



Root Extensions and Factorization in Affine Domains

P. Etingof, P. Malcolmson, and F. Okoh

Abstract. An integral domain R is IDPF (Irreducible Divisors of Powers Finite) if, for every non-zero element a in R , the ascending chain of non-associate irreducible divisors in R of a^n stabilizes on a finite set as n ranges over the positive integers, while R is atomic if every non-zero element that is not a unit is a product of a finite number of irreducible elements (atoms). A ring extension S of R is a *root extension* or *radical extension* if for each s in S , there exists a natural number $n(s)$ with $s^{n(s)}$ in R . In this paper it is shown that the ascent and descent of the IDPF property and atomicity for the pair of integral domains (R, S) is governed by the relative sizes of the unit groups $U(R)$ and $U(S)$ and whether S is a root extension of R . The following results are deduced from these considerations: An atomic IDPF domain containing a field of characteristic zero is completely integrally closed. An affine domain over a field of characteristic zero is IDPF if and only if it is completely integrally closed. Let R be a Noetherian domain with integral closure S . Suppose the conductor of S into R is non-zero. Then R is IDPF if and only if S is a root extension of R and $U(S)/U(R)$ is finite.

1 Introduction

In this paper all rings are integral domains. For any element a in R , the set of prime divisors of a^n coincides with the set of prime divisors of a . This elementary fact played a key role in [15], where we investigated integral domains with the property that every non-zero element is contained in only finitely many principal prime ideals. The results there led to another proof of Zariski's version of the Nullstellensatz [15, Corollary 1.15].

We considered the consequences of working with irreducible elements instead of prime elements [16]. This led us to the notion of IDPF. An integral domain R is IDPF if for every non-zero element a in R the ascending chain of non-associate irreducible divisors in R of a^n , $n = 1, 2, \dots$ stabilizes on a finite set. If every non-zero element in an integral domain R has only finitely many non-associate irreducible divisors, R is said to be IDF, see [10]. Thus if R is IDPF, then it is IDF, but not conversely [16]. The concept of IDPF is also defined in [9] under the term *locally finitely generated*. In [9] there are many results in IDPF of an asymptotic nature. In [9, 16] it was proved that a Krull domain, in particular a Noetherian integrally closed domain, is IDPF. We now give the definition of IDPF used in this paper. For any element $a \in R$, let $D_R(a)$ denote the set $\bigcup_{n=1}^{\infty} D_n(a)$, where $D_n(a)$ is the set of non-associated irreducible divisors in R of a^n . Thus R is IDPF if $D_R(a)$ is finite for every non-zero element a in R and R is IDF if $D_1(a)$ is finite for every non-zero element a in R . Let $R \subseteq S$ be a ring extension with S IDPF. Following [6], we say that a domain R is atomic if every

Received by the editors April 10, 2007; revised August 28, 2008.
Published electronically December 4, 2009.
AMS subject classification: 13F15, 14A25.

non-zero element in R that is not a unit is a product of a finite number of irreducible elements (atoms).

A ring extension $R \subseteq S$ is a *root extension* or *radical extension* if for each $s \in S$, there exists a natural number $n(s)$ depending on s with $s^{n(s)} \in R$. In [13, 19] it was shown that when R and S are fields and S is a root extension, they must have positive characteristic. In [5] the authors use the results in [8, 13] to show the following.

Theorem 1.1 *If R is a domain that contains a field of characteristic zero and R is a proper subring of a domain S , then S is not a root extension of R .*

It was shown in [16, §§2, 3] that a subring R of the ring of Gaussian integers S is IDPF if and only if S is a root extension of R . As a result, $\mathbf{Z}[2i]$ is IDPF while $\mathbf{Z}[5i]$ is not IDPF. Hence *field* cannot be deleted from Theorem 1.1.

However every subring of the Gaussian integers is atomic and IDF. It was shown that a domain R is atomic and IDF if and only if it is FFD (Finite Factorization Domain), that is, every non-zero element is contained in only finitely many principal ideals [1]. The similarity between IDPF and FFD invites comparison between the results of [2] and those in this paper. In that connection we recall the following results from [2] after fixing some notation. Throughout the paper S is a ring extension of R . The conductor of S to R , $\{r \in R : rS \subseteq R\}$, will be denoted by $[R:S]$ and the unit group of R will be denoted by $U(R)$. We follow the practice in [14] by calling each of our results a theorem.

Remark 1.2 A local domain (R, M) with R/M infinite is FFD if and only if R is integrally closed [2, Corollary 4], while an FFD containing a field of characteristic zero need not be integrally closed [2, Remark 4].

Theorem 1.3 (i) *Suppose that $R \subseteq S$ is a pair of integral domains with non-zero conductor. Then R an FFD implies that $U(S)/U(R)$ is finite and S is an FFD. [2, Theorem 4]*

(ii) *Let R be a Noetherian domain with its integral closure S a finitely generated R -module. Then R is an FFD if and only if $U(S)/U(R)$ is finite (see [2, Corollary 3] or [12, Theorem 7]).*

Throughout the paper, a certain comparability result is used several times. Given two n -tuples of non-negative integers $a = (a_1, \dots, a_n)$ and $b = (b_1, \dots, b_n)$, we say $a \leq b$ if $a_i \leq b_i$ for $i = 1, 2, \dots, n$. In that case we say a and b are *comparable*.

Lemma 1.4 ([16, Lemma 3.1]) *Let n be any positive integer. Then every infinite set of n -tuples contains comparable pairs of n -tuples x and y with $x \neq y$.*

2 Root Extensions and the IDPF Property

In this section we discuss the descent and ascent of atomicity and the IDPF property in ring extensions.

Theorem 2.1 (Descent of atomicity and the IDPF property) *Let $R \subseteq S$ with S atomic and IDPF. Suppose $U(S)/U(R)$ is finite. If S a root extension of R , then R is IDPF and atomic.*

Proof To prove R atomic, we proceed by contradiction. Suppose R is not atomic. Then R is not FFD; that is, some non-zero element $g \in R$ has infinitely many non-associated divisors in R . Since S is FFD, all but finitely many of these divisors in R are associated in S . Let $A = \{g_1, g_2, \dots\}$ be the resulting infinite set of elements that are associated in S . Then $g_i = u_i h$ where h is a fixed member of A and $u_i \in U(S)$.

Since $U(S)/U(R)$ is finite, infinitely many of the u_i 's are in the same coset of $U(R)$ in $U(S)$. By renumbering, this means that $\{u_1, u_2, \dots\} \subseteq uU(R)$ for some $u \in U(S)$. Hence $u_2 = uv_2$ and $u_3 = uv_3$, where $\{v_2, v_3\} \subseteq U(R)$. But $g_2 = u_2 h, g_3 = u_3 h$, and $u_2 = uv_3$, where $v = u_2/u_3 \in U(R)$. So $u_2 h = vu_3 h$, i.e. g_2 and g_3 are associated in R . This contradicts the choice of the g_i 's.

We now prove that R is IDPF. Suppose not. Then for some $0 \neq g \in R - U(R)$, $D_R(g)$ is infinite. Since S is IDPF, $D_S(g)$ is some finite set $\{g_1, \dots, g_k\}$.

Since S is a root extension of R , there is a positive integer m with $g_i^m \in R$ for every i with $1 \leq i \leq k$. Form $\mathbf{Z}_m^k = \{(n_1, n_2, \dots, n_k) : 0 \leq n_i < m\}$. For each $\tau = (z_1, \dots, z_k) \in \mathbf{Z}_m^k$ and each coset $uU(R)$ (with u in $U(S)$ a fixed representative of $uU(R)$), consider

$$T_{\tau,u} = \{h \in D_R(g) : h \text{ is associated in } R \text{ with } u \prod_{i=1}^k g_i^{r_i}, \text{ with } r_i \equiv z_i \pmod{m}\}.$$

Each element $h \in D_R(g)$ is associated in S with a product of the g_i 's because $\{g_1, \dots, g_k\} = D_S(g)$. There are only finitely many $T_{\tau,u}$'s because \mathbf{Z}_m^k and $U(S)/U(R)$ are finite sets. So $D_R(g) = \bigcup_{\tau,u} T_{\tau,u}$, as τ ranges over \mathbf{Z}_m^k and u ranges over the set of representatives of the cosets of $U(R)$ in $U(S)$, is a finite union. Since $D_R(g)$ is infinite, one of the $T_{\tau,u}$'s is infinite.

Choose and fix one such infinite $T_{\tau,u}$ and let $\mathbf{W} = \{0, 1, 2, \dots\}$. Define $\Phi: \mathbf{W}^k \rightarrow S$ by $\Phi(x_1, x_2, \dots, x_k) = u g_1^{mx_1+z_1} \dots g_k^{mx_k+z_k}$. Observe that Φ maps onto the infinite set $T_{\tau,u}$ consisting of irreducible elements associated with elements in $D_R(g)$. Therefore $\Phi^{-1}(T_{\tau,u})$ is an infinite subset of \mathbf{W}^k . By Lemma 1.4 there must exist $x = (x_1, \dots, x_k)$ and $y = (y_1, \dots, y_k)$, $x \neq y$, in $\Phi^{-1}(T_{\tau,u})$ that satisfy $x_i \leq y_i$ for all i . Then $y_i = x_i + d_i$ with $d_i \geq 0$ and

$$\begin{aligned} \Phi(y_1, \dots, y_k) &= u g_1^{mx_1+md_1+z_1} \dots g_k^{mx_k+md_k+z_k} = u(g_1^{mx_1+z_1} \dots g_k^{mx_k+z_k})(g_1^{md_1} \dots g_k^{md_k}) \\ &= \Phi(x_1, \dots, x_k)(g_1^m)^{d_1} \dots (g_k^m)^{d_k}. \end{aligned}$$

Since $\Phi(y_1, \dots, y_k) \in T_{\tau,u}$ is irreducible in R , we must have $d_1 = \dots = d_k = 0$. So $(y_1, \dots, y_k) = (x_1, \dots, x_k)$. This contradicts $x \neq y$. Hence R is IDPF. ■

The following example from [2, Remark 2, p. 392] shows that the hypothesis $U(S)/U(R)$ finite is necessary in Theorem 2.1.

Example 2.2 Let $R = F_1 + XF_2[[X]]$ and let $S = F_2[[X]]$, where F_1 is an infinite algebraic extension of its prime subfield \mathbf{Z}_p and F_1 is a subfield of F_2 with $1 < [F_2:F_1] < \infty$ and $F_2[[X]]$ is the power series over F_2 in the variable X . Then $U(S)/U(R) \cong U(F_2)/U(F_1)$ is torsion. Since F_1 is an infinite field and $F_1 \neq F_2$, $U(F_2)/U(F_1)$ is infinite [4]. To see that S is a root extension of R , let $f = f_0 + f_1X + \dots$. If $f_0 = 0$,

then $f \in R$. If $f_0 \neq 0$, then $f = f_0(1 + \frac{f}{f_0}X + \dots)$. Since $U(F_2)/U(F_1)$ is torsion, $f_0^k \in U(F_1)$ for some positive integer k . Then $f^k = f_0^k(1 + \frac{f}{f_0}X + \dots)^k \in R$. Thus S is a root extension of R . As noted in [2], R is not an FFD. Both R and S are Noetherian, hence atomic. So R not an FFD means that R is not IDF, hence not IDPF.

Theorem 2.3 (Ascent of atomicity and the IDPF property) *Let $R \subseteq S$ with $[R:S] \neq \{0\}$. If R is atomic and IDPF, then S is atomic and IDPF, $U(S)/U(R)$ is finite, and S is a root extension of R .*

Proof Since R is atomic and IDPF it is atomic and IDF, and hence R is FFD, as noted in the introduction. Then by Theorem 1.3, we get that $U(S)/U(R)$ is finite and S is an FFD, hence is atomic and IDF.

We first prove that S is a root extension of R . So for each $g \in S$ we must find $n = n(s)$ such that $g^n \in R$. If $g \in U(S)$, then $g^n \in U(R)$, where $n = |U(S)/U(R)|$. So let $g \in S - U(S)$. We have by hypothesis that $cS \subseteq R$ for some $0 \neq c \in R$. In particular, $cg \in R$. Since R is IDPF, there is a finite set of atoms $\{F_1, \dots, F_k\} \subseteq R$ such that $D_R(cg) = \{F_1, \dots, F_k\}$.

Now cg^m divides $(cg)^m$ in R . Since R is atomic, $cg^m = \prod_{i=1}^l G_i$, where G_1, \dots, G_l are atoms in R . Each G_i also divides $(cg)^m$ in R . So $G_i \in D_R(cg) = \{F_1, \dots, F_k\}$. Hence $cg^m = u_m F_1^{\alpha_1(m)} \dots F_k^{\alpha_k(m)}$, where $u_m \in U(R)$ and $\alpha_i(m)$'s are nonnegative integers. Every factorization in R of cg^m comes with a k -tuple $\alpha(m) = (\alpha_1(m), \dots, \alpha_k(m))$. For each positive integer m , we choose one such $\alpha(m)$. Let $\Phi(m) = \alpha(m)$. In this way we get a map $\Phi: \mathbf{N} \rightarrow \mathbf{W}^k$, where \mathbf{N} and \mathbf{W} are the set of natural numbers and the set of nonnegative integers respectively.

If $\text{Im}(\Phi)$ is infinite, then by Lemma 1.4 there are distinct elements x and y in $\text{Im}(\Phi)$ with $x \leq y$. So for some positive integer m and some non-zero integer r ,

$$x = (\alpha_1(m), \dots, \alpha_k(m)) \quad \text{and} \quad y = (\alpha_1(m+r), \dots, \alpha_k(m+r)).$$

Then $(\alpha_1(m), \dots, \alpha_k(m)) \leq (\alpha_1(m+r), \dots, \alpha_k(m+r))$. Hence

$$\begin{aligned} cg^{m+r} &= u_{m+r} F_1^{\alpha_1(m+r)} \dots F_k^{\alpha_k(m+r)} \\ &= \frac{u_{m+r}}{u_m} u_m F_1^{\alpha_1(m)} \dots F_k^{\alpha_k(m)} F_1^{\alpha_1(m+r)-\alpha_1(m)} \dots F_k^{\alpha_k(m+r)-\alpha_k(m)} \\ &= \frac{u_{m+r}}{u_m} F_1^{\alpha_1(m+r)-\alpha_1(m)} \dots F_k^{\alpha_k(m+r)-\alpha_k(m)} \\ &= \frac{u_{m+r}}{u_m} cg^m F_1^{\alpha_1(m+r)-\alpha_1(m)} \dots F_k^{\alpha_k(m+r)-\alpha_k(m)}. \end{aligned}$$

Cancelling cg^m we get that $g^r = F_1^{\alpha_1(m+r)-\alpha_1(m)} \dots F_k^{\alpha_k(m+r)-\alpha_k(m)} \in R$. If $r < 0$, then $g^r \in U(S)$ because $g \in S$, $g^r \in S$, and $g^{-r} \in S$. So $g \in U(S)$, contradicting the hypothesis that $g \notin U(S)$. So $r > 0$ and $g^r \in R$ as required. Thus we are done if $\text{Im}(\Phi)$ is infinite.

Suppose $\text{Im}(\Phi)$ is finite. Then $(\alpha_1(m), \dots, \alpha_k(m)) = (\alpha_1(m+r), \dots, \alpha_k(m+r))$ for some positive integers m and r . Then

$$cg^{m+r} = u_{m+r} F_1^{\alpha_1(m)} \dots F_k^{\alpha_k(m)} = u_{m+r}/u_m cg^m,$$

so $g^r = u_{m+r}/u_m \in U(R)$. Hence $g \in U(R) \subseteq U(S)$, contradicting the hypothesis that $g \notin U(S)$.

Thus far we have proved that S is atomic, IDF, and a root extension of R . We now prove that S is IDPF. Let $g \in S$, g not a unit, $g \neq 0$. The proof is by contradiction. Suppose $D_S(g)$ is infinite. Let $n > 0$ with $g^n \in R$ (using that s a root extension of R). Note that $D_S(g)$ infinite implies that $D_S(g^n)$ is also infinite. Let h_1, h_2, \dots , be respective non-associated irreducible divisors in S of $g^{nk_1}, g^{nk_2}, \dots$. Then $g^{nk_j} = g_j h_j$, $h_j, g_j \in S$. Let $0 \neq c \in [R:S]$. Then for $k_j \geq 3$, $c^{k_j} g^{nk_j} = c^{k_j} h_j g_j = (ch_j)(cg_j)c^{k_j-2}$. Each factor on the right-hand side is in R . Thus ch_j divides $(cg^n)^{k-j}$ in R . Since R is IDPF, there are only finitely many non-associated irreducible divisors of $(g^n)^k, k = 3, 4, \dots$ in R . So $D_R(g^n) = \{F_1, F_2, \dots, F_l\}$, some finite set of atoms in R . So each $ch_j = u_j F_1^{\alpha_1(j)} \dots F_l^{\alpha_l(j)}$, where u_j is in $U(R)$ and $\alpha_i(j)$ is a non-negative integer for $i = 1, \dots, l$. Among such factorizations in R of ch_j , choose one. In this way we get a map $\Phi: \mathbf{N} - \{1, 2\} \rightarrow \mathbf{W}^l$, given by $\Phi(j) = (\alpha_1(j), \dots, \alpha_l(j))$. If the image of Φ is finite, then for some $r > 0$ and some $m > 0$, $\Phi(m) = \Phi(m+r)$. Then

$$ch_m = u_m F_1^{\alpha_1(m)} \dots F_l^{\alpha_l(m)} \quad \text{and} \quad ch_{m+r} = u_{m+r} F_1^{\alpha_1(m+r)} \dots F_l^{\alpha_l(m+r)}.$$

So $ch_{m+r} = u_{m+r} u_m^{-1} ch_m, u_{m+r} u_m^{-1} \in U(R) \subseteq U(S)$. Cancelling c contradicts that h_m and h_{m+r} are non-associated in S . So we may assume that the image of Φ is infinite. By Lemma 1.4, there is a comparable pair $\alpha_m = (\alpha_1(m), \dots, \alpha_l(m))$ and $\alpha_{m+r} = (\alpha_1(m+r), \dots, \alpha_l(m+r))$ with $\alpha_m \neq \alpha_{m+r}$. So $\alpha_j(m+r) > \alpha_j(m)$ for some $j \in \{1, 2, \dots, l\}$. Then $ch_{m+r} = u_{m+r} u_m^{-1} F_1^{\alpha_1(m+r)-\alpha_1(m)} \dots F_l^{\alpha_l(m+r)-\alpha_l(m)} ch_m$, where $\alpha_j(m+r) > \alpha_j(m)$ for some j and $\alpha_j(m+r) \geq \alpha_j(m)$ for each $j \in \{1, 2, \dots, l\}$.

If $F_1^{\alpha_1(m+r)-\alpha_1(m)} \dots F_l^{\alpha_l(m+r)-\alpha_l(m)}$ is a unit in S , then once again, cancelling c contradicts the hypothesis that h_m and h_{m+r} are non-associated in S . If $F_1^{\alpha_1(m+r)-\alpha_1(m)} \dots F_l^{\alpha_l(m+r)-\alpha_l(m)}$ is not a unit in S , again cancelling c leads to a proper factorization of h_{m+r} in S contradicting the hypothesis that h_{m+r} is irreducible in S . Therefore $D_S(g^n)$ is finite. As remarked earlier, this implies that $D_S(g)$ is finite. Since g was an arbitrary element of S , this proves that S is IDPF. ■

The ring extension $\mathbf{Z}[X] \subseteq \mathbf{Q}[X]$ shows that we cannot drop the conductor condition in Theorem 2.3. We now bring in our next theme: the influence of the complete integral closure of a ring on the IDPF property.

Denote by $Q(R)$ the quotient field of R . Recall that an element g in $Q(R)$ is *almost integral* if there exists an element $0 \neq c \in R$ such that $cg^m \in R$ for each $m \geq 1$. The *complete integral closure* of R is the set of all almost integral elements in $Q(R)$. A ring is completely integrally closed if it is equal to its complete integral closure.

Lemma 2.4 ([2, Corollary 1]) *If S is the complete integral closure of an FFD, then $U(S)/U(R)$ is torsion.*

Theorem 2.5 *Let R be atomic and IDPF with S as its complete integral closure. Then S is a root extension of R .*

Proof Just as in the proof of Theorem 2.3, R is FFD. By Lemma 2.4, $U(S)/U(R)$ is torsion.

To prove that S is a root extension of R , for each $g \in S$ we must find $n = n(s)$ such that $g^n \in R$. If $g \in U(S)$, then $g^n \in U(R)$ where n is the order of g in the torsion group $U(S)/U(R)$. Suppose $g \in S - U(S)$. Since g is almost integral over R , we have the elements cg^m used in the proof of Theorem 2.3 that S is a root extension of R . ■

Theorem 2.6 *Let R be atomic and IDPF and R contains a field of characteristic zero. Then R is completely integrally closed.*

Proof Combine Theorem 2.5 and Theorem 1.1. ■

Example 2.7 We give an atomic completely integrally closed domain R that contains a field of characteristic zero but R is not IDPF.

First we recall that a Noetherian domain is integrally closed if and only if it is completely integrally closed. But an ascending union of completely integrally closed domains need not be completely integrally closed. For instance, let A be a Noetherian integrally closed domain that contains a prime element p . Let

$$R = A[pX, pX^2, \dots, pX^n, \dots] = \bigcup_{n=1}^{\infty} A_n,$$

where $A_n = A[pX, pX^2, \dots, pX^n]$. The proof in [16, Example 6.3] that A is integrally closed also works to show that the Noetherian ring A_n is integrally closed, hence completely integrally closed. But R is not completely integrally closed because $pX^n \in R$ for $n = 1, 2, \dots$ but $X \notin R$.

Let $\{X_1, X_2, \dots\}$ and $\{Y_1, Y_2, \dots\}$ be two sets of indeterminates, and let K be a field of characteristic zero. Let $R_0 = K[Z]$, where Z is an indeterminate. Let

$$R_1 = K[X_1, Y_1]/\langle X_1Y_1 - Z \rangle, \quad R_2 = R_1[X_2, Y_2]/\langle X_2Y_2 - Z \rangle.$$

For each positive integer k , let $R_{k+1} = R_k[X_{k+1}, Y_{k+1}]/\langle X_{k+1}Y_{k+1} - Z \rangle$. Each R_k is Noetherian. By [20, Lemma 2.12], R_k is integrally closed, hence completely integrally closed.

Let $R = \bigcup_{k=1}^{\infty} R_k$. If $0 \neq r \in R$ is not a unit, then $r \in R_n$ for some n . As R_n is Noetherian, R_n is atomic. Thus $r = r_1 \cdots r_m$, where each r_i is an atom in R_n . If no r_i is Z , then r_i does not split and we are done. If some r_i is Z , then in R_{n+1} , r splits into a product of atoms. So R is atomic. To show that R is completely integrally closed, let d and x be non-zero elements of $Q(R)$ with $dx^n \in R$ for all $n \geq 1$. We must show that $x \in R$. For some positive integer l , we have that d, x , and thus dx^n are in $Q(R_l)$ for all $n \geq 1$. Consider the retract of R to R_l obtained by $X_i \mapsto Z$ and $Y_i \mapsto 1$ for all X_i, Y_i not in R_l . This retract is the identity map on R_l . It also fixes dx^n for all $n \geq 1$. Hence $dx^n \in R_l$ for all $n \geq 1$. Since R_l is completely integrally closed, $x \in R_l \subset R$. So R is completely integrally closed. Since Z has infinitely many non-associate divisors X_i , R is not FFD. Since it is atomic, it is not IDF, hence not IDPF.

The following facts are needed in the proof of the next theorem. The integral closure of a Noetherian ring is Krull (see [18, Theorem 33.10]) and a Krull ring is atomic [2] and IDPF [9, 16].

Theorem 2.8 *Let R be a Noetherian domain with integral closure S and $[R:S] \neq \{0\}$. Then the following are equivalent.*

- (i) R is IDPF.
- (ii) $U(S)/U(R)$ is finite and S is a root extension of R .

Proof Since R is Noetherian, R is atomic. Hence Theorem 2.3 says that (i) implies (ii). That (ii) implies (i) follows from Theorem 2.1 and the remarks preceding Theorem 2.8. ■

Example 2.9 [5] Let $R = \mathbf{Z}[nX, X^2, X^3]$ and $S = \mathbf{Z}[X]$, where n is any positive integer and X is an indeterminate. Both R and S are Noetherian, hence atomic. For any $f \in S$, we have $f^n \in R$ and $nf \in R$. Since $U(S) = U(R)$, Theorem 2.8 implies that R is IDPF. The proof of [16, Proposition 1.7] can be adapted to show that if m and n are distinct positive integers, then $\mathbf{Z}[mX, X^2, X^3]$ and $\mathbf{Z}[nX, X^2, X^3]$ are non-isomorphic rings. Hence $\mathbf{Z}[X]$ contains infinitely many non-isomorphic subrings that are IDPF.

Theorem 2.10 *Let K be a field of characteristic zero. Let R be the coordinate ring of an affine variety over K . Then R is normal if and only if it is IDPF.*

Proof Since R is affine, it is Noetherian, hence atomic. Also for Noetherian rings, completely integrally closed and normal coincide. If R is IDPF, then R is completely integrally closed by Theorem 2.6. On the other hand, if R is integrally closed, then it is Noetherian and integrally closed, hence IDPF as already remarked in the preamble to Theorem 2.8. ■

Since a curve is non-singular if and only if it is normal (see [11]), IDPF characterizes non-singular curves in zero characteristic.

Theorem 2.11 below and Example 2.9 present a contrast between the polynomial ring $\mathbf{Z}[T]$ and the polynomial ring $K[T]$, where K is a field of characteristic zero, as far as IDPF-subrings are concerned.

Theorem 2.11 *Let K be a field of characteristic zero, and $K[T]$ the polynomial ring over K . Then any K -subalgebra R of $K[T]$ that is IDPF is isomorphic to $K[T]$.*

Proof By [7], R may be considered up to isomorphism as an affine subalgebra of $K[T]$ with $K[T]$ integral over A . If R is IDPF, then by Theorem 2.10, $R \cong K[T]$. ■

There is another situation where an analogue of Theorem 2.8 can be obtained. First we note the following fact.

Theorem 2.12 *If R is a subring of a factorial domain S with $U(S) \cap R = U(R)$. Then R is atomic.*

Proof Let $0 \neq g \in R - U(R)$. Let $g = h_1 \cdots h_l$ where each h_j is irreducible in S . Suppose $g = g_1 \cdots g_k$ is a factorization into non-units in R with $k > l$. Since S is factorial, (after possibly permuting), $g_i = u_i h_i$, where $u_i \in U(S)$. Since $k > l$, this implies that g_{l+1} is a unit in S , hence a unit in R because $U(S) \cap R = U(R)$. This contradicts the assumption that g_{l+1} is not a unit in R . Hence $k \leq l$. One deduces from this that g is a product of at most l atoms in R . Hence R is atomic. ■

Theorem 2.13 ([17, Theorem 2.3]) *Let S be a factorial domain that contains a field K . Let I be a non-zero proper ideal of S . Let $R = K + I$. Then the following are equivalent.*

- (i) R is IDPF
- (ii) $U(S)/U(R)$ is finite and S is a root extension of R .

Proof Since S is factorial, it is atomic and IDPF. Hence Theorem 2.1 says that (ii) implies that R is atomic and IDPF.

As for (i) implies (ii), Theorem 2.12 gives us that R is atomic. Also $[R:S]$ contains the non-zero ideal I . By [17, Lemma 2.1(b)], $U(S) \cap R = U(R)$. Hence by Theorem 2.12, R is atomic. So by Theorem 2.3, (i) implies (ii). ■

Remark 2.14 *The positive characteristic situation.* Let K be a field of characteristic $p > 0$. The cuspidal algebra $K[T^2, T^3]$ is shown in [16, Lemma 4.2] to be IDPF, while [16, Proposition 4.5] shows that the nodal algebra $K[T^2 - 1, T(T^2 - 1)]$ is not IDPF if $p \neq 2$. Is this slim evidence a precursor of a significant relationship between the types of singularities of curves and the IDPF-status of the corresponding coordinate rings?

Is the domain in Theorem 2.6 Krull? That is, one may wonder if a domain R that is atomic and IDPF and contains a field of characteristic zero must be Krull. Since Theorem 2.6 says that R is completely integrally closed, we are reduced by [3, Theorem 2, p. 480] to asking whether R has the ascending chain condition on divisorial integral ideals.

Acknowledgment Theorems 2.5 and 2.6 were suggested by the referee. The same referee made comments that contributed to Theorem 2.8. The one-dimensional version of Theorem 2.8 was conjectured by a referee of [17]. We also thank John Lawrence of the University of Waterloo for informing us about [5]. The results there enabled us to remove an uncountability hypothesis in characteristic zero.

References

- [1] D. D. Anderson, D. F. Anderson, and M. Zafrullah, *Factorization in integral domains*. J. Pure Appl. Algebra **69**(1990), no. 1, 1–19. doi:10.1016/0022-4049(90)90074-R
- [2] D. D. Anderson and B. Mullins, *Finite factorization domains*. Proc. Amer. Math. Soc. **124**(1996), no. 2, 389–396. doi:10.1090/S0002-9939-96-03284-4
- [3] N. Bourbaki, *Commutative Algebra*. Elements of Mathematics, Springer-Verlag, Berlin, 1989.
- [4] A. Brandis, *Über die multiplikative Struktur von Körpererweiterungen*. Math. Z. **87**(1965), 71–73. doi:10.1007/BF01109932
- [5] M. Chacron, J. Lawrence, and D. Madison, *A note on radical extensions of rings*. Canad. Math. Bull. **18**(1975), no. 3, 423–424.
- [6] P. M. Cohn, *Bezout rings and their subrings*. Proc. Cambridge Philos. Soc. **64**(1968), 251–264. doi:10.1017/S0305004100042791
- [7] P. M. Eakin, *A note on finite-dimensional subrings of polynomial rings*. Proc. Amer. Math. Soc. **31**(1972), 75–80. doi:10.2307/2038515
- [8] C. Faith, *Radical extensions of rings*. Proc. Amer. Math. Soc. **12**(1961), 274–283. doi:10.2307/2034321
- [9] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations*. In: Algebraic, Combinatorial and Analytic Theory. Pure and Applied Mathematics 278. Chapman and Hall, Boca Raton, FL, 2006.
- [10] A. Grams and H. Warner, *Irreducible divisors in domains of finite character*. Duke Math. J. **42**(1975), 271–284. doi:10.1215/S0012-7094-75-04225-8

- [11] R. Hartshorne, *Algebraic Geometry*. Graduate Texts in Mathematics 52. Springer-Verlag, New York, 1977.
- [12] F. Halter-Koch, *Finiteness theorems for factorizations*. Semigroup Forum **44**(1992), no. 1, 1–12. doi:10.1007/BF02574329
- [13] I. Kaplansky, *A theorem on division rings*. Canad. J. Math. **3**(1951), 290–292.
- [14] ———, *Commutative Rings*. Revised Edition. University of Chicago Press, Chicago, 1974.
- [15] P. Malcolmson and F. Okoh, *Expansions of prime ideals*. Rocky Mountain J. Math. **35**(2005), no. 5, 1689–1706. doi:10.1216/rmj/1181069657
- [16] ———, *A class of integral domains between factorial domains and IDF-domains*. Houston J. Math. **32**(2006), no. 2, 399–421.
- [17] ———, *Factorization in subalgebras of the polynomial algebra*. Houston J. Math. **35**(2009), no. 4, 991–1012.
- [18] M. Nagata, *Local Rings*. Interscience Tracts in Pure and Applied Mathematics 13. Interscience Publishers, New York, 1962.
- [19] ———, *A type of integral extensions*. J. Math. Soc. Japan **20**(1968), 266–267. doi:10.2969/jmsj/02010266
- [20] M. Roitman, *Polynomial extensions of atomic domains*. J. Pure Appl. Algebra **87**(1993), no. 2, 187–199. doi:10.1016/0022-4049(93)90122-A

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA
e-mail: etingof@math.mit.edu

Department of Mathematics, Wayne State University, Detroit, MI 48202, USA
e-mail: petem@math.wayne.edu
okoh@math.wayne.edu