HAL
open science

Imaginary bicyclic biquadratic function fields in characteristic two

Yves Aubry, Dominique Le Brigand

▶ To cite this version:

Yves Aubry, Dominique Le Brigand. Imaginary bicyclic biquadratic function fields in characteristic two. Journal of Number Theory, 1999, 77, pp.36–50. hal-00977317

HAL Id: hal-00977317
https://hal.science/hal-00977317v1

Submitted on 15 Apr 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Imaginary bicyclic biquadratic function fields in characteristic two

Yves Aubry and Dominique Le Brigand*

Abstract

We are interested in the analogue of a result proved in the number field case by E. Brown and C.J. Parry and in the function field case in odd characteristic by Zhang Xianke. Precisely, we study the ideal class number one problem for imaginary quartic Galois extensions of $k = \mathbb{F}_q(x)$ of Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ in even characteristic.
Let L/k be such an extension and let K_1, K_2 and K_3 be the distinct subfields extensions of L/k. In even characteristic, the fields K_i are Artin-Schreier extensions of k and L is the compositum of any two of them.
Using the factorization of the zeta functions of this fields, we get a formula between their ideal class numbers which enables us to find all imaginary quartic Galois extensions L/k of Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with ideal class number one.
Key words - Ideal class number, function fields, Artin-Schreier extensions, zeta functions.

1 Introduction

E. Brown and C.J. Parry have shown in [2] that there are exactly 47 imaginary bicyclic biquadratic number fields with ideal class number one. The analogous problem in the function field case consists in checking for all imaginary quartic Galois extensions of $k = \mathbb{F}_q(x)$, with Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, such that their ideal class number is equal to one. If L/k is such an extension, there exists exactly three distincts K_1, K_2 and K_3 subfields of L which are quadratic extensions of k.

*The work of the second author is partially supported by INRIA-Rocquencourt - Projet Codes

In [12], Zhang Xianke has given all solutions to the preceding problem in case of odd characteristic : for each solution, at least one subfield K_i has a zero genus. Our purpose here is to study the problem in even characteristic.

In the following, $\mathbb{F}_q$ will denote the finite field with q elements, with q a power of a prime, and $k = \mathbb{F}_q(x)$ for an x transcendental over $\mathbb{F}_q$. All function fields $F/\mathbb{F}_q$ will be supposed to admit $\mathbb{F}_q$ as full constant field and we always assume that F is contained in a separable closure of k. If F is a finite extension of k, let us denote by $S_\infty(F)$ the set of places of F above the infinite place ∞ of k and by $s_\infty(F)$ the order of $S_\infty(F)$. The elements of $S_\infty(F)$ will be called the **infinite places of** F/k. If $s_\infty(F) = [F : k]$, that is when the infinite place of k splits in F, one says that F/k is **real**, otherwise it is **imaginary**. A quadratic imaginary extension F/k is called **ramified** or **inert** according to whether the infinite place of k is ramified or inert in F.
Let us denote by $\mathcal{O}_F$ the integral closure of $\mathbb{F}_q[x]$ in F. Then $\mathcal{O}_F$ is a Dedekind domain and we denote by $h_{\mathcal{O}_F}$ the order of its ideal class group, called the **ideal class number** of $\mathcal{O}_F$ or of F/k.
A quartic Galois extension F/k of Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ will be called a **bicyclic biquadratic extension of** k.
This paper is organized as follows. In Section 2, we give a relation between the ideal class number of an imaginary bicyclic biquadratic extension L/k and those of the three intermediate field extensions.
In Section 3, for the convenience of the reader, we recall some previously known results concerning Artin-Schreier extensions in even characteristic.
In Section 4, we prove the main theorem which gives all imaginary bicyclic biquadratic extensions L/k such that $h_{\mathcal{O}_L} = 1$.

2 Factorization of class numbers

In this section, we show results analogous to the ones given by Zhang in odd characteristic (see [13]).

2.1 Schmidt's relation

Let F be a finite extension of k and let h_F be its divisor class number, that is the number of rational points over $\mathbb{F}_q$ of the jacobian of F. Then we have the following relation due to F. K. Schmidt ([10]):

$$r_{\mathcal{O}_F} h_{\mathcal{O}_F} = \delta_{\mathcal{O}_F} h_F \,, \tag{1}$$

where $\delta_{\mathcal{O}_F}$ is the gcd of the degrees of the infinite places of F/k and $r_{\mathcal{O}_F}$ is the order of the group of zero-degree divisors with support in $S_\infty(F)$ modulo the principal ones. The **regulator** of F/k, denoted by $R_{\mathcal{O}_F}$, is defined by:

$$r_{\mathcal{O}_F} = \frac{\delta_{\mathcal{O}_F} R_{\mathcal{O}_F}}{\prod_{i=1}^{s_\infty(F)} \deg \wp_i},$$

where the denominator is the product of the degrees of the infinite places of F/k.

Remark 2.1

- *Notice that, if* $\deg \wp_i = 1$ *for all* $\wp_i \in S_\infty(F/k)$*, then* $r_{\mathcal{O}_F} = R_{\mathcal{O}_F}$.
- *If* $S_\infty(F) = \{\wp_1, \wp_2\}$*, with* $\deg \wp_1 = \deg \wp_2$*, then* $r_{\mathcal{O}_F}$ *is just the order of the class of the zero-degree divisor* $(\wp_1 - \wp_2)$ *in the jacobian of* F/k *and if moreover* $g_F > 0$ *and* $\deg \wp_1 = \deg \wp_2 = 1$*, then* $r_{\mathcal{O}_F} > 1$.
- *Recall that for any function field* $F/\mathbb{F}_q$ *of zero genus, we have* $h_F = h_{\mathcal{O}_F} = 1$.

2.2 Behaviour of places and zeta functions in a quartic extension

Let L/k be an imaginary bicyclic biquadratic extension. Since L/k is Galois of Galois group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, there is by Galois theory three distinct subfield extensions K_i/k.
For a place p of k, we denote by g_p the number of places $\wp$ of L lying over p, f_p their relative degree and e_p their ramification index. Only five situations may occur. Indeed, we have $e_p f_p g_p = 4$ and thus only 6 possibilities for (e_p, f_p, g_p). The situation $(e_p, f_p, g_p) = (1, 4, 1)$ is impossible, since, for such a place, the quotient of the decomposition group by the inertia group is isomorphic to the Galois group of L/k which is bicyclic and also isomorphic to the Galois group of the residue class extension $L_\wp/k_p$ which is cyclic. Thus we only have to consider the following cases:

1. $p\mathcal{O}_L = \wp_1\wp_2\wp_3\wp_4$,
2. $p\mathcal{O}_L = \wp^4$,
3. $p\mathcal{O}_L = \wp^2$,
4. $p\mathcal{O}_L = \wp_1^2\wp_2^2$,
5. $p\mathcal{O}_L = \wp_1\wp_2$.

We see that in the first case p is totally decomposed in all the K_i and in the second one p is totally ramified in all the K_i. Using the properties of the decomposition field and the inertia field, we can show that, in case three p is inert in one K_i and ramified in the two others, in case four p is decomposed in one K_i and ramified in the two others, and finally in case five p is decomposed in one K_i and inert in the others.
Thus, if we focus on the infinite place of k, we have the following different situations:

- **case 1** - all K_i/k, $i = 1, 2, 3$, are real,
- **case 2** - all K_i/k, $i = 1, 2, 3$, are ramified,
- **case 3** - two K_i/k are ramified, the third one is inert,
- **case 4** - two K_i/k are ramified, the third one is real,
- **case 5** - two K_i/k are inert, the third one is real.

Case 1 cannot occur since we assumed that L/k is imaginary.

Remark 2.2 *If the characteristic of k is odd, case 2 cannot occur, since if K_1/k and K_2/k are ramified, then, for $i = 1, 2$, $K_i = k(y_i)$, with $y_i^2 = f_i(x)$ where $f_i \in k[x]$ is a monic square-free polynomial of odd degree and we see that K_3/k is real since $K_3 = k(y_3)$ with $y_3^2 = f_3(x)$, where $f_3 = (f_1\, f_2)/gcd(f_1,\, f_2)^2$ is a monic square-free polynomial of even degree.*

For an extension F of k, let $\zeta_{\mathcal{O}_F}$ be the zeta function of $\mathcal{O}_F$, defined by

$$\zeta_{\mathcal{O}_F}(s) = \sum_I \frac{1}{N(I)^s} = \prod_{\wp} \Big(1 - \frac{1}{N(\wp)^s}\Big)^{-1},$$

where $s \in \mathbb{C}$, the sum ranges over the nonzero ideals I of $\mathcal{O}_F$ and $N(I)$ stands for the norm of the ideal I, that is by definition the number of elements of the residue class ring $\mathcal{O}_F/I$, and finally the product ranges over the nonzero prime ideals $\wp$ of $\mathcal{O}_F$.
The zeta function of the function field $F/\mathbb{F}_q$ is such that

$$\zeta_F(s) = \zeta_{\mathcal{O}_F}(s) \prod_{\wp \in S_\infty(F)} \Big(1 - \frac{1}{N(\wp)^s}\Big)^{-1}. \tag{2}$$

Then we have:

Theorem 2.3 *Let L be an imaginary bicyclic biquadratic extension of k and let K_1, K_2 and K_3 be the three intermediate fields of L/k. Then we have:*

$$\zeta_{\mathcal{O}_L}(s)/\zeta_{\mathcal{O}_k}(s) = \prod_{i=1}^{3} \Big(\zeta_{\mathcal{O}_{K_i}}(s)/\zeta_{\mathcal{O}_k}(s)\Big) .$$

Proof: If we denote by Spec $(\mathcal{O}_F)$ the set of prime ideals of $\mathcal{O}_F$, we have for all $i \in \{1, 2, 3\}$:

$$\zeta_{\mathcal{O}_{K_i}}(s) = \prod_{p \in \text{Spec } (\mathcal{O}_k)-\{0\}} \prod_{\wp | p} \Big(1 - \frac{1}{N(\wp)^s}\Big)^{-1} .$$

But, as the prime ideal p of $\mathcal{O}_k$ is inert, ramified or splits in K_i/k, the norm $N(\wp)$ of $\wp|p$ is equal to $N(p)^2$, $N(p)$ or $N(p)$. Thus we obtain:

$$\zeta_{\mathcal{O}_{K_i}}(s) = \zeta_{\mathcal{O}_k}(s) L_{\mathcal{O}_k}(s, \chi) ,$$

where

$$L_{\mathcal{O}_k}(s, \chi) = \prod_{p \in \text{Spec } (\mathcal{O}_k)-\{0\}} \Big(1 - \frac{\chi(p)}{N(p)^s}\Big)^{-1} ,$$

with $\chi(p) = -1$, 0, or 1, according whether p is inert, ramified or splits in K_i/k. Then we have to consider the behaviour of a place p of k in the different extensions and remark that the norm of a place $\wp$ over p in L equals $N(p)$ or $N(p)^2$, according whether $\wp$ is of degree one or two. A simple calculation gives us the result. □

Corollary 2.4

$$\big(\zeta_L/\zeta_k\big)(s) = \prod_{i=1}^{3} \big(\zeta_{K_i}/\zeta_k\big)(s)$$

Proof: According to (2), we have to look at the behaviour of the infinite places of these fields. □

2.3 Formula for class numbers

Using the previous results, we have the following proposition.

Corollary 2.5 *If the imaginary bicyclic biquadratic extension L/k has a real quadratic subfield, say $K = K_1$ (cases 4 and 5), we have:*

$$\frac{R_{\mathcal{O}_L}}{R_{\mathcal{O}_K}} h_{\mathcal{O}_L} = h_{\mathcal{O}_K} h_{\mathcal{O}_{K_2}} h_{\mathcal{O}_{K_3}} .$$

Else (cases 2 and 3), we have:

$$h_{\mathcal{O}_L} = h_{\mathcal{O}_{K_1}} h_{\mathcal{O}_{K_2}} h_{\mathcal{O}_{K_3}}.$$

Proof: For any function field $L/\mathbb{F}_q$, a residue calculus gives (see [8]):

$$\zeta_{\mathcal{O}_L}(s) = \frac{-h_{\mathcal{O}_L} R_{\mathcal{O}_L}}{(q-1)} (\ln q)^{s_\infty(L)-1} s^{s_\infty(L)-1} + O(s^{s_\infty(L)}).$$

Then, if we set $\Lambda_{\mathcal{O}_L}(s) = \zeta_{\mathcal{O}_L}(s)/s^{s_\infty(L)-1}$, we have

$$\Lambda_{\mathcal{O}_L}(0) = \frac{-h_{\mathcal{O}_L} R_{\mathcal{O}_L}}{(q-1)} (\ln q)^{s_\infty(L)-1}$$

and since $s_\infty(L) - s_\infty(k) = s_\infty(K_1) + s_\infty(K_2) + s_\infty(K_3) - 3s_\infty(k)$ we obtain

$$\big(\Lambda_{\mathcal{O}_L}/\Lambda_{\mathcal{O}_k}\big)(0) = \prod_{i=1}^{3} \big(\Lambda_{\mathcal{O}_{K_i}}/\Lambda_{\mathcal{O}_k}\big)(0),$$

which gives us:

$$R_{\mathcal{O}_L} h_{\mathcal{O}_L} = \prod_{i=1}^{3} R_{\mathcal{O}_{K_i}} h_{\mathcal{O}_{K_i}}.$$

One gets the result observing that, in any function field F/k, if there is only one place in F above the infinite place of k, then the regulator $R_{\mathcal{O}_F}$ is equal to one. □

Let L/k be an imaginary bicyclic biquadratic extension which has a real quadratic subfield K. By Dirichlet's theorem the unit group of L and K are of rank 1. We set $Q_{L/K} = [\mathcal{O}_L^* : \mathcal{O}_K^*]$ for the index of the units.

Lemma 2.6 *Let L be an imaginary bicyclic biquadratic extension of k which has a real quadratic subfield K. Then we have:*

- $Q_{L/K} = 1$ or 2.
- $\frac{R_{\mathcal{O}_L}}{R_{\mathcal{O}_K}} = \frac{2}{Q_{L/K}}$.

Proof: Let ε_K and ε_L be the fundamental units of K and L respectively. We have $\varepsilon_K \in \mathcal{O}_L^*$ thus $\varepsilon_K = \varepsilon_L^{Q_{L/K}}$. If we denote by $N_{L/K}$ the norm of L/K, we have $\varepsilon_K^2 = N_{L/K}(\varepsilon_K) = N_{L/K}(\varepsilon_L^{Q_{L/K}}) = N_{L/K}(\varepsilon_L)^{Q_{L/K}} = \varepsilon_K^{mQ_{L/K}}$, where m is an integer, thus $mQ_{L/K} = 2$ and then $Q_{L/K} = 1$ or 2. Note that this a particular case of the situation considered in [1] from which we can also deduce the second statement. □

Proposition 2.7 *Let L/k be an imaginary bicyclic biquadratic extension and let K_i, $i = 1, 2, 3$, be the three intermediate fields. We have*

$$h_{\mathcal{O}_L} = \frac{Q}{2} h_{\mathcal{O}_{K_1}} h_{\mathcal{O}_{K_2}} h_{\mathcal{O}_{K_3}}, \tag{3}$$

where $Q = 2$ if none of the K_i/k is real and $Q = Q_{L/K} = 1$ or 2 if one K_i, say K, is real.

This is a trivial consequence of Corollary 2.5 and Lemma 2.6. Since $h_{\mathcal{O}_K}$ is even if K/k is an inert quadratic extension, we see that $h_{\mathcal{O}_L}$ is even in cases 3 and 4. Thus if we want $h_{\mathcal{O}_L} = 1$, we will have to consider only cases 2 and 5 of Section 2.2. Moreover, using Proposition 2.7, we have the following result.

Corollary 2.8 *Let L/k be an imaginary bicyclic biquadratic extension and let K_i, $i = 1, 2, 3$, be the three intermediate fields.*

1. *If all K_i/k are ramified* (case 2) *then*

$$h_{\mathcal{O}_L} = 1 \iff (h_{\mathcal{O}_{K_i}})_{1 \le i \le 3} = (1, 1, 1)\,.$$

2. *If two K_i/k are ramified and the third one is real* (case 5) *then*

$$h_{\mathcal{O}_L} = 1 \iff \begin{cases} (h_{\mathcal{O}_{K_i}})_{1 \le i \le 3} = (1, 1, 2) \text{ and } Q = 1\,, \\ \text{or} \\ (h_{\mathcal{O}_{K_i}})_{1 \le i \le 3} = (1, 1, 1) \text{ and } Q = 2\,. \end{cases}$$

3 Quadratic extensions in even characteristic

3.1 Equation of Artin-Schreier extensions

Let us recall the Hasse normalized equation for an Artin-Schreier extension in even characteristic.

Proposition 3.1 - (see [3] or [4]) - *Let $k = \mathbb{F}_q(x)$, with q a power of 2, and let K/k be an Artin-Schreier extension. Then $K = k(y)$, where y verifies the following equation*

$$y^2 + y = f(x) = \lambda \frac{N(x)}{\prod_{i=1}^{r} P_i(x)^{n_i}}\,, \tag{4}$$

with

- $\lambda \in \mathbb{F}_q^*$,
- *N and P_i are monic polynomials of $\mathbb{F}_q[x]$ and $N(x)$ is prime to $\prod_{i=1}^r P_i(x)$,*
- *n_i is odd for all i, $1 \leq i \leq r$.*

We set

$$s = \sum_{i=1}^{r} \deg(P_i),\ t = \sum_{i=1}^{r} n_i \deg(P_i),\ n = \deg(N)\,.$$

For a fixed x, there exists $y \in K$ such that $K = k(y)$, where y satisfies (4) *and furthermore,*

1. *in case $g_K \geq 1$,*

$$\begin{array}{ll} \text{if } K/k \text{ is ramified,} & s+n \text{ is odd, } t < n\ ,\ g_K = \frac{s+n-1}{2}\,, \\ \text{if } K/k \text{ is real,} & n < t\ ,\ g_K = \frac{s+t}{2} - 1\,, \\ \text{if } K/k \text{ is inert,} & n = t\ ,\ \lambda \neq c^2 + c\,, \forall c \in \mathbb{F}_q\ ,\ g_K = \frac{s+t}{2} - 1\,. \end{array}$$

2. *in case $g_K = 0$, (with $a \in \mathbb{F}_q$)*

$$\begin{array}{ll} \text{if } K/k \text{ is ramified,} & y^2 + y = x + a, \\ \text{if } K/k \text{ is real,} & y^2 + y = \frac{a}{x}, \\ \text{if } K/k \text{ is inert,} & y^2 + y = \lambda\,\frac{x+a}{x},\ a \neq 0 \text{ and } \lambda \neq c^2 + c\,, \forall c \in \mathbb{F}_q\,. \end{array}$$

If an Artin-Schreier extension K/k is such that $K = k(y)$, with y satifying equation (4), we will set $K = K_f$.

Remark 3.2 *The number r which appears in* (4) is the number of finite places of k which are ramified in K.

fixed.

3.2 Parity of the ideal class number

Let us quote a result concerning the parity of the ideal class number of a quadratic extension K/k. In [14], the quadratic extensions K/k with an odd ideal class number are characterized in the odd characteristic case. For even characteristic one has the following result.

Proposition 3.3 *Assume that the characteristic of k equals* 2*. Let K/k be a quadratic extension, $K = k(y)$, where y satisfies* (4)*. Then the ideal class number $h_{\mathcal{O}_K}$ is odd if and only if the number r of finite places of k which are ramified in K is such that*

- $r = 0$, *or*
- $r = 1$ *and* K/k *is real.*

Recall that if K/k is inert, then, according to (1), $h_{\mathcal{O}_K}$ is even.
Sketch of proof: (see [9]) We have $K = k(y)$, with

$$y^2 + y = f(x) = \lambda \frac{N(x)}{\prod_{i=1}^{r} P_i(x)^{n_i}} .$$

Let us show that the 2-rank, R, of the ideal class group of K/k is equal to

$$R = \begin{cases} r & \text{if } K/k \text{ is imaginary} \\ r-1 & \text{if } K/k \text{ is real} \end{cases} .$$

We denote by H the Hilbert class field of (K, S_∞) and by M/K the maximal 2-primary subextension of H/K. One can define M explicitly. In fact, consider the partial decomposition of $f(x)$:

$$f(x) = S_0(x) + \sum_{i=1}^{r} \frac{N_i(x)}{P_i(x)^{n_i}} ,$$

where $S_0(x) \in \mathbb{F}_q[x]$ ($S_0(x) = 0$ if K/k is real) and $\deg N_i(x) < n_i \deg P_i(x)$. Set

$$S_i(x) = \frac{N_i(x)}{P_i(x)^{n_i}} , i = 1, \ldots, r .$$

It can be shown that $M = K(y_0, \ldots, y_r)$ (resp. $M = K(y_1, \ldots, y_r)$) if K/k is imaginary (resp. real), where y_i satisfies the equation $y_i^2 + y_i = S_i(x)$. Since $[M : K] = 2^R$, we obtain the result. □

3.3 Quadratic extensions with a small ideal class number

We will also use the following result, which, in even characteristic, gives all imaginary quadratic extensions K/k such that $h_{\mathcal{O}_K} = 1$ or 2. The case $h_{\mathcal{O}_K} = 1$ is due to [7] and [6] and the case $h_{\mathcal{O}_K} = 2$, to [5] or [4].

Proposition 3.4 *Assume that the characteristic of k equals 2 and let K/k be an imaginary quadratic extension. Let $K = k(y)$, then one has (up to an isomorphism leaving the infinite place of k fixed). We denote by α a generator of $\mathbb{F}_4^*$.*

1. *If $g_K \geq 1$, then $h_{\mathcal{O}_K} = 1$ only if*

- $k = \mathbb{F}_2(x)$ *with* $y^2 + y = x^3 + x + 1$ *or* $y^2 + y = x^5 + x^3 + 1$.
- $k = \mathbb{F}_4(x)$ *with* $y^2 + y = x^3 + \alpha$.

2. *If* $g_K \geq 1$ *and* K/k *is ramified, then* $h_{\mathcal{O}_K} = 2$ *only if*

   - $k = \mathbb{F}_2(x)$, *where* $y^2 + y = f(x)$ *with*

$$\begin{array}{ll} g_K = 1 \text{ and} & f(x) = x + 1 + \frac{1}{x} \\ g_K = 2 \text{ and} & f(x) = x + 1 + \frac{x}{x^2+x+1} \\ & f(x) = x^3 + 1 + \frac{1}{x} \\ & f(x) = x + 1 + \frac{1}{x^3} (*) \\ g_K = 3 \text{ and} & f(x) = x^3 + x + \frac{1}{x^2+x+1} \\ & f(x) = x + 1 + \frac{x}{x^3+x+1} \,. \end{array}$$

   $(*)$ *this case is obtained applying transformation* $x \mapsto \frac{1}{x}$ *to the preceeding one.*

   - $k = \mathbb{F}_4(x)$, *where* $y^2 + y = f(x)$ *with*

$$g_K = 2 \text{ and } y^2 + y = x + \frac{\alpha}{x} \,.$$

For a bicyclic biquadratic extension L/k, one can relate an intermediate field with the two others.

3.4 Compositum of Artin-Schreier extensions

Lemma 3.5 *Assume that the characteristic of* k *equals* 2. *Let* L/k *be a bicyclic biquadratic extension. Then* L *is the compositum of* $K_1 = K_{f_1}$ *and* $K_2 = K_{f_2}$, *with* f_1, f_2 $\mathbb{F}_2$*-linearly independent and the third intermediate field is* $K_3 = K_{f_3}$, *with* $f_3 = f_1 + f_2$. *The genus of* L *is*

$$g_L = g_1 + g_2 + g_3 \,. \tag{5}$$

Proof: It is consequence of the results quoted in [11]. □

Note that, if $K_i = K(y_i)$, with $y_i^2 + y_i = f_i(x)$ for $i = 1, 2$, then $(y_1 + y_2)$ is a primitive element of K_3, that is $K_3 = k(y_1 + y_2)$. One can also show that $t = y_1 y_2$ is a primitive element of $L = K_1 K_2$.

4 Principal imaginary bicyclic biquadratic function fields in even characteristic

The solutions to the ideal class number one problem for imaginary bicyclic biquadratic function fields in even characteristic are listed in the following theorem.

Theorem 4.1 *Let L be an imaginary bicyclic biquadratic extension of $k = \mathbb{F}_{2^e}(x)$ and let K_i, $i = 1, 2, 3$, be the three distinct intermediate fields. The extensions L/k with ideal class number equal to one are exactly the following (up to isomorphism leaving the infinite place of k fixed) : $L = k(y, z)$, where*

1. *$k = \mathbb{F}_{2^e}(x)$, $y^2 + y = f(x)$, $z^2 + z = g(x)$, with degree one polynomials $f, g \in \mathbb{F}_{2^e}[x]$ that are independent over $\mathbb{F}_{2^e}$ and then $g_L = 0$.*
2. *$k = \mathbb{F}_4(x)$, $y^2 + y = x^3 + \alpha$, $z^2 + z = ax + b$, $(a, b) \in \mathbb{F}_4^* \times \mathbb{F}_4$, and then $g_L = 2$.*
3. *$k = \mathbb{F}_4(x)$, $y^2 + y = x + \frac{\alpha}{x}$ and $z^2 + z = x$ and then $g_L = 1$.*
4. *$k = \mathbb{F}_2(x)$, $y^2 + y = x + 1 + \frac{1}{x}$ and $z^2 + z = x + 1$ and then $g_L = 1$.*
5. *$k = \mathbb{F}_2(x)$, $y^2 + y = x + 1 + \frac{x}{x^2+x+1}$ and $z^2 + z = x + 1$ and then $g_L = 3$.*
6. *$k = \mathbb{F}_2(x)$, $y^2 + y = x + 1 + \frac{1}{x^3}$, $z^2 + z = x + 1$ and then $g_L = 3$.*
7. *$k = \mathbb{F}_2(x)$, $y^2 + y = x + 1 + \frac{x}{x^3+x+1}$ and $z^2 + z = x + 1$ and then $g_L = 5$.*

As previously, we denote by α a generator of $\mathbb{F}_4^*$.

Proof: The genus of a solution L/k will be easily computed using (5). For each subfield $K_i = k(y_i)$ of L, we will consider the equation $y_i^2 + y_i = f_i(x)$, where $f_i(x) \in k(x)$. According to Corollary 2.3, we only have to consider cases 2 and 5 of Section 2.2.

1. (case 2) All K_i/k are ramified and $(h_{\mathcal{O}_{K_i}})_{1 \le i \le 3} = (1, 1, 1)$.
   (a) If two K_i/k are ramified and with genera equal to 0 then so is the third one (see Proposition 3.1). We can take three $K_i = K_{f_i}$ such that the corresponding f_i's are linear polynomials, independent over $\mathbb{F}_q$. This gives solution 1 of the Theorem.

(b) If $q = 4$ and $g_K > 0$, then, according to Proposition 3.4, there is a unique K such that $h_{\mathcal{O}_K} = 1$. Let $K_1 = k(y)$, with $y^2+y = x^3+\alpha$ and $g_1 = 1$, and let K_2 be k-isomorphic to K_1 and also ramified. Then $K_2 = k(z)$ with $z^2+z = x^3+ax+b$, where $a, b \in \mathbb{F}_4$. Thus, we obtain $K_3 = k(u)$, $u^2+u = ax+(b+\alpha)$ with $g_3 = 0$ and this gives solution 2 of the Theorem.

(c) If $q = 2$ and $g_K > 0$, then according to Proposition 3.4, there are exactly two K such that $h_{\mathcal{O}_K} = 1$, which are $k(u)$, with $u^2+u = x^3+x+1$, $g = 1$, and $k(v)$, with $v^2+v = x^5+x^3+1$, $g = 2$. They both define ramified extensions K/k. Let us take $K_1 = k(u)$ or a ramified extension K_1/k k-isomorphic to $k(u)/k$ and $K_2 = k(v)$ or a ramified extension K_2/k k-isomorphic to $k(v)/k$. Then K_3 has genus 2 and, since it must have an ideal class number equal to 1, it has to be k-isomorphic to $k(v)$. There are no solutions in this case.
It can easily be shown that if one takes $K_1 = k(u)$ and K_2 (ramified) k-isomorphic to $k(u)$, there are no solutions too. Same conclusion if one takes $f(v)$ instead of $k(u)$.

2. (case 5) Two K_i/k are ramified, the third one is real and $(h_{\mathcal{O}_{K_i}})_{1\le i\le 3} = (1,1,2)$ and $Q = 1$, or $(h_{\mathcal{O}_{K_i}})_{1\le i\le 3} = (1,1,1)$ and $Q = 2$.

(a) If the two ramified fields have genus 0, there are no solutions, since the third field will also be ramified (see Proposition 3.1).

(b) Now we take one ramified field, say K_1, with genus 0 and the other ramified field, say K_2, such that $g_2 > 0$ and $h_{\mathcal{O}_{K_2}} = 1$ or 2. Then, according to Proposition 3.4, we must have $q = 2$ or 4.

i. If $h_{\mathcal{O}_{K_2}} = 1$, it can easily be shown as previously that the third field will be ramified too, so this case cannot occur.

ii. If $h_{\mathcal{O}_{K_2}} = 2$ and $q = 4$, the unique possibility (up to isomorphism) is $K_2 = k(y)$, where $f_2(x) = x + \frac{\alpha}{x}$. Then $K_1 = k(z)$, where $f_1(x) = ax+b$, and $K_2 = k(y)$ give $K_3 = K(u)$, where $u^2+u = (a+1)x+b+\frac{\alpha}{x}$. Since K_3/k has to be real, we must have $a = 1$ and $b = 0$. Then $g_3 = 0$ (so $h_{\mathcal{O}_{K_3}} = 1$) and this will give a solution if $Q = 1$. The genus of L is $g_L = 1$ and the two places of $S_\infty(L)$ are of degree one because there is some ramification in K_1 and K_2. So, since $g_L > 0$, the

regulator of L is strictly greater than 1 and, since $g_3 = 0$, the regulator of K_3 equals 1, so $Q = 1$. This is solution 3 of the Theorem.

iii. If $h_{\mathcal{O}_{K_2}} = 2$ and $q = 2$, we consider the six possibilities for $K_2 = K_{f_2}$ given in Proposition 3.4. In the following, we set $K_1 = k(z)$, $K_2 = k(y)$ and $K_3 = k(u)$, with $u = y + z$.

- Since the third subfield K_3 of L has to be real, we must have $K_3 = K_{f_3}$, with $\deg(f_3) < 0$ and, since f_1 is a linear polynomial, we will have no solutions if the polynomial part of f_2 has a degree greater than 1.
  Thus $f_2(x) = x^3 + 1 + \frac{1}{x}$ or $f_2(x) = x^3 + x^2 + \frac{1}{x^2+x+1}$ give no solution.
- If $f_2(x) = x + 1 + \frac{1}{x}$, then $f_1(x) = x + 1$ is the only possibility to obtain a real third subfield. It gives $K_3 = K(u)$, where $u^2 + u = \frac{1}{x}$, which is a real extension of k such that $g_3 = 0$. With the same argument as above, we show that this is a solution (solution 4 of the Theorem) and $g_L = 1$.
- If $f_2(x) = x + 1 + \frac{x}{x^2+x+1}$, then $f_1(x) = x + 1$ is the only possibility to obtain a real third subfield. It gives $f_3(x) = \frac{x}{x^2+x+1}$, $g_3 = 1$. We can show that the divisor class number of K_3 is $h_3 = 4$. Since $(x^2 + x + 1)$ is irreducible over $\mathbb{F}_2$, $h_{\mathcal{O}_{K_3}}$ is odd because of Proposition 3.3. Then $4 = h_3 = h_{\mathcal{O}_{K_3}} r_{\mathcal{O}_{K_3}}$, implies that $h_{\mathcal{O}_{K_3}} = 1$ and $r_{\mathcal{O}_{K_3}} = 4$, since $r_{\mathcal{O}_{K_3}} > 1$ (see remark 2.1). This will give a solution only if $Q = 2\, r_{\mathcal{O}_{K_3}}/r_{\mathcal{O}_L} = 1$. Let us compute $r_{\mathcal{O}_L}$. We consider L as a real quadratic extension of $K_1 = k(z)$: indeed, we have $L = K_1(u)$ with
  $$u^2 + u = \frac{z^2 + z + 1}{z^4 + z + 1}\,, \tag{6}$$
  and it is easy to show that $g_L = 3$, $h_L = 8$. Since K_1/k is ramified, we have $S_\infty(K_1) = \{P\}$, with $\deg P = 1$. The integral closure of $\mathbb{F}_q[x]$ in L is clearly equal to the integral closure of $k[z]$ in L. Applying Proposition 3.3 to the real quadratic extension L/K_1 defined by (6), we obtain that $h_{\mathcal{O}_L}$ is odd. Then $h_L = h_{\mathcal{O}_L} r_{\mathcal{O}_L}$ implies that $h_{\mathcal{O}_L} = 1$ and $r_{\mathcal{O}_L} = 8$, so that $Q = 2\, r_{\mathcal{O}_{K_3}}/r_{\mathcal{O}_L} = 1$. This gives solution 5 of the Theorem.

- If $f_2(x) = x+1+\frac{1}{x^3}$, $f_1(x) = x+1$ is the only possibility to obtain a real third subfield. It gives $f_3(x) = \frac{1}{x^3}$, $g_3 = 1$ and $h_3 = 3$. Thus $h_{\mathcal{O}_{K_3}} = 1$ and $r_{\mathcal{O}_{K_3}} = 3$. As previously, L is a real quadratic extension of $K_1 = k(z)$ and $L = K_1(u)$ with
$$u^2 + u = \frac{1}{(z^2+z+1)^3},$$
$g_L = 3$, $h_L = 6$. We conclude that $Q = 1$ as before. This gives solution 6 of the Theorem.
- If $f_2(x) = x+1+\frac{x}{x^3+x+1}$, $f_1(x) = x+1$ is the only possibility to obtain a real third subfield. It gives $f_3(x) = \frac{x}{x^3+x+1}$ and we can show that $g_3 = 2$ and $h_3 = 11$. Since $g_3 > 0$, we have $r_{\mathcal{O}_{K_3}} > 1$ (see Remark 2.1). Thus $h_3 = h_{\mathcal{O}_{K_3}} r_{\mathcal{O}_{K_3}}$ implies $h_{\mathcal{O}_{K_3}} = 1$ and $r_{\mathcal{O}_{K_3}} = 11$. Then
$$L = K_1(u),, \text{ with } u^2 + u = \frac{z^2+z+1}{z^6+z^5+z^3+z^2+1},$$
$g_L = 5$, $h_L = 22$. Since $(z^6+z^5+z^3+z^2+1)$ is irreducible, $h_{\mathcal{O}_L}$ is odd. As previously, we have $r_{\mathcal{O}_L}/r_{\mathcal{O}_{K_3}} = 2/Q = 2$ or 1. Then, since $h_L = 22 = h_{\mathcal{O}_L} r_{\mathcal{O}_L}$, we have $r_{\mathcal{O}_L} = 22$, so that $Q = 1$. This gives solution 7 of the Theorem.

iv. If the two ramified fields have genus > 0 and an ideal class number equal to 1, the third one will not be real: just look at the possibilities given in Proposition 3.4.
Assume now that $h_{\mathcal{O}_{K_1}} = 1$, $h_{\mathcal{O}_{K_2}} = 2$ and $g_i > 0$ for $i = 1, 2$.
- If $q = 4$, according to Proposition 3.4 we must have $f_1(x) = x^3 + \alpha$ (up to isomorphism) and $f_2 = x + \frac{a}{x}$ (up to isomorphism). One cannot obtain a third real subfield.
- If $q = 2$, it is easy to see that there are no solutions for similar reasons than previously.

□

5 Conclusion

If the characteristic of k is even, we have given all imaginary bicyclic biquadratic extensions L/k with ideal class number one. As for odd characteristic (see [12]), all such extensions have at least one intermediate field with genus 0.

References

[1] Aubry, Y. *Class number in totally imaginary extensions of totally real function fields*, Finite fields and applications, London Math. Soc., Lect. Notes **233**, Cambridge University Press, (1996), 23-29.

[2] Brown, E. and Parry, C., *The imaginary bicyclic biquadratic fields with class number* 1, J. reine angew. math. **266** (1974), 118-120.

[3] Hasse, H. *Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper*, J. Reine Angew. Math. **172** (1934), 37-54.

[4] Le Brigand, D. *Quadratic algebraic function fields with ideal class number two*, "Arithmetic, Geometry and Coding Theory", editors R. Pellikaan, M. Perret and S. Vlăduţ, W. de Gruyter (1996), 105-126.

[5] J. R. C. Leitzel, M. L. Madan and C. S. Queen, *Algebraic function fields with small class number*, J. Number Theory **7** (1975), 11-27.

[6] Madan, M. L. and C. S. Queen, *Algebraic function fields of class number one*, Acta Arithmetica 20 (1972), 423-432.

[7] R. E. MacRae, *On Unique Factorization in Certain Rings of Algebraic Functions*, J. Algebra 17 (1971), 243-261.

[8] Rosen, M., *The Hilbert class field in function fields*, Expo. Math. **5** (1987), 365-378.

[9] Sémirat, S., *Genus theory for quadratic function fields and applications*, preprint Université Paris VI (1998).

[10] F. K. Schmidt, *Analytische Zahlentheorie in Körpern der Charakteristik p*, Math. Zeitschr. **33** (1931), 1-32.

[11] van der Geer, G. and van der Vlugt, M., *Fibre product of Artin-Schreier curves and generalized Hamming weights of codes*, J. Comb. Th. A **70** (1995), 337-348.

[12] Zhang, Xian-Ke, *Determination of algebraic function fields of type* $(2, 2, .., 2)$ *with class number one*, Scientia Sinica A **31**, n. 8 (1988), 908-915.

[13] Zhang, Xian-Ke, *Algebraic function fields of type* $(2, 2, \cdots, 2)$, Scientia Sinica A **31**, n. 5 (1988), 521-530.

[14] Zhang, Xian-Ke, *Ambiguous classes and 2-rank of class group of quadratic function field*, J. China Univ. Sci. Technol. **17**, n. 4 (1987), 425-431.

Yves Aubry
Département de Mathématiques
Université de Caen
Campus II, B.P. 5186
14032 Caen, France
aubry@math.unicaen.fr

Dominique Le Brigand
Institut de Mathématiques de Jussieu
Université Paris VI
Case 82, 75252 Paris cedex 05
France
Dominique.Lebrigand@math.jussieu.fr