COLLOQUIUM MATHEMATICUM

VOL. 142 2016 NO. 2

FACTORIAL FERMAT CURVES OVER THE RATIONAL NUMBERS

BY

PETER MALCOLMSON (Detroit, MI), FRANK OKOH (Detroit, MI)
and VASUVEDAN SRINIVAS (Mumbai)

Abstract. A polynomial f in the set $\{X^n + Y^n, X^n + Y^n - Z^n, X^n + Y^n + Z^n, X^n + Y^n - 1\}$ lends itself to an elementary proof of the following theorem: if the coordinate ring over $\mathbb{Q}$ of f is factorial, then n is one or two. We give a list of problems suggested by this result.

1. Introduction. This paper was motivated by some results on factorial domains and half-factorial domains. A domain is *half-factorial* if every non-zero element that is not a unit is the product of a unique number of irreducible elements. A recent exploration of half-factorial subrings of factorial domains is [MO3]. The emphasis there was on half-factorial subrings of polynomial rings over factorial domains. We now introduce the cast of polynomials in the present paper.

Let K be a field that does not contain a square root of -1. Then $R = K[X,Y]/\langle X^2 + Y^2\rangle$ is isomorphic to $K + XK[i][X]$, where i is a square root of -1. It is shown in [MO5] that R has the following properties:

(1) R is half-factorial.
(2) The power series extension $R[[X]]$ is half-factorial.
(3) The power series extension $R[[X,Y]]$ is not half-factorial.

Whether there is a factorial domain with the corresponding properties is an open question (see [F], [S1], and [S3]). See also [L, Chapter IV, Section 9]. Do coordinate rings of $X^n + Y^n$, n an arbitrary natural number, have the same property?

Let $\mathrm{Cl}(R)$ denote the divisor class group of R or the class group of R, whichever makes sense. In [CA], it is proved that a number ring R is half-factorial if and only if $|\mathrm{Cl}(R)| \le 2$. Motivated by questions in [N], Zaks [Z, Theorem 2.4] proved that a Krull domain R has the property that the polynomial ring $R[X]$ is half-factorial if and only if $|\mathrm{Cl}(R)| \le 2$. However, a Krull domain D with $|\mathrm{Cl}(D)| > 2$ can be half-factorial (see [LY]). The following theorem of Samuel's [S2] is Proposition 11.5 in [F].

2010 *Mathematics Subject Classification*: Primary 13F15; Secondary 14H05.
Key words and phrases: factorial, half-factorial, coordinate rings.

DOI: 10.4064/cm142-2-9

THEOREM 1.1. *Let F be a non-degenerate quadratic form in $K[X_1, X_2, X_3]$. Let $A_F = K[X_1, X_2, X_3]/\langle F\rangle$. Then* $\mathrm{Cl}(A_F) = \mathbb{Z}/2\mathbb{Z}$ *if and only if there is a non-trivial solution to $F(X_1, X_2, X_3) = 0$ in K. If no such solution exists, then A_F is factorial.*

We replace the quadratic forms in Samuel's theorem by $aX^n+bY^n+cZ^n$, a, b, c integers with $abc \neq 0$. In this paper we deal only with the simplest case: $abc = \pm 1$. We now recall the result that led us to consider X^n+Y^n-1, n an arbitrary natural number. It is shown [F, Proposition 11.8] that $|\mathrm{Cl}(\mathbb{R}[X_0, X_1]/\langle X_0^2+X_1^2-1\rangle|=2$, while $|\mathrm{Cl}(\mathbb{C}[X_0, X_1]/\langle X_0^2+X_1^2-1\rangle| = 1$, Hence $\mathbb{R}[X_0, X_1]/\langle X_0^2+X_1^2-1\rangle$ is half-factorial and $\mathbb{C}[X_0, X_1]/\langle X_0^2+X_1^2-1\rangle$ is factorial. Replacing 2 with n gives us the last set of polynomials in our list:

$$\mathcal{F} = \{X^n + Y^n, X^n + Y^n - Z^n, X^n + Y^n + Z^n, X^n + Y^n - 1\}.$$

The following theorem gives examples of factorial domains that do not come from quadratic forms. If $R = \mathbb{C}[X_1, X_2, X_3, X_4]$ is the polynomial ring in four variables over $\mathbb{C}$, then for *almost all* homogeneous forms of degree at least four, $R/\langle f\rangle$ is factorial. This is the Noether–Lefschetz theorem (see [EI, p. 520] for unexplained terminology and references on related theorems). In turn, the references in [PS1] and [PS2] include variations on Noether–Lefschetz theory. Other results on factoriality of complex affine domains can be found in [GP]. All of these results are over algebraically closed fields. The lack of corresponding theorems for the field of rational numbers led us to the working hypothesis that, amongst homogeneous polynomials, only those of degree one or two have a chance of giving factorial coordinate rings or half-factorial coordinate rings over $\mathbb{Q}$. This paper tests this hypothesis on the set $\mathcal{F}$.

This paper also plays to our interest in linking factorization properties to well-known top-drawer theorems. Here is one outcome of this interest. An integral domain is *PPF* (*Principal Primes Finite*) if every non-zero element is contained in only finitely many principal prime ideals. Investigation of this property led us to Corollary 1.15 in [MO1]: If A is an affine commutative algebra over a field k, then any field between A and k is algebraic over k; this is a slight generalization of Zariski's version of the Nullstellensatz [FU, p. 31]. See [EMO], [MO2], and [MO4] for other examples relating factorization properties to some algebraic geometry in an elementary way.

Problems arising. We list some problems which we do not treat in this paper in order to keep the focus on the main theorem.

We say that a polynomial $\mathcal{P}(\mathbf{X})$ in $\mathbb{Q}[\mathbf{X}]$ is *factorial* (respectively, *half-factorial*) over $\mathbb{Q}$ if the coordinate ring $\mathbb{Q}[\mathbf{X}]/\langle\mathcal{P}(\mathbf{X})\rangle$ is factorial (respectively, half-factorial). In general, we use the polynomial as a stand-in for its corresponding coordinate ring over $\mathbb{Q}$.

(1) *The abc-problem.* For which triples (a, b, c) of non-zero integers is $aX^n + bY^n + cZ^n$ factorial or half-factorial?

(2) *The n-tuple problem.* For which positive integers n and for which n-tuples of non-zero integers $(a_1, \ldots, a_n)$ is $a_1X_1^n + \cdots + a_nX^n$ factorial or half-factorial?

It is well-known, and documented in [CMO], that most generalizations of factoriality are unstable under the standard ring extensions, as listed in [BO, p. 622]. The factorial domains R in this paper are principal ideal domains. Hence $R[[X]]$ is also factorial (see [S1] or [K, Theorem 188]). In the case when R is half-factorial, but not factorial, $R[X]$ is half-factorial by Zaks's theorem quoted above. This leads to the next problem.

(3) *The power series problem.* Suppose R is one of the coordinate rings in this paper with $|\mathrm{Cl}(R)| = 2$. Is $R[[X]]$ half-factorial?

An integral domain is said to be *atomic* if every non-zero element that is not a unit is a finite product of irreducible elements of D. The extent to which D fails to be half-factorial is measured by the *elasticity* of D, denoted by $\rho(D)$, where $\rho(D) := \sup\{m/n : x_1 \cdots x_m = y_1 \cdots y_n$ with $x_1, \ldots, x_m, y_1, \ldots, y_n$ being irreducible elements of $D\}$. By definition, an atomic domain D is half-factorial if and only if $\rho(D) = 1$. The concept of elasticity was introduced in [V]. We refer to [GPR] for more information and references on elasticity.

(4) *The elasticity problem.* What are the elasticities of the non-half-factorial polynomials in $\mathcal{F}$?

The notation below will be in force throughout the paper:

- Let D be an integral domain.
- For $C \subseteq D$, $\langle C \rangle$ denotes the ideal of D generated by C.
- $\mathrm{U}(D)$ denotes the unit group of D.
- $\mathrm{Irr}(D)$ is the set of irreducible elements of D.
- $\deg \mathcal{P}$ denotes the degree of the polynomial $\mathcal{P}$, while I denotes the ideal $\langle \mathcal{P} \rangle$. The corresponding coordinate ring $\mathbb{Q}[\mathbf{X}]/I$ is denoted by R. The context will clarify the variables that constitute $\mathbf{X}$.
- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ denote the usual rings and K denotes an arbitrary field.
- $|S|$ denotes the cardinality of the set S.

2. Elementary criteria for irreducibility in factor rings. The first proposition tells us when irreducibility of a polynomial $f \in K[\mathbf{X}]$ can be deduced from the irreducibility of a specialization of f to a polynomial of one variable.

Proposition 2.1. *Let f be a homogeneous polynomial in $K[\mathbf{X}]$ of degree m in k variables. Suppose f has a non-zero term of the form X_1^m and suppose $a_2, \dots, a_k$ are elements in K such that $f(X_1, a_2, \dots, a_k)$ is in $\mathrm{Irr}(K[X_1])$. Then f is in $\mathrm{Irr}(K[\mathbf{X}])$.*

Proof. Suppose that $f(\mathbf{X}) = g(\mathbf{X})h(\mathbf{X})$. Then $\deg g + \deg h = m$ and $f(X_1, a_2, \dots, a_k) = g(X_1, a_2, \dots, a_k)h(X_1, a_2, \dots, a_k)$. By assumption, $g(X_1, a_2, \dots, a_k)$ (say) is in $\mathrm{U}(K)$. This implies that X_1^m appears entirely in h. Since g and h may be assumed homogeneous, $g(\mathbf{X})$ must be a constant. ∎

Proposition 2.2 lists some well-known elements of $\mathrm{Irr}(\mathbb{Q}[\mathbf{X}])$.

Proposition 2.2.

(a) *Let k be any positive integer ≥ 2 and n a power of 2. Then $\sum_{j=1}^{k} X_j^n$ is in $\mathrm{Irr}(\mathbb{Q}[\mathbf{X}])$.*
(b) *Let k be any positive integer ≥ 3 and n any positive integer. Then $\sum_{j=1}^{k} X_j^n$ is in $\mathrm{Irr}(\mathbb{Q}[\mathbf{X}])$.*
(c) *For n a positive integer, the polynomial $X^n + Y^n$ is in $\mathrm{Irr}(\mathbb{Q}[\mathbf{X}])$ if and only if $n = 2^m$ for some positive integer m.*
(d) *The polynomial $X^n + Y^n - 1$ is in $\mathrm{Irr}(\mathbb{Q}[\mathbf{X}])$ for every natural number n.*

Proof. (a) The proof is by induction on $k \geq 2$. First $X^{2^m}+1$ is irreducible in $\mathbb{Q}[\mathbf{X}]$ by Eisenstein's criterion with the test-prime 2, after replacing X by $X+1$. Hence $X^{2^m}+Y^{2^m}$ is irreducible in $\mathbb{Q}[X, Y]$ by Proposition 2.1. Assume that $\sum_{j=1}^{k} X_j^n$ is irreducible over $\mathbb{Q}$, hence prime in $\mathbb{Q}[X_1, \dots, X_n]$. Then $(\sum_{j=1}^{k} X_j^n) + X_{k+1}^n$, considered as a polynomial in $(\mathbb{Q}[X_1, \dots, X_n])[X_{k+1}]$, is irreducible by Eisenstein's criterion with $\sum_{j=1}^{k} X_j^n$ as the test prime.

(b) Part (a) allows us to assume that $n = 2^m l$ where l is odd and $l \geq 3$. The proof is by induction on $k \geq 3$. Suppose $k = 3$. We deduce that $X_1^n + X_2^n + X_3^n \in (\mathbb{Q}[X_2, X_3])[X_1]$ is irreducible by Eisenstein's criterion with any irreducible divisor of $X_2^n + X_3^n$ as a test prime. We now conclude the proof as in (a).

(c) Write $n = 2^m l$, l odd. If $l = 1$, irreducibility follows from (a). If $l \geq 3$, then $X^{2^m} + Y^{2^m}$ divides $X^n + Y^n$.

(d) follows from Eisenstein's criterion with $Y - 1$ as the test prime. ∎

The next proposition is the first step in obtaining elements of $\mathrm{Irr}(R)$ from some elements of $\mathrm{Irr}(\mathbb{Q}[\mathbf{X}])$. It is also a precursor of a process we call the *adjustment*.

Proposition 2.3. *Let $\{\mathcal{P}, \mathcal{A}\}$ be a subset of $\mathrm{Irr}(\mathbb{Q}[\mathbf{X}])$ with $\mathcal{P}$ homogeneous and $\deg \mathcal{A} < \deg \mathcal{P}$. Then $\mathrm{U}(R) = \mathrm{U}(\mathbb{Q}) + I$ and $\mathcal{A} + I$ is in $\mathrm{Irr}(R)$.*

Proof. Let $f+I \in \mathrm{U}(R)$. Then for some $\{g,h\} \subseteq \mathbb{Q}[\mathbf{X}]$, we have $1-fg = \mathcal{P}h$. Write

$$f = f_0 + f_1 + \cdots + f_M,$$
$$g = g_0 + g_1 + \cdots + g_P,$$
$$h = h_0 + h_1 + \cdots + h_D$$

as sums of their homogeneous parts. Here and in "The adjustment", D is the degree of h and is not to be confused with D in "Notation". We may assume that if $f_i \neq 0$, then $\mathcal{P}$ does not divide f_i, because if $\mathcal{P} \mid f_i$, then I absorbs f_i. An analogous statement applies to g_i. Suppose $h \neq 0$ after this procedure. Comparison of leading terms gives $f_M g_P = \mathcal{P}h_D$. Hence $\mathcal{P} \mid f_M$ or $\mathcal{P} \mid g_P$, a contradiction. Hence $h = 0$. Therefore $f \in \mathrm{U}(\mathbb{Q})$, giving $\mathrm{U}(R) = \mathrm{U}(\mathbb{Q}) + I$. The proof that $\mathcal{A} + I \in \mathrm{Irr}(R)$ is identical to the above with 1 replaced by $\mathcal{A}$. Since $\deg \mathcal{A} < \deg \mathcal{P}$, $\mathcal{A}$ does not contribute when we compare leading terms in $\mathcal{A}(\mathbf{X}) - fg = \mathcal{P}h$. Since $\mathcal{A} \in \mathrm{Irr}(R)$, $\mathcal{A} = fg$ implies that $f + I$ or $g + I$ is in $\mathrm{U}(R)$. ∎

The set-up for Proposition 2.4 is the same as for Proposition 2.3 except that $\mathcal{P}$ is not assumed homogeneous.

PROPOSITION 2.4. *Let* $\mathcal{A}(\mathbf{X})$ *be in* $\mathrm{Irr}(\mathbb{Q}[\mathbf{X}])$ *with* $\deg \mathcal{A} < \deg \mathcal{P}$. *If the leading homogeneous term of* $\mathcal{P}$ *is in* $\mathrm{Irr}(\mathbb{Q}[\mathbf{X}])$, *then* $\mathcal{A} + I$ *is in* $\mathrm{Irr}(R)$.

Proof. Suppose $\mathcal{A} - fg = \mathcal{P}h$ in the notation of the proof of Proposition 2.3. Amongst all such expressions choose one with $\deg f + \deg g$ minimum.

Suppose $h_D \neq 0$ for that choice. Let L be the leading homogeneous term of $\mathcal{P}$. By hypothesis, L is irreducible, hence prime in $\mathbb{Q}[\mathbf{X}]$ and $\deg L = \deg \mathcal{P}$. Then $f_M g_P = L h_D$. Say $L \mid f_M$. Let $f_\star = f_0 + f_1 + \cdots + f_M - (f_M/L)(L + \mathcal{P}_\star)$ where $\mathcal{P}_\star = \mathcal{P} - L$. Then $f_\star + I = f + I$ and $\mathcal{A} - f_\star g = \mathcal{P}h_\star$ for some $h_\star \in \mathbb{Q}[\mathbf{X}]$. Since $\deg \mathcal{P}_\star < \deg L$, we get $\deg f_\star + \deg g < \deg f + \deg g$. This contradicts minimality. Hence $h = 0$. As in the proof of Proposition 2.3, we conclude that $\mathcal{A} \in \mathrm{Irr}(R)$. ∎

We now give examples that show that the conditions in Propositions 2.3 and 2.4 are necessary for membership in $\mathrm{Irr}(R)$.

EXAMPLE 1 (Necessity of homogeneity of $\mathcal{P}$). Let $\mathcal{P}$ be the non-homogeneous polynomial $X^3 + Y^3 - 1$. Let $\mathcal{A} = X^3 + Y^3 + Y^2 - 1 \in \mathrm{Irr}(\mathbb{Q}[X,Y])$. We have $\mathcal{A} + I = Y^2 + I$. Hence $\mathcal{A} + I \notin \mathrm{Irr}(R)$.

In Example 1, $\deg \mathcal{A} = \deg \mathcal{P}$, leaving room for the possibility that if $\mathcal{A}$ is in $\mathrm{Irr}(\mathbb{Q}[\mathbf{X}])$, homogeneous or not, and $\deg \mathcal{A} < \deg \mathcal{P}$, then $\mathcal{A} + I$ is in $\mathrm{Irr}(R)$. Example 2 rules out this possibility.

Example 2. Let $\mathcal{P} = X^p + Y^p - 1$, where p is an odd prime. Let

$$B = X + Y, \qquad A = \frac{X^p + Y^p}{B}.$$

The homogeneous polynomial A is in $\mathrm{Irr}(\mathbb{Q}[X,Y])$ and A is the leading term of $A+B-2$. By Proposition 2.1, $A+B-2 \in \mathrm{Irr}(\mathbb{Q}[X,Y])$. We now show that $A+B-2+I \notin \mathrm{Irr}(R)$ by noting that $A+B-2+I = (1-A)(B-1)+I$. Neither $(1-A)+I$ nor $(B-1)+I$ is in $\mathrm{U}(R)$: suppose $((1-A)+I))(f+I) = 1+I$ for some $f \in \mathbb{Q}[X,Y]$. Then $(1-A)f-1 = (X^p+Y^p-1)g$ for some $g \in \mathbb{Q}[X,Y]$. Substituting $Y = 0$ and $X = 1$ leads to the contradiction $0 = 1$. A similar proof shows that $B-1+I \notin \mathrm{U}(R)$. Noting that $\deg(A+B-2) = p-1 < p$, we have the required example.

Example 3 (Necessity of lower degree). Let $\mathcal{P} = XY - Z^2$ and $\mathcal{A} = X^2 + YZ$. Both $\mathcal{A}$ and $\mathcal{P}$ are in $\mathrm{Irr}(\mathbb{Q}[X,Y,Z])$. However $(X^2+YZ)+I = ((X+Z)+I)((X+Y-Z)+I)$. Neither of these factors is in $\mathrm{U}(R)$. Hence $\mathcal{A}+I \notin \mathrm{Irr}(R)$.

When does an element in $\mathrm{Irr}(R)$ give an element in $\mathrm{Irr}(\mathbb{Q}[X,Y])$? Our small answer below involves lower degree.

Proposition 2.5. *Suppose* $\mathrm{U}(R) = \mathrm{U}(\mathbb{Q}) + I$ *and* $\deg \mathcal{A} < \deg \mathcal{P}$. *If* $\mathcal{A} + I$ *is in* $\mathrm{Irr}(R)$, *then* $\mathcal{A}$ *is in* $\mathrm{Irr}(\mathbb{Q}[X,Y])$.

Proof. Suppose $\mathcal{A} = fg$ in $\mathbb{Q}[\mathbf{X}]$. Then $f+I$ or $g+I$ is in $\mathrm{U}(R)$ because $\mathcal{A}+I$ is in $\mathrm{Irr}(R)$. Say $f+I = u+I$ for some $u \in \mathrm{U}(\mathbb{Q})$. Hence $f = u+\mathcal{P}h$ for some $h \in \mathbb{Q}[\mathbf{X}]$. The degree hypothesis on $\mathcal{A}$ implies that $h = 0$. Hence $f \in \mathrm{U}(\mathbb{Q})$. ■

The examples above necessitate our case-by-case approach to establishing membership in $\mathrm{Irr}(R)$.

3. Non-factorial Fermat curves. Recall that a polynomial $\mathcal{P}$ in $\mathbb{Q}[\mathbf{X}]$ is said to be *factorial* if $R = \mathbb{Q}[\mathbf{X}]/\langle\mathcal{P}\rangle$ is factorial. Let $x \in R-(\mathrm{U}(R)\cup\{0\})$. We define the *set of lengths* of x as follows:

$$L(x) := \{m \in \mathbb{N} : x = x_1 \cdots x_m, \text{ where } \{x_1,\ldots,x_m\} \subseteq \mathrm{Irr}(R)\}.$$

If $m \in L(x)$, we say that x has a *factorization of length* m or simply *length* m. We refer to [GH, p. 20] for references to the literature on *systems of sets of lengths*.

Lemma 3.1. *If* R *is factorial, then* $|L(x)|=1$ *for all* x *in* $R-(\mathrm{U}(R)\cup\{0\})$.

Lemma 3.1 and Propositions 2.3 and 2.4 are used in the rest of the paper, often implicitly.

Theorem 3.2. *The following homogeneous polynomials in* $\mathbb{Q}[\mathbf{X}]$ *are not factorial:*

(a) $X^{2^k} + Y^{2^k}$, $k \geq 1$.
(b) $X^n + Y^n - Z^n$, $n \geq 3$.
(c) $X^n + Y^n + Z^n$, $n \geq 3$ *and* n *is not a power of* 2.

Proof. (a) We deduce from Proposition 2.4 that $\{X+I, (X^{2^{k-1}} + Y^{2^{k-1}}) + I\} \subseteq \mathrm{Irr}(R)$ and $X^{2^{k-1}} - Y^{2^{k-1}} + I$ has a factorization of length $\leq 2^{k-1}$. On the other hand, $2X^{2^k} + I$ has a factorization of length $2^k > 2^{k-1} + 1$. Since $2X^{2^k} + I = X^{2^k} - Y^{2^k} + I = ((X^{2^{k-1}} - Y^{2^{k-1}}) + I)((X^{2^{k-1}} + Y^{2^{k-1}}) + I)$, we get $|L(2X^{2^k} + I)| > 1$. Hence R is not factorial by Lemma 3.1.

(b) Since $n \geq 3$, $Z^n - Y^n + I$ has an irreducible factor $g+I$ where $\deg g \geq 2$ and $g \in \mathrm{Irr}(\mathbb{Q}[\mathbf{X}])$. Therefore $Z^n - Y^n + I$ has a factorization of length $< n$. Since $X^n + I$ has a factorization of length n and $X^n + I = Z^n - Y^n + I$, we get $|L(X^n + I)| > 1$. Hence R is not factorial by Lemma 3.1.

(c) Let $n = 2^k m$, $m \geq 3$. Since $Y^{2^k} + Z^{2^k}$ is in $\mathrm{Irr}(\mathbb{Q}[\mathbf{X}])$ (by Proposition 2.2) and is a factor of $Y^n + Z^n$, we use $X^n + I = -(Y^n + Z^n) + I$ to complete the proof of (c) in the same way as in (b). ∎

The next theorem handles the case $n = 2^k$ in $X^n + Y^n + Z^n$.

THEOREM 3.3. *The polynomial* $X^n + Y^n + Z^n$ *is not factorial when* n *is a power of* 2 *and* $n \geq 3$.

Proof. Suppose $X^n + Y^n + Z^n$ is factorial. Then any closed point in the projective curve would have residue class field divisible by n by [H, Chapter 2, Exercise 6.3(c)]. The geometric class group must be cyclic. It is generated by the hyperplane intersection. On the other hand, the above model of the Fermat curve of degree $n > 2$ has closed points of degree $< n$. For example, if n is a power of 2, then we can always find points of the form $(a, a^2, 1)$, where a is either a primitive cube root of 1 or a primitive sixth root of 1. ∎

We want to give explicit examples that show the non-factoriality of $X^{2^k} + Y^{2^k} + Z^{2^k}$.

THEOREM 3.4.

(a) $X^{2^2} + Y^{2^2} + Z^{2^2}$ *is not factorial.*
(b) $X^{2^k} + Y^{2^k} + Z^{2^k}$, $k \geq 2$, *is not factorial.*

Proof. (a) $2(X^2 + Y^2 + XY)^2 + I = (X+Y+Z)(X+Y-Z)((X+Y)^2 + Z^2) + I$. Non-factoriality of $X^{2^2} + Y^{2^2} + Z^{2^2}$ follows from this equation, Proposition 2.3, and Lemma 3.1.

(b) We replace X, Y, Z in (a) respectively by $X^{2^{k-2}}$, $Y^{2^{k-2}}$, $Z^{2^{k-2}}$ to get $2(X^{2^{k-1}} + Y^{2^{k-1}} + X^{2^{k-2}} Y^{2^{k-2}})^2 + I = (X^{2^{k-2}} + Y^{2^{k-2}} + Z^{2^{k-2}})(X^{2^{k-2}} + Y^{2^{k-2}} - Z^{2^{k-2}})((X^{2^{k-2}} + Y^{2^{k-2}})^2 + Z^{2^{k-1}}) + I$. Just as in (a) this equation yields non-factoriality of $X^{2^k} + Y^{2^k} + Z^{2^k}$, $k \geq 2$. ∎

Homogeneity has played a key role in our results so far. We now turn our attention to the non-homogeneous polynomials $X^n + Y^n - 1$. The next proposition will help with deciding the factoriality of these polynomials. Recall that the *radical* of a natural number $n \geq 2$, written $\mathrm{rad}(n)$, is the product of the distinct prime divisors of n.

PROPOSITION 3.5. *The second non-zero term in the cyclotomic polynomial of order n occurs at the degree $\varphi(n) - n/\mathrm{rad}(n)$.*

Proof. Since the cyclotomic polynomial $\Phi_n(T)$ is symmetric, that is, $\Phi_n(1/T)T^{\varphi(n)} = \Phi_n(T)$, we examine the second lowest degree term instead. We have the known formula $\Phi_n(T) = \pm\prod_{d|n}(1 - T^d)^{\mu(n/d)}$, where μ is the Möbius function. Expanding the factors with $\mu(n/d) = -1$ shows that the second lowest non-zero term occurs at degree $\mathrm{rad}(n)$. Reflecting Φ gives the result. ■

The idea underlying the *adjustment* was used in the proof of Propositions 2.3 and 2.4.

The adjustment. Let $\mathcal{A} \in \mathrm{Irr}(\mathbb{Q}[\mathbf{X}])$ and $I = \langle X^n + Y^n - 1\rangle$. We want to decide whether $\mathcal{A} + I$ is in $\mathrm{Irr}(R)$. Suppose $\mathcal{A} + I = (f + I)(g + I)$. Then for some $\{f, g, h\} \subseteq \mathbb{Q}[\mathbf{X}]$, we have

$$\mathcal{A} - (X^n + Y^n - 1)h = fg. \tag{3.1}$$

Write

$$\begin{aligned} f &= f_0 + f_1 + \cdots + f_M, \\ g &= g_0 + g_1 + \cdots + g_P, \\ h &= h_0 + h_1 + \cdots + h_D \end{aligned} \tag{3.2}$$

as sums of their homogeneous parts.

We assume that $\deg \mathcal{A} < n + D = M + P$. (This will be the case in Theorem 3.6.)

The point of the *adjustment* is to change f and g in (3.1) with degree of h reduced. We note that $X^n + Y^n$ has no multiple roots. Suppose $X^n + Y^n = FG$, where F and G are relatively prime with F dividing $f_M, f_{M-1}, f_{M-2}, \ldots, f_K$, and G dividing $g_P, g_{P-1}, g_{P-2}, \ldots, g_L$, where $K \leq M$ and $L \leq P$.

Let

$$\begin{aligned} f^\star &= f_M + f_{M-1} + f_{M-2} + \cdots + f_K, \\ g^\star &= g_M + g_{M-1} + g_{M-2} + \cdots + g_L, \\ f_\star &= f - f^\star, \\ g_\star &= g - g^\star. \end{aligned}$$

These are the ingredients for adjusting $\mathcal{A} - (X^n + Y^n - 1)h = fg$. We write

$$
\begin{aligned}
(3.3)\qquad & \left[\frac{f + (X^n + Y^n - 1)f_\star}{F}\right]\left[\frac{g + (X^n + Y^n - 1)g_\star}{G}\right] \\
&= \left[\frac{f - f_\star + (X^n + Y^n)f_\star}{F}\right]\left[\frac{g - g_\star + (X^n + Y^n)g_\star}{G}\right] \\
&= \left[\frac{f^\star}{F} + f_\star G\right]\left[\frac{g^\star}{G} + g_\star F\right] = f_\star g^\star + f^\star g_\star + \frac{f^\star g^\star}{FG} + f_\star g_\star FG \\
&= fg + (FG - 1)f_\star g_\star - (1 - FG)\frac{f^\star g^\star}{FG} \\
&= \mathcal{A} - (FG - 1)h + (FG - 1)f^\star g^\star - (FG - 1)\frac{f^\star g^\star}{FG} \\
&= \mathcal{A} - (X^n + Y^n - 1)\left[h - f_\star g_\star + \frac{f^\star g^\star}{FG}\right].
\end{aligned}
$$

We can write

$$
\begin{aligned}
&\left[\frac{f + (X^n + Y^n - 1)f_\star}{F}\right]\left[\frac{g + (X^n + Y^n - 1)g_\star}{G}\right] \\
&\qquad\qquad = \mathcal{A} - (FG - 1)h + (FG - 1)f^\star g^\star - (FG - 1)\frac{f^\star g^\star}{FG}
\end{aligned}
$$

as $\mathcal{A} - (X^n + Y^n - 1)h_A = f_A g_A$, A for adjusted. The leading term of $\frac{f^\star g^\star}{FG}$ is

$$\frac{f_M g_P}{FG} = -h_D$$

and $\deg f_\star g_\star \le (K - 1) + (L - 1)$.

If $K + L - 2 < D$ or if $f_\star g_\star = 0$, then $\deg h_A < \deg h$. Hence the degree of h has been reduced. Since $F + I$ and $G + I$ are units in R, we see that $f_A + I$ and $g_A + I$ are respective associates in R of $f + I$ and $g + I$.

This completes the description of the adjustment.

We use the notion of the adjustment in the long proof of the next theorem. There is perhaps a dose of geometry that can be applied to shorten the proof. We have not been successful in finding one.

Theorem 3.6. *Let $\mathcal{P}$ be $X^n + Y^n - 1$. Suppose $\mathcal{A}$ is an irreducible factor of $Y^n - 1$ in $\mathbb{Q}[Y]$. Then $\mathcal{A} + I$ is in* Irr(R)*.*

Proof. Suppose $\mathcal{A} + I \notin \mathrm{Irr}(R)$. Then for some non-constant polynomials f, g in $\mathbb{Q}[X, Y]$ and some non-zero polynomial h in $\mathbb{Q}[X, Y]$, we have

$\mathcal{A} - (X^n + Y^n - 1)h = fg$. Since $h = 0$ is ruled out by the assumption that $\mathcal{A} \in \mathrm{Irr}(\mathbb{Q}[X,Y])$, we choose h to have the minimal possible degree ≥ 0 amongst all f, g, h that satisfy (3.1).

Write f, g, and h as sums of their respective homogeneous parts as in the *adjustment*; hence $f_M g_P h_D \neq 0$. If $(X^n + Y^n) \mid f_M$, then in the adjustment, $F = X^n + Y^n$, $G = 1$, $K = M$, and $L = 0$. Hence $g_\star = 0$ and $f_\star g_\star = 0$. Therefore, $\deg h$ is reduced. With $(F, f_\star)$ replaced by $(G, g_\star)$ we get the same conclusion if $(X^n + Y^n) \mid g_P$. We now address the situation where $X^n + Y^n$ divides neither f_M nor g_P. We have to find appropriate F and G with $X^n + Y^n = FG$ to which we can apply the adjustment.

Now $X^n + Y^n$ factors into elements in $\mathrm{Irr}(\mathbb{Q}[X,Y])$ each dividing $X^{2n} - Y^{2n}$. Let $\mathcal{L}$ be the factor with the largest degree; deg $\mathcal{L}$ is $\varphi(2n)$, where φ is the totient function. Since $-(X^n + Y^n)h_D = f_M g_P$, we may assume that $\mathcal{L}$ divides f_M after possibly reversing f and g. Let $F = \gcd(f_M, X^n + Y^n)$, so $\mathcal{L} \mid F$. We now get $\varphi(2n) \leq \deg F \leq M$. Then $X^n + Y^n = FG$, where $G \notin \mathbb{Q}$ because $X^n + Y^n$ does not divide f_M. Since $X^n + Y^n$ has no repeated roots, G is relatively prime to f_M. Hence $G \mid g_P$.

Case 1: $D \geq n$. In (3.1), $\deg \mathcal{A} < n$, $\deg h = D$. Hence the following comparison of homogeneous terms of degree $h > D$ involves only terms of $(X^n + Y^n)h$:

$$\begin{aligned}
-(X^n + Y^n)h_D &= f_M g_P, \\
-(X^n + Y^n)h_{D-1} &= f_M g_{P-1} + f_{M-1} g_P, \\
&\vdots \\
-(X^n + Y^n)h_{D-n+1} &= \\
& f_M g_{P-n+1} + f_{M-1} g_{P-n+2} + \cdots + f_{M-n+1} g_P.
\end{aligned} \tag{3.4}$$

Starting from $G \mid g_P$ and the fact that G and f_M are relatively prime, we deduce from $-(X^n + Y^n)h_{D-1} = f_M g_{P-1} + f_{M-1} g_P$ that $G \mid g_{P-1}$. Working down (3.4) we find by induction that $G \mid g_{P-i}$, $i = 0, 1, \ldots, n-1$. Now back to the adjustment with $L = P - n + 1$ and $K = M$ from $f \mid f_M$, we have $n + D = M + P$ and $K + L - 2 = M + P - n + 1 - 2 = D - 1 < D$. The adjustment has lowered $\deg h$. We have thus proved that Case 1 is untenable. Therefore, $D < n$.

Case 2: $D \geq a = \deg \mathcal{A}$. We now have $D < n$. We examine terms of degree $> D$. The last equation in (3.5) compares terms of homogeneous degree equal to $D + 1$. Again since $\deg \mathcal{A} \leq D$ and deg $h = D < n$, only terms of $(X^n + Y^n)h$ are involved in (3.5):

$$
\begin{aligned}
-(X^n+Y^n)h_D &= f_M g_P,\\
-(X^n+Y^n)h_{D-1} &= f_M g_{P-1} + f_{M-1} g_P,\\
&\ \vdots\\
-(X^n+Y^n)h_0 &= f_M g_{P-D} + f_{M-1} g_{P-D+1} + \cdots + f_{M-D} g_P,\\
0 &= f_M g_{P-D-1} + \cdots + f_{M-D-1} g_P,\\
&\ \vdots\\
0 &= f_M g_{P-n+1} + \cdots + f_{M-n+1} g_P.
\end{aligned} \tag{3.5}
$$

Replacing (3.4) with (3.5), we deduce as in Case 1 that D has been lowered. This time we conclude that $D < a = \deg \mathcal{A}$. Since $a < n$, we recover $D < n$.

Case 3: $\deg f = M > a$. We now also have $D < a$. Then $n - P = M - D > M - a$. Since $0 < M - D = n - P$, we get $P < n$ and $P - n + 1 \le 0$.

Now we consider terms of homogeneous degree $> a$. Since $D < a$, only terms of $(X^n + Y^n)h$ contribute to the analogue of (3.5) whose last line is $0 = f_M g_{a+1-M} + \cdots + f_{a+1-P} g_P$. Just as in Case 1, we find by induction that $G \mid g_P, \ldots, G \mid g_{a+1-M}$.

Next we consider the degree a. Since $a > D$, h does not contribute any terms. We have $Y^a = f_M g_{a-M} + f_{M-1} g_{a+1-M} + \cdots + f_{a-P} g_P$. Now, $G \mid g_{a+1-M}, \ldots, G \mid g_P$, and G does not divide Y^a because as a non-constant divisor of $X^n + Y^n$, G has X-terms. Therefore, G does not divide $f_M g_{a-M}$. Hence $g_{a-M} \neq 0$ and $a - M \geq 0$, contradicting $M > a$. Hence $M \le a$.

Bearing in mind that $F \mid f_M$, $\deg F \ge \varphi(2n)$, and that the degree of every irreducible factor of $Y^n - 1$ is bounded by $\varphi(n)$, we obtain the following inequalities from the three cases: $M \le a \le \varphi(n) \le \varphi(2n) \le \deg F \le M$. Hence each of the inequalities is an equality.

We draw the following conclusions, called the Adjustment Lemma, from these equalities.

Adjustment Lemma. *In the above circumstances, we have $\varphi(n) = \varphi(2n) = M$. Hence n is odd. Moreover, $f_M = cF$ for some $c \in \mathrm{U}(\mathbb{Q})$, $F = \mathcal{L}$, and $a = \varphi(n)$ implies that $\mathcal{A}$ is the cyclotomic polynomial of order n. Moreover, F is the irreducible factor of $X^n + Y^n$ of degree $\varphi(2n) = \varphi(2n)$.*

Case 4: *Examining terms of degree $> a = \deg \mathcal{A} > D = \deg h$.* Neither h nor $\mathcal{A}$ contributes to these terms because their degrees are less than a. We consider

$$\begin{aligned}
-(X^n+Y^n)h_D &= f_M g_P,\\
-(X^n+Y^n)h_{D-1} &= f_M g_{P-1} + f_{M-1} g_P,\\
&\vdots\\
-(X^n+Y^n)h_0 &= f_M g_{P-D} + f_{M-1} g_{P-D+1} + \cdots + f_{M-D} g_P,\\
0 &= f_M g P - D - 1 + \cdots + f_{M-D-1} g_P,\\
&\vdots\\
0 &= f_M g_1 + \cdots + f_{M-P+1} g_P.
\end{aligned} \tag{3.6}$$

As in Case 1 we get $G \mid g_P, \dots, G \mid g_1$. We now turn our attention to F. First, $F \in \mathrm{Irr}(\mathbb{Q}[X,Y])$ as in the Adjustment Lemma. Suppose $F \mid g_P$. Since F and G are relatively prime and $G \mid g_P$, we conclude that $X^n + Y^n = FG$ divides g_P. Since $P = \deg G$, this is not possible. So F does not divide g_P. We deduce from the first equation in (3.6) that $F \mid f_M$. By an analogous induction argument to that for G, we find that $F \mid f_M, \dots, F \mid f_{M-P+1}$. Now we use $K = M - P + 1$ and $L = 1$ for the adjustment of D. This will reduce D if $M - P + 1 + 1 - 2 = M - P < D$. Therefore, by minimality of D, we get $D \le M - P$. Since $D \ge 0$ we have $M \ge P$.

Using the Adjustment Lemma and $n + D = M + P$ we get $(n+D)+D \le (M+P)+(M-P)$. So $2D \le 2M - n$. Hence $D \le M - n/2 = \varphi(n) - n/2$. In particular,

$$\deg \mathcal{A} = a = \varphi(n) \ge n/2.$$

In order to obtain information on $\varphi(n)$, we let $p_1, \dots, p_k$ be the distinct prime divisors of n. Then $(p_1-1)\cdots(p_k-1) \le p_1 \cdots p_k - 1$. Hence $2(p_1-1)\cdots(p_k-1) - p_1\cdots p_k \le (p_1-1)\cdots(p_k-1) - 1$. Multiply the last inequality by $n/\mathrm{rad}(n)$ to get $2\varphi(n) - n \le \varphi(n) - n/\mathrm{rad}(n)$.

Recalling that $h = 0$ was ruled out at the start of the proof, we have $D \ge 0$ in $P + M = n + D$. Since $M = \varphi(n)$, we have $P - D = n - \varphi(n)$. Hence

$$\begin{aligned}
&D \le \varphi(n) - n/2 \le l/2,\\
&P \ge n - \varphi(n),\\
&M - P = \varphi(n) - P \le 2\varphi(n) - n \le l.
\end{aligned} \tag{3.7}$$

Recall that the second non-zero term of $\mathcal{A}$ occurs at degree l by Proposition 3.5. In the comparison of the non-zero term of degree l only $\mathcal{A}$ contributes because $l < n$ and $D \le \varphi(n) - n/2$. Now examining the non-zero term of degree l, we get

$$\begin{aligned}
\alpha Y^l &= f_M g_{l-M} + f_{M-1} g_{l-M+1} + \cdots + f_l g_0 + \cdots + f_{l-P} g_P\\
&= f_l g_0 + \cdots + f_{l-P} g_P,
\end{aligned}$$

using $g_{l-M+i} = 0$ when $l - M + i < 0$. Since $G \mid g_1, \dots, G \mid g_P$, the left-hand side is not divisible by G but every term of the right-hand side except $f_l g_0$ is divisible by G. In fact if G divides $f_l g_0$ then it would divide αY^l and it does not. Hence $f_l \neq 0$. But F divides $f_M, f_{M-1}, \dots, f_{M-P+1}$ and F does not divide αY^l. Hence $l \leq M - P$. Combining this with (3.7) we find that $M - P = l = \varphi(n) - n/\mathrm{rad}(n)$, $M - P = 2\varphi(n) - n$, $P = n - \varphi(n)$. From $M + P = n + D$, we conclude that $D = 0$.

Consequently, (3.1) assumes the form $\mathcal{A} - (X^n + Y^n - 1)h_0 = -X^n h_0 + [\mathcal{A} - (Y^n - 1)h_0]$. Recall that we already have $\phi(n) = \deg \mathcal{A} \geq n/2$, n odd. Hence $\phi(n) \geq (n+1)/2$. We have $\deg \mathcal{A}^2 = 2\varphi(n) \geq n+1 > \deg(\mathcal{A} - (Y^n - 1)h_0)$. Since $\mathcal{A}$ divides $Y^n - 1$, we deduce from Eisenstein's criterion that $X^n h_0 + [\mathcal{A} - (Y^n - 1)h_0]$ is in $\mathrm{Irr}(\mathbb{Q}[Y][X])$. Hence either f or g is in $\mathrm{U}(R)$. By the *adjustment*, any other f, g are associates. Therefore $\mathcal{A}$ is in $\mathrm{Irr}(R)$.

This finishes the proof of Theorem 3.6. ∎

THEOREM 3.7. *If $\mathbb{Q}[X,Y]/\langle X^n + Y^n - 1\rangle$ is factorial, then n is at most two.*

Proof. We have $X^n + I = (1 - Y^n) + I$. If $n \geq 3$, the left-hand side has length a multiple of n, and the right-hand side has length $< n$ by Theorem 3.6. Hence $R = \mathbb{Q}[X,Y]/\langle X^n + Y^n - 1\rangle$ is not factorial by Lemma 3.1. ∎

4. Factorial Fermat curves. We proved in the last section that a Fermat curve of degree at least three is not factorial. We did so by showing that for some element x in the coordinate ring R, we have $x = x_1 \cdots x_m = y_1 \cdots y_n$, where $\{x_1, \dots, x_m, y_1, \dots y_n\} \subseteq \mathrm{Irr}(R)$ and $m \neq n$. In other words, R is not even half-factorial. In the notation of Section 3, R is half-factorial if and only if $|L(x)| = 1$ for all x in $R - (\mathrm{U}(R) \cup \{0\})$. Half-factoriality now has a wide scope (see [GKR], [GP], [KR], [PS1], and [PS2]). Examples of half-factorial domains are in [R] in the context of composition of polynomials, pre-dating the introduction of the terminology *half-factorial* by fifty-eight years. If $f = g \circ h$, we say that we have a *decomposition* of f. We refer to [GS] for counterexamples to Ritt's theorem for rational functions. It is noted in [GS] that the function

$$f = \frac{X^3(X+6)^3(X^2 - 6X + 36)^3}{(X-3)^3(X^2+3X+9)^3} \quad \text{in } \mathbb{Q}(X)$$

arises in the context of *Monstrous Moonshine*. It is shown that f has two decompositions of lengths 4 and 2. The problem of complete decomposition of rational functions seems to be related to the open problem of classes of rational functions which commute with respect to composition, as noted in the review of [GS] by Carlos D'Andrea.

We now return to the focus of our paper. In this section we show that the Fermat curves of degree two are at least half-factorial, while a linear change of variables tells us that a Fermat curve of degree one is factorial.

PROPOSITION 4.1.

(a) ([F, Theorem 8.1]) *Let A be a Krull domain and X an indeterminate. Then* $\mathrm{Cl}(A) = \mathrm{Cl}(A[X])$.
(b) ([F, Corollary 7.3]) *Let S be a multiplicatively closed subset of a domain A. If S is generated by prime elements, then* $\mathrm{Cl}(A)=\mathrm{Cl}(S^{-1}A)$.

Here is the main theorem of this section.

THEOREM 4.2.

(a) $X^2+Y^2+Z^2$ *is factorial.*
(b) $X^2+Y^2-Z^2$ *is half-factorial, but not factorial.*
(c) X^2+Y^2-1 *is half-factorial, but not factorial.*
(d) X^2+Y^2 *is half-factorial, but not factorial.*

Proof. (a) follows from Theorem 1.1, while (b) follows from Theorem 1.1 and [Z, Theorem 2.4] already quoted in the Introduction.

(c) We adapt to $\mathbb{Q}$ the argument used in [F, Proposition 11.8] for $\mathbb{R}$. Let X, Y, T be algebraically independent indeterminates. Consider $R = \mathbb{Q}[X,Y]/\langle X^2+Y^2-1\rangle$. Then using Proposition 4.1 and Theorem 1.1, we get $\mathrm{Cl}(R) = \mathrm{Cl}(\mathbb{Q}[X,Y,T]/\langle X^2+Y^2-1\rangle) = \mathrm{Cl}(\mathbb{Q}[X,Y,T,T^{-1}]/\langle X^2+Y^2-1\rangle) = \mathrm{Cl}(\mathbb{Q}[XT,YT,T]/\langle (XT)^2+(YT)^2-T^2\rangle) = \mathbb{Z}/2\mathbb{Z}$. Theorem 2.4 of [Z] then gives us (c).

(d) We observe that $R = \mathbb{Q}[X,Y]/\langle X^2+Y^2\rangle \cong \mathbb{Q}+X\mathbb{Q}[i][X]$, $i^2=-1$. Since R is not integrally closed, it is not factorial. However R is half-factorial (see for instance [AAZ, Theorem 5.3] or [MO4, Proposition 1.4]). ∎

The following theorem summarizes our results on Fermat curves.

THEOREM 4.3. *Let f be a polynomial in the set $\{X^n+Y^n, X^n+Y^n-Z^n, X^n+Y^n+Z^n, X^n+Y^n-1\}$. Then the corresponding coordinate ring over $\mathbb{Q}$ of f is half-factorial if and only if n is one or two.*

The proof of Theorem 4.3 goes through to give the following proposition.

PROPOSITION 4.4. *Let* $c \in \mathrm{U}(\mathbb{Q})$.

(a) *If the polynomial $cX^n+Y^n-Z^n$ is half-factorial, then n is one or two.*
(b) *If n is not a power of two, then the polynomial $X^n+Y^n+cZ^n$ is not half-factorial.*

For convenience, we call $aX^3+bY^3+cZ^3$, where a, b, c are non-zero integers, a *Selmer curve*. The Selmer curve $2X^3+3Y^3+5Z^3$ has rational points, unlike the famous Selmer curve $3X^3+4Y^3+5Z^3$. Proposition 4.4

tells us that $X^3+Y^3+abcZ^3$ is not half-factorial. We do not know whether an arbitrary Selmer curve is half-factorial.

Our methods are specific to homogeneous curves or non-homogeneous curves to which we can apply the *adjustment*. We can also handle non-homogeneous curves which can be made homogeneous by a suitable reassignment of degrees to the variables. We illustrate this procedure in Proposition 4.5.

PROPOSITION 4.5. *The polynomial* $\mathcal{P} = Y(Y-d)-(X-a)(X-b)(X-c)$, *where* $\{a,b,c,d\} \subseteq \mathbb{Q}$, *is not half-factorial.*

Proof. We have $\mathcal{P} = Y^2 - X^3 - g(X,Y)$ where $\deg g(X,Y) \leq 2$. Change the degree function so that $\deg Y = 3$ and $\deg X = 2$. Then $Y^2 - X^3$ is the homogeneous leading term of $\mathcal{P}$ and is in $\mathrm{Irr}(\mathbb{Q})$. We then deduce from the equation $Y(Y-d)+I = (X-a)(X-b)(X-c)+I$ and Proposition 2.4 that $|L(Y(Y-d)+I)| > 1$. Hence $\mathcal{P}$ is not half-factorial. ∎

Acknowledgements. We gratefully acknowledge conversations with W. Fulton and David Eisenbud, and e-mail exchanges with D. McKinnon of the University of Waterloo, about geometric criteria for irreducibility in coordinate rings. We thank the referee for giving us helpful suggestions.

REFERENCES

[AAZ] D. D. Anderson, D. F. Anderson, and M. Zafrullah, *Rings between* $D[X]$ *and* $K[X]$, Houston J. Math. 17 (1991), 109–129.

[BO] N. Bourbaki, *Elements of Mathematics. Commutative Algebra*, Addison-Wesley, Reading, MA, 1972.

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

[CMO] J. Coykendall, P. Malcolmson, and F. Okoh, *On fragility of generalizations of factoriality*, Comm. Algebra 41 (2013), 3355–3375.

[EI] D. Eisenbud, *Commutative Algebra. With a View Toward Algebraic Geometry*, Grad. Texts in Math. 150, Springer, New York, 1995.

[EMO] P. Etingof, P. Malcolmson, and F. Okoh, *Root extensions and factorization in affine domains*, Canad. Math. Bull. 53 (2010), 247–255.

[F] R. M. Fossum, *The Divisor Class Group of a Krull Domain*, Springer, Berlin, 1973.

[FU] W. Fulton, *Algebraic Curves. An Introduction to Algebraic Geometry*, Math. Lecture Notes Ser., W. A. Benjamin, New York, 1969.

[GH] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations*, Chapman & Hall, 2006.

[GKR] A. Geroldinger, F. Kainrath, and A. Reinhart, *Arithmetic of semi-normal weakly Krull domains*, J. Algebra, to appear.

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

[GP] R. V. Gurjar and S. Paul, *A classification of factorial domains of non-general type*, Michigan Math. J. 61 (2012), 517–529.

[GS] J. Gutierrez and D. Sevilla, *Building counterexamples to generalizations for rational functions of Ritt's decomposition theorem*, J. Algebra 303 (2006), 655–667.

[H] R. Hartshorne, *Algebraic Geometry*, Springer, New York, 1977.

[K] I. Kaplansky, *Commutative Rings*, Polygonal Publ. House, Washington, DC, 1994.

[KR] D. Kriz, *On a conjecture concerning the maximal cross number of unique factorization indexed sequences*, J. Number Theory 133 (2013), 3033–3056.

[L] S. Lang, *Algebra*, revised 3rd ed., Grad. Texts in Math. 211, Springer, New York, 2002.

[LY] B. R. Lynch, *Elasticity of Krull domains with infinite divisor class group*, Ph.D. thesis, Univ. of Tennessee, Knoxville, 2010.

[MO1] P. Malcolmson and F. Okoh, *Expansions of prime ideals*, Rocky Mountain J. Math. 35 (2005), 1689–1706.

[MO2] P. Malcolmson and F. Okoh, *A class of integral domains between factorial domains and IDF-domains*, Houston J. Math. 32 (2006), 399–421.

[MO3] P. Malcolmson and F. Okoh, *Power series extensions of half-factorial domains*, J. Pure Appl. Algebra 213 (2009), 493–495.

[MO4] P. Malcolmson and F. Okoh, *Factorization in subalgebras of the polynomial algebra*, Houston J. Math. 35 (2009), 991–1012.

[MO5] P. Malcolmson and F. Okoh, *Half-factorial subrings of factorial domains*, J. Pure Appl. Algebra, to appear.

[N] W. Narkiewicz, *Some unsolved problems*, Bull. Soc. Math. France 25 (1971), 159–164.

[PS1] A. J. Parameswaran and V. Srinivas, *A variant of the Noether–Lefschetz theorem: some new examples of unique factorisation domains*, J. Algebraic Geom. 3 (1994), 81–115.

[PS2] A. J. Parameswaran and V. Srinivas, *A variant of Noether normalisation*, Rend. Sem. Mat. Univ. Politec. Torino 48 (1990), 483–490.

[R] L. J. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. 23 (1922), 51–66, 431.

[S1] P. Samuel, *On unique factorization domains*, Illinois J. Math. 5 (1961), 1–17.

[S2] P. Samuel, *Lectures on unique factorization domains*, Tata Inst. Fund. Res. Lecture Notes Math. 30, Tata Inst. Fund. Res., Bombay, 1964.

[S3] P. Samuel, *Unique factorization*, Amer. Math. Monthly 75 (1968), 945–952.

[V] R. J. Valenza, *Elasticity of factorization in number fields*, J. Number Theory 36 (1990), 212–218.

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

Peter Malcolmson, Frank Okoh
Department of Mathematics
Wayne State University
Detroit, MI 48202, U.S.A.
E-mail: petem@math.wayne.edu
okoh@math.wayne.edu

Vasuvedan Srinivas
School of Mathematics
Tata Institute of Fundamental Research
Mumbai 400005, India
E-mail: srinivas@math.tifr.res.in

Received 28 January 2015;
revised 15 July 2015 (6526)