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.

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