq i \leq r$, then it follows that $\mathbb{Z}[n\omega][X] \subseteq \mathbb{Z}[\omega][X]$ is a root extension. By lemma 29, $\mathbb{Z}[\omega][X]$ is a root extension of $\mathbb{Z}[p_i^{l_i}\omega][X]$. That is, given any $h \in \mathbb{Z}[\omega][X]$, the ω-part of h^{p^k} is divisible by p^k. Thus, $h^{p^k} \in \mathbb{Z}[p^k\omega][X]$. Since the $p_i^{l_i}$ are relatively prime for all i, it follows that given any $h \in \mathbb{Z}[\omega][X]$, $h^{p_1^{l_1} \cdots p_r^{l_r}} \in \mathbb{Z}[n\omega][X]$. For, $p_i^{l_i}$ divides the ω-part of $h^{p_1^{l_1} \cdots p_r^{l_r}} = \left(h^{p_i^{l_i}}\right)^{p_1^{l_1} \cdots p_{i-1}^{l_{i-1}} p_{i+1}^{l_{i+1}} \cdots p_r^{l_r}}$. Since the $p_i^{l_i}$ are relatively prime, $p_1^{l_1} \cdots p_r^{l_r}$ divides the ω-part of $h^{p_1^{l_1} \cdots p_r^{l_r}}$, whence $\mathbb{Z}[n\omega][X] \subseteq \mathbb{Z}[\omega][X]$ is a root extension. ■

We have seen if $n = p_1^{l_1} \cdots p_r^{l_r}$, where $p_i | \delta_{\mathbb{Q}(\sqrt{d})}$ for all $1 \leq i \leq r$, then $\mathbb{Z}[n\omega][X]$ is IDPF. One might wonder if there are any other n such that $\mathbb{Z}[n\omega][X]$ is IDPF. The answer is no as we will see in the next section.

4.4 Are there any other n for which $\mathbb{Z}[n\omega]$ IDPF implies $\mathbb{Z}[n\omega][X]$ is IDPF?

Let $n > 1$ be a positive integer with prime factorization $n = p_1^{l_1} \cdots p_r^{l_r}$. To prove that $\mathbb{Z}[n\omega][X]$ is IDPF precisely when $p_i | \delta_{\mathbb{Q}(\sqrt{d})}$ for all $1 \leq i \leq r$ and $\mathbb{Z}[n\omega]$ is IDPF, we must prove that if $\mathbb{Z}[n\omega][X]$ is IDPF, then $p_i | \delta_{\mathbb{Q}(\sqrt{d})}$ for all $1 \leq i \leq r$ and $\mathbb{Z}[n\omega]$ is IDPF. We will prove the contrapositive. That is, suppose n is such that $\mathbb{Z}[n\omega]$ is not IDPF, or some p_i does not divide the discriminant, $\delta_{\mathbb{Q}(\sqrt{d})}$, of $\mathbb{Q}(\sqrt{d})$. Then $\mathbb{Z}[n\omega][X]$ is not IDPF. To do this, we must establish some lemmas. The first lemma shows that the element $f_n(X) = (\omega + X)^n$ has unique factorization into irreducibles in $\mathbb{Z}[\omega][X]$, even though the domain $\mathbb{Z}[\omega][X]$ is not necessarily a UFD.

Lemma 31 *If $p_1, p_2, \ldots, p_n$ are prime elements, not necessarily distinct, in an integral domain A, then $d = p_1 p_2 \cdots p_n$ has unique factorization into irreducibles in A up to order of factors and units.*

Proof. We induct on n. If $n = 1$, then $d = p_1$, and since a prime element is irreducible, there is nothing to prove. Suppose the result is true for $n = k$. We will show the result is true for $n = k+1$.

Suppose that

$$p_1 p_2 \cdots p_k p_{k+1} = d = a_1 \cdots a_r.$$

Now, p_{k+1} prime implies p_{k+1} divides a_i, for some i. Without loss of generality, say p_{k+1} divides a_1. Then, since a_1 is irreducible, $a_1 = p_{k+1} u_1$, where u_1 is a unit in A. Thus,

$$p_1 p_2 \cdots p_k p_{k+1} = u p_{k+1} a_2 \cdots a_r.$$

So,

$$p_1 p_2 \cdots p_k = u a_2 \cdots a_r.$$

By the induction hypothesis, $a_i = u_{i-1} p_{\sigma(i-1)}$, where σ is a permutation of $\{1, 2, \ldots, k\}$ and $2 \leq i \leq k+1$. ■

Lemma 32 *Suppose that* $\left(\frac{d}{p}\right) = -1$ *for some odd prime* p *and* $d \equiv 1 \mod 4$. *Then, the* $\omega -$ *part of* ω^{p^r} *is not divisible by* p *for any positive integer* r.

Proof. Throughout the proof, let the integer N_{p^r} denote the $\omega -$ part of ω^{p^r}. We induct on r. Suppose first that $r = 1$. Then, we have

$$\begin{aligned}
\left(\frac{-1+\sqrt{d}}{2}\right)^p &= \sum_{j=0}^{p} \binom{p}{j} \left(\frac{-1}{2}\right)^{p-j} \left(\frac{\sqrt{d}}{2}\right)^j \\
&= \sum_{\text{j even}} \binom{p}{j} (-1)^{p-j} \left(\frac{1}{2}\right)^p \sqrt{d}^j + \sum_{\text{j odd}} \binom{p}{j} (-1)^{p-j} \left(\frac{1}{2}\right)^p d^{\frac{j-1}{2}} \\
&+ \sum_{\text{j odd}} \binom{p}{j} (-1)^{p-j} \left(\frac{1}{2}\right)^{p-1} d^{\frac{j-1}{2}} \left(\frac{-1+\sqrt{d}}{2}\right)
\end{aligned}$$

So,

$$N_p = \sum_{\text{j odd}} \binom{p}{j} \left(\frac{1}{2}\right)^{p-1} d^{\frac{j-1}{2}}$$

Thus, we get

$$2^{p-1} N_p = \sum_{\text{j odd}} \binom{p}{j} d^{\frac{j-1}{2}}$$

By Euler's criterion, Fermat's Little Theorem and the fact that $\binom{p}{j} \equiv_p 0$ for $0 < j < p$, taking both sides of the above equation mod p, we obtain

$$N_p \equiv_p -1.$$

Thus, the ω-part of ω^p is not divisible by p. Suppose the result holds for r. We will show that the result holds for $r+1$. Now,

$$\begin{aligned}
\left(\frac{-1+\sqrt{d}}{2}\right)^{p^{r+1}} &= \left(\left(\frac{-1+\sqrt{d}}{2}\right)^{p^r}\right)^p \\
&= \left[\left(\sum_{\text{j even}} \binom{p^r}{j}(-1)^{p^r-j}\left(\frac{1}{2}\right)^{p^r}\sqrt{d}^{\,j} + \sum_{\text{j odd}} \binom{p^r}{j}\left(\frac{1}{2}\right)^{p^r} d^{\frac{j-1}{2}}\right)\right. \\
&\quad \left. + \sum_{\text{j odd}} \binom{p^r}{j} d^{\frac{j-1}{2}}\left(\frac{-1+\sqrt{d}}{2}\right)\right]^p
\end{aligned}$$

By the induction hypothesis, we have that

$$N_{p^r} = \sum_{\text{j odd}} \binom{p^r}{j} d^{\frac{j-1}{2}}$$

is not divisible by p. Using the binomial expansion to expand the above equation, we get

$$\begin{aligned}
\left(\frac{-1+\sqrt{d}}{2}\right)^{p^{r+1}} &= \sum_{k=0}^{p}\binom{p}{k}\left(\sum_{\text{j even}} \binom{p^r}{j}(-1)^{p^r-j}\left(\frac{1}{2}\right)^{p^r}\sqrt{d}^{\,j} + \sum_{\text{j odd}} \binom{p^r}{j}\left(\frac{1}{2}\right)^{p^r} d^{\frac{j-1}{2}}\right)^{p-k} \\
&\quad \cdot \left(\sum_{\text{j odd}} \binom{p^r}{j} d^{\frac{j-1}{2}}\right)^k \left(\frac{-1+\sqrt{d}}{2}\right)^k
\end{aligned}$$

Now, $\binom{p}{k} \equiv_p 0$ for $0 < k < p$. If $k = 0$, we have a strictly real part. So, we need only consider the case when $k = p$. If $k = p$, we get

$$\left(\sum_{\text{j odd}} \binom{p^r}{j} d^{\frac{j-1}{2}}\right)^p \left(\tfrac{-1+\sqrt{d}}{2}\right)^p.$$

But, $N_p \equiv_p -1$, and by the induction hypothesis, $\sum_{\text{j odd}} \binom{p^r}{j} d^{\frac{j-1}{2}}$ is not divisible by p. So, $N_{p^{r+1}}$ is not divisible by p. ■

We state a lemma due to Malcolmson and Okoh ([22, Lemma 2.1]). In [22], Malcolmson and Okoh show that given an odd positive integer k and p an odd prime that divides k, with $k = p^r m$, $\gcd(m, p) = 1$, then p^r does not divide $\binom{k}{p^r}$. This lemma holds in more generality. We omit the proof as it is similar to the proof in [22].

Lemma 33 *Let k be a positive integer. For any prime p that divides k, let $k = p^r m$, where p does not divide m. Then p does not divide $\binom{k}{p^r}$.*

We are now ready to prove the main proposition of this section. This result enables us to prove precisely when the subring $\mathbb{Z}[n\omega][X]$ of $\mathbb{Z}[\omega][X]$ is IDPF.

Proposition 34 *Let n be a positive integer for which $\mathbb{Z}[n\omega]$ is IDPF. If $n = p_1^{l_1} \cdots p_r^{l_r}$ is the factorization of n into primes and some p_i does not divide $\delta_{\mathbb{Q}(\sqrt{d})}$, then $\mathbb{Z}[n\omega][X]$ is not IDPF.*

Proof.

Throughout the proof, let N_{p^r} denote the ω-part of ω^{p^r}. There are two cases to consider. Suppose first that $d \equiv 1 \mod 4$, so that $\omega = \frac{-1+\sqrt{d}}{2}$. Note that in this case, each p_i must be odd since $\left(\frac{d}{p_i}\right) \neq 1$. For, if p_i is even, then $p_i = 2$ and $x^2 \equiv d \mod 2$ has a solution since $d \equiv 1 \mod 4$ implies that $d = 4k + 1 = 2(2k) + 1$, for some positive integer k. Thus, $d \equiv 1 \mod 2$ and $x^2 \equiv 1 \mod 2$ has a solution. Without loss of generality, suppose p_1 does not divide $\delta_{\mathbb{Q}(\sqrt{d})} = d$. We claim that for any odd positive integer k, the polynomial

$$f_k = n\,(\omega + X)^k$$

is irreducible in $\mathbb{Z}[n\omega][X]$, or has an irreducible factor of the form

$$n_1\,(\omega + X)^k$$

where $n_1 | n$. Since f_k factors uniquely in $\mathbb{Z}[\omega][X]$, by Lemma 31, any factorization of f_k in $\mathbb{Z}[\omega][X]$ is of the form

$$n_1 (\omega + X)^{k_1} n_2 (\omega + X)^{k_2}$$

where one of the k_i is odd, and the other is even. Without loss of generality, suppose k_1 is odd and $1 < n_1 < n$. Then,

$$n_1 (\omega + X)^{k_1} = n_1 \sum_{j=0}^{k_1} \binom{k_1}{j} X^{k_1 - j} \omega^j.$$

Consider the $j = 1$ term which is

$$n_1 \binom{k_1}{1} X^{k_1 - 1} \omega.$$

Now, n must divide $n_1 \binom{k_1}{1} = n_1 k_1$. If p_1 does not divide k_1, then $p_1^{l_1}$ divides n_1. If p_1 divides k_1, write $k_1 = p_1^r m$, with $\gcd(p_1, m) = 1$. In the binomial expansion of $n_1 (\omega + X)^{k_1}$, consider the $j = p_1^r$ term, which is

$$n_1 \binom{k_1}{p_1^r} \omega^{p_1^r} X^{k_1 - p_1^r}.$$

By Lemma 32 and Lemma 33, p_1 does not divide $\binom{k_1}{p_1^r}$ and p_1 does not divide $N_{p_1^r}$. Thus, $p_1^{l_1}$ does not divide $\binom{k_1}{p_1^r}$ and $p_1^{l_1}$ does not divide $N_{p_1^r}$. Since n must divide the integer coefficient of

$$n_1 \binom{k_1}{p_1^r} \omega^{p_1^r} X^{k_1 - p_1^r},$$

which is $n_1 \binom{k_1}{p_1^r} N_{p_1^r}$, it follows that $p_1^{l_1}$ divides n_1. So, in either case, $p_1^{l_1}$ divides n_1. Thus, $n_1 = p_1^{l_1} s_1$, for some positive integer s_1, with $\gcd(p_1, s_1) = 1$. We look at $n_2 (\omega + X)^{k_2}$. Now, n must divide the integer coefficient of the first term in the binomial expansion of

$$n_2 (\omega + X)^{k_2},$$

which is

$$n_2 \binom{k_2}{1} = n_2 k_2.$$

Now, if p_1^t divides n_2 for any positive integer t, we get that $n = p_1^{l_1} p_1^t s_1 s_2$, for some positive integer s_2. But this contradicts the unique factorization of n into primes. So, $p_1^{l_1}$ divides k_2. Now, write $k_2 = p_1^r m$, with $\gcd(p_1, m) = 1$ and consider the integer coefficient of the $j = p_1^r$ term in the binomial expansion of

$$n_2 (\omega + X)^{k_2},$$

which is

$$n_2 \binom{k_2}{p_1^r} N_{p_1^r}.$$

Now, p_1 does not divide n_2, $\binom{k_2}{p_1^r}$, or $N_{p_1^r}$. So, n does not divide the integer coefficient of some monomial of the ω-part in the binomial expansion. So, we must have $k_1 = k$. Applying the above argument with $k = k_1$, we get $n_1|n$. Thus, if k is any odd positive integer, the polynomial

$$f_k = n\,(\omega + X)^k$$

is irreducible or has an irreducible factor of the form

$$n_1\,(\omega + X)^k\,,$$

where $n_1|n$. One of these irreducible factors divides $(n\,(\omega + X))^k$ whence $D\,(n\,(w + X))$ is infinite.

The case of $d \equiv 2,\ 3 \mod 4$ uses techniques similar to the proof given in [14, Theorem 2.2] for $\mathbb{Z}[i]$. We sketch the proof here, using a different element of $\mathbb{Z}[\sqrt{d}][X]$, so that we will have unique factorization of that element in $\mathbb{Z}[\sqrt{d}][X]$. We show that for any odd positive integer k, the polynomial

$$f_k = n(\sqrt{d} + X)^k$$

is irreducible in $\mathbb{Z}[n\sqrt{d}]$ or has an irreducible factor of the form

$$n_1(\sqrt{d} + X)^k,$$

where $n_1|n$. Since $(\sqrt{d} + X)^k$ has unique factorization in $\mathbb{Z}[\sqrt{d}][X]$, by Lemma 31, any factorization of f_k in $\mathbb{Z}[\sqrt{d}][X]$ is of the form

$$n_1(\sqrt{d} + X)^{k_1} n_2(\sqrt{d} + X)^{k_2},$$

where one of k_1 is odd and the other is even. Without loss of generality, take k_1 odd and $1 < n_1 < n$. Consider the binomial expansion

$$n_1(\sqrt{d} + X)^{k_1} = n_1 \sum_{j=0}^{k_1} \binom{k_1}{j} (\sqrt{d})^j X^{k_1 - j}$$

Now, k_1 odd implies that we can consider the $j = k_1$ term, which has a non-zero $\sqrt{d}$-part, and it is

$$n_1 d^{\frac{k_1-1}{2}}.$$

Now, n divides $n_1 d^{\frac{k_1-1}{2}}$. But, some odd prime, say p_1, does not divide d (odd because 2 divides $\delta_{\mathbb{Q}(\sqrt{d})} = 4d$). So, $p_1^{l_1}$ must divide n_1. Thus, $n_1 = p_1^{l_1} s_1$, for some positive integer s_1 with $\gcd(p_1, s_1) = 1$. We look at k_2. Now, n divides $n_2\binom{k_2}{1} = n_2 k_2$, the integer coefficient of the $\sqrt{d}$-part of the first term in the binomial expansion of $n_2(\sqrt{d} + X)^{k_2}$. If p_1^t divides n_2 for any positive integer t, then we get $n = p_1^{l_1} p_1^t s_1 s_2$ for some positive integer s_2, a contradiction to the uniqueness of the prime factorization of n. Thus, $p_1^{l_1}$ divides k_2. Write $k_2 = p_1^r m$, where $\gcd(p, m) = 1$. Consider the integer coefficient of the $j = p_1^r$ term in the binomial expansion of $(\sqrt{d} + X)^{k_2}$. This term is

$$n_2\binom{k_2}{p_1^r} d^{\frac{p_1^r-1}{2}}.$$

Now, p_1 does not divide n_2, $\binom{k_2}{p_1^r}$, and d. So, n does not divide the integer coefficient of some monomial of the $\sqrt{d}$-part in the binomial expansion. So, we must have $k = k_1$. If $k_1 = k$, the above argument gives $n_1 | n$. Thus, if k is any odd positive integer, the polynomial $f_k = n(\sqrt{d} + X)^k$ is irreducible in $\mathbb{Z}[n\sqrt{d}][X]$ or has an irreducible factor of the form $n_1(\sqrt{d} + X)^k$, where n_1 divides n. Thus, $D(n(\sqrt{d} + X))$ is infinite. ■

We are now ready to state and prove the main result of this chapter.

Theorem 35 *Let n be a positive integer with prime factorization $n = p_1^{l_1} \cdots p_r^{l_r}$. Then, the following are equivalent:*

1. *$\mathbb{Z}[n\omega][X]$ is IDPF*

2. *$p_i | \delta_{\mathbb{Q}(\sqrt{d})}$ for every $1 \leq i \leq r$ and $\mathbb{Z}[n\omega]$ is IDPF.*

Proof. We first prove that if $\mathbb{Z}[n\omega][X]$ is IDPF, then $p_i | \delta_{\mathbb{Q}(\sqrt{d})}$ for every $1 \leq i \leq r$ and $\mathbb{Z}[n\omega]$ is IDPF. By contraposition, suppose that some p_i does not divide $\delta_{\mathbb{Q}(\sqrt{d})}$ or $\mathbb{Z}[n\omega]$ is not IDPF. If $\mathbb{Z}[n\omega]$ is not IDPF, then it is clear that $\mathbb{Z}[n\omega][X]$ is not IDPF. So, suppose $\mathbb{Z}[n\omega]$ is IDPF and some p_i does not divide $\delta_{\mathbb{Q}(\sqrt{d})}$. Then, by Proposition 34, $\mathbb{Z}[n\omega][X]$ is not IDPF.
Conversely, suppose that $p_i | \delta_{\mathbb{Q}(\sqrt{d})}$ for every $1 \leq i \leq r$ and $\mathbb{Z}[n\omega]$ is IDPF. Then, by Proposition 30, $\mathbb{Z}[n\omega][X]$ is IDPF. ■

4.5 Orders of the Ring of Integers in Cyclotomic Field Extensions

Let $[F : \mathbb{Q}]$ be finite and let A be the ring of integers in F. Suppose that R is an order with a positive integer in $[R : A]$. Let n be the least positive integer in $[R : A]$ and let $n = p_1^{l_1} \cdots p_r^{l_r}$ be the prime factorization of n. One might wonder if $R[X]$ is IDPF if and only if each p_i divides the discriminant δ_F of F, as was the case for the quadratic integer rings. To answer this question, let's examine the cyclotomic field extensions.

Lemma 36 *Let ζ be a primitive pth root of unity and let $\{1, \zeta, \ldots, \zeta^{p-2}\}$ be a basis for $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$. (Then, it is known that $\{1, \zeta, \ldots, \zeta^{p-2}\}$ is an integral basis for the ring of integers A in $\mathbb{Q}(\zeta)$; that is, $A = \mathbb{Z}[\zeta]$.) Let $R = \mathbb{Z}[n\zeta] = span_{\mathbb{Z}}\{1, n\zeta, \ldots, n\zeta^{p-2}\}$, and let $n = p_1^{l_1} \ldots p_r^{l_r}$ be the prime factorization of n. If $R[X]$ is IDPF, then $p_i | \delta_{\mathbb{Q}(\zeta)}$ for every $1 \leq i \leq r$.*

Proof. Suppose some p_i does not divide $\delta_{\mathbb{Q}(\zeta)} = (-1)^{\phi(p)/2} p^{p-2}$ [23, Proposition 2.7]. Without loss of generality, suppose p_1 does not divide $\delta_{\mathbb{Q}(\zeta)} = (-1)^{\phi(p)/2} p^{p-2}$. Then, $p_1 \neq p$. Let

$$f_k(X) = n\,(\zeta + X)^k\,.$$

Then, we claim that $f_k(X)$ is irreducible in $R[X]$ for all k with $\gcd(k, n) = 1$. Now, as before, $(\zeta + X)^k$ has unique factorization in $A[X]$ (Lemma 31). Factoring $f_k(X)$ in $A[X]$, we obtain

$$f_k(X) = n_1\,(\zeta + X)^{k_1}\,n_2\,(\zeta + X)^{k_2}\,.$$

Now, consider the $j = 1$ term in the binomial expansion

$$n_1\,(\zeta + X)^{k_1} = n_1 \sum_{j=0}^{k_1} \binom{k_1}{j} \zeta^j X^{k_1 - j}.$$

The $j = 1$ term is $n_1 k_1 \zeta X^{k_1 - 1}$. The integer coefficient is $n_1 k_1$. So, $n | n_1 k_1$. If p_1 does not divide k_1, then $p_1^{l_1}$ divides n_1. If p_1 divides k_1, write $k_1 = p_1^r m$, with $\gcd(p_1, m) = 1$. So, consider the $j = p_1^r$ term in the above binomial expansion, which is $n_1 \binom{k_1}{p_1^r} \zeta^{p_1^r} X^{k_1 - p_1^r}$. Since $p_1 \neq p$, it must be that $\zeta^{p_1^r} \neq 1$. For, if $\zeta^{p_1^r} = 1$, then $p_1^r = ap$, where a is a positive integer. But, then p divides p_1^r and hence p divides p_1. So, $p = p_1$, a contradiction to $p \neq p_1$. Now, if p_1^r is not congruent to $p - 1$ modulo p, then $\zeta^{p_1^r}$ contributes no integer coefficient in $n_1 \binom{k_1}{p_1^r} \zeta^{p_1^r} X^{k_1 - p_1^r}$. If p_1^r is congruent

to $p-1$ modulo p, then we can express $\zeta^{p_1^r}$ in terms of the basis elements as

$$\zeta^{p_1^r} = -1 - \zeta - \cdots - \zeta^{p-2}.$$

So,

$$n_1 \binom{k_1}{p_1^r} \zeta^{p_1^r} X^{k_1 - p_1^r} = n_1 \binom{k_1}{p_1^r} (-1 - \zeta - \cdots - \zeta^{p-2}) X^{k_1 - p_1^r},$$

and the integer coefficient of this monomial is $n_1 \binom{k_1}{p_1^r}$.

So, in either case, the integer coefficient of $n_1 \binom{k_1}{p_1^r} \zeta^{p_1^r} X^{k_1 - p_1^r}$ is $n_1 \binom{k_1}{p_1^r}$. So, n must divide $n_1 \binom{k_1}{p_1^r}$. But, p_1 does not divide $\binom{k_1}{p_1^r}$, by Lemma 33. Thus, $p_1^{l_1}$ divides n_1. So, in either case, $p_1^{l_1}$ divides n_1. Thus, $n_1 = p_1^{l_1} s_1$, with $\gcd(s_1, p_1) = 1$. Consider $n_2 (\zeta + X)^{k_2}$. Now, n must divide the $j = 1$ coefficient in the binomial expansion

$$n_2 (\zeta + X)^{k_2} = n_2 \sum_{j=0}^{k_2} \binom{k_2}{j} \zeta^j X^{k_2 - j}.$$

The $j = 1$ coefficient is $n_2 k_2$. If p_1^t divides n_2 for any integer $t \geq 1$, then $n_2 = p_1^t s_2$ and hence $n = n_1 n_2 = p_1^{l_1} s_1 p_1^t s_2$, a contradiction to the unique factorization of n into primes. So, $p_1^{l_1}$ divides k_2. Thus, $k_2 = p_1^r m'$, where $r \geq l_1$ and $\gcd(p_1, m') = 1$. Now, n must divide the $j = p_1^r$ coefficient in the above binomial expansion of $n_2 (\zeta + X)^{k_2}$. This coefficient is $n_2 \binom{k_2}{p_1^r}$. But, p_1 does not divide n_2 and p_1 does not divide $\binom{k_2}{p_1^r}$ by Lemma 33. This is a contradiction. Thus, $k = k_1$. So, $f_k(X) = n_1 n_2 (\zeta + X)^k$. Now, n must divide the $j = 1$ term in the binomial expansion

$$\widetilde{f_k}(X) = n_2 (\zeta + X)^k .$$

The $j = 1$ coefficient is $n_2 k$. But, $\gcd(n, k) = 1$ So, n divides n_2. Thus, $n_1 = 1$ and $n = n_2$. So, $f_k(X) = n (\zeta + X)^k$ is irreducible for every k with $\gcd(n, k) = 1$. Therefore, $D(n (\zeta + X))$ is infinite in $R[X]$. So, $R[X]$ is not IDPF. ■

We can extend this result to all cyclotomic extensions by induction. Before we do this, we need the following lemma.

Lemma 37 *Let ζ be a primitive mth root of unity, where $m \geq 3$, and m has at least two prime factors, not necessarily distinct. Let p be a prime factor of m. (So, $\zeta^{m/p}$ is a pth root of unity) Let A_p and A_m denote the ring of integers in $\mathbb{Q}(\zeta^{m/p})$ and $\mathbb{Q}(\zeta)$ respectively. (So that A_p has integral basis $\left\{1, \zeta^{m/p}, \ldots, \left(\zeta^{m/p}\right)^{p-2}\right\}$ and A_m has integral basis $\left\{1, \zeta, \ldots, \zeta^{\phi(m)-1}\right\}$) Let $R_p = span_{\mathbb{Z}}\left\{1, n\zeta^{m/p}, \ldots, n\left(\zeta^{m/p}\right)^{p-2}\right\}$ and $R_m = span_{\mathbb{Z}}\left\{1, n\zeta, \ldots, n\zeta^{\phi(m)-1}\right\}$. Then,*

1. *$R_p = A_p \cap R_m$,*
2. *$(A_p \cap R_m)[X] = A_p[X] \cap R_m[X]$, and*
3. *$U(A_p[X] \cap R_m[X]) = U(A_p[X]) \cap U(R_m[X])$.*

Proof.

1. We must show that $R_p = A_p \cap R_m$. Let $x \in R_p$. Then, $x = z_0 + nz_1\zeta^{m/p} + \cdots + nz_{p-2}\left(\zeta^{m/p}\right)^{p-2}$, where $z_i \in \mathbb{Z}$. Then, x is clearly in A_p. Now, for $\left(\zeta^{m/p}\right)^i$, $0 \leq i \leq p-2$, if $(m/p)\, i > \phi(m) - 1$, we can express $\left(\zeta^{m/p}\right)^i$ in terms of the basis elements $\{1, \zeta, \ldots, \zeta^{\phi(m)-1}\}$ for A_m over $\mathbb{Z}$. Since $z_i \in \mathbb{Z}$ and each term of x with ζ^i, $1 \leq i \leq \phi(m) - 1$ is divisible by n, it follows that $x \in R_m$. Thus, $x \in A_p \cap R_m$. Conversely, let $x \in A_p \cap R_m$. Then, $x \in R_m$ implies that $x = z_0 + nz_1\zeta + \cdots + nz_{\phi(m)-1}\zeta^{\phi(m)-1}$. But, $x \in A_p$ implies that $z_i = 0$ for any i that is not an integer multiple of m/p. Thus, $x \in R_p$. So, $R_p = A_p \cap R_m$.

2. We must show that $(A_p \cap R_m)[X] = A_p[X] \cap R_m[X]$. Let $f(X) \in (A_p \cap R_m)[X]$. Then, $f(X) = a_0 + a_1X + \cdots + a_qX^q$, where $a_i \in A_p \cap R_m$. Thus, $f(X) \in A_p[X] \cap R_m[X]$. Conversely, let $f(X) \in A_p[X] \cap R_m[X]$. Then, $f(X) = a_0 + a_1X + \cdots + a_qX^q$, and the $a_i \in A_p$ and $a_i \in R_m$. Thus, $f(X) \in (A_p \cap R_m)[X]$. So, $(A_p \cap R_m)[X] = A_p[X] \cap R_m[X]$.

3. We must show that $U(A_p[X] \cap R_m[X]) = U(A_p[X]) \cap U(R_m[X])$. Let $f(X) \in U(A_p[X] \cap R_m[X])$. Then, there exists a $g(X) \in A_p[X] \cap R_m[X]$ such that $f(X)g(X) = 1$. Now, $f(X)$, $g(X) \in A_p[X]$ and $f(X)g(X) = 1$. Thus, $f(X) \in U(A_p[X])$. Similarly, $f(X) \in U(R_m[X])$. Thus, $f(X) \in U(A_p[X]) \cap U(R_m[X])$. Conversely, let $f(X) \in U(A_p[X]) \cap U(R_m[X])$. Then, $f(X) \in U(A_p[X])$ implies that there exists $g(X) \in A_p[X]$ with $f(X)g(X) = 1$. Now, $f(X) \in U(R_m[X])$ implies that there exists $h(X) \in U(R_m[X])$ such that $f(X)h(X) = 1$. But, $f(X)$, $g(X)$, $h(X) \in A_m[X]$. So, by the

uniqueness of inverses in $A_m[X]$, $g(X) = h(X)$. Thus, $f(X) \in U(A_p[X] \cap R_m[X])$. So, $U(A_p[X] \cap R_m[X]) = U(A_p[X]) \cap U(R_m[X])$.

■

Theorem 38 *Let ζ_m be an mth root of unity, where $m \geq 3$. Let $\left\{1, \zeta_m, \ldots, \zeta_m^{\phi(m)-1}\right\}$ be a basis for $\mathbb{Q}(\zeta_m)$ over $\mathbb{Q}$. (Then, the ring of integers A_m in $\mathbb{Q}(\zeta_m)$ has an integral basis $\{1, \zeta_m, \ldots, \zeta_m^{\phi(m)-1}\}$.) Let R be the order $R = span_{\mathbb{Z}}\left\{1, n\zeta_m, \ldots, n\zeta_m^{\phi(m)-1}\right\}$, and let $n = p_1^{l_1} \ldots p_r^{l_r}$ be the prime factorization of n. If $R[X]$ is IDPF, then $p_i | \delta_{\mathbb{Q}(\zeta_m)}$ for every $1 \leq i \leq r$.*

Proof. We induct on the number of prime factors in m. If $m = p$, then this is Lemma 36. Suppose the result holds for all m having less than or equal to r prime factors. Let m have $r+1$ prime factors and let $\zeta = e^{\frac{2\pi i}{m}}$. Let p be a prime factor of m and let A_p denote the ring of integers in $\mathbb{Q}(\zeta^{m/p})$. Now, $\zeta^{m/p}$ is a pth root of unity. So, A_p has an integral basis $\left\{1, \zeta^{m/p}, \ldots, \left(\zeta^{m/p}\right)^{p-2}\right\}$. Let A_m denote the ring of integers in $\mathbb{Q}(\zeta)$. Let $R_m = \text{span}_{\mathbb{Z}}\left\{1, n\zeta, \ldots, n\zeta^{\phi(m)-1}\right\}$ and $R_p = \text{span}_{\mathbb{Z}}\left\{1, n\zeta^{m/p}, \ldots, n\left(\zeta^{m/p}\right)^{p-2}\right\}$. From Lemma 37, $R_p = A_p \cap R_m$. Since R_m is an order in A_m, R_m is Noetherian; that is, R_m is Noetherian since R_m is a finitely generated $\mathbb{Z}$-module. Also, $R_m \subseteq A_m$, A_m is integrally closed, and R_m and A_m have the same quotient fields. Thus, the integral closure of R_m is A_m; that is, $\widetilde{R_m} = A_m$. Finally, $n \in [R_m : A_m]$. So, $R_m[X]$ is Noetherian, $\widetilde{R_m[X]} = \widetilde{R_m}[X] = A_m[X]$, and $n \in [R_m[X] : A_m[X]]$. By hypothesis, $R_m[X]$ is IDPF. So, by [14, Theorem 2.8], $R_m[X] \subseteq A_m[X]$ is a root extension and $U\left(A_m[X]\right)/U\left(R_m[X]\right)$ is finite. By similar reasoning, $\widetilde{R_p[X]} = A_p[X]$, $R_p[X]$ is Noetherian, and $n \in [R_p[X] : A_p[X]]$. So, in order to show that $R_p[X]$ is IDPF, and hence apply the induction hypothesis, we must show that $U(A_p[X])/U(R_p[X])$ is finite and $R_p[X] \subseteq A_p[X]$ is a root extension. By Lemma 37, $(A_p \cap R_m)[X] = A_p[X] \cap R_m[X]$ and $U(A_p[X] \cap R_m[X]) = U(A_p[X]) \cap U(R_m[X])$. So, by the second isomorphism theorem, we have

$$\begin{aligned}
\left|\frac{U(A_p[X])}{U(R_p[X])}\right| &= \left|\frac{U(A_p[X])}{U(A_p[X] \cap R_m[X])}\right| \\
&= \left|\frac{U(A_p[X])}{(U(A_p[X]) \cap U(R_m[X]))}\right| \\
&= \left|\frac{U(A_p[X])U(R_m[X])}{U(R_m[X])}\right| \\
&\leq \left|\frac{U(A_m[X])}{U(R_m[X])}\right| \\
&< \infty
\end{aligned}$$

Thus, $U(A_p[X])/U(R_p[X])$ is finite. Now, let $f(X) \in A_p[X]$. Then, $f(X) \in A_m[X]$. Since $R_m[X] \subseteq A_m[X]$ is a root extension, there exists a positive integer c such that $(f(X))^c \in R_m[X]$. But, $(f(X))^c \in A_p[X]$ by closure. Thus, $(f(X))^c \in R_m[X] \cap A_p[X] = (R_m \cap A_p)[X] = R_p[X]$. So, $R_p[X] \subseteq A_p[X]$ is a root extension. Since, $U(A_p[X])/U(R_p[X])$ is finite and $R_p[X] \subseteq A_p[X]$ is a root extension, it follows from [14, Theorem 2.8] that $R_p[X]$ is IDPF. By the induction hypothesis, p_i divides $\delta_{\mathbb{Q}(\zeta^{m/p})}$ for every i. We claim that $\delta_{\mathbb{Q}(\zeta^{m/p})}$ divides $\delta_{\mathbb{Q}(\zeta)}$. For, by [23, Proposition 2.7],

$$\delta_{\mathbb{Q}(\zeta^{m/p})} = (-1)^{\phi(p)/2} p^{p-2}.$$

Now, p divides m. Write $m = p^r a$, where $\gcd(p, a) = 1$. Then, by [23, Proposition 2.7],

$$\begin{aligned}
\delta_{\mathbb{Q}(\zeta)} &= (-1)^{\phi(m)/2} \frac{m^{\phi(m)}}{\prod_{q|m} q^{\phi(m)/(q-1)}} \\
&= (-1)^{\phi(p^r a)/2} \frac{(p^r a)^{\phi(p^r a)}}{\prod_{q|m} q^{\phi(p^r a)/(q-1)}} \\
&= (-1)^{\phi(p^r)\phi(a)/2} \frac{(p^r)^{\phi(p^r)\phi(a)} a^{\phi(p^r)\phi(a)}}{p^{(\phi(p^r)\phi(a))/(p-1)} \prod_{q|m,\, q\neq p} q^{\phi(p^r)\phi(a)/(q-1)}} \\
&= (-1)^{\phi(p^r)\phi(a)/2} \, \frac{p^{r(p-1)p^{r-1}\phi(a)}}{p^{p^{r-1}\phi(a)}} \, \frac{a^{\phi(a)\phi(p^r)}}{\prod_{q|m,\, q\neq p} q^{(\phi(a)/(q-1))\phi(p^r)}} \\
&= p^{p^{r-1}\phi(a)(r(p-1)-1)} \left(\frac{(-1)^{\phi(a)/2} a^{\phi(a)}}{\prod_{q|a} q^{\phi(a)/(q-1)}} \right)^{\phi(p^r)} \\
&= p^{p^{r-1}\phi(a)(r(p-1)-1)} \left(\delta_{\mathbb{Q}(\zeta^{m/(p^r)})} \right)^{\phi(p^r)}
\end{aligned}$$

.

Since $r \geq 1$, it follows that p^{p-2} divides $\delta_{\mathbb{Q}(\zeta)}$. So, $\delta_{\mathbb{Q}(\zeta^{m/p})} | \delta_{\mathbb{Q}(\zeta)}$ and since $p_i | \delta_{\mathbb{Q}(\zeta^{m/p})}$ for all i, it follows that $p_i | \delta_{\mathbb{Q}(\zeta)}$ for every i. ■

Unfortunately, the condition that p_i divides $\delta_{\mathbb{Q}(\zeta)}$ in the previous theorem is not sufficient.

Example 39 *The condition in Theorem 38 that p_i divides $\delta_{\mathbb{Q}(\zeta)}$ is not sufficient.*

Let $\zeta = e^{\frac{2\pi i}{15}}$. Then, by [23, Proposition 2.7],

$$\begin{aligned}\delta_{\mathbb{Q}(\zeta)} &= (-1)^{\phi(15)/2}\frac{15^{\phi(15)}}{3^{\phi(15)/2}5^{\phi(15)/4}} \\ &= 3^4 5^6.\end{aligned}$$

Thus, $\delta_{\mathbb{Q}(\zeta)}$ is divisible by 3. Now, $\phi(15) = 8$, so $\{1, \zeta, \zeta^2, \ldots, \zeta^7\}$ is a basis for $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$. If A denotes the ring of integers in $\mathbb{Q}(\zeta)$, then it follows that $\{1, \zeta, \zeta^2, \ldots, \zeta^7\}$ is an integral basis for A. Let $R = \text{span}_{\mathbb{Z}}\{1, 3\zeta, \ldots, 3\zeta^7\}$. Then, R is an order in A. We claim that $R[X] \subseteq A[X]$ is not a root extension. For, consider $f(X) = 1 + \zeta X \in D[X]$. Let m be a positive integer. Then, from the binomial expansion, we have that

$$(1 + \zeta X)^m = \sum_{j=0}^{m} \binom{m}{j} \zeta^j X^j.$$

If $j = 1$, we get the monomial $m\zeta X$, and the integer coefficient is m. If m is not divisible by 3, then $(1 + \zeta X)^m \notin R[X]$. If m is divisible by 3, write $m = 3^r a$, $r \geq 1$, and $\gcd(3, a) = 1$. Consider the $j = 3^r$ term, which is $\binom{m}{3^r}\zeta^{3^r} X^{3^r}$. Observe that $\zeta^{3^r} \neq 1$. For, if $\zeta^{3^r} = 1$, then $3^r = 15x$, for some positive integer x. Thus, $3^{r-1} = 5x$, a contradiction to the unique factorization of 3^{r-1}. So, $j = 3^r$ has a nonzero ζ part. Now, either ζ^{3^r} is a basis element, or not. If not, ζ^{3^r} can be written as a linear combination of the basis elements $\{1, \zeta, \ldots, \zeta^7\}$ over $\mathbb{Z}$. Using the irreducible polynomial for ζ over $\mathbb{Q}$, which is $\Phi_{15}(X) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$, we see that

$$\begin{aligned}\zeta^8 &= \zeta^7 - \zeta^5 + \zeta^4 - \zeta^3 + \zeta - 1 \\ \zeta^9 &= \zeta^7 - \zeta^6 - \zeta^3 + \zeta^2 - 1 \\ \zeta^{10} &= -\zeta^5 - 1 \\ \zeta^{11} &= -\zeta^6 - \zeta\end{aligned}$$

$$\begin{aligned}
\zeta^{12} &= -\zeta^7 - \zeta^2 \\
\zeta^{13} &= -\zeta^7 + \zeta^5 - \zeta^4 - \zeta + 1 \\
\zeta^{14} &= -\zeta^7 + \zeta^6 - \zeta^4 + \zeta^3 - \zeta^2 + 1.
\end{aligned}$$

The largest common integer factor of each of $\zeta^8, \ldots, \zeta^{14}$ is 1. Thus, the integer coefficient of the $j = 3^r$-monomial is $\binom{m}{3^r}$ which is not divisible by 3. Thus, $(f(X))^m \notin R[X]$ for any m. Since $R[X]$ is Noetherian, $\widetilde{R[X]} = A[X]$ and $3 \in [R[X] : A[X]]$, it follows from [14, Theorem 2.8] that $R[X]$ is not IDPF. So, we have seen that the condition that p_i divide $\delta_{\mathbb{Q}(\zeta)}$ in Theorem 38 is not sufficient. However, if ζ is a p^mth root of unity, this condition is sufficient. Recall that if ζ is a p^mth root of unity, then the only prime divisor of $\delta_{\mathbb{Q}(\zeta)}$ is p.

Theorem 40 *Let ζ be a p^mth root of unity with basis $\{1, \zeta, \ldots, \zeta^{\phi(p^m)-1}\}$ for $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$. Let A be the ring of integers in $\mathbb{Q}(\zeta)$ (Then, $\{1, \zeta, \ldots, \zeta^{\phi(m)-1}\}$ is an integral basis for A). Let $R = span_{\mathbb{Z}}\{1, p^k\zeta, \ldots, p^k\zeta^{\phi(p^m)-1}\}$, where k is any positive integer. Then, $R[X]$ is IDPF.*

Proof. We claim that $R[X] \subseteq A[X]$ is a root extension. To prove this, we induct on k. Suppose that $k = 1$. Then,

$$\begin{aligned}
(f(X))^{p^m} &= \left(g_0(X) + g_1(X)\zeta + \cdots + g_{\phi(p^m)-1}(X)\zeta^{\phi(p^m)-1}\right)^{p^m} \\
&= \sum_{j=0}^{p^m} \binom{p^m}{j} g_0(X)^{p^m-j} \left(g_1(X)\zeta + \cdots + g_{\phi(p^m)-1}(X)\zeta^{\phi(m)-1}\right)^j
\end{aligned}$$

If $j = 0$, we do not have a nonzero ζ^i term. For $j = 1, \ldots, p^m - 1$, $\binom{p^m}{j}$ is divisible by p. If $j = p^m$, we have

$$
\begin{aligned}
& \left(g_1(X)\zeta + \cdots + g_{\phi(p^m)-1}(X)\zeta^{\phi(p^m)-1}\right)^{p^m} \\
= \; & \zeta^{p^m}\left(g_1(X) + \cdots + g_{\phi(p^m)-2}(X)\right)^{p^m} \\
= \; & \left(g_1(X) + \cdots + g_{\phi(p^m)-2}(X)\right)^{p^m} \\
= \; & \sum_{j=0}^{p^m} \binom{p^m}{j} g_1(X)^{p^m-j}\left(g_2(X) + \cdots + g_{\phi(p^m)-1}(X)\zeta^{\phi(p^m)-2}\right)^j
\end{aligned}
$$

Again, $j = 0$ gives no nonzero ζ^i terms. For $j = 1, \ldots, p^m - 1$, $\binom{p^m}{j}$ is divisible by p. If $j = p^m$, we get

$$
\begin{aligned}
& \left(g_2(X)\zeta + \cdots + g_{\phi(p^m)-1}(X)\zeta^{\phi(p^m)-2}\right)^{p^m} \\
= \; & \zeta^{p^m}\left(g_2(X) + \cdots + g_{\phi(p^m)-3}(X)\right)^{p^m} \\
= \; & \left(g_2(X) + \cdots + g_{\phi(p^m)-3}(X)\right)^{p^m} \\
= \; & \sum_{j=0}^{p^m} \binom{p^m}{j} g_2(X)^{p^m-j}\left(g_3(X) + \cdots + g_{\phi(p^m)-1}(X)\zeta^{\phi(p^m)-3}\right)^j
\end{aligned}
$$

Continuing in this manner, we obtain

$$
\left(g_{\phi(p^m)-2}(X) + g_{\phi(p^m)-1}(X)\zeta\right)^{p^m} = \sum_{j=0}^{p^m} \binom{p^m}{j} g_{\phi(p^m)-2}(X)^{p^m-j}\left(g_{\phi(p^m)-1}(X)\right)^j \zeta^j
$$

For $j = 0$, there is no nonzero ζ^i term. For $j = 1, \ldots, p^m - 1$, $\binom{p^m}{j}$ is divisible by p. For $j = p^m$, we get, $g_{\phi(p^m)-1}(X)\zeta^{p^m} = g_{\phi(p^m)-1}(X)$ and hence there is no nonzero ζ^i term. Thus, the ζ^i-parts of $(f(X))^{p^m}$ are all divisible by p. Now, for the induction step, we get

$$
\begin{aligned}
(f(X))^{p^{m(k+1)}} &= \left(\left(g_0(X) + g_1(X)\zeta + \cdots + g_{\phi(p^m)-1}(X)\zeta^{\phi(p^m)-1}\right)^{p^{mk}}\right)^{p^m} \\
&= \left(g_0(X) + p^k\widetilde{g_1}(X)\zeta + \cdots + p^k\widetilde{g_{\phi(p^m)-1}}(X)\zeta^{\phi(p^m)-1}\right)^{p^m} \\
&= \sum_{j=0}^{p^m} \binom{p^m}{j} g_0(X)^{p^m-j}\left(p^k\widetilde{g_1}(X)\zeta + \cdots + p^k\widetilde{g_{\phi(p^m)-1}}(X)\zeta^{\phi(p^m)-1}\right)^j
\end{aligned}
$$

For $j = 0$, we have no nonzero ζ^i part. For $j = 1, \ldots, p^m - 1$, $\binom{p^m}{j}$ is divisible by p and each term has a common factor of p^k. Thus, each term has the common factor of $\binom{p^m}{j} p^{kj}$ which is divisible by p^{k+1}. If $j = p^m$, we get

$$\left(p^k \widetilde{g_1}(X)\zeta + \cdots + p^k \widetilde{g_{\phi(p^m)-1}}(X)\zeta^{\phi(p^m)-1}\right)^{p^m} = p^{kp^m}\left(\widetilde{g_1}(X)\zeta + \cdots + \widetilde{g_{\phi(p^m)-1}}(X)\zeta^{\phi(p^m)-1}\right),$$

which is divisible by p^{k+1}. So, $R[X] \subseteq A[X]$ is a root extension. Thus, $R \subseteq A$ is a root extension. Since R is an order in an algebraic number ring, R is IDPF by [8, Proposition 9]. Since $p^k \in [R : A]$, $\widetilde{R} = A$, R is Noetherian and R is IDPF, [14, Theorem 2.8] gives that $U(A)/U(R)$ is a finite group. Thus, $U(A[X])/U(R[X])$ is a finite group. Since $R[X] \subseteq A[X]$ is a root extension and $U(A[X])/U(R[X])$ is finite, it follows from [14, Theorem 2.8] that $R[X]$ is IDPF. ■

4.6 Conclusion

In this chapter, we have seen that R IDPF may or may not imply that $R[X]$ is IDPF. In particular, for quadratic integer rings, $\mathbb{Z}[\omega]$, where

$$\omega = \begin{cases} \frac{-1+\sqrt{d}}{2} & \text{if } d \equiv 1 \mod 4 \\ \sqrt{d} & \text{if } d \equiv 2,\ 3 \mod 4 \end{cases},$$

we know that the order $\mathbb{Z}[n\omega]$ is IDPF if and only if $\left(\frac{\delta_{\mathbb{Q}(\sqrt{d})}}{p}\right) \neq 1$, for every $p | \delta_{\mathbb{Q}(\sqrt{d})}$ [8, Example 3]. We have shown that the only orders $\mathbb{Z}[n\omega]$ such that $\mathbb{Z}[n\omega][X]$ is IDPF are precisely the orders where $\left(\frac{\delta_{\mathbb{Q}(\sqrt{d})}}{p}\right) = 0$, for every prime p dividing n. That is, if $\mathbb{Z}[n\omega]$ is IDPF and some prime divisor p of n is such that $\left(\frac{\delta_{\mathbb{Q}(\sqrt{d})}}{p}\right) = -1$, then $\mathbb{Z}[n\omega][X]$ is not IDPF, even though $\mathbb{Z}[n\omega]$ is IDPF. On the other hand, if $\mathbb{Z}[n\omega]$ is IDPF and all prime divisors p of n are such that $\left(\frac{\delta_{\mathbb{Q}(\sqrt{d})}}{p}\right) = 0$, then $\mathbb{Z}[n\omega][X]$ is IDPF. We then looked at the ring of integers in cyclotomic field extensions $\mathbb{Q}(\zeta)$, where ζ is a primitive root of unity. Given the order $R = \mathbb{Z}[n\zeta]$, we showed that if $R[X]$ is IDPF, then $p_i | \delta_{\mathbb{Q}(\sqrt{d})}$ for every i, where $n = p_1^{l_1} \cdots p_r^{l_r}$. In contrast with the quadratic integer rings, we saw that this condition is not sufficient by looking at the case where ζ is a primitive 15th root of unity. We then showed that if ζ is a p^mth primitive root of unity, where p is

prime, then the condition is sufficient. In the next chapter, we show that given an order R of a quadratic integer ring, $R[X]$ is IDPF if and only if $R[X]$ is inside factorial if and only if $R[X]$ is almost Schreier.

Chapter 5

Polynomial Rings With Coefficients From Orders in Quadratic Integer Rings and Factorization

5.1 Introduction

Let $\mathbb{Z}[\omega]$ denote a quadratic integer ring, where

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

Let R be an order in this quadratic integer ring. Then, it is well known (see for example [9]) that

$$R = \mathbb{Z}[n\omega] = \{a + nb\omega : a,\ b,\ n \in \mathbb{Z},\ \text{with}\ \ n > 1\}.$$

Let $\delta_{\mathbb{Q}(\sqrt{d})}$ denote the discriminant of $\mathbb{Q}(\sqrt{d})$. Then, it is well known (see for example [19]) that

$$\delta_{\mathbb{Q}(\sqrt{d})} = \begin{cases} d & \text{if } d \equiv 1 \mod 4 \\ 4d & \text{if } d \equiv 2,\ 3 \mod 4 \end{cases}.$$

In this chapter, we show that given an order R of the quadratic integer rings, $R[X]$ is IDPF if and only if $R[X]$ is inside factorial if and only if $R[X]$ is almost Schreier if and only if some number theoretic property on the prime divisors of $n \in [R :_R \widetilde{R}]$ holds. In general, the above three factorization properties are not equivalent. For example, for a general integral domain R, if R is inside factorial, then R is almost Schreier by [11, Proposition 2.2(e)]. However, the converse does not hold. The domain $\mathbb{C}[[X^2, X^3]]$, which is the ring of all formal power series with coefficients in $\mathbb{C}$ and zero linear term, is almost Schreier [11, Example 4.2]. But, it is not inside factorial by [8, Theorem 7(a)], as $\mathbb{C}[[X^2, X^3]] \subseteq \mathbb{C}[[X]]$ is not a root extension. The notions of inside factorial and IDPF are completely independent. For example, every Krull domain is IDPF by [21, Corollary 3.3]. However, not every Krull domain has torsion class group, and hence by [8, Theorem 7(a)], not every IDPF domain is inside factorial. On the other hand, $\mathbb{Z}[2i][[X]]$ is inside factorial, as $\mathbb{Z}[2i][[X]] \subseteq \mathbb{Z}[i][[X]]$ is a root extension and $\mathbb{Z}[i][[X]]$ is a UFD. However, by [14, Theorem 2.8], $\mathbb{Z}[2i][[X]]$ is not IDPF, as $U(\mathbb{Z}[i][[X]])/U(\mathbb{Z}[2i][[X]])$ is an infinite group. The above examples also serve to show the independence of the almost Schreier property and IDPF. For, by [11, Proposition 2.2(e)], $\mathbb{Z}[2i][[X]]$ is almost Schreier and not IDPF. To see that IDPF does not imply almost Schreier, we may take a Krull domain with non-torsion class group (see [14, Corollary 3.3] and [11, Theorem 3.1]).

5.2 Quadratic Integer Rings and Factorization

We first classify the orders R of the quadratic integer rings with $R[X]$ almost Schreier.

Theorem 41 *Let $\mathbb{Z}[n\omega]$ be an order in $\mathbb{Z}[\omega]$. Then, $\mathbb{Z}[n\omega][X]$ is almost Schreier if and only if every prime divisor p of n has $p \mid \delta_{\mathbb{Q}(\sqrt{d})}$.*

Proof. If $p \mid \delta_{\mathbb{Q}(\sqrt{d})}$ for every prime p dividing n, then $\mathbb{Z}[n\omega][X]$ is IDPF by Theorem 35. As $[\mathbb{Z}[n\omega][X] :_{\mathbb{Z}[n\omega][X]} \mathbb{Z}[\omega][X]] \neq \{0\}$ and $\mathbb{Z}[n\omega][X]$ is Noetherian, it follows that $\mathbb{Z}[n\omega][X] \subseteq \widetilde{\mathbb{Z}[n\omega][X]} = \mathbb{Z}[\omega][X]$ is a root extension ([14, Theorem 2.8]). Since $\mathbb{Z}[\omega]$ is a Krull domain, $\mathbb{Z}[\omega][X]$ is a Krull domain. Also, since $\mathbb{Z}[\omega]$ has finite, and hence torsion, class group, it follows that $\mathbb{Z}[\omega][X]$ has torsion class group. Thus, $\mathbb{Z}[n\omega][X]$ is inside factorial ([8, Theorem 7(a)]). Therefore, $\mathbb{Z}[n\omega][X]$ is almost Schreier ([11, Proposition 2.2(e)]).

Conversely, suppose some prime divisor p of n has $p \not\mid \delta_{\mathbb{Q}(\sqrt{d})}$. If $\left(\frac{\delta_{\mathbb{Q}(\sqrt{d})}}{p}\right) = 1$, then $\mathbb{Z}[n\omega] \subseteq \mathbb{Z}[\omega]$ is not a root extension ([8, Example 3(1)]). Thus, $\mathbb{Z}[n\omega][X]$ is not almost Schreier

([11, Proposition 4.1]). Now, suppose $\left(\frac{\delta_{\mathbb{Q}(\sqrt{d})}}{p}\right) = -1$. There are two cases to consider. Suppose first that $d \equiv 1 \bmod 4$. Since $\left(\frac{\delta_{\mathbb{Q}(\sqrt{d})}}{p}\right) = -1$, it follows that p is an odd prime. For, if $p = 2$, then $x^2 \equiv d \bmod 2 \equiv 1 \bmod 2$, and this has an integer solution. So, we may assume that p is odd. Let m be such that $p^m \mid n$ and $p^{m+1} \nmid n$. Then, $p^{2m} \mid n(\omega + X)n(\overline{\omega} + X)$ in $\mathbb{Z}[n\omega][X]$. For,

$$\begin{aligned} n(\omega + X)n(\overline{\omega} + X) &= n^2(\omega\overline{\omega} + (\omega + \overline{\omega})X + X^2) \\ &= n^2(\omega\overline{\omega} + (\omega - 1 - \omega)X + X^2) \\ &= n^2(\omega\overline{\omega} - X + X^2), \end{aligned}$$

and $\omega\overline{\omega} - X + X^2 \in \mathbb{Z}[n\omega][X]$, as $d \equiv 1 \bmod 4$. Now, we claim that p^{2m} is not almost primal in $\mathbb{Z}[n\omega][X]$. Suppose it is. Then, there exists an integer $k \geq 1$ and $a,\ b \in \mathbb{Z}[n\omega]$ such that $p^{2mk} = ab$ with $a \mid n^k(\omega + X)^k$ and $b \mid n^k(\overline{\omega} + X)^k$. Now, $p^{2mk} = ab$ is a factorization of p^{2mk} in $\mathbb{Z}[\omega]$. Since $\left(\frac{\delta_{\mathbb{Q}(\sqrt{d})}}{p}\right) = -1$ and $p \neq 2$, (p) remains prime in $\mathbb{Z}[\omega]$ ([19, Proposition 13.1.3(ii)]). Thus, p is prime in $\mathbb{Z}[\omega]$. So, p^{2mk} has a unique factorization into irreducibles in $\mathbb{Z}[\omega]$, up to unit multiples and order of the factors, by Lemma 31. So, $a = up^{l_1}$ and $b = u^{-1}p^{l_2}$, where $u \in U(\mathbb{Z}[\omega])$, $l_1,\ l_2 \in \mathbb{N}$ and $l_1 + l_2 = 2mk$. As $\mathbb{Z}[n\omega] \subseteq \mathbb{Z}[\omega]$ a root extension ([8, Example 3]), we may assume without loss of generality, that $u = 1$. Now, either $l_1 \geq mk$ or $l_2 \geq mk$. Suppose first that $l_1 \geq mk$. Then, p^{l_1} divides

$$n^k(\omega + X)^k = n^k \sum_{j=0}^{k} \binom{k}{j} \omega^j X^{k-j}.$$

Write $k = p^r z$, where $\gcd(p, z) = 1$. Then, consider the $j = p^r$ term of $(\omega + X)^k$, which is $\binom{k}{p^r}\omega^{p^r}X^{k-p^r}$. The ω-part of ω^{p^r} is not divisible by p by Lemma 32. Also, by Lemma 33, $\binom{k}{p^r}$ is not divisible by p. Thus, the ω-part of the coefficient of the $j = p^r$ term of $(\omega + X)^k$ is not divisible by n and hence $(\omega + X)^k \notin \mathbb{Z}[n\omega][X]$. So, for p^{l_1} to divide $n^k(\omega + X)^k$ in $\mathbb{Z}[n\omega][X]$, we must have

$p^{l_1} \mid n^{k-1}$. But, $l_1 \geq mk$, so this is impossible. So, it must be that $l_2 \geq mk$. So, p^{l_2} divides

$$\begin{aligned} n^k(\overline{\omega}+X)^k &= n^k \sum_{j=0}^{k} \binom{k}{j} (\overline{\omega})^j X^{k-j} \\ &= n^k \sum_{j=0}^{k} \binom{k}{j} (-1-\omega)^j X^{k-j} \end{aligned}$$

Consider the $j = p^r$ term of $(\overline{\omega}+X)^k$, which is

$$\binom{k}{p^r}(-1-\omega)^{p^r} X^{k-p^r}.$$

Now, as before, $p \nmid \binom{k}{p^r}$, and we claim that p does not divide the ω-part of $(-1-\omega)^{p^r}$. For,

$$(-1-\omega)^{p^r} = \sum_{t=0}^{p^r} \binom{p^r}{t} (-1)^{p^r-t}(-\omega)^t.$$

Now, $p \mid \binom{p^r}{t}$ for $1 \leq t \leq p^r - 1$. If $t = 0$, we get zero ω-part. If $t = p^r$, we get $-\omega^{p^r}$, and p does not divide the ω-part of this expression by Lemma 32. So, p does not divide the ω-part of $(-1-\omega)^{p^r}$. Thus, p does not divide the ω-part of some coefficient of $(\overline{\omega}+X)^k$ and hence n does not divide the ω-part of some coefficient of $(\overline{\omega}+X)^k$. Therefore, $(\overline{\omega}+X)^k \notin \mathbb{Z}[n\omega][X]$. So, for p^{l_2} to divide $n^k(\overline{\omega}+X)^k$ in $\mathbb{Z}[n\omega][X]$, we must have $p^{l_2} \mid n^{k-1}$. But, $l_2 \geq mk$, so this is impossible. Thus, p^{2m} is not almost primal in $\mathbb{Z}[n\omega][X]$ and hence $\mathbb{Z}[n\omega][X]$ is not almost Schreier.

We now consider the case when $d \equiv 2,\ 3 \bmod 4$. As $\left(\frac{\delta_{\mathbb{Q}(\sqrt{d})}}{p}\right) = -1$, $p \nmid \delta_{\mathbb{Q}(\sqrt{d})} = 4d$. Thus, $p \neq 2$. Again, we claim that p^{2m} is not almost primal in $\mathbb{Z}[n\omega][X]$. For, consider $p^{2m} \mid n(\sqrt{d}+X)n(-\sqrt{d}+X) = n^2(-d+X^2)$. As $-d+X^2 \in \mathbb{Z}[n\omega][X]$,
$p^{2m} \mid n(\sqrt{d}+X)n(-\sqrt{d}+X)$ in $\mathbb{Z}[n\omega][X]$. Suppose p^{2m} is almost primal in $\mathbb{Z}[n\omega][X]$. Then, there exists an integer $k \geq 1$ and $a,\ b \in \mathbb{Z}[n\omega]$ such that $p^{2mk} = ab$ with $a \mid n^k(\sqrt{d}+X)^k$ and $b \mid n^k(-\sqrt{d}+X)^k$. Since $p \neq 2$ and $\left(\frac{\delta_{\mathbb{Q}(\sqrt{d})}}{p}\right) = -1$, (p) remains prime in $\mathbb{Z}[\omega]$ ([19, Proposition 13.1.3(ii)]). Thus, p is prime in $\mathbb{Z}[\omega]$ and so p^{2mk} has a unique factorization into irreducibles, up to unit multiples and order of the factors, by Lemma 31. So, $a = up^{l_1}$ and $b = u^{-1}p^{l_2}$, where $u \in \mathbb{Z}[\omega]$, $l_1,\ l_2 \in \mathbb{N}$ with $l_1 + l_2 = 2mk$. As $\mathbb{Z}[n\omega] \subseteq \mathbb{Z}[\omega]$ is a root extension ([8, Example 3]), we may assume without loss of generality that $u = 1$. Now, either $l_1 \geq mk$ or $l_2 \geq mk$. Suppose first that $l_1 \geq mk$.

Then, p^{l_1} divides

$$n^k(\sqrt{d}+X)^k = n^k \sum_{j=0}^{k} \binom{k}{j} (\sqrt{d})^j X^{k-j}.$$

Write $k = p^r z$, where $\gcd(p, z) = 1$. Consider the $j = p^r$ term of $(\sqrt{d}+X)^k$, which is

$$\binom{k}{p^r} d^{\frac{p^r-1}{2}} \sqrt{d} X^{k-p^r}.$$

Now, $p \not| \ d$ and $p \not| \binom{k}{p^r}$. Thus, p does not divide the ω-part of the coefficient of the $j = p^r$ term of $(\sqrt{d}+X)^k$ and hence n does not divide the ω-part of the coefficient of the $j = p^r$ term of $(\sqrt{d}+X)^k$. Therefore, $(\sqrt{d}+X)^k \notin \mathbb{Z}[n\omega][X]$. So, for p^{l_1} to divide $n^k(\sqrt{d}+X)^k$ in $\mathbb{Z}[n\omega][X]$, we must have $p^{l_1} \mid n^{k-1}$. But, $l_1 \geq mk$, so this is impossible. A similar argument shows that if $l_2 \geq mk$, then p^{l_2} does not divide $n^k(-\sqrt{d}+X)^k$ in $\mathbb{Z}[n\omega][X]$. Thus, p^{2m} is not almost primal in $\mathbb{Z}[n\omega][X]$ and hence $\mathbb{Z}[n\omega][X]$ is not almost Schreier. ■

As a corollary, we will now show that for an order R in the quadratic integer rings, $R[X]$ is IDPF if and only if $R[X]$ is inside factorial if and only if $R[X]$ is almost Schreier if and only if the following number theoretic property on $n \in [R :_R \widetilde{R}]$ holds.

Corollary 42 *Let $\mathbb{Z}[n\omega]$ be an order in the quadratic integer ring $\mathbb{Z}[\omega]$. Then, the following are equivalent.*

1. *$\mathbb{Z}[n\omega][X]$ is IDPF*
2. *$\mathbb{Z}[n\omega][X]$ is inside factorial*
3. *$\mathbb{Z}[n\omega][X]$ is almost Schreier*
4. *$\mathbb{Z}[n\omega][X] \subseteq \widetilde{\mathbb{Z}[n\omega][X]} = \mathbb{Z}[\omega][X]$ is a root extension*
5. *Every prime p dividing n also divides $\delta_{\mathbb{Q}(\sqrt{d})}$.*

Proof.

Since $\mathbb{Z}[n\omega]$ is Noetherian, $\mathbb{Z}[n\omega][X]$ is Noetherian. Also, $\mathbb{Z}[\omega]$ is Krull whence $\mathbb{Z}[\omega][X]$ is Krull. Now, $n \in [\mathbb{Z}[n\omega] :_{\mathbb{Z}[n\omega]} \mathbb{Z}[\omega]]$ and $n \in [\mathbb{Z}[n\omega][X] :_{\mathbb{Z}[n\omega][X]} \mathbb{Z}[\omega][X]]$. Finally, $Cl_t(\mathbb{Z}[\omega])$ is finite and hence torsion, whence $Cl_t(\mathbb{Z}[\omega][X])$ is torsion.

(1) $\Rightarrow$ (2): Since $\mathbb{Z}[n\omega][X]$ is IDPF, $\mathbb{Z}[n\omega][X] \subseteq \mathbb{Z}[\omega][X]$ is a root extension ([14, Theorem 2.8]). From our above observations, the result follows from [8, Theorem 7(a)].

(2) $\Rightarrow$ (1): If $\mathbb{Z}[n\omega][X]$ is inside factorial, $\mathbb{Z}[n\omega]$ is inside factorial (else $\mathbb{Z}[n\omega] \subseteq \mathbb{Z}[\omega]$ is not a root extension, a contradiction to $\mathbb{Z}[n\omega][X]$ inside factorial). By [8, Proposition 9], $\mathbb{Z}[n\omega]$ is IDPF. Thus, $U(\mathbb{Z}[\omega])/U(\mathbb{Z}[n\omega]) = U(\mathbb{Z}[\omega][X])/U(\mathbb{Z}[n\omega][X])$ is a finite group. By the above observations and the fact that $\mathbb{Z}[n\omega][X] \subseteq \mathbb{Z}[\omega][X]$ is a root extension, the result follows by [14, Theorem 2.8].

(1) $\Leftrightarrow$ (4): This follows from [14, Theorem 2.8]. For, $\mathbb{Z}[n\omega][X] \subseteq \mathbb{Z}[\omega][X]$ a root extension implies that $\mathbb{Z}[n\omega] \subseteq \mathbb{Z}[\omega]$ is a root extension. By [8, Proposition 9], $\mathbb{Z}[n\omega]$ is IDPF, and hence $U(\mathbb{Z}[\omega])/U(\mathbb{Z}[n\omega]) = U(\mathbb{Z}[\omega][X])/U(\mathbb{Z}[n\omega][X])$ is a finite group.

(1) $\Leftrightarrow$ (5): This is Theorem 35.

(3) $\Leftrightarrow$ (5): This is Theorem 41.

(2) $\Rightarrow$ (3): This is [11, Proposition 2.2(e)]. ■

5.3 Conclusion

We have seen that for polynomial rings over orders in the quadratic integer rings, the notions of almost Schreier, IDPF, and inside factorial are equivalent and we have given a number theoretic condition for determining precisely when $R[X]$ has one, and hence all, of these properties (Corollary 42). We wonder if these factorization properties are equivalent in a more general setting.

Chapter 6

Conclusion and Future Work

We have investigated the inside factorial, almost Schreier, and IDPF properties in graded domains and, in particular, commutative semigroup rings. We have classified when an M-graded domain is almost Schreier, under the assumption that $R \subseteq \widetilde{R}$ is a root extension, where $\widetilde{R}$ denotes the integral closure of R (see Theorem 10). We then specialized to the case of commutative semigroup rings and proved that if $R[M] \subseteq \widetilde{R[M]}$ is a root extension, then $R[M]$ is almost Schreier if and only if R is an almost Schreier domain and M is an almost Schreier monoid (see Corollary 14). Next, we gave a classification of the graded domains that are inside factorial, via the almost primal property (see Theorem 15). As a corollary, we offered a new proof of the well known result due to Krause ([20, Theorem 3.2]), which gives a classification of when commutative semigroup rings are inside factorial (see Corollary 16).

We continued our investigation of commutative semigroup rings and factorization, proving that no proper numerical semigroup ring of characteristic zero is IDPF (see Theorem 25), even though they are all FFDs (under the assumption that the base ring is an atomic IDPF domain). Then, we determined when numerical semigroup rings of characteristic $q > 0$ are IDPF (see Theorem 26).

Next, we gave a classification of the orders R of the quadratic integer rings such that $R[X]$ is IDPF (see Theorem 35). We were then able to extend this result to include the almost Schreier and inside factorial properties. That is, we showed that given an order R of a quadratic integer ring, $R[X]$ is IDPF if and only if $R[X]$ is inside factorial if and only if $R[X]$ is almost Schreier if and only if $R[X] \subseteq \widetilde{R[X]}$ is a root extension if and only if every prime divisor of n divides $\delta_{\mathbb{Q}(\sqrt{d})}$, the discriminant of $\mathbb{Q}(\sqrt{d})$, where n is the least positive integer in $[R :_R \widetilde{R}]$.

In the future, there are a few things we would like to investigate. In the immediate future, we would like to know whether or not $R[M]$ is almost Schreier if and only if R is an almost Schreier domain, M is an almost Schreier monoid and $R[M] \subseteq \widetilde{R[M]}$ is a root extension. More generally, we would like to know when M-graded domains are almost Schreier. Finally, we would be interested in knowing when graded domains are IDPF.

As a larger project, we would like to determine the relationship between factorization in integral domains and algebraic geometry. In their paper [14, Remark 2.14], Etingof, Malcolmson, and Okoh state that their may be "a significant relationship between the types of singularities of curves and the IDPF-status of the corresponding coordinate rings." In light of the similarities between the IDPF property and the inside factorial and almost Schreier properties in certain settings, we wonder if there could be a connection between types of singularities of curves and whether or not the coordinate ring satisfies some factorization property, such as almost Schreier or inside factorial?

Bibliography

[1] D.D. Anderson and D.F. Anderson, Divisibility Properties of Graded Domains, *Can. J. Math*, Vol. XXXIV, **No.1** (1982), 196-215.

[2] D.D. Anderson and D.F. Anderson, Divisorial Ideals and Invertible Ideals in a Graded Domain, *Journal of Algebra*, **76** (1982), 549-569.

[3] D.D. Anderson, D.F. Anderson, and M. Zafrullah, Factorization in Integral Domains, *Journal of Pure and Applied Algebra*, **69** (1990), 1-19.

[4] D.D. Anderson and B. Mullins, Finite Factorization Domains, *Proceedings of the American Mathematical Society*, **124**, **No.2** (1996), 389-396.

[5] J. Bennett and D. Rush, When Graded Domains are Almost Schreier, In Preparation.

[6] A. Bouvier and M. Zafrullah, On Some Class Groups of an Integral Domain, *Bulletin of the Greek Mathematical Society*, **29** (1988), 45-59.

[7] G. Brookfield and D. Rush, When Graded Domains are Schreier or pre-Schreier, *Journal of Pure and Applied Algebra*, **195** (2005), 225-230.

[8] S. Chapman, F. Halter-Koch, and U. Krause, Inside Factorial Monoids and Integral Domains, *Journal of Algebra*, **252** (2002), 350-375.

[9] H. Cohn, *Advanced Number Theory*, Dover Publications, New York, 1980.

[10] J. Coykendall and T. Dumitrescu, Integral Domains Having Nonzero Elements with Infinitely Many Prime Divisors, *Comm. Algebra*, **4** (2007), 1333-1339.

[11] T. Dumitrescu and W. Khalid, Almost-Schreier Domains, *Comm. Algebra*, **38** (2010), 2981-2991.

[12] D. Dobbs, G. Picavet, and M. Picavet-L'Hermitte, *Arithmetical Properties of Commutative Rings and Monoids*, **241** CRC Press, Florida, (2005), 233-252.

[13] H. Edwards, *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*, Springer, New York, 1977.

[14] P. Etingof, P. Malcolmson, and F. Okoh, Root Extensions and Factorization in Affine Domains, *Canadian Mathematical Bulletin* , **53**, **No.2** (2010), 247-255.

[15] R. Gilmer, *Commutative Semigroup Rings*, The University of Chicago Press, Chicago, 1984.

[16] R. Gilmer, *Multiplicative Ideal Theory*, Queens Papers in Pure and Applied Mathematics, Volume 90, Ontario, Canada, 1992.

[17] A. Grams, Atomic Domains and the Ascending Chain Condition for Principal Ideals, *Math. Proc. Cambridge Philos. Soc.*, **75** (1974), 321-329.

[18] A. Grams and H. Warner, Irreducible Divisors in Domains of Finite Character, *Duke Math Journal*, **42** (1975), 271-284.

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

[20] U. Krause, Semigroup Rings that are Inside Factorial and their Cale Representation *Rings, Modules, Algebras, and Abelian Groups*, Lecture Notes in Pure and Appl. Math., **236**, Dekker, New York, (2004), 353-363.

[21] P. Malcolmson and F. Okoh, A Class of Integral Domains Between Factorial Domains and IDF-Domains, *Houston Journal of Mathematics* , **32**, **No.2** (2006), 399-421.

[22] P. Malcolmson and F. Okoh, Polynomial Extensions of IDF-Domains and of IDPF-Domains, *Proceedings of the American Mathematical Society*, **No.2** (2009), 431-437.

[23] L. Washington, *Introduction to Cyclotomic Fields*, Springer Verlag, New York, 1997.

[24] M. Zafrullah, A General Theory of Almost Factoriality, *Manuscripta Mathematica*, **No.51** (1985), 29-62.

Appendix A

Main Definitions

Throughout this Appendix, R will denote an integral domain, K will denote its quotient field, and $F(R)$ will denote the fractional ideals of R. The reference used for the *-operation and v-operation is [16, Chapter 32 and Chapter 34] and the reference used for the t-operation is [6]. The references for the remaining definitions are [3], [7], [8], [11], [16], [21], and [24].

ACCP: R is said to satisfy the *ascending chain condition on principal ideals (ACCP)* if every ascending chain of principal ideals stabilizes.

AGCD Domain: R is said to be an *almost greatest common divisor domain (AGCD Domain)* if for $x,\ y \in R$, there is an $n \in \mathbb{N}$ such that $x^nR \cap y^nR$ is principal.

Almost Primal: A nonzero element $p \in R$ is said to be *almost primal* if whenever $p \mid xy$ in R, there exists an integer $k \geq 1$ and $p_1,\ p_2 \in R$ such that $p^k = p_1p_2$ with $p_1 \mid x^k$ and $p_2 \mid y^k$.

Almost Schreier: R is said to be *almost Schreier* if every nonzero element of R is almost primal.

Atomic: R is said to be *atomic* if every nonzero nonunit element of R has a factorization into a finite number of irreducibles (atoms).

Divisor Homomorphism: A monoid homomorphism $\phi : D \to H$ is called a *divisor homomorphism* if for any $a,\ b \in D$, $\phi(a) \mid \phi(b)$ in H implies $a \mid b$ in D.

FFD: R is said to be a *finite factorization domain (FFD)* if each nonzero nonunit element of R has only a finite number of non-associate divisors (and hence a finite number of factorizations up to order and associates).

Frobenius Number of a Numerical Semigroup: For a numerical semigroup S, the *Frobenius number of S* , denoted $g = g(S)$, is the largest element of $\mathbb{Z}$ not in S.

GCD Domain: R is said to be a *greatest common divisor domain (GCD Domain)* if for $x,\ y \in R$, $xR \cap yR$ is principal.

Generalized Krull Domain: A *generalized Krull domain* is a locally finite intersection of rank one valuation rings.

gr-Almost-Schreier: A graded domain $R = \bigoplus_{m \in M} R_m$ is said to be *gr-almost-Schreier* if whenever $s \mid xy,\ s,\ x,\ y$ nonzero homogeneous elements, there exists an integer $k \geq 1$ and $s_1,\ s_2$ such that $s^k = s_1 s_2$ with $s_1 \mid x^k$ and $s_2 \mid y^k$.

gr-pre-Schreier: A graded domain $R = \bigoplus_{m \in M} R_m$ is said to be *gr-pre-Schreier* if whenever $s \mid xy$, $s,\ x,\ y$ nonzero homogeneous elements, there exists $s_1,\ s_2$ such that $s = s_1 s_2$ with $s_1 \mid x$ and $s_2 \mid y$.

HFD: An atomic domain R is said to be a *half factorial domain (HFD)* if for any nonzero, nonunit element $a \in R$ any two factorizations of an element a into irreducibles has the same length.

IDF: R is said to be *irreducible divisors finite (IDF)* if each nonzero element of R has at most a finite number of non-associate irreducible divisors.

IDPF: Let a be a nonzero element of R and let $D_n(a)$ denote the set of irreducible divisors of a^n. Then, R is said to be *irreducible divisors of powers finite (IDPF)* if for each nonzero $a \in R$, the set $D(a) = \bigcup_{n=1}^{\infty} D_n(a)$ is finite.

Inside Factorial: A monoid H is called *inside factorial* if there exists a divisor homomorphism $\phi : D \to H$ from a factorial monoid D such that for every $x \in H$ there exists some $n \in \mathbb{N}$ such that $x^n \in \phi(D)$. R is called *inside factorial* if its multiplicative monoid $R^* = R - \{0\}$ is inside factorial.

Krull Domain: A *Krull domain* is a locally finite intersection of discrete valuation rings.

Multiplicity of a Numerical Semigroup: For a numerical semigroup S, the *multiplicity* of S, denoted e, is the smallest positive integer in S.

Numerical Semigroup: A *numerical semigroup* S is a submonoid of $\mathbb{N} = \{0, 1, 2, \dots\}$ with $\mathbb{Z}$ as the group generated by S.

Pre-Schreier: R is said to be a *pre-Schreier* domain if every nonzero element of R is primal.

Primal: A nonzero element $p \in R$ is said to be *primal* if whenever $p \mid xy$, there exists $p_1,\ p_2 \in R$ such that $p = p_1 p_2$ with $p_1 \mid x$ and $p_2 \mid y$.

Rational Generalized Krull Domain: A *rational generalized Krull domain* is a locally finite intersection of rank one valuation rings $\{V_\lambda\}$ such that the value group of each V_λ is isomorphic to an additive subgroup of $\mathbb{Q}$.

Root Extension: An extension of domains $R \subseteq T$ is said to be a *root extension* of domains if for every element $t \in T$, there exists an integer $n \geq 1$ such that $t^n \in R$.

*-Operation: A map $\phi : F(R) \to F(R)$ by $F \mapsto F^*$ is called a **-operation* on R if the following conditions hold for each $a \in K$ and $A,\ B \in F(R)$:

1. $(a)^* = (a)$ and $(aA)^* = aA^*$
2. $A \subseteq A^*$ and if $A \subseteq B$, then $A^* \subseteq B^*$
3. $(A^*)^* = A^*$.

t-Class Group: Let $T(R)$ denote the set of all t-invertible t-ideals. $T(R)$ is a group under t-multiplication (defined by the equations $(AB)_t = (A_tB)_t = (A_tB_t)_t$ for all $A,\ B \in F(R)$). The group $T(R)$ contains as a subgroup $P(R)$, the set of all principal fractional ideals. The quotient group $Cl_t(R) = T(R)/P(R)$ is called the *t-class group* of R.

t-ideal: An ideal $F \in F(R)$ is said to be a *t-ideal* if $F_t = F$.

t-invertible: A fractional ideal $A \in F(R)$ is said to be a *t-invertible ideal* if there exists a fractional ideal $B \in F(R)$ such that $(AB)_t = R$.

t-Operation: For $F \in F(R)$, let $F_t = \bigcup I_v$, where I ranges over finitely generated R-submodules of F. The mapping $F \mapsto F_t$ is a *-operation called the *t-operation*.

UFD: R is said to be a *unique factorization domain (UFD)* if every nonzero, nonunit has a unique factorization into a finite product of irreducibles, up to order of the factors and associates.

v-Operation: For $F \in F(R)$, let F^{-1} denote the fractional ideal $[R :_K F]$ of R. We denote by F_v the mapping $F \mapsto (F^{-1})^{-1}$ and this mapping is a *-operation called the *v-operation*.