Available online at www.sciencedirect.com

ScienceDirect

Journal of Number Theory 121 (2006) 90–113

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

# Power integral bases for Selmer-like number fields

Louis J. Ratliff Jr. [a,*], David E. Rush [a], Kishor Shah [b]

[a] *Department of Mathematics, University of California, Riverside, CA 92521-0135, USA*
[b] *Department of Mathematics, Southwest Missouri University, Springfield, MO 65802, USA*

Received 21 June 2005; revised 7 November 2005

Available online 29 March 2006

Communicated by David Goss

## Abstract

The Selmer trinomials are the trinomials $f(X) \in \{X^n - X - 1, X^n + X + 1 \mid n > 1$ is an integer$\}$ over $\mathbb{Z}$. For these trinomials we show that the ideal $C = (f(X), f'(X))\mathbb{Z}[X]$ has height two and contains the linear polynomial $(n-1)X + n$. We then give several necessary and sufficient conditions for $D[X]/(f(X)D[X])$ to be a regular ring, where $f(X)$ is an arbitrary polynomial over a Dedekind domain $D$ such that its ideal $C$ has height two and contains a product of primitive linear polynomials. We next specialize to the Selmer-like trinomials $bX^n + cX + d$ and $bX^n + cX^{n-1} + d$ over $D$ and give several more such necessary and sufficient conditions (among them is that $C$ is a radical ideal). We then specialize to the Selmer trinomials over $\mathbb{Z}$ and give quite a few more such conditions (among them is that the discriminant $\operatorname{Disc}(X^n - X - 1) = \pm(n^n - (1-n)^{n-1})$ of $X^n - X - 1$ is square-free (respectively $\operatorname{Disc}(X^n + X + 1) = \pm(n^n + (1-n)^{n-1})$ of $X^n + X + 1$ is square-free)). Finally, we show that $n^n + (1-n)^{n-1}$ is never square-free when $n \equiv 2 \pmod 3$ and $n > 2$, but, otherwise, both are very often (but not always) square-free.

*MSC:* primary 12A40, 12E10, 12F05, 13F05, 13H05; secondary 12-04, 12B10

*Keywords:* Content of a polynomial; Dedekind domain; Discriminant; Mathematica program; Noetherian ring; Power integral basis; Prime ideal; Radical ideal; Ramify; Regular ring; Resultant; Selmer trinomial

[*] Corresponding author.
*E-mail addresses:* ratliff@math.ucr.edu (L.J. Ratliff Jr.), rush@math.ucr.edu (D.E. Rush), kis100f@smsu.edu (K. Shah).

0022-314X/$ – see front matter © 2006 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2006.01.012

## 1. Introduction

A classical and much studied question in algebraic number theory is to determine if the integers $\mathbb{Z}_K$ of a number field $K$ of degree $n$ has a basis over $\mathbb{Z}$ of the form $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Such a basis is called a *power integral basis* and if such a basis exists, $K$ is said to be *monogenic*. Among the advantages of having a power integral basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is that in this case, determining how a rational prime $p$ factors in $\mathbb{Z}_K$ reduces to factoring the minimal monic polynomial of $\alpha$ in $(\mathbb{Z}/p\mathbb{Z})[X]$. The monogeneity of quadratic and cyclotomic fields is classical, and more recent results on the existence of power integral bases have tended to focus on number fields of small degree, or number fields which are either abelian or very close to abelian. See, for example, [4,9] and the references listed there. In this note we consider the monogeneity of number fields which arise from the polynomials $s_{n,1,-1,-1}(X) = X^n - X - 1$ and $s_{n,1,1,1}(X) = X^n + X + 1$ considered by Selmer [14]. He proved in [14, Theorem 1] that the $s_{n,1,-1,-1}(X)$ are irreducible over $\mathbb{Z}$ and, for $n \not\equiv 2 \pmod 3$, the $s_{n,1,1,1}(X)$ are irreducible over $\mathbb{Z}$, as is $s_{2,1,1,1}(X) = X^2 + X + 1$, but for $n \equiv 2 \pmod 3$ and $n \neq 2$ the $s_{n,1,1,1}(X)$ are each the product of $s_{2,1,1,1}(X)$ and one other irreducible polynomial. The fields $\mathbb{Q}[X]/(s_{n,1,-1,-1}(X)\mathbb{Q}[X])$ (respectively, $\mathbb{Q}[X]/(s_{n,1,1,1}(X)\mathbb{Q}[X])$) are far from abelian in that $X^n - X - 1$ has Galois group $S_n$, as does $X^n + X + 1$ for $n \not\equiv 2 \pmod 3$ [10, Theorem 1].

Some of these trinomials are well known in other contexts. For example $s_{2,1,-1,-1}(X) = X^2 - X - 1$ is the characteristic polynomial of the Fibonacci and Lucas sequences [7,16] and, of course, its positive root is the golden ratio. Similarly $s_{3,1,-1,-1}(X) = X^3 - X - 1$ is the characteristic polynomial of recurrence sequences that have been considered by several authors in relation to certain primality tests (for example, see [1,3,11]). The positive root of $X^3 - X - 1$ is sometimes called the plastic number, and in [16] it is shown that it has some properties which are analogous to properties of the golden ratio. The density of the set of rational primes $\pi$ such that $s_{n,1,-1,-1}(X) = X^n - X - 1$ has a linear factor in $(\mathbb{Z}/\pi\mathbb{Z})[X]$ was considered in [15], especially for $n = 2$, 3, and 4.

In the following, we study the structure of $\mathbb{Z}[X]/(s_{n,1,-1,-1}(X)) = \mathbb{Z}[x]$ and some related extension rings. To describe our results further, we recall some facts concerning the discriminant (see, for example, [13, Theorem 1, pp. 38–41, 73–76]). Recall that if the commutative ring $B$ is a free module of rank $n$ over its subring $A$, which we assume for now to be a principal ideal domain, and $(x_1, \ldots, x_n) \in B^n$, then the *discriminant of* $(x_1, \ldots, x_n)$ is defined as $\mathrm{Disc}(x_1, \ldots, x_n) = \det(\mathrm{Tr}_{B/A}(x_i x_j))$, where det denotes determinant and $\mathrm{Tr}_{B/A}(y)$ denotes the trace of the multiplication map $y : B \to B$ for $y \in B$. If $(y_1, \ldots, y_n) \in B^n$ and $y_i = \sum_{j=1}^n a_{i,j} x_j$, then $\mathrm{Disc}(y_1, \ldots, y_n) = \det(a_{ij})^2 \mathrm{Disc}(x_1, \ldots, x_n)$. It follows that if $(x_1, \ldots, x_n)$ is a basis of $B$, then $(y_1, \ldots, y_n)$ is a basis of $B$ if and only if $\mathrm{Disc}(x_1, \ldots, x_n)$ and $\mathrm{Disc}(y_1, \ldots, y_n)$ are associates. Further, if $(y_1, \ldots, y_n)$ is not a basis of $B$, then $\mathrm{Disc}(y_1, \ldots, y_n)$ is divisible by a square. Thus the square-freeness of the integer $\mathrm{Disc}(y_1, \ldots, y_n)$ is a sufficient condition for $(y_1, \ldots, y_n)$ to be a $\mathbb{Z}$-basis for $B$, but it is not a necessary condition.

In the case that $B = A[X]/(f(X)A[X]) = A[x]$ for a monic $f(X) \in A[X]$ of degree $n$, it turns out that $\mathrm{Disc}(1, x, \ldots, x^{n-1}) = \mathbf{Disc(f(x))}$ (= the discriminant of the polynomial $f(X)$ evaluated at $x$). Among our characterizations of when $\mathbb{Z}[X]/(s_{n,1,-1,-1}(X))$ is regular (equivalently, integrally closed) is $\mathrm{Disc}(1, x, \ldots, x^{n-1})$ is square-free. We are then able to show that $\mathrm{Disc}(1, x, \ldots, x^{n-1})$ is not square-free for some $s_{n,1,-1,-1}(X)$.

Instead of working inside of an algebraic number field $L = \mathbb{Q}(\theta)$, where $\theta$ is a root of an irreducible monic $f(X) \in \mathbb{Q}[X]$, and considering when $\{1, \theta, \ldots, \theta^{n-1}\}$ is a $\mathbb{Z}$-basis for the integers $\mathbb{Z}_L$ of $L$, we work directly with rings of the form $B = A[X]/(f(X)A[X])$ and derive conditions for $B$ to be regular, since some of our results do not require that $f(X)$ be either irreducible or monic. However, in (4.5) we give several necessary and sufficient conditions for $\{1, \alpha, \dots, \alpha^{n-1}\}$ to be a power integral basis for the integers of $\mathbb{Q}(\alpha)$, when $\alpha$ is a root of $f(X) = X^n - X - 1$, and the analogous result for $\alpha$ a root of $f(X) = X^n + X + 1$ is given in (5.21).

In Section 2 we give (in (2.6) and (2.8)) several necessary and sufficient conditions for the extension ring $D[X]/(f(X)D[X])$ of $D$ to be a regular ring, where $f(X)$ is a polynomial (with coefficients in a Dedekind domain $D$) that has the following property in common with the Selmer trinomials: $C = (f(X), f'(X))D[X]$ is a height two ideal that contains a product of primitive polynomials of degree one in $D[X]$ (here, $f'(X)$ is the derivative of $f(X)$). Then in Section 3 we apply (2.6) to the Selmer-like trinomials $s_{n,b,c,d}(X) = bX^n + cX + d$ and $t_{n,b,c,d}(X) = bX^n + cX^{n-1} + d$ (with $b, c, d$ arbitrary nonzero elements in $D$). In Section 4 we specialize the results in Sections 2 and 3 to the Selmer trinomials $s_{n,1,-1,-1}(X)$ over $D = \mathbb{Z}$, and for each integer $n \geqslant 2$ we give quite a few additional necessary and sufficient conditions for $\mathbb{Z}[X]/(s_{n,1,-1,-1}(X)\mathbb{Z}[X])$ to be a Dedekind domain; among them is that $\operatorname{Disc}(s_{n,1,-1,-1}(X)) = \pm(n^n - (1-n)^{n-1})$ is square-free. In Section 5 we show that the analogous necessary and sufficient conditions apply for $\mathbb{Z}[X]/(s_{n,1,1,1}(X)\mathbb{Z}[X])$ to be a Dedekind domain, and then show that, for all positive integers $n$ of the form $3k+2$, $\operatorname{Disc}(s_{n,1,1,1}(X)) = \pm(n^n + (1-n)^{n-1})$ is *never* square-free.

## 2. On the regularity of Selmer-like extensions

The main results in this section, (2.6) and (2.8), give several necessary and sufficient conditions for $D[x] = D[X]/(f(X)D[X])$ to be a regular ring. (Recall that a ring $R$ is said to be a *regular ring*, in case $R$ is a Noetherian ring and $R_p$ is a regular local domain for each maximal ideal $p$ of $R$; however, $R$ need not be an integral domain.) Here, $f(X)$ is a polynomial (not necessarily monic) with a certain property in common with the Selmer-like trinomials $bX^n + cX + d$ and $bX^n + cX^{n-1} + d$ (where $b, c, d$ are nonzero elements in a Dedekind domain $D$). To prove (2.6) and (2.8), we need to prove several preliminary results. For the first of these, (2.1.2) is a slight variation of the main result of [2].

**Proposition 2.1.** *Let $R$ be a regular ring and let $f(X)$ be a nonzero divisor in $R[X]$. Then the following hold*:

(2.1.1) *If $f'(X) \neq 0$, where $f'(X)$ is the derivative of $f(X)$, then $R[X, \frac{1}{f'(X)}]/(f(X)R[X, \frac{1}{f'(X)}])$ is a regular ring.*

(2.1.2) *$R[X]/(f(X)R[X])$ is a regular ring if and only if $f(X) \notin M^2$ for each maximal ideal $M$ of $R[X]$.*

**Proof.** (2.1.1) follows from [12, Proposition II.8] and [12, p. 75, Exercise].

For (2.1.2), assume first that $f(X) \in M^2$ for some maximal ideal $M$ of $R[X]$. Then $f(X) \in M^2R[X]_M$, so $R[X]_M/(f(X)R[X]_M)$ is not a regular ring, by [8, (25.18)], hence $R[X]/(f(X)R[X])$ is not a regular ring.

For the converse, assume that $f(X) \notin M^2$ for each maximal ideal $M$ of $R[X]$. Then $f(X) \notin M^2R[X]_M$ for each maximal ideal $M$ of $R[X]$, since $M^2$ is primary (so $M^2 = M^2R[X]_M \cap R[X]$). Therefore $R[X]_M/(f(X)R[X]_M)$ is a regular local domain for each maximal ideal $M$ of $R[X]$ that contains $f(X)$, by [8, (25.18)], hence $R[X]/(f(X)R[X])$ is a regular ring. □

**Corollary 2.2.** *Let $R$ be a regular ring, let $f(X)$ be a nonzero divisor in $R[X]$, and let $R[x] = R[X]/(f(X)R[X])$. Then the following hold*:

(2.2.1) *If $(f(X), f'(X))R[X] = R[X]$, then $R[x]$ is a regular ring.*
(2.2.2) *If $P$ is a prime ideal in $R[X]$ such that $f(X) \in P$ and $f'(X) \notin P$, then $R[x]_p$ is a regular local domain, where $p = P/(f(X)R[X])$.*
(2.2.3) *If* $\text{altitude}(R) = 1$ *and* $\text{ht}((f(X), f'(X))R[X]) = 2$, *then $R[x]_p$ is a regular local domain for all but finitely many maximal ideals $p$ of $R[x]$. In particular, if $p$ is a maximal ideal in $R[x]$ and $P$ is the pre-image in $R[X]$ of $p$, then $R[x]_p$ is not a regular local domain if and only if $f(X) \in P^2$.*

**Proof.** Parts (2.2.1) and (2.2.2) follow immediately from (2.1.1).

For (2.2.3), if $\text{altitude}(R) = 1$ and $\text{ht}((f(X), f'(X))R[X]) = 2$, then there are at most finitely many prime ideals in $R[X]$ that contain $(f(X), f'(X))R[X]$ (since $R$ (and hence $R[X]$) is Noetherian and $\text{altitude}(R[X]) = 2$). Also, if $P$ is a prime ideal in $R[X]$ such that $f(X) \in P$ and $f'(X) \notin P$, and if $p$ is the image in $R[x]$ of $P$, then $R[x]_p$ is a regular local domain, by (2.2.2). The first statement in (2.2.3) clearly follows from this, and the second statement follows from the proof of (2.1.2). □

In the following lemma and the remainder of this paper, we use $\mathbf{Res(g(X), h(X))}$ to denote the *resultant* of the polynomials $g(X)$ and $h(X)$.

**Lemma 2.3.** *Let $R$ be a Noetherian integral domain of altitude one, and let $g(X), h(X) \in R[X]$ with $(g(X), h(X))R[X] \nsubseteq pR[X]$ for any nonzero prime ideal $p$ of $R$. Then* $\text{ht}((g(X), h(X)) R[X]) = 2$ *if and only if* $\text{Res}(g(X), h(X))$ *is a nonzero nonunit of $R$. If these hold, then a maximal ideal $\pi$ of $R$ contains* $\text{Res}(g(X), h(X))$ *if and only if $\pi = P \cap R$ for some maximal ideal $P$ of $R[X]$ that contains $(g(X), h(X))R[X]$.*

**Proof.** Let $K$ be the quotient field of $R$ and assume $\text{ht}((g(X), h(X))R[X]) = 2$. Then since $\text{Res}(g(X), h(X)) \in (g(X), h(X))R[X]$, $\text{Res}(g(X), h(X))$ is not a unit of $R$. If $\text{Res}(g(X), h(X)) = 0$, then $g(X)$ and $h(X)$ have a common root $\alpha$ in some extension field of $K$, by [6, Corollary 8.4, p. 203]. Then the minimal monic polynomial $f(X) \in K[X]$ of $\alpha$ is a common factor of $g(X)$ and $h(X)$ in $K[X]$, and $f(X)K[X] \cap R[X]$ is a height one prime ideal of $R[X]$ containing $(g(X), h(X))R[X]$, by [5, Theorems 39 and 149], contradicting $\text{ht}((g(X), h(X))R[X]) = 2$. Thus $\text{Res}(g(X), h(X))$ is a nonzero nonunit of $R$.

Conversely, if $\text{Res}(g(X), h(X)) \in \pi$ for some maximal ideal $\pi$ of $R$, then the images $\bar{g}(X)$ and $\bar{h}(X)$ in $(R/\pi)[X]$ of $g(X)$ and $h(X)$ have a common irreducible factor $\overline{f}(X)$ in $(R/\pi)[X]$, for some $f(X) \in R[X]$. Then $(\pi, f(X))R[X] = P$ is a height 2 prime ideal of $R[X]$ containing $(g(X), h(X))R[X]$. Further, every prime ideal $P$ of $R[X]$ containing $(g(X), h(X))R[X]$, must have $\text{Res}(g(X), h(X)) \in P \cap R = \pi$ (by [6, p. 202]). Thus each prime ideal containing $(g(X), h(X))R[X]$ must be of the form $P = (\pi, f(X))R[X]$, where $\pi$ is a maximal ideal of $R$ containing $\text{Res}(g(X), h(X))$ and $f(X) \in R[X]$ is such that its image $\overline{f}(X) \in (R/\pi)[X]$ is irreducible (so $\text{ht}(g(X), h(X))R[X] = 2$). □

**Remark 2.4.** Let $R$ and $g(X), h(X) \in R[X]$ be as in the above lemma. If $\text{Res}(g(X), h(X)) = 0$, then the first paragraph of the above proof shows that $(g(X), h(X))R[X]$ is contained in a height one prime ideal $P$ of $R[X]$ with $P \cap R = \{0\}$, so $\mathrm{ht}((g(X), h(X))R[X]) = 1$. If $\mathrm{Res}(g(X), h(X))$ is a unit of $R$, then clearly $(g(X), h(X))R[X] = R[X]$.

*For the remainder of this section and for Section* 3, *$D$ denotes a Dedekind domain which is not a field. For simplicity, we also assume $D$ has characteristic zero.* (Therefore $D[X]$ is a regular domain of altitude two. Also, $D[X]/(f(X)D[X])$ is a regular ring if and only if $D[X]/(f(X)D[X])$ is integrally closed, since $\mathrm{altitude}(D[X]/(f(X)D[X])) \leqslant 1$.)

If $f(X) = c_0 + c_1X + \cdots + c_nX^n \in D[X]$, we define the *content* $c_D(f(X))$ of $f(X)$ by $c_D(f(X)) = (c_0, c_1, \ldots, c_n)D$. If $H \subseteq D[X]$, we define the *content* $c_D(H)$ to be the ideal generated by $\{c_D(h(X)) \mid h(X) \in H\}$. It follows that if $I$ is an ideal of $D[X]$ generated by a set $H$, then $c_D(I) = c_D(H)$. If $c_D(f(X)) = D$, we say $f(X)$ *has content one* or is *primitive*, and similarly for an ideal $I$ of $D[X]$. It is clear that an ideal, or a polynomial has content one if and only if it is not contained in any prime ideal of the form $pD[X]$, where $p$ is a prime ideal of $D$. In particular, a product of primitive polynomials is primitive. Two elements or ideals of $D$ are said to be *coprime* if they generate the ideal $D$.

**Lemma 2.5.** *Let $I$ be an ideal of $D[X]$ of height* 2, *let $P_1, \ldots, P_e$ be the prime ideals in $D[X]$ that contain $I$, and let $\pi_i = P_i \cap D$ for $i = 1, \ldots, e$ (possibly $\pi_i = \pi_j$ for some $i \neq j$ in $\{1, \ldots, e\}$). Then the following are equivalent*:

(2.5.1) *$I$ contains a product $l_1(X) \cdots l_k(X)$ of primitive polynomials $l_j(X) = \alpha_jX + \beta_j$ of degree one (where $\alpha_j, \beta_j \in D$).*
(2.5.2) *The homomorphism $\varphi_i : D/\pi_i \to D[X]/P_i$ is an isomorphism for $i = 1, \ldots, e$.*
(2.5.3) *Each $P_i$ is of the form $(\pi_i, l_j(X))D[X] = (\pi_i, X - a_i)D[X]$ for some $j \in \{1, \ldots, e\}$ and for some $a_i \in D$. Further, for each $n \in \mathbb{N}$, we may choose the $a_i \in D$ such that $(\pi_i^n, l_j(X))D[X] = (\pi_i^n, X - a_i)D[X]$.*

**Proof.** (2.5.3) ⇒ (2.5.2) is clear.

For (2.5.2) ⇒ (2.5.1), fix $i \in \{1, \ldots, e\}$, so $\mathrm{ht}(P_i) = 2$ (since $\mathrm{ht}(I) = 2 = \mathrm{altitude}(D[X])$), hence $\pi_i \neq (0)$. Therefore $D[X]/P_i \cong D/\pi_i$ if and only if $X - a_i \in P_i$ for some $a_i \in D$. It follows that if $D[X]/P_i \cong D/\pi_i$ for $i = 1, \ldots, e$, then $[(X - a_1)\cdots(X - a_e)]^h \in I$ for all large integers $h$ (so $I$ contains a product of primitive polynomials of degree one).

For (2.5.1) ⇒ (2.5.3), assume that $l_1(X) \cdots l_k(X) \in I$, where $l_j(X) = \alpha_jX + \beta_j$ ($\alpha_j, \beta_j \in D$) is a primitive polynomial of degree one for $j = 1, \ldots, k$. If $X \in P_i$, then $X - a_i \in P_i$ for each $a_i \in \pi_i$, and it is clear that $P_i = (\pi_i, X - a_i)D[X]$ for each $a_i \in \pi_i$. Further, for each $n \in \mathbb{N}$, we have $(\pi_i^n, l_j(X))D[X] = (\pi_i^n, X - a_i)D[X]$ for each $a_i \in \pi_i^n$ in this case. On the other hand, if $X \notin P_i$, then $P_i$ contains some $l_j(X)$ (so $P_i = (\pi_i, l_j(X))D[X]$). Since $l_j(X) = \alpha_jX + \beta_j$, $\alpha_j, \beta_j$ must be coprime nonzero elements in $D$ such that $\alpha_j\beta_j \notin P_i$ (since $\alpha_jX + \beta_j$ is a primitive polynomial in $P_i$ and $X \notin P_i$). Thus since $\alpha_j \notin \pi_i$, we may write $1 = r + s_j\alpha_j$ (for some $r \in \pi_i^n$ and $s_j \in D \setminus \pi_i$) and let $a_i = -s_j\beta_j$. Then $s_jl_j(X) = s_j\alpha_jX + s_j\beta_j \equiv X - a_i \mod \pi_i^n$. Therefore (2.5.3) holds. □

In the next theorem we use the following: [6, Eq. (2), p. 203],

$$\mathrm{Res}\big(\alpha X + \beta, f(X)\big) = \alpha^n f\left(\frac{-\beta}{\alpha}\right),$$
$$\text{where } \mathrm{Deg}\big(f(X)\big) = n \text{ and } \alpha \neq 0,\ \beta \in D. \qquad (*\mathrm{Res})$$

**Theorem 2.6.** *Let $f(X) = c_nX^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0 \in D[X]$ be a polynomial of degree $n \geqslant 2$ such that $c_0 \neq 0$, and let $C = (f(X), f'(X))D[X]$. Assume that* $\operatorname{ht}(C) = 2$ *and that $C$ contains a product $l_1(X)l_2(X)\cdots l_k(X)$ of primitive polynomials $l_j(X) = \alpha_jX + \beta_j$ in $D[X]$ of degree one* (*where $\alpha_j, \beta_j \in D$*)*. Let $P_1, \dots, P_e$ be the associated prime ideals of $C$ and let $\pi_i = P_i \cap D$ for $i = 1, \dots, e$* (*possibly $\pi_i = \pi_j$ for some $i \neq j$*)*. Then $P_i = (\pi_i, l_j(X))D[X] = (\pi_i, X - a_i)D[X]$ for some $j \in \{1, \dots, k\}$ and for some $a_i \in D$ which we choose so that $(\pi_i^2, l_j(X))D[X] = (\pi_i^2, X - a_i)D[X]$. Also, $\pi_1, \dots, \pi_e$ are the associated prime ideals of* $\operatorname{Res}(f(X), f'(X))$. *Further, the following are equivalent for each $i = 1, \dots, e$*:

(2.6.1) *$D[x]_{p_i}$ is a regular local domain, where $D[x] = D[X]/(f(X)D[X])$ and $p_i = P_i/(f(X)D[X])$.*
(2.6.2) *$f(X) \notin P_i^2$.*
(2.6.3) *$f(a_i) \notin \pi_i^2$.*
(2.6.4) $\operatorname{Res}(l_j(X), f(X)) \notin \pi_i^2$.

**Proof.** (2.5.1) ⇒ (2.5.3) shows that each $P_i$ has the form $(\pi_i, \alpha_jX + \beta_j)D[X] = (\pi_i, X - a_i)D[X]$. Also, it follows from (2.3) that $\pi_1, \dots, \pi_e$ are the associated prime ideals of $\operatorname{Res}(f(X), f'(X))$.

(2.6.1) ⇔ (2.6.2), by (2.2.3).

(2.6.2) ⇔ (2.6.3). Since $f(X)$ and $f'(X)$ are in $C \subseteq P_i = (\pi_i, X - a_i)D[X]$, it follows that, modulo $\pi_iD[X]$, their residue classes have $\overline{a_i}$ as a root (where the overline denotes residue class modulo $\pi_i$). Therefore there exists a polynomial $\bar{q}_2(X)$ (of degree $n-2$) in $(D/\pi_i)[X]$ such that

$$\overline{f}(X) = (X - \overline{a_i})^2\bar{q}_2(X) \tag{2.6)(*}$$

(by [6, Proposition 1.11, p. 179]). By the division algorithm in $D[X]$, there exists a polynomial $q_1(X)$ (of degree $n-1$) in $D[X]$ such that

$$f(X) = (X - a_i)q_1(X) + f(a_i). \tag{2.6)(**}$$

By reducing the coefficients of this equation modulo $\pi_i$, it follows from (2.6)(∗) that $\overline{f(a_i)} \in ((X - \overline{a_i})(D/\pi_i)[X]) \cap (D/\pi_i) = (0)$. So $f(a_i) \in \pi_i$ and hence the residue class in $(D/\pi_i)[X]$ of $q_1(X)$ is $(X - \overline{a_i})\bar{q}_2(X)$ (by (2.6)(∗)). Therefore $q_1(X) \in (\pi_i, X - a_i)D[X]$, so $(X - a_i)q_1(X) \in P_i^2$. Therefore it follows from (2.6)(∗∗) that $f(X) \notin P_i^2$ if and only if $f(a_i) \notin P_i^2 \cap D = \pi_i^2$, hence (2.6.2) ⇔ (2.6.3).

(2.6.3) ⇔ (2.6.4). By (∗Res) (preceding this theorem), $\operatorname{Res}(X - a_i, f(X)) = f(a_i)$ and $\operatorname{Res}(\alpha_jX + \beta_j, f(X)) = \alpha_j^n f(\frac{-\beta_j}{\alpha_j})$. So we must show $f(a_i) \in \pi_i^2$ if and only if $\alpha_j^n f(\frac{-\beta_j}{\alpha_j}) \in \pi_i^2$.

Since $(\pi_i, \alpha_jX + \beta_j)D[X] = (\pi_i, X - a_j)D[X]$, $\alpha_j \notin \pi_i$. So we may write $1 = r + s_j\alpha_j$ (for some $r \in \pi_i^2$ and $s_j \in D \setminus \pi_iD$), and since $(\pi_i^2, X - a_i)D[X] = (\pi_i^2, \alpha_jX + \beta_j)D[X] = (\pi_i^2, s_j\alpha_jX + s_j\beta_j)D[X]$, we have $a_i \equiv -s_j\beta_j \pmod{\pi_i^2}$. Then $\alpha_j^n f(\frac{-\beta_j}{\alpha_j}) = c_n(-\beta_j)^n + c_{n-1}(-\beta_j)^{n-1}\alpha_j + c_{n-2}(-\beta_j)^{n-2}\alpha_j^2 + \cdots + c_0\alpha_j^n \in \pi_i^2 \Leftrightarrow s_j^n\alpha_j^n f(\frac{-\beta_j}{\alpha_j}) \in \pi_i^2$. But $s_j^n\alpha_j^n f(\frac{-\beta_j}{\alpha_j}) \equiv c_n(-s_j\beta_j)^n + c_{n-1}(-s_j\beta_j)^{n-1} + \cdots + c_0 \equiv f(a_i) \bmod \pi_i^2$. □

**Remark 2.7.** (2.7.1) It follows immediately from (2.2.2), (2.2.3), and (2.6) (and the fact that $C = (f(X), f'(X))D[X]$) that $D[x] = D[X]/(f(X)D[X])$ is a regular ring if and only if the equivalent statements (2.6.1)–(2.6.4) hold for $i = 1, \dots, e$.

(2.7.2) In (2.6), if $P_i = (\pi_i, X)D[X]$ (so we may assume that $a_i = 0$), then $c_0$ (the constant term of $f(X)$) is in $P_i$ (since $f(X) \in P_i$), so $c_0$ *must* be a nonunit in $D$ (nonzero by hypothesis). Therefore $f(a_i) = f(0) = c_0$, so it follows from (2.6.2) $\Leftrightarrow$ (2.6.3) that $f(X) \notin P_i^2$ if and only if $c_0 \notin \pi_i^2$. It follows that if $c_0$ is *square-free* in $D$ (that is, $c_0 \notin \pi^2$ for each nonzero prime ideal $\pi$ of $D$; in particular, every unit in $D$ is square-free), then $f(X) \notin P_i^2$ (so $D[x]_{p_i}$ is a regular local domain, by (2.6.1) $\Leftrightarrow$ (2.6.2)).
(2.7.3) Assume that $c_0$ is a unit in $D$. Then it follows from (2.7.2) that no $P_i$ $(i = 1, \dots, e)$ can contain $X$. Since $P_1, \dots, P_e$ are all the associated prime ideals of $C$, it follows that if $X^m l_1(X) \cdots l_h(X) \in C$ (with each $l_j(X)$ primitive in $D[X]$ of degree one and $m, h$ nonnegative integers), then $l_1(X) \cdots l_h(X) \in C$. In particular, the situation $c_0$ is a unit in $D$ and $h = 0$ (that is, $X^m \in C$ for some nonnegative integer $m$) cannot occur.
(2.7.4) Assume that $X^h \in C \neq D[X]$ for some positive integer $h$ and that $c_0$ is a square-free nonunit in $D$. Then it follows that $\operatorname{ht}(C) = 2$, and $C$ contains a product of primitive polynomials of degree one (since $X^h \in C$), so it follows from (2.7.2) and (2.7.1) that $D[x]$ is a regular ring.
(2.7.5) The hypothesis that $C$ contains a product of primitive polynomials in (2.6) implies that $f(X)$ is a primitive polynomial, since a product of primitive polynomials is primitive and $c_D(C) = c_D(f(X)) + c_D(f'(X)) = c_D(f(X))$. Thus by (2.3), the hypothesis in (2.6) that $\operatorname{ht}(C) = 2$ is equivalent to $\operatorname{Res}(f(X), f'(X))$ is a nonzero nonunit of $D$.
(2.7.6) Since $\operatorname{Res}(f(X), f'(X))$ is a "polynomial" $H(c_0, c_1, \dots, c_n)$ in the coefficients of $f(X)$, if each coefficient but one, say $c_j$, is fixed, then there will be only finitely many choices of $c_j$ for which $\operatorname{Res}(f(X), f'(X)) = 0$, and thus for which $\operatorname{ht}(C) = 1$. Further, if $D$ has only finitely many units, as in the case $D = \mathbb{Z}$ considered later, there will be only finitely many choices of $c_j$ for which $\operatorname{ht}(C) \neq 2$.
(2.7.7) In (2.6), if $f(X)$ is irreducible over the quotient field $K$ of $D$, then $f(X)$ and $f'(X)$ can have no common factor of positive degree. Therefore it follows from the other hypothesis in (2.6) and from (2.4) that either $C = D[X]$ or $\operatorname{ht}(C) = 2$.

Concerning the hypothesis "$l_1(X) \cdots l_k(X) \in C$" in (2.6), it is shown in Sections 4 and 5 that, for the Selmer trinomials $f(X) \in \{X^n - X - 1, X^n + X + 1\}$ over $\mathbb{Z}$, there is an irreducible polynomial of degree one in the ideal $C = (f(X), f'(X))\mathbb{Z}[X]$, and in this case there are quite a few additional necessary and sufficient conditions for $\mathbb{Z}[X]/(f(X)\mathbb{Z}[X])$ to be a regular ring (see (4.15) and (5.13)). In the next result we show that several of these conditions apply in the more general case that there is a product $l_1(X) \cdots l_k(X)$ of primitive linear polynomials $l_j(X)$ in $C$ such that each associated prime ideal of $C$ contains a unique factor $l_j(X)$. (This condition is stronger than the condition in (2.6): For example, $X^3 + 2$ satisfies the hypothesis of (2.6) over $D = \mathbb{Z}[1/3]$, but not the hypothesis of (2.8).)

**Theorem 2.8.** *With the notation of* (2.6), *assume that* $\operatorname{ht}(C) = 2$ *and that there exists a product* $l_1(X) \cdots l_k(X) \in C$ *of primitive polynomials* $l_j(X) = \alpha_j X + \beta_j$ *of degree one such that each of the associated prime ideals* $P_1, \dots, P_e$, *of* $C$ *contains a unique factor* $l_j(X)$ $(j \in \{1, \dots, k\})$. *Then for each* $i = 1, \dots, e$, *the following are equivalent*:

(2.8.1) $D[x]_{p_i}$ *is a regular local domain, where* $D[x] = D[X]/(f(X)D[X])$ *and* $p_i = P_i/(f(X)D[X])$.
(2.8.2) $C : \pi_i D[X] \nsubseteq P_i$.
(2.8.3) $CD[X]_{P_i} = P_i D[X]_{P_i}$.
(2.8.4) $f'(x)D[x]_{p_i} = p_i D[x]_{p_i}$, *where* $D[x] = D[X]/(f(X)D[X])$.

(2.8.5) $f(x')D[x']_{q_i} = q_i D[x']_{q_i}$, *where* $D[x'] = D[X]/(f'(X)D[X])$ *and* $q_i = P_i/(f'(X)D[X])$.

**Proof.** Assume (2.8.1) holds. Now $l_1(X)\cdots l_k(X) \in C \subseteq P_i$ and $l_j(X)$ is the only $l_h(X)$ that is in $P_i$ (by hypothesis), so it follows that $l_j(X) \in C_i^* = CD[X]_{P_i} \cap D[X] \subseteq P_i$. Therefore $l_j(X), f(X) \in C_i^*$, so $\rho_{i,j} = \mathrm{Res}(l_j(X), f(X)) \in C_i^* \cap D$ (by [6, p. 202]). Since $C_i^* \cap D \subseteq P_i \cap D = \pi_i$, it follows that $\rho_{i,j} \in \pi_i$. Also, $\rho_{i,j} \notin \pi_i^2$ (by (2.6.1) $\Rightarrow$ (2.6.4)), so it follows that $\rho_{i,j} D_{\pi_i} = \pi_i D_{\pi_i}$, hence $\pi_i D[X]_{P_i} = \rho_{i,j} D[X]_{P_i} \subseteq C_i^* D[X]_{P_i} = CD[X]_{P_i}$. Therefore $(C : \pi_i D[X])D[X]_{P_i} = CD[X]_{P_i} : \pi_i D[X]_{P_i} = D[X]_{P_i}$. Also, $P_i D[X]_{P_i} \neq D[X]_{P_i}$, so $C : \pi_i D[X] \nsubseteq P_i$, hence (2.8.1) $\Rightarrow$ (2.8.2).

Assume (2.8.2) holds, so it follows that $\sigma_i \in CD[X]_{P_i}$, where $\sigma_i$ is a generator of $\pi_i D_{\pi_i}$. Also, $l_1(X)\cdots l_k(X) \in C$ and $l_j(X)$ is the unique $l_h(X)$ that is in $P_i$ (by hypothesis), so it follows that $l_j(X) \in CD[X]_{P_i}$. Since $P_i = (\pi_i, l_j(X))D[X]$ and $\sigma_i D[X]_{P_i} = \pi_i D[X]_{P_i}$, it follows that $CD[X]_{P_i} = P_i D[X]_{P_i}$, hence (2.8.2) $\Rightarrow$ (2.8.3).

Since $C = (f(X), f'(X))D[X]$ and $D[x] = D[X]/(f(X)D[X])$ (respectively, $D[x'] = D[X]/(f'(X)D[X])$), it follows that (2.8.3) $\Rightarrow$ (2.8.4) (respectively, (2.8.3) $\Rightarrow$ (2.8.5)).

Finally, if (2.8.4) holds, then the height one maximal ideal $p_i D[x]_{p_i}$ is principal, so (2.8.4) $\Rightarrow$ (2.8.1). Similarly, (2.8.5) $\Rightarrow$ (2.8.1). □

For (2.9), recall that an ideal $I$ in a Noetherian ring $R$ is said to be a *radical ideal* in case $I$ is a finite intersection of prime ideals.

**Corollary 2.9.** *With the notation and hypothesis of* (2.8), $D[x]$ *is a regular ring if and only if* $C$ *is a radical ideal.*

**Proof.** Since $P_1, \ldots, P_e$ are all the associated prime ideals of $C$, this follows immediately from the definition of "radical ideal" and (2.8.1) $\Leftrightarrow$ (2.8.3) (and (2.7.1)). □

**Remark 2.10.** (2.10.1) It follows immediately from (2.8) (and (2.7.1)) that $D[x]$ is a regular ring if and only if $CD_S[X] \supseteq (\pi_1\cdots\pi_e, l_1(X)\cdots l_k(X))D_S[X]$, where $S = D \setminus (\pi_1 \cup \cdots \cup \pi_e)$. Also, if $CD[X]_{P_i} = P_i D[X]_{P_i}$, then since $(f(X), f'(X))D[X]_{P_i} = CD[X]_{P_i} = P_i D[X]_{P_i} = (\pi_i, l_j(X))D[X]_{P_i}$, it follows (by considering these equalities modulo $\pi_i D[X]_{P_i}$) that $(\pi_i, f'(X))D[X]_{P_i} = P_i D[X]_{P_i}$.

(2.10.2) Fix $i \in \{1, \ldots, e\}$ and resubscript the $P_i$ so that $P_1, \ldots, P_b$ are the prime ideals in $\{P_1, \ldots, P_e\}$ that lie over $\pi_i$. Also, resubscript the $l_h(X) = \alpha_h X + \beta_h$ so that $l_j(X)$ is the unique $l_h(X)$ that is in $P_j$ for $j \in \{1, \ldots, b\}$ (so these $l_j(X)$ are distinct and $P_j = (\pi_i, \alpha_j X + \beta_j)D[X]$). Then, since $(D/\pi_i)[X]$ is a UFD, let $\overline{f_1}(X), \ldots, \overline{f_d}(X)$ be distinct monic irreducible polynomials in $(D/\pi_i)[X]$ that are not an associate of $\overline{l_h}(X)$ $(h = 1, \ldots, b)$ and let $\bar{v}_i$ be a unit in $D/\pi_i$ such that

$$\overline{f}(X) = \bar{v}_i(\overline{\alpha_1}X + \overline{\beta_1})^{n_1}\cdots(\overline{\alpha_b}X + \overline{\beta_b})^{n_b}\big(\overline{f_1}(X)\big)^{m_1}\cdots\big(\overline{f_d}(X)\big)^{m_d}$$

is a factorization of $\overline{f}(X)$ into irreducible factors. Then it can be shown (as in the proof of (4.9) below) that $n_1 = \cdots = n_b = 2$ and $m_1 = \cdots = m_d = 1$.

## 3. Conditions for $D[X]/((bX^n + cX + d)D[X])$ to be regular

In this section we specialize (2.6) and (2.8) to the Selmer-like trinomials $s_{n,b,c,d}(X) = bX^n + cX + d$ and $t_{n,b,c,d}(X) = bX^n + cX^{n-1} + d$. (Of course, the $s$ in $s_{n,b,c,d}(X)$ is in honor of Selmer, and the $t$ in $t_{n,b,c,d}(X)$ is because these trinomials are obtained from the corresponding $s_{n,b,c,d}(X)$ by the transformation described in the last two paragraphs of the proof of (3.6).)

We begin by fixing the notation that will be used throughout this section. (It should be noted that the assumption "$C \neq D[X]$" in (3.1) is not a severe restriction for our purposes, since we want conditions for $D[x]$ to be a regular ring, and (2.2.1) shows that this holds if $C = D[X]$.)

**Notation 3.1.** Let $n \geqslant 2$ be a positive integer, let $b, c, d \in D \setminus \{0\}$, let $s_{n,b,c,d}(X) = bX^n + cX + d$ and $t_{n,b,c,d}(X) = bX^n + cX^{n-1} + d$, and let $D[x] = D[X]/(s_{n,b,c,d}(X)D[X])$. Let $l(X) = c(n-1)X + dn$, so $l(X) = Xs'_{n,b,c,d}(X) - ns_{n,b,c,d}(X) \in C = (s_{n,b,c,d}(X), s'_{n,b,c,d}(X))D[X]$. Assume that $C \neq D[X]$, let $P_1, \ldots, P_e$ be the associated prime ideals of $C$, and for $i = 1, \ldots, e$ let $\pi_i = P_i \cap D$ (possibly $\pi_i = (0)$ for some $i \in \{1, \ldots, e\}$ or $\pi_i = \pi_j$ for some $i \neq j \in \{1, \ldots, e\}$). Also, let $\rho_{n,b,c,d} = \operatorname{Res}(l(X), s_{n,b,c,d}(X))$, so $\rho_{n,b,c,d} = (c(n-1))^n s_{n,b,c,d}(\frac{-dn}{c(n-1)})$ (by ($*$Res) (preceding (2.6))) $= (c(n-1))^n[b(\frac{-dn}{c(n-1)})^n + c\frac{-dn}{c(n-1)} + d]$, so

$$\rho_{n,b,c,d} = b(-dn)^n - cd\big[c(n-1)\big]^{n-1}. \tag{3.1.1}$$

**Remark 3.2.** In order to apply (2.6) (and (2.8)) to the trinomials $s_{n,b,c,d}(X)$ we need to ensure that:

(i) $C$ contains a product of primitive polynomials in $D[X]$ of degree one; and,
(ii) $\operatorname{ht}(C) = 2$.

When (3.2)(i) and (ii) hold, several necessary and sufficient conditions for $D[x]$ to be a regular ring are given in (3.6). First, however, in (3.3) we show that the hypotheses of (3.6) "$b \notin c(n-1)D$, $(c(n-1), dn)D = D$, and $C \neq D[X]$" imply that (3.2)(i) and (ii) hold, and in (3.5.1) we show that the second of these implies that $\rho_{n,b,c,d}D_{\pi_i} = \operatorname{Disc}(s_{n,b,c,d}(X))D_{\pi_i}$ for $i = 1, \ldots, e$.

**Lemma 3.3.** *Assume that $b \notin c(n-1)D$ and that $(c(n-1), dn)D = D$. If $C \neq D[X]$, then conditions* (i) *and* (ii) *of* (3.2) *hold.*

**Proof.** The hypothesis $(c(n-1), dn)D = D$ shows that $l(X) = c(n-1)X + dn$ is primitive in $D[X]$ of degree one (since $c(n-1) \neq 0$), so (3.2)(i) holds (since $l(X) \in C$, by (3.1)).

For (3.2)(ii), by hypothesis $C \neq D[X]$, so $\operatorname{ht}(C) \in \{1, 2\}$. To see that $\operatorname{ht}(C) = 2$, note that it follows from $b \notin c(n-1)D$ that $s_{n,b,c,d}(X) \notin l(X)D[X]$. Since $l(X)D[X]$ is a prime ideal in $D[X]$ (it is well known and readily shown that a primitive polynomial of degree one over a Noetherian domain $R$ generates a prime ideal in $R[X]$), and since $(l(X), s_{n,b,c,d}(X))D[X] \subseteq C$ (by (3.1)), it follows that $\operatorname{ht}(C) = 2$. □

**Lemma 3.4.** *Assume that $(c(n-1), dn)D = D$. Then $bcdn(n-1) \notin \pi_i$ for $i = 1, \ldots, e$.*

**Proof.** Suppose that $bcdn(n-1) \in \pi_i$ for some $i = 1, \ldots, e$. It will be shown that this leads to a contradiction by considering the five possible cases.

Assume that $b \in \pi_i$. Since $l(X) = c(n-1)X + dn \in C = (bX^n + cX + d, bnX^{n-1} + c)D[X] \subseteq P_i$, it follows that $cX + d$ ($= (bX^n + cX + d) - bX^n$) and $c$ ($= (bnX^{n-1} + c) - bnX^{n-1}$) are in $P_i$, hence $c, d \in P_i \cap D$. However, this contradicts the hypothesis that $c, d$ are coprime in $D$, so $b \notin \pi_i$ for $i = 1, \dots, e$.

Assume that $c \in \pi_i$. Then $bnX^{n-1}$ ($= (bnX^{n-1} + c) - c = s'_{n,b,c}(X) - c) \in P_i$. By the preceding case it may be assumed that either $n$ or $X$ is in $P_i$. However, $c, n$ are coprime in $D$, so $X \in P_i$. But $bX^n + cX + d \in P_i$, so it follows that $c, d$ are in $P_i \cap D$, in contradiction to the hypothesis that $c, d$ are coprime in $D$. Therefore $c \notin \pi_i$ for $i = 1, \dots, e$.

Assume that $d \in \pi_i$. Then $c(n-1)X$ ($= (c(n-1)X + dn) - dn = l(X) - dn) \in P_i$. It follows from the preceding paragraph that $c \notin P_i$, so either $X$ or $n - 1 \in P_i$. If $X \in P_i$, then $c$ ($= (bnX^{n-1} + c) - bnX^{n-1} = s'_{n,b,c,d}(X) - bnX^{n-1}) \in P_i$, so $c, d \in P_i$, and this contradicts the hypothesis that $c, d$ are coprime in $D$. Therefore it follows that $n - 1 \in P_i$, and this contradicts the hypothesis that $d, n - 1$ are coprime in $D$. Therefore $d \notin \pi_i$ for $i = 1, \dots, e$.

The cases $n \in \pi_i$ and $n - 1 \in \pi_i$ are similar. □

**Lemma 3.5.**

(3.5.1) *$\rho_{n,b,c,d} D = bd \cdot \mathrm{Disc}(s_{n,b,c,d}(X))D = d \cdot \mathrm{Res}(s_{n,b,c,d}(X), s'_{n,b,c,d}(X))D$. Therefore, if $(c(n-1), dn)D = D$, then, for $i = 1, \dots, e$, $\rho_{n,b,c,d} D_{\pi_i} = \mathrm{Disc}(s_{n,b,c,d})D_{\pi_i} = \mathrm{Res}(s_{n,b,c,d}(X), s'_{n,b,c,d}(X))D_{\pi_i}$.*

(3.5.2) *Let $k(X) = nbX + c(n-1)$ and let $\psi_{n,b,c,d} = \mathrm{Res}(k(X), t_{n,b,c,d}(X))$. Then $\psi_{n,b,c,d} D = bd^{n-2} \cdot \mathrm{Disc}(t_{n,b,c,d}(X))D = d^{n-2} \cdot \mathrm{Res}(t_{n,b,c,d}(X), t'_{n,b,c,d}(X))D$. Therefore, if $(c(n-1), dn)D = D$, then, for $i = 1, \dots, e$, $\psi_{n,b,c,d} D_{\pi_i} = \mathrm{Disc}(t_{n,b,c,d})D_{\pi_i} = \mathrm{Res}(t_{n,b,c,d}(X), t'_{n,b,c,d}(X))D_{\pi_i}$.*

**Proof.** For (3.5.1), from the identity $(-1)^{n(n-1)/2} b \cdot \mathrm{Disc}(s_{n,b,c,d}(X)) = \mathrm{Res}(s_{n,b,c,d}(X), s'_{n,b,c,d}(X))$ [6, p. 204], and the identity $\mathrm{Res}(f, rf + sg) = \mathrm{Res}(f, s) \cdot \mathrm{Res}(f, g)$, which is immediate from [6, Eq. (2), p. 203], we have

$$\begin{aligned}\rho_{n,b,c,d} &= \mathrm{Res}\big(l(X), s_{n,b,c,d}(X)\big) = (-1)^n \mathrm{Res}\big(s_{n,b,c,d}(X), l(X)\big)\\ &= (-1)^n \mathrm{Res}\big(s_{n,b,c,d}(X), Xs'_{n,b,c,d}(X) - ns_{n,b,c,d}(X)\big)\\ &= (-1)^n \mathrm{Res}\big(s_{n,b,c,d}(X), X\big) \cdot \mathrm{Res}\big(s_{n,b,c,d}(X), s'_{n,b,c,d}(X)\big)\\ &= \pm d \cdot b \cdot \mathrm{Disc}\big(s_{n,b,c,d}(X)\big).\end{aligned}$$

It follows that $\rho_{n,b,c,d} D = bd \cdot \mathrm{Disc}(s_{n,b,c,d}(X))D = d \cdot \mathrm{Res}(s_{n,b,c,d}(X), s'_{n,b,c,d}(X))D$. Therefore if $b \notin c(n-1)D$ and $(c(n-1), dn)D = D$, then it follows from (3.4) that, for $i = 1, \dots, e$, $\rho_{n,b,c,d} D_{\pi_i} = \mathrm{Disc}(s_{n,b,c,d})D_{\pi_i} = \mathrm{Res}(s_{n,b,c,d}(X), s'_{n,b,c,d}(X))D_{\pi_i}$.

The proof of (3.5.2) is similar. □

**Theorem 3.6.** *Assume that $b \notin c(n-1)D$, $(c(n-1), dn)D = D$, and $C \neq D[X]$. Then $D[x]$ is a regular ring if and only if $C$ is a radical ideal if and only if the following equivalent conditions hold for each $P_i$ ($i \in \{1, \dots, e\}$):*

(3.6.1) *$D[x]_{p_i}$ is a regular local domain, where $p_i = P_i/(s_{n,b,c,d}(X)D[X])$.*
(3.6.2) *$s_{n,b,c,d}(X) \notin P_i^2$.*

(3.6.3) $s_{n,b,c,d}(a_i) \notin \pi_i^2 D$, *where* $a_i \in D$ *is such that* $(\pi_i, X - a_i)D[X] = (\pi_i, c(n-1)X + dn)D[X]$.

(3.6.4) $\rho_{n,b,c,d} \notin \pi_i^2$, *where* $\rho_{n,b,c,d}$ *is given by* (3.1.1).

(3.6.5) $C : \pi_i D[X] \nsubseteq P_i$.

(3.6.6) $CD[X]_{P_i} = P_i D[X]_{P_i}$.

(3.6.7) $s'_{n,b,c,d}(x)D[x]_{p_i} = p_i D[x]_{p_i}$.

(3.6.8) $s_{n,b,c,d}(x')D[x']_{q_i} = q_i D[x']_{q_i}$, *where* $D[x'] = D[X]/(s'_{n,b,c,d}(X)D[X])$ *and* $q_i = P_i/(s'_{n,b,c,d}(X)D[X])$.

(3.6.9) $\mathrm{Disc}(s_{n,b,c,d}(X)) \notin \pi_i^2$.

(3.6.10) $\mathrm{Res}(s_{n,b,c,d}(X), s'_{n,b,c,d}(X)) \notin \pi_i^2$.

*Further, these conditions hold for each i if and only if* $\mathrm{Res}(s_{n,b,c,d}(X), s'_{n,b,c,d}(X))$ *is square-free in D.*

*Moreover, if* $D[x]$ *is a regular ring and if b is square-free in D, then* $D[X]/(t_{n,d,c,b}(X)D[X])$ *is also a regular ring.*

**Proof.** By (3.3), (3.2)(i) and (ii) hold; that is, the hypotheses of (2.6) hold for $f(X) = s_{n,b,c,d}(X)$ (under the conditions (on $n, b, c, d$) in this theorem). Also, $D[x]$ is a regular ring if and only if $C$ is a radical ideal, by (2.9). Further, each $P_i$ must contain $l(X)$, by (3.1), so it follows from (2.6) that (3.6.1)–(3.6.4) are equivalent for each $P_i$ ($i \in \{1, \ldots, e\}$). Moreover, (3.1) shows that $l(X) \in C$ (and it has already been noted that $l(X)$ is primitive), so the hypothesis of (2.8) holds, hence it follows from (2.8) that (3.6.5)–(3.6.8) are each equivalent to (3.6.1). And (3.6.4) $\Leftrightarrow$ (3.6.9) $\Leftrightarrow$ (3.6.10), by (3.5.1).

For the "Further" statement in the theorem, since the $\pi_i$ are the associated prime ideals of $\mathrm{Res}(s_{n,b,c,d}(X), s'_{n,b,c,d}(X))$ (by (2.3)) and do not contain $b$ (by (3.4)), it follows from (3.5.1) that $\mathrm{Res}(s_{n,b,c,d}(X), s'_{n,b,c,d}(X))$ is square-free in $D$ if and only if (3.6.4) holds.

Now assume that $D[x]$ is a regular ring and that $b$ is square-free in $D$. Let $Y = 1/X$ and for an arbitrary polynomial $h(X) = c_m X^m + \cdots + c_0 \in D[X]$ let $h^*(Y) = c_0 Y^m + \cdots + c_m$. Then $D[X, Y] = D[X, 1/X] = D[Y, 1/Y]$ is a localization of $D[X]$ and of $D[Y]$, and $h^*(Y) \in D[Y]$. In particular, $s^*_{n,b,c,d}(Y) = dY^n + cY^{n-1} + b = t_{n,d,c,b}(Y)$ and $l^*(Y) = dnY + c(n-1)$.

Also, $t'_{n,d,c,b}(Y) = dnY^{n-1} + c(n-1)Y^{n-2} = Y^{n-2}l^*(Y)$. Further, there exists a one-to-one correspondence between the prime ideals $P$ in $D[X]$ that do not contain $X$ and the prime ideals $P^*$ in $D[Y]$ that do not contain $Y$ given by $P^* = PD[X, 1/X] \cap D[Y]$ and $P = P^*D[Y, 1/Y] \cap D[X]$. Moreover, for each such $P$ and corresponding $P^*$ there exists a one-to-one correspondence between the $P$-primary ideals $q$ in $D[X]$ and the $P^*$-primary ideals $q^*$ in $D[Y]$ given by $q^* = qD[X, 1/X] \cap D[Y]$ and $q = q^*D[Y, 1/Y] \cap D[X]$. (It therefore follows that $s_{n,b,c,d}(X)D[X, 1/X] = Y^n s_{n,b,c,d}(X)D[X, 1/X] = X^n t_{n,d,c,b}(Y)D[Y, 1/Y] = t_{n,d,c,b}(Y)D[Y, 1/Y]$, so since $s_{n,b,c,d}(X) \notin P_i^2$ for $i = 1, \ldots, e$ (by the first part of this theorem and the assumption that $D[x]$ is a regular ring), it follows that $t_{n,d,c,b}(Y) \notin (P_i^*)^2$ for $i = 1, \ldots, e$ ($X \notin P_i$, since $s_{n,b,c,d}(X), s'_{n,b,c,d}(X) \in C \subseteq P_i$ and their constant terms $c, d$ are coprime in $D$).)

Finally, let $Q$ be a prime ideal in $D[Y]$ that contains $C' = (t_{n,d,c,b}(Y), t'_{n,d,c,b}(Y))D[Y]$. Then $Y^{n-2}l^*(Y) = t'_{n,d,c,b}(Y) \in Q$, and $l^*(Y)$ is primitive in $D[Y]$ (by the same argument to show that $l(X)$ is primitive in $D[X]$), so (3.2)(i) holds for $C'$. Therefore, to complete the proof of this theorem it must be shown that $\mathrm{ht}(Q) = 2$ (so (3.2)(ii) holds for $C'$) and that $t_{n,d,c,b}(Y) \notin Q^2$. For this, by what was shown at the end of the preceding paragraph it may be assumed that

$Q \notin \{P_1^*, \ldots, P_e^*\}$. Therefore $Y \in Q$, so $b \in Q \cap D$ (so $\mathrm{ht}(Q) = 2$), and since $b$ is square-free in $D$ it follows from (2.7.2) that $t_{n,d,c,b}(Y) \notin Q^2$. Therefore, $D[Y]/(t_{n,d,c,b}(Y)D[Y])$ is a regular ring by (2.7.1), so the last statement in this theorem follows by changing notation from $Y$ to $X$. □

**Corollary 3.7.** *With the notation of* (3.6), *if $b$ is a unit, then $D[x]$ is a regular ring if and only if* $\mathrm{Disc}(s_{n,b,c,d}(X))$ *is square-free in $D$.*

**Proof.** This follows immediately from the "Further" part of (3.6) together with (3.5.1). □

**Remark 3.8.** There exists a one-to-one correspondence between the associated prime ideals $p$ of $\mathrm{Res}(s_{n,b,c,d}(X), s'_{n,b,c,d}(X))\mathbb{Z})$ and the associated prime ideals $P$ of $C$ (given by $p = P \cap \mathbb{Z}$). (This follows, since $P_1, \ldots, P_e$ are all the associated prime ideals of $C$ (by hypothesis), and $\pi_1, \ldots, \pi_e$ are all the associated prime ideals of $\mathrm{Res}(s_{n,b,c,d}(X), s'_{n,b,c,d}(X))\mathbb{Z}$ (by (2.3).) Also, it follows from (3.6.1) ⇔ (3.6.10) and (2.9) that $\mathrm{Res}(s_{n,b,c,d}(X), s'_{n,b,c,d}(X))\mathbb{Z} = \mathrm{Rad}(\mathrm{Res}(s_{n,b,c,d}(X), s'_{n,b,c,d}(X))\mathbb{Z})$ if and only if $C = \mathrm{Rad}(C)$. And, of course, $\mathrm{Res}(s_{n,b,c,d}(X), s'_{n,b,c,d}(X))\mathbb{Z} = \mathrm{Rad}(\mathrm{Res}(s_{n,b,c,d}(X), s'_{n,b,c,d}(X))\mathbb{Z})$ if and only if $\mathrm{Res}(s_{n,b,c,d}(X), s'_{n,b,c,d}(X))$ is square-free.

## 4. Conditions for $\mathbb{Z}[X]/((X^n - X - 1)\mathbb{Z}[X])$ to be a Dedekind domain

In this section we specialize (2.6) and (3.6) to the Selmer trinomials $s_{n,1,-1,-1}(X) = X^n - X - 1$ over the Dedekind domain $D = \mathbb{Z}$ of rational integers. For this, we first fix the notation, then show (in (4.4)) that $\mathbb{Z}[X]/((X^n - X - 1)\mathbb{Z}[X])$ is a Dedekind domain if and only if $n^n - (1-n)^{n-1}$ is square free. Then in (4.6) we give several specific cases of (3.6) for these trinomials. We then examine how the primes dividing $\mathrm{Disc}(X^n - X - 1) = \pm(n^n - (1-n)^{n-1})$ split in $\mathbb{Z}[X]/((X^n - X - 1)\mathbb{Z}[X])$ and use this to prove (in (4.15)) quite a few additional necessary and sufficient conditions for the factor domains modulo these trinomials to be Dedekind domains. (Analogous results for the Selmer trinomials $s_{n,1,1,1}(X) = X^n + X + 1$ are given in the next section.)

**Notation 4.1.** Let $n \geqslant 2$ be a positive integer, let $s_n(X) = s_{n,1,-1,-1}(X)$ (so $s_n(X) = X^n - X - 1$), let $l_n(X) = (n-1)X + n$, let $C = (s_n(X), s'_n(X))\mathbb{Z}[X]$, let $P_1, \ldots, P_e$ be the associated prime ideals of $C$, for $i = 1, \ldots, e$, let $\pi_i D = P_i \cap D$, and let $\rho_n = \mathrm{Res}(l_n(X), s_n(X))$, so

$$\rho_n = n^n - (1-n)^{n-1} = n^n + (-1)^n (n-1)^{n-1}. \tag{4.1.1}$$

**Remark 4.2.** (4.2.1) As noted in (3.1), $l_n(X) = Xs'_n(X) - ns_n(X) \in C$ (so (3.2)(i) holds for $C$). Also, for $i = 1, \ldots, e$, $P_i = (\pi_i, l_n(X))\mathbb{Z}[X]$ (by (2.6)) and $\pi_i$ is relatively prime to $n-1$ and to $n$, by (3.4) (with $b = 1$ and $c = d = -1$). Further, $\mathrm{ht}(C) = 2$, by (4.3) below, so $\pi_i \neq 0$ for $i = 1, \ldots, e$. Moreover, it follows from (3.1.1) (with $b = 1$ and $c = d = -1$) that $\mathrm{Res}(l_n(X), s_n(X)) = n^n - (1-n)^{n-1}$.

(4.2.2) The hypothesis $b \notin c(n-1)D$ of (3.3), (3.6), and (3.7) does not hold for $s_2(X) = X^2 - X - 1$. However, it is readily checked that $\mathrm{ht}(C) = 2$ for $C = (s_2(X), s'_2(X))\mathbb{Z}[X] = (X^2 - X - 1, 2X - 1)\mathbb{Z}[X]$. Since $b \notin c(n-1)D$ was only used in Section 3 (specifically, in (3.3)) to show that $\mathrm{ht}(C) = 2$ (where $C = (bX^n + cX + d, nbX^{n-1} + c)D[X]$), it follows that the conclusions of (3.3), (3.6), and (3.7) hold for $s_2(X)$.

**Proposition 4.3.** *With $C$ as in* (4.1), $\mathrm{ht}(C) = 2$.

**Proof.** By (3.6), it suffices to show that $C \neq \mathbb{Z}[X]$. By (3.5.1) we have $\mathrm{Res}(s_n(X), s_n'(X)) = \pm\rho_n = \pm\,\mathrm{Disc}(s_n(X))$, and it is clear that $\rho_n \geqslant 2$ for $n \geqslant 2$. Thus (2.3) shows that $\mathrm{ht}(C) = 2$. □

For the first of the main results in this section, (4.4), recall that it is said that a prime integer $\pi$ in $\mathbb{Z}$ *ramifies* in an extension domain $A$ of $\mathbb{Z}$ in case $\pi \in p^2$ for some height one prime ideal $p$ in $A$.

**Theorem 4.4.** *For each integer $n \geqslant 2$, the following are equivalent*:

(4.4.1) $\mathbb{Z}[x_n] = \mathbb{Z}[X]/((X^n - X - 1)\mathbb{Z}[X])$ *is a Dedekind domain.*
(4.4.2) $\mathbb{Z}[y_n] = \mathbb{Z}[X]/((X^n + X^{n-1} - 1)\mathbb{Z}[X])$ *is a Dedekind domain.*
(4.4.3) $\mathrm{Disc}(s_n(X))$ *is square-free.*
(4.4.4) $\rho_n = n^n - (1-n)^{n-1}$ *is square-free in* $\mathbb{Z}$.

*If these hold, then a prime $\pi \in \mathbb{Z}$ ramifies in $\mathbb{Z}[x_n]$ if and only if it ramifies in $\mathbb{Z}[y_n]$.*

**Proof.** (4.4.4) ⇔ (4.4.3), by (3.5.1).

Since the rings $\mathbb{Z}[x_n]$ and $\mathbb{Z}[y_n]$ are domains (by [14]), and have altitude one, they are Dedekind if and only if they are regular. Therefore (4.4.3) ⇔ (4.4.1), by the “Further” part of (3.6) and (3.5.1) (since $b = 1$ and $d = -1$).

(4.4.1) ⇒ (4.4.2), by the last two paragraphs of the proof of (3.6). (Those two paragraphs apply, since $b = 1$ is square-free in $D = \mathbb{Z}$ and since $(X^n - X - 1)^* = -Y^n - Y^{n-1} + 1$, so by replacing $Y$ with $X$ we get $-(-X^n - X^{n-1} + 1) = X^n + X^{n-1} - 1$.)

Now let $t_n(X) = X^n + X^{n-1} - 1$, so $t_n'(X) = X^{n-2}(nX + (n-1))$. Let $C' = (t_n(X), t_n'(X))\mathbb{Z}[X]$ (so $C'$ corresponds to $C$). Then it follows from (2.7.3) that $nX + (n-1) \in C'$, and it follows as in the derivation of (4.1.1) that $\mathrm{Res}(nX + n - 1, t_n(X)) = -\rho_n$ (with $\rho_n$ as in (4.1.1)). The final statement of this theorem follows from this and [13, Theorem 1, p. 74].

Finally, since $\mathrm{Res}(nX + n - 1, t_n(X)) = -\rho_n$ (by the preceding paragraph), to show that (4.4.2) ⇒ (4.4.4), it suffices (by (2.6.1) ⇒ (2.6.4) and (2.7.1)) to show that $\pi_1, \ldots, \pi_e$ are prime factors of $\rho_n$ and, in fact, are all of the prime factors of $\rho_n$. For this, (2.3) shows that $\pi_1 D, \ldots, \pi_e D$ are all the associated prime ideals of $\mathrm{Res}(s_n(X), s_n'(X))\mathbb{Z}$, and $\mathrm{Res}(s_n(X), s_n'(X))\mathbb{Z} = \mathrm{Disc}(s_n(X))\mathbb{Z} = \rho_n\mathbb{Z}$, by (3.5.1), so $\pi_1, \ldots, \pi_e$ are all the prime factors of $\rho_n$. □

For ease of future reference, we give the following alternate form of Theorem 4.4.

**Theorem 4.5.** *Let $n \geqslant 2$ be an integer and let $\alpha$, $\beta \in \mathbb{C}$ be roots of $s_n(X) = X^n - X - 1$ and $X^n + X^{n-1} - 1$, respectively. Then the following are equivalent*:

(4.5.1) $\{1, \alpha, \ldots, \alpha^{n-1}\}$ *is a $\mathbb{Z}$-basis for the integers $\mathbb{Z}_{\mathbb{Q}(\alpha)}$ of $\mathbb{Q}(\alpha)$.*
(4.5.2) $\{1, \beta, \ldots, \beta^{n-1}\}$ *is a $\mathbb{Z}$-basis for the integers $\mathbb{Z}_{\mathbb{Q}(\beta)}$ of $\mathbb{Q}(\beta)$.*
(4.5.3) $\mathrm{Disc}(s_n(X))$ *is square-free.*
(4.5.4) $\rho_n = n^n - (1-n)^{n-1}$ *is square-free in* $\mathbb{Z}$.

*If these hold, then a prime $\pi \in \mathbb{Z}$ ramifies in $\mathbb{Z}[\alpha]$ if and only if it ramifies in $\mathbb{Z}[\beta]$.*

It follows from (4.2) (and (4.3)) that (3.2)(i) and (ii) hold for $C$, so we can apply (3.6) to the trinomials $s_n(X)$.

**Proposition 4.6.** $\mathbb{Z}[x_n] = \mathbb{Z}[X]/(s_n(X)\mathbb{Z}[X])$ *is a Dedekind domain for* $n = 2, 3, \ldots, 50$. *Further* 59 *is the smallest prime* $\pi$ *such that* $\pi^2$ *divides some* $\rho_n$, *and* 257 *is the smallest* $n$ *such that* $59^2$ *divides* $\rho_n$. *So each* $n$ *such that* $\mathbb{Z}[x_n] = \mathbb{Z}[X]/(s_n(X)\mathbb{Z}[X])$ *is not a Dedekind domain is divisible by* $\pi^2$ *for some prime* $\pi \geqslant 59$.

**Proof.** Mathematica shows that $\rho_n = n^n - (1-n)^{n-1}$ $(= \mathrm{Res}((n-1)X + n, X^n - X - 1))$ is square-free in $\mathbb{Z}$ for $n = 2, \ldots, 50$. By [14, Theorem 1], $\mathbb{Z}[x_n]$ is an integral domain. It is clearly integral over $\mathbb{Z}$, and is integrally closed, either by (3.6), or [13, Theorem 1, p. 76] (and the fact that $\rho_n = \pm\,\mathrm{Disc}(X^n - X - 1)$, by (3.5.1)). Thus $\mathbb{Z}[x_n]$ is a Dedekind domain.

The "Further" statement of (4.6) follows from Mathematica using the following algorithm, and the following lemma. □

**Program 4.7.** `stmp = OpenAppend["Output"]`

```
c = 0;
d = 0;
For[p = 2, p < 60, p++,
   If[PrimeQ[p],
      j = 2;
      While[$j$ < $(p^3-p^2)$,
         a = Mod[$j^j$, $p^2$];
         b = Mod[$(1-j)^{(j-1)}$, $p^2$];
         k = Mod[$a-b$, $p^2$];
         If[k == 0,
            WriteString[stmp,"p=",p,"  j=",j," minus "];
            c = 1];
         h = Mod[$a+b$, $p^2$];
         m = Mod[j,3];
         If[(h == 0) && ((m == 0) || (m == 1)),
            WriteString[stmp,"p=",p,"  j=",j," plus "];
            d = 1];
         If[c+d == 2, $j = p^3-p^2$];
         If[Mod[j,1000] == 0,
            Print[p," ",j]];
      j++]]]
Print["done"]
```

By using a variation of (4.7) (searching for a prime integer $p$ with $p^2$ dividing $\rho_n$, $50 < n < 257$ and $60 < p < 2\,000\,000$), Mathematica shows that 130 is the smallest $n < 257$ with a repeated prime factor $p < 2\,000\,000$ (and $\rho_{130}$ is divisible by $83^2$). (Of course, there could be $n \in \{51, \ldots, 129\}$ such that $\rho_n$ has a square prime factor greater than $2\,000\,000$.)

**Lemma 4.8.** *For all integers* $n \geqslant 2$ *and prime integers* $\pi > 2$, $\rho_n \equiv \rho_{n+i(\pi^3-\pi^2)} \pmod{\pi^2}$ *for all positive integers* $i$.

**Proof.** There are $\pi^2 - \pi$ units in $\mathbb{Z}/(\pi^2\mathbb{Z})$, so $x^{\pi^2-\pi} = 1$ for all units $x$ in $\mathbb{Z}/(\pi^2\mathbb{Z})$. So if $a \in (\pi^2 - \pi)\mathbb{Z}$, then $x^a = 1$ for all units $x$ in $\mathbb{Z}/(\pi^2\mathbb{Z})$. Fix positive integers $n, \pi, i$ such that $n \geqslant 2$ and $\pi$ is an odd prime with $n(n-1) \notin \pi\mathbb{Z}$, and let $d = \pi^3 - \pi^2$. Then modulo $\pi^2$, we have $\rho_{n+id} = (n+id)^{n+id} - (1-n-id)^{n+id-1} \equiv n^{n+id} - (1-n)^{n+id-1} \equiv n^n n^{id} - (1-n)^{n-1}(1-n)^{id} \equiv n^n - (1-n)^{n-1} = \rho_n$. □

We now examine how the primes dividing $\mathrm{Disc}(X^n - X - 1) = \pm(n^n - (1-n)^{n-1})$ split in $\mathbb{Z}[X]/((X^n - X - 1)\mathbb{Z}[X])$ and use this to prove (in (4.15)) quite a few additional necessary and sufficient conditions for the factor domains modulo these trinomials to be Dedekind domains. In the case $n = 3$, more detailed results are given in [3] on how primes in $\mathbb{Z}$ split in $\mathbb{Z}[X]/(s_3(X)\mathbb{Z}[X])$, and more such results are given in the cases $n = 2, 3, 4, 5$ in [15].

**Remark 4.9.** In the principal ideal domain $(\mathbb{Z}/(\pi_i\mathbb{Z}))[X] = \mathbb{Z}[X]/(\pi_i\mathbb{Z}[X])$ let $\overline{f_{i,j}}(X)$ be distinct monic irreducible polynomials such that no $\overline{f_{i,j}}(X)$ is an associate of $\overline{l_n(X)} = \overline{n-1}X + \bar{n}$ and such that $X^n - X - \bar{1} = \overline{v_i}(\overline{f_{i,1}}(X))^{g_{i,1}} \cdots (\overline{f_{i,k_i}}(X))^{g_{i,k_i}} (\overline{n-1}X + \bar{n})^{h_i}$ is a factorization of $X^n - X - \bar{1}$ into irreducible factors (where $\overline{v_i}$ is the unit $(\bar{n} - \bar{1})^{-h_i} \in \mathbb{Z}/(\pi_i\mathbb{Z})$). Then $h_i = 2$ and $g_{i,j} = 1$ for $i = 1, \ldots, e$ and $j = 1, \ldots, k_i$.

**Proof.** To see that $h_i = 2$, note first that $h_i \geqslant 2$, by the proof of (2.6.2) (see (2.6)(∗)). Also, $s'_n(X) = nX^{n-1} - 1$ and $s''_n(X) = n(n-1)X^{n-2}$, so since $n(n-1)$ and $\pi_i$ are relatively prime (by (4.2)), $\overline{s'_n(X)}$ and $\overline{s''_n(X)}$ cannot have a common root. Therefore it follows from [6, Proposition 1, p. 131] that, modulo $\pi_i\mathbb{Z}[X]$, $\overline{n-1}X + \bar{n}$ cannot be a factor of multiplicity greater than two of $X^n - X - \bar{1}$, hence $h_i = 2$.

To see that each $g_{i,j} = 1$, suppose the contrary holds, so $g_{i,j} > 1$ for some $i \in \{1, \ldots, e\}$ and $j \in \{1, \ldots, k_i\}$. Therefore by taking the derivative of $X^n - X - \bar{1} = \overline{v_i}(\overline{f_{i,1}}(X))^{g_{i,1}} \cdots (\overline{f_{i,k_i}}(X))^{g_{i,k_i}} (\overline{n-1}X + \bar{n})^2$, it follows that $(X^n - X - \bar{1}, \bar{n}X^{n-1} - \bar{1})(\mathbb{Z}/(\pi_i\mathbb{Z}))[X] \subseteq p = \overline{f_{i,j}}(X)(\mathbb{Z}/(\pi_i\mathbb{Z}))[X]$ ($\bar{n} \neq 0$, by (4.2)). Therefore the pre-image $P$ in $\mathbb{Z}[X]$ of $p$ contains $(\pi_i, C)\mathbb{Z}[X]$, hence $P = P_i$ $(= (\pi_i, l_n(X))\mathbb{Z}[X])$, and this contradicts the fact that $\overline{f_{i,j}}(X)$ and $\overline{l_n(X)} = \overline{n-1}X + \bar{n}$ are nonassociate irreducible polynomials in $\mathbb{Z}[X]/(\pi_i\mathbb{Z}[X])$. It follows that each $g_{i,j} = 1$. □

**Notation 4.10.** With the notation of (4.9), for $i = 1, \ldots, e$ and for $j = 1, \ldots, k_i$, let $f_{i,j}(X)$ be distinct monic irreducible polynomials in the UFD $\mathbb{Z}[X]$ such that $f_{i,j}(X) + \pi_i\mathbb{Z}[X] = \overline{f_{i,j}}(X)$, let $Q_{i,j} = (\pi_i, f_{i,j}(X))\mathbb{Z}[X]$, let $p_i = P_i/(s_n(X)\mathbb{Z}[X])$, and let $q_{i,j} = Q_{i,j}/(s_n(X)\mathbb{Z}[X])$.

**Remark 4.11.** Each $Q_{i,j}$ is a maximal ideal such that $l_n(X) \notin Q_{i,j}$, $s_n(X) \in Q_{i,j}$, and $Q_{i,j}\mathbb{Z}[X]_{Q_{i,j}} = (\pi_i, s_n(X))\mathbb{Z}[X]_{Q_{i,j}}$, so $q_{i,j}\mathbb{Z}[x_n]_{q_{i,j}} = \pi_i\mathbb{Z}[x_n]_{q_{i,j}}$.

**Proof.** $Q_{i,j}$ is a maximal ideal and $l_n(X) \notin Q_{i,j}$, since $Q_{i,j}/(\pi_i\mathbb{Z}[X]) = \overline{f_{i,j}}(X)(\mathbb{Z}/(\pi_i\mathbb{Z}))[X]$ is a maximal ideal and $\overline{l_n(X)} \notin \overline{f_{i,j}}(X)(\mathbb{Z}/(\pi_i\mathbb{Z}))[X]$. Also, it follows from (4.9) that $(n-1)^2 s_n(X) - (l_n(X))^2 f_{i,1}(X) \cdots f_{i,k_i}(X) \in \pi_i\mathbb{Z}[X]$ (and $n-1$ and $\pi_i$ are relatively prime), so it follows that $s_n(X) \in Q_{i,j}$ and that $Q_{i,j}\mathbb{Z}[X]_{Q_{i,j}} = (\pi_i, f_{i,j}(X))\mathbb{Z}[X]_{Q_{i,j}} = (\pi_i, s_n(X))\mathbb{Z}[X]_{Q_{i,j}}$. Therefore, modulo $s_n(X)\mathbb{Z}[X]_{Q_{i,j}}$ is follows that $q_{i,j}\mathbb{Z}[x_n]_{q_{i,j}} = \pi_i\mathbb{Z}[x_n]_{q_{i,j}}$. □

The equalities involving $s'_n(X)$ and $s_n(X)$ in (4.12) will be useful in the remainder of this section.

**Remark 4.12.** (4.12.1) There exists $q(X) \in \mathbb{Z}[X] \setminus (P_1 \cup \cdots \cup P_e)$ such that $(1-n)^{n-1}s'_n(X) = l_n(X)q(X) + \rho_n$.

(4.12.2) Let $g^*(X) = (1-n)^{n-3}X^{n-2} + 2n(1-n)^{n-4}X^{n-3} + \cdots + in^{i-1}(1-n)^{n-i-2}X^{n-i-1} + \cdots + (n-2)n^{n-3}X - n^{n-2}$. Then: $g^*(X) \in \mathbb{Z}[X] \setminus (P_1 \cup \cdots \cup P_e)$; $Q_{i,j}\mathbb{Z}[X]_{Q_{i,j}} = (\pi_i, g^*(X))\mathbb{Z}[X]_{Q_{i,j}}$ for $i = 1, \ldots, e$ and $j = 1, \ldots, k_i$; and $(1-n)^{n-1}s_n(X) = (l_n(X))^2 g^*(X) + \rho_n(X+1)$.

**Proof.** For (4.12.1), there exists $q_1(X) \in \mathbb{Z}[\frac{n}{1-n}][X]$ such that

$$s'_n(X) = \left(X - \frac{n}{1-n}\right)q_1(X) + s'_n\left(\frac{n}{1-n}\right), \tag{4.12)(*}$$

and it is readily seen that $s'_n(\frac{n}{1-n}) = \frac{\rho_n}{(1-n)^{n-1}}$. By multiplying both sides of (4.12)(∗) by $(1-n)^{n-1}$ we get $(1-n)^{n-1}s'_n(X) = l_n(X)q(X) + \rho_n$ for some $q(X) \in \mathbb{Z}[X]$.

To see that $q(X) \notin P_1 \cup \cdots \cup P_e$, suppose the contrary holds and fix $P_i$ such that $q(X) \in P_i$. Now $P_i = (\pi_i, l_n(X))\mathbb{Z}[X]$, by (4.2), so $P_i/(\pi_i\mathbb{Z}[X])$ is generated by $\overline{l_n}(X) = (\overline{n-1})X + \bar{n}$. Since $s'_n(X), q(X) \in P_i$, it follows that their residue classes modulo $\pi_i\mathbb{Z}[X]$ are each a multiple of $\overline{l_n}(X)$. Also, since $\pi_i$ is a factor of $\rho_n$, it follows from $(1-n)^{n-1}s'_n(X) = l_n(X)q(X) + \rho_n$ that $\overline{l_n}(X)\bar{q}(X)(\mathbb{Z}/(\pi_i\mathbb{Z}))[X] = \bar{s}'_n(X)(\mathbb{Z}/(\pi_i\mathbb{Z}))[X]$, hence $(\overline{l_n}(X))^2$ is a factor of the residue class of $s'_n(X)$, and this contradicts what was shown in the first paragraph of the proof of (4.9). Therefore the supposition is false, so $q(X) \notin P_i$ for $i = 1, \ldots, e$.

For (4.12.2), by long division in $\mathbb{Z}[\frac{n}{1-n}][X]$ it follows that

$$s_n(X) = \left(X - \frac{n}{1-n}\right)^2 q_2(X) + r(X) \tag{4.12)(**}$$

for some $q_2(X) \in \mathbb{Z}[\frac{n}{1-n}][X]$, and it is readily seen that $r(X) = \frac{\rho_n(X+1)}{(1-n)^{n-1}}$. By multiplying both sides of (4.12)(∗∗) by $(1-n)^{n-1}$ we get $(1-n)^{n-1}s_n(X) = (l_n(X))^2 g^*(X) + \rho_n(X+1)$.

To see that $g^*(X) \notin P_1 \cup \cdots \cup P_e$, fix $i \in \{1, \ldots, e\}$, and note that $\pi_i$ is a factor of $\rho_n$, so by reducing the coefficients of $(1-n)^{n-1}s_n(X) = (l_n(X))^2 g^*(X) + \rho_n(X+1)$ modulo $\pi_i\mathbb{Z}$ we get

$$(\bar{1} - \bar{n})^{n-1}\overline{s_n}(X) = \left(\overline{l_n}(X)\right)^2\overline{g^*}(X). \tag{4.12)(***}$$

Since $(\bar{1} - \bar{n})^{n-1}$ is a unit in $\mathbb{Z}/(\pi_i\mathbb{Z})$ (by (4.2)), since $P_i/(\pi_i\mathbb{Z}[X])$ is generated by $\overline{l_n}(X)$, and since $\overline{s_n}(X)$ is not divisible by $(\overline{l_n}(X))^3$ (by (4.9)), it follows that $g^*(X) \notin P_i$.

Finally, (4.12)(∗∗∗) shows that $\overline{s_n}(X) = \bar{u}_i(\overline{l_n}(X))^2\overline{g^*}(X)$, where $\bar{u}_i = (\bar{1} - \bar{n})^{1-n}$. Therefore, since $\pi_i$ and $1-n$ are relatively prime in $\mathbb{Z}$ (by (4.2)), it follows that $(\pi_i, s_n(X))\mathbb{Z}[X] = (\pi_i, (l_n(X))^2 g^*(X))\mathbb{Z}[X]$. Therefore it follows from (4.11) (twice) that

$$Q_{i,j}\mathbb{Z}[X]_{Q_{i,j}} = \left(\pi_i, s_n(X)\right)\mathbb{Z}[X]_{Q_i,j} = \left(\pi_i, \left(l_n(X)\right)^2 g^*(X)\right)\mathbb{Z}[X]_{Q_i,j} = \left(\pi_i, g^*(X)\right)\mathbb{Z}[X]_{Q_i,j}$$

for $i = 1, \ldots, e$ and $j = 1, \ldots, k_i$. □

The next result considers the ideals generated by pairs of the elements in $\{s_n(X), s'_n(X), l_n(X), \rho_n\}$.

**Proposition 4.13.**

(4.13.1) $C = (s_n(X), s'_n(X))\mathbb{Z}[X] = (l_n(X), s_n(X))\mathbb{Z}[X] = (l_n(X), s'_n(X))\mathbb{Z}[X] = (\rho_n, l_n(X))\mathbb{Z}[X]$. *Also,* $C\mathbb{Z}[X]_{P_i} = (\rho_n, s'_n(X))\mathbb{Z}[X]_{P_i}$ *for* $i = 1, \ldots, e$.

(4.13.2) $(\rho_n, (l_n(X))^2)\mathbb{Z}[X] = ((l_n(X))^2, s_n(X))\mathbb{Z}[X]$. *Also,* $(\rho_n, s_n(X))\mathbb{Z}[X]_{P_i} = (\rho_n, (l_n(X))^2)\mathbb{Z}[X]_{P_i} = ((l_n(X))^2, s_n(X))\mathbb{Z}[X]_{P_i}$ *for* $i = 1, \ldots, e$.

**Proof.** (NOTE: in the following proof we use several times the readily checked result: If $I$ is an ideal in a ring $R$ and if $b \in R$ is such that $(b, I)R = R$, then $J : bR = J$ for all ideals $J$ in $R$ that contain $I$ and that do not contain $b$.)

For (4.13.1), by (4.1), $C = (s_n(X), s'_n(X))\mathbb{Z}[X]$, and it was noted in (4.2) that

$$Xs'_n(X) - ns_n(X) = l_n(X). \tag{4.13($*$)}$$

It follows from (4.13)($*$) that $(l_n(X), s_n(X))\mathbb{Z}[X] \subseteq C$ and that $(l_n(X), s_n(X))\mathbb{Z}[X] : X\mathbb{Z}[X]$ contains $s'_n(X)$. Also, $(X, s'_n(X))\mathbb{Z}[X] = \mathbb{Z}[X]$, so it follows from the NOTE that $(l_n(X), s_n(X))\mathbb{Z}[X] : X\mathbb{Z}[X] = (l_n(X), s_n(X))\mathbb{Z}[X]$. So $(s_n(X), s'_n(X))\mathbb{Z}[X] \subseteq (l_n(X), s_n(X))\mathbb{Z}[X]$, hence $(s_n(X), s'_n(X))\mathbb{Z}[X] = (l_n(X), s_n(X))\mathbb{Z}[X]$.

It also follows from (4.13)($*$) that $(l_n(X), s'_n(X))\mathbb{Z}[X] \subseteq C$ and that $(l_n(X), s'_n(X))\mathbb{Z}[X]: n\mathbb{Z}[X]$ contains $s_n(X)$. Also, $(n, s'_n(X))\mathbb{Z}[X] = \mathbb{Z}[X]$, so it follows from the NOTE that $(l_n(X), s'_n(X))\mathbb{Z}[X] : n\mathbb{Z}[X] = (l_n(X), s'_n(X))\mathbb{Z}[X]$, so $(s_n(X), s'_n(X))\mathbb{Z}[X] \subseteq (l_n(X), s'_n(X))\mathbb{Z}[X]$, hence $(s_n(X), s'_n(X))\mathbb{Z}[X] = (l_n(X), s'_n(X))\mathbb{Z}[X]$.

Also, by (4.12.1), $(1-n)^{n-1}s'_n(X) = l_n(X)q(X) + \rho_n$, for some $q(X) \in \mathbb{Z}[X]$, so:

(a) $\rho_n \in (l_n(X), s'_n(X))\mathbb{Z}[X]$ $(= C)$;
(b) $s'_n(X) \in (\rho_n, l_n(X))\mathbb{Z}[X] : (1-n)^{n-1}\mathbb{Z}[X]$; and,
(c) $l_n(X) \in (\rho_n, s'_n(X))\mathbb{Z}[X] : q(X)\mathbb{Z}[X]$.

Now note that in (b), $(\rho_n, l_n(X))\mathbb{Z}[X] : (1-n)^{n-1}\mathbb{Z}[X] = (\rho_n, l_n(X))\mathbb{Z}[X]$ (by the NOTE, since $(1-n, l_n(X))\mathbb{Z}[X] = \mathbb{Z}[X]$). It follows from this and (a) that $(\rho_n, l_n(X))\mathbb{Z}[X] = C$.

It follows from what has already been shown that $(\rho_n, s'_n(X))\mathbb{Z}[X] \subseteq C$, so $(\rho_n, s'_n(X))\mathbb{Z}[X]_{P_i} \subseteq C\mathbb{Z}[X]_{P_i}$ for $i = 1, \ldots, e$. For the opposite inclusion, note that $q(X) \notin P_i$ for $i = 1, \ldots, e$, by (4.12.1), so it follows from (c) that $l_n(X) \in (\rho_n, s'_n(X))\mathbb{Z}[X]_{P_i}$, hence $C\mathbb{Z}[X]_{P_i} = (l_n(X), s'_n(X))\mathbb{Z}[X]_{P_i} \subseteq (\rho_n, s'_n(X))\mathbb{Z}[X]_{P_i}$, as desired.

For (4.13.2), it follows from (4.12.2) that $(1-n)^{n-1}s_n(X) = (l_n(X))^2 g^*(X) + \rho_n(X+1)$, where $g^*(X)$ is as in (4.12.2), so:

(a) $\rho_n \in ((l_n(X))^2, s_n(X))\mathbb{Z}[X] : (X+1)\mathbb{Z}[X]$;
(b) $s_n(X) \in (\rho_n, (l_n(X))^2)\mathbb{Z}[X] : (1-n)^{n-1}\mathbb{Z}[X]$; and,
(c) $(l_n(X))^2 \in (\rho_n, s_n(X))\mathbb{Z}[X] : g^*(X)\mathbb{Z}[X]$.

Now $(s_n(X), X+1)\mathbb{Z}[X] = \mathbb{Z}[X] = (\rho_n, 1-n)\mathbb{Z}[X]$, so it follows from the NOTE (and (a) and (b)) that $((l_n(X))^2, s_n(X))\mathbb{Z}[X] = (\rho_n, (l_n(X))^2)\mathbb{Z}[X]$.

Finally, it follows from (4.12.2) that $g^*(X) \notin P_i\mathbb{Z}[X]_{P_i}$ for $i = 1, \ldots, e$. Therefore it follows from (c) that $(l_n(X))^2 \in (\rho_n, s_n(X))\mathbb{Z}[X]_{P_i}$ for $i = 1, \ldots, e$, so it follows from what was shown in the preceding paragraph that $(\rho_n, s_n(X))\mathbb{Z}[X]_{P_i} = (\rho_n, (l_n(X))^2)\mathbb{Z}[X]_{P_i} = ((l_n(X))^2, s_n(X))\mathbb{Z}[X]_{P_i}$. □

**Corollary 4.14.** *$\rho_n L_i = (l_n(x_n))^2 L_i$, where $L_i = \mathbb{Z}[x_n]_{p_i}$ (with $p_i = P_i/(s_n(X)\mathbb{Z}[X])$) for $i = 1, \dots, e$.*

**Proof.** This follows immediately from (4.13.2). □

For the final result in this section, recall that an ideal $I$ is a *reduction* of an ideal $J$ in case $I \subseteq J$ and $IJ^n = J^{n+1}$ for some nonnegative integer $n$. (In (4.15.9)–(4.15.11) it is readily seen that $\mathbb{Z}[\frac{n}{1-n}] = \mathbb{Z}[\frac{1}{n-1}]$.)

**Theorem 4.15.** *Let $\mathbb{Z}[x_n'] = \mathbb{Z}[X]/(s_n'(X)\mathbb{Z}[X])$ and let $\mathbb{Z}[x_n] = \mathbb{Z}[X]/(s_n(X)\mathbb{Z}[X])$. Then the following statements are equivalent:*

(4.15.1) *$\mathbb{Z}[x_n]$ is a Dedekind domain.*
(4.15.2) *$\rho_n\mathbb{Z}$ is a radical ideal.*
(4.15.3) *$C$ is a radical ideal in $\mathbb{Z}[X]$.*
(4.15.4) *$l_n(x_n)\mathbb{Z}[x_n]$ is a radical ideal.*
(4.15.5) *$s_n'(x_n)\mathbb{Z}[x_n]$ is a radical ideal.*
(4.15.6) *$l_n(x_n')\mathbb{Z}[x_n']$ is a radical ideal.*
(4.15.7) *$s_n(x_n')\mathbb{Z}[x_n']$ is a radical ideal.*
(4.15.8) *$\rho_n\mathbb{Z}[x_n']_{q_i} = q_i\mathbb{Z}[x_n']_{q_i}$ for $i = 1, \dots, e$, where $q_i = P_i/(s_n'(X)\mathbb{Z}[X])$.*
(4.15.9) *$s_n(\frac{n}{1-n})\mathbb{Z}[\frac{n}{1-n}]$ is a radical ideal.*
(4.15.10) *$s_n'(\frac{n}{1-n})\mathbb{Z}[\frac{n}{1-n}]$ is a radical ideal.*
(4.15.11) *$\rho_n\mathbb{Z}[\frac{n}{1-n}]$ is a radical ideal.*
(4.15.12) *$l_n(X)(\mathbb{Z}/(\rho_n\mathbb{Z}))[X]$ is a radical ideal.*
(4.15.13) *$s_n'(X)(\mathbb{Z}[X]/(\rho_n\mathbb{Z}[X]))_{m_i} = m_i(\mathbb{Z}[X]/(\rho_n\mathbb{Z}[X]))_{m_i}$ for $i = 1, \dots, e$, where $m_i = P_i/(\rho_n\mathbb{Z}[X])$.*
(4.15.14) *$(l_n(X))^2 g^*(X) \notin (\pi_i^2, \pi_i l_n(X), s_n(X))\mathbb{Z}[X]$ for $i = 1, \dots, e$, where $g^*(X)$ is as in (4.12.2).*
(4.15.15) *$(l_n(X))^2 g(X) \notin (\pi_i^2, \pi_i l_n(X), s_n(X))\mathbb{Z}[X]$ for $i = 1, \dots, e$ and for all $g(X) \in \mathbb{Z}[X] \setminus P_i$.*
(4.15.16) *$\pi_i\mathbb{Z}[x_n]_{p_i}$ is not a reduction of $p_i\mathbb{Z}[x_n]_{p_i}$ for $i = 1, \dots, e$ (where $p_i = P_i/(s_n(X)\mathbb{Z}[X])$).*

**Proof.** Since $\rho_n\mathbb{Z} \neq \mathbb{Z}$, it follows from the definitions that $\rho_n\mathbb{Z}$ is a radical ideal if and only if $\rho_n$ is a square-free element in $\mathbb{Z}$. Therefore (4.15.1) ⇔ (4.15.2), by (4.4.1) ⇔ (4.4.4).

(4.15.1) ⇔ (4.15.3), by (2.9).

The equivalence of (4.15.3)–(4.15.13) follows from (4.13.1).

(4.15.1) ⇒ (4.15.16). It follows from (2.6.1) ⇒ (2.6.4) that if (4.15.1) holds, then $\pi_i\mathbb{Z}_{\pi_i\mathbb{Z}} = \rho_n\mathbb{Z}_{\pi_i\mathbb{Z}}$ for $i = 1, \dots, e$, so $(\pi_i, s_n(X))\mathbb{Z}[X]_{P_i} = (\rho_n, s_n(X))\mathbb{Z}[X]_{P_i}$, hence $\pi_i L_i = \rho_n L_i$ for $i = 1, \dots, e$, where $L_i = \mathbb{Z}[x_n]_{p_i}$ (with $p_i = P_i/(s_n(X)\mathbb{Z}[X])$). Also, $\rho_n L_i = (l_n(x_n))^2 L_i$, by (4.13.2), so $\pi_i \in p_i^2 L_i$ (since $\pi_i, l_n(x_n)$ generate $p_i$). It follows that, for $i = 1, \dots, e$, $\pi_i\mathbb{Z}[x_n]_{p_i}$ cannot be a reduction of $p_i\mathbb{Z}[x_i]_{p_i}$, hence (4.15.1) ⇒ (4.15.16).

Assume that (4.15.16) holds, and suppose that $(l_n(X))^2 g(X) \in (\pi_i^2, \pi_i l_n(X), s_n(X))\mathbb{Z}[X]$ for some $i = 1, \dots, e$ and for some $g(X) \in \mathbb{Z}[X] \setminus P_i$. Then $(l_n(x_n))^2 g(x_n) \in (\pi_i^2, \pi_i l_n(x_n))\mathbb{Z}[x_n]$. Let $L_i = \mathbb{Z}[x_n]_{p_i}$. Then since $\pi_i, l_n(x_n)$ generate $p_i$ and $g(x_n) \notin p_i L_i$, it follows that $(l_n(x_n))^2 \in \pi_i(\pi_i, l_n(x_n))L_i$, so $\pi_i(\pi_i, l_n(x_n))L_i = p_i^2 L_i$, hence $\pi_i L_i$ is a reduction of $p_i L_i$, and this contradicts (4.15.16). Therefore the supposition is false, so (4.15.16) ⇒ (4.15.15).

It is clear that (4.15.15) ⇒ (4.15.14).

Finally, assume that (4.15.14) holds. Now it follows from (4.9) (and (4.11)) that $s_n(X) - v_i f_{i,1}(X)\cdots f_{i,k_i}(X)((n-1)X+n)^2 \in \pi_i\mathbb{Z}[X]$ (for $i = 1,\dots,e$), where $v_i \in \mathbb{Z}$ is such that $v_i + \pi_i\mathbb{Z} = \overline{v_i}$. Also, for $j \in \{1,\dots,k_i\}$, the polynomials $f_{i,j}(X)$ are units in $\mathbb{Z}[X]_{P_i}$, as is $v_i$, so it follows that $((n-1)x_n+n)^2 \in \pi_i L_i$, where $L_i = \mathbb{Z}[x_n]_{p_i}$. Therefore $(l_n(x_n))^2 \in \pi_i L_i \cap p_i^2 L_i = \pi_i(p_i^2 L_i : \pi_i L_i)$, so

$$\bigl(l_n(x_n)\bigr)^2 \in \pi_i\bigl(p_i^2 L_i : \pi_i L_i\bigr). \tag{4.15)(*}$$

Now either: (a) $\pi_i(p_i^2 L_i : \pi_i L_i) = \pi_i L_i$ (and this holds if and only if $\pi_i \in p_i^2 L_i$); or, (b) $\pi_i(p_i^2 L_i : \pi_i L_i) = \pi_i p_i L_i$ (and this holds if and only if $\pi_i \notin p_i^2 L_i$). Also, if (b) holds for some $i \in \{1,\dots,e\}$, then since $l_n(x_n), \pi_i$ generate $p_i L_i$, it follows from (4.15)(∗) that $p_i^2 L_i = \pi_i p_i L_i$, so $(l_n(x_n))^2 \in p_i^2 = p_i^2 L_i \cap \mathbb{Z}[x_n] = \pi_i p_i L_i \cap \mathbb{Z}[x_n]$. However, $\pi_i p_i L_i \cap \mathbb{Z}[x_n]$ is the $p_i$-primary component of $\pi_i p_i$, so $\pi_i p_i L_i \cap \mathbb{Z}[x_n] = \pi_i p_i : g^*(x_n)\mathbb{Z}[x_n]$ (since $g^*(x_n) \notin p_i$ (for $i = 1,\dots,e$) and $g^*(x_n)$ is in every other primary component of $\pi_i p_i$ (by (4.12.2), since these other primary components are, in fact, the prime ideals $q_{i,j}$, by (4.11)). It follows that $(l_n(X))^2 g^*(X) \in (\pi_i^2, \pi_i l_n(X), s_n(X))\mathbb{Z}[X]$ for some $i = 1,\dots,e$, and this contradicts the hypothesis. Therefore (a) holds for $i = 1,\dots,e$; that is, $\pi_i \in p_i^2 L_i$. Therefore, since $\pi_i, l_n(x_n)$ generate $p_i L_i$, it follows that $l_n(x_n)$ generates $p_i L_i$, so $L_i$ is a regular local domain for $i = 1,\dots,e$. It follows from (3.6.1) that $\mathbb{Z}[x_n]$ is a regular ring, so $\mathbb{Z}[X]$ is a Dedekind domain, hence (4.15.14) ⇒ (4.15.1). □

## 5. Conditions for $\mathbb{Z}[X]/((X^n + X + 1)\mathbb{Z}[X])$ to be a Dedekind domain

The results in the first part of this section are analogs of the results in Section 4, and their proofs are similar, so they are generally omitted. The results in the last part of this section show that $\mathbb{Z}[X]/(X^n + X + 1)\mathbb{Z}[X])$ is *never* a regular ring when $n > 2$ and $n \equiv 2 \pmod 3$.

As usual, we begin by fixing the notation.

**Notation 5.1.** Let $n \geqslant 2$ be a positive integer, let $u_n(X) = s_{n,1,1,1}(X)$ (so $u_n(X) = X^n + X + 1$), let $l_n(X) = (n-1)X + n$, let $C = (u_n(X), u_n'(X))\mathbb{Z}[X]$, let $P_1,\dots,P_e$ be the associated prime ideals of $C$, for $i = 1,\dots,e$, let $\pi_i D = P_i \cap D$, and let $\rho_n = \operatorname{Res}(l_n(X), u_n(X))$, so

$$\rho_n = (-n)^n - (n-1)^{n-1} = (-1)^n\bigl[n^n + (1-n)^{n-1}\bigr]. \qquad 5.1.1$$

**Remark 5.2.** (5.2.2) Observe that $l_n(X) = nu_n(X) - Xu_n'(X) \in C$ (so (3.2)(i) holds for $C$). Also, for $i = 1,\dots,e$, $P_i = (\pi_i, l_n(X))\mathbb{Z}[X]$ (by (2.6)) and $\pi_i$ is relatively prime to $n-1$ and to $n$, by (3.4) (with $b = c = d = 1$). Further, $\operatorname{ht}(C) = 2$, by (5.3) below, so $\pi_i \neq 0$ for $i = 1,\dots,e$. Moreover, it follows from (3.1.1) (with $b = c = d = 1$) that $\operatorname{Res}(l_n(X), u_n(X)) = (-n)^n - (n-1)^{n-1} = (-1)^n[n^n + (1-n)^{n-1}]$.

(5.2.2) The hypothesis $b \notin c(n-1)D$ of (3.3), (3.6), and (3.7) does not hold for $u_2(X) = X^2 + X + 1$. However, it is readily checked that $\operatorname{ht}(C) = 2$ for $C = (u_2(X), u_2'(X))\mathbb{Z}[X] = (X^2 + X + 1, 2X + 1)\mathbb{Z}[X]$. Since $b \notin c(n-1)D$ was only used in Section 3 (specifically, in (3.3)) to show that $\operatorname{ht}(C) = 2$ (where $C = (bX^n + cX + d, nbX^{n-1} + c)D[X]$), it follows that the conclusions of (3.3), (3.6), and (3.7) hold for $u_2(X)$.

**Proposition 5.3.** *With C as in* (5.1), $\operatorname{ht}(C) = 2$.

For the next few results (up through (5.13)) we give (for each fixed integer $n \geqslant 2$) several necessary and sufficient conditions for $\mathbb{Z}[x_n]$ to be a Dedekind domain. These results are analogous to the results in Section 4, and their proofs are similar to the corresponding results in Section 4, so we omit the proofs. (In (5.4), which is the $u_n(X)$ analog of (4.4), we use "regular ring" in place of "Dedekind domain," since $\mathbb{Z}[X]/(u_{3k+2}(X)\mathbb{Z}[X])$ is never an integral domain (by [14]) (so it cannot be a Dedekind domain). However, it could still be a regular ring (but we show in (5.17) that, in fact, it never is). After showing this, we revisit this theorem in (5.20), and then give the $u_n(X)$ power integral basis form of (5.20) (and of (5.4)) in (5.21).)

**Theorem 5.4.** *For each integer $n \geqslant 2$, the following are equivalent*:

(5.4.1) $\mathbb{Z}[x_n] = \mathbb{Z}[X]/((X^n + X + 1)\mathbb{Z}[X])$ *is regular.*
(5.4.2) $\mathbb{Z}[y_n] = \mathbb{Z}[X]/((X^n + X^{n-1} + 1)\mathbb{Z}[X])$ *is regular.*
(5.4.3) $\mathrm{Disc}(u_n(X))$ *is square-free in* $\mathbb{Z}$.
(5.4.4) $\rho_n = (-1)^n[n^n + (1-n)^{n-1}]$ *is square-free in* $\mathbb{Z}$.

*If these hold, then a prime $\pi \in \mathbb{Z}$ ramifies in $\mathbb{Z}[x_n]$ if and only if it ramifies in $\mathbb{Z}[y_n]$.*

It follows from (5.2) (and (5.3)) that (3.2)(i) and (ii) hold for $C$, so we can apply (3.6) to the trinomials $u_n(X)$.

**Proposition 5.5.** $\mathbb{Z}[x_n] = \mathbb{Z}[X]/(u_n(X)\mathbb{Z}[X])$ *is a Dedekind domain for $n = 2$ and for $n = 3, 4, \dots, 49$ and $n \not\equiv 2 \pmod 3$. Further 59 is the smallest prime $\pi$ such that $\pi^2$ divides some $\rho_n$ (with $n \not\equiv 2 \pmod 3$), and 339 is the smallest $n$ such that $59^2$ divides $\rho_n$. So each $n$ such that $n \not\equiv 2 \pmod 3$ and $\mathbb{Z}[x_n] = \mathbb{Z}[X]/(u_n(X)\mathbb{Z}[X])$ is not a Dedekind domain is divisible by $\pi^2$ for some prime $\pi \geqslant 59$.*

The program in (4.7) was used to show the "Further" part of (5.5). By using a variation of that program (searching for a square prime factor of $\rho_n$ with $50 < n < 339$ and $n \not\equiv 2 \pmod 3$ and $60 < p < 2\,000\,000$), Mathematica shows that 339 is the smallest $n < 340$ with a repeated prime factor $p < 2\,000\,000$.

**Lemma 5.6.** *For all integers $n \geqslant 2$ and prime integers $\pi > 2$, $\rho_n \equiv \rho_{n+i(\pi^3-\pi^2)} \pmod{\pi^2}$ for all positive integers $i$.*

**Remark 5.7.** In the principal ideal domain $(\mathbb{Z}/(\pi_i\mathbb{Z}))[X] = \mathbb{Z}[X]/(\pi_i\mathbb{Z}[X])$ let $\overline{f_{i,j}}(X)$ be distinct monic irreducible polynomials such that no $\overline{f_{i,j}}(X)$ is an associate of $\overline{l_n(X)} = \overline{n-1}X + \bar{n}$ and such that $X^n + X + \bar{1} = \overline{v_i}(\overline{f_{i,1}}(X))^{g_{i,1}} \cdots (\overline{f_{i,k_i}}(X))^{g_{i,k_i}}(\overline{n-1}X + \bar{n})^{h_i}$ is a factorization of $X^n + X + \bar{1}$ into irreducible factors (where $\overline{v_i}$ is the unit $(\bar{n} - \bar{1})^{-h_i} \in \mathbb{Z}/(\pi_i\mathbb{Z})$). Then $h_i = 2$ and $g_{i,j} = 1$ for $i = 1, \dots, e$ and $j = 1, \dots, k_i$.

**Notation 5.8.** With the notation of (5.7), for $i = 1, \dots, e$ and for $j = 1, \dots, k_i$, let $f_{i,j}(X)$ be distinct monic irreducible polynomials in the UFD $\mathbb{Z}[X]$ such that $f_{i,j}(X) + \pi_i\mathbb{Z}[X] = \overline{f_{i,j}}(X)$, let $Q_{i,j} = (\pi_i, f_{i,j}(X))\mathbb{Z}[X]$, let $p_i = P_i/(u_n(X)\mathbb{Z}[X])$, and let $Q_{i,j}/(u_n(X)\mathbb{Z}[X]) = q_{i,j}$.

**Remark 5.9.** Each $Q_{i,j}$ is a maximal ideal such that $l_n(X) \notin Q_{i,j}$, $u_n(X) \in Q_{i,j}$, and $Q_{i,j}\mathbb{Z}[X]_{Q_{i,j}} = (\pi_i, u_n(X))\mathbb{Z}[X]_{Q_{i,j}}$, so $q_{i,j}\mathbb{Z}[x_n]_{q_{i,j}} = \pi_i\mathbb{Z}[x_n]_{q_{i,j}}$.

**Remark 5.10.** (5.10.1) There exists $q(X) \in \mathbb{Z}[X] \setminus (P_1 \cup \cdots \cup P_e)$ such that $(1-n)^{n-1}u'_n(X) = l_n(X)q(X) + \rho_n$.

(5.10.2) Let $g^*(X) = (1-n)^{n-3}X^{n-2} + 2n(1-n)^{n-4}X^{n-3} + \cdots + in^{i-1}(1-n)^{n-i-2} X^{n-i-1} + \cdots + (n-2)n^{n-3}X - n^{n-2}$. Then: $g^*(X) \in \mathbb{Z}[X] - (P_1 \cup \cdots \cup P_e)$; $Q_{i,j}\mathbb{Z}[X]_{Q_{i,j}} = (\pi_i, g^*(X))\mathbb{Z}[X]_{Q_{i,j}}$ for $i = 1, \ldots, e$ and $j = 1, \ldots, k_i$; and $(1-n)^{n-1}u_n(X) = (l_n(X))^2 g^*(X) + (-1)^n \rho_n(X+1)$.

**Proposition 5.11.**

(5.11.1) $C = (u_n(X), u'_n(X))\mathbb{Z}[X] = (l_n(X), u_n(X))\mathbb{Z}[X] = (l_n(X), u'_n(X))\mathbb{Z}[X] = (\rho_n, l_n(X))\mathbb{Z}[X]$. *Also,* $C\mathbb{Z}[X]_{P_i} = (\rho_n, u'_n(X))\mathbb{Z}[X]_{P_i}$ *for* $i = 1, \ldots, e$.

(5.11.2) $(\rho_n, (l_n(X))^2)\mathbb{Z}[X] = ((l_n(X))^2, u_n(X))\mathbb{Z}[X]$. *Also,* $(\rho_n, u_n(X))\mathbb{Z}[X]_{P_i} = (\rho_n, (l_n(X))^2)\mathbb{Z}[X]_{P_i} = ((l_n(X))^2, u_n(X))\mathbb{Z}[X]_{P_i}$ *for* $i = 1, \ldots, e$.

**Corollary 5.12.** $\rho_n L_i = (l_n(x_n))^2 L_i$, *where* $L_i = \mathbb{Z}[x_n]_{p_i}$ (*with* $p_i = P_i/(u_n(X)\mathbb{Z}[X])$) *for* $i = 1, \ldots, e$.

**Theorem 5.13.** *Let* $\mathbb{Z}[x'_n] = \mathbb{Z}[X]/(u'_n(X)\mathbb{Z}[X])$ *and let* $\mathbb{Z}[x_n] = \mathbb{Z}[X]/(u_n(X)\mathbb{Z}[X])$. *Then the following statements are equivalent*:

(5.13.1) $\mathbb{Z}[x_n]$ *is a Dedekind domain.*
(5.13.2) $\rho_n\mathbb{Z}$ *is a radical ideal.*
(5.13.3) $C$ *is a radical ideal in* $\mathbb{Z}[X]$.
(5.13.4) $l_n(x_n)\mathbb{Z}[x_n]$ *is a radical ideal.*
(5.13.5) $u'_n(x_n)\mathbb{Z}[x_n]$ *is a radical ideal.*
(5.13.6) $l_n(x'_n)\mathbb{Z}[x'_n]$ *is a radical ideal.*
(5.13.7) $u_n(x'_n)\mathbb{Z}[x'_n]$ *is a radical ideal.*
(5.13.8) $\rho_n\mathbb{Z}[x'_n]_{q_i} = q_i\mathbb{Z}[x'_n]_{q_i}$ *for* $i = 1, \ldots, e$, *where* $q_i = P_i/(u'_n(X)\mathbb{Z}[X])$.
(5.13.9) $u_n(\frac{n}{1-n})\mathbb{Z}[\frac{n}{1-n}]$ *is a radical ideal.*
(5.13.10) $u'_n(\frac{n}{1-n})\mathbb{Z}[\frac{n}{1-n}]$ *is a radical ideal.*
(5.13.11) $\rho_n\mathbb{Z}[\frac{n}{1-n}]$ *is a radical ideal.*
(5.13.12) $l_n(X)(\mathbb{Z}/(\rho_n\mathbb{Z}))[X]$ *is a radical ideal.*
(5.13.13) $u'_n(X)(\mathbb{Z}[X]/(\rho_n\mathbb{Z}[X]))_{m_i} = m_i(\mathbb{Z}[X]/(\rho_n\mathbb{Z}[X]))_{m_i}$ *for* $i = 1, \ldots, e$, *where* $m_i = P_i/(\rho_n\mathbb{Z}[X])$.
(5.13.14) $(l_n(X))^2 g^*(X) \notin (\pi_i^2, \pi_i l_n(X), u_n(X))\mathbb{Z}[X]$ *for* $i = 1, \ldots, e$, *where* $g^*(X)$ *is as in* (5.10.2).
(5.13.15) $(l_n(X))^2 g(X) \notin (\pi_i^2, \pi_i l_n(X), u_n(X))\mathbb{Z}[X]$ *for* $i = 1, \ldots, e$ *and for all* $g(X) \in \mathbb{Z}[X] \setminus P_i$.
(5.13.16) $\pi_i\mathbb{Z}[x_n]_{p_i}$ *is not a reduction of* $p_i\mathbb{Z}[x_n]_{p_i}$ *for* $i = 1, \ldots, e$ (*where* $P_i/(u_n(X)\mathbb{Z}[X]) = p_i$).

In the remainder of this section we show that $\mathbb{Z}[X]/(u_n(X)\mathbb{Z}[X])$ is not a regular ring when $n > 2$ and $n \equiv 2 \pmod 3$. For this, we begin by defining the polynomial that is the co-factor of $u_2(X)$ for $u_{3k+2}(X)$ (see (5.15.2)).

**Definition 5.14.** For each positive integer $n$ let $h_{3n}(X) = X^{3n} - X^{3n-1} + X^{3n-3} - X^{3n-4} + \cdots + X^3 - X^2 + 1$.

**Remark 5.15.** (5.15.1) It should be noted that $h_{3n}(X)$ can be defined recursively by: $h_3(X) = X^3 - X^2 + 1$ and for $n > 1$, $h_{3n}(X) = X^3 h_{3(n-1)}(X) - X^2 + 1$.

(5.15.2) Selmer proved in [14] that, for all positive integers $k$, $u_{3k+2}(X) = u_2(X)h_{3k}(X)$ and that $u_2(X), h_{3k}(X)$ are irreducible in $\mathbb{Z}[X]$.

**Lemma 5.16.** *With the above notation, we have*

$$\operatorname{Res}\bigl(u_2(X), h_{3n}(X)\bigr) = (n+1)^2 + n^2 + n(n+1) = 3n^2 + 3n + 1.$$

**Proof.** Let $\zeta, \zeta^2$ be the roots of the cyclotomic polynomial $u_2(X) = X^2 + X + 1 = \Phi_3(X)$ (so $\zeta^3 = 1$). We first prove, by induction on $n$, the identities

$$h_{3n}(\zeta) = n + 1 - n\zeta^2 \quad \text{and} \quad h_{3n}\bigl(\zeta^2\bigr) = n + 1 - n\zeta.$$

For $n = 1$, we have $h_3(\zeta) = \zeta^3 - \zeta^2 + 1 = 2 - \zeta^2$ and $h_3(\zeta^2) = \zeta^6 - \zeta^4 + 1 = 2 - \zeta$. Assuming the result for $n = k - 1$, we have by (5.15.1), $h_{3k}(\zeta) = \zeta^3 h_{3(k-1)}(\zeta) - \zeta^2 + 1 = [k - (k-1)\zeta^2] - \zeta^2 + 1 = (k+1) - k\zeta^2$ and $h_{3k}(\zeta^2) = \zeta^3 h_{3(k-1)}(\zeta^2) - \zeta^4 + 1 = [k - (k-1)\zeta] - \zeta + 1 = (k+1) - k\zeta$.

Using the above identities and [6, Eq. (2), p. 203], we get that $\operatorname{Res}(u_2(X), h_{3n}(X)) = h_{3n}(\zeta)h_{3n}(\zeta^2) = (n + 1 - n\zeta^2)(n + 1 - n\zeta) = (n+1)^2 + n^2 + n(n+1) = 3n^2 + 3n + 1$. □

**Theorem 5.17.** *For all $n \in \mathbb{N}$, $\mathbb{Z}[x_{3n+2}] = \mathbb{Z}[X]/(u_{3n+2}(X)\mathbb{Z}[X])$ is not a regular ring.*

**Proof.** By (5.16), $\operatorname{Res}(u_2(X), h_{3n}(X)) = 3n^2 + 3n + 1$. Thus, if $\pi$ is a prime integer dividing $3n^2 + 3n + 1$, then by (2.3), $u_2(X)$ and $h_{3n}(X)$ are contained in a height 2 prime ideal $P = (\pi, g(X))\mathbb{Z}[X]$ of $\mathbb{Z}[X]$. Let $p = P + u_{3n+2}\mathbb{Z}[X]$ in $\mathbb{Z}[X]/(u_{3n+2}(X)\mathbb{Z}[X]) = \mathbb{Z}[x_{3n+2}]$. Then $\mathbb{Z}[x_{3n+2}]_p$ is not an integral domain (since both the associated prime ideals of zero in $\mathbb{Z}[x_{3n+2}]$ (namely, $u_2(x_{3n+2})\mathbb{Z}[x_{3n+2}]$ and $h_{3n}(x_{3n+2})\mathbb{Z}[x_{3n+2}]$) are contained in $p$), and thus $\mathbb{Z}[x_{3n+2}]$ is not a regular ring. □

**Corollary 5.18.** *The integer $n^n + (1-n)^{n-1}$ is not square-free for any integer $n > 2$ with $n \equiv 2 \pmod 3$.*

**Proof.** Since by (5.17), $\mathbb{Z}[X]/(u_{3n+2}(X)\mathbb{Z}[X])$ is not a regular ring for such integers $n$, $n^n + (1-n)^{n-1}$ is not square-free for such $n$ by (5.4). □

**Remark 5.19.** A natural question now is to find a square $> 1$ dividing $n^n + (1-n)^{n-1}$ for $n = 3k + 2$. Observe that if $f, g \in R[X]$ (any ring $R$), then

$$\begin{aligned}\operatorname{Res}\bigl(fg, (fg)'\bigr) &= \operatorname{Res}(fg, f'g + fg') = \operatorname{Res}(f, f'g + fg')\operatorname{Res}(g, f'g + fg')\\ &= \operatorname{Res}(f, f'g)\operatorname{Res}(g, fg') = \pm\operatorname{Res}(f, f')\operatorname{Res}(f, g)^2\operatorname{Res}(g, g').\end{aligned}$$

Taking $f = u_2(X)$ and $g = h_{3k}(X)$, and $n = 3k + 2$, we have by (5.15.2) that, for all positive integers $k$, $u_{3k+2}(X) = u_2(X)h_{3k}(X)$. Also, by (5.16) we have $\operatorname{Res}(u_2(X), h_{3k}(X)) =$

$3k^2+3k+1$. Therefore $(\mathrm{Res}(u_2(X),h_{3k}(X)))^2=(3k^2+3k+1)^2$ divides $\mathrm{Disc}(u_{3k+2}(X))=\pm\mathrm{Res}(u_{3k+2}(X),u_{3k+2}(X)')=n^n+(1-n)^{n-1}=(3k+2)^{3k+2}+(-3k-1)^{3k+1}$.

**Corollary 5.20.** *For each integer $n\geqslant 2$, the following are equivalent*:

(5.20.1) $\mathbb{Z}[x_n]=\mathbb{Z}[X]/((X^n+X+1)\mathbb{Z}[X])$ *is a Dedekind domain.*
(5.20.2) $\mathbb{Z}[y_n]=\mathbb{Z}[X]/((X^n+X^{n-1}+1)\mathbb{Z}[X])$ *is a Dedekind domain.*
(5.20.3) $\mathrm{Disc}(u_n(X))$ *is square-free in* $\mathbb{Z}$.
(5.20.4) $\rho_n=(-1)^n[n^n+(1-n)^{n-1}]$ *is square-free in* $\mathbb{Z}$.

*If these hold, then*: *A prime $\pi\in\mathbb{Z}$ ramifies in $\mathbb{Z}[x_n]$ if and only if it ramifies in $\mathbb{Z}[y_n]$*; *and, either $n=2$ or $n\not\equiv 2$* (mod 3).

**Proof.** If $n=2$ or if $n\not\equiv 2$ (mod 3), then $\mathbb{Z}[x_n]$ and $\mathbb{Z}[y_n]$ are domains by [14], and thus for these $n$, $\mathbb{Z}[x_n]$ (respectively $\mathbb{Z}[y_n]$) is Dedekind if and only if it is regular. If $n\neq 2$ and $n\equiv 2$ (mod 3), then $\mathbb{Z}[x_n]$ and $\mathbb{Z}[y_n]$ are not domains by [14], and thus for these $n$, $\mathbb{Z}[x_n]$ and $\mathbb{Z}[y_n]$ are not Dedekind. The result thus follows from (5.18) and (5.4). □

The next result is the power integral basis form of Corollary 5.20.

**Corollary 5.21.** *Let $n\geqslant 2$ be an integer and let $\alpha,\beta\in\mathbb{C}$ be roots of $u_n(X)=X^n+X+1$ and $X^n+X^{n-1}+1$, respectively. Then the following are equivalent*:

(5.21.1) $\{1,\alpha,\ldots,\alpha^{n-1}\}$ *is a $\mathbb{Z}$-basis for the integers $\mathbb{Z}_{\mathbb{Q}(\alpha)}$ of $\mathbb{Q}(\alpha)$.*
(5.21.2) $\{1,\beta,\ldots,\beta^{n-1}\}$ *is a $\mathbb{Z}$-basis for the integers $\mathbb{Z}_{\mathbb{Q}(\beta)}$ of $\mathbb{Q}(\beta)$.*
(5.21.3) $\mathrm{Disc}(u_n(X))$ *is square-free.*
(5.21.4) $\rho_n=(-1)^n[n^n+(1-n)^{n-1}]$ *is square-free in* $\mathbb{Z}$.

*If these hold, then*: *A prime $\pi\in\mathbb{Z}$ ramifies in $\mathbb{Z}[\alpha]$ if and only if it ramifies in $\mathbb{Z}[\beta]$*; *and, either $n=2$ or $n\not\equiv 2$* (mod 3).

**Remark 5.22.** It can be shown (much as in the proof of (5.17)) that, for all positive integers $k$ and for each prime factor $\pi$ of $3k^2+3k+1$, the prime ideal $P=(\pi,(3k+1)X+(3k+2))\mathbb{Z}[X]$ contains both $u_2(X)$ and $h_{3k}(X)$, so $p=P/(u_{3k+2}(X)\mathbb{Z}[X])$ splits in the integral closure $\mathbb{Z}[x_{3k+2}]'=\mathbb{Z}[x_2]\oplus(\mathbb{Z}[y_{3k}])'$ of $\mathbb{Z}[x_{3k+2}]$, where $y_{3k}=X+h_{3k}(X)\mathbb{Z}[X]$.

## References

[1] W. Adams, D. Shanks, Strong primality tests that are not sufficient, Math. Comp. 39 (1982) 255–300.
[2] T. Albu, On a paper of Uchida concerning simple finite extensions of Dedekind domains, Osaka J. Math. 16 (1979) 65–69.
[3] S. Arno, A note on Perrin pseudoprimes, Math. Comp. 56 (1991) 371–376.
[4] I. Gaál, Diophantine Equations and Power Integral Bases, New Computational Methods, Birkhäuser, Boston, MA, 2002.
[5] I. Kaplansky, Commutative Rings, Allyn and Bacon, Boston, MA, 1970.
[6] S. Lang, Algebra, third ed., Addison–Wesley, Reading, MA, 1993.
[7] E. Lucas, Theorie des Fonctions Numeriques Simplement Periodiques, Amer. J. Math. 1 (1878) 184–245.
[8] M. Nagata, Local Rings, Interscience, Wiley, New York, 1962.
[9] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, Springer-Verlag, New York, 1990.
[10] H. Osada, The Galois groups of the polynomials $X^n+aX^l+b$, J. Number Theory 25 (1987) 230–238.

[11] R. Perrin, Item 1484, L'Intermèdiare Math. 6 (1899) 76–77.
[12] M. Raynaud, Anneaux Local Hensélians, Lecture Notes in Math., vol. 169, Springer-Verlag, New York, 1970.
[13] P. Samuel, Algebraic Theory of Numbers, Houghton Mifflin, Boston, MA, 1970.
[14] E.S. Selmer, On the irreducibility of certain trinomials, Math. Scand. 4 (1956) 287–302.
[15] J.-P. Serre, On a theorem of Jordan, Bull. Amer. Math. Soc. 40 (2003) 429–440.
[16] Ian Stewart, Tales of a neglected number, Sci. Amer. (1996) 102–103.