Class number in non Galois quartic and non abelian Galois octic function fields over finite fields

Yves Aubry

G. R. I. M.
Université du Sud Toulon-Var
83 957 La Garde Cedex
France
yaubry@univ-tln.fr

Abstract

We consider a totally imaginary extension of a real extension of a rational function field over a finite field of odd characteristic. We prove that the relative ideal class number one problem for such non Galois quartic fields is equivalent to the one for non abelian Galois octic imaginary functions fields. Then, we develop some results on characters which give a method to evaluate the ideal class number of such quartic function fields.

1 Introduction

Let L be a totally imaginary extension of a function field K which is itself a real extension of a rational function field $k = \mathbf{F}_q(x)$. This means that the infinite place ∞ of k totally splits in the extension K/k and that this places have only one place above each of them in the extension L/K. The determination of all such imaginary fields L with L/k Galois and cyclic and with ideal class number one has been done by S. Sémirat in [11]. The quartic bicyclic Galois case has been solved by X. Zhang in [13] in odd characteristic and by the author and Dominique Le Brigand in [3] in even characteristic.

We are interested here in the determination of all such non Galois quartic fields L with ideal class number equal to one (which will be called the ideal class number one problem), a problem which has been solved by K. Uchida in [12] and by S. Louboutin in [8] in the number field case.

[0]2000 Mathematics Subject Classification. 11G20, 11R29, 11M06, 14G10, 14G15.
Key words and phrases. Function fields, class number.
[0]The author is very grateful to the "Institut de Mathématiques de Luminy" - C.N.R.S. - Marseille - France for its hospitality during this work.

In section 2, we recall some definitions and some general results without any assumption on the degrees of L/K and K/k. We give also an ambiguous classes formula for cyclic extensions.

In section 3, we suppose that L/K is quadratic. We give a result on the dyadic valuation of the relative ideal class number of L. Then, we give a formula for it in terms of a character χ, which is a particular case of the Galois situation studied in [10].

Section 4 is devoted to the quartic situation : L/K and K/k are supposed to be quadratic. Firstly, we show, as K. Uchida and S. Louboutin for number fields (see respectively [12] and [8]), that the relative ideal class number one problem for such non Galois quartic fields is equivalent to the one for non abelian Galois octic imaginary fields. Secondly, if we suppose furthermore that K has ideal class number one, we give a method to evaluate the character χ. Thirdly, we investigate the case where L has ideal class number one.

2 Preliminaries

2.1 The general setting

Let K be an algebraic function field in one variable over a finite constant field $\mathbf{F}_q$ with q elements (q odd) and let S_K be a non empty finite set of places (i.e. prime divisors) of K (called places at infinity of K, the places not in S_K will be called finite places). Let $\mathcal{O}_K$ be the ring of elements of K whose poles are in S_K. The ring $\mathcal{O}_K$ is a Dedekind domain and we denote by $\mathrm{Cl}(\mathcal{O}_K)$ its ideal class group and by $h_{\mathcal{O}_K}$ its order, called the ideal class number of K.

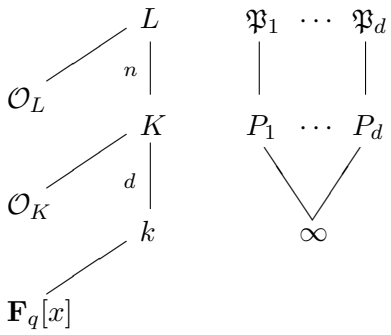
Let L be a finite extension of K contained in a separable closure of K with constant field $\mathbf{F}_q$ and let S_L be the set of places of L which extend those in S_K. By analogy with the number field case, the extension L/K is called real if the number of places in S_L is equal to $|S_L| = [L : K]\ |S_K|$, i.e. every place in S_K splits completely in L. Otherwise, the extension is called imaginary, and totally imaginary if $|S_L| = |S_K|$ (i.e. every place in S_K has only one place above it in L).

Let $\mathcal{O}_L$ be the ring of elements of L whose poles are in S_L. This ring is also the integral closure of $\mathcal{O}_K$ in L.

Let $k = \mathbf{F}_q(x)$ be a rational function field and $S_k = \{\infty\}$ be the place at infinity of k corresponding to $1/x$. Note that the "ring of integers" of k with respect to S_k is $\mathcal{O}_k = \mathbf{F}_q[x]$ the polynomial ring with coefficients in $\mathbf{F}_q$.

In this paper, all the functions fields will be supposed to have for exact constant field $\mathbf{F}_q$ with q odd and will be contained in a separable closure of $k = \mathbf{F}_q(x)$.

Now consider a real extension K/k of degree d and denote by $S_K = \{P_1, \cdots, P_d\}$ the set of places of K above the infinite place ∞ of k. Let us consider finally a totally imaginary extension L of K of degree n and denote by $S_L = \{\mathfrak{P}_1, \cdots, \mathfrak{P}_d\}$ the set of places of L above the P_i's. Our situation is the following one:



Note that this data is equivalent to the data consisting of a degree n totally imaginary extension L/K of functions fields and a non empty finite set $S_K = \{P_1, \cdots, P_d\}$ of places of K. Indeed, by Riemann-Roch theorem, we get the existence of a function $x \in K$ such that K is a degree d extension of $k(x)$ and such that the places of K over ∞ are exactely $P_1, \cdots, P_d$.

Note also that if the imaginary extension L/k is Galois, K can also be described as the fixed field of the inertia group of ∞, that is the maximal real subfield of L (the maximal subfield of L in which ∞ splits totally).

2.2 Units, regulators and class numbers

Let h_F denotes the divisor class number of a function field $F/\mathbf{F}_q$, that is the number of rational points over $\mathbf{F}_q$ of the Jacobian of the smooth projective algebraic curve associated to F. We have the following well-known relation due to F.K. Schmidt:

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

where $h_{\mathcal{O}_F}$ is the ideal class number of F with respect to the set of places S_F, $\delta_{\mathcal{O}_F}$ is the gcd of the degrees of the places of S_F and $r_{\mathcal{O}_F}$ is the index of the group of principal divisors supported on S_F in the group of zero degree divisors supported on S_F.

Let $R_{\mathcal{O}_F}$ be the regulator of $\mathcal{O}_F$ (which corresponds to the $R^q_{S_K}$-regulator defined in [10]). We have the following relation which can be considered here as a definition of $R_{\mathcal{O}_F}$:

$$r_{\mathcal{O}_F} = \frac{\delta_{\mathcal{O}_F} R_{\mathcal{O}_F}}{\prod_{P \in S_F} \deg P}.$$

The analogue of Dirichlet unit theorem states that the two unit groups $\mathcal{O}_L^*$ and $\mathcal{O}_K^*$ of L and K (modulo $\mathbf{F}_q^*$) are of rank $|S_K| - 1 = |S_L| - 1 = d - 1$. The point is that these two abelian groups have the same rank. We can estimate the index $Q_{L/K}$ of $\mathcal{O}_K^*$ in $\mathcal{O}_L^*$, analogue to the Hasse index in the number field case (see [2] for instance for a proof):

Proposition 1 *Let L/K be totally imaginary. Then, we have:*
(i) $Q_{L/K} := [\mathcal{O}_L^* : \mathcal{O}_K^*]$ divides $[L : K]^{\sharp S_K - 1}$.
(ii) $R_{\mathcal{O}_L}/R_{\mathcal{O}_K} = [L : K]^{\sharp S_K - 1}/Q_{L/K}$.

It is well-known that for any finite separable extension L/K of function fields, the divisor class number of K divides that of L (in fact, the polynomial $P_K(T)$ on the numerator of the zeta function of K divides $P_L(T)$, that of L, in $\mathbf{Z}[T]$, see for example [2] for a proof). For totally imaginary extensions L/K, the result holds also for ideal class numbers, as shown in the next proposition (see [9] for a proof with the additional assumption that some finite place of K is totally ramified in L or some infinite prime of K is inert in L).

Proposition 2 *If L/K is a totally imaginary extension, i.e. if every place in S_K has only one place above it in L, then the ideal class number $h_{\mathcal{O}_K}$ of K divides that $h_{\mathcal{O}_L}$ of L. Define the relative ideal class number by*

$$h^-_{\mathcal{O}_L} = h_{\mathcal{O}_L}/h_{\mathcal{O}_K}.$$

Proof. Let $K^{\mathcal{O}_K}$ denote the Hilbert class field of K with respect to $\mathcal{O}_K$ i.e. $K^{\mathcal{O}_K}$ is the maximal unramified abelian extension of K in which every place of S_K splits completely. The field $LK^{\mathcal{O}_K}$ is contained in the Hilbert class field $L^{\mathcal{O}_L}$ of L and thus $[LK^{\mathcal{O}_K} : L]$ divides $[L^{\mathcal{O}_L} : L]$ which is precisely the ideal class number of $\mathcal{O}_L$.
The isomorphism given by the restriction $\mathrm{Gal}(LK^{\mathcal{O}_K}/L) \longrightarrow \mathrm{Gal}(K^{\mathcal{O}_K}/L \cap K^{\mathcal{O}_K})$ defined by $\sigma \longmapsto \sigma|_{K^{\mathcal{O}_K}}$ gives us $[LK^{\mathcal{O}_K} : L] = [K^{\mathcal{O}_K} : L \cap K^{\mathcal{O}_K}]$.
Finally, we have $L \cap K^{\mathcal{O}_K} = K$ since first, the infinite places of K split in $K^{\mathcal{O}_K}$ and thus in $L \cap K^{\mathcal{O}_K}$, and secondly they are totally ramified or inert in L and thus in $L \cap K^{\mathcal{O}_K}$.
Thus, $[LK^{\mathcal{O}_K} : L] = [K^{\mathcal{O}_K} : K] = h_{\mathcal{O}_K}$ divides $[L^{\mathcal{O}_L} : L] = h_{\mathcal{O}_L}$. □

2.3 The zeta function

Let us introduce now the zeta function $\zeta_{\mathcal{O}_K}(s)$ of the Dedekind domain $\mathcal{O}_K$ by

$$\zeta_{\mathcal{O}_K}(s) = \sum_I \frac{1}{N(I)^s}$$

where $s \in \mathbf{C}$, the field of complex numbers, where the sum ranges over the nonzero ideals I of $\mathcal{O}_K$, and where $N(I)$ is the norm of the ideal I, that is, by definition the number of elements of the residue class ring $\mathcal{O}_K/I$.

Unique factorization of ideals in $\mathcal{O}_K$ implies the following Euler product representation:

$$\zeta_{\mathcal{O}_K}(s) = \prod_{P \in \mathrm{Spec}(\mathcal{O}_K) - \{0\}} \Big(1 - \frac{1}{N(P)^s}\Big)^{-1}$$

where $\mathrm{Spec}(\mathcal{O}_K)$ is the set of prime ideals of $\mathcal{O}_K$.

In a same way, we define the zeta function $\zeta_{\mathcal{O}_L}(s)$ of the Dedekind domain $\mathcal{O}_L$, and we have:

$$\zeta_{\mathcal{O}_L}(s) = \prod_{\mathfrak{P} \in \mathrm{Spec}(\mathcal{O}_L) - \{0\}} \Big(1 - \frac{1}{N(\mathfrak{P})^s}\Big)^{-1} = \prod_{P \in \mathrm{Spec}(\mathcal{O}_K) - \{0\}} \prod_{\mathfrak{P} | P} \Big(1 - \frac{1}{N(\mathfrak{P})^s}\Big)^{-1}.$$

2.4 Ambiguous classes in cyclic extensions

If we suppose that the extension L/K is cyclic, then we can prove the following ambigous classes formula in the same way as the one in lemma 4.1. p. 307 of [6] for number fields.

Lemma 3 *Let L/K be a cyclic extension of Galois group G, $C_L = Cl(\mathcal{O}_L)$ be the ideal class group of $\mathcal{O}_L$, C_L^G be the ambiguous ideal class group (the subgroup of C_L of elements fixed under G) and $e(L/K) = \prod_{P \notin S_K} e(P) \prod_{P \in S_K} e(P)f(P)$ where $e(P)$ and $f(P)$ stand for the ramification index $e(\mathfrak{P} \mid P)$ and residual degree $f(\mathfrak{P} \mid P)$ of any place $\mathfrak{P}$ in L over P. Then,*

$$|C_L^G| = \frac{h_{\mathcal{O}_K} e(L/K)}{[L:K][\mathcal{O}_K^* : N_{L/K} L^* \cap \mathcal{O}_K^*]}$$

where $N_{L/K}$ denotes the norm of L over K.

Proof. The proof given in [6] for number fields also holds in the function field case. The point is the use of corollary 2 p. 192 of [5] which gives that:

$$\frac{H^0(G, \mathcal{O}_L^*)}{H^1(G, \mathcal{O}_L^*)} = \frac{1}{[L:K]} \prod_{P \in S_K} | \, G_P \, |$$

where G_P denotes the decomposition group of P in the cyclic extension L/K, which has order $e(P)f(P)$. This gives the contribution of the places at infinity in the definition of $e(L/K)$. □

3 The relative ideal class number for L/K quadratic

In this section, we suppose that the imaginary extension L/K is quadratic.

3.1 On the dyadic valuation of the relative ideal class number

Proposition 4 *Let L/K be an imaginary quadratic extension and K/k be a real extension of the rational function field $k = \mathbf{F}_q(x)$. Let $t_{L/K}$ be the number of finite places (i.e. not in S_K) ramified in L/K. Then, $2^{t_{L/K}-1}$ divides $h_{\mathcal{O}_L}^-$.*

Proof. By the ambiguous class formula (lemma 3), we have:

$$|C_L^{\mathrm{Gal}(L/K)}| = \frac{h_{\mathcal{O}_K} 2^{t_{L/K} + \sharp S_K}}{2[\mathcal{O}_K^* : N_{L/K} L^* \cap \mathcal{O}_K^*]},$$

since $e(L/K) = \prod_{P \notin S_K} e(P) \prod_{P \in S_K} e(P)f(P) = 2^{t_{L/K}} \times 2^{\sharp S_K}$. Moreover, we clearly we have

$$\mathcal{O}_K^{*2} \subset N_{L/K} L^* \cap \mathcal{O}_K^*$$

since $[L:K]=2$. Thus, $[\mathcal{O}_K^* : N_{L/K}L^* \cap \mathcal{O}_K^*]$ divides $[\mathcal{O}_K^* : \mathcal{O}_K^{*2}]$. But

$$[\mathcal{O}_K^* : \mathcal{O}_K^{*2}] = [\mathbf{F}_q^* : \mathbf{F}_q^{*2}].2^{rk(\mathcal{O}_K^*)} = 2^{\sharp S_K}$$

since the rank $rk(\mathcal{O}_K^*)$ of the finitely generated group $\mathcal{O}_K^*$ is equal to $\sharp S_K - 1$ by Dirichlet's theorem and since the non zero squares in a finite field of odd characteristic have index 2 in its multiplicative group. Thus $2^{t_{L/K}-1}h_{\mathcal{O}_K}$ divides the order of $C_L^{\mathrm{Gal}(L/K)}$ which divides itself the ideal class number $h_{\mathcal{O}_L}$ by Lagrange theorem on group order, hence the result. □

3.2 Relative ideal class number and L-functions

The following investigation is actually a particular case of Galois extensions dealt with in [10] but we will write the things explicitly because of the simplicity of the purpose.

As the prime ideals P of $\mathcal{O}_K$ are inert, ramified or splits in L/K, we see immediately that the norm $N(\wp)$ of $\wp \mid P$ is equal to $N(P)^2$, $N(P)$ or $N(P)$. Thus, we obtain:

$$\zeta_{\mathcal{O}_L}(s) = \zeta_{\mathcal{O}_K}(s) L_{\mathcal{O}_K}(s,\chi) \tag{3}$$

where

$$L_{\mathcal{O}_K}(s,\chi) = \prod_{P \in \mathrm{Spec}(\mathcal{O}_K)-\{0\}} \Big(1 - \frac{\chi(P)}{N(P)^s}\Big)^{-1}$$

with $\chi(P) = -1,\ 0,\ 1$ according as P is inert, ramified or splits in L/K.

To obtain a relation between the zeta function $\zeta_{\mathcal{O}_K}(s)$ of $\mathcal{O}_K$ and its class number $h_{\mathcal{O}_K}$, one can define the zeta function of the function field K by:

$$\zeta_K(s) = \prod_P \Big(1 - \frac{1}{N(P)^s}\Big)^{-1}$$

where P ranges over all the places (i.e. prime divisors) of K. Then, we have

$$\zeta_K(s) = \zeta_{\mathcal{O}_K}(s) \prod_{P \in S_K} \Big(1 - \frac{1}{N(P)^s}\Big)^{-1} = Z_K(q^{-s}) = \frac{P_K(q^{-s})}{(1-q^{-s})(1-q^{1-s})} \tag{4}$$

A residue calculus gives us (see [9]):

$$\zeta_{\mathcal{O}_K}(s) = \frac{-h_{\mathcal{O}_K} R_{\mathcal{O}_K}}{q-1} (\ln q)^{\sharp S_K - 1} s^{\sharp S_K - 1} + O(s^{\sharp S_K}),$$

and thus we obtain

$$h_{\mathcal{O}_L} R_{\mathcal{O}_L} = h_{\mathcal{O}_K} R_{\mathcal{O}_K} L_{\mathcal{O}_K}(0,\chi). \tag{5}$$

Proposition 5 *Let L/K be an imaginary quadratic extension and K/k be a real extension of degree d of the rational function field $k = \mathbf{F}_q(x)$. Then, we have:*

$$h_{\mathcal{O}_L}^- = Q_{L/K} 2^{1-d} L_{\mathcal{O}_K}(0,\chi)$$

Proof. The equality follows from (5) and proposition 1. □

Proposition 6 *Let L/K be an imaginary quadratic extension and K/k be a real extension of the rational function field $k = \mathbf{F}_q(x)$. Then, $L_{\mathcal{O}_K}(s,\chi)$ is a polynomial in q^{-s} of degree $\partial = 2(g_L - g_K) + j$, with $j = \sharp\{P_i \in S_K \mid P_i \text{ inert in } L/K\}$ and where g_L and g_K are the genus of the functions fields L and K.*

Proof. Equations (3) and (4) implies:

$$L_{\mathcal{O}_K}(s,\chi) = \frac{\zeta_{\mathcal{O}_L}(s)}{\zeta_{\mathcal{O}_K}(s)} = \frac{\zeta_L(s)}{\zeta_K(s)} \frac{\prod_{P\in S_K}\left(1-\frac{1}{N(P)^s}\right)^{-1}}{\prod_{\wp\in S_L}\left(1-\frac{1}{N(\wp)^s}\right)^{-1}} = \frac{\zeta_L(s)}{\zeta_K(s)} L_\infty(s)$$

where $L_\infty(s) = \dfrac{\prod_{P\in S_K}\left(1-\frac{1}{N(P)^s}\right)^{-1}}{\prod_{\wp\in S_L}\left(1-\frac{1}{N(\wp)^s}\right)^{-1}}$. The divisibility of the numerators of the zeta function of the functions fields L and K shown in [2] implies that $(\zeta_L/\zeta_K)(s)$ is a polynomial in q^{-s} of degree $2(g_L - g_K)$. The extension K/k being totally real, the infinite places of K have degree 1 and for $P \in S_K$ we get: $1 - \frac{1}{N(P)^s} = 1 - q^{-s}$. The result follows from the fact that $N(\mathfrak{P}_i) = N(P_i)^2$ if and only if P_i is inert in L/K.

□

Now, we extend χ multiplicatively to the nonzero ideals of $\mathcal{O}_K$. If I is a nonzero ideal of $\mathcal{O}_K$, define the degree of I by $N(I) = q^{\deg I}$. For any integer i, consider as in [4], the sum

$$S_i(\chi) = \sum_{\deg I = i} \chi(I)$$

where the sum ranges over all nonzero ideal I of $\mathcal{O}_K$ of degree i. Remark that we have $S_0(\chi) = 1$.

Consider the sum $\sum_{i=0}^{\partial} S_i(\chi)$ with ∂ defined in proposition 6. This sum is finite since there exist only finitely many ideals in $\mathcal{O}_K$ of fixed degree.

We have:

Proposition 7 *Let ∂ be as in proposition 6. We have*

$$L_{\mathcal{O}_K}(0,\chi) = \sum_{i=0}^{\partial} S_i(\chi).$$

Proof. In the following, the sums range over nonzero ideals I of $\mathcal{O}_K$.

$$\begin{aligned} L_{\mathcal{O}_K}(s,\chi) &= \prod_{P\in \mathrm{Spec}(\mathcal{O}_K)-\{0\}} \Big(1-\frac{\chi(P)}{N(P)^s}\Big)^{-1} \\ &= \sum_I \frac{\chi(I)}{N(I)^s} = \sum_I \frac{\chi(I)}{q^{s\deg I}} \\ &= \sum_{i=0}^{\infty} \sum_{\deg I=i} \frac{\chi(I)}{q^{is}} = \sum_{i=0}^{\infty} \frac{1}{q^{is}} \sum_{\deg I=i} \chi(I) \\ &= \sum_{i=0}^{\infty} (q^{-s})^i S_i(\chi) = \sum_{i=0}^{\partial} (q^{-s})^i S_i(\chi), \end{aligned}$$

where the last equality holds by proposition 6. □

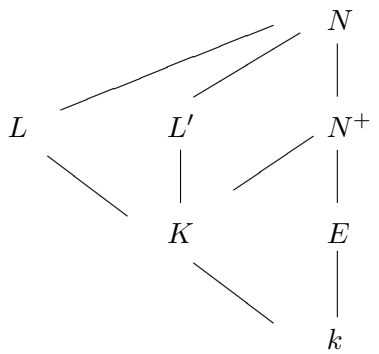
4 The quartic case

4.1 The relation with the Galois closure

Lemma 8 *let L/K be an imaginary quadratic extension and K/k be a real quadratic extension. If L/k is non Galois then the Galois closure of L is a dihedral octic function field (i.e. $[L:k]=8$ and $\mathrm{Gal}(L/k)\simeq D_4$ the dihedral group of order 8).*

Proof. The Galois closure N of L is just the compositum of L and its conjugate L' by the non trivial element of the Galois group $\mathrm{Gal}(L/K)$. The function field N has degree 8 over k, is not abelian and has more than one subfield of degree 4 over k, which excludes the quaternionic case. □

Thus, we are in the following situation, where all the extensions are quadratic:



where L' is the conjugate of L.

Lemma 9 *Let L/K be imaginary quadratic, K/k be real quadratic, L/k be non Galois and N be the Galois closure of L. Then, we have the following relation between their zeta functions:*

$$\zeta_N(s)/\zeta_{N^+}(s) = (\zeta_L(s)/\zeta_K(s))^2.$$

Proof. Since the extension N/K is abelian, we can show as in [3] (see also chapter 14 of [10]) that we have the factorization:

$$\zeta_N(s)/\zeta_K(s) = (\zeta_L(s)/\zeta_K(s))(\zeta_{L'}(s)/\zeta_K(s))(\zeta_{N^+}(s)/\zeta_K(s))$$

which implies that:

$$\zeta_N(s)/\zeta_{N^+}(s) = (\zeta_L(s)/\zeta_K(s))(\zeta_{L'}(s)/\zeta_K(s)).$$

But the functions fields L and L', with L' the conjugate of L under $\mathrm{Gal}(K/k)$, have the same zeta function. Then, the result follows. □

We are now in position to give a relation between the relative ideal class numbers of N and L:

Proposition 10 *Let L/K be imaginary quadratic, K/k be real quadratic, L/k be non Galois and N be the Galois closure of L. Then we have:*

$$h^-_{\mathcal{O}_N} = \frac{Q_{N/N^+}}{2}(h^-_{\mathcal{O}_L})^2.$$

Proof. We have seen that for any function field $\mathcal{K}$, we have:

$$\zeta_{\mathcal{O}_\mathcal{K}}(s) = \frac{-h_{\mathcal{O}_\mathcal{K}} R_{\mathcal{O}_\mathcal{K}}}{q-1}(\ln q)^{\sharp S_\mathcal{K}-1} s^{\sharp S_\mathcal{K}-1} + O(s^{\sharp S_\mathcal{K}}).$$

Considering the function $\Lambda_{\mathcal{O}_\mathcal{K}}(s) = \zeta_{\mathcal{O}_\mathcal{K}}(s)/s^{\sharp S_\mathcal{K}-1}$, we get by lemma 9

$$\Big(\Lambda_{\mathcal{O}_N}/\Lambda_{\mathcal{O}_{N^+}}\Big)(0) = \Big(\Lambda_{\mathcal{O}_L}/\Lambda_{\mathcal{O}_K}\Big)^2(0)$$

since $\sharp S_N - \sharp S_{N^+} = \sharp S_L - \sharp S_K = 0$. Thus, we obtain:

$$\frac{R_{\mathcal{O}_N}}{R_{\mathcal{O}_{N^+}}} h^-_{\mathcal{O}_N} = \Big(\frac{R_{\mathcal{O}_L}}{R_{\mathcal{O}_K}} h^-_{\mathcal{O}_L}\Big)^2.$$

Thus, proposition 1 and $\sharp S_{N^+} = 2\sharp S_K$ give us:

$$h^-_{\mathcal{O}_N} = \frac{Q_{N/N^+}}{2}\Big(\frac{h^-_{\mathcal{O}_L}}{Q_{L/K}}\Big)^2.$$

Now, we show that, under the hypothesis of the proposition, we have $Q_{L/K} = 1$. Suppose on the contrary that $Q_{L/K} = 2$ (by proposition 1, it is 1 or 2) and let us show that this implies that L/k is Galois. If $Q_{L/K} = 2$, we can write $L = K(\sqrt{\varepsilon_K})$ with ε_K a fundamental unit of $\mathcal{O}_K$. Consider the constant field extensions $\tilde{\mathcal{K}} = \mathcal{K} \otimes_{\mathbf{F}_q} \mathbf{F}_{q^2}$ for $\mathcal{K} = k, K, L$ and N. The extension $\tilde{L}/\tilde{k}$ is Galois since $\tilde{L} = \tilde{K}(\sqrt{\varepsilon_K})$, $\tilde{K}/\tilde{k}$ is real and the norm $N_{\tilde{K}/\tilde{k}}(\varepsilon_K)$ is a square in $\tilde{K}$ (see lemma 16 (i)). Moreover, the extension $\tilde{N}/k$ is Galois of Galois group $D_4 \times \mathbf{Z}/2\mathbf{Z}$ and thus $\tilde{N}/\tilde{k}$ is Galois of Galois group the dihedral group D_4. Hence $\tilde{L}$ is the fixed field of $\tilde{N}$ by a normal subgroup H of order 2 of D_4. Thus:

$$L = \tilde{L} \cap N = \tilde{N}^{H \times \{1\}} \cap \tilde{N}^{\{1\} \times \mathbf{Z}/2\mathbf{Z}} = \tilde{N}^{H \times \mathbf{Z}/2\mathbf{Z}}.$$

Since H is a normal subgroup of D_4 this implies that $H \times \mathbf{Z}/2\mathbf{Z}$ is a normal subgroup of $D_4 \times \mathbf{Z}/2\mathbf{Z}$ and we obtain that L/k is Galois, which is in contradiction with our hypothesis. Finally, the Hasse index $Q_{L/K} = 1$ and the proposition is proved. □

The Hasse index Q_{N/N^+} is equal to 1 or 2 according to proposition 1. Thus, remarking that relative class numbers are integers, we have the following corollary.

Corollary 11 *Let L/K be imaginary quadratic, K/k be real quadratic, L/k be non Galois and N be the Galois closure of L. Then we have:*

$$h^-_{\mathcal{O}_N} = 1 \Longleftrightarrow h^-_{\mathcal{O}_L} = 1.$$

In other words, the relative ideal class number one problem for imaginary quartic non Galois function field having a real subquadratic field is equivalent to the one in the octic Galois dihedral case.

In fact, it remains to consider the general octic Galois case since the quaternionic case can be set aside by the following proposition.

Proposition 12 *Let N/N^+ be imaginary, N^+/k be real with N/k Galois with Galois group Q_8 the quaternionic group of order 8. Then, $h^-_{\mathcal{O}_N}$ is even.*

Proof. By proposition 4, it suffices to show that the number t_{N/N^+} of finite ramified places in N/N^+ is at least 2. But since the extension N/k is quaternionic, this implies that the extension N^+/k is biquadratic (i.e. $\mathrm{Gal}(N^+/k) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$). Combined with the fact that N^+/k is real , this implies that there is at least two finite places ramified in N^+/k. But they are also ramified in N/N^+ since the subgroup of order 2 of Q_8 is contained in all the non trivial ones and thus any inertia group contains this group. Hence, any place ramified in N^+/k is ramified in N/N^+. □

4.2 A formula for quartic extensions with principal real quadratic subfield

We are interested now in the case where L/k has degree 4 with $h_{\mathcal{O}_L} = 1$. Thus, we suppose that L/K is imaginary quadratic and that K/k is real quadratic and we assume furthermore that $\mathcal{O}_K$ is a principal domain, i.e. that $h_{\mathcal{O}_K} = 1$ (since $h_{\mathcal{O}_L} = 1$ implies that $h_{\mathcal{O}_K} = 1$ by proposition 2). Now, let us study the symbol $\chi(P)$ previously defined (recall that L has odd characteristic).

Suppose that $K = k(\sqrt{m})$ with $m = m_K \in \mathbf{F}_q[X]$ a square-free polynomial. Since we assume that the place ∞ splits in K/k, then m is necessarily a polynomial of even degree with leading coefficient a square in $\mathbf{F}_q^*$.

Suppose that $L = K(\sqrt{M})$ with $M = M_L \in \mathcal{O}_K$ square-free in $\mathcal{O}_K$.

Let $P = \pi\mathcal{O}_K$ be a principal prime ideal of $\mathcal{O}_K$ generated by π. Let $p \in \mathbf{F}_q[X]$ be such that $P \mid p$, that is such that $P \cap \mathbf{F}_q[X] = p\mathbf{F}_q[X]$.

Definition. *If Q is an element of $\mathcal{O}_K$, we define the symbol $[\frac{Q}{P}]$ to be 0 if $Q \in P$, 1 if Q is congruent to a square modulo P, and -1 otherwise.*

Lemma 13 *We have*

$$\chi(P) = [\frac{M}{P}].$$

Proof. The result follows from the fact that M is square-free in $\mathcal{O}_K$. □

Lemma 14 *If $n \in \mathbf{F}_q[X]$ and if p is not inert, we have:*

$$[\frac{n}{P}] = (\frac{n}{p})$$

where $(\frac{n}{p})$ is the quadratic character on $\mathbf{F}_q[X]$ defined to be 0 if $p \mid n$, 1 if n is congruent to a square modulo p, and -1 otherwise.

Proof. We have $[\frac{n}{P}] \equiv n^{\frac{N(P)-1}{2}} \bmod P$ and $(\frac{n}{p}) \equiv n^{\frac{N(p)-1}{2}} \bmod p$. But $N(P) = N(p) = q^{\deg p}$ if p is not inert. □

Let $\mathrm{Gal}(K/k) = \{Id, \sigma\}$. We set $\sigma(\pi) = \bar{\pi}$, and Tr will denote the trace of K/k. The following theorem is an analogue of the one that holds in the number field case (see [7]).

Theorem 15 *(i) If p splits in K/k then $[\frac{M}{P}] = [\frac{M}{(\pi)}] = (\frac{Tr(\pi)Tr(M\bar{\pi})}{p})$ and $[\frac{M}{(\pi)}][\frac{M}{(\bar{\pi})}] = (\frac{M\bar{M}}{p})$.*

(ii) If p is inert in K/k then $[\frac{M}{P}] = (\frac{M\bar{M}}{p})$.

(iii) If p is ramified in K/k then $[\frac{M}{P}] = (\frac{2Tr(M)}{p})$.

Proof. (i) First, let us remark that if p splits in K/k then $\mathrm{Tr}(\pi) \notin (\pi)$. Indeed, $\mathrm{Tr}(\pi) \in (\pi)$ iff $\bar{\pi} \in (\pi)$ iff $(\bar{\pi}) = (\pi)$ iff p does not split.

Now, $\mathrm{Tr}(M\bar{\pi}) = M\bar{\pi} + \bar{M}\pi = M(\pi + \bar{\pi}) + \pi(\bar{M} - M) \equiv M\,\mathrm{Tr}(\pi) \bmod \pi$. Thus, $\mathrm{Tr}(\pi)\,\mathrm{Tr}(M\bar{\pi}) \equiv M(\mathrm{Tr}(\pi))^2 \bmod \pi$ and

$$\Big[\frac{\mathrm{Tr}(\pi)\,\mathrm{Tr}(M\bar{\pi})}{(\pi)}\Big] = \Big[\frac{M(\mathrm{Tr}(\pi))^2}{(\pi)}\Big].$$

But $\mathrm{Tr}(\pi)\,\mathrm{Tr}(M\bar{\pi}) \in \mathbf{F}_q[X]$ thus by lemma 14 we get:

$$\Big[\frac{\mathrm{Tr}(\pi)\,\mathrm{Tr}(M\bar{\pi})}{(\pi)}\Big] = \Big(\frac{\mathrm{Tr}(\pi)\,\mathrm{Tr}(M\bar{\pi})}{p}\Big)$$

and

$$\Big[\frac{M(\mathrm{Tr}(\pi))^2}{(\pi)}\Big] = \Big(\frac{\mathrm{Tr}(\pi)\,\mathrm{Tr}(M\bar{\pi})}{p}\Big).$$

Since $\mathrm{Tr}(\pi) \notin (\pi)$ we obtain $[\frac{M}{P}] = [\frac{M}{(\pi)}] = (\frac{\mathrm{Tr}(\pi)\,\mathrm{Tr}(M\bar{\pi})}{p})$. Furthermore, we can show easily that:

$$\Big[\frac{M}{(\pi)}\Big]\Big[\frac{M}{(\bar{\pi})}\Big] = \Big[\frac{M\bar{M}}{p}\Big]$$

(ii) If p is inert, we have $\mathcal{O}_K/p\mathcal{O}_K = \mathcal{O}_K/\pi\mathcal{O}_K$ which is an extension of degree 2 of $\mathbf{F}_q[X]/(p) \simeq \mathbf{F}_{q^{\deg p}} = \mathbf{F}_{N(p)}$. We have in this case $\bar{M} \equiv M^{q^{\deg p}} \bmod p\mathcal{O}_K$. Furthermore, we can easily show that, if $n \in \mathbf{F}_q[X]$, then

$$\Big(\frac{n}{p}\Big) \equiv n^{(q^{\deg p}-1)/2} \bmod (p)$$

Then, we have

$$(\frac{M\bar{M}}{p}) \equiv (M\bar{M})^{\frac{N(p)-1}{2}} \equiv (MM^{q^{\deg p}})^{\frac{q^{\deg p}-1}{2}} \equiv M^{\frac{N^2(p)-1}{2}} \equiv [\frac{M}{(\pi)}] \bmod p\mathcal{O}_K.$$

(iii) By the property of the different, we know that (π) divides the different $\mathcal{D}_{\mathcal{O}_K/\mathbf{F}_q[X]}$ and that $\mathcal{D}_{\mathcal{O}_K/\mathbf{F}_q[X]}$ is the greater common divisor of all ideal $(f'_\alpha(\alpha))$ where α is an integral generator of K over k and f is the irreducible polynomial for α over k (see [5]). Since $f_M(X) = X^2 - \mathrm{Tr}(M)X + N(M)$, we have $f'_M(M) = M - \bar{M}$ and thus $\mathcal{D}_{\mathcal{O}_K/\mathbf{F}_q[X]}$ divides $\bar{M} - M$. Hence, $\bar{M} - M \in (\pi)$ and $2\,\mathrm{Tr}(M) = 2M + 2\bar{M} = 4M + 2(\bar{M} - M) \equiv 4M \bmod(\pi)$. Thus, $[\frac{M}{(\pi)}] = [\frac{4M}{(\pi)}] = [\frac{2\,\mathrm{Tr}(M)}{(\pi)}] = (\frac{2\,\mathrm{Tr}(M)}{(p)})$, by lemma 14. □

This theorem provides us with a method for calculating $\chi(P)$ for any nonzero principal prime ideal P of $\mathcal{O}_K$, hence for calculating $S_i(\chi)$, hence $L_{\mathcal{O}_K}(0,\chi)$ by proposition 7, hence $h^-_{\mathcal{O}_L}$ by proposition 5.

4.3 Principal Non Galois quartic extension

The ideal class number one problem for bicyclic quartic Galois extension is treated in [13] and [3] according as the characteristic of k is odd or even. The case of cyclic quartic Galois extension L/k is derived from [11] which solved the prime power cyclic case. We now investigate the non Galois quartic case.

Consider, as in the previous section, a quartic function field extension L/k with L/K imaginary quadratic and K/k real quadratic. We set also $K = k(\sqrt{m})$ with $m \in \mathbf{F}_q[X]$ a square-free polynomial, $\mathrm{Gal}(K/k) = \{Id, \sigma\}$ and $L = K(\sqrt{M})$ with $M \in \mathcal{O}_K$ square-free in $\mathcal{O}_K$.

Lemma 16 *(i) The extension L/k is Galois if and only if the norm $N_{K/k}(M) := \sigma(M)M$ is a square in K. Moreover, $N_{K/k}(M)$ is a square in K if and only if $N_{K/k}(M)$ is a square in k or $N_{K/k}(M)/m$ is a square in k.*

(ii) If $h_{\mathcal{O}_L} = 1$ then at least one of the infinite places P_1 or P_2 of K is ramified in L.

Proof. (i) It is easily seen that L/k is Galois if and only if $\sigma(M)/M$ is a square in K which is equivalent to $N_{K/k}(M)$ is a square in K. Moreover, if $N_{K/k}(M) = (a(x) + b(x)\sqrt{m})^2 = a(x)^2 + b(x)^2 m + 2a(x)b(x)\sqrt{m}$ and since it lies in k, we get the equivalence.

(ii) As remarked in [11], the constant field extension $(\mathbf{F}_{q^{\delta_{\mathcal{O}_L}}}.L)/L$ has degree $\delta_{\mathcal{O}_L}$ and is contained in the Hilbert class field of L, thus $\delta_{\mathcal{O}_L}$ divides $h_{\mathcal{O}_L}$. Since $\delta_{\mathcal{O}_L} = \gcd(\deg \mathfrak{P}_1, \deg \mathfrak{P}_2)$ where $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are the infinite places of L, we obtain that at least one of these degrees is equal to one (L/K is not supposed to be Galois) and thus the corresponding place is ramified. □

Proposition 17 *With the notations above, if we suppose that $h_{\mathcal{O}_L} = 1$ and that the genus g_K of K is non zero then the cardinality of the finite base field $\mathbf{F}_q$ is less than or equal to 5.*

Proof. Since the function field L is an extension of the function field K, it follows that the numerator polynomial $P_K(T)$ of the zeta function of K divides that of L (see [2] for a proof). This means that the relative divisor class number $h_L^- = \frac{P_L(1)}{P_K(1)}$ can be written as a product $h_L^- = \prod_{i=1}^{2(g_L - g_K)}(1 - \omega_i)$ with ω_i complex numbers of modulus $\sqrt{q}$ (Riemann Hypothesis). Thus, we have the following lower bound:

$$h_L^- \geq (\sqrt{q} - 1)^{2(g_L - g_K)} = (\sqrt{q} - 1)^{2(g_K - 1) + \deg \mathrm{Diff}_{L/K}}$$

where $\deg \mathrm{Diff}_{L/K}$ is the degree of the different of L/K (the last equality comes from Riemann-Hurwitz theorem).

Moreover, using the Schmidt relation, we obtain the following lower bound for the ideal class number of L:

$$h_{\mathcal{O}_L} \geq h_{\mathcal{O}_K} \frac{Q_{L/K}}{2} \prod_{i=1}^{2} \deg \mathfrak{P}_i (\sqrt{q} - 1)^{2(g_K - 1) + \deg \mathrm{Diff}_{L/K}}. \tag{6}$$

But now, if we suppose that $h_{\mathcal{O}_L} = 1$ then by proposition 2, we obtain that $h_{\mathcal{O}_K} = 1$ and by lemma 16, (ii), we obtain that $\deg \mathrm{Diff}_{L/K} \neq 0$ (which implies that $\deg \mathrm{Diff}_{L/K} \geq 2$ since it is even by the Riemann-Hurwitz theorem). Thus, the inequality becomes :

$$(\sqrt{q} - 1)^a \leq 2$$

with $a \geq 2$ which gives the bound on q. □

Remarks. For $q = 5$, the inequality (6) implies that $g_L = 2$, $g_K = 1$, $\deg \mathrm{Diff}_{L/K} = 2$, $\deg \mathfrak{P}_1 = \deg \mathfrak{P}_2 = 1$ (the two places that ramify in L/K are P_1 and P_2) and $Q_{L/K} = 1$. We have just finitely many cases to consider. Recall that the 2-rank

$$rk_2(\mathrm{Cl}(\mathcal{O}_F)) = \dim_{\mathbf{F}_2} \mathrm{Cl}(\mathcal{O}_F)/\mathrm{Cl}(\mathcal{O}_F)^2$$

of the ideal class group $\mathrm{Cl}(\mathcal{O}_F)$ of a quadratic function field $F = k(\sqrt{m})$ in odd characteristic is given by (see [1]): $rk_2(\mathrm{Cl}(\mathcal{O}_F)) = n - 1 - \mu_F$ if m has an irreductible factor of odd degree and $rk_2(\mathrm{Cl}(\mathcal{O}_F)) = n - \mu_F$ otherwise, where n is the number of monic irreducible polynomial factors of m and μ_F is equal to 0 or 1 according as F/k is imaginary or real.

Thus, for a real quadratic function field extension F/k, we have that the ideal class number $h_{\mathcal{O}_F}$ is odd if and only if m is an irreducible polynomial of even degree (with leading coefficient a square in $\mathbf{F}_q^*$) or m is the product of two monic irreducible polynomials of odd degree. Since we have found that the genus g_K must be equal to 1 for $q = 5$ and since $g_K = \frac{\deg m - 2}{2}$ for a real quadratic function field $k(\sqrt{m})$, we obtain that the polynomial m must have degree 4.

Then, the results of subsection 3.2 combined with those of subsection 4.2 provide us a method for calculating class numbers in the remain cases given by 4.3.

For $q = 3$, unfortunately, the inequality (6) doesn't give us any bound on the genus.

Acknowledgments. The author would like to thank Stéphane Louboutin, Marc Perret and Dominique Le Brigand for many helpful discussions.

References

[1] E. Artin, Quadratische Körper in Gebiete der höheren Kongruenzen, I, II, *Math. Zeit.*, **19**, 153-246, (1924).

[2] Y. Aubry, Class number in totally imaginary extensions of totally real function fields, *Third International Conference on Finite fields and Applications*, Lecture Note Series of the London Mathematical Society, Cambridge University Press (1996), 23-29.

[3] Y. Aubry, D. Le Brigand, Imaginary bicyclic biquadratic functions fields in characteristic two, J. Number Theory **77**, 36-50 (1999).

[4] S. Galovich, M. Rosen, The class number of cyclotomic function fields, J. Number Theory **13** (1981), 363-375.

[5] S. Lang, Algebraic number theory, Addison-Wesley Series in Math., (1970).

[6] S. Lang, Cyclotomic fields I and II, Graduate Texts in Math. **121**, Springer-Verlag (1990).

[7] S. Louboutin, L-functions and class numbers of imaginary quadratic fields and of quadratic extensions of an imaginary quadratic field, Math. Comp. **59**, (1992), 213-230.

[8] S. Louboutin, R. Okazaki, Determination of all non-normal quartic CM-fields and of all non-abelian normal octic CM-fields with class number one, Acta Arith. **67**, no. 1, (1994), 47-62.

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

[10] M. Rosen, Number theory in function fields, Graduate Texts in Maths **210**, Spinger-Verlag (2002).

[11] S. Sémirat, Class number one problem for imaginary function fields: the cyclic prime power case, J. Number Theory **84**, 166-183 (2000).

[12] K. Uchida, Relative class numbers of normal CM-fields, Tôhoku Math. Journ. **25**, 347-353 (1973).

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