Séminaires & Congrès
11, 2005, p. 143–169

REAL QUADRATIC EXTENSIONS OF THE RATIONAL FUNCTION FIELD IN CHARACTERISTIC TWO

by

Dominique Le Brigand

Abstract. — We consider real quadratic extensions of the rational field over a finite field of characteristic two. After recalling the equation of such extensions, we present a geometric approach of the continued fraction expansion algorithm to compute the regulator. Finally, we study the ideal class number one problem and give numerous examples for which the ideal class number equals one.

Résumé **(Extensions quadratiques réelles du corps rationnel en caractéristique** 2)

Nous étudions les extensions quadratiques réelles du corps rationnel sur un corps fini de caractéristique 2. On rappelle la forme générale de telles extensions puis on donne une approche géométrique de l'algorithme des fractions continues qui permet de calculer le régulateur. Enfin on s'intéresse aux extensions quadratiques réelles dont le nombre de classes d'idéaux de l'anneau des entiers est égal à un et on donne un grand nombre d'exemples pour lesquels cette situation est réalisée.

1. Introduction

We consider a separable quadratic extension K of the rational field $k = \mathbb{F}_q$, such that the full constant field of the function field $K/\mathbb{F}_q$ is $\mathbb{F}_q$. We denote by $\mathcal{O}_x$ the integral closure of $\mathbb{F}_q[x]$ in K and by h_x the ideal class-number of $\mathcal{O}_x$. It is easy to prove that there is only a finite number of imaginary quadratic extensions such that $h_x =$ constant. For real quadratic extensions and when the constant field $\mathbb{F}_q$ is fixed, it is not known whether this result is false or not. The Gauss conjecture for function fields pretends that there is an infinite number of real quadratic extensions such that $h_x = 1$. The main motivation for this paper was to examine the validity of the Gauss conjecture in the characteristic 2 case. Unfortunately, we have no answer. This paper is organized as follows. In Section 2, we recall basic results about quadratic extensions. In Section 3, we focus on real quadratic extensions in characteristic 2 and

2000 ***Mathematics Subject Classification.*** — 11R58, 11A55.
Key words and phrases. — Real quadratic extension, continued fraction expansion algorithm, regulator, ideal class number.

© Séminaires et Congrès 11, SMF 2005

give some geometric approach of the continued fraction expansion (CFE) algorithm. In Section 4, we study the ideal class number one problem in characteristic 2 and give examples. In particular, we give all the real quadratic extensions of a particular form such that $h_x = 1$.

2. Quadratic extensions

Let $q = p^e$, and let x be transcendental over $\mathbb{F}_q$, $k = \mathbb{F}_q(x)$, finally let K/k be a (separable) quadratic extension. We always assume that $\mathbb{F}_q$ is the full constant field of the hyperelliptic function field $K/\mathbb{F}_q$ and that the genus of K is $g \geqslant 1$. The places of the rational function field $k = \mathbb{F}_q(x)$ are ∞, the pole of x, and the other places, called *finite places of* $k/\mathbb{F}_q$, are in one to one correspondence with the monic irreducible polynomials of $\mathbb{F}_q[x]$. We denote by (P) the place corresponding to the monic irreducible polynomial $P \in \mathbb{F}_q[x]$. The degree of the place (P) is equal to the degree, $\operatorname{Deg} P$, of the polynomial P. If $\wp$ is a place of $K/\mathbb{F}_q$ which is above a finite place (P) of k (we denote this by $\wp|(P)$), we say that $\wp$ is a *finite place of* K. We say that a finite place $\wp$ of K, $\wp|(P)$, is inert (resp. split, resp. ramified) if (P) is inert (resp. split, resp. ramified) in the extension K/k. We denote by $\operatorname{supp} D$ the support of a divisor D of $K/\mathbb{F}_q$, by $\deg D$ its degree. The principal divisor of a $u \in K^*$ is denoted by $\operatorname{div}(u)$ and $\operatorname{div}(u) = \operatorname{div}_0(u) - \operatorname{div}_\infty(u)$, with $\operatorname{div}_0(u)$ (resp. $\operatorname{div}_\infty(u)$) the zero divisor (resp. the pole divisor) of u. We denote by h the divisor class number of $K/\mathbb{F}_q$, *i.e.* the order of the jacobian over $\mathbb{F}_q$, $\mathcal{J}\mathrm{ac}(K/\mathbb{F}_q)$, considered as the group of classes of zero degree divisors modulo principal ones. The class in $\mathcal{J}\mathrm{ac}(K/\mathbb{F}_q)$ of a zero-degree divisor R is denoted by $[R]$. Let $\mathcal{O}_x$ be the integral closure of $\mathbb{F}_q[x]$ in K. Then $\mathcal{O}_x$ is the ring of S_x-integers, S_x being the set of places of K above the infinite place ∞ of the rational field k. $\mathcal{O}_x$ is a Dedekind domain and a $k[x]$-module of rank 2. The group of fractionary ideals modulo principal ones is finite and its order h_x is the *ideal class-number of* $\mathcal{O}_x$. The ring $\mathcal{O}_x$ is principal if and only if $h_x = 1$. In this paper, we will say that h_x is the ideal class-number of $\mathcal{O}_x$ or the ideal class-number of the quadratic extension K/k. We recall that

– if $\operatorname{card} S_x = 1$, K/k *is an imaginary quadratic extension*: if $S_x = \{P_\infty\}$, with $\deg P_\infty = 1$, K/k *is ramified* and if $S_x = \{\wp_\infty\}$, with $\deg \wp_\infty = 2$, K/k *is inert*;

– if $\operatorname{card} S_x = 2$, K/k *is a real quadratic extension* and we set $S_x = \{\infty_1, \infty_2\}$.

This situation was studied by Artin [**1**] in his thesis, when $p = \operatorname{char} \mathbb{F}_q > 2$. The two class numbers h and h_x are linked by Schmidt's formula (*cf.* [**29**]) $h_x r_x = h\delta_x$, where r_x is the *regulator of the extension* K/k and $\delta_x = \gcd\{\deg \wp, \wp|\infty\}$. If the extension K/k is an imaginary quadratic extension, $r_x = 1$ and $h_x = h$ (resp. $h_x = 2h$) if ∞ ramifies (resp. is inert) in K. If the extension K/k is real quadratic, r_x is the order of the subgroup of the jacobian of $K/\mathbb{F}_q$ generated by the class $C_\infty = [\infty_2 - \infty_1]$. Moreover, we have $h_x = 1$ if and only if $\mathcal{J}\mathrm{ac}(K/\mathbb{F}_q)$ is a cyclic group generated by C_∞. Finally, notice that the study of the jacobian of a hyperelliptic function field is of theoretical interest in cryptography in relation with the discrete logarithm problem. Many papers deal with that subject (see for instance [**25**] and [**33**] for odd characteristic and [**26**] for $p = 2$).

2.1. Affine model of a quadratic extension. — In characteristic $p = 2$, the equation defining a real extension K/k is less well known than in the odd characteristic case. For sake of completeness we recall both situations.

Theorem 1. — *Let $q = p^e$ and let $K/\mathbb{F}_q$ be a hyperelliptic function field of genus $g \geqslant 1$, such that the full constant field of $K/\mathbb{F}_q$ is $\mathbb{F}_q$. Let $x \in K$ be transcendental over $\mathbb{F}_q$, $k = \mathbb{F}_q(x)$, such that K/k is separable and quadratic. We denote by λ_x the number of finite places of k which ramify in K.*

(1) *Case $p > 2$. Then $K = k(y)$, with $F(x, y) = y^2 - f(x) = 0$, where $f \in \mathbb{F}_q[x]$ and $f = aP_1 \cdots P_r \in \mathbb{F}_q[x]$, the P_i's being pairwise distinct monic irreducible polynomials and $a \in \mathbb{F}_q^*$. Moreover the finite places of k which ramify in K are the (P_i)'s, so $\lambda_x = r$. Set $m = \operatorname{Deg} f$.*

(a) *If the quadratic extension K/k is imaginary and ∞ ramifies in K, y may be chosen such that $a = 1$, $m = 2g + 1$.*

(b) *If the quadratic extension K/k is imaginary and ∞ is inert in K, y may be chosen such that a is a non-square, $m = 2g + 2$.*

(c) *If the quadratic extension K/k is real, y may be chosen such that $a = 1$, $m = 2g + 2$.*

(2) *Case $p = 2$. Then $K = k(y)$, with $F(x, y) = y^2 + B(x)y + C(x) = 0$, where B, $C \in (\mathbb{F}_q[x])^*$ are such that B is monic and all irreducible factors of B (if any) are simple factors of C, i.e.*

$$B = \prod_{i=1}^{r} B_i^{n_i} \quad \text{and} \quad C = aN \prod_{i=1}^{r} B_i,$$

the B_i's are pairwise distinct monic irreducible polynomials, $N \in \mathbb{F}_q[x]^*$ is monic and prime to B, $a \in \mathbb{F}_q^*$. Moreover the finite places of k which ramify in K are the (B_i)'s, so $\lambda_x = r$. Set $m = \operatorname{Deg} C$.

(a) *If the quadratic extension K/k is imaginary and ∞ ramifies in K, y may be chosen such that $m = 2g + 1$, $\operatorname{Deg} B \leqslant g$, $a = 1$.*

(b) *If the quadratic extension K/k is imaginary and ∞ is inert in K, y may be chosen such that $m = 2g + 2$, $\operatorname{Deg} B = g + 1$, $\operatorname{trace}_{\mathbb{F}_q/\mathbb{F}_2}(a) = 1$.*

(c) *If the quadratic extension K/k is real, y may be chosen such that $\operatorname{Deg} B = g + 1$, and $m < 2g + 2$.*

Reciprocally, any separable quadratic extension K of the rational function field $k = \mathbb{F}_q(x)$ is of the preceding form according to the behaviour of the infinite place of k in the extension K/k.

Remark 2. — We give some comments about this theorem for the characteristic 2 case (compare with [**8**]). First of all, everything goes back to Hasse (see also [**35**] for instance), since setting $v = y/B$, one obtains an equation in Hasse normal form (see [**14**]):

$$G(v, s) = v^2 + v + \frac{aN}{\prod_{i=1}^{r} B_i^{2n_i-1}} = 0 \,. \tag{1}$$

So this is well known. Observe that K/k is an *Artin-Schreier extension.* The condition B monic is not a restriction, since otherwise change y in $y' = y/b$, if $b \neq 1$ is the leading coefficient of B. If the quadratic extension K/k is real, it is unnecessary to consider the case $\operatorname{Deg} B = g+1$, $m = 2g+2$ and the leading coefficient a of C is such that $a = c + c^2$, with $c \in \mathbb{F}_q^*$ (*i.e.* $\operatorname{trace}_{\mathbb{F}_q/\mathbb{F}_2}(a) = 0$), since otherwise change y in $y' = y + cx^{g+1}$ and then $\operatorname{Deg} B = g+1$, and $m < 2g+2$. Finally, the condition: "all irreducible factors of B are simple factors of C" is quoted in [**4**] (for instance) and used in [**20**] to obtain the characterization of imaginary quadratic extensions.

Definition 3. — If K/k is a quadratic extension, we call *normal affine model of* K/k a plane affine curve $\mathcal{C}$ with equation $F(x, y) = 0$ satisfying the conditions of the preceding Theorem and say that F is a *normal equation of* K/k.

2.2. Hyperelliptic involution. — Consider a quadratic extension K/k and let $\mathcal{C} = \{F(x, y) = 0\}$ be an affine normal model of K/k. The *hyperelliptic involution* σ is the k-automorphism of K such that

$$\sigma(y) = \begin{cases} -y & \text{if } p > 2 \\ y + B(x) & \text{if } p = 2. \end{cases}$$

For $u \in K$, we set $\widetilde{u} = \sigma(u)$. The *norm of* u is defined by

$$N(u) = u\widetilde{u}.$$

The hyperelliptic involution acts on the finite places $\wp$ of $K/\mathbb{F}_q$ and $\widetilde{\wp} = \wp^\sigma$ is the *conjugated place* of $\wp$. Considering σ as an $\overline{\mathbb{F}_q}(x)$-automorphism of $\overline{K} = \overline{\mathbb{F}_q}K$, it acts on the affine points of $\mathcal{C}$: if $P = (a, b) \in \overline{\mathbb{F}_q}^2$ is such that $F(a, b) = 0$, then $P^\sigma = (a, -b)$ (resp. $P^\sigma = (a, b + B(a))$) if $p > 2$ (resp. $p = 2$) is an affine point of $\mathcal{C}$. We set $\widetilde{P} = P^\sigma$. Since an affine normal model $\mathcal{C}$ is a smooth affine curve in any characteristic, we identify the finite (degree one) places of $\overline{K} = K\overline{\mathbb{F}_q}$ with the (smooth) affine points $P = (a, b)$ of a normal affine model $\mathcal{C}$. Given any finite place (a, b) of $\overline{K}$, there is a unique finite place $\wp$ of K, such that its conorm in the constant field extension $\overline{K}/\overline{\mathbb{F}_q}$ of $K/\mathbb{F}_q$ is

$$\operatorname{Conorm}_{\overline{K}/K}(\wp) = \sum_{\tau \in \operatorname{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)} (a, b)^\tau.$$

2.3. Representation of elements in the jacobian of a hyperelliptic function field

2.3.1. Representation with reduced divisors

Definition 4. — Let K/k be a quadratic extension. An effective divisor A of the hyperelliptic function field $K/\mathbb{F}_q$ is called *quasi-reduced* if its support does not contain a pole of x, nor conorms (with respect to K/k) of places of $k/\mathbb{F}_q$. A quasi-reduced divisor A of $K/\mathbb{F}_q$ is called *reduced* if $\deg A \leqslant g$. We consider that $A = 0$ is reduced. We denote by $\mathcal{D}^+_{\mathrm{red}}$ the set of reduced divisors.

Note that if A is quasi-reduced, then its support $\operatorname{supp} A$ does not contain any inert finite place $\wp$ of K. Moreover, if a ramified finite place is in the support of A, then its valuation equals one and if a split finite place $\wp$ is in the support on A, then $\widetilde{\wp}$ is not in the support of A. In [**27**], the following representation of the elements of the jacobian of K/k is given (in the ramified case it goes back to [**1**] or [**6**] for $p \neq 2$ and [**16**] for $p = 2$). Observe that the authors of [**27**] assume that $p \neq 2$. But the results are also true for $p = 2$ considering an appropriate affine model.

Proposition 5. — *Let K/k be a quadratic extension and let g be the genus of the hyperelliptic function field $K/\mathbb{F}_q$.*

(1) *If K/k is ramified, then*

$$\mathcal{J}\mathrm{ac}(K/\mathbb{F}_q) = \{[A - (\deg A)P_\infty],\ A \in \mathcal{D}^+_{\mathrm{red}}\}.$$

(2) *If K/k is real, then*

$$\mathcal{J}\mathrm{ac}(K/\mathbb{F}_q) = \{[A - (\deg A)\infty_2 + n(\infty_1 - \infty_2)],\ A \in \mathcal{D}^+_{\mathrm{red}} \text{ and } 0 \leqslant n \leqslant g - \deg A\}.$$

Proof. — see [**27**]. □

Corollary 6. — *Let K/k be a real quadratic extension. The regulator of K/k is such that $r_x \geqslant g + 1$, where g is the genus of the hyperelliptic function field $K/\mathbb{F}_q$.*

Proof. — This a trivial consequence of the previous proposition, since

$$r_x = \inf\{n \in \mathbb{N}^*,\ n(\infty_1 - \infty_2) \text{ is a principal divisor}\}$$

and $n(\infty_1 - \infty_2)$ is not principal for all $0 \leqslant n \leqslant g$. □

2.3.2. Representation with reduced ideals. — Let K/k be a ramified or real quadratic extension given by a normal equation $F(x, y) = 0$. Then an integral basis of $\mathcal{O}_x$ is $(1, y)$ and we write this $\mathcal{O}_x = [1, y]$. We recall the following definitions.

Definition 7. — An ideal $\mathfrak{A}$ of $\mathcal{O}_x$ is called an *integral ideal.* Two integral ideals $\mathfrak{A}$ and $\mathfrak{B}$ are said to be *equivalent* if there exist non-zero $\alpha, \beta \in \mathcal{O}_x$ such that $(\alpha)\mathfrak{A} = (\beta)\mathfrak{B}$. An integral ideal $\mathfrak{A}$ is *principal* if there exists $\alpha \in K$ such that $\mathfrak{A} = (\alpha)\mathcal{O}_x$. The *conjugate of an integral ideal* $\mathfrak{A}$ is the integral ideal $\widetilde{\mathfrak{A}}$ such that $\widetilde{\mathfrak{A}} = \{\widetilde{\alpha},\ \alpha \in \mathfrak{A}\}$. An integral ideal $\mathfrak{A}$ is *ambiguous* if $\mathfrak{A} = \widetilde{\mathfrak{A}}$. The *polynomial norm* of $\mathfrak{A}$ is the polynomial $\mathcal{N}\mathfrak{A} \in \mathbb{F}_q[x]$ such that $\mathfrak{A}\widetilde{\mathfrak{A}} = (\mathcal{N}\mathfrak{A})\mathcal{O}_x$. The *degree of* $\mathfrak{A}$ is $\deg \mathfrak{A} = \operatorname{Deg} \mathcal{N}\mathfrak{A}$.

Definition 8. — Let K/k be a ramified or real quadratic extension. Let $\mathfrak{A}$ be a non-zero integral ideal and consider its factorization in prime ideals $\mathfrak{A} = \prod_{i\in I} \wp_i^{e_i}$. We say that $\mathfrak{A}$ is *quasi-reduced* (resp. *reduced*) if the corresponding effective divisor $A = \sum_{i\in I} e_i \wp_i$ is quasi-reduced (resp. reduced). We consider that $\{0\}$ is a reduced ideal.

For a ramified or real quadratic extension K/k, Proposition 5 can be written in terms of reduced ideals (see [**27**]). Let us recall the result for a real quadratic extension.

2.3.3. Case of a real quadratic extension. — If K/k is a real quadratic extension, an integral ideal $\mathfrak{A}$ has a $\mathbb{F}_q[x]$-basis such that: $\mathfrak{A} = (S)[Q, y + P]$, where $S, Q, P \in \mathbb{F}_q[x]$ and Q divides $N(y + P)$. If $p > 2$, this representation goes back to [**1**] (see also [**27**] and, if $p = 2$, [**37**, Th. 11].

Definition 9. — A *primitive ideal* is an integral ideal such that $\mathfrak{A} = [Q, y + P]$, with $Q|N(y + P)$ (*i.e.* $S = 1$).

It can be proved that a primitive ideal $\mathfrak{A}$ is quasi-reduced and it is reduced if and only if $\deg \mathfrak{A} \leqslant g$. We will see this further in case $p = 2$.

Corollary 10. — *Let K/k be a real quadratic extension. There is a canonical bijection between $\mathcal{J}\mathrm{ac}(K/\mathbb{F}_q)$ and the following set*

$$\mathbb{A} = \{(\mathfrak{a}, n),\ \mathfrak{a} \text{ reduced ideal and } 0 \leqslant n \leqslant g - \deg \mathfrak{a}\}.$$

Proof. — This is a straightforward consequence of Proposition 5 and of the definitions. We will not explain the group law on $\mathbb{A}$ (see [**27**] or [**37**] if $p = 2$). □

Corollary 11. — *Let K/k be a real quadratic extension.*

(1) *There is a canonical bijection between the cyclic subgroup of $\mathcal{J}\mathrm{ac}(K/\mathbb{F}_q)$ generated by the class $[\infty_2 - \infty_1]$ and the following set*

$$\{(\mathfrak{a}, n),\ \mathfrak{a} \text{ principal and reduced such that } 0 \leqslant n \leqslant g - \deg \mathfrak{a}\}.$$

(2) *The ideal class number h_x of K/k equals 1 if and only if all reduced ideals are principal.*

Proof. — Clear. □

Note that if the order h of the jacobian $\mathcal{J}\mathrm{ac}(K/\mathbb{F}_q)$ is a prime number, then of course $h_x = 1$.

2.4. Regular differentials of a hyperelliptic function field. — Let $K/\mathbb{F}_q$ be a hyperelliptic function field. In [**2**, p. 261] and for $p > 2$, it is said that any quasi-reduced divisor D of degree $\geqslant g$ is non-special. A similar result holds for characteristic $p = 2$. Let us recall both cases.

Lemma 12. — *Let $K/\mathbb{F}_q$ be a hyperelliptic function field and let x and y be such that $K = \mathbb{F}_q(x, y)$, with $F(x, y) = 0$ for F a normal equation of $K/k = \mathbb{F}_q(x)$. Then a $\mathbb{F}_q$-basis of the vector space of regular differentials $\Omega_K(0)$ is $(\omega_0,\, x\omega_0, \dots,\, x^{g-1}\omega_0)$, where*

$$\omega_0 = \begin{cases} dx/y & \text{if } p \neq 2 \\ dx/B(x) & \text{if } p = 2. \end{cases}$$

Proof. — By [**34**, Proposition VI.2.4], a basis of $\Omega_K(0)$ is $(\omega_0,\, x\omega_0, \dots,\, x^{g-1}\omega_0)$, where

$$\operatorname{div}(\omega_0) = (g-1)\operatorname{div}_\infty(x).$$

(1) Case $p \neq 2$. We have $F(x, y) = y^2 - f(x) = y^2 - aP_1(x)\dots P_r(x)$. Denote by $\mathfrak{p}_i$ the unique place of K above (P_i). Moreover

$$\operatorname{div}_\infty(x) = \begin{cases} 2P_\infty & \text{if } K/k \text{ ramifies} \\ \wp_\infty & \text{if } K/k \text{ is inert} \\ \infty_1 + \infty_2 & \text{if } K/k \text{ is real} \end{cases}$$

It is easy to show that $\operatorname{div}_\infty(y) = \sum_{i=1}^r \mathfrak{p}_i \operatorname{div}_\infty(y)$, where

$$\operatorname{div}_\infty(y) = \begin{cases} (2g+1)P_\infty & \text{if } K/k \text{ ramifies} \\ (g+1)\wp_\infty & \text{if } K/k \text{ is inert} \\ (g+1)(\infty_1 + \infty_2) & \text{if } K/k \text{ is real} \end{cases}$$

Since the extension K/k is a Kummer extension, the different of K/k is (see [**34**, III.7.6. p. 113])

$$\operatorname{Diff}_{K/k} = \sum_{i=1}^r \mathfrak{p}_i + \eta P_\infty$$

with $\eta = 1$ if K/k is ramified (resp. $\eta = 0$ otherwise). Then

$$\operatorname{div}(dx) = \operatorname{Diff}_{K/k} - 2\operatorname{div}_\infty(x) = \sum_{i=1}^r \mathfrak{p}_i + \eta P_\infty - 2\operatorname{div}_\infty(x)$$

and the result follows.

(2) Case $p = 2$. This result is classical concerning Artin-Schreier extension (one can adapt [**35**, p.168] to the non-algebraically closed case). We have $F(x, y) = y^2 + B(x)y + C(x) = y^2 + y\prod_{i=1}^r B_i^{n_i} + aN\prod_{i=1}^r B_i$. In case $\operatorname{Deg} B \geqslant 1$, let $\mathfrak{b}_i$ be the

unique place of K above the finite place (B_i) of k. Then

$$\operatorname{div}(dx) = \begin{cases} 2\sum_{i=1}^r n_i\mathfrak{b}_i - 2\operatorname{div}_\infty(x) & \text{if } K/k \text{ is real or inert} \\ 2\sum_{i=1}^r n_i\mathfrak{b}_i - (\sum_{i=1}^r n_i \deg \mathfrak{b}_i - g + 1)\operatorname{div}_\infty(x) & \text{if } K/k \text{ is ramified} \end{cases}$$

and

$$\operatorname{div}(B(x)) = 2\sum_{i=1}^r n_i\mathfrak{b}_i - \left(\sum_{i=1}^r n_i \deg \mathfrak{b}_i\right)\operatorname{div}_\infty(x).$$

The result follows. □

Proposition 13. — *Let K/k be a quadratic extension.*

(1) *If K/k is ramified or inert, any quasi-reduced divisor D of degree $\geqslant g$ is non-special.*

(2) *Assume K/k is real. Let $D = A + r\infty_i$, $i = 1$ or 2 and $r \in \mathbb{N}$, be an effective divisor of K/k of degree $\geqslant g$ such that A is quasi-reduced. Then D is non-special.*

Proof. — Let us show that $i(D) = \dim_{\mathbb{F}_q}\Omega(D) = 0$. Assume $\omega \in \Omega(D)^*$. Then, using Lemma 12, $\omega = (\sum_{i=0}^{g-1}\lambda_i x^i)\omega_0$ and $\operatorname{div}(\omega) \geqslant D$. Set $T(x) = \sum_{i=0}^{g-1}\lambda_i x^i \neq 0$, $e = \operatorname{Deg} T < g$. Then $T = \operatorname{div}_0(T(x))$ is a conorm with respect to K/k of degree $2e$. Moreover

$$\operatorname{div}(\omega) = T - e\ \operatorname{div}_\infty(x) + \operatorname{div}(\omega_0) = T + (g-1-e)\operatorname{div}_\infty(x).$$

(1) If K/k is ramified or inert, $\operatorname{div}(\omega) \geqslant D \iff T \geqslant D$. Since D is a quasi-reduced divisor and T is a conorm, $T \geqslant D$ implies $e \geqslant \deg D$ and we obtain $\deg D \leqslant g-1$ which is not true.

(2) If K/k is real, $\operatorname{div}(\omega) \geqslant D = A + r\infty_i \iff T + (g-1-e-r)\infty_i \geqslant A$, which is equivalent to $T \geqslant A$ and $r \leqslant g-1-e$. As before, we have $e \geqslant \deg A$ and we obtain $\deg D = \deg A + r \leqslant g-1$ which is not true. □

2.5. Ideal class number for quadratic extensions. — The classification of all imaginary quadratic extensions which have a given ideal class number is the analogue of the ideal class number problem for imaginary quadratic number fields. The ideal class number one problem ($h_x = 1$) for imaginary quadratic extensions has been settled by R.E. MacRae [**21**]. He proved that there is only one imaginary quadratic field if $p > 2$ (as predicted by Artin [**1**]) and three if $p = 2$. The analogue for function fields of the famous *Gauss Conjecture* for number fields is the following. For a fixed finite field $\mathbb{F}_q$, is there infinitely many real quadratic extensions $K/\mathbb{F}_q(x)$ such that the integral closure of $\mathbb{F}_q[x]$ in K is a principal domain? In [**7**], S. Chowla "presents a case where (this) conjecture ... is proved in a parallel case in function field theory, under the assumption of a very plausible conjecture in number theory". Without the assumption q fixed, there is a positive answer to the question. It has been proved first by M.L. Madan in [**22**] in the odd characteristic case. Other papers deal with similar results (see [**30**], [**13**], [**15**], [**19**], [**9**],...). But, as far as we know, the precise analogue for function fields of the Gauss conjecture remains unproved. The ideal class number h_x of a quadratic extension K/k is always even if K/k is inert, since then $h_x = 2h$. If K/k is ramified, h_x and h have the same parity, since $h = h_x$. We recall the following result concerning the parity of the ideal class number of a quadratic extension.

Proposition 14. — *Let K/k be a real quadratic extension, $k = \mathbb{F}_q(x)$. The ideal class number h_x of K/k is odd if and only if*

- case $p > 2$: *$K = k(y)$ with $y^2 = f(x)$, where $f \in \mathbb{F}_q[x]$ is such that*
  f is a monic irreducible polynomial of even degree, or
  $f = p_1 p_2$, p_1 and p_2 being monic irreducible polynomials of odd degree.
- case $p = 2$: *$K = k(y)$ with*

$$y^2 + b(x)^n y + aN(x)b(x) = 0, \tag{2}$$

where $aN \in \mathbb{F}_q[x]^*$, $b \in \mathbb{F}_q[x]^*$ is a monic irreducible polynomial, $\gcd(N, b) = 1$ *and* $\operatorname{Deg} N < (2n-1)\operatorname{Deg} b$.

Proof. — See [**36**] for $p > 2$ and [**31**] for any p. To prove this, one has to study the 2-rank of the ideal class group, which is related to the number of ambiguous ideals. □

If one wants to study the ideal class number one problem in characteristic 2, then the solutions have a normal equation given by (2).

3. Real quadratic extensions in even characteristic

We will now focus on the characteristic $p = 2$ case. There are similar results in the odd characteristic case. *In Section 3, we keep the following conventions or notations: $q = 2^e$, $k = \mathbb{F}_q(x)$, and K/k is a real quadratic extension defined by a normal equation*

$$F(x, y) = y^2 + B(x)y + C(x) = 0, \tag{3}$$

$B = \prod_{i=1}^{r} B_i^{n_i}$ and $C = aN \prod_{i=1}^{r} B_i$, the B_i's are monic irreducible distinct polynomials, $N \in \mathbb{F}_q[x]^*$ is monic, $\gcd(B, N) = 1$, *$a \in \mathbb{F}_q^*$ and* $m = \operatorname{Deg} C < 2(g+1) = 2\operatorname{Deg} B$. Recall that $S_x = \{\infty_1, \infty_2\}$ is the set of (degree one) places of K above the infinite place ∞ of k. We denote by ν_1 (resp. ν_2) the valuation at ∞_1 (resp. ∞_2), and by $\operatorname{val}_\wp(u)$ (resp. $\operatorname{ord}_\wp(u) = |\operatorname{val}_\wp(u)|$) the valuation (resp. the order) of any $u \in K^*$ at a place $\wp$ of K.

Remark 15. — In odd characteristic, an affine normal model of a real quadratic extension has a unique point at infinity, which is singular. Further in that case, the pole divisor of y is $\operatorname{div}_\infty(y) = (g+1)(\infty_1 + \infty_2)$. In characteristic 2, the situation is quite different. A normal affine model $\mathcal{C}$ has one or two points at infinity (see [**20**] for instance). If $g + 1 \leqslant m < 2(g+1)$ (thus $g \geqslant 2$), $\mathcal{C}$ has one singular point at infinity (the point $P_0 = (0:1:0)$ in homogeneous projective coordinates) and there are two places of degree one, ∞_1 and ∞_2, above P_0. If $m < g + 1$, $\mathcal{C}$ has two points at infinity: one is smooth, say ∞_1, and P_0 is singular if $g \geqslant 2$ and there is a unique place of degree one, say ∞_2, above P_0.

3.1. Principal divisors of K. — If $\alpha = u+vy \in K$, we recall that $\widetilde{\alpha} = u+(v+B)y$ and the norm of u is

$$N(\alpha) = \alpha\widetilde{\alpha} = u^2 + uvB + Cv^2.$$

Between the two places at infinity, we select a place, say ∞_2, such that $\nu_2(y) \leqslant \nu_1(y)$. In the next Lemma, we will see that this place is well defined. Since K/k is real, $1/x$ is a local parameter at ∞_i, $i = 1, 2$. We consider (see [**34**, p. 143]) the ∞_2-*adic completion of* K, denoted by $\widehat{K}_2$, and the embedding of K in $\widehat{K}_2$

$$\begin{aligned} K &\longrightarrow \widehat{K}_2 \\ \alpha &\longmapsto \sum_{i=-\infty}^{n} c_i x^i,\ c_i \in \mathbb{F}_q \text{ and } c_n \neq 0. \end{aligned}$$

Observe that $n = -\nu_2(\alpha)$ and, if $\alpha = P(x) \in \mathbb{F}_q[x]$, $n = \operatorname{Deg} P$. We denote by $\lfloor \alpha \rfloor$ the *polynomial part of the* ∞_2-*adic power series expansion of* α, *i.e.* $\lfloor \alpha \rfloor = \sum_{i=0}^{n} c_i x^i$ if $n \geqslant 0$, and $= 0$ otherwise.

Definition 16. — We say that $\alpha \in K$ is *reduced with respect to* ∞_2 if ∞_2 is a pole of α and a zero of $\widetilde{\alpha}$.

Further we will say "reduced" instead of "reduced with respect to ∞_2".

Lemma 17. — *Let K/k be a real quadratic extension with normal equation given by* (3).

(1) *Let $\mathfrak{b}_i$ be the unique place of K above the finite place (B_i) of k. Then*

$$\operatorname{div}(B(x)) = 2\sum_{i=1}^{r} n_i \mathfrak{b}_i - (g+1)(\infty_1 + \infty_2).$$

(2) *If* $\operatorname{Deg} N > 0$ *(otherwise $l = 0$), consider the factorization $N(x) = \prod_{j=1}^{l} N_j(x)^{l_j}$. Each finite place (N_j) of k splits in K and we denote by $\mathfrak{n}_j$ and $\widetilde{\mathfrak{n}}_j$ the places of K above (N_j). Then,*

$$\operatorname{div}(y) = \sum_{i=1}^{r} \mathfrak{b}_i + \sum_{j=1}^{l} l_j \mathfrak{n}_j + (g+1-m)\infty_1 - (g+1)\infty_2,$$

and

$$\operatorname{div}(\widetilde{y}) = \sum_{i=1}^{r} \mathfrak{b}_i + \sum_{j=1}^{l} l_j \widetilde{\mathfrak{n}}_j + (g+1-m)\infty_2 - (g+1)\infty_1.$$

(3) *The polynomial part of the ∞_2-adic power series expansion of y is monic and* $\operatorname{Deg}\lfloor y \rfloor = g+1 = \operatorname{Deg} B$. *If $1 \leqslant m < g+1$, $\lfloor y \rfloor = B$ and, if $g+1 \leqslant m < 2(g+1)$, $\lfloor y \rfloor \neq B$ but the coefficients of $x^{g+1}, \ldots, x^{m-g}$ in $\lfloor y \rfloor$ and B are equal.*

Proof. — (1) Recall that, for all $1 \leqslant i \leqslant r$, the finite place (B_i) of k is ramified in K. Let $\mathfrak{b}_i$ be the unique place of K above (B_i). Its degree is $\deg \mathfrak{b}_i = \operatorname{Deg} B_i$ and its conorm in the constant field extension $\overline{K}/\overline{\mathbb{F}_q}$ of $K/\mathbb{F}_q$ is

$$\mathrm{Conorm}_{\overline{K}/K}(\mathfrak{b}_i) = \sum_{B_i(a)=0} (a, 0),$$

thus $\mathfrak{b}_i$ is a zero for y. Since $\operatorname{Deg} B = g+1$, one has

$$\operatorname{div}(B(x)) = 2\sum_{i=1}^{r} n_i \mathfrak{b}_i - (g+1)(\infty_1 + \infty_2).$$

(2) Using $y\widetilde{y} = C(x)$, we see that the finite zeroes of y (resp. $\widetilde{y}$) are among the zeroes of $C(x)$ and the only possible poles for y (resp. $\widetilde{y}$) are the poles of x, *i.e.* ∞_1 and ∞_2.

(a) The place $\mathfrak{b}_i$ is a zero of y of order one and also a zero of $\widetilde{y} = y + B$ of order one, since B_i is a simple factor of C.

(b) If $N = \prod_{j=1}^{l} N_j^{l_j}$, with $l \geqslant 1$, the places (N_j) of k split in K. We denote by $\mathfrak{n}_j$ and $\widetilde{\mathfrak{n}}_j$ the two places above (N_j). Their respective degree equals $\operatorname{Deg} N_j$. Let $a \in \overline{\mathbb{F}_q}$ be a zero of N_j, then

$$\mathrm{Conorm}_{\overline{K}/K}(\mathfrak{n}_j) = \sum_{N_j(a)=0} (a, 0), \ \text{ and } \ \mathrm{Conorm}_{\overline{K}/K}(\widetilde{\mathfrak{n}}_j) = \sum_{N_j(a)=0} (a, B(a)).$$

Thus, $\mathfrak{n}_j$ is a zero of y and $\widetilde{\mathfrak{n}}_j$ is a zero of $y + B$. Since $y(y+B) = C$ and $\operatorname{Deg} C = m$, one obtains

$$\operatorname{div}(y) + \operatorname{div}(y+B) = \sum_{j=1}^{l} l_j(\mathfrak{n}_j + \widetilde{\mathfrak{n}}_j) + 2\sum_{i=1}^{r} \mathfrak{b}_i - m(\infty_1 + \infty_2). \tag{4}$$

Thus, $\mathfrak{n}_j$ is a zero of y of order l_j and $\widetilde{\mathfrak{n}}_j$ is a zero of $\widetilde{y}$ of order l_j. We have obtained all the finite zeroes of y and $\widetilde{y}$ and the degree of the finite zero divisor of y (resp. $\widetilde{y}$) is

$$\deg\left(\sum_{i=1}^{r} \mathfrak{b}_i + \sum_{j=1}^{l} l_j \mathfrak{n}_j\right) = \deg\left(\sum_{i=1}^{r} \mathfrak{b}_i + \sum_{j=1}^{l} l_j \widetilde{\mathfrak{n}}_j\right) = m.$$

(c) Observe that $[K : \mathbb{F}_q(y)] = \max\{m, g+1\} = \deg(\operatorname{div}_\infty(y)) = \deg(\operatorname{div}_0(y))$. We set $v = y/B(x)$ and consider equation (1). Then $\nu_j(v) < 0$, for $j = 1$ or 2, is impossible, since

$$\nu_j(v) + \nu_j(v+1) = \nu_j\left(\frac{N(x)}{\prod_{i=1}^{r} B_i(x)^{2n_i-1}}\right) = 2(g+1) - m > 0.$$

If $\nu_j(v) = 0$, then $\nu_j(v+1) = 2(g+1) - m$. If $\nu_j(v) > 0$, then $\nu_j(v+1) = 0$, thus $\nu_j(v) = 2(g+1) - m$. Since $\nu_j(y) = \nu_j(v) + \nu_j(B(x)) = \nu_j(v) - (g+1)$, this implies $\nu_j(y) = -(g+1)$ or $\nu_j(y) = (g+1) - m > -(g+1)$. If $g+1 \leqslant m < 2(g+1)$, one obtains $\deg(\operatorname{div}_\infty(y)) = m$, so $\nu_j(y) = -(g+1)$ and $\nu_{j'}(y) = (g+1) - m \leqslant 0$ for

$j' \neq j$. If $1 \leqslant m < g+1$, one obtains $\deg(\mathrm{div}_\infty(y)) = g+1$, so $\nu_j(y) = -(g+1)$ and $\nu_{j'}(y) = m-(g+1) > 0$ for $j' \neq j$. Thus $\nu_j(y) = -(g+1)$ for at least one j, say $j=2$. It can be shown that this is coherent with the notations in Remark 15. To conclude, we have obtained that

$$\mathrm{div}(y) = \sum_{i=1}^{r} \mathfrak{b}_i + \sum_{j=1}^{l} l_j \mathfrak{n}_j + (g+1-m)\infty_1 - (g+1)\infty_2,$$

and, using (4),

$$\mathrm{div}(\widetilde{y}) = \sum_{i=1}^{r} \mathfrak{b}_i + \sum_{j=1}^{l} l_j \widetilde{\mathfrak{n}} + (g+1-m)\infty_2 - (g+1)\infty_1.$$

(3) Set $d(x) = \lfloor y \rfloor \in k[x]$. Then, $\operatorname{Deg} d = -\nu_2(y) = g+1 = \operatorname{Deg} B$ and $\nu_2(y+B) = (g+1)-m$. If $1 \leqslant m < g+1$, we obtain that $\nu_2(y+B) > 0$, so $\lfloor y \rfloor = d(x) = B(x)$ and, since B is monic, d is monic too. If $g+1 \leqslant m < 2(g+1)$, we obtain that $\nu_2(y+B) \leqslant 0$. Thus $d+B \neq 0$ and $0 \leqslant \operatorname{Deg}(d+B) = m-(g+1) < g+1 = \operatorname{Deg} B$. So d is monic and the coefficients of $x^{g+1}, \ldots, x^{m-g}$ in d and B are equal. □

3.2. Quadratic irrationals. — We consider some particular elements in K, which are related to the representation of primitive ideals (see Section 2.3.2).

Definition 18. — We say that $\alpha \in K$ is a *quadratic irrational of* K, if $\alpha = (y+P)/Q$, with $(Q, P) \in k[x]^* \times k[x]$ and Q divides $N(y+P)$,

(5) $$N(y+P) = (y+P)(y+P+B) = P^2 + BP + C.$$

If $\alpha = (y+P)/Q$ is a quadratic irrational, α is reduced with respect to ∞_2, or for short, α is reduced if and only if

$$-\nu_2(y+P+B) < \operatorname{Deg} Q < -\nu_2(y+P).$$

Remark 19. — Let us show that, if $\alpha = (y+P)/Q$ is reduced, one has $\operatorname{Deg} P < g+1$ and $\operatorname{Deg} Q < g+1$ (compare with [**37**, p. 567]). Remember that B and $\lfloor y \rfloor$ are monic of degree $g+1 = -\nu_2(y)$ and thus $B + \lfloor y \rfloor = 0$ or $\operatorname{Deg}(B + \lfloor y \rfloor) < g+1$. If α is reduced, one has $\operatorname{Deg} Q < -\nu_2(y+P)$ thus $\lfloor y \rfloor + P \neq 0$. Then

(6) $$\alpha \text{ is reduced} \iff -\nu_2(y+P+B) < \operatorname{Deg} Q < \operatorname{Deg}(\lfloor y \rfloor + P).$$

(1) If $P \neq \lfloor y \rfloor + B$, α is reduced if and only if $\operatorname{Deg}(\lfloor y \rfloor + P + B) < \operatorname{Deg} Q < \operatorname{Deg}(P + \lfloor y \rfloor)$. One obtains $\operatorname{Deg} P < g+1$ and $\operatorname{Deg} Q < g+1$.

(2) If $P = \lfloor y \rfloor + B$, then $-\nu_2(y+P+B) < 0$, $\operatorname{Deg} P = \operatorname{Deg}(\lfloor y \rfloor + B) < g+1$ and α is reduced if and only if $\operatorname{Deg} Q < g+1$.

Lemma 20. — *y is a quadratic irrational which is reduced if and only if $\lfloor y \rfloor = B$, i.e. $1 \leqslant m < g+1$. Moreover, if y is reduced, all quadratic irrationals $\alpha = (y+P)/Q$ such that* $\operatorname{Deg} P < \operatorname{Deg} Q < g+1$ *are reduced.*

Proof. — For $\alpha = y$, we have $P = 0$, $Q = 1$ and Q divides $N(y) = y(y+B) = C$, thus y is a quadratic irrational. By Lemma 17, y is reduced if and only if $1 \leqslant m < g+1$ and if and only if $\lfloor y \rfloor = B$. Note that, if y is not reduced, then $y + \lfloor y \rfloor$ is reduced.

Using (6), we see that, if y is reduced, all quadratic irrationals $\alpha = (y+P)/Q$ such that $\operatorname{Deg} P < \operatorname{Deg} Q < g+1$ are reduced. □

We prove the following result, which is a generalization of the case $\alpha = y$ seen in Proposition 17. It is the equivalent result for characteristic 2 of results in [**2**] (see also [**28**, prop. 9] and [**3**]).

Proposition 21. — *Let $\alpha = (y+P)/Q$ be a quadratic irrational. Set $a_0 = \lfloor \alpha \rfloor$ and let $Q' \in \mathbb{F}_q[x]$ be such that*

$$QQ' = N(y+P) = (y+P)(y+P+B) = P^2 + BP + C. \tag{7}$$

(1) *Let I (resp. I') be the set of i, $1 \leqslant i \leqslant r$, such that B_i divides Q (resp. Q'). Then $I \cap I' = \varnothing$ and the factorizations of Q and Q' are*

$$Q(x) = \prod_{j\in J} U_j(x)^{n_j} \prod_{i \in I} B_i(x),\ Q'(x) = \prod_{j \in J'} U'_j(x)^{n'_j} \prod_{i\in I'} B_i(x),$$

where all places (U_j) (resp. (U'_j)), if any, are split. We denote by $\mathfrak{u}_j$ and $\widetilde{\mathfrak{u}}_j$ (resp. $\mathfrak{u}'_j$ and $\widetilde{\mathfrak{u}}'_j$) the two finite conjugated places above (U_j) (resp. (U'_j)).

(2) *We consider the following quasi-reduced divisors D and D' of respective degree* $\operatorname{Deg} Q$ *and* $\operatorname{Deg} Q'$

$$D = \sum_{i\in I} \mathfrak{b}_i + \sum_{i \in J} n_j \mathfrak{u}_j,\ D' = \sum_{i \in I'} \mathfrak{b}_i + \sum_{i\in J} n'_j \mathfrak{u}'_j.$$

The finite pole (resp. zero) divisors of α and $\widetilde{\alpha}$ are

$$\operatorname{div}_{\infty,f}(\alpha) = \widetilde{D}\ \operatorname{div}_{0,f}(\alpha) = \widetilde{D}'$$
$$\operatorname{div}_{\infty,f}(\widetilde{\alpha}) = D\ \operatorname{div}_{0,f}(\widetilde{\alpha}) = D'.$$

(3) *Assume moreover that α is reduced. Then*

(a) $\operatorname{Deg} a_0 = g + 1 - \operatorname{Deg} Q > 0$, $\operatorname{Deg} Q' < g+1$.

(b) $\nu_2(\alpha) = \nu_1(\widetilde{\alpha}) = \operatorname{Deg} Q - (g+1) = -\operatorname{Deg} a_0 < 0$ *and* $\nu_1(\alpha) = \nu_2(\widetilde{\alpha}) = g + 1 - \operatorname{Deg} Q' > 0$.

(c) *The principal divisors of α and $\widetilde{\alpha}$ are*

$$\operatorname{div}(\alpha) = \widetilde{D}' + (g+1-\operatorname{Deg} Q')\infty_1 - \widetilde{D} - (\operatorname{Deg} a_0)\infty_2,$$
$$\operatorname{div}(\widetilde{\alpha}) = D' + (g+1-\operatorname{Deg} Q')\infty_2 - D - (\operatorname{Deg} a_0)\infty_1.$$

The pole divisor (resp. zero divisor) of α and of $\widetilde{\alpha}$ are non-special divisors of degree $g+1$.

Proof. — (1) Assume B_i divides Q. Using (7) and the fact that B_i is a simple factor of C, we have that B_i is a simple factor of Q and it is not a factor of Q'. Let $I \subset \{1, \ldots, r\}$ (resp. I') be the set of i such that B_i divides Q (resp. Q'). Of course, the set I or I' may be empty. We have $I \cap I' = \varnothing$. Notice that, if B_i divides Q, B_i is also a factor of P and, since B_i is ramified, $\mathrm{val}_{\mathfrak{b}_i}(P) \geqslant 2$. Let $a \in \overline{k}$ be such that $Q(a) = 0$ and $B(a) \neq 0$. Then a is a zero of a U_j and there are exactly two places above the finite place $(x-a)$ of $\overline{k}(x)$, which are (a,b) and $\widetilde{(a,b)} = (a, b + B(a))$, $b = y(a) \in \overline{k}$ being such that $b^2 + bB(a) + C(a) = 0$. The places (a,b) and $\widetilde{(a,b)} = (a, b+B(a))$ are zeroes of Q of order n_j. Since Q divides $(P+y)(P+B+y)$, (a,b) or $\widetilde{(a,b)} = (a, b+B(a))$ is a zero of $P+y$, *i.e.* $b = P(a)$ or $b = P(a) + B(a)$. If (a,b) is a zero of $P+y$, then it is not a zero of $P+y+B$ and $\widetilde{(a,b)}$ is a zero of $P+B+y$ and not a zero of $P+y$. Thus there exists a finite place $\mathfrak{u}_j$ of K such that $\mathrm{Conorm}_{\overline{K}/K}(\mathfrak{u}_j) = \sum_{U_j(a)=0}(a, P(a))$ which is a zero of $P+y$ and not a zero of $P+y+B$, $\widetilde{\mathfrak{u}}_j$ is a zero of $P+y+B$ and not a zero of $P+y$. This proves also that (U_j) is split. Finally

$$\mathrm{div}(Q) = \sum_{j\in J} n_j(\mathfrak{u}_j + \widetilde{\mathfrak{u}}_j) + 2\sum_{i\in I}\mathfrak{b}_i - (\mathrm{Deg}\, Q)(\infty_1 + \infty_2).$$

Similarly, we can show that

$$\mathrm{div}(Q') = \sum_{j\in J'} n'_j(\mathfrak{u}'_j + \widetilde{\mathfrak{u}}'_j) + 2\sum_{i\in I'}\mathfrak{b}_i - (\mathrm{Deg}\, Q')(\infty_1 + \infty_2).$$

(2) The finite poles of $\alpha = (y+P)/Q$ (resp. $\widetilde{\alpha}$) are among the zeroes of Q.

(a) If $\mathfrak{b}_i$ is a zero of Q, we have seen that $\mathrm{val}_{\mathfrak{b}_i}(Q) = 2$, $\mathrm{val}_{\mathfrak{b}_i}(P) \geqslant 2$ and $\mathfrak{b}_i$ is a simple zero of y (see Lemma 17). So $\mathrm{val}_{\mathfrak{b}_i}(P+y) = 1$ and $\mathfrak{b}_i$ is a pole for α of order 1.

(b) If $\mathfrak{u}_j$ is a zero of Q, we have seen that it is a zero of $P+y$ and not a zero of $P+y+B$. Moreover, $0 < \mathrm{val}_{\mathfrak{u}_j}(Q) \leqslant \mathrm{val}_{\mathfrak{u}_j}(P+y)$ and $\mathfrak{u}_j$ is not a pole for α. But then $\widetilde{\mathfrak{u}}_j$ (resp. $\mathfrak{u}_j$) is a pole for α (resp. $\widetilde{\alpha}$) of order n_j.

Finally, $\mathrm{div}_{\infty,f}(\alpha) = \widetilde{D}$ and $\mathrm{div}_{\infty,f}(\widetilde{\alpha}) = D$. Considering the quadratic irrational $\alpha' = (y+P)/Q'$, we have a similar result, $\mathrm{div}_{\infty,f}(\alpha') = \widetilde{D}'$ and $\mathrm{div}_{\infty,f}(\widetilde{\alpha}') = D'$. But since by (7), $\alpha' = (y+P)/Q' = Q/(y+P+B) = 1/\widetilde{\alpha}$, we have $\mathrm{div}_{\infty,f}(\alpha') = \mathrm{div}_{0,f}(\widetilde{\alpha})$ and $\mathrm{div}_{\infty,f}(\widetilde{\alpha}') = \mathrm{div}_{0,f}(\alpha)$, so the result follows.

(3) If α is reduced, $\mathrm{Deg}\, P < g+1 = \mathrm{Deg}\lfloor y \rfloor$ and $\mathrm{Deg}\, Q < g+1$ by Remark 19.

(a) Thus, since $\mathrm{Deg}\lfloor y \rfloor = g+1 > \mathrm{Deg}\, P$, $a_0 = \lfloor (P+y)/Q \rfloor = \lfloor \lfloor y \rfloor / Q \rfloor$, $\mathrm{Deg}\, a_0 = (g+1) - \mathrm{Deg}\, Q > 0$ and, since $\mathrm{Deg}\, C < 2(g+1)$, $\mathrm{Deg}\, Q' < g+1$.

(b) Since $\alpha\widetilde{\alpha} = Q'/Q$, for all place $\wp$ of K,

$$\mathrm{val}_\wp(\alpha) + \mathrm{val}_\wp(\widetilde{\alpha}) = \mathrm{val}_\wp(Q') - \mathrm{val}_\wp(Q). \tag{8}$$

Since $\mathrm{Deg}\, P < \mathrm{Deg}\, B = g+1 = -\nu_2(y)$, one has $\nu_2(y+P) = -(g+1)$ and ∞_2 is a pole for α such that $\nu_2(\alpha) = \mathrm{Deg}\, Q - (g+1) = -\mathrm{Deg}\, a_0$. Similarly, $\nu_1(y+P+B) = -(g+1)$, thus ∞_1 is a pole for $\widetilde{\alpha}$ and $\nu_1(\widetilde{\alpha}) = \mathrm{Deg}\, Q - (g+1) = -\mathrm{Deg}\, a_0$. Using (8), we obtain $\nu_1(\alpha) = g+1-\mathrm{Deg}\, Q' > 0$ and $\nu_2(\widetilde{\alpha}) = g+1-\mathrm{Deg}\, Q' > 0$.

(c) The pole (resp. zero) divisors of α and $\widetilde{\alpha}$ are reduced of degree $g+1$ and by Proposition 13 these divisors are non-special. □

From the proof of the preceding Proposition, we can deduced the following trivial observation.

Lemma 22. — *Let $Q \in \mathbb{F}_q[x]$ be monic and irreducible. Then the following assertions are equivalent:*

(1) *There exists $P \in \mathbb{F}_q[x]$ such that Q divides $N(y+P)$.*
(2) *The equation $T^2+BT+C=0 \bmod Q$ has at least one solution in $\mathbb{F}_q[x]$.*
(3) *either $Q|B$ and then the place (Q) of k ramifies in K (and $P=0$)*
or $\gcd(Q,B)=1$ *and then the place (Q) of k splits in K (this is the case for instance if $Q|C$).*

No finite place (Q) of k, which is inert in K, is such that $Q|N(y+P)$ for some $P \in \mathbb{F}_q[x]$.

3.3. Reduced integral ideals. — As said before, an integral ideal is of the following form $\mathfrak{A}=(S)[Q,y+P]$, where $S,Q,P \in \mathbb{F}_q[x]$ and Q divides $N(y+P)=P^2+BP+C$. Without loss of generality, it can be assumed that Q, S are monic and $\operatorname{Deg} P < \operatorname{Deg} Q$ and then the representation of $\mathfrak{A}$ is unique.

Lemma 23. — *Let $\mathfrak{A}=[Q,y+P]$ be a primitive ideal of $\mathcal{O}_x$. Then $\mathfrak{A}$ is quasi-reduced. Moreover, $\mathfrak{A}$ is reduced if and only if* $\deg Q \leqslant g$.

Proof. — (see also [**37**, Th. 12]). First notice that an integral ideal can be quasi-reduced only if it is primitive. Let $\mathfrak{A}=\prod_{i\in\mathcal{I}}\wp_i^{e_i}$ be the factorization of a primitive ideal $\mathfrak{A}=[Q,y+P]$. Then, each $\wp_i$ is a common zero of Q and $y+P$. None of the $\wp_i$'s are equal to ∞_j, $j=1$ or 2, and none of them are inert (*cf.* Lemma 22). Moreover, if $Q(x)=\prod_{j\in J}U_j(x)^{n_j}\prod_{i\in I}B_i(x)$, then (using the notations of the proof of Proposition 21)

$$\mathfrak{A}=\prod_{j\in J}\mathfrak{u}_j^{n_j}\prod_{i\in I}\mathfrak{b}_i,$$

and $\mathfrak{A}$ is quasi-reduced. The polynomial norm of $\mathfrak{A}$ is $\mathcal{N}\mathfrak{A}=Q$ and $\deg\mathfrak{A}=\operatorname{Deg} Q$. Thus $\mathfrak{A}$ is reduced if and only if $\operatorname{Deg} Q \leqslant g$. □

Without loss of generality, it can be assumed that any reduced ideal is such that $\mathfrak{A}=[Q,y+P]$, with $Q|P^2+BP+C$, $\operatorname{Deg} P < \operatorname{Deg} Q < \operatorname{Deg} B$ and Q is monic. Notice that, if $\alpha=(P+y)/Q$ is a reduced quadratic irrational, then $\mathfrak{A}=[Q,y+P]$ is reduced. But, conversely, if $\mathfrak{A}=[Q,y+P]$ is a reduced ideal, with $Q|P^2+BP+C$, $\operatorname{Deg} P < \operatorname{Deg} Q < \operatorname{Deg} B$ and Q is monic, then $\alpha=(P+y)/Q$ is not always reduced. But, according to Remark 19, if y is reduced, then $\alpha=(P+y)/Q$ is reduced.

3.4. Fundamental unit ε and regulator r_x. — The unit group of $\mathcal{O}_x$ is $\mathcal{O}_x^* = \mathbb{F}_q^* \times \langle\varepsilon\rangle$, where ε is a *fundamental unit.* Then the regulator of K/k is $r_x = |\nu_1(\varepsilon)| = |\nu_2(\varepsilon)|$ and

$$\operatorname{div}(\varepsilon) = r_x(\infty_1 - \infty_2).$$

Our purpose is now to compute the ideal class number h_x of $\mathcal{O}_x$. For that, we can apply Schmidt's formula $h = h_x r_x$, compute the divisor class number using for instance the zeta function ($h = L(1)$, where $L(t)$ is the numerator polynomial of the zeta function) and compute the regulator. This last task can be achieved using the continued fraction expansion of y.

3.5. Continued fraction expansion (CFE) in characteristic 2. — For any p, the results concerning the continued fraction expansion algorithm are very similar to the number field case. There are plenty of references for the odd characteristic case. For the case $p = 2$, we refer to [**37**] (see also [**24**]). In this section, we recall basic results.

3.5.1. Definitions

Definition 24. — Let $\alpha_0 = (y + P_0)/Q_0 \in K$ be a quadratic irrational and set $a_0 = \lfloor\alpha_0\rfloor$. For $i \geqslant 1$, define the *i-th iterate* α_i recursively by

$$a_{i-1} = \lfloor\alpha_{i-1}\rfloor,\ \alpha_i = \frac{1}{\alpha_{i-1} + a_{i-1}}.$$

The CFE of α_0 is the sequence $[a_0;\, a_1,\, a_2,\, \ldots]$. For $i \geqslant 1$, we consider the functions $\widetilde{\theta}_i$ defined by

$$\widetilde{\theta}_1 = 1,\quad \text{and for } i \geqslant 1,\ \widetilde{\theta}_{i+1} = \prod_{j=1}^{i} \frac{1}{\widetilde{\alpha}_j}.$$

If $\alpha = (y + P)/Q$ is a quadratic irrational, we will say "the CFE of α" or "the CFE of $\mathfrak{A} = [Q, y + P]$". The CFE is finite if and only if $\alpha_0 = (y + P_0)/Q_0 \in \mathbb{F}_q[x]$. If $\alpha_0 \in K \smallsetminus \mathbb{F}_q[x]$, the CFE is quasi–periodic and periodic, the *period* τ (resp. the *quasi-period* ρ) is the least integer n such that $\alpha_n = \alpha_{n_0}$ (resp. $\alpha_n = c\alpha_{n_0}$, $c \in \mathbb{F}_q^*$), with $0 \leqslant n_0 < n$. The CFE of α_0 is obtained as follows. For all $i \geqslant 0$,

$$\alpha_i = \frac{P_i + y}{Q_i},$$

where the P_i's and Q_i's are defined recursively as follows:

$$P_{i+1} = a_i Q_i + P_i + B,\ Q_{i+1}Q_i = P_{i+1}^2 + BP_{i+1} + C.$$

Another way to compute the P_i's and Q_i's is the following. Set $Q_{-1} = (P^2 + BP + C)/Q$ and $d = \lfloor y\rfloor$, then, for all $i \geqslant 0$, compute recursively $a_i,\ P_{i+1},\ Q_{i+1}$ using the following formulae

$$\begin{aligned} a_i &= \left\lfloor \frac{P_i + d}{Q_i} \right\rfloor \\ r_i &= P_i + d \pmod{Q_i} \\ P_{i+1} &= d + r_i + B \\ Q_{i+1} &= Q_{i-1} + a_i(r_i + r_{i-1}). \end{aligned}$$

Notice that

$$Q_{i+1}Q_i = P_{i+1}^2 + BP_{i+1} + C = N(P_{i+1} + y) = (P_{i+1} + y)(P_{i+1} + B + y). \tag{9}$$

Remark 25. — If α_i is reduced, then α_j is reduced for all $j \geqslant i$. Moreover, there exists $i \geqslant 0$ such that α_i is reduced (see [**37**, Th. 1]). If $\alpha_0 = y$ is not reduced, then α_i is reduced for all $i \geqslant 1$ and then all α_i's, for $i \geqslant 1$, are reduced. In fact, if y is not reduced, then $\lfloor y \rfloor + B \neq 0$. The first data of the CFE of y are : $P_0 = 0$ and $Q_0 = 1$, $r_0 = 0$, $Q_{-1} = C$, $a_0 = d = \lfloor y \rfloor$, $P_1 = d + B$, $Q_1 = d(d + B) + C$ and $\alpha_1 = (y + P_1)/Q_1$. Since $Q_1 = P_1^2 + P_1 B + C = (y + d)(y + d + B)$ and $\nu_2(y + d) > 0$, we have

$$\nu_2(Q_1) = -\operatorname{Deg}(Q_1) = \nu_2(y + d) + \nu_2(y + d + B) > -\operatorname{Deg}(B) = g + 1$$

thus $\operatorname{Deg}(Q_1) < g + 1$. The result follows from Remark 19.

If α_i is reduced, then $\operatorname{Deg} P_i$ and $\operatorname{Deg} Q_i$ are $< g + 1$, thus

$$a_i = \left\lfloor \frac{P_i + d}{Q_i} \right\rfloor = \left\lfloor \frac{d}{Q_i} \right\rfloor, \; 1 \leqslant \operatorname{Deg} a_i = g + 1 - \operatorname{Deg} Q_i \leqslant g + 1. \tag{10}$$

Using (9), one obtains $N(\widetilde{\alpha}_i) = \alpha_i \, \widetilde{\alpha}_i = Q_{i-1}/Q_i$ and $1/\widetilde{\alpha}_i = (P_i + y)/Q_{i-1}$. Then $N(\widetilde{\theta}_{i+1}) = Q_i/Q_0$ and

$$\widetilde{\theta}_{i+1} = \frac{1}{\widetilde{\alpha}_i} \, \widetilde{\theta}_i = \frac{P_i + y}{Q_{i-1}} \, \widetilde{\theta}_i, \quad \text{for all } i \geqslant 1. \tag{11}$$

Notice that, for $i \geqslant 2$, $\widetilde{\theta}_{i+1} = a_{i-1}\widetilde{\theta}_i + \widetilde{\theta}_{i-1}$ and the $\widetilde{\theta}_i$ can be computed recursively.

Lemma 26. — *Consider the CFE of a primitive ideal* $\mathfrak{A}_1 = [Q_0, y + P_0]$ *and set*

$$\mathfrak{A}_i = [Q_{i-1}, y + P_{i-1}], \quad \textit{for all } i \geqslant 1.$$

All the $\mathfrak{A}_i$ *are equivalent to* $\mathfrak{A}_1$. *Conversely, if* $\mathfrak{A}$ *and* $\mathfrak{B}$ *are equivalent reduced ideals, then in the CFE of* $\mathfrak{A}$, *there exists* n *such that* $\mathfrak{B} = \mathfrak{A}_n$. *In particular, in the CFE of* y *we have for all* $i \geqslant 1$,

$$\mathfrak{A}_i = (\widetilde{\theta}_i)\mathcal{O}_x$$

and we obtain all the principal reduced ideals of $\mathcal{O}_x$.

Proof. — see [**37**, th. 13 and 17]. Notice that is easy to show, using (9), that for all $i \geqslant 1$, $(Q_i)\mathfrak{A}_i = (P_i + y + B)\mathfrak{A}_{i+1}$. Thus all the $\mathfrak{A}_i$'s are equivalent to $\mathfrak{A}_1$ and $(Q_0 \, \theta_i)\mathfrak{A}_i = (Q_i)\mathfrak{A}_1$. For $\mathfrak{A}_1 = \mathcal{O}_x = [1, y]$, $\mathfrak{A}_i$ is reduced for all $i \geqslant 2$ and, using (11), one obtains $\mathfrak{A}_i = (\widetilde{\theta}_i)\mathcal{O}_x$. □

3.5.2. The CFE of y. — The CFE of y has a lot of nice properties (*cf.* [**37**]). We have seen that it produces all the principal reduced ideals of $\mathcal{O}_x$. Now we want to show that the regulator of the extension can be computed from this CFE. First, we have the following result, which is an analogous result in characteristic 2 of [**3**, Lemma 3] (*cf.* also [**28**]). The proof is very similar to the odd characteristic case.

Proposition 27. — *We consider the CFE of a reduced quadratic irrational $\alpha_0 = (P_0+y)/Q_0$. For $i \geqslant 1$, the divisors of the α_i's are*

$$\begin{aligned}
\operatorname{div}(\alpha_1) &= \widetilde{D}_0 + (\operatorname{Deg} a_0)\infty_1 - \widetilde{D}_1 - (\operatorname{Deg} a_1)\infty_2\\
\operatorname{div}(\alpha_2) &= \widetilde{D}_1 + (\operatorname{Deg} a_1)\infty_1 - \widetilde{D}_2 - (\operatorname{Deg} a_2)\infty_2\\
&\ \vdots\\
\operatorname{div}(\alpha_i) &= \widetilde{D}_{i-1} + (\operatorname{Deg} a_{i-1})\infty_1 - \widetilde{D}_i - (\operatorname{Deg} a_i)\infty_2\\
\operatorname{div}(\alpha_{i+1}) &= \widetilde{D}_i + (\operatorname{Deg} a_i)\infty_1 - \widetilde{D}_{i+1} - (\operatorname{Deg} a_{i+1})\infty_2,\\
&\ \vdots
\end{aligned}$$

where, for all $i \geqslant 0$, the divisors $\widetilde{D}_i$ are reduced and such that $\deg \widetilde{D}_i = \operatorname{Deg} Q_i$.

Proof. — For all $i \geqslant 0$, one has

$$\alpha_i = a_i + \frac{1}{\alpha_{i+1}}.$$

Then the finite zeroes of α_{i+1} are the finite poles of α_i. The result follows from Proposition 21 and (10). Since $\alpha_{i+1}\widetilde{\alpha}_{i+1} = Q_i/Q_{i+1}$, we deduce that, for $i \geqslant 0$,

$$\operatorname{div}\left(\frac{1}{\widetilde{\alpha}_{i+1}}\right) = D_{i+1} + (\operatorname{Deg} a_{i+1})\infty_1 - D_i - (\operatorname{Deg} a_i)\infty_2. \tag{12}$$

Proposition 21 gives the values of the D_i's. □

Corollary 28. — *Consider the CFE of a reduced quadratic irrational $\alpha_0 = (P_0+y)/Q_0$. Set*

$$R_0 = 0,\ R_i = \sum_{j=1}^{i} \operatorname{Deg}(a_j), \quad \textit{for all } i \geqslant 1.$$

Then $\operatorname{div}(\widetilde{\theta}_1) = 0$ *and, for all $i \geqslant 1$,*

$$\operatorname{div}(\widetilde{\theta}_{i+1}) = D_i + R_i\infty_1 - D_0 - (R_{i-1} + \operatorname{Deg} a_0)\infty_2, \tag{13}$$

where D_i is the finite zero divisor of $\widetilde{\alpha}_i$. In particular, D_i is reduced of degree $g+1-$ $\operatorname{Deg} a_i$. *Considering the CFE of $\alpha_0 = y$, one has, for all $i \geqslant 1$,*

$$\operatorname{div}(\widetilde{\theta}_{i+1}) = D_i + R_i\infty_1 - (R_{i-1} + g + 1)\infty_2. \tag{14}$$

Proof. — To prove (13), use (12), the definition of $\widetilde{\theta}_{i+1}$ and Proposition 27. If $\alpha_0 = y$, we have proved that α_i is reduced at least for $i \geqslant 1$. Thus we can apply (13) with $D_0 = 0$ (since $Q_0 = 1$). Notice that, if y is reduced, then $d = a_0 = B$, $\widetilde{\theta}_2 = y$, $R_1 = g+1-m > 0$, and $\operatorname{div}(\widetilde{\theta}_2) = \operatorname{div}(y) = D_1 + R_1\infty_1 - (g+1)\infty_2$. The value of D_1 is given in Lemma 17. □

We obtain an analogous result in characteristic 2 of [**3**, Th. 2].

Proposition 29. — *We assume that y is reduced and consider the CFE of y.*

(1) *For all i, $\ell((R_i+g+1)\infty_2) - \ell((R_{i-1}+g+1)\infty_2) = \operatorname{Deg} a_i$.*

(2) *Let R be an integer. Then $\ell(R\infty_2) = 1$ if $0 \leqslant R < g+1$ and $\ell(R\infty_2) = R-g+1$ if $R \geqslant g+1$. Assume $R \geqslant g+1$ and let $j \geqslant 2$ be such that $R_{j-2} \leqslant R-(g+1) < R_{j-1}$. A k-basis of $\mathcal{L}(R\infty_2)$ is composed of the following functions*

- *$\widetilde{\theta}_i$, for $1 \leqslant i \leqslant j$,*
- *for $2 \leqslant i \leqslant j$ and if $\operatorname{Deg} a_{i-1} > 1$, $x^\gamma \widetilde{\theta}_i$, with $1 \leqslant \gamma \leqslant \operatorname{Deg} a_{i-1} - 1$,*
- *if $R_{j-2} < R-(g+1)$, $x^\gamma \widetilde{\theta}_j$, with $1 \leqslant \gamma \leqslant R-(g+1)-R_{j-2}$.*

Proof

(1) According to Proposition 13, all divisors $N\infty_2$ are non-special if $N \geqslant g$. Thus, for all $i \geqslant 1$,

$$\ell((R_i+g+1)\infty_2) - \ell((R_{i-1}+g+1)\infty_2) = R_i - R_{i-1} = \operatorname{Deg} a_i.$$

(2) By (14), we have that $\widetilde{\theta}_i \in \mathcal{L}((R_{i-2}+g+1)\infty_2)$ for all $i \geqslant 2$.

(a) Since y is reduced, $\widetilde{\theta}_2 = y$ and $y \in \mathcal{L}((g+1)\infty_2)$. Moreover $(g+1)\infty_2$ is non-special, so $\ell((g+1)\infty_2) = 2$ and $(1, y)$ is a k-basis for $\mathcal{L}((g+1)\infty_2)$. Of course 1 is a basis of $\mathcal{L}(R\infty_2)$ for all R, $0 \leqslant R < R_1 = g+1$.

(b) If $R \geqslant g+1$, then $\ell(R\infty_2) = R-g+1$. Let j be such that $R_{j-2} \leqslant R-(g+1) < R_{j-1}$. This condition means that

$$\mathcal{L}((R_{j-2}+g+1)\infty_2) \subset \mathcal{L}(R\infty_2) \subsetneq \mathcal{L}((R_{j-1}+g+1)\infty_2).$$

For $1 \leqslant i \leqslant j$, one has $\widetilde{\theta}_i \in \mathcal{L}(R\infty_2)$. Then, we proceed recursively, using that for any $i \geqslant 2$ and $\gamma > 0$

$$\operatorname{div}(x^\gamma \widetilde{\theta}_i) = \gamma \operatorname{div}_0(x) + D_{i-1} + (R_{i-1}-\gamma)\infty_1 - (R_{i-2}+(g+1)+\gamma)\infty_2.$$

– Set

$$n = \ell(R\infty_2) - \ell((R_{j-2}+g+1)\infty_2) = R-(g+1)-R_{j-2}.$$

If $n = 0$, a basis of $\mathcal{L}(R\infty_2)$ is a basis of $\mathcal{L}((R_{j-2}+g+1)\infty_2)$ and if $n > 0$, we obtain a basis of $\mathcal{L}(R\infty_2)$ adding to a basis of $\mathcal{L}((R_{j-2}+g+1)\infty_2)$ the functions $x^\gamma \widetilde{\theta}_j$ for $1 \leqslant \gamma \leqslant n$.

– Assume $j \geqslant 3$. Then, for all i such that $2 \leqslant i \leqslant (j-1)$ and $\operatorname{Deg}(a_{i-1}) > 1$, all the functions $x^\gamma \widetilde{\theta}_i$, for $1 \leqslant \gamma \leqslant \operatorname{Deg} a_{i-1} - 1$, are in $\mathcal{L}((R_{j-2}+g+1)\infty_2)$ thus in $\mathcal{L}(R\infty_2)$.

We have found N functions in $\mathcal{L}(R\infty_2)$,

$$N = j + \sum_{i=2}^{j-1} (\operatorname{Deg} a_{i-1} - 1) + (R-(g+1)-R_{j-2}) = R-g+1 = \ell(R\infty_2),$$

having pairwise distinct valuations at ∞_2, so the result follows. It is easy to see that the preceding functions have also pairwise distinct valuations at ∞_1. □

Proposition 30. — *In the CFE of y, let ρ be the least integer such that $Q_i \in \mathbb{F}_q^*$, then ρ is the quasi-period and* $\operatorname{div}(\widetilde{\theta}_{\rho+1}) = R_\rho(\infty_1 - \infty_2)$. *Moreover $\widetilde{\theta}_{\rho+1}$ is a fundamental unit and R_ρ is the regulator.*

Proof. — Equation (14) can be written

$$\operatorname{div}(\widetilde{\theta}_{i+1}) = D_i - (\operatorname{Deg} D_i)\infty_2 + R_i(\infty_1 - \infty_2).$$

Recall that D_i is a reduced divisor of degree $g+1-\operatorname{Deg} a_i$ and that $R_i = R_{i-1}+\operatorname{Deg} a_i$. Thus the principal divisor of $\widetilde{\theta}_{i+1}$ shows the equivalence between the two zero-degree divisors $D_i - (\operatorname{Deg} D_i)\infty_2$ and $R_i(\infty_2 - \infty_1)$ and more generally,

$$D_i - (\operatorname{Deg} D_i)\infty_2 + n(\infty_1 - \infty_2) \sim (R_i - n)(\infty_2 - \infty_1),$$
$$\text{for all } 0 \leqslant n \leqslant g - \operatorname{Deg} D_i = \operatorname{Deg} a_i + 1,$$

so $R_{i-1} + 1 \leqslant R_i - n \leqslant R_i$. It is easy to show that, if ρ is the least integer such that $Q_i \in \mathbb{F}_q^*$, then for $1 \leqslant i \leqslant \rho$, all D_i's are pairwise distinct. Using Corollary 11, we obtain the result. □

4. Ideal class number one problem and examples

Now we want to study the ideal class number problem in characteristic 2 for real quadratic extensions and genus $g \geqslant 1$. According to Proposition 14, a normal equation of K/k must be given by:

$$y^2 + b^n y + aNb = 0, \tag{15}$$

with $b \in \mathbb{F}_{2^e}[x]$ monic irreducible of degree β, $\gcd(N, b) = 1$, $\operatorname{Deg} N < (2n-1)\beta$.

Lemma 31. — *Let K/k be defined by* (15) *with $n \geqslant 2$. Consider the CFE of y.*

(1) *There exists $k \geqslant 1$ such that $\mathcal{A}_{k+1} = [b, y]$.*
(2) *Set $R_k = \nu_1(\widetilde{\theta}_{k+1})$. The regulator is $r_x = 2(R_k + \operatorname{Deg} b)$.*

Proof. — The condition $n \geqslant 2$ tells us that $\beta < g + 1 = n\beta$. The finite place (b) is the only ramified place and we denote by $\mathfrak{b}$ the place above it. Since b divides the norm of y, $\mathcal{B} = [b, y]$ is a primitive ideal. It is reduced because $\operatorname{Deg} \mathcal{B} = \beta \leqslant g$ and ambiguous. Moreover, $\mathcal{B}^2$ is a principal ideal:

$$[b, y]^2 = [b^2, by, y^2] = (b)[b, y, b^{n-1}y + aN] = (b)[1, y]$$

(use $\gcd(b, N) = 1$) and thus $\mathcal{B}$ is principal, since the ideal class number is odd. Applying Lemma 26, there exists $k \leqslant \rho - 1$ such that $\mathcal{A}_{k+1} = [b, y] = (\widetilde{\theta}_{k+1})\mathcal{O}_x$ and by (14)

$$\operatorname{div}(\widetilde{\theta}_{k+1}) = D_k + R_k\infty_1 - (R_{k-1} + g + 1)\infty_2 = D_k + R_k\infty_1 - (R_k - \operatorname{Deg} a_k + g + 1)\infty_2,$$

where $\deg D_k = g+1-\operatorname{Deg} a_k = \beta$, since $a_k = \lfloor d/b \rfloor = b^{n-1}$. In fact $D_k = \mathfrak{b}$ (see Corollary 28). We obtain that

$$\operatorname{div}\left(\frac{\widetilde{\theta}_{k+1}^2}{b}\right) = 2(R_k+\beta)(\infty_1 - \infty_2),$$

thus $r_x | 2(R_k+\beta)$. Using the formulae giving the data P_i and Q_i of a CFE, one sees that $P_{k+1} = P_{k-1}$. Then it can be shown that the quasi-period ρ is even and that $\varepsilon = \widetilde{\theta}_{\rho+1} = \widetilde{\theta}_{k+1}^2/b$, thus $r_x = 2(R_k+\beta)$ (see [**37**, Th. 7, 8]). We could say more about the regulator but we do not want to pursue here. □

4.1. Case $N=1$. — First, we compute the regulator of a real quadratic extension $K = \mathbb{F}_{2^e}(x,y)/\mathbb{F}_{2^e}(x)$ having a normal equation (3) with $N=1$.

Proposition 32. — *Let $q = 2^e$ and let K/k be the real quadratic extension with normal equation* (3)*, with*

$$B(x) = \prod_{i=1}^r B_i(x)^{n_i}, \quad C(x) = a\prod_{i=1}^r B_i(x), \quad a \in \mathbb{F}_q^*.$$

Then the regulator is $r_x = \sum_{i=1}^r (2n_i - 1)\operatorname{Deg} B_i$.

Proof. — Notice that $m = \sum_{i=1}^r \operatorname{Deg} B_i < 2(g+1) = \sum_{i=1}^r 2n_i \operatorname{Deg} B_i$.

– If $m \geqslant g+1$, obviously $m = g+1$, $n_i = 1$ for all $1 \leqslant i \leqslant r$ and $aB(x) = C(x)$. y is not reduced and its polynomial part is (see Lemma 17) $d = \lfloor y \rfloor = \sum_{j=0}^{g+1} c_j x^j = B + a$. Then

$$\begin{array}{l|l|l|l|l}
 & Q_{-1} = C = aB & & & \\
\mathcal{A}_1 = [1,y] & Q_0 = 1 & P_0 = 0 & a_0 = B + a & r_0 = 0 \\
\mathcal{A}_2 = [a^2, y+a] & Q_1 = a^2 & P_1 = a & a_1 = \frac{1}{a^2}B &
\end{array}$$

The regulator is $r_x = \deg a_1 = g+1$ and the fundamental unit is $\varepsilon = \widetilde{\theta}_2 = y + a$.

– If $1 \leqslant m < g+1$, y is reduced and its polynomial part is $d = B$. The CFE of y is

$$\begin{array}{l|l|l|l|l}
 & Q_{-1} = C & & & \\
\mathcal{A}_1 = [1,y] & Q_0 = 1 & P_0 = 0 & a_0 = B & r_0 = 0 \\
\mathcal{A}_2 = [C,y] & Q_1 = C & P_1 = 0 & a_1 = \frac{1}{a}\prod_{r=1}^t B_r(x)^{n_r - 1} & r_1 = 0 \\
\mathcal{A}_3 = [1,y] & Q_2 = 1 & P_2 = 0 & a_2 = B &
\end{array}$$

The period and quasi-period equal 2 and the regulator is $r_x = \deg a_1 + \deg a_2 = 2(g+1) - m$. Moreover, the fundamental unit is $\varepsilon = \widetilde{\theta}_3 = \frac{1}{a}y + 1$. □

In the case where $N=1$, we see that the regulator grows slower with the genus than the divisor class number. Thus, there are only a finite number of real extensions such that $h_x = 1$. To be more precise, we will use the following Lemma.

Lemma 33. — *Let $K/\mathbb{F}_q$ be a function field of genus $g \geqslant 2$. Denote by A_i the number of effective divisors of degree i and by π_i the reciprocal roots of $L(t)$, where $L(t)$ is the numerator polynomial of the zeta function of $K/\mathbb{F}_q$. Then*

$$\sum_{i=0}^{g-2} A_i + \sum_{i=0}^{g-1} q^{g-1-i} A_i = h \sum_{i=1}^{g} \frac{1}{|1-\pi_i|^2} \leqslant h \frac{(g+1)(q+1)-A_1}{(q-1)^2}. \tag{16}$$

In particular, we have the following lower bounds for the divisor class number h

$$h \geqslant \frac{q^{g-1}(q-1)^2}{(g+1)(q+1)-A_1} \tag{17}$$

$$h \geqslant \frac{(q-1)^2(q^{g-1}+1)+A_1(q-1)(q^{g-1}-1)}{(g+1)(q+1)-A_1}. \tag{18}$$

Proof (*cf.* [**18**, Th. 1 and Th. 2]). — Notice that $A_0 = 1$, A_1 is the number of degree one places and $A_i \geqslant A_1$ for all $i > 0$. Moreover $(g+1)(q+1) - A_1 > 0$ by the Hasse-Weil bound. Set $\Sigma_K = \sum_{i=0}^{g-2} A_i + \sum_{i=0}^{g-1} q^{g-1-i} A_i$. The first lower bound is obtained from

$$\Sigma_K \geqslant q^{g-1}.$$

In case $g = 1$, one has $h = A_1$, but the bound (17) is also true.
The second lower bound follows from

$$\Sigma_K \geqslant 1 + q^{g-1} + A_1 \sum_{i=1}^{g-1} q^{g-1-i} = 1 + q^{g-1} + A_1 \frac{q^{g-1}-1}{q-1}. \qquad \square$$

Lemma 34. — *Let $K = \mathbb{F}_{2^e}(x,y)$, with $y^2 + b^n y + ab = 0$, $a \in (\mathbb{F}_{2^e})^*$, $b \in \mathbb{F}_{2^e}[x]$ monic irreducible of degree β and $g+1 = n\beta \geqslant 2$. The ideal class number is equal to one if and only if*

– *$n = 1$ and all finite places of k of degree $\leqslant g$ are inert in K,*
– *$n > 1$ and all finite places of k of degree $\leqslant g$ are inert in K, except (b) which is ramified.*

Proof. — Lemma 26 tells us that all reduced principal ideals are obtain in the CFE of y. In the proof of Proposition 32, we have seen that no non-zero reduced ideals are principal if $n = 1$ and if $n > 1$ the only one is $[b, y]$. Then using Corollary 11 we obtain the result. $\square$

Theorem 35. — *Let $q = 2^e$, $K = \mathbb{F}_q(x,y)$, with $y^2 + b^n y + ab = 0$, $a \in (\mathbb{F}_q)^*$, $b \in \mathbb{F}_q[x]$ monic irreducible of degree β and $g+1 = n\beta \geqslant 2$. The regulator is equal to $r_x = (2n-1)\beta$. The only real quadratic extensions $K/\mathbb{F}_q(x)$ such that $h_x = 1$ are (up to* *isomorphism* $x \mapsto x + c$, $c \in \mathbb{F}_q$*)*

q	g	*normal equation*	$r_x = h$
2	1	$y^2 + x^2y + x = 0$	3
	1	$y^2 + (x^2 + x + 1)y + (x^2 + x + 1) = 0$	2
	2	$y^2 + x^3y + x = 0$	5
	2	$y^2 + (x^3 + x + 1)y + (x^3 + x + 1) = 0$	3
	3	$y^2 + x^4y + x = 0$	7
	3	$y^2 + (x^2 + x + 1)^2y + (x^2 + x + 1) = 0$	6
	3	$y^2 + (x^4 + x^3 + 1)y + (x^4 + x^3 + 1) = 0$	4
4	1	$y^2 + x^2y + ax = 0$, $a \neq 0, 1$	3
	1	$y^2 + (x^2 + x + a)y + (x^2 + x + a) = 0$, $a \neq 0, 1$	2
	1	$y^2 + (x^2 + a^2x + 1)y + a(x^2 + a^2x + 1) = 0$, $a \neq 0, 1$	2

Proof. — By Proposition 32, $r_x = 2(g + 1) - \beta = (2n - 1)\beta$, since $g + 1 = n\beta$. We denote by m_i the number of places of $K/\mathbb{F}_q$ of degree i (thus $A_1 = m_1$). Assume $h_x = 1$ or, which is equivalent, $h = r_x$. By the preceding Lemma, all the finite places (Q) of k, except (b) if $n > 1$, of degree $\leqslant g$ are inert in K, thus $m_1 = 2$ if $\beta > 1$ (resp. $m_1 = 3$ if $\beta = 1$, since (b) is ramified). Using (17) and (18), we have $h > r_x$ and thus $h_x \neq 1$ if

$$q^{g-1}(q - 1)^2 - (qg + q + g + 1 - m_1)(2g + 2 - d) > 0. \tag{19}$$

or, in case $g \geqslant 2$, if

$$(q-1)^2(q^{g-1}+1)+m_1(q-1)(q^{g-1}-1)-(qg+q+g+1-m_1)(2g+2-d) > 0. \tag{20}$$

We obtain that $h_x \neq 1$ in the following cases (remember that β is a divisor of $g + 1$)

(1) $q \geqslant 8$,
(2) $q = 4$ and $g \geqslant 2$,
(3) $q = 2$, $g = 7$ and $\beta = 8$ or $g \geqslant 8$.

For $q = 4$, $g = 1$ and $\beta = 1$ or 2, we find four solutions, where a is a generator of $\mathbb{F}_4$,

$$\begin{aligned}
&y^2 + x^2y + ax = 0\\
&y^2 + (x^2 + x + a)y + (x^2 + x + a) = 0\\
&y^2 + (x^2 + a^2x + 1)y + a(x^2 + a^2x + 1) = 0\\
&y^2 + (x^2 + a^2x + a^2)y + a(x^2 + a^2x + a^2) = 0
\end{aligned}$$

and the last two are isomorphic. We are left with the cases $g \leqslant 7$ and $q = 2$. It is possible to eliminate many other cases since one can compute h using Lemma 34. Then, we obtain the solutions using the *Magma Computational Algebra System* [**23**]. Notice that, if $q = 2$ and $K/\mathbb{F}_q(x)$ has the following normal equation $y^2 + x^ny = x$, its divisor class number can be computed. In fact, setting $u = 1/x$ and $v = y/x^n$, we obtain a new equation for K: $v^2 + v = u^{2n-1}$. The extension $K/\mathbb{F}_q(u)$ is ramified. Now in [**17**] or [**5**], the divisor class number h of K is computed using Jacobi sums. □

4.2. Case $N = x$. — We studied several families of real quadratic extensions of $k = \mathbb{F}_2(x)$ and give examples below. Most of the computations have been made using MAGMA. We did not try to write an optimized program and use only the magma functions giving the regulator and divisor class number.

Example 36. — $K = \mathbb{F}_2(x, y)$, $y^2 + (x+1)^n y + x(x+1) = 0$, $n \geqslant 2$, $g = n - 1$.

n	r_x	h_x	n	r_x	h_x	n	r_x	h_x
2	5	1	13	2959	3	24	42876735	1
3	15	1	14	2677	13	25	55901823	1
4	27	1	15	19917	5	26	101905709	1
5	65	1	16	495	147	27	334830407	1
6	139	1	17	1025	205	28	81854593	5
7	273	1	18	599805	1	29	785928983	1
8	119	3	19	1040817	1	30	2391795091	1
9	255	5	20	1256061	1	31	2935590243	1
10	1165	1	21	8471363	1	32	2015	3787245
11	315	9	22	6761103	1	33	4095	7186725
12	13315	1	23	9575379	1	34	20384932205	1

Example 37. — $K = \mathbb{F}_2(x, y)$, $y^2 + (x^2 + x + 1)^n y + x(x^2 + x + 1) = 0$.

n	g	r_x	h_x	n	g	r_x	h_x
1	1	4	1	9	17	345070	1
2	3	22	1	10	19	1195202	1
3	5	98	1	11	21	5472974	1
4	7	278	1	12	23	16281926	1
5	9	1030	1	13	25	81072778	1
6	11	5662	1	14	27	371552998	1
7	13	24866	1	15	29	876838458	1
8	15	69598	1	16	31	1210377186	5

Example 38. — $K = \mathbb{F}_2(x,y)$, $y^2 + (x^3+x^2+1)^n y + x(x^3+x^2+1) = 0$.

n	g	r_x	h_x	n	g	r_x	h_x
1	2	9	1	7	20	24866	1
2	5	63	1	8	23	18991601	1
3	8	1001	1	9	26	185173607	1
4	11	6809	1	10	29	1399623165	1
5	14	31579	1	11	32	3269773683	3
6	17	399509	1	12	35	32383683053	3

5. Conclusion

It is of course hopeless to prove the Gauss conjecture for function fields in that way, even if it seems that there are plenty of real quadratic extensions such that the ideal class number equals 1. Concerning the distribution of the ideal class number and analogous to Cohen-Lenstra heuristics, there are many results for the function fields case in odd characteristic, for instance see [**10**], [**12**], [**11**], [**13**], [**32**]. For $p=2$, we want to give the following computational result.

Theorem 39. — *We denote by $\mathcal{B}_\beta$ the set of monic irreducible polynomials of degree $\beta \geqslant 2$ in $\mathbb{F}_2[x]$ and set $n_\beta = \operatorname{card} \mathcal{B}_\beta$. We consider the real quadratic extensions $K_B/\mathbb{F}_2(x)$ defined by $K_B = \mathbb{F}_2(x,y)$, where $y^2 + By + xB = 0$ with $B \in \mathcal{B}_\beta$. Consider the ratio*

$$\Delta_\beta = \frac{\operatorname{card}\{K_B/\mathbb{F}_2(x),\ B \in \mathcal{B}_\beta,\ \textit{such that } h_x \neq 1\}}{n_\beta}.$$

Then $\Delta_\beta < .25$ for $2 \leqslant \beta \leqslant 16$.

β	Δ_β
$2, \cdots, 6$	$= 0$
7	$< .0556$
8	$= .1$
9	$< .1965$
10	$< .2021$
11	$< .2044$
12	$< .2478$
13	$< .2429$
14	$< .2335$
15	$< .2498$
16	$< .2437$

References

[1] E. Artin – Quadratische Körper im Gebiete der höheren Kongruenzen, I and II, *Math. Z.* **19** (1924), p. 153–246.

[2] T.G. Berry – On periodicity of continued fractions in hyperelliptic function fields, *Arch. Math. (Basel)* **55** (1990), no. 3, p. 259–266.

[3] ______, Continued fractions in hyperelliptic function fields, in *Coding theory, cryptography and related areas (Guanajuato, 1998)*, Springer, Berlin, 2000, p. 29–41.

[4] U. Bhosle – Pencils of quadrics and hyperelliptic curves in characteristic two, *J. reine angew. Math.* **407** (1990), p. 75–98.

[5] J. Buhler & N. Koblitz – Lattice basis reduction, Jacobi sums and hyperelliptic cryptosystems, *Bull. Austral. Math. Soc.* **58** (1998), no. 1, p. 147–154.

[6] D.G. Cantor – Computing in the Jacobian of a hyperelliptic curve, *Math. Comp.* **48** (1987), no. 177, p. 95–101.

[7] S. Chowla – On the class numbers of some function fields $y^2 = f(x)$ over $GF(p)$, I and II, *Norske Vid. Selsk. Forh. (Trondheim)* **39** (1966), p. 86–88, and **40** (1967), p. 7–10.

[8] A. Enge – How to distinguish hyperelliptic curves in even characteristic?, in *Public-key cryptography and computational number theory (Warsaw, 2000)*, de Gruyter, Berlin, 2001, p. 49–58.

[9] Feng Keqin & Hu Weiqun – On real quadratic function fields of Chowla type with ideal class number one, *Proc. Amer. Math. Soc.* **127** (1999), no. 5, p. 1301–1307.

[10] E. Friedman & L.C. Washington – On the distribution of divisor class groups of curves over a finite field, in *Théorie des nombres (Quebec, PQ, 1987)*, de Gruyter, Berlin, 1989, p. 227–239.

[11] C. Friesen – Class group frequencies of real quadratic function fields: the degree 4 case, *Math. Comp.* **69** (2000), no. 231, p. 1213–1228.

[12] ______, Bounds for frequencies of class groups of real quadratic genus 1 function fields, *Acta Arith.* **96** (2001), no. 4, p. 313–331.

[13] C. Friesen & P. van Wamelen – Class numbers of real quadratic function fields, *Acta Arith.* **LXXXI** (1997), no. 1, p. 45–55.

[14] H. Hasse – Theorie der relativ-zyklischen algebraischen Funktionenkörpern, insbesondere bei endlichem Konstantenkörpern, *J. reine angew. Math.* **172** (1935), p. 37–64.

[15] Humio Ichimura – Class numbers of real quadratic function fields of genus one, *FFA* **3** (1997), p. 181–185.

[16] N. Koblitz – Hyperelliptic cryptosystems, *J. Cryptology* **1** (1989), no. 3, p. 139–150.

[17] ______, Jacobi sums and cryptography, *Canad. Math. Bull.* **34** (1991), p. 229–235.

[18] G. Lachaud & M. Martin-Deschamps – Nombre de points des jacobiennes sur un corps fini, *Acta Arith.* **56** (1990), no. 4, p. 329–340.

[19] G. Lachaud & S. Vlăduţ – Gauss problem for function fields, *J. Number Theory* **85** (2000), no. 2, p. 109–129.

[20] D. Le Brigand – Quadratic algebraic function fields with ideal class number two, in *Arithmetic, Geometry and Coding Theory*, de Gruyter, Berlin, 1996, p. 105–126.

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

[22] M.L. Madan – Note on a problem of S. Chowla, *J. Number Theory* **2** (1970), p. 279–281.

[23] `http://magma.maths.usyd.edu.au/magma/`.

[24] M. Mkaouar – Sur le développement en fraction continue des séries formelles quadratiques sur $\mathbb{F}_2(X)$, *J. Number Theory* **80** (2000), p. 169–173.

[25] V. Müller, A. Stein & C. Thiel – Computing discrete logarithms in real quadratic congruence function fields of large genus, *Math. Comp.* **68** (1999), no. 226, p. 807–822.

[26] V. Müller, S. Vanstone & R. Zuccherato – Discrete Logarithm Based Cryptosystems in Quadratic Function Fields of Characteristic 2, *Designs codes and Cryptography* **14** (1998), no. 2, p. 159–178.

[27] S. Paulus & H.-G. Rück – Real and imaginary representations of hyperelliptic function fields, *Math. Comp.* **68** (1999), no. 227, p. 1233–1242.

[28] R. Paysant-LeRoux – Périodicité des fractions continues dans un corps de fonctions hyperelliptiques, *Arch. Math. (Basel)* **61** (1993), no. 1, p. 46–58.

[29] F.K. Schmidt – Analytische Zahlentheorie in Körpern der Charakteristik p, *Math. Z.* **33** (1931), p. 1–32.

[30] T.A. Schmidt – Infinitely many real quadratic fields of class-number one, *J. Number Theory* **54** (1995), p. 203–205.

[31] S. Sémirat – Genus theory for quadratic function fields and applications, preprint Université Paris VI, 1998.

[32] A. Stein & E. Teske – Explicit bounds and heuristics on class numbers in hyperelliptic function fields, *Math. Comp.* **71** (2002), no. 238, p. 837–861, electronic.

[33] A. Stein & H.C. Williams – Some methods for evaluating the regulator of a real quadratic function field, *Experiment. Math.* **8** (1999), no. 2, p. 119–133.

[34] H. Stichtenoth – *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993.

[35] R.C. Valentini & M.L. Madan – A Hauptsatz of L.E. Dickson and Artin-Schreier extensions, *J. reine angew. Math.* **318** (1980), p. 156–177.

[36] X.-K. Zhang – Ambiguous classes and 2-rank of class group of quadratic function fields, *J. China Univ. Sci. Tech.* **17** (1987), p. 425–431.

[37] R.J. Zuccherato – The continued fraction algorithm and regulator for quadratic function fields of characteristic 2, *J. Algebra* **190** (1997), p. 563–587.

D. Le Brigand, Institut de Mathématiques de Jussieu, Équipe Analyse Algébrique, Université Pierre et Marie Curie - Paris VI, Case 82, 4 place Jussieu, 75252 Paris Cedex 05
E-mail : dominique.lebrigand@math.jussieu.fr