Contributions to Discrete Mathematics

Volume 2, Number 1, Pages 44–61
ISSN 1715-0868

AN EXPLICIT TREATMENT OF BIQUADRATIC FUNCTION FIELDS

QINGQUAN WU AND RENATE SCHEIDLER

Abstract. We provide a comprehensive description of biquadratic function fields and their properties, including a characterization of the cyclic and radical cases as well as the constant field. For the cyclic scenario, we provide simple explicit formulas for the ramification index of any rational place, the field discriminant, the genus, and an algorithmically suitable integral basis. In terms of computation, we only require square and fourth power testing of constants, extended gcd computations of polynomials, and the squarefree factorization of polynomials over the base field.

1. Introduction

Efficient computation in algebraic function fields can be quite challenging. While there exist theoretical results for finding quantities such as signatures and constant fields, these methods can be complicated or do not lend themselves well to explicit computation. With the exception of quadratic and, to some extent, certain other types of fields (such as cubic, superelliptic, and Artin-Schreier extensions), there are very few effective descriptions or explicit formulas available.

In this paper, we provide a comprehensive description of biquadratic function fields, including explicit formulas and characterizations. These fields are degree 4 extensions of a rational function field (of characteristic different from 2) that have an intermediate quadratic subfield; they include all quartic Galois extensions. We first give a method for finding a computationally suitable minimal polynomial of a biquadratic extension. From this so-called standard form, it is possible to determine the constant field and characterize cyclic and radical extensions completely and explicitly. Furthermore, for the cyclic scenario (and a perfect base field), we can find the ramification index of any rational place, and use this quantity to develop simple formulas for the discriminant and the genus, and ultimately, to state

Received by the editors May 10, 2006, and in revised form December 19, 2006.

2000 *Mathematics Subject Classification.* Primary 11R16. Secondary 11R58, 11R27, 14H05.

Key words and phrases. Biquadratic function field, constant field, cyclic extension, radical extension, genus, discriminant, integral basis.

Research of the second author supported by NSERC of Canada.

explicitly a computationally suitable triangular integral basis of our extension. "Triangular" here means that if we write our biquadratic field in the form $K = k(t, \rho)$, then the transformation matrix with respect to the basis $\{1, \rho, \rho^2, \rho^3\}$ of the extension $K/k(t)$ is triangular, and is in fact sparse, i.e. every row has only one or two non-zero entries.

Methods for computing an integral basis of a field extension, such as the Round 2 algorithm and its variants, were given in [17] and [3], and have been implemented in Magma [2] [13] and KANT [11]. Integral bases for certain types of quartic number fields were given in [10] and [9]. For function fields over algebraically closed fields of characteristic 0, we refer to [20], and function fields over the rationals were discussed in [21]. For global separable function fields, a result of Chistov [4] implies that an integral basis can be computed in time that is polynomial in the extension degree and the coefficient degrees of the minimal polynomial. In fact, by adapting the above mentioned algorithm given in [3], Chistov's result extends to almost all fields, with some minor extra conditions on the base field if the degree of the extension exceeds the characteristic, see [8]. However, Chistov's method is complicated, whereas our technique is simple and straightforward. Moreover, our integral basis construction does not require any algorithm such as the ones cited above, and it has the added advantage that we can derive a very explicit complexity result, namely that the running time is at the very worst cubic (and frequently significantly better than cubic) in the number of operations in the base field.

The only restriction on our base field k is that its characteristic be different from 2; for Sections 7 and 8, we also require k to be perfect. All our results can be obtained solely and directly from the defining polynomial of our biquadratic extension. All that is needed are a few squarefree factorizations and extended gcd's (the latter only for the integral basis) of polynomials over k, as well as square and fourth power tests on constants in k. No other algorithms are required. Moreover, the type of sparse integral basis that we provide here for a biquadratic function field need not exist in a biquadratic number field.

2. Overview and Notation

A general introduction to function fields can be found in [19] and [18]; we only summarize some basic terminology and standard results here. Throughout this paper, let k be a field and t a fixed transcendental element over k. A *function field* K is a finite extension of $k(t)$. We assume that the characteristic of k, denoted by $\mathrm{char}(k)$, is either 0 or not a divisor of the extension degree $n = [K : k(t)]$, so $K/k(t)$ is separable. The *constant field* k' of K is the set of elements in K that are algebraic over k; note that $[k' : k]$ divides n. If $k' = k$, or equivalently, any minimal polynomial of the extension $K/k(t)$ is absolutely irreducible, then k' is the *full* constant field of k. The integral closure $\mathcal{O}_K$ of $k[t]$ is the *maximal order* or *coordinate ring* of K;

it is a subring of K and a free $k[t]$-module of rank n whose discriminant is referred to as the *discriminant* of $K/k(t)$ and is denoted by $\mathrm{disc}(K)$. A $k[t]$-basis of $\mathcal{O}_K$ is called an *integral basis* of K.

Denote by $\mathbb{P}_K$ the set of *places* of K. Every place of K corresponds to a normalized discrete valuation $v_P : K \to \mathbb{Z} \cup \{\infty\}$. All places of $k(t)$, except for the *infinite place* P_∞, are said to be *finite* and can be bijectively identified with the monic irreducible polynomials in $k[t]$. For non-zero $F \in k[t]$ and $P \in \mathbb{P}_{k(t)}$, $v_P(F)$ is the exact power of P that divides F if P is finite, and $v_{P_\infty}(F) = -\deg(F)$.

Let L be any function field containing K with $\mathrm{char}(k) \nmid [L : K]$, and let $P \in \mathbb{P}_K$ and $P' \in \mathbb{P}_L$. The tuple of pairs $(e(P'|P), f(P'|P))$ with P' lying over P, usually sorted in lexicographical order, is the *P-signature* of L/K; here, $e(P'|P), f(P'|P)$ denote the *ramification index* and the *relative degree* of $P' \mid P$, respectively. If L/K is Galois, then all $P' \mid P$ have the same ramification index and relative degree; for brevity, we denote these quantities by $e(P)$ and $f(P)$, respectively, and the number of places lying above P by $r(P)$. We have $\sum_{P'|P} e(P'|P)f(P'|P) = [L : K]$. The extension L/K is *tame* if $\mathrm{char}(k) = 0$ or $\mathrm{char}(k) \nmid e(P'|P)$ for any place $P \in \mathbb{P}_K$ and any $P' \in \mathbb{P}_L$ with $P' \mid P$. When L/K is tame, for any $P \in \mathbb{P}_K$, we define the quantity

$$\delta_{L/K}(P) = \sum_{P'|P} (e(P'|P) - 1) f(P'|P). \tag{1}$$

Returning to the case $K/k(t)$, we simply write $\delta_K(P)$ for $\delta_{K/k(t)}(P)$. If k is perfect, then $\delta_K(P) = v_P(\mathrm{disc}(K))$ for every finite place P of $k(t)$. From the Hurwitz genus formula (Theorem III.4.12, p. 88, of [19]), it then follows that the *genus* g of K is given by

$$g = \frac{\deg(\mathrm{disc}(K)) + \delta_K(P_\infty) - 2[K : k(t)]}{2[k' : k]} + 1. \tag{2}$$

3. Biquadratic Function Fields

A *biquadratic function field* is a function field $K = k(t)(\rho)$, where ρ is a fixed root of $f(Y) = Y^4 + AY^2 + B = 0$ with A, $B \in k[t]$, $f(Y)$ is irreducible over $k(t)$, and $\mathrm{char}(k) \neq 2$. Note that $K/k(t)$ is separable and tame, and that the roots of $f(Y) = 0$ are the algebraic functions $\pm\sqrt{(-A \pm \sqrt{A^2 - 4B})/2}$; here, as always, we fix one square-root out of the two candidates in a fixed algebraic closure of K. We denote these four roots by $\pm\rho, \pm\omega$. Without loss of generality, we can assume that there exists no $Q \in k[t] \setminus k$ such that $Q^2 \mid A$ and $Q^4 \mid B$. A function field $K = k(t, \rho)$ with this property, and the minimal polynomial $f(Y)$ of ρ, are said to be in *standard form*. Given A and B, one can efficiently find A_0, $B_0 \in k[t]$ such that $f_0(Y) = Y^4 + A_0Y^2 + B_0 = 0$ is in standard form and defines a biquadratic function field that is $k(t)$-isomorphic to K as follows:

Algorithm 3.1 (Standard Form)

Inputs: $A, B \in k[t]$ where $f(Y) = Y^4 + AY^2 + B$ is irreducible over $k(t)$.
Outputs: $A_0, B_0 \in k[t]$ so that the polynomial $f_0(Y) = Y^4 + A_0Y^2 + B_0$ is in standard form and the respective biquadratic function fields defined by $f(Y)$ and $f_0(Y)$ are $k(t)$-isomorphic.

1: Set $D = \gcd(A, B)$.
2: Compute the squarefree factorizations of D and B, say $D = \prod_i E_i^i$, $B = sgn(B) \prod_j F_j^j$.
3: Compute[1] $E = \prod_i E_i^{\lfloor i/2 \rfloor}$ and $F = \prod_j F_j^{\lfloor j/4 \rfloor}$. Set $Q = \gcd(E, F)$, $A_0 = A/Q^2$, $B_0 = B/Q^4$. Output A_0, B_0.

We recall here that the *squarefree factorization* of a non-zero polynomial $F \in k[t]$ is the unique factorization of F of the form $F = \operatorname{sgn}(F) \prod_i H_i^i$, where $\operatorname{sgn}(F)$ is the leading coefficient of F and all the $H_i \in k[t]$ are monic, squarefree, and pairwise coprime. If $d = \deg(F)$, then the squarefree factorization of F can be found using at worst $O(d^2 \max\{d, \log(q)\})$ operations in k if $k = \mathbb{F}_q$ is a finite field, and $O(d^3)$ operations in k when $\operatorname{char}(k) = 0$ (see Algorithm 3.4.2, p. 125, of [6]); this asymptotic complexity can be considerably improved in many cases.

Note that the polynomial $f_0(Y)$ in Algorithm 3.1 is the minimal polynomial of ρ/Q over $k(t)$.

Henceforth, unless specified otherwise, we let $K = k(t, \rho)$ be a biquadratic function field in standard form, where ρ is a fixed root of $f(Y) = Y^4 + AY^2 + B = 0$ with A, $B \in k[t]$. We assume that we have computed the squarefree parts of $A^2 - 4B$ and B, i.e. we have polynomials $G, H, S, T \in k[t]$ with G, H squarefree, S, T monic, and

$$A^2 - 4B = GS^2, \qquad B = HT^2. \tag{3}$$

The polynomials G, S, H, T can be easily obtained from the squarefree factorizations of $A^2 - 4B$ and B, respectively. Note that since $f(Y)$ is irreducible over $k(t)$, $A^2 - 4B$, and hence G, cannot be a square in $k[t]$.

The following result motivates the term "biquadratic":

Proposition 3.1. (*Biquadratic Characterization*) *Let K be a function field with $[K : k(t)] = 4$ and $\operatorname{char}(k) \neq 2$. Then $K/k(t)$ is biquadratic if and only if it contains a quadratic extension $M/k(t)$.*

Proof. If K is biquadratic, then $K = k(t, \rho)$ where ρ is a fixed root of $Y^4 + AY^2 + B = 0$ with A, $B \in k[t]$. Then $M = k(t, \rho^2) = k(t, \sqrt{G})$ is an extension of $k(t)$ with minimal polynomial $g(Z) = Z^2 + AZ + B$ over $k(t)$, so $M/k(t)$ is our desired quadratic extension.

[1] As usual, $\lfloor r \rfloor$ and $\lceil r \rceil$ denote the floor and the ceiling, respectively, of $r \in \mathbb{R}$, i.e. $\lfloor r \rfloor$ is the maximal integer not exceeding r, and $\lceil r \rceil$ is the minimal integer no less than r.

Conversely, suppose M is a subfield of K with $[K : M] = [M : k(t)] = 2$. Write $M = k(t, \alpha)$ and $K = M(\theta)$ where $\alpha \in M$ and $\theta \in K$. Since $\mathrm{char}(k) \neq 2$, we may assume that $\alpha^2 \in k(t)$ and $\theta^2 \in M$. If we write $\alpha^2 = C$ and $\theta^2 = D + E\alpha$ with $C, D, E \in k(t)$, then it is easy to check that $g(Y) = Y^4 - 2DY^2 + D^2 - E^2C \in k(t)[Y]$ is the minimal polynomial of θ over $k(t)$. So $K = k(t, \theta)$. Let F be the lowest common denominator of D and $D^2 - E^2C$. Then $K = k(t, \rho)$ where $\rho = F\theta$, and the minimal polynomial of ρ over $k(t)$ is $f(Y) = F^4 g(Y/F) = Y^4 + AY^2 + B$ with $A = -2DF^2 \in k[t]$ and $B = F^4(D^2 - E^2C) \in k[t]$. Hence $K/k(t)$ is biquadratic. □

In lieu of Proposition 3.1, many of the results on biquadratic function field extensions $K/k(t)$ that we present here can be derived by obtaining corresponding results in the quadratic extension $M/k(t)$ and the relative quadratic extension K/M. In this sense, biquadratic function fields offer non-trivial examples for relative function field extensions.

4. Constant Field

In many treatments of algebraic function fields $K/k(t)$, it is tacitly assumed that k is the full constant field of K. However, it may be tedious to check this in practice, since determining the extension degree $[k' : k]$ may require factoring the minimal polynomial $f(Y)$ of $K/k(t)$ over $\overline{k}(t)$, where $\overline{k}$ is an algebraic closure of k. In general, if $k = \mathbb{F}_q$ is a finite field, this can be done algorithmically, see [16] and [15]. In fact, it suffices to factor f over $\mathbb{F}_{q^n}(t)$ where $n = [K : k(t)]$.

For the biquadratic scenario, however, we can find the degree $[k' : k]$ in a much more straight-forward manner; in particular, when $K/k(t)$ is cyclic, we have $k' = k$ if and only if G as given in (3) is not a constant, see Corollary 5.2. We will therefore investigate the field of constants of a biquadratic function field in more detail. This has two advantages. Not only does it allow us to include constant field extensions in our discussion, but we are also able to provide a computationally simple characterization, in terms of $f(Y)$, for the case $k' = k$. Furthermore, in view of (2), we also require the extension degree $[k' : k]$ to find the genus of a biquadratic function field.

We let k' be the constant field of a biquadratic function field $K = k(t, \rho)$. Since $[k' : k]$ divides $[K : k(t)] = 4$, we have $[k' : k] \in \{1, 2, 4\}$. Note that $[k' : k] = 4$ if and only if $K = k'(t)$ is a rational function field, and $[k' : k] = 2$ if and only if K is a quadratic extension of $k'(t)$. Before we determine $[k' : k]$ explicitly, we first provide some simple sufficient conditions under which an irreducible polynomial $f(Y) = Y^4 + AY^2 + B$ with $A, B \in k[t]$ is absolutely irreducible, i.e. defines a biquadratic function field with full constant field k.

Proposition 4.1. *Let $f(Y) = Y^4 + AY^2 + B$ with $A, B \in k[t]$ irreducible over $k(t)$. Then f is absolutely irreducible under any of the following conditions:*

(1) *There exists $P \in \mathbb{P}_{k(t)} \setminus \{P_\infty\}$ with $v_P(A) \geq v_P(B) \geq 1$ and $v_P(B)$ is odd;*

(2) $\deg(B)$ *is odd and* $\deg(B) - \deg(A) \geq 2\lceil \deg(B)/4 \rceil$*;*
(3) $\deg(A)$ *is odd and* $\deg(A) \geq \deg(B) \geq 0$.

Proof. Parts 1 and 2 follow from Eisenstein's Criterion (Proposition III.1.14, pp. 66-67, of [19]), applied to an irreducible divisor $\overline{P}$ in $\overline{k}[t]$ of P and to P_∞, respectively. For part 3, direct computation using symbolic factorization reveals that f is absolutely irreducible. □

Conditions 2 and 3 of Proposition 4.1 are easily verifiable, and condition 1 is simple to check, provided $\gcd(A, B)$ can be factored quickly. Unfortunately, the above conditions are not necessary for f to be absolutely irreducible; for example, $f(Y) = Y^4 + Y^2 + t^4$ does not satisfy any of the conditions of Proposition 4.1, but is easily seen to be absolutely irreducible over any field of characteristic different from 2.

To find the full constant field k' of K, we make use of the following:

Lemma 4.2. *Let l be any field of characteristic different from 2 and let $L = l(t, \theta)$ with $\theta^2 = F \in l[t]$ be a quadratic extension of $l(t)$. Then l is the full constant field of L if and only of there exists $P \in \mathbb{P}_{l(t)}$ with $v_P(F)$ odd.*

Proof. We have that $v_P(F)$ is even for all $P \in \mathbb{P}_{l(t)}$ if and only if the squarefree part a of F is a constant in l. Since $[L : l(t)] = 2$, a cannot be a square in k, but it has a square root in the full constant field l' of L. Thus, a is constant if and only if $[l' : l] = 2$. □

Proposition 4.3. *Let $K = k(t, \rho)$ be a biquadratic function field. Then $[k' : k] = 4$ if and only if G is a non-square in k^* and ρ^2 is the product of a non-square in $k(\sqrt{G})^*$ and a square in $k(\sqrt{G})[t]$.*

Proof. Let $M = k(t, \rho^2) = k(t, \sqrt{G})$, and let k'' be the constant field of M. Then $[k' : k] = 4$ if and only if $[k' : k''] = [k'' : k] = 2$. Now $[k'' : k] = 2$ if and only if $v_P(G)$ is even for all $P \in \mathbb{P}_{k(t)}$ by Lemma 4.2. Since G is squarefree, this is equivalent to G being constant, and hence a non-square in k^* by the irreducibility of $f(Y) = Y^4 + AY^2 + B$ over $k(t)$.

Furthermore, this is exactly the case when $k'' = k(\sqrt{G})$, $M = k''(t)$, and $K = M(\rho) = k''(t, \rho)$ with $\rho^2 \in k''[t]$ where we have $\rho^2 = (-A \pm S\sqrt{G})/2$ for one choice of sign. So again by Lemma 4.2, $[k' : k''] = 2$ if and only if $v_{P''}(\rho^2)$ is even for all $P'' \in \mathbb{P}_{k''(t)}$, or equivalently, ρ^2 is the product of a square in $k''(t)$ (and hence in $k''[t]$) and a constant in k'', which again must be a non-square in k'' by the irreducibility of $f(Y)$ over k''. □

Proposition 4.4. *Let $K = k(t, \rho)$ be a biquadratic function field over a perfect field k. Then $[k' : k] = 2$ if and only if $[k' : k] \neq 4$ and either G is a non-square in k^*, or G is non-constant, $H \in k^*$, and exactly one of $-A \pm 2\sqrt{H}T$ is the product of an element in $k(\sqrt{H})^*$ and a square in $k(\sqrt{H})[t]$.*

Proof. Let M and k'' be as in the proof of Proposition 4.3. Then $[k' : k] = 2$ if and only if either $[k'' : k] = 2$, or $k' \neq k'' = k$. The first condition holds

if and only if k is not the full constant field of M, which by Lemma 4.2 is equivalent to $v_P(G)$ even for all $P \in \mathbb{P}_{k(t)}$. As in the previous proof, this is the case if and only if G is a non-square in k^*.

We need to establish that $k' \neq k'' = k$ if and only if H is constant and exactly one of $-A \pm 2\sqrt{H}T$ is the product of an element in $k(\sqrt{H})^*$ and a square in $k(\sqrt{H})[t]$. By Lemma 4.2, $k'' = k$ if and only if $v_P(G)$ is odd for some $P \in \mathbb{P}_{k(t)}$. Since $k'(t)/k(t)$ is a constant field extension and hence unramified by Theorem III.6.3 (a) of [19], this holds if and only if $v_{P'}(G)$ is odd for some $P' \in \mathbb{P}_{k'(t)}$. We thus see that $k' \neq k'' = k$ if and only $[k'(t, \sqrt{G}) : k(t)] = [k'(t, \sqrt{G}) : k'(t)][k'(t) : k(t)] = 2 \cdot 2 = 4$, or equivalently, $K = k'(t, \sqrt{G})$. This in turns holds if and only if $\rho \in k'(t, \sqrt{G})$. Since ρ is integral over $k[t]$, and hence over $k'[t]$, this is the case if and only if ρ is in the integral closure of $k'[t]$ in K, which is $k'[t, \sqrt{G}]$, i.e. if and only if ρ can be written in the form $\rho = C + D\sqrt{G}$ for some $C, D \in k'[t]$.

Recall that $\rho^2 = (-A \pm S\sqrt{G})/2$ for one of the signs. Now $(C + D\sqrt{G})^2 = (-A + S\sqrt{G})/2$ if and only if $(C - D\sqrt{G})^2 = (-A - S\sqrt{G})/2$, so $\rho \in k'[t, \sqrt{G}]$ if and only if there exists $C, D \in k'[t]$ with $(C + D\sqrt{G})^2 = (-A + S\sqrt{G})/2$, or equivalently, $C^2 + D^2G = -A/2$ and $2CD = S/2$, since 1 and $\sqrt{G}$ are linearly independent over $k'[t]$. This in turn is easily verified to hold if and only if the equation

$$16Y^4 + 8AY^2 + (A^2 - 4B) = 0 \tag{4}$$

has a root $C \in k'(t)$ (in which case $D = S/(4C)$); the other three roots are $-C$ and $\pm D\sqrt{G}$. Since the four roots of (4) are $\pm\sqrt{-A \pm 2\sqrt{B}}/2$, we see that (4) has a root in $k'(t)$ if and only if B is a square in $k'(t)$ and at least one of $-A \pm 2\sqrt{B}$ is a square in $k'(t)$. Since $(-A + 2\sqrt{H}T)(-A - 2\sqrt{H}T) = A^2 - 4B = GS^2$ is not a square in $k'(t)$ (as G is non-constant), at most one of $-A \pm 2\sqrt{H}T$ can be a square in $k'(t)$. Now B is a square in $k'(t)$ if and only if $H \in k^*$. Then $-A \pm 2\sqrt{H}T \in k(\sqrt{H})[t]$ is a square in $k'(t)$ if and only if the squarefree part of $-A \pm 2\sqrt{H}T$ in $k(\sqrt{H})(t)$ is constant, i.e. if and only if it is the product of a constant in $k(\sqrt{H})^*$ and a square in $k(\sqrt{H})[t]$. □

The squarefree factorizations of $A^2 - 4B$ and of B will reveal if G, respectively H, is constant. To test the other conditions in Propositions 4.3 and 4.4, it suffices to check that the squarefree part of a polynomial of the form $U + V\sqrt{h}$ in $k(\sqrt{h})[t]$ ($U, V \in k[t]$, $h \in k^*$) is a constant in $k(\sqrt{h})$. This is in fact possible without knowing a square root of h if we use symbolic arithmetic on the polynomial coefficients in $k(\sqrt{h})$ when performing the polynomial divisions in the squarefree factorization algorithm over $k(\sqrt{h})[t]$: as usual, for $a, b, c, d \in k^*$, we have $(a + b\sqrt{h}) \pm (c + d\sqrt{h}) = (a \pm c) + (b \pm d)\sqrt{h}$, $(a + b\sqrt{h})(c + d\sqrt{h}) = (ac + bdh) + (ad + bc)\sqrt{h}$, and if c and d are not both zero, $(c + d\sqrt{h})^{-1} = (c - d\sqrt{h})/(c^2 - d^2h)$.

5. Cyclic Biquadratic Fields

A quartic Galois extension $K/k(t)$ with $\mathrm{char}(k) \neq 2$ has a Galois group that is isomorphic to $\mathbb{Z}_4$ (the *cyclic* case) or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ (the *bicyclic* case). Both these groups have a subgroup of order 2, so $K/k(t)$ has an intermediate quadratic field. It follows from Proposition 3.1 that every quartic Galois extension is biquadratic. In fact, a cyclic quartic extension has a unique intermediate quadratic field, while a bicyclic one has three distinct intermediate quadratic fields. The cyclic case can be characterized as follows (see [12], [14] for a number field analogue).

Theorem 5.1. (*Cyclic Characterization*) *Let $K = k(t, \rho)$ be a biquadratic function field. Then $K/k(t)$ is cyclic if and only if $H = a^2G$ for some $a \in k^*$, or equivalently, if and only if $(A^2 - 4B)B$ is a square in $k[t]$.*

Proof. Recall that $\pm\rho, \pm\omega$ denote the four roots of $f(Y) = Y^4 + AY^2 + B = 0$. Suppose first that $K/k(t)$ is cyclic, and let σ be a generator of the Galois group $\mathrm{Gal}(K/k(t)) \cong \mathbb{Z}_4$. Since σ has order 4 in $\mathrm{Gal}(K/k(t))$, we have $\sigma(\rho) \neq \pm\rho$. By switching ω and $-\omega$ if necessary, we may assume that $\sigma(\rho) = \omega$ without loss of generality. Since $K/k(t)$ is Galois, $K = k(t)(\omega)$, so similarly $\sigma(\omega) = \pm\rho$, hence $\sigma(\rho\omega) = \pm\rho\omega$. If $\rho\omega \in k(t)$, then the plus sign would hold, implying $\sigma^2(\rho) = \sigma(\omega) = \sigma(\rho\omega)/\sigma(\rho) = \rho\omega/\omega = \rho$, in which case σ^2 would be the identity, a contradiction to σ having order 4. Hence $\rho\omega \notin k(t)$.

Since $(\rho\omega)^2 = B$, we have $k(t, \rho\omega) = k(t, \sqrt{B}) = k(t, \sqrt{H})$, and hence $[k(t)(\rho\omega) : k(t)] = 2$. Now $M = k(t, \rho^2) = k(t, \sqrt{G})$ is the unique intermediate quadratic field of $K/k(t)$, so we must have $M = k(t, \sqrt{G}) = k(t, \sqrt{H})$. A simple argument shows that G and H differ by a square factor in $k(t)$, and the fact that G and H are squarefree implies that this factor is constant.

Conversely, suppose that $H = a^2G$ for some $a \in k^*$. Then $\rho\omega = \pm\sqrt{B} \in k(t, \sqrt{H}) = k(t, \sqrt{G}) = k(t, \rho^2)$, hence $\omega \in k(t, \rho)$, implying that $K/k(t)$ is Galois, with a Galois group of order 4. Let $\gamma = (\rho^2 - \omega^2)\rho\omega \in K$. Then

$$\gamma^2 = \left((\rho^2 + \omega^2)^2 - 4(\rho\omega)^2\right)(\rho\omega)^2 = (A^2 - 4B)B = GS^2HT^2 = (aGST)^2,$$

so $\gamma \in k[t]$. Now suppose $\sigma(\rho\omega) = \rho\omega$ for all $\sigma \in \mathrm{Gal}(K/k(t))$. Then $\rho\omega \in k(t)$, and hence B is a square in $k(t)$. Since B and $A^2 - 4B$ differ by a square in $k(t)$, $A^2 - 4B$ is also a square in $k(t)$, contradicting the irreducibility of $f(Y)$ over $k(t)$. Hence there exists $\sigma \in \mathrm{Gal}(K/k(t))$ with $\sigma(\rho\omega) \neq \rho\omega$. Since σ permutes the four roots $\pm\rho, \pm\omega$, this forces $\sigma(\rho\omega) = -\rho\omega$. If $\sigma(\rho) = \pm\rho$, then $\sigma(\omega) = \mp\omega$ for suitable sign, implying $\gamma = \sigma(\gamma) = -\gamma$ which is impossible. Therefore $\sigma(\rho) = \pm\omega$, and since $\sigma(\rho\omega) = -\rho\omega$, we have $\sigma(\omega) = \mp\rho$. But then $\sigma^2(\rho) = -\rho$, so σ does not have order 2. Thus, σ has order 4, and $\mathrm{Gal}(K/k(t)) \cong \mathbb{Z}_4$. □

The above cyclicity criterion only requires a comparison of two polynomials and a square test in k. Note that if $k = \mathbb{F}_q$ is a finite field of order

q, then $b \in k^*$ is a square in k if and only if $b^{(q-1)/2} = 1$, which is easily verifiable.

Corollary 5.2. *Let $K/k(t)$ be a cyclic biquadratic function field. Then $k' = k$ if and only if G is not a constant in k.*

Proof. Clear from Proposition 4.3, Proposition 4.4 and Theorem 5.1. □

6. Radical Quartic Fields

We briefly discuss radical quartic function fields, which are fields of the form $K = k(t)(\sqrt[4]{F})$ for some $F \in k[t]$. Clearly, every radical quartic function field extension $K/k(t)$ is biquadratic (with $A = 0$ and $B = -F$). The following theorem gives simple necessary and sufficient conditions under which the converse holds.

Theorem 6.1. (*Radical Characterization*) *Let $K = k(t, \rho)$ be a biquadratic function field. Then $K/k(t)$ is radical if and only if any one of the following conditions holds:*

1. *-1 is a square in k^* and $H = a^2G$ for some $a \in k^*$;*
2. *-1 is a non-square in k^* and $H = -a^2G$ for some $a \in k^*$;*
3. *B is a square in $k[t]$ and exactly one of $A \pm 2\sqrt{B}$ is a square in $k[t]$.*

Furthermore, condition 1 implies that $K/k(t)$ is cyclic, condition 2 implies that K is not cyclic (i.e. either not Galois or bicyclic Galois), and condition 3 implies that $K/k(t)$ is bicyclic, -1 is a non-square in k^*, and $[k' : k] > 1$.

Proof. A result by Chu and Kang [5] for quartic extensions of characteristic different from 2 states that $K/k(t)$ is radical if and only if either $-B(A^2-4B)$ is a square in $k(t)$ or (4) has a root in $k(t)$. It is easy to see that properties 1 and 2 above are both equivalent to the first of these two conditions. As in the proof of Proposition 4.4, the roots of (4) are $\pm\sqrt{A \pm 2\sqrt{B}}/2$, so this equation has a root in $k(t)$ if and only if condition 3 above holds (the fact that at most one of $A \pm 2\sqrt{B}$ can be a square was already proved in Proposition 4.4).

Now by Theorem 5.1, conditions 1 and 2 imply that $K/k(t)$ is cyclic, respectively, not cyclic. Suppose that condition 3 holds. Since B is a square in $k[t]$, we have $H \in k^*$, so Proposition 4.4 implies that $[k' : k] \geq 2$. Now $\rho\omega = \sqrt{B} \in k(t)$, so $\omega \in k(t, \rho)$, and $K/k(t)$ is hence Galois. Since B is a square and $A^2 - 4B$ is not a square in $k[t]$, $H \in k^2$ and $G \notin k^2$ cannot differ by a constant square, so by Theorem 5.1, $K/k(t)$ cannot be cyclic and is hence bicyclic. Since $K/k(t)$ is radical, -1 cannot be a square in k^* by Kummer theory. □

Note that if $k = \mathbb{F}_q$ is a finite field of order q, then -1 is a square in k^* if and only if $q \equiv 1 \pmod 4$, which is easily verifiable.

7. P-Signatures, Discriminant and Genus — Cyclic Perfect Case

Throughout this and the next section, we only consider cyclic quartic extensions over a perfect field k. While the questions discussed in Sections 7 and 8 can be addressed algorithmically for other biquadratic extensions, it is unclear how to obtain results that are as explicit as those given below for the special case of cyclic quartic extensions.

We begin with a simple description of any P-signature of a radical cyclic quartic function field. First, two useful lemmas:

Lemma 7.1. (*Proposition III.7.3 (b), pp. 110-111, of* [19]) *Let k be a perfect field, E a function field over k, and $L = E(\rho)$ a radical extension of E of degree n with $\rho^n = D \in E$ and* $\mathrm{char}(k) \nmid n$. *If $P \in \mathbb{P}_E$ and $P' \in \mathbb{P}_L$ lies over P, then $e(P'|P) = n/\gcd(n, v_P(D))$.*

Lemma 7.2. (*Satz 1, p. 171, of* [1] *and Proposition 14.6, p. 248, of* [18]) *Let k be a perfect field and let $M = k(t, \alpha)$ with $\alpha^2 = D \in k[t]$ squarefree. Then for any $P \in \mathbb{P}_{k(t)}$, the P-signature in M is given as follows:*

For $P \neq P_\infty$:

$$(e(P), f(P), r(P)) = \begin{cases} (2,1,1) & \text{if } v_P(D) = 1, \\ (1,2,1) & \text{if } v_P(D) = 0 \text{ and} \\ & \quad D \text{ is a non-square in } k(t)/(P), \\ (1,1,2) & \text{if } v_P(D) = 0 \text{ and} \\ & \quad D \text{ is a square in } k(t)/(P). \end{cases}$$

For $P = P_\infty$:

$$(e(P), f(P), r(P)) = \begin{cases} (2,1,1) & \text{if } \deg(D) \text{ is odd,}, \\ (1,2,1) & \text{if } \deg(D) \text{ is even and} \\ & \quad \mathrm{sgn}(D) \text{ is a non-square in } k^*, \\ (1,1,2) & \text{if } \deg(D) \text{ is even and} \\ & \quad \mathrm{sgn}(D) \text{ is a square in } k^*. \end{cases}$$

Theorem 7.3. *Let $K = k(t, \rho)$ a radical cyclic function field over a perfect field k, where $\rho^4 = D \in k[t]$ and D is 4-th power free. Then for any $P \in \mathbb{P}_{k(t)}$, the P-signature of $K/k(t)$ is given as follows:*

$r(P) = 4$, $e(P) = f(P) = 1$ *if*

- $P \neq P_\infty$, $v_P(D) \equiv 0 \pmod 4$, *and* $D/P^{v_P(D)}$ *is a 4-th power in* $k[t]/(P)$,
- $P = P_\infty$, $\deg(D) \equiv 0 \pmod 4$, *and* $\mathrm{sgn}(D)$ *is a 4-th power in* k^*,

$r(P) = 2$, $e(P) = 1$, $f(P) = 2$ *if*

- $P \neq P_\infty$, $v_P(D) \equiv 0 \pmod 4$, *and* $D/P^{v_P(D)}$ *is a square but not a 4-th power in* $k[t]/(P)$,
- $P = P_\infty$, $\deg(D) \equiv 0 \pmod 4$, *and* $\mathrm{sgn}(D)$ *is a square but not a 4-th power in* k^*,

$r(P) = 2$, $e(P) = 2$, $f(P) = 1$ *if*

- $P \neq P_\infty$, $v_P(D) \equiv 2 \pmod 4$, *and* $D/P^{v_P(D)}$ *is a square in* $k[t]/(P)$,
- $P = P_\infty$, $\deg(D) \equiv 2 \pmod 4$, *and* $\operatorname{sgn}(D)$ *is a square in* k^*,

$r(P) = e(P) = 1$, $f(P) = 4$ *if*

- $P \neq P_\infty$, $v_P(D) \equiv 0 \pmod 4$, *and* $D/P^{v_P(D)}$ *is not a square in* $k[t]/(P)$,
- $P = P_\infty$, $\deg(D) \equiv 0 \pmod 4$, *and* $\operatorname{sgn}(D)$ *is not a square in* k^*,

$r(P) = 1$, $e(P) = f(P) = 2$ *if*

- $P \neq P_\infty$, $v_P(D) \equiv 2 \pmod 4$, *and* $D/P^{v_P(D)}$ *is not a square in* $k[t]/(P)$,
- $P = P_\infty$, $\deg(D) \equiv 2 \pmod 4$, *and* $\operatorname{sgn}(D)$ *is not a square in* k^*,

$r(P) = 1$, $e(P) = 4$, $f(P) = 1$ *if*

- $P \neq P_\infty$ *and* $v_P(D)$ *is odd,*
- $P = P_\infty$ *and* $\deg(D)$ *is odd.*

Proof. Set $M = k(t, \rho^2)$. Let $P' \in \mathbb{P}_M$ lie over P and $P'' \in \mathbb{P}_K$ lie over P'. The values for $e(P''|P)$ follow immediately from Lemma 7.1. If $v_P(D)$ is odd, then $e(P''|P) = 4$, so assume now that $v_P(D)$ is even, which forces $e(P''|P) = 2$ or 1.

If $e(P''|P) = 2$, then $M = k(t, \beta)$ with $\beta^2 = D/P^{v_P(D)}$, and we can find the values of $f(P'|P)$ and $r(P'|P)$ using Lemma 7.2. By using $f(P''|P) = f(P''|P')f(P'|P)$ (similarly for $r(P''|P)$), this yields our signatures.

If $e(P''|P) = 1$, then $v_P(D) \equiv 0 \pmod 4$ by Lemma 7.1, so $K = k(t, \gamma)$ with $\gamma^4 = D/P^{v_P(D)}$. By Theorem III.3.7, p. 76, of [19], $r(P''|P)$ is equal to the number of distinct irreducible factors of $Y^4 - D/P^{v_P(D)} \pmod P$, and $f(P''|P) = 4/r(P''|P)$ is equal to the degree of each such factor. □

For biquadratic cyclic (but not necessarily radical) function fields, we only compute the ramification index (rather than the whole signature) for each place of $k(t)$, since it is sufficient for finding the genus and the discriminant by (2) and our remarks at the end of Section 2. We find all these ramification indices by making use of Lemma 7.1.

Theorem 7.4. *Let* $K = k(t, \rho)$ *be a cyclic biquadratic function field in standard form over a perfect field* k*. Then for any* $P \in \mathbb{P}_{k(t)}$*, we have*

$$e(P) = \begin{cases} 1 & \text{if } v_P(A^2 - 4B) \text{ is even and} \\ & \quad \min\{v_P(A),\, v_P(A^2 - 4B)/2\} \text{ is even,} \\ 2 & \text{if } v_P(A^2 - 4B) \text{ is even and} \\ & \quad \min\{v_P(A),\, v_P(A^2 - 4B)/2\} \text{ is odd,} \\ 4 & \text{if } v_P(A^2 - 4B) \text{ is odd.} \end{cases}$$

Proof. As before, set $M = k(t, \sqrt{G}) = k(t, \sqrt{A^2 - 4B})$, and let $\alpha \in K$ with $\alpha^2 \in M$, so $K = M(\alpha)$. Let $P' \in \mathbb{P}_M$ lie over P and $P'' \in \mathbb{P}_K$ lie over P'.

Then by Lemma 7.1,

$$e(P'|P) = \frac{2}{\gcd(2, v_P(A^2-4B))}\ , \quad e(P''|P') = \frac{2}{\gcd(2, v_{P'}(\alpha^2))}\ .$$

Note that since $K/k(t)$ is Galois, we can choose $\alpha = \rho$ or $\alpha = \omega$, in which case $\alpha^2 = (-A \pm \sqrt{A^2-4B})/2$ for one choice of sign. Since $e(P''|P')$ is independent of the choice of α, $v_{P'}(\rho^2)$ and $v_{P'}(\omega^2)$ must have the same parity, and for one of these choices, we must have

$$v_{P'}(\alpha^2) = \min\{v_{P'}(A),\, v_{P'}(\sqrt{A^2-4B})\}. \tag{5}$$

Assume first that $v_P(A^2-4B)$ is odd, so $e(P'|P) = 2$. Since $K/k(t)$ is cyclic, $(A^2-4B)B$ is a square by Theorem 5.1, so $v_P(B)$ is odd as well. Since $v_P(A^2)$ is even, the the strict triangle inequality yields $v_P(A^2-4B) = \min\{v_P(A^2),\, v_P(B)\} = v_P(B) < v_P(A^2)$. If follows that the minimum in (5) is $v_{P'}(\sqrt{A^2-4B}) = v_P(A^2-4B)$ which is also odd. Therefore, $e(P''|P') = 2$ and hence $e(P''|P) = e(P''|P')e(P'|P) = 4$.

Suppose now that $v_P(A^2-4B)$ is even, so $e(P'|P) = 1$, and hence

$$v_{P'}(\alpha^2) = v_P(\alpha^2) = \min\{v_P(A),\, v_P(A^2-4B)/2\}.$$

If this minimum is odd, then $e(P''|P') = 2$ and hence $e(P''|P) = 2$, whereas if the minimum is even, then $e(P''|P') = 1$, implying $e(P''|P) = 1$. □

Corollary 7.5. *Let $K = k(t,\rho)$ be a cyclic biquadratic function field in standard form over a perfect field k. Then for any $P \in \mathbb{P}_{k(t)}$, we have*

$$\delta_K(P) = \begin{cases} 0 & \text{if } v_P(A^2-4B) \text{ is even and} \\ & \quad \min\{v_P(A),\, v_P(A^2-4B)/2\} \text{ is even,} \\ 2 & \text{if } v_P(A^2-4B) \text{ is even and} \\ & \quad \min\{v_P(A),\, v_P(A^2-4B)/2\} \text{ is odd,} \\ 3 & \text{if } v_P(A^2-4B) \text{ is odd,} \end{cases}$$

where $\delta_K(P) = \delta_{K/k(t)}(P)$ was defined in (1).

Using Corollary 7.5, we can now explicitly state the discriminant (Theorem 7.6) and the genus (Corollary 7.7) of a cyclic biquadratic function field.

Theorem 7.6. *Let $K = k(t,\rho)$ be a cyclic biquadratic function field in standard form over a perfect field k. Then*

$$\operatorname{disc}(K) = 16G^3 \gcd(S,T)^2 / \gcd(G,S,T)^2.$$

Proof. For brevity, set $D = \gcd(S,T)$. Then we need to prove that the leading coefficients of $\operatorname{disc}(K)$ and $16G^3$ match, and that $v_P(\operatorname{disc}(K)) = v_P(G^3D^2/\gcd(G,D)^2)$ for every finite $P \in \mathbb{P}_{k(t)}$.

By direct computation, we obtain that the discriminant of ρ is $\operatorname{disc}(\rho) = 16G^3S^4T^2$, so $16\operatorname{sgn}(G)^3 = \operatorname{sgn}(\operatorname{disc}(\rho)) = \operatorname{sgn}(\operatorname{disc}(K))$, since the two

discriminants differ by a factor that is a monic polynomial. Now recall from Section 2 that $v_P(\mathrm{disc}(K)) = \delta_K(P)$, so it suffices to show that

$$v_P(G^3D^2/\gcd(G,D)^2) = \delta_K(P),$$

for each $P \in \mathbb{P}_{k(t)} \setminus \{P_\infty\}$. We compute $v_P(G^3D^2/\gcd(G,D)^2)$ for every possibility of P dividing any combination of G, S, T (including dividing none of them), and compare this value with that of $\delta_K(P)$ given in Theorem 7.4 for each possibility.

Let P be any finite place of $k(t)$. We first claim that $v_P(D) \leq 1$. To that end, suppose that $P^2 \mid D$. Then $P^4 \mid T^2 \mid B$ and $P^4 \mid GS^2 + 4B = A^2$, hence $P^2 \mid A$. But this violates the standard form assumption. So $v_P(D) \leq 1$.

We now divide our proof into different cases, according to which of G, S, T (if any) P divides.

Case 1: $P \nmid GST$:
Then $v_P(G^3D^2/\gcd(G,D)^2) = 0$ and $v_P(\mathrm{disc}(K)) = 0$, since $v_P(\mathrm{disc}(\rho))$ $= 0$ and $\mathrm{disc}(K)$ divides $\mathrm{disc}(\rho)$.

Case 2: $P \mid G$:
Then $v_P(G) = 1$, since G is squarefree. If $P \mid D$, then $v_P(D) = v_P(\gcd(G,D)) = 1$, so $v_P(G^3D^2/\gcd(G,D)^2) = 5 - 2 = 3$. If $P \nmid D$, then $v_P(D) = v_P(\gcd(G,D)) = 0$, so $v_P(G^3D^2/\gcd(G,D)^2) = 3 - 0 = 3$ also. On the other hand, $v_P(A^2 - 4B)$ is odd (again as G is squarefree), so $\delta_K(P) = 3$ by Corollary 7.5. It follows that $v_P(\mathrm{disc}(K)) = v_P(G^3D^2/\gcd(G,D)^2)$.

Case 3: $P \nmid G$, $P \mid ST$:
Then $v_P(G^3D^2/\gcd(G,D)^2) = 2v_P(D)$, so we need to show that $\delta_K(P)$ $= 2v_P(D)$. We see that $v_P(A^2 - 4B) = v_P(GS^2) = 2v_P(S)$ is even. As in the proof of Theorem 7.4, we have $A^2 = G(S^2 + 4a^2T^2)$, so $2v_P(A) = v_P(S^2 + 4a^2T^2)$.

Case 3.1: $P \nmid D$:
Then P divides exactly one of S and T. In both cases, $v_P(A) = v_P(S^2+4a^2T^2)/2 = 0$ by the strict triangle inequality, so $\min\{v_P(A), v_P(A^2-4B)/2\} = 0$ is even. By Corollary 7.5, $\delta_K(P) = 0 = 2v_P(D)$.

Case 3.2: $P \mid D$:
Then $\min\{v_P(S), v_P(T)\} = v_P(D) = 1$.

Case 3.2.1: $v_P(S) \neq v_P(T)$:
Then $v_P(A) = \min\{v_P(S), v_P(T)\} = 1$ is odd, by the strict triangle inequality. Since $v_P(A^2-4B)/2 = v_P(S) \geq v_P(A)$, we see that $\min\{v_P(A), v_P(A^2 - 4B)/2\} = v_P(A) = 1$ is odd, so by Corollary 7.5, $\delta_K(P) = 2 = 2v_P(D)$.

Case 3.2.2: $v_P(S) = v_P(T)$:
Then $v_P(S) = v_P(T) = 1$, since $v_P(D) = 1$. So $v_P(A) \geq \min\{v_P(S), v_P(T)\} = 1$ and $v_P(A^2 - 4B)/2 = v_P(S) = 1$. It

follows that $\min\{v_P(A),\, v_P(A^2-4B)/2\} = v_P(A^2-4B)/2 = 1$ is odd, so once again by Corollary 7.5, $\delta_K(P) = 2 = 2v_P(D)$. □

Note that the analogue to Theorem 7.6 does not hold in general for number fields, due to the fact that the equality $\delta_P(K) = v_P(\mathrm{disc}(K))$ is only true for tamely ramified P after localization and completion on P.

Corollary 7.7. *Let $K = k(t,\rho)$ be a cyclic biquadratic function field in standard form over a perfect field k and with constant field k'. Then K has genus*

$$g = \frac{3\deg(G) + 2\deg(\gcd(S,T)) - 2\deg(\gcd(G,S,T)) + \epsilon - 8}{2[k':k]} + 1,$$

where

$$\epsilon = \begin{cases} 0 & \text{if } \deg(A^2-4B) \text{ is even and} \\ & \quad \max\{\deg(A),\, \deg(A^2-4B)/2\} \text{ is even,} \\ 2 & \text{if } \deg(A^2-4B) \text{ is even and} \\ & \quad \max\{\deg(A),\, \deg(A^2-4B)/2\} \text{ is odd,} \\ 3 & if \deg(A^2-4B) \text{ is odd.} \end{cases}$$

Proof. This follows immediately from Theorem 7.6, (2) and the fact that $\epsilon = \delta_K(P_\infty)$ by Corollary 7.5. □

8. Integral Basis – Cyclic Perfect Case

We conclude our investigation by giving a computationally very suitable integral basis of a cyclic biquadratic function field in standard form over a perfect field. This basis can be found easily from the polynomials G, S, T in (3), and has no number field analogue.

The construction for such a basis is combinatorial and is aided by the explicit formula for $\mathrm{disc}(K)$ given in Theorem 7.6. It makes use of the fact that a set of linearly independent elements in K is an integral basis if and only if every element is integral and the set has the right discriminant, namely $\mathrm{disc}(K)$. To that end, we first start with a set of linearly independent integral elements; without loss of generality, the coefficients of these elements with respect to the $k(t)$-basis $\{1, \rho, \rho^2, \rho^3\}$ of K form a triangular 4×4 matrix with entries in $k(t)$. The assumption that $K/k(t)$ is cyclic Galois further forces certain of the coefficients to vanish. We then maximize the degrees of the denominators of the non-zero coefficients one by one, while still keeping the integrality of every element in the set. The integral basis is obtained when all the degrees of the denominators become maximal. We spare the reader the details of deriving the particular form of our integral basis, i.e. the proof given below is simply a validation of the statement of Theorem 8.1.

Theorem 8.1. *Let $K = k(t, \rho)$ be a cyclic biquadratic function field in standard form over a perfect field k. Then an integral basis of K is given by*

$$\left\{1,\ \rho,\ \frac{\rho^2 + A/2}{S},\ \frac{\rho^3 + C\rho}{ED}\right\}$$

with polynomials $C, D, E, F, L_1, M_1, L_2, M_2 \in k[t]$ given by

$$D = \gcd(G, S, T), \quad E = \operatorname{lcm}(S, T), \quad F = \gcd(S, T),$$

$$L_1 S + M_1 T = F, \quad L_2 E + M_2 D^2 = \gcd(E, D^2) = D,$$

$$C = M_2 A D\, \frac{M_1 T/2 + L_1 S}{F}.$$

Proof. We first show that $D = \gcd(E, D^2)$. It is clear that $D \mid \gcd(E, D^2)$. To show equality, let $P \in \mathbb{P}_{k(t)} \setminus \{P_\infty\}$ with $P \mid \gcd(E, D^2)$. Then $P \mid D$, so if suffices to show that $v_P(E) = 1$ as D is squarefree. Since $B = a^2 G T^2$ for some $a \in k^*$ by Theorem 5.1, we see as in the proof of Theorem 7.6 that $v_P(A^2) = v_P(G(S^2 + 4a^2T^2)) \geq 3$, so $v_P(A) \geq 2$. Since K is in standard form, we must have $v_P(B) \leq 3$, so $v_P(G) = v_P(T) = 1$ and $v_P(GS^2) = v_P(A^2 - 4a^2GT^2) = 3$ by the strict triangle inequality. Hence $v_P(S) = 1$, implying $v_P(E) = 1$.

It now follows that the polynomials L_1, M_1, L_2, M_2, C are all well-defined. Set $\alpha = (\rho^2 + A/2)/S \in K$, and $\beta = (\rho^3 + C\rho)/ED \in K$. Then the minimal polynomial of α is easily verified to be $g(Y) = Y^2 - G/4 \in k[t][Y]$, so α is integral over $k[t]$.

To prove the integrality of β, consider any element of the form $\gamma = (\rho^3 + U\rho)/V \in K$ with $U, V \in k[t]$, $V \neq 0$. We establish necessary and sufficient conditions on U and V under which γ is integral over $k[t]$. A straightforward, though tedious computation yields that the minimal polynomial of γ over $k(t)$ is of the form $Y^4 + H_2 Y^2 + H_0$ where H_2, $H_0 \in k(t)$ are determined uniquely by U and V, and

$$\begin{aligned} &(4A^3B - 3AB^2 - A^5) + 4U(A^4 - 3A^2B + B^2) + 6U^2(2AB - A^3) \\ (6)\qquad &+4U^3(A^2 - B) - U^4 A + V^2 H_2((A^2 - B) - 2AU + U^2) \;=\; 0, \\ &(3A^2B^2 - A^4B - B^3) + 4U(A^3B - 2AB^2) + 6U^2(B^2 - A^2B) \\ (7)\qquad &+4U^3AB - U^4B + V^2H_2(AB - 2BU) + H_0V^4 \;=\; 0. \end{aligned}$$

We wish to simplify (6) by dividing by $U^2 - 2AU + (A^2 - B)$, so we need to ensure that this quantity is non-zero. By Theorem 5.1 and (3), B and $A^2 - 4B$ differ by a square factor in $k(t)$; in particular, B cannot be a square in $k[t]$ as otherwise $A^2 - 4B$ would be a square, making $f(Y)$ reducible over $k(t)$. It follows that the polynomial $h(Y) = Y^2 - 2AY + (A^2 - B)$ of discriminant $4B$ is irreducible over $k[t]$; in particular, $h(U) \neq 0$.

Dividing both sides of (6) by $h(U)$ simplifies (6) to

$$(8)\qquad V^2 H_2 = (A^3 - 3AB) + U(4B - 2A^2) + U^2 A.$$

Substituting (8) into (7), we obtain

$$V^4 H_0 = B(B - AU + U^2)^2. \tag{9}$$

So we see that γ is integral over $k[t]$ if and only if (8) and (9) have solutions (U, V, H_2, H_0) with $U, V, H_2, H_0 \in k[t]$.

It is easy to verify that (A, T, HA, H^3T^2) and $(A/2, S, GA/4, G^2B/16)$ are two such solutions, so $(\rho^3 + A\rho)/T$ and $(\rho^3 + (A/2)\rho)/S$ are both integral over $k[t]$. Using the identities $M_1T + L_1S = F$ and $ST = EF$, we obtain

$$L_1\frac{\rho^3 + A\rho}{T} + M_1\frac{\rho^3 + (A/2)\rho}{S} = \frac{F\rho^3 + (M_1TA/2 + L_1SA)\rho}{ST} = \frac{\rho^3 + C_0\rho}{E},$$

with $C_0 = A(M_1T/2 + L_1S)/F$. It follows that $(\rho^3 + C_0\rho)/E$ is also integral over $k[t]$.

Since D is squarefree, we have $v_D(G) = v_D(S) = v_D(T) = 1$, where $v_D(F)$ refers to the non-negative integer such that $D^{v_D(F)}$ divides F exactly in $k[t]$. So $v_D(B) = 3$, hence $B^3/D^8 \in k[t]$. Furthermore, we saw earlier that $v_D(A) \geq 2$, so $v_D(A^3 - 3AB) = v_D(AG(S^2 + a^2T^2)) \geq 5$, and hence $(A^3 - 3AB)/D^4 \in k[t]$. It is now easy to verify that $(U, V, H_2, H_0) = (0, D^2, (A^3 - 3AB)/D^4, B^3/D^8)$ is another integral solution of (8) and (9), so ρ^3/D^2 is integral over $k[t]$. Since $L_2E + M_2D^2 = D$ and $\operatorname{lcm}(E, D^2) = ED^2/\gcd(E, D^2) = ED$, we obtain

$$M_2\frac{\rho^3 + C_0\rho}{E} + L_2\frac{\rho^3}{D^2} = \frac{D\rho^3 + M_2C_0D^2\rho}{ED^2} = \frac{\rho^3 + C\rho}{ED} = \beta,$$

so β is integral over $k[t]$.

It follows that the elements $1, \rho, \alpha, \beta$ in K are all integral over $k[t]$. Since $EF = ST$, we obtain from Theorem 7.6 that

$$\operatorname{disc}(1, \rho, \alpha, \beta) = \frac{\operatorname{disc}(\rho)}{(SED)^2} = \frac{16G^3S^2T^2}{E^2D^2} = \frac{16G^3F^2}{D^2} = \operatorname{disc}(K).$$

Therefore, $\{1, \rho, \alpha, \beta\}$ is an integral basis of K. □

Note that calculating the integral basis of Theorem 8.1 requires only the squarefree factorizations given in (3) as well as a few extended gcd computations in $k[t]$.

We point out that Theorem 8.1 is based on Theorem 7.6, which does not hold in the number field case. In fact, the simplest integral basis of a cyclic biquadratic number field has a much more complicated and non-uniform description [10], and a sparse integral basis of the form given in Theorem 8.1 need not exist for a biquadratic number field $K = \mathbb{Q}(\rho)$.

For example, let ζ be a primitive 5-th root of unity, and set $K = \mathbb{Q}(\zeta)$. Then $K = \mathbb{Q}(\rho)$ with $\rho = \zeta - \zeta^{-1}$. Since the minimal polynomial of ρ over $\mathbb{Q}$ is $f(Y) = Y^4 + 5Y^2 + 5$, K is a cyclic biquadratic number field in standard form. Using the fact that $\{1, \zeta, \zeta^2, \zeta^3\}$ is an integral basis of $K/\mathbb{Q}$ and that $\beta = (\rho^2 + \rho + 1)/2 = \zeta^3 + \zeta^2 + \zeta$ is integral over $\mathbb{Z}$, we see that the third element of any integral basis of K containing 1 and ρ cannot be of the form $(\rho^2 + a)/b$ with $a, b \in \mathbb{Z}$.

Acknowledgments

The first author wishes to thank Hugh C. Williams for inviting him to visit the University of Calgary and introducing him to the second author for academic collaboration, during which time this work was conceived. Both authors thank the referee for his or her comments.

References

1. E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen*, Math. Zeit. **19** (1924), 153–206.
2. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symb. Comp. **24** (1997), 235–265.
3. J. A. Buchmann and Jr. H. W. Lenstra, *Approximating rings of integers in number fields*, J. Theor. Nombres Bordeaux **6** (1994), 221–260.
4. A. L. Chistov, *The complexity of constructing the ring of integers in a global field*, Soviet. Math. Dokl. **39** (1989), 597–600.
5. H. Chu and M-C. Kang, *Quartic fields and radical extensions*, J. Symb. Comp. **34** (2002), 83–89.
6. H. Cohen, *A Course in Computational Algebraic Number Theory*, GTM, vol. 138, Springer-Verlag, Berlin-Heidelberg, 1993.
7. M. Deuring, *Lectures on the Theory of Algebraic Functions in One Variable*, LNM, vol. 314, Springer-Verlag, Berlin, 1973.
8. F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symb. Comp. **33** (2002), 425–445.
9. J.G. Huard, B.K. Spearman, and K.S. Williams, *Integral bases for quartic fields with quadratic subfields*, J. Number Theory **51** (1995), 103–117.
10. R.H. Hudson and K.S. Williams, *The integers of a cyclic quartic field*, Rocky Mountain J. Math. **20** (1990), 145–150.
11. KANT/KASH, *Computational Algebraic Number Theory/KAnt SHell*, `http://www.math.tu-berlin.de/~kant/kash.html`.
12. K.-C. Kappe and B. Warren, *An elementary test for the Galois group of a quartic polynomial*, Amer. Math. Monthly **96** (1989), 133–137.
13. Magma, *The Magma Computational Algebra System*, `http://magma.maths.usyd.edu.au/magma/`.
14. Y. Motoda, *Notes on quartic fields*, Rep. Fac. Sci. Engrg. Saga. Univ. Math. **32** (2002), 1–19.
15. J. M. Omaña and M. Pohst, *Factoring polynomials over global fields II*, J. Symb. Comp. **40** (2005), 1325–1339.
16. M. Pohst, *Factoring polynomials over global fields I*, J. Symb. Comp. **39** (2005), 617–630.
17. M. Pohst and H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Cambridge University Press, Cambridge, 1997.
18. M. Rosen, *Number theory in function fields*, GTM, vol. 210, Springer-Verlag, New York-Berlin-Heidelberg, 2002.
19. H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 1993.
20. M. van Hoeij, *An algorithm for computing an integral basis in an algebraic function field*, J. Symb. Comp. **18** (1994), 353–363.
21. P.G. Walsh, *A polynomial-time complexity bound for the computation of the singular part of a Puiseux expansion of an algebraic function*, Math. Comp. **69** (2000), 1167–1182.

Department of Mathematics, University of Illinois at Urbana-Champaign

Urbana, IL, USA 61801
E-mail address: qwu@uiuc.edu

Department of Mathematics and Statistics, University of Calgary
Calgary, AB, Canada T2N 1N4
E-mail address: rscheidl@math.ucalgary.ca