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 $\mathrm{Disc}(X^n - X - 1) = \pm(n^n - (1-n)^{n-1})$ of $X^n - X - 1$ is square-free (respectively $\mathrm{Disc}(X^n + X + 1) = \pm(n^n + (1-n)^{n-1})$ 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 $\{1, \alpha, \dots, \alpha^{n-1}\}$. 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 $\{1, \alpha, \dots, \alpha^{n-1}\}$ is that in this case, determining how a rational prime p factors in $\mathbb{Z}_K$ reduces to factoring the minimal monic polynomial of α 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 π 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 $(x_1, \dots, x_n) \in B^n$, then the *discriminant of* $(x_1, \dots, x_n)$ is defined as $\mathrm{Disc}(x_1, \dots, x_n) = \det(\mathrm{Tr}_{B/A}(x_i x_j))$, 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 $(y_1, \dots, y_n) \in B^n$ and $y_i = \sum_{j=1}^{n} a_{i,j} x_j$, then $\mathrm{Disc}(y_1, \dots, y_n) = \det(a_{ij})^2 \, \mathrm{Disc}(x_1, \dots, x_n)$. It follows that if $(x_1, \dots, x_n)$ is a basis of B, then $(y_1, \dots, y_n)$ is a basis of B if and only if $\mathrm{Disc}(x_1, \dots, x_n)$ and $\mathrm{Disc}(y_1, \dots, y_n)$ are associates. Further, if $(y_1, \dots, y_n)$ is not a basis of B, then $\mathrm{Disc}(y_1, \dots, y_n)$ is divisible by a square. Thus the square-freeness of the integer $\mathrm{Disc}(y_1, \dots, y_n)$ is a sufficient condition for $(y_1, \dots, y_n)$ 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 $\mathrm{Disc}(1, x, \dots, x^{n-1}) = \mathbf{Disc}(\mathbf{f}(\mathbf{x}))$ (= 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 $\mathrm{Disc}(1, x, \dots, x^{n-1})$ is square-free. We are then able to show that $\mathrm{Disc}(1, x, \dots, x^{n-1})$ 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 θ is a root of an irreducible monic $f(X) \in \mathbb{Q}[X]$, and considering when $\{1, \theta, \dots, \theta^{n-1}\}$ 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