THE HALF-FACTORIAL PROPERTY IN POLYNOMIAL RINGS

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

By

Mark Thomas Batell

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

Major Department:
Mathematics

July 2014

Fargo, North Dakota

North Dakota State University
Graduate School

Title

THE HALF-FACTORIAL PROPERTY IN POLYNOMIAL RINGS

By

Mark Thomas Batell

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

DOCTOR OF PHILOSOPHY

SUPERVISORY COMMITTEE:

Jim Coykendall
Co-Chair

Benton Duncan
Co-Chair

Sean Sather-Wagstaff

Ryan Limb

Approved:

July 2, 2014 — Date

Benton Duncan — Department Chair

ABSTRACT

This dissertation investigates the following question: If R is a half-factorial domain (HFD) and x is an indeterminate, under what conditions is the polynomial ring $R[x]$ an HFD?

The question has been answered in a few special cases. A classical result of Gauss states that if R is a UFD, then $R[x]$ is a UFD. Also, Zaks showed that if R is a Krull domain with class group $Cl(R)$, then $R[x]$ is an HFD if and only if $|Cl(R)| \leqslant 2$.

In the proof of his result, Zaks did not use Gauss's methods. We give a new proof that does. We also study the question in domains other than Krull domains.

ACKNOWLEDGMENTS

My advisor, Jim Coykendall, has been a tremendously helpful resource during the research and writing phases of this dissertation. I am very grateful for his advice and support during these times.

I would also like to thank the other members my dissertation committee–Benton Duncan, Sean Sather-Wagstaff, and Ryan Limb–for reading the manuscript and making very helpful suggestions.

Finally, I would like to express my heartfelt gratitude to my family for being a great source of inspiration and encouragement in this endeavor.

TABLE OF CONTENTS

1. INTRODUCTION AND MOTIVATION

The first section of this introductory chapter contains the prerequisite ideal theory and lots of notation. The book [12] is a standard reference for most of the ideal theory we will use. In Section 2, we introduce the concept of elasticity and record some interesting results in this area. In Section 3, we give a thorough discussion of the main problem, which is to characterize the integral domains R whose polynomial rings $R[x]$ are half-factorial.

1.1. Basic Concepts and Notation

Let R be an integral domain. The letter K will always denote the quotient field of R. The units of R will be denoted $U(R)$. For the ring $R[x]$ of polynomials in the indeterminate x, with coefficients in R, we note that $U(R[x]) = U(R)$ [15, p. 162].

A *fractional ideal* of R is a nonzero R-submodule I of K such that $aI \subseteq R$ for some nonzero $a \in R$. An *integral ideal* is a fractional ideal I such that $I \subseteq R$. If $I = Ru$ for some $u \in K$ we say that I is *principal.* For a fractional ideal I, we define $I^{-1} = \{u \in K \mid ua \in R \text{ for all } a \in I\}$. I^{-1} is also a fractional ideal. We say I is *invertible* if $II^{-1} = R$.

For a fractional ideal I of R, we denote $I_v = (I^{-1})^{-1}$, and say that I is a *v-ideal* (or *divisorial*) if $I_v = I$. We note that I_v is the intersection of the principal fractional ideals containing I, that is, $I_v = \bigcap\{(u) \mid u \in K,\ I \subseteq (u)\}$ [12, Theorem 34.1]. I is *v-invertible* if there exists a fractional ideal J such that $(IJ)_v = R$, or equivalently, if $(II^{-1})^{-1} = R$.

A *Krull domain* is a completely integrally closed domain which satisfies the ascending chain condition (ACC) on v-ideals [12, p. 556]. Krull domains have a unique factorization theorem: If I is a nonzero integral ideal of a Krull domain R such that $I_v \neq R$, there are unique (but not necessarily distinct) prime v-ideals $P_1, P_2, \ldots, P_n$ such that $I_v = (P_1P_2 \cdots P_n)_v$ [5, Theorem 2.5].

A *Mori domain* is a domain which has ACC on v-ideals. A domain R is Mori if and only if each nonzero ideal $I \subseteq R$ is v-finite, i.e., there exist $a_0, a_1, \ldots, a_n \in R$ such that $I_v = (a_0, a_1, \ldots, a_n)_v$. A Mori domain is Krull if and only if it is completely integrally closed. If R is an integrally closed Mori domain, then the complete integral closure of R is a Krull domain [3, Theorem 7.7].

In a domain R, the fractional v-ideals form a monoid if we define the product of two v-ideals I, J to be $(IJ)_v$. The v-invertible v-ideals form a subgroup. The quotient group of v-invertible v-ideals modulo the subgroup of principal fractional ideals will be called the *class group* and be denoted by $Cl_v(R)$. If R is completely integrally closed (if R is Krull, for example), then every ideal of R is v-invertible, and in this case we shall write $Cl(R)$ instead of $Cl_v(R)$. For proofs of the results in this paragraph, refer to Section 34 in the book [12].

Let $I = (a_0, a_1, \ldots, a_n)$ be a finitely generated integral ideal of R. We say that I is *primitive* if it is contained in no proper principal ideal of R; that is, if $a_0, a_1, \ldots, a_n$ have no proper common divisor ([2, Definition 1.1]). We say that I is *superprimitive* if $I^{-1} = R$. These concepts are related by the following result.

Theorem 1.1. [17, Theorem C] *Every superprimitive ideal is primitive.*

Proof. Let $I = (a_0, a_1, \ldots, a_n)$ be a superprimitive ideal of R, and assume I is contained in a proper principal ideal of R, say $d \in R \backslash U(R)$ and $I \subseteq (d)$. For each $1 \leqslant i \leqslant n$, there exists $b_i \in R$ such that $a_i = db_i$. Thus $\frac{a_i}{d} \in R$ for each i, which implies $\frac{1}{d} I \subseteq R$ and $\frac{1}{d} \in I^{-1}$. Since I is superprimitive, it follows that $\frac{1}{d} \in R$, so that d is a unit, contrary to the fact Rd is a proper principal ideal of R. $\square$

The converse of the previous theorem is false. For example, in the polynomial ring $R := \mathbb{Q}[x^2, x^3] = \{a_0 + a_2x^2 + a_3x^3 + \cdots + a_nx^n \mid a_0, a_2, \ldots, a_n \in \mathbb{Q}\}$, the ideal $I = (x^2, x^3)$ is primitive (note that $x \notin R$) but not superprimitive because $x \in I^{-1}$

and hence $I^{-1} \neq R$.

For an element f of the polynomial ring $K[x]$, the notation A_f is often used to denote the ideal generated by the coefficients of f; that is, if $f = u_0 + u_1x + \cdots u_nx^n$, then $A_f = Ru_0 + Ru_1 + \cdots + Ru_n$. If $f \in R[x]$, we say that f is a *primitive polynomial* if the ideal A_f is primitive, and *superprimitive* if A_f is superprimitive.

The greatest common divisor of $a_0, a_1, \ldots, a_n \in R$, if it exists, will always be denoted $[a_0, a_1, \ldots, a_n]$. If every pair $a, b \in R \backslash \{0\}$ has a greatest common divisor, then R is called a *GCD-domain.* Let $f(x) = ax + b$ be a linear polynomial with coefficients $a, b \in R$; then f is irreducible in $R[x]$ if and only if $[a, b] = 1$. If $a_0, a_1, \ldots, a_n \in R$ and $(a_0, a_1, \ldots, a_n)_v$ is principal, then the greatest common divisor $[a_0, a_1, \ldots, a_n]$ exists.

1.2. Elasticity

Let R be a domain with quotient field K. We let $\mathrm{Irr}(R)$ denote the irreducible elements of R, and $\mathrm{A}(R)$ will be the elements of R that can be expressed as a product of irreducibles. We say that R is *atomic* if every nonzero nonunit of R belongs to $A(R)$ (irreducibles are sometimes called *atoms*). For a nonzero nonunit element $x \in \mathrm{A}(R)$, we define the *elasticity of* x to be

$$\rho(x) = \sup\left\{\frac{n}{m} \mid x = \pi_1\pi_2\cdots\pi_n = \xi_1\xi_2\cdots\xi_m\right\}$$

where each π_i, ξ_j is an irreducible element (or atom) of R. For example, if x is a product of primes or is a nonzero nonunit of a unique factorization domain (UFD), then $\rho(x) = 1$. If $x \notin \mathrm{A}(R)$ then $\rho(x)$ is undefined.

We can now define the *elasticity of* R to be

$$\rho(R) = \sup\{\rho(x) | x \in \mathrm{A}(R)\}.$$

As previously, we say that the elasticity of a domain without any atoms is undefined.

If R is atomic and $\rho(R) = 1$, then R is called a *half-factorial domain* (HFD). We remark that every UFD is an HFD, but there exist HFD that are not UFD (examples will be given later). In the nonatomic case, the situation can be more exotic. For example in [11] a domain was constructed with a unique (up to associates) irreducible element. Such a domain, R, is necessarily nonatomic, but $\rho(R) = 1$.

More generally in [10] it is shown that any atomic monoid can be realized as the "atomic part" of an integral domain (again, usually non-atomic). Hence, one can construct nonatomic domains that display any prescribed elasticity.

We remark that if R is an HFD, the *length* of a nonzero nonunit $r \in R$, denoted $\ell(r)$, is the unique length of any factorization of r into irreducible elements of R.

The main purpose of this dissertation is to investigate the extent of the relationship between $\rho(R)$ and $\rho(R[x])$. More specifically, we will concentrate on the atomic case and the problem of determining necessary and sufficient conditions for $\rho(R[x])$ to be 1, that is, for $R[x]$ to be an HFD. A detailed discussion of the problem will not be given until the next section. For now, we merely point out that since any factorization of a constant in $R[x]$ must be a factorization in R, it is always the case that $\rho(R[x]) \geq \rho(R)$.

It is sometimes very difficult to compute the elasticity of a domain. In this introductory section, our purpose will be to illustrate the problem and help the reader become comfortable with the concept of elasticity. To do so, let us consider a sequence of integral domains

$$R = R_0 \subseteq R_1 \subseteq R_2 \subseteq \cdots \subseteq K$$

and ask what is the relationship between $\rho(R_0 + R_1x + R_2x^2 + \cdots)$ and the collection of data $\rho(R_i)$? Some special cases of this general construction worth noting are the polynomial ring ($R_i = R$ for all $i \geq 0$), the construction $R + xK[x]$ ($R_0 = R$ and

$R_i = K$ for all $i \geq 1$), and $R + Rx + x^2K[x]$ ($R_0 = R_1 = R$ and $R_i = K$ for all $i \geq 2$).

Definition 1.1. We say that the integral domain, R, is an *AP-domain* if every irreducible (atom) in R is prime.

Lemma 1.1. *Let R be an AP-domain with at least one irreducible element, then $\rho(R) = 1$.*

Proof. Of course, if R is an AP-domain vacuously (that is, in the case that R has no atoms), then $\rho(R)$ is undefined. Suppose, on the other hand, that $\mathrm{Irr}(R)$ is nonempty. Since all atoms in an AP-domain, are prime, any irreducible factorization is a prime factorization and therefore is unique. Hence $\rho(x) = 1$ for all $x \in \mathrm{A}(R)$ and so $\rho(R) = 1$. $\square$

Lemma 1.2. *Let R be a domain, $p \in R$ be a nonzero prime element, and $a \in A(R)$. Then $\rho(a) \geq \rho(ap)$.*

Proof. Suppose we have the following irreducible factorization of ap:

$$ap = \xi_1\xi_2 \cdots \xi_n,$$

where each $\xi_i \in \mathrm{Irr}(R)$ for all $1 \leq i \leq n$. Since $p \in R$ is prime, p must be associated with one of the ξ_i; we will say, without loss of generality, that $\xi_n = up$ for some $u \in U(R)$. Since R is an integral domain, we cancel the factor of p to obtain

$$a = \xi_1\xi_2 \cdots \xi_{n-1}u.$$

The upshot is that an arbitrary irreducible factorization of ap is (up to associates) p times an irreducible factorization of a. Hence there is a factorization of ap of length $m + 1$, if and only if there is a corresponding factorization of a of length m. Since

$m \geq k \geq 1$ implies that $\frac{m}{k} \geq \frac{m+1}{k+1}$, we have that $\rho(a) \geq \rho(ap)$. $\square$

Remark 1.1. To tie up a loose end, we note that the inequality in the previous result can be strict. For example, in the ring $\mathbb{Z}[\sqrt{-14}]$ the element 81 has precisely two irreducible factorizations (up to associates and reordering):

$$81 = (3)(3)(3)(3) = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14}).$$

So $\rho(81) = 2$. Now consider the element 81 as an element of $\mathbb{Z}[\sqrt{-14}][x]$. As before 81 has only two irreducible factorizations (the ones mentioned previously) and x is a prime element. An easy check shows that $\rho(81x) = \frac{5}{3} < 2$.

We now present the following theorem.

Theorem 1.2. *Let R be an integral domain with quotient field K. If R contains at least one atom, then $\rho(R) = \rho(R + xK[x])$. If R has no atoms (that is, R is an antimatter domain) then $\rho(R)$ is undefined and $\rho(R + xK[x]) = 1$.*

Proof. Let $g(x)$ be a nonconstant polynomial in $R + xK[x]$. We claim that if $g(x)$ is irreducible, then $g(x)$ is (up to associates) either x or of the form $1 + xf(x)$ where $1 + xf(x) \in \mathrm{Irr}(K[x])$. To see this, note that if $g(x)$ is nonconstant, then $g(x) = r + xk(x)$ with $k(x) \in K[x] \setminus \{0\}$. If $r = 0$ then the stipulation that $g(x)$ is irreducible forces the condition $k(x) \in U(R)$. On the other hand, if $r \neq 0$, then the factorization $g(x) = r(1 + \frac{1}{r}xk(x))$ shows that if $g(x)$ is irreducible, then $r \in U(R)$ and $1 + \frac{1}{r}xk(x) \in \mathrm{Irr}(K[x])$. This establishes the claim.

We also note that the elements x and $1 + xf(x) \in \mathrm{Irr}(K[x])$ are, in fact, prime elements of $R + xK[x]$. The fact that x is prime is straightforward. For an irreducible of the form $1 + xf(x)$, note that if $1 + xf(x)$ divides the product $h(x)k(x)$ (with $h(x), k(x) \in R + xK[x]$) then without loss of generality, $1 + xf(x)$ divides $h(x)$ in

$K[x]$. We say that $h(x) = (1 + xf(x))q(x)$, and comparing constant terms, we see that $q(x) \in R + xK[x]$. Hence x and irreducibles of the form $1 + xf(x)$ are prime in $R + xK[x]$.

From the previous observations, we see that if R is an antimatter domain, then $R+xK[x]$ is an AP-domain (with $\mathrm{Irr}(R+xK[x])$ nonempty) and hence $\rho(R+xK[x]) = 1$ by Lemma 1.1.

Now suppose that R has at least one irreducible element. Since any element of R, factored as an element of $R[x]$, has only factors from R (and any irreducible in R remains irreducible in $R[x]$), we have that $\rho(R + xK[x]) \geq \rho(R)$. On the other hand, let $f(x) \in \mathrm{A}(R + xK[x])$. We factor $f(x)$ into irreducibles as follows:

$$f(x) = \pi_1\pi_2 \cdots \pi_m g_1(x)g_2(x) \cdots g_k(x)$$

with $\pi_i \in \mathrm{Irr}(R)$ and $g_i(x) \in \mathrm{Irr}(R + xK[x])$ of degree at least 1. By our previous remarks, each $g_i(x)$ is prime. Hence by Lemma 1.2, $\rho(f(x)) \leq \rho(\pi_1\pi_2 \cdots \pi_m)$. Hence $\rho(R + xK[x]) \leq \rho(R)$ and so, we have equality. □

In stark contrast, the next result shows that a minor tweaking of the previous construction can yield a domain with infinite elasticity. This also gives a strong indication of the level of difficulty of determining the elasticity of $R_0+R_1x+R_2x^2+\cdots$ in terms of the elasticities $\rho(R_i)$.

Proposition 1.1. *Let R be a domain that contains at least one atom, then*

$$\rho(R + Rx + x^2K[x]) = \infty.$$

Proof. Let $\pi \in \mathrm{Irr}(R)$. For all $n \in \mathbb{N}_0$ the polynomial $(\pi^n \pm x) \in \mathrm{Irr}(R+Rx+x^2K[x])$. The irreducible factorizations

$$(\pi^n + x)(\pi^n - x) = \pi^{2n}(1 - \frac{1}{\pi^{2n}}x^2)$$

have lengths 2 and $2n+1$ respectively. Hence we see that $\rho(R+Rx+x^2K[x]) = \infty$. $\square$

Next, we begin to discuss the case of the polynomial ring $R[x]$.

1.3. Polynomial Rings

As indicated earlier, our main problem is to determine when the polynomial ring $R[x]$ is an HFD. The problem is a special case of the more general problem of computing the elasticity $\rho(R[x])$. In comparing the elasticities $\rho(R)$ and $\rho(R[x])$, there are two dynamics to consider. The first is the factorization of constants (which is reflected in $\rho(R)$) and the different factorizations that may result from the polynomial structure. To illustrate we consider the following examples.

Example 1.1. It is well-known (see for example [7]) that $\mathbb{Z}[\sqrt{-3}]$ is a half-factorial domain (and hence has elasticity 1). The domain $\mathbb{Z}[\sqrt{-3}][x]$ is not an HFD. The irreducible factorizations

$$(2x + (1 + \sqrt{-3}))(2x + (1 - \sqrt{-3})) = (2)(2)(x^2 + x + 1)$$

demonstrates that the elasticity of the polynomial extension exceeds 1.

A close look at the mechanics of the previous example reveals that the failure of the domain $\mathbb{Z}[\sqrt{-3}]$ to be integrally closed allowed the creation of this "bad factorization." In the proof of the main theorem in [8] it is shown that if R is not integrally closed, a similar effect occurs.

It is known (see [18]) that if R is a Krull domain, then $R[x]$ is an HFD if and only if $|Cl(R)| \leq 2$. It is also known from [4] that if R is a ring of algebraic integers (and hence, certainly a Krull domain), then R is an HFD if and only if $|Cl(R)| \leq 2$.

Hence if R is a ring of algebraic integers with $|Cl(R)| \leq 2$, then R is an HFD and so is $R[x]$. In this case $\rho(R) = \rho(R[x])$, but the equality can be delicate as we will demonstrate in the following example. The following example should be contrasted with the previous as this one is integrally closed.

Example 1.2. The integral domain $R := \mathbb{Z}[\sqrt{-5}]$ is a ring of integers of class number precisely 2 (see, for example, the tables in [6]) and hence is an HFD that does not have unique factorization. But although $\rho(R[x]) = 1$, the factorizations can be exotic. The elements $2x^2 + 2x + 3$, 2, $2x + 1 + \sqrt{-5}$, and $2x + 1 - \sqrt{-5}$ are all elements of $\text{Irr}(R[x])$. Consider the factorizations

$$(2)(2x^2 + 2x + 3) = (2x + 1 + \sqrt{-5})(2x + 1 - \sqrt{-5}).$$

The upshot is that even in this relatively "nice" domain, the factorizations of elements can depend on how the polynomials break down (with respect to degree) in a nontrivial way.

It is well-known that if R is a UFD with quotient field K, then any irreducible polynomial over $R[x]$ remains irreducible over $K[x]$. More generally, domains, R, for which every irreducible polynomial of degree at least one remains irreducible in $K[x]$ would seem to be the basic case to solve. For these domains, it would seem likely that there is a more direct correlation between $\rho(R)$ and $\rho(R[x])$, since there must be a one to one correspondence between irreducible factors of degree at least 1 for any two irreducible factorizations of the same element. Certainly, bad factorizations of the ilk of the previous two examples would be precluded.

Although it may seem reasonable to consider domains where irreducibles of degree at least one in $R[x]$ remain irreducible in $K[x]$, it is not obvious that in this case $\rho(R) = \rho(R[x])$. To illustrate the problem, consider the irreducible factorizations

$$\pi_1\pi_2\cdots\pi_k f_1(x)f_2(x)\cdots f_m(x) = \xi_1\xi_2\cdots\xi_t g_1(x)g_2(x)\cdots g_n(x)$$

with each $\pi_i, \xi_j \in \mathrm{Irr}(R)$ and $f_i(x), g_j(x)$ all irreducible of degree at least one.

Even if we have that $m = n$ and each $f_i(x)$ and $g_j(x)$ pair off (up to units in K), there is no guarantee that the ratio of k and t are within the elasticity bounds of R (precisely because there is ambiguity up to units in K).

That being said, we present the following theorem. The next chapter will be devoted to establishing this result.

Theorem 1.3. *Let R be a domain such that every irreducible of $R[x]$ of degree greater than or equal to 1 is irreducible in $K[x]$. Then if $\rho(R)$ is defined, then $\rho(R) = \rho(R[x])$.*

As noted before, these conditions are not necessary as Example 1.2 shows.

2. GAUSS' LEMMA

2.1. Polynomial Extensions of UFDs

In this section we give a presentation of the well-known result that if R is a UFD, then $R[x]$ is a UFD. Although our proof is essentially the same as the ones found in textbooks, we think it is more streamlined for our purpose, which is to establish Theorem 1.3. It assumes Gauss' Lemma, which states that if R is a UFD, then the product of two primitive polynomials is primitive. Later, we will generalize this result and see how it can be used in the problem of determining when the HFD property is preserved in polynomial extensions.

Recall that a nonzero constant polynomial $f \in R[x]$ is simply a polynomial of degree zero, i.e., an element of the coefficient ring R. Also, note that if $f \in K[x]$, say $f(x) = \frac{c_0}{d_0} + \frac{c_1}{d_1}x + \cdots + \frac{c_n}{d_n}x^n$, and if d serves as a common multiple of the denominators (e.g., $d = d_0 d_1 \cdots d_n$), then $df \in R[x]$.

Lemma 2.1. *Let R be a UFD with quotient field K. If $f \in R[x]$ is a nonconstant irreducible polynomial, then f is irreducible in $K[x]$.*

Proof. Assume f is not irreducible in $K[x]$. Then there exist nonconstant polynomials $g, h \in K[x]$ such that $f = gh$. We choose $b, d \in R$ such that $bg, dh \in R[x]$ and upon multiplying both sides by bd we obtain the following equation in $R[x]$.

$$bdf = (bg)(dh)$$

Let u, v be the greatest common divisors of the coefficients of bg and dh, respectively, so that $bg = ug'$ and $dh = vh'$, where g', h' are primitive polynomials over R. Dividing both sides the above equation by uv yields the equation

$$\frac{bd}{uv}f = g'h'$$

Since f is irreducible over R, the greatest common divisor of its coefficients is 1; hence, as R is a UFD, it follows that the greatest common divisor of the coefficients of bdf is bd. Noting that uv divides the coefficients of bdf, we then conclude that $uv \mid bd$, so that $\frac{bd}{uv} \in R$. Since f', g' are primitive, Gauss' Lemma implies that $\frac{bd}{uv}$ is a unit in R. This contradicts the hypothesis that f is irreducible in $R[x]$. □

Theorem 2.1. *If R is a UFD, then $R[x]$ is a UFD.*

Proof. Assume $a_1 \cdots a_n f_1 \cdots f_k = b_1 \cdots b_m g_1 \cdots g_j$, where the f's and g's are nonconstant irreducibles of $R[x]$ and the a's and b's are constant irreducibles of $R[x]$. We must show that $m + j = n + k$ and verify uniqueness. By the lemma, the f's and g's are irreducible (hence prime) elements of $K[x]$. As $K[x]$ is a UFD, it follows that $k = j$, and after a renumbering we can assume f_i is an associate of g_i in $K[x]$, $i = 1, \ldots, k$. So $f_i = \frac{r_i}{s_i} g_i$ with $r_i, s_i \in R$, that is, $s_i f_i = r_i g_i$. Equating the greatest common divisors of the coefficients, we obtain $r_i = u_i s_i$ for some unit $u_i \in R$, or $f_i = u_i g_i$. Cancelling the f's and g's, we obtain $a_1 \cdots a_n = u b_1 \cdots b_m$ where u is a unit. Now R is a UFD by hypothesis, so $m = n$; hence, $n + k = m + j$ and $a_i = v_i b_i$, where v_i is a unit. It follows that $R[x]$ is a UFD. □

2.2. Irreducibles of $R[x]$ Versus Irreducibles of $K[x]$

The proof that unique factorization is preserved in polynomial extensions, as outlined in the previous section, boiled down to establishing the following property of a UFD R:

(P) Every nonconstant irreducible polynomial $f \in R[x]$ is irreducible in $K[x]$

Gauss's Lemma was the key which allowed the proof to go through in this case. Our goal in this section is to determine the general class of domains R which satisfy property (P).

Conditions under which the product of two primitive polynomials remains primitive has been studied in more general domains (see for instance, [17] and [2]). It turns out that the domains satisfying property (P) must satisfy a condition somewhat stronger than Gauss's Lemma; they must satisfy what is called the *PSP-property* (see [2, Proposition 1.2]).

Definition 2.1. A domain R has the *PSP-property* if whenever $a_0 + a_1x + \cdots + a_nx^n$ is a primitive polynomial over R and $z \in (a_0, a_1, \ldots, a_n)^{-1}$, then $z \in R$.

In other words, a domain has the PSP-property if every primitive polynomial is superprimitive (see Section 1.1). For integral domains, the following implications are well-known

$$\text{UFD} \Longrightarrow \text{GCD-domain} \Longrightarrow \text{PSP-property} \Longrightarrow \text{GL-property} \Longrightarrow \text{AP-property}.$$

and in [1] it is shown that all of these types are equivalent for atomic domains.

Arnold and Sheldon [2, Example 2.5] gave an example of a domain satisfying Gauss's Lemma (such domains are said to have the *GL-property*), but failing to have the PSP-property. The domain they considered was the domain

$$F[\{x^\alpha : \alpha \geqslant 0\}, \{y^\alpha : \alpha \geqslant 0\}, \{z^\alpha x^\beta : \alpha, \beta > 0\}, \{z^\alpha y^\beta : \alpha, \beta > 0\}]$$

Here, all exponents α and β are understood to be taken from the field $\mathbb{Q}$ of rational numbers. This is an example of a monoid domain, and can intuitively be thought of as the ring of all formal polynomials in the given "indeterminates" with coefficients in F, a field with two elements. We note that $yt + x$ is a primitive polynomial in t that fails to be superprimitive, as $z \in (x, y)^{-1}$. This leads us to the following result.

Proposition 2.1. *Assume every nonconstant irreducible $f \in R[x]$ is irreducible in $K[x]$. Then R is integrally closed and has the PSP-property.*

Proof. Assume R is not integrally closed. Choose an element $\omega \in K$ that satisfies a monic irreducible polynomial $f \in R[x]$ of degree ≥ 2. Since ω is a root of f, the division algorithm in $K[x]$ implies that $f = (x - \omega)g$, where g is a polynomial in $K[x]$ of degree ≥ 1. Hence f is irreducible over R but reducible over K. This is a contradiction.

Next, we assume R does not have the PSP-property. Let $y_0 + y_1x + \cdots + y_nx^n$ be a primitive polynomial and let $z \in K$ be such that $z \in (y_0, y_1, \ldots, y_n)^{-1}$ but $z \notin R$. In the collection of all primitive polynomials that are not superprimitive, we assume that $I := y_0 + y_1x + \cdots + y_nx^n$ is one of minimal degree. In $K[x]$ we have the factorization

$$y_nx^{n+1}+(y_{n-1}+zy_n)x^n+\cdots+(y_0+zy_1)x+zy_0 = (x+z)(y_nx^n+y_{n-1}x^{n-1}+\cdots+y_1x+y_0)$$

where the polynomial f on the left side belongs to $R[x]$. We claim that f is irreducible over R. If $f = gh$ for some $g, h \in R[x]$ then $x + z$ divides g or h in $K[x]$, say $g = (x + z)p(x)$. Since R is integrally closed, $p(x) \in R[x]$ (see [12, Theorem 10.4]), say $p(x) = a_kx^k+a_{k-1}x^{k-1}+\cdots+a_1x+a_0$. Then $g(x) = a_kx^{k+1}+(a_{k-1}+za_k)x^k+\cdots+(a_0+za_1)x+za_0$, so that $za_0, za_1, \ldots, za_k \in R$, and hence $p(x)$ is not superprimitive. But $p(x)$ is a factor of the primitive polynomial I. Hence $p(x)$ is primitive, so that the minimality assumption on I implies that $k = n$. It follows that h is a unit so that f is irreducible over R, but not over K, the desired contradiction. $\square$

Thus in our search for the domains satisfying property (P), we may restrict our attention to integrally closed domains having the PSP-property.

To show that a particular domain has property (P), one possible strategy is the following: Suppose $f \in R[x]$ is a nonconstant polynomial that is irreducible over R, but fails to be irreducible over the field of fractions K, say $f = gh$ in $K[x]$. Now "clear the denominators," that is, choose nonzero $b, d \in R$ such that $bdf = (bg)(dh)$ and $bg, dh \in R[x]$. At this point, we might try to find some way to cancel out b and d to get a contradiction, namely, that $f = g'h'$ for some $g', h' \in R[x]$. It turns out that if R has the PSP-property, then we can assert, after clearing denominators, that the greatest common divisor of the coefficients of bdf exists and is equal to bd, as shown by the following.

Proposition 2.2. *Let R be a domain. The following are equivalent.*

a) *R has the PSP-property.*

b) *Whenever the elements $a_1, a_2, \ldots, a_n \in R$ have a greatest common divisor and $0 \neq b \in R$, then $[ba_1, ba_2, \ldots, ba_n] = b[a_1, a_2, \ldots, a_n]$.*

Proof. Assume R has the PSP-property and $[a_1, a_2, \ldots, a_n] = g$. Given $b \in R$, it is clear that bg is a common divisor of $ba_1, ba_2, \ldots, ba_n$. If x is some other common divisor, then $\frac{bg}{x} \in (\frac{a_1}{g}, \frac{a_2}{g}, \ldots, \frac{a_n}{g})^{-1}$. This implies $\frac{bg}{x} \in R$ since R is PSP. In other words, $x|bg$ so that $[ba_1, ba_2, \ldots, ba_n] = bg$.

Conversely, assume b) holds and $\frac{r}{s} \in (a_1, a_2, \ldots, a_n)^{-1}$, where $a_0+a_1x+\cdots+a_nx^n$ is some primitive polynomial over R. Then $s|ra_i$ for all i, so b) implies that $s|r$. Thus $\frac{r}{s} \in R$, so that R is PSP. $\square$

Proposition 2.3. *Let R be an integrally closed PSP-domain. The following are equivalent.*

a) *Every nonconstant irreducible polynomial $f \in R[x]$ is irreducible in $K[x]$*

b) *Whenever $f = gh$ in $R[x]$ and the greatest common divisor of the coefficients of f exists, then the greatest common divisor of the coefficients of g exists*

Proof. b) $\implies$ a). Assume b) holds. Let $f \in R[x]$ be a nonconstant irreducible polynomial (hence the greatest common divisor of the coefficients is 1). Suppose $f = gh$, where $g, h \in K[x]$ have degrees $\geqslant 1$. Choose nonzero $b, d \in R$ such that $bg, dh \in R[x]$. Then we have the equation $bdf = (bg)(dh)$ in $R[x]$, and since R is PSP, Proposition 2.2 implies that the greatest common divisor of the coefficients of bdf exists and is equal to bd. Hence the greatest common divisor of the coefficients of bg exists, say u, and the greatest common divisor of the coefficients of dh exists, say v. Note that uv divides the coefficients of bdf. Hence $\frac{bd}{uv}f = g_1h_1$, where g_1, h_1 are primitive. Since R has the GL-property, $\frac{bd}{uv}f$ is primitive, so $\frac{bd}{uv}$ is a unit. But then f is reducible over R, a contradiction.

a) $\implies$ b). Assume a) holds. Suppose $f = gh$ in $R[x]$ and the greatest common divisor of the coefficients of f exists, say s. We can assume $\deg f \geqslant 1$. Then $f = sf'$, where f' is primitive. Since f' is primitive, f' is a product of irreducibles, say $f' = f_1f_2\cdots f_k$. By unique factorization in $K[x]$, $g = uf_1f_2\cdots f_r$ for some $r \leqslant k$ (without loss of generality) and some $u \in K$. Since R is PSP, $u \in R$ and the greatest common divisor of the coefficients of g equals u. □

In the paper [2], Arnold and Sheldon proved the following theorem.

Theorem 2.2. *Let R be a domain with quotient field K. The following are equivalent.*

1) *$R[x]$ is an AP-Domain*

2) *$R[x]$ is a GL-Domain*

3) *Each of the following holds:*

   (α) *R has the PSP-property*

   (β) *R is integrally closed, and*

   (γ) *Whenever B, C are finitely generated fractional ideals of R such that $(BC)_v = R$, then B_v is principal*

Condition (γ) clearly has a resemblance to condition *b*) of the proposition we just proved. In fact, we have the following theorem.

Proposition 2.4. *Let R be an integrally closed PSP-domain. The following are equivalent.*

a) *Every nonconstant irreducible polynomial $f \in R[x]$ is irreducible in $K[x]$*

b) *Whenever $f = gh$ in $R[x]$ and the greatest common divisor of the coefficients of f exists, then the greatest common divisor of the coefficients of g exists*

c) *Whenever B, C are finitely generated fractional ideals of R such that $(BC)_v = R$, then B_v is principal*

Proof. We already proved the equivalence of a) and b).

b) $\Longrightarrow$ c). Suppose $(BC)_v = R$. Let g be a polynomial whose coefficients are the generators of B (if generators of B are chosen in order $B = (b_0, b_1, \ldots, b_n)$ we will define, $g = b_0 + b_1x + \cdots + b_nx^n$) and let h be defined similarly with respect to chosen generators of C. Choose nonzero $b, c \in R$ such that $bg, ch \in R[x]$. Since R is integrally closed, $(A_{gh})_v = (A_gA_h)_v$ [12, Proposition 34.8], so that $(A_{gh})_v = R$. Since

$(bcA_{gh})_v = bc((A_{gh})_v)$ [12, Proposition 32.1(1)], we therefore have $(bcA_{gh})_v = bcR$. This implies that the greatest common divisor of the coefficients of $bcgh$ equals bc. Since $bcgh = (bg)(ch)$, it follows by assumption that the greatest common divisor of the coefficients of bg exists, so that $(A_{bg})_v = (bB)_v$ is principal [1, Theorem 3.3]. Hence B_v is principal.

c) $\Longrightarrow$ b). Suppose $f = gh$ in $R[x]$ and the greatest common divisor of the coefficients of f exists, say s. Let $f_1 = \frac{f}{s}$ and $h_1 = \frac{h}{s}$. Then $(A_g A_{h_1})_v = (A_{gh_1})_v = (A_{f_1})_v$, so $(A_g A_{h_1})_v = R$. Hence $(A_g)_v$ is principal. Hence the greatest common divisor of the coefficients of g exists. $\square$

Putting together the results of this section we obtain our main result, which is the following.

Theorem 2.3. *Let R be a domain with quotient field K. The following are equivalent.*

1) *Every nonconstant irreducible polynomial $f \in R[x]$ is irreducible in $K[x]$*

2) *$R[x]$ is an AP-Domain*

3) *$R[x]$ is a GL-Domain*

4) *Each of the following holds:*

   (α) *R has the PSP-property*

   (β) *R is integrally closed, and*

   (γ) *Whenever B, C are finitely generated fractional ideals of R such that $(BC)_v = R$, then B_v is principal*

We close this section with a few observations. First, it is a note that if $R[x]$ is atomic, then $R[x]$ is an AP-domain if and only if R is a UFD. Also we note that our main theorem of the previous section has its resolution in this stronger result. Indeed, if we have the hypothesis of Theorem 1.3, then $R[x]$ is an AP-domain. Hence R is an AP-domain. If R has at least one atom then $\rho(R) = \rho(R[x]) = 1$.

Finally, if R is a Prüfer domain satisfying property (P) then since every finitely generated ideal is invertible we must have B_v principal for each B. Hence R is a GCD-domain. And if $[a_0, \ldots, a_n] = 1$, then $(a_0, \ldots, a_n)^{-1} = R$. Hence there exist $r_0, \ldots, r_n \in R$ such that $r_0a_0 + \cdots + r_na_n = 1$. We conclude that the greatest common divisor of a finite set of elements is a linear combination of that set, and so R is a Bézout domain. Thus we obtain [12, Theorem 28.8], which says (paraphrasing) that a Prüfer domain R has property (P) if and only if R is Bézout.

3. A NEW PROOF OF THE RESULT ON POLYNOMIAL HFDS

A result due to Zaks gave a characterization of polynomial HFDs in the case where the coefficient ring R is a Krull domain [18, Theorem 2.4]. We introduce some concepts which, in Section 3.2, will allow us to give a new proof of this result using Gauss's ideas. We end the chapter with some illustrative examples.

3.1. The Z-property

Recall that if $a, b \in R$, the symbol $[a, b]$ denotes the greatest common divisor, if it exists. We shall often write $[a, b] \neq 1$ for the negation of the statement $[a, b] = 1$.

Definition 3.1. We say that a domain R has the *Z-property* if given nonunits $a, b, c, d, e \in R$ such that $abc = de$, then $[ab, e] \neq 1$ or $[ab, d] \neq 1$.

Proposition 3.1. *If $R[x]$ is an HFD, then R has the Z-property.*

Proof. Assume $abc = de$ and $[ab, e] = 1$. Let $f = abx + e$ and $g = abx + d$. The product of these two polynomials can be written

$$fg = abh$$

where $h = abx^2 + (d + e)x + c$. Note that f is irreducible and since a, b are nonunits and $R[x]$ is an HFD, this equation implies that the polynomial g is not irreducible, i.e., $[ab, d] \neq 1$. □

If R is an HFD and a is a nonzero nonunit, recall that $\ell(a)$ denotes the length of any factorization of a into irreducibles (atoms).

Proposition 3.2. *Let R be atomic. If R has the Z-property, then R is an HFD.*

Proof. Assume

$$\alpha_1\alpha_2\cdots\alpha_n = \beta_1\beta_2\cdots\beta_m \tag{1}$$

where the α's and β's are irreducible elements of R. We assume $n > m$ and derive a contradiction. Consider first the case $m = 2$. Then $n \geqslant 3$; hence the Z-property implies that $[\alpha_1\alpha_2, \beta_1] \neq 1$ or $[\alpha_1\alpha_2, \beta_2] \neq 1$. Since each β is irreducible we may assume without loss of generality that

$$\alpha_1\alpha_2 = \beta_1 x \tag{2}$$

for some $x \in R$. Using (2) in (1) we get

$$x\alpha_3\cdots\alpha_n = \beta_2$$

so x is a unit, contrary to equation (2). Done with the case $m = 2$, we now proceed by induction, that is, we assume that any two factorizations of an element have the same length if the one with the shortest length has length $\leqslant m - 1$, and we consider an equation (1) with $n > m$. Then either (i) $[\alpha_1\alpha_2, \beta_m] \neq 1$ or (ii) $[\alpha_1\alpha_2, \beta_1\beta_2\cdots\beta_{m-1}] \neq 1$. In case (i) we have

$$\alpha_1\alpha_2 = \beta_m x$$

for some x, so the induction assumption implies that $\ell(x) = 1$. Equation (1) becomes

$$x\alpha_3\cdots\alpha_n = \beta_1\cdots\beta_{m-1} \tag{3}$$

and the induction assumption applied to (3) yields $m - 1 = n - 1$, i.e., $m = n$. Case (ii) implies $\alpha_1\alpha_2 = \xi x$ and $\beta_1\cdots\beta_{m-1} = \xi y$ for some nonunit $\xi \in R$ so $\ell(x) = 1$ and $\ell(y) = m-2$. The original equation (1) becomes $x\alpha_3\cdots\alpha_n = y\beta_m$, so $\ell(y)+1 = n-1$, i.e., $m = n$. $\square$

Definition 3.2. [16, Proposition 1.1] If $a_0, a_1, \ldots, a_n \in R$, a common divisor g of $a_0, a_1, \ldots, a_n$ is called a *maximal common divisor* (MCD) if $[\frac{a_0}{g}, \frac{a_1}{g}, \ldots, \frac{a_n}{g}] = 1$.

If R is an HFD, then it is easy to see that any finite collection of elements of R has an MCD. In particular, for any fraction $\frac{r}{s} \in K$, if we cancel enough common factors of r and s we will obtain a reduced fraction, i.e we can find $u, v \in R$ such that $r = bu$, $s = bv$, $\frac{r}{s} = \frac{u}{v}$, and $[u, v] = 1$.

Proposition 3.3. *Let R be atomic. The following are equivalent.*

a) *R has the Z-property*

b) *If $I = (a_0, a_1)$ is a two-generated primitive ideal of R and $\frac{r}{s} \in I^{-1}$, where $r, s \in R$, then there exists a common divisor g of r and s such that $\ell(\frac{s}{g}) \leqslant 1$.*

We remark that even in the case where R is not an HFD and the length $\ell(r)$ is not uniquely defined, the statement that $\ell(r) \leqslant 1$ in this proposition is understood to be equivalent to the statement that r is a unit or an irreducible element of R. In particular, we shall occasionally write $\ell(r) = 0$ to indicate that r is a unit. Also, if $\frac{r}{s} \in I^{-1}$, as in part b) of this proposition, and we reduce the fraction to get $r = bu$, $s = bv$, $[u, v] = 1$, then $\ell(v) \leqslant 1$ would be a sufficient condition for the conclusion of b) to be satisfied (with $g = b$). We are now ready for the proof of Proposition 3.3.

Proof. a) $\Rightarrow$ b) Assume $\frac{r}{s} \in I^{-1}$ and put

$$\frac{r}{s}a_0 = b_0 \;\text{ and }\; \frac{r}{s}a_1 = b_1 \tag{4}$$

Assume $\frac{r}{s}$ has already been reduced, so that $[r, s] = 1$ (we can always reduce, as long as R is an HFD). Then it is enough to show that $\ell(s) \leqslant 1$. Suppose on the contrary that $\ell(s) \geqslant 2$. We consider first the case where a_0 and b_0 are relatively prime. In this case, we combine the two equations in (4) to get

$$a_0 b_1 = a_1 b_0 \tag{5}$$

If b_0 is a unit, then $\frac{r}{s} = \frac{b_0}{a_0} \in I^{-1}$, contrary to the fact that I is primitive. If $\ell(a_0) \geqslant 2$, then (5) and the Z-property implies $[a_0, a_1] \neq 1$, a contradiction. Hence $\ell(a_0) = 1$. But (4) implies

$$sb_0 = ra_0 \tag{6}$$

and since $[s, r] = 1$, the Z-property implies $a_0 \mid s$, say $s = a_0 t$. Using this in (6) we obtain $r = tb_0$, so $t \mid r$ and $t \mid s$, a contradiction, since $\frac{r}{s}$ is reduced.

The other case, where a_0 and b_0 are not relatively prime, can be reduced to the first. Let g be an MCD of a_0 and b_0, so that $a_0 = ga_0'$, $b_0 = gb_0'$. Cancelling g from a_0 and b_0 in (4) we obtain $\frac{r}{s}a_0' = b_0'$, $\frac{r}{s}a_1 = b_1$, where a_0' and b_0' are relatively prime.

b) $\Rightarrow$ a) Assume $abc = de$ (all nonunits) and $[ab, e] = 1$. Then $\frac{d}{ab} \in (e, ab)^{-1}$, so by b) there exists a common divisor g of ab and d such that $\ell(\frac{ab}{g}) \leqslant 1$. In particular, since a and b are nonunits, we have $\ell(g) \geqslant 1$, so $[ab, d] \neq 1$. □

Proposition 3.4. *Assume R is an atomic domain with the Z-property. Then each of the following hold.*

(a) *If $a_0, a_1 \in R$, then all MCDs of a_0 and a_1 have the same length*

(b) *Every linear polynomial $f = a_0 + a_1 x$ in $R[x]$ has elasticity one*

Proof. (a) If g, d are both MCDs of a_0, a_1, then $(a_0, a_1) = gI = dJ$, for some primitive ideals $I = (b_0, b_1)$ and $J = (c_0, c_1)$. Then $\frac{g}{d} \in I^{-1}$, so by Proposition 3.3 we have $\frac{g}{d} = \frac{r}{\xi}$ for some atom ξ. Similarly the reciprocal $\frac{d}{g} = \frac{s}{\pi}$ for some atom π. Thus $\frac{r}{\xi} = \frac{\pi}{s}$ and since R is an HFD, we have $\ell(r) = 1 = \ell(s)$. It follows that $\ell(g) = \ell(d)$.

(b) Let $f = a_0 + a_1 x$ be linear. Every factorization of f into irreducibles has the form $g(b_0 + b_1 x)$, where g is a MCD of a_0 and a_1, i.e., every factorization must include a linear primitive polynomial. Thus all factorization of f have the same length if and only if all MCDs of a_0 and a_1 have the same length. So (b) follows from (a). □

The following theorem will reappear several times in this paper. The theorem was used to characterize the Noetherian domains R whose polynomial extensions are HFDs. For more details, refer to the paper [8].

Theorem 3.1. [8] *If $R[x]$ is an HFD, then R is integrally closed.*

Because of this result and Proposition 3.1, we shall mostly be concerned with integrally closed domains having the Z-property. With that in mind, we give the following characterization of the Z-property for integrally closed domains.

Proposition 3.5. *Assume R is atomic and integrally closed. The following statements are equivalent.*

a) *R has the Z-property*

b) *any constant factor of a product of two linear primitive polynomials has length at most one.*

c) *if $[a, b] = [a, c] = 1$, any common factor of a and bc has length at most one.*

Before giving the proof, we remark that condition c) is analogous to the so-called PP-property used in Theorem 3.1 of the paper [1] to characterize the domains with the GL-property.

Proof. a) $\Rightarrow$ b) Assume by way of contradiction that $(ux + v)(rx + s) = af$, where $(ux + v), (rx + s)$ are primitive polynomials in $R[x]$ and $\ell(a) \geqslant 2$. Since f is a product of linear polynomials in $K[x]$, we can certainly find a monic factor and write

$f = (x + z)(cx + d)$, and since R is integrally closed, we have $c, d \in R$ [G, Theorem 10.4]. Write $c = gc'$, $d = gd'$, so that $[c', d'] = 1$. Since $f \in R[x]$, we have $z \in (c, d)^{-1}$, and hence $zg \in (c', d')^{-1}$. Now Proposition 3.3 implies $zg = \frac{t}{\xi}$, where ξ is an atom. Then $\xi f = \xi(x + z)(cx + d) = (\xi gx + \xi zg)(c'x + d') = (\xi gx + t)(c'x + d')$, so the polynomial ξf is a product of linear polynomials over R. Therefore, by factoring out constants from the linear polynomials in the foregoing factorization of ξf, we can find an expression of the form $\xi f = e(u'x + v')(r'x + s')$, where $(u'x + v'), (r'x + s')$ are primitive and $e \in R$. Dividing this expression by ξ we can write

$$\frac{e}{\xi}(u'x + v')(r'x + s') = f = \frac{1}{a}(ux + v)(rx + s) \tag{7}$$

Then unique factorization in $K[x]$ applied to (7) gives (without loss of generality) that

$$(u'x + v') = \frac{\alpha_1}{\beta_1}(ux + v) \text{ and } (r'x + s') = \frac{\alpha_2}{\beta_2}(rx + s) \tag{8}$$

where the α's and β's belong to R. Then Proposition 3.4 gives $\ell(\alpha_i) = \ell(\beta_i)$ for $i = 1, 2$. Using (8) in (7) we obtain the equation

$$\frac{e}{\xi}\beta_1\beta_2 = \frac{1}{a}\alpha_1\alpha_2$$

and since R is an HFD, this implies $\ell(a) + l(e) = \ell(\xi) = 1$, contrary to the fact that $\ell(a) \geqslant 2$.

b) $\Rightarrow$ a) This follows by the proof of Proposition 3.1.

b) $\Rightarrow$ c) Assume $[a, b] = 1 = [a, c]$, but a and bc have a common factor of length $\geqslant 2$. Then it is easy to see that $(ax + b)(ax + c)$ has a constant factor of length $\geqslant 2$.

c) $\Rightarrow$ a) Assume $\alpha_1\alpha_2\alpha_3 = \beta_1\beta_2$ (all nonunits), but both $[\alpha_1\alpha_2, \beta_1] = 1$ and $[\alpha_1\alpha_2, \beta_2] = 1$. Put $a = \alpha_1\alpha_2$, $b = \beta_1$, and $c = \beta_2$. Then $[a, b] = 1 = [a, c]$, but a and bc have a factor of length $\geqslant 2$, since $a \mid bc$. $\square$

3.2. The Proof

In this section, we build on the previous one to give a list of sufficient conditions for a polynomial ring $R[x]$ to be an HFD. Also, we show that the conditions are necessary ones in the case where R is a Krull domain. Combining the results, we obtain a new proof of the following result, due to Zaks.

Theorem 3.2. [18, Theorem 2.4] *If R is a Krull domain, then $R[x]$ is an HFD if and only if $|Cl(R)| \leqslant 2$.*

Moreover, we note that for a Krull domain R, the class groups of R and $R[x]$ are isomorphic [12, Theorem 45.5]; hence the theorem is valid for an arbitrary collection of indeterminates.

We now proceed to give our proof. We start with a lemma.

Lemma 3.1. *Assume R has the property that whenever I is a primitive ideal and $\frac{r}{s} \in I^{-1}$, then there is a common divisor g of r and s such that $\ell(\frac{s}{g}) \leqslant 1$. Then any two MCDs of an arbitrary collection of elements $a_0, a_1, \ldots, a_n \in R$ have the same length.*

Proof. Same proof as in Proposition 3.4 part a). □

Theorem 3.3. *Consider the following conditions on a domain R:*

a) *R is integrally closed*

b) *If $f, g \in R[x]$ and fg is primitive, then f is superprimitive or g is superprimitive*

c) *If f, g are primitive polynomials over R and $a \in R$ is a constant factor of the product fg, then $\ell(a) \leqslant 1$*

d) *If I is a primitive ideal and $\frac{r}{s} \in I^{-1}$, then there is a common divisor g of r and s such that $\ell(\frac{s}{g}) \leqslant 1$.*

If R is an atomic domain satisfying all of the above, then $R[x]$ is an HFD.

Proof. The proof has three steps.

Step 1. We show that if $f \in R[x]$ is a nonconstant irreducible polynomial which is not irreducible in $K[x]$, then there exists $a \in R$ such that $af = bgh$, where (i) $g, h \in R[x]$ are irreducible polynomials such that g is irreducible in $K[x]$, (ii) $b \in R$, and (iii) $\ell(a) = \ell(b) + 1$

For, let g be an irreducible factor of f in $K[x]$. Pick g such that $g \in R[x]$ and g is primitive over R. So $f = gf'$ for some nonconstant $f' \in K[x]$. Choose $a \in R$ such that $af' \in R[x]$, so that $af = g(af')$. Let b be an MCD of the coefficients of af' so that $af' = bh$ for some primitive $h \in R[x]$. Then

$$af = bgh \tag{9}$$

We must show that a, g, and h satisfy the requirements in the statement of Step 1. Note $\frac{a}{b} \in {A_f}^{-1}$, so if it happened that $l(b) \geqslant 2$, then by condition d) we could cancel some factors common to both a and b. Even better, it allows us to assume without loss of generality that $[a, b] = 1$ and $\ell(b) \leqslant 1$. Let c be an MCD of the coefficients of gh, so that $gh = c\phi$ with ϕ a primitive polynomial over R. From (9) we deduce that

$$\frac{bc}{a} \in {A_\phi}^{-1} \tag{10}$$

Note $\ell(c) \leqslant 1$ by condition c) and also that the relation (10) above must obey condition d). It then follows that $\ell(a) \leqslant 2$. If $\ell(b) = 0$ (i.e., b is a unit), then by similar reasoning we deduce that $\ell(a) = 1$, and hence the requirement $\ell(a) = \ell(b) + 1$ is satisfied in this case. Suppose $\ell(b) = 1$. If $\ell(a) = 1$, then (9) implies gh is primitive.

Then condition b) implies, without loss of generality, that h is superprimitive, so that ${A_{gh}}^{-1} = {A_g}^{-1}$. But $\frac{b}{a} \in {A_{gh}}^{-1}$, contrary to the fact that f is irreducible. Hence, in both cases, the requirement $\ell(a) = \ell(b) + 1$ is satisfied. Finally, it must also be shown, in both cases, that the polynomials g, h are irreducible. For the case where $\ell(b) = 0$, if also $h = h'h''$, then h'' is superprimitive without loss of generality, which forces $\frac{1}{a} \in A_{gh'}^{-1}$ and contradicts the fact that f is irreducible. The case $\ell(b) = 1$ is similar.

Step 2. If $f \in R[x]$ is a nonconstant irreducible polynomial which is not irreducible in $K[x]$, then there exists $a \in R$ such that $af = bf_1 f_2 \cdots f_k$, where (i) the f_i are nonconstant irreducible polynomials of $R[x]$ which are irreducible in $K[x]$ $(i = 1, \ldots, k)$, (ii) $b \in R$, and (iii) $\ell(a) + 1 = \ell(b) + k$

Applying Step 1 to f we obtain $a_1 f = b_1 f_1 f'$, where $l(a_1) + 1 = l(b_1) + 2$ and $f_1, f' \in R[x]$ are irreducible polynomials such that f_1 is irreducible in $K[x]$. In particular, both sides of the equation have the same length and so it does not violate the half-factorial property. Continuing the process, if f' is not irreducible in $K[x]$, we apply Step 1 to it and obtain a_2, f_2, f''. This process must eventually end. Since each application of Step 1 does not violate the half-factorial property, we end up at the situation described in Step 2.

Step 3. $R[x]$ is an HFD

To prove this, we shall use a slight modification of the argument in Theorem 2.1, using some of the ideas in Chapter 2, Section 2. To start, we assume that

$$\alpha_1 \cdots \alpha_k f_1 \cdots f_m = \beta_1 \cdots \beta_j g_1 \cdots g_n \tag{11}$$

are two irreducible factorizations, where each α and β is a constant irreducible polynomial of $R[x]$ and each f and g is a nonconstant irreducible of $R[x]$. We must prove that $k + m = j + n$. Applying Step 2 to f_i for each $i = 1, \ldots, m$, we can write $a_i f_i = b_i f_{i1} \cdots f_{il_i}$, where

$$\ell(a_i) + 1 = \ell(b_i) + l_i \tag{12}$$

Likewise, for g_i $(i = 1, \ldots, n)$, we can write $c_i g_i = d_i g_{i1} \cdots g_{ih_i}$, where

$$\ell(c_i) + 1 = \ell(d_i) + h_i \tag{13}$$

Multiplying equation (11) by $\prod_{i=1}^{m} a_i \prod_{i=1}^{n} c_i$ we obtain

$$\alpha_1 \cdots \alpha_k \prod_{i=1}^{n} c_i \prod_{i=1}^{m} b_i \prod_{u=1}^{l_i} f_{iu} = \beta_1 \cdots \beta_j \prod_{i=1}^{m} a_i \prod_{i=1}^{n} d_i \prod_{u=1}^{h_i} g_{iu} \tag{14}$$

The f's and g's in equation (14) are irreducible in $K[x]$, so the number of f's equals the number of g's in this equation, i.e.,

$$\sum_{i=1}^{m} l_i = \sum_{i=1}^{n} h_i \tag{15}$$

Now (14) can be written

$$\alpha_1 \cdots \alpha_k \prod_{i=1}^{n} c_i \prod_{i=1}^{m} b_i \prod_{i=1}^{p} F_i = \beta_1 \cdots \beta_j \prod_{i=1}^{m} a_i \prod_{i=1}^{n} d_i \prod_{i=1}^{p} G_i \tag{16}$$

where $\prod_{i=1}^{p} F_i$ is the product of the f's in some order and $\prod_{i=1}^{p} G_i$ is the product of the g's in some order and where F_i is associated to G_i $(i = 1, \ldots, p)$, that is,

$$F_i = \frac{r_i}{s_i} G_i \tag{17}$$

with $r_i, s_i \in R$. We remark that condition d) and Lemma 3.1 imply that

$$\ell(r_i) = \ell(s_i) \tag{18}$$

for each i. Using the relation (17) in equation (16) we obtain the following equation over R

$$\alpha_1 \cdots \alpha_k \prod_{i=1}^{n} c_i \prod_{i=1}^{m} b_i \prod_{i=1}^{p} r_i = \beta_1 \cdots \beta_j \prod_{i=1}^{m} a_i \prod_{i=1}^{n} d_i \prod_{i=1}^{p} s_i \tag{19}$$

Since R is an HFD,

$$k + \sum_{i=1}^{n} \ell(c_i) + \sum_{i=1}^{m} \ell(b_i) + \sum_{i=1}^{p} \ell(r_i) = j + \sum_{i=1}^{m} \ell(a_i) + \sum_{i=1}^{n} \ell(d_i) + \sum_{i=1}^{p} \ell(s_i)$$

Then (18) and a rearrangement gives

$$k + \sum_{i=1}^{m} [\ell(b_i) - \ell(a_i)] = j + \sum_{i=1}^{n} [\ell(d_i) - \ell(c_i)]$$

By (12) and (13) we obtain

$$k + \sum_{i=1}^{m} [1 - l_i] = j + \sum_{i=1}^{n} [1 - h_i]$$

that is,

$$k + m - \sum_{i=1}^{m} l_i = j + n - \sum_{i=1}^{n} h_i$$

Therefore, by (15) we conclude that

$$k + m = j + n$$

and hence $R[x]$ is an HFD. $\square$

The converse of the previous theorem is false; we will prove this in Section 4.

Theorem 3.4. *The conclusion of Theorem* 3.3 *follows from a), b) and the following condition*

e) *R has the Z-property and for each primitive ideal J in R, we can find relatively prime $a, b \in R$ such that $(a, b)_v \subseteq J_v$*

Proof. It suffices to show that conditions e), a), and b) imply c) and d).

To prove c), if f, g are primitive, then e) implies there are linear polynomials F, G such that $(A_F)_v \subseteq (A_f)_v$ and $(A_G)_v \subseteq (A_g)_v$. For each constant factor a of the product fg we therefore have (by [12, Proposition 34.8]) that $A_{FG} \subseteq (A_{FG})_v = (A_F A_G)_v \subseteq (A_f A_g)_v = (A_{fg})_v \subseteq (a)$, so that a is a factor of the product FG also. Hence $\ell(a) \leqslant 1$ by Proposition 3.5 part b).

For d), if I is a primitive ideal then by assumption, $(a, b)_v \subseteq I_v$ for some two-generated primitive ideal (a, b). Hence $I^{-1} \subseteq (a, b)^{-1}$. Therefore $\omega \in I^{-1}$ implies $\omega \in (a, b)^{-1}$, so that condition d) follows from Proposition 3.3. $\square$

Theorem 3.5. *If R is a Krull domain, then $R[x]$ is an HFD if and only if R satisfies conditions a)–d) of Theorem* 3.3.

Proof. If $R[x]$ is an HFD, then R has the Z-property. Also, the proof of [12, Corollary 44.3] implies that R has property e) in the previous theorem. By Theorem 3.2, we can assume $|Cl(R)| = 2$. To prove b), we can assume neither f nor g is super-primitive; hence both $(A_f)_v$ and $(A_g)_v$ belong to the non-principal class of $Cl(R)$. Since $|Cl(R)| = 2$, it follows that $(A_f A_g)_v$ is principal. But $(A_f A_g)_v = (A_{fg})_v$ [12, Proposition 38.4], and fg is primitive, so $(A_{fg})_v = R$. Hence fg is superprimitive, which implies f and g are superprimitive, a contradiction. Hence R satisfies c) and d) by the proof of Theorem 3.4. □

If R is Krull and $|Cl(R)| = 2$, we can give a more direct proof that R satisfies conditions a)–d) as follows. If $abc = de$ and $(ab) = (P_1P_2P_3P_4)_v$, then (d) or (e) is contained in at least two of the P's. That is, $[ab, d] \neq 1$ or $[ab, e] \neq 1$. Hence R has the Z-property and a)–d) now follow.

Let x and y be indeterminates. We close this section with the following note.

Proposition 3.6. *If $R[x, y]$ is an HFD, then R satisfies conditions a), c), and d) of Theorem* 3.3.

Proof. Assume $R[x, y] \cong R[x][y]$ is an HFD. For a), we note that $R[x]$ is an HFD. Hence R is integrally closed by Theorem 3.1.

For c), we note that $R[x]$ has the Z-property by Proposition 3.1. We argue by contradiction. Assume $f, g \in R[x]$ are primitive polynomials over R and $fg = ah$, where $h \in R[x]$, $a \in R$, and $\ell(a) \geqslant 2$. Since f, g are primitive, we have $[a, f] = 1$ and $[a, g] = 1$. Hence $R[x]$ does not have the Z-property.

For d), assume $\frac{r}{s} \in I^{-1}$, where $I = (a_0, a_1, \ldots, a_n)$ is primitive in R, $[r, s] = 1$, and $\ell(s) \geqslant 2$. Let $f = a_0 + a_1 + \cdots + a_nx^n$ and $h = (x + \frac{r}{s})f$. Multiplying by s we obtain $sh = (sx + r)f$ and $[s, sx + r] = 1 = [s, f]$. Again, $R[x]$ does not have the Z-property. □

3.3. Examples

In the first example, we give two domains that do not have the Z-property. We conjecture that both are also HFDs, but are unable to find proof; because of this, we cannot state for certain that the Z-property and half-factorial property are distinct notions.

Example 3.1. Let F be a field with two elements and $R_1 = F[x, y, zx, zy]$ and $R_2 = F[x, y, zx^2, zy^2]$. Then $((zy)^2(x)^2 = (zx)^2(y)^2$ in R_1 and $(zy^2)(x)^2 = (zx^2)(y)^2$ in R_2, so neither of these domains have the Z-property. For example, in R_1, we have $[x^2, (zx)^2] = 1 = [x^2, y^2]$.

Next we give an example of a Dedekind domain R with the Z-property and $|Cl(R)| \geqslant 3$. Thus, for a Dedekind domain R, it is not the case that R has the Z-property if and only if $|Cl(R)| \leqslant 2$.

Example 3.2. Let R be Dedekind with $Cl(R) \cong \mathbb{Z}_3 = \{[0], [1], [2]\}$ such that the ideal class corresponding to $[1]$ contains all nonprincipal primes. (Such a domain exists by [14, Corollary 1.5]). Then R has the Z-property.

Proof. Assume $abc = de$; we claim $[ab, d] \neq 1$ or $[ab, e] \neq 1$. We can assume a, b are nonprime irreducibles. Write $(a) = P_1P_2P_3$ and $(b) = P_4P_5P_6$. Then there are ideals I, J such that $(d) = P_{i_1} \cdots P_{i_k}I$ and $(e) = P_{i_{k+1}} \cdots P_{i_6}J$ for some permutation $i_1, \ldots, i_6$ of the indices $1, \ldots, 6$. If $k \geqslant 3$, then it follows $[ab, d] \neq 1$. Else $6 - k \geqslant 3$ and it follows $[ab, e] \neq 1$. $\square$

Example 3.3. The domain $R := F[x][\{xy^n \mid n > 0\}, \{xz^m \mid m > 0\}]$ does not have the Z-property, since $(xyz)^3 = (xz)(xz^2)(xy^3) = (xy)(xy^2)(xz^3)$ and $[(xy)(xz^3), xz^2] = 1 = [(xy)(xz^3), (xz)(xy^3)]$. We do not know if R is an HFD. Even if it is, we should note that R is not integrally closed, as $(xyz)^2 \in R$, but $xyz \notin R$.

Next, we introduce a concept which is similar although not equivalent to the Z-property. If R is an atomic domain with the property that for all atoms $\xi, \alpha_1, \ldots, \alpha_n \in R$, some proper subproduct of $\alpha_1 \cdots \alpha_n$ belongs to the ideal (ξ) whenever the whole product belongs to (ξ) and $n \geqslant 3$, then it is clear that R has the Z-property. The converse is false by considering the following example.

Example 3.4. If $R := \mathbb{Z} + x2\mathbb{Z}[x]$, then R has the Z-property because its polynomial extension is an HFD [13, Proposition 1.4]. To justify our claim, we note that $(2x^3)(2)(2) = (2x)(2x)(2x)$ and no proper subproduct of the right side belongs to the ideal $(2x^3)$.

3.4. A Counterexample

In this section we will show that the converse of Theorem 3.3 is false. The counterexample we shall use is the power series ring

$$R := \mathbb{Q} + (x, y)\mathbb{Q}(z)[[x, y]]$$

where x, y, z are indeterminates; that is, $R = \mathbb{Q} + I$, where I is the maximal ideal of $\mathbb{Q}(z)[[x, y]]$. The complete integral closure is

$$R^* = \mathbb{Q}(z)[[x, y]]$$

Note that $I = (R : R^*)$, hence if t is another indeterminate, then $(R[t] : R^*[t]) = IR[t]$.

Proposition 3.7. *Every irreducible $f \in R$ is irreducible in R^*.*

Proof. If $f = gh$ in R^* with $g, h \notin U(R^*)$, then $g, h \in R$. □

Lemma 3.2. (cf. [13, Lemma 1.3]) *If $G, H \in R^*[t]$ and $GH \in R[t] \backslash I[t]$, then there exists $u \in U(R^*)$ such that $uG, u^{-1}H \in R[t]$. In particular, every nonconstant irreducible $F \in R[t] \backslash I[t]$ is irreducible in $R^*[t]$.*

Proof. Over R, the ideal A_{GH} contains a unit since $A_{GH} \nsubseteq I$. Thus $(A_G A_H)_v = (A_{GH})_v = R$ [12, Theorem 10.4]. Therefore, if $G = g_0(x, y) + g_1(x, y)t + \cdots +$

$g_n(x,y)t^n$ and $H = h_0(x,y) + h_1(x,y)t + \cdots + h_m(x,y)t^m$, where each $g_i, h_j \in R^*$, then $J := A_G A_H = (g_i h_j \mid 0 \leqslant i \leqslant n, 0 \leqslant j \leqslant m)$ satisfies $J_v = R$. If each generator $g_i h_j \in I$, then $J \subseteq I$ implies $J_v \subseteq I_v = I$, a contradiction. So there exist $0 \leqslant i_0 \leqslant n$, $0 \leqslant j_0 \leqslant m$ such that $g_{i_0} h_{j_0} \in U(R)$. Let $u = {g_{i_0}}^{-1}$. We must show $uG, u^{-1}H \in R[t]$. For each j we have $u^{-1}h_j = ug_{i_0}u^{-1}h_j = g_{i_0}h_j \in R$, which gives $u^{-1}H \in R[t]$. For each i we have $ug_iu^{-1}h_{j_0} = g_ih_{j_0} \in R$ and $u^{-1}h_{j_0}$ is a unit of R. Hence $ug_i \in R$ for each i, so that $uG \in R[t]$. $\square$

Proposition 3.8. *The domain R satisfies conditions a), c), d) and the conclusion of Theorem* 3.3*, but it does not satisfy condition b).*

Proof. For b), we consider the polynomial $f(t) = x + yt$ in $R[t]$ and note that f^2 is primitive, but f is not superprimitive, since $z \in {A_f}^{-1}$, $z \notin R$.

To prove that $R[t]$ is an HFD, we argue as in the proof of [13, Proposition 1.4]. Let F be a nonzero nonunit of $R[t]$. Write $F = p_1 \cdots p_n q_1 \cdots q_m$ where each p and q is prime in the UFD $R^*[t]$ and each $p \in R[t]$ and each $q \notin R[t]$. Choose n as large as possible. We claim n is the length of any irreducible factorization of F in $R[t]$. For, if $F = F_1 \cdots F_s G_1 \cdots G_t$ is an irreducible factorization in $R[t]$, where each $F_i \in I[t]$ and each $G_k \notin I[t]$, then by the lemma each G_k is irreducible in $R^*[t]$. For each i, suppose $F_i = F_{i1}F_{i2}\cdots F_{in_i}$ where each F_{ij} is prime in $R^*[t]$. Since $F_i \in I[t]$, a prime ideal, we can assume without loss of generality that $F_{i1} \in I[t]$. If $u \in U(R^*[t])$ and $k \in J = \{2, 3, \ldots, n_i\}$ are such that $uF_{ik} \in R[t]$ then $F_i = uF_{ik}\left(u^{-1}F_{i1}\prod_{j \neq k} F_{ij}\right)$, contrary to the fact that F_i is irreducible in $R[t]$. It follows that $s + t = n$.

To prove a), note that $\mathbb{Q}$ is integrally closed in $\mathbb{Q}(z)$. Hence R is integrally closed in R^*, and thus $R[t]$ is integrally closed in $R^*[t]$.

For c), we argue by contradiction. Suppose $FG = abH$, where F, G are primitive polynomials over $R[t]$, $a, b \in R \notin U(R)$, and $H \in R[t]$. Then $a, b \notin U(R^*)$. Moreover, we can assume that a, b are prime in R^* because any proper factor of a or b could be absorbed by H without sacrificing the generality of the argument. Then a divides F or G in $R^*[t]$, as does b. In fact, since F, G are irreducible in $R[t]$, we can assume that $F = aF'$ and $G = bG'$ with $F', G' \in R^*[t]$. Then $F'G' = H \in R[t]$. By the lemma, F' or G' belongs to $R[t]$, contrary to the fact that F and G are primitive.

Finally, for d), assume $J = (a_0, a_1, \dots, a_k)$ is a primitive ideal in R and $\frac{r}{s} \in J^{-1}$. We assume $\frac{r}{s}$ has already been reduced, so that $[r, s] = 1$. If $\ell(s) = 1$, we have the result. Therefore, it suffices to show that $\ell(s) \geqslant 2$ leads to a contradiction. If $F = a_0 + a_1 t + \cdots + a_k t^k$, then there exists a polynomial $G \in R[t]$ such that $rF = sG$. Now s has at least two prime factors in $R^*[t]$ and at most one of them can divide F because J is primitive. Hence r shares one of these factors with s, so $r = pw$, $s = pv$ where $w \in R^*$, $v \in R$ and $p \in R^*$ is prime. Choose $u \in U(R^*)$ such that $uw \in R$. Then $u^{-1}p$ divides both r and s in R, a contradiction. $\square$

4. RESULTS ON SPECIAL CLASSES OF DOMAINS

4.1. K+yB[y] Domains

Let Δ be a domain of the form

$$\Delta := K + yB[y]$$

where K is a field, B is an integrally closed domain, and y is an indeterminate. In [9, Theorem 2.1], it is shown that Δ is half-factorial if and only if B is integrally closed. We will approach the problem of determining when $\Delta[x]$ is half-factorial in a manner consistent with the ideas developed earlier.

The order of a nonzero polynomial $f(y) \in R[y]$, denoted $\operatorname{ord}(f)$, is the unique integer $n \geqslant 0$ such that $f(y) = y^n g(y)$ and g has nonzero constant term, i.e., $g(0) \neq 0$. This is the usual definition of order when f is considered as an element of the power series ring $R[[y]]$.

Proposition 4.1. *Δ has the Z-property.*

Proof. We assume $f_1 f_2 f_3 = g_1 g_2$, where the f's and g's are nonunits of R. We must show that $[f_1 f_2, g_1] \neq 1$ or $[f_1 f_2, g_2] \neq 1$. We break the problem into two cases.

In the first case, we assume either f_1 or f_2 has an irreducible factor f such that $f(0) \neq 0$. Then [9, Corollary 2.3] implies that f is prime in R. So $f|g_1$ or $f|g_2$ in R and the result follows easily in this case.

In the second case, both f_1 and f_2 have orders $\geqslant 1$. Cancel the prime factors of order zero of f_3 with those of g_1 and g_2. We obtain an equation of the form $f_1 f_2 f_3' = g_1' g_2'$, where g_1' and g_2' are factors of g_1 and g_2, respectively, and where f_3' has order $\geqslant 1$. Then $\operatorname{ord}(f_1 f_2 f_3') \geqslant 3)$, so $\operatorname{ord}(g_1') \geqslant 2$ or $\operatorname{ord}(g_2') \geqslant 2$. From this we obtain easily that x divides g_1' or g_2'. Also x divides $f_1 f_2$. The Z-property now follows. □

Proposition 4.2. *If $J = (g_1, g_2, \ldots, g_n)$ is a primitive ideal in Δ and $ord(g_i) = 0$ for some $i \in \{1, \ldots, n\}$, then J is primitive in $B[y]$.*

Proof. Suppose $g_i = fh_i$ in $B[y]$ for each $i = 1, \ldots, n$. Then $g_i = (f(0)^{-1}f)(f(0)h_i)$ for each i; these equations show that $g_1, \ldots, g_n$ are not relatively prime in Δ, a contradiction. $\square$

Proposition 4.3. *If $J = (g_1, g_2, \ldots, g_n)$ is a primitive ideal in Δ and $ord(g_i) = 0$ for some i, then J is superprimitive.*

Proof. Assume $\frac{\psi_1}{\psi_2} \in J^{-1}$ where $\psi_1, \psi_2 \in \Delta$. Assume, by way of contradiction, that ψ_2 does not divide ψ_1. We can assume $\frac{\psi_1}{\psi_2}$ is already reduced, so that ψ_1 and ψ_2 are relatively prime in Δ. By assumption, since $\frac{\psi_1}{\psi_2} \in I^{-1}$, there exist h_j in Δ such that $\psi_1 g_j = h_j \psi_2$ for each $j = 1, \ldots, n$. Consider the decomposition of g_i as a product of primes [9, Corollary 2.3]. If no prime factor of g_i divides ψ_2, then ψ_2 must divide ψ_1, a contradiction. Hence there exists a prime ϕ dividing both g_i and ψ_2. From the other equations with $j \neq i$, we obtain that ϕ divides g_j for all j, contrary to the fact that the g_j are relatively prime. $\square$

Corollary 4.1. *If $g, h \in \Delta[x]$ and and gh is primitive, then g is superprimitive or h is superprimitive.*

Proof. Assume neither g nor h is superprimitive. Since their product is primitive, we can assume without loss of generality that one of the coefficients of g has order zero. But then g is superprimitive by the previous, a contradiction. $\square$

Proposition 4.4. *In the domain Δ, if there exists $b \in B \backslash K$, then $(y, by)_v = yB[y]$.*

Proof. Let $I = (y, by)$ in Δ. If $\omega \in I^{-1}$, then $\omega = \frac{1}{y} f$ for some $f \in \Delta$. If $f(0) \neq 0$, then $bf = by\omega \in \Delta$, so $b \in K$, a contradiction. Hence $f(0) = 0$. It follows that $I^{-1} = B[y]$. Hence $I_v = ((I^{-1})^{-1} = yB[y]$, as desired. $\square$

Proposition 4.5. *If $J = (g_1, \dots, g_n)$ is a primitive ideal of Δ, then there are relatively prime $h_1, h_2 \in \Delta$ such that $(h_1, h_2)_v \subseteq I_v$.*

Proof. Consider an element $\frac{\psi_1}{\psi_2} \in J^{-1}$ with ψ_1, ψ_2 relatively prime in Δ. Then there are $h_j \in \Delta$ such that $\psi_1 g_j = h_j \psi_2$. If ϕ is prime and $\phi \mid g_i$, then ϕ does not divide ψ_2 because ϕ would necessarily divide the other g_j's. Hence $\phi \mid h_i$. Hence if g_i' denotes g_i divided by the product of all prime factors of g_i, then $\frac{\psi_1}{\psi_2} g_i' \in R$. Since i was arbitrary, we conclude that if $J' = (g_1', \dots, g_n')$, then $J^{-1} \subseteq (J')^{-1}$. Since each g_j' has no factors of order zero, at least one of them, say g_k', must be irreducible, since J is primitive. Choose $g' \in J'$ such that $g' \notin (g_k')$, and let $J'' = (g', g_k')$. Then J'' is primitive, two-generated, and $(J'')_v \subseteq (J')_v \subseteq J_v$, as required. $\square$

Corollary 4.2. *If Δ is integrally closed, then $\Delta[x]$ is an HFD.*

Proof. This follows by Theorem 3.4 and the results of this section. $\square$

4.2. Prüfer Domains and the PSP2-Property

Several characterizations of the PSP2-property were given in [1]. We recall the definition.

Definition 4.1. A domain R has the *PSP2-property* if whenever $I = (a_0, a_1)$ is a primitive ideal and $\frac{r}{s} \in I^{-1}$, then $\frac{r}{s} \in R$

Proposition 3.3 indicates a similarity between the Z-property and the PSP2-property. This similarity prompts the following question: When does the PSP2-property imply the PSP-property? The answer to this question could be useful in our attempt to characterize polynomial HFDs. In this section we answer the question in the setting of Prüfer domains.

The following result is well-known, but we repeat the proof here for convenience.

Proposition 4.6. *Let R be a Prüfer domain. If $F = (u, v)$ is a two-generated nonzero fractional ideal, then F^{-1} is two-generated.*

Proof. Since R is Prüfer, F is invertible, so $FF^{-1} = R$. Hence there exist $\omega_1, \omega_2 \in F^{-1}$ such that $\omega_1 u + \omega_2 v = 1$. Clearly $(\omega_1, \omega_2) \subseteq F^{-1}$. Moreover, if $x \in F^{-1}$, then $x = x1 = x(\omega_1 u + \omega_2 v) = \omega_1(xu) + \omega_2(xv) \in (\omega_1, \omega_2)$. Hence $F^{-1} = (\omega_1, \omega_2)$, so F^{-1} is two-generated. $\square$

Theorem 4.1. *Let R be a Prüfer domain and I an ideal of R. Then $I^{-1} \subseteq \bigcup\{(a,b)^{-1} \mid a, b \in R \text{ and } I_v \subseteq (a,b)_v\}$.*

Proof. Let $x \in I^{-1}$. We claim x belongs to the union of ideals as described in the theorem. Since $(x) \subseteq I^{-1}$, $I_v \subseteq (\frac{1}{x})$. Put $F = (\frac{1}{x}) \bigcap R$, so that $I_v \subseteq F$. Note $F = (1, x)^{-1}$, so by Proposition 4.6, F is two-generated, say $F = (a, b)$, where $a, b \in R$. Note $xF = x(1,x)^{-1} = (\frac{1}{x}, 1)^{-1} \subseteq R$, so $x \in F^{-1} = (a,b)^{-1}$. Since $(a, b) = (1, x)^{-1}$, (a, b) is divisorial. So not only $x \in (a, b)^{-1}$, but we also have $I_v \subseteq F = (a, b) = (a, b)_v$, so x belongs to the union as claimed. $\square$

Corollary 4.3. *Let R be a Prüfer domain and I an ideal of R. Then $I_v = \bigcap\{(a,b)_v : a, b \in R \text{ and } I_v \subseteq (a,b)_v\}$*

Proof. It is easy to verify the general relation $(\bigcup A_i)^{-1} = \bigcap A_i^{-1}$. Now taking the inverse of the equation in the previous theorem we obtain the inclusion $I_v \supseteq (\bigcup (a,b)^{-1})^{-1} = \bigcap (a,b)_v$. The other inclusion is trivial because I_v is contained in each $(a, b)_v$ by definition. $\square$

Corollary 4.4. *Let R be a Prüfer domain with the PSP2-property. Then*

a) *R has the PSP-property.*

b) *Moreover, if I is a primitive ideal, then $I = R$*

Proof. a) Let I be a finitely generated primitive ideal. If $x \in I^{-1}$, then by Theorem 4.1, $x \in (a,b)^{-1}$ for some $I_v \subseteq (a,b)_v$, where $a, b \in R$. If $(a,b) \subseteq (r)$ for some $r \in R$, then $(a,b)_v = \bigcap(\omega) \subseteq (r)$, so $I \subseteq I_v \subseteq (r)$ also. Hence r is a unit since I is primitive. Thus (a,b) is primitive, so $x \in R$ since R has PSP2.

b) If I is primitive, then $II^{-1} = R$. But part a) showed that $I^{-1} = R$. Hence $I = R$. □

Corollary 4.5. *Let R be an atomic Prüfer domain with the Z-property. If I is a primitive ideal and $\frac{r}{s} \in I^{-1}$, then there exists a common divisor g of r, s such that $\ell(\frac{s}{g}) \leqslant 1$.*

Proof. The same argument in the previous corollary shows that $\frac{r}{s} \in J^{-1}$ for some two-generated primitive ideal. Hence the result follows by the Proposition 3.3. □

Before closing this section, we consider a couple more propositions regarding the PSP-property. If $f \in R[x]$, then the greatest common divisor of the coefficients of f, if it exists, will be denoted $c(f)$.

Proposition 4.7. *Let R be a domain. The following are equivalent.*

a) *R has the PSP-property*

b) *If $f, g \in R[x]$, and $c(f)$, $c(g)$ exist, then $c(fg) = c(f)c(g)$*

Proof. a) $\Rightarrow$ b) If (a) holds and if $c(f)$, $c(g)$ exist, then $\frac{1}{c(f)}f, \frac{1}{c(g)}g$ are primitive, hence superprimitive polynomials over R. Hence the product $h = \frac{1}{c(f)}f\frac{1}{c(g)}g$ is also superprimitive [17, Theorem D], and it follows that $c(fg) = c(f)c(g)$.

b) $\Rightarrow$ a) Assume b) holds and that $c(f)$ exists. If $b \in R\backslash\{0\}$ then $c(bf) = bc(f)$. Hence R has the PSP-property by Proposition 2.2. $\square$

An ideal I is *strong* if $II^{-1} = I$ [3].

Proposition 4.8. *Let R be an integrally closed domain. Then R has the PSP-property if and only if every primitive ideal is strong.*

Proof. Assume R has the PSP-property. If $I = (a_0, a_1, \ldots, a_n)$ is a primitive ideal of R, then by assumption $I^{-1} = R$ and hence $II^{-1} = IR = I$, so that I is strong. Conversely, if I is primitive and strong, and if $\omega \in I^{-1}$, then $\omega I \subseteq II^{-1} = I$. It follows that $\omega \in R$, since R is integrally closed [12, Proposition 34.7] $\square$

4.3. Completely Integrally Closed Domains

In this section we consider the case of a completely integrally closed domain R with finite class group $Cl_v(R)$. Recall that every ideal in a completely integrally closed domain is v-invertible. The main result here is that if the polynomial extension of such a domain is half-factorial, then R is necessarily a Krull domain. We do not say anything about the case where $Cl_v(R)$ is infinite.

Recall that R has ACCP if it has the ascending chain condition on principal ideals. We repeat the proof of the following well-known result. Compare with [3, Theorem 2.1].

Lemma 4.1. *Let R be a domain. Then R has ACCP if and only if every decreasing chain of integral principal ideals with nonzero intersection stabilizes.*

Proof. If $(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq (1)$, then $(\frac{1}{a_0}) \supsetneq (\frac{1}{a_1}) \supsetneq (\frac{1}{a_2}) \supsetneq \cdots \supsetneq (1)$. Multiplying by a_0 we obtain $(1) \supsetneq (\frac{a_0}{a_1}) \supsetneq (\frac{a_0}{a_2}) \supsetneq \cdots \supsetneq (a_0)$. Therefore, the chain $(1) \supsetneq (\frac{a_0}{a_1}) \supsetneq (\frac{a_0}{a_2}) \supsetneq \cdots$ has nonzero intersection. The converse is proved in a similar fashion. $\square$

Theorem 4.2. *Let R be a domain with finite class group $Cl_v(R)$. The following are equivalent.*

a) *R has ACC on v-invertible integral v-ideals*

b) *R has ACCP*

Proof. a) $\Rightarrow$ b) Clear.

b) $\Rightarrow$ a) Assume that $J_1 \subsetneq J_2 \subsetneq J_3 \subsetneq \cdots \subsetneq R$ is a strictly increasing chain of v-invertible v-ideals. Since $Cl_v(R)$ is finite, the pigeon-hole principle implies the existence of infinitely many ideals in this sequence which are all equivalent in $Cl_v(R)$, that is, there exists a subsequence $J_{n_1} \subsetneq J_{n_2} \subsetneq J_{n_3} \subsetneq \cdots$ and $\omega_k \in K$ such that $J_{n_k} = \omega_k J_{n_{k+1}}$ for each $k = 1, 2, 3, \ldots$. Since ${J_{n_{k+1}}}^{-1} \subseteq {J_{n_k}}^{-1}$, we can write $(\omega_k) = \omega_k \left(J_{n_{k+1}} {J_{n_{k+1}}}^{-1}\right)_v = \omega_k \left(\frac{1}{\omega_k} J_{n_k} {J_{n_{k+1}}}^{-1}\right)_v \subseteq \left(J_{n_k} {J_{n_k}}^{-1}\right)_v \subseteq R$. Thus $J_{n_1} = \omega_1 J_{n_2} = \omega_1\omega_2 J_{n_3} = \cdots = \omega_1\omega_2\cdots\omega_k J_{n_{k+1}}$ for each k, where each ω_j is a nonunit of R. Thus if x is a nonzero element of J_1 we can construct a strictly decreasing chain $(\omega_1) \supsetneq (\omega_1\omega_2) \supsetneq (\omega_1\omega_2\omega_3) \supsetneq \cdots \supsetneq (x)$, and hence Lemma 4.1 implies that R is not ACCP. $\square$

Corollary 4.6. *Let R be a completely integrally closed domain with finite class group $Cl_v(R)$. Then R is Krull if and only if R has ACCP.*

Proof. If R has ACCP, then the previous result implies that R has ACC on v-invertible integral v-ideals. But every ideal is v-invertible since R is completely integrally closed. Hence R is a completely integrally closed Mori domain, i.e., a Krull domain. $\square$

Corollary 4.7. *Let R be a completely integrally closed domain with finite class group $Cl_v(R)$. If $R[x]$ is an HFD, then R is a Krull domain.*

Proof. It is easy to see that any HFD has ACCP. Hence the result follows from the previous corollary. $\square$

4.4. Mori Domains

In this section we consider the following condition on a domain R:

(C) If $f \in R[x]$ is primitive, then $(A_f)_v$ contains an irreducible element of R

Proposition 4.9. *Let R be a domain satisfying condition (C). If $f \in R[x]$ is primitive, there exist $b \in A_f$ and an atom $a \in (A_f)_v$, such that (a, b) is primitive and $(a, b)_v \subseteq (A_f)_v$.*

Proof. If f is superprimitive, the result is trivial. Assume this is not the case. By assumption there is an atom $a \in (A_f)_v$. The result follows once we choose $b \in A_f$ such that $b \notin (a)$, i.e., $[a, b] = 1$. $\square$

Proposition 4.10. *Let R be a Mori domain with the Z-property. The following are equivalent.*

a) If f, g are primitive polynomials over R and $fg = ah$, where $h \in R[x]$ and $a \in R$, then $\ell(a) \leqslant 1$

b) R satisfies condition (C)

Proof. a) $\Rightarrow$ b) Assume a) holds, but b) is false. Let a be an element of $(A_f)_v$ of minimal length. Since R is Mori, there exists $g \in K[x]$ such that $A_f^{-1} = (A_g)_v$. Let $g' = ag$. If $g' = rg''$, with $r \in R$ and $g'' \in R[x]$, then $\frac{a}{r} \in (A_f)_v$, so r is a unit by the minimality assumption. Thus g' is primitive. The product $fg' = afg$ and $fg \in R[x]$, contrary to hypothesis.

b) $\Rightarrow$ a) By the previous result, we can find primitive linear polynomials $f', g' \in R[x]$ such that $(A_{f'})_v \subseteq (A_f)_v$ and $(A_{g'})_v \subseteq (A_g)_v$. Thus $(A_{f'g'})_v \subseteq (A_f A_g)_v \subseteq (a)$. The Z-property implies $\ell(a) \leqslant 1$, as desired. $\square$

Proposition 4.11. *Assume R is integrally closed and satisfies condition (C). Then R has the Z-property*

Proof. Assume $fg = ah$, but $\ell(a) \geqslant 2$, where f, g are linear. By the previous, we can find elements such that $(a_1, b_1)_v \subseteq (A_f)_v$ and $(a_2, b_2)_v \subseteq (A_g)_v$, where $\ell(a_1) = 1 = \ell(a_2)$. Then $(a_1x + b_1)(a_2x + b_2) = a_1a_2h'$, with $h' \in R[x]$. So $(x + \frac{b_1}{a_1})(x + \frac{b_2}{a_2}) \in R[x]$, so a_i divides b_i [12, Theorem 10.4], a contradiction. □

Proposition 4.12. *Let R be a Mori domain and x, y be indeterminates. If $R[x, y]$ is an HFD, then R satisfies condition (C).*

Proof. If R does not satisfy (C), there exists a primitive polynomial $f \in R[x]$ such that $(A_f)_v$ contains no atom. Let $a \in (A_f)_v$ be an element of minimal length. Let $g \in K[x]$ be a polynomial such that ${A_f}^{-1} = (A_g)_v$ and put $h = ag \in R[x]$. Note that $[a, h] = 1$ by the minimality assumption. Also $fg \in R[x]$, $[a, h] = 1$, $[a, f] = 1$, and $hf = agf$, so $R[x]$ does not have the Z-property. Hence $R[x, y]$ is not an HFD by Proposition 3.1. □

5. CONCLUSION

The ultimate goal of this dissertation was to characterize the domains R such that $R[x]$ is an HFD. Our approach was to generalize the proof of Gauss's result on polynomial extensions of UFDs, and we succeeded in many respects. Further research may suggest a logical next step toward the solution of this problem. To that end, we offer the following list of open questions which have arisen out of our study.

1. If $R[x]$ is an HFD, which conditions in Theorem 3.3 must be satisfied by R? (cf. Chapter 3, Section 4)

2. If R has the PSP2-property, does it follow that R has the PSP-property? (cf. Chapter 4, Section 2)

3. Characterize the domains R which have the following property: If I is a v-finite ideal, then $I_v = (a, b)_v$ for some $a, b \in K$. (cf. Theorem 3.4)

4. We have shown that if $R[x]$ is completely integrally closed HFD with $|Cl(R)| < \infty$, then R is a Krull domain (Corollary 4.7). What if $Cl(R)$ is infinite?

5. It is known that if R is an integrally closed Mori domain, then its complete integral closure R^* is a Krull domain (Chapter 1, Section 1). If $R[x]$ is an HFD, does it follow that $|Cl(R^*)| \leqslant 2$?

6. Let F be a field with two elements and x, y, z indeterminates. Is $F[x, y, zx, zy]$ an HFD? (cf. Example 3.15)

REFERENCES

[1] D.D. Anderson and R.O. Quintero, *Some generalizations of GCD-domains*, Lecture Notes in Pure and Appl. Math., 189, Marcel Dekker, 1997, 189–195.

[2] J. Arnold and P. Sheldon, *Integral domains that satisfy Gauss's lemma*, Michigan Math. J. **22** (1975), 39–51.

[3] V. Barucci, *Mori Domains*, Non-Noetherian commutative ring theory **520**, (2000), 57-73.

[4] L. Carlitz, *A characterization of algebraic number fields with class number two*, Proc. Amer. Math. Soc. **11** (1960), 391–392.

[5] G.W. Chang and H. Kim, *Integral domains with a free semigroup of $*$-invertible integral $*$-ideals*, Bull. Korean Math. Soc., **48** (2011), 1207–1218.

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

[7] J. Coykendall, *Half-factorial domains in quadratic fields*, J. Algebra, **235** (2001), 417–430.

[8] J. Coykendall, *A characterization of polynomial rings with the half-factorial property*, Lecture Notes in Pure and Appl. Math., 189, Marcel Dekker, 1997, 291–294.

[9] J. Coykendall, T. Dumitrescu, and M. Zafrullah, *The half-factorial property and domains of the form $A + XB[X]$*, Houston J. Math., **32** (2006), 33-46.

[10] J. Coykendall and B. Mammenga, *An embedding theorem*, J. Algebra, **325** (2011), 177–185.

[11] J. Coykendall and M. Zafrullah, *AP-domains and unique factorization*, *J. Pure Appl. Algebra*, **189** (2004), 27–35.

[12] R. Gilmer, *Multiplicative Ideal Theory*, Marcel Dekker, 1972.

[13] N. Gonzalez, *Elasticity of $A+XI[X]$ domains where A is a UFD*, J. Pure Appl. Algebra **160** (2001), 183–194.

[14] A. Grams, *The distribution of prime ideals of a Dedekind domain*, Bull. Austral. Math. Soc. **11** (1974), 429-441.

[15] T. Hungerford, *Algebra*. Springer, 1974.

[16] M. Roitman, *Polynomial extensions of atomic domains*, J. Pure Appl. Algebra, **87** (1993), 187–199.

[17] H. Tang, *Gauss' lemma*, Proc. Amer. Math. Soc. **35** (1972), 372–376.

[18] A. Zaks, *Half-factorial domains*, Israel J. Math., **37** (1980), 281–302.