MATHEMATICS OF COMPUTATION
Volume 68, Number 227, Pages 1233–1241
S 0025-5718(99)01066-2
Article electronically published on February 15, 1999

REAL AND IMAGINARY QUADRATIC REPRESENTATIONS OF HYPERELLIPTIC FUNCTION FIELDS

SACHAR PAULUS AND HANS-GEORG RÜCK

ABSTRACT. A hyperelliptic function field can be always be represented as a real quadratic extension of the rational function field. If at least one of the rational prime divisors is rational over the field of constants, then it also can be represented as an imaginary quadratic extension of the rational function field. The arithmetic in the divisor class group can be realized in the second case by Cantor's algorithm. We show that in the first case one can compute in the divisor class group of the function field using reduced ideals and distances of ideals in the orders involved. Furthermore, we show how the two representations are connected and compare the computational complexity.

1. INTRODUCTION

Let k be a field (not necessarily finite) whose characteristic is different from 2. We consider a hyperelliptic function field K over k of genus g, i.e. a quadratic extension of the rational function field over k of one variable. Then K can be generated over the rational function field by the square root of a polynomial of degree $2g+1$ or $2g+2$.

We distinguish two cases. In the first case we assume $K = k(x)(\sqrt{F(x)})$, where $F(x) \in k[x]$ is a separable polynomial of degree $2g+1$. This can only be achieved if at least one of the ramified prime divisors in $K/k(x)$ is rational over k. One calls K then an imaginary quadratic function field. The second case is $K = K(t)(\sqrt{D(t)})$, where $D(t) \in k[t]$ is a monic, separable polynomial of degree $2g+2$. This occurs if a prime divisor in $k(t)$ splits into two extensions in K. Then K is called a real quadratic function field. We neglect here the case that the leading coefficient of the polynomial $D(t)$ is not a square in k^*. A constant field extension of degree 2 over k leads to our second case.

We want to express in both cases the arithmetic in the (degree 0) divisor class group of K in terms of reduced ideals in the corresponding orders $k[x][\sqrt{F(x)}]$, resp. $k[t][\sqrt{D(t)}]$. The imaginary quadratic case is well known [2, 4, 6]. We list it here for sake of completeness and because we want to compare it to the second case. If K is a real quadratic function field, we show that the reduced ideals plus some natural numbers represent uniquely the elements of the divisor class group of K. These extra natural numbers are closely related to the distance between two

Received by the editor July 24, 1997 and, in revised form, November 3, 1997 and January 20, 1998.

1991 *Mathematics Subject Classification.* Primary 11R58, 14Q05; Secondary 11R65, 14H05, 14H40.

Key words and phrases. Hyperelliptic curves, divisor class groups, real quadratic model.

ideals [9]. This representation allows an efficient realization of the addition in the divisor class group even if no ramified prime is rational over k. We emphasize that always the divisor class group of the function field and not the ideal class group of the orders involved is at the center of our interest.

The common object in both cases is the function field K. It is independent of the generating polynomials and orders involved. Any imaginary quadratic function field can be viewed as a real quadratic function field. The converse is only true if at least one ramified prime is rational over k. We explain this correspondence in abstract algorithmic terms. From this one can deduce explicit formulae which were found for fields of genus 1 in an ad hoc construction [1, 9].

2. The function field K

Let K be a function field over k of genus g. We denote by $Div_0(K)$ the group of divisors of degree 0. The group of principal divisors $P(K) = \{(f) \mid f \in K^*\}$ is a subgroup of $Div_0(K)$ and the factor group $Cl_0(K) = Div_0(K)/P(K)$ is called the divisor class group (of degree 0) of K. We denote by $[D] \in Cl_0(K)$ the class of $D \in Div_0(K)$. For details in the theory of function fields we refer to [10].

We fix an effective divisor D_∞ of degree g. If $D \in Div_0(K)$ is any divisor, the Riemann-Roch theorem yields that $\dim(D + D_\infty) \geq 1$, i.e. there is a function $f \in K^*$ and an effective divisor D_0 of degree g such that $(f) = D_0 - (D_\infty + D)$. Hence any divisor class $[D] \in Cl_0(K)$ has a representative of the form $[D] = [D_0 - D_\infty]$, where D_0 is an effective divisor of degree g. It remains a problem to determine such a representative uniquely. This will be done in the next two sections, depending on special generators of K.

3. K as an imaginary quadratic function field

Let $F(x) \in k[x]$ be a separable polynomial of degree $2g + 1$. Then $K = k(x)(\sqrt{F(x)})$ is a function field over k of genus g. The pole divisor ∞ of x in $k(x)$ is ramified under the extension to K; let P_∞ be its extension in K. We fix the divisor $D_\infty := gP_\infty$ (cf. Section 2) and represent each element of $Cl_0(K)$ in the form $[D_0 - gP_\infty]$. If B is a divisor in K which is the conorm of a divisor of $k(x)$, then $\deg(B)$ is even and $B - \deg(B)P_\infty$ is a principal divisor. Therefore one can get rid of conorms in D_0. Furthermore one cancels contributions of P_∞ in D_0. One gets the well known result [2, 4, 6]:

Proposition 3.1. *Each divisor class $[D] \in Cl_0(K)$ has a unique representation of the form $[D] = [A - \deg(A)P_\infty]$, where A is an effective divisor of K with $\deg(A) \leq g$ which is divisible neither by P_∞ nor by the conorm of a divisor of $k(x)$.*

Above we showed the existence of such a divisor A. The uniqueness follows from the fact that a function in K, whose pole divisor equals sP_∞ with $0 \leq s \leq 2g$, is an element of $k(x)$ (cf. the proof of the corresponding result in Section 4).

Now we consider the Dedekind domain $O_K^{(x)} = k[x][\sqrt{F(x)}]$ which is the integral closure of $k[x]$ in K. Any ideal $\mathfrak{a} \subset O_K^{(x)}$ can be given in the form

$$\mathfrak{a} = T(x)(U(x)k[x] + (V(x) + \sqrt{F(x)})k[x])$$

with $T(x), U(x), V(x) \in k[x]$, where $U(x)$ divides $F(x) - V(x)^2$. If $\deg V(x) < \deg U(x)$ and if the leading coefficients of $U(x)$ and $T(x)$ are 1, then this representation by $(T(x), U(x), V(x))$ is unique. The degree of $\mathfrak{a}$ satisfies $\deg(\mathfrak{a}) = \deg(U(x)T(x)^2)$.

Each prime ideal in $O_K^{(x)}$ defines a valuation on K. Therefore one can associate with it a prime divisor of K. This gives an isomorphism from the group of ideals of $O_K^{(x)}$ onto the group of divisors of K which are prime to P_∞ (and induces an isomorphism between the ideal class group of $O_K^{(x)}$ and $Cl_0(K)$). Hence we can associate to each divisor A of Proposition 3.1 an ideal $\mathfrak{a} \subset O_K^{(x)}$ with $\deg(\mathfrak{a}) = \deg(A) \leq g$ which is not divisible by an ideal of the form $T(x)O_K^{(x)}$ with $T(x) \in k[x]$.

An ideal $\mathfrak{a}$ which corresponds to a divisor A of Proposition 3.1 is called a *reduced ideal*. It has a unique reduced basis $(U(x), V(x))$ where the leading coefficient of $U(x)$ is 1, $\deg V(x) < \deg U(x) \leq g$ and $U(x)$ divides $F(x) - V(x)^2$.

Now we formulate Proposition 3.1 in terms of ideals and get

Theorem 3.2. *There is a canonical bijection between the divisor class group $Cl_0(K)$ and the set of reduced ideals in $O_K^{(x)}$. This bijection induces the following group law $\mathfrak{a} * \mathfrak{b} = \mathfrak{c}$ on the set of reduced ideals: multiply the ideals $\mathfrak{a}$ and $\mathfrak{b}$ and let $\mathfrak{c}$ be the unique reduced ideal in the ideal class of $\mathfrak{ab}$.*

One can make Theorem 3.2 explicit by working with the reduced bases of the ideals $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{c}$. This gives the so-called Cantor algorithm [4], which for $g = 1$ yields nothing else but the well known addition formulas for elliptic curves.

4. K as a real quadratic function field

Let $D(t) \in k[t]$ be a monic, separable polynomial of degree $2g + 2$. Then $K = k(t)(\sqrt{D(t)})$ is a function field over k of genus g. The pole divisor ∞ of t in $k(t)$ decomposes into two different prime divisors P_1 and P_2 of K. Let ν_1 and ν_2 be the corresponding normalized valuations of K.

We choose and fix the divisor $D_\infty := gP_2$ (cf. Section 2) and represent each element of $Cl_0(K)$ in the form $[D_0 - gP_2]$. If B is a divisor in K which is the conorm of a divisor of $k(t)$, then $\deg(B)$ is even and $B - (\deg(B)/2)(P_1 + P_2)$ is a principal divisor. With this remark we can cancel conorms in D_0, and we get

$$[D_0 - gP_2] = [A + nP_1 - mP_2],$$

where A is an effective divisor in K which is not divisible by a conorm, by P_1 or by P_2. Since A is effective, n and m are integers with $0 \leq \deg(A) + n = m \leq g$. We change this slightly to

$$[A + nP_1 - mP_2] = [A - (m - n)P_2] + n[P_1 - P_2].$$

Proposition 4.1. *Each divisor class $[D] \in Cl_0(K)$ has a unique representation of the form $[D] = [A - \deg(A)P_2] + n[P_1 - P_2]$, where A is an effective divisor of K with $\deg(A) \leq g$ which is divisible neither by P_1 or P_2 nor by the conorm of a divisor of $k(t)$, and where n is an integer with $0 \leq n \leq g - \deg(A)$.*

Proof. We already saw the existence of a pair (A, n) with the demanded properties. Now we show that this representation is unique. We start with an identity

$$[A_1 - \deg(A_1)P_2] + n_1[P_1 - P_2] = [A_2 - \deg(A_2)P_2] + n_2[P_1 - P_2],$$

where (A_1, n_1) and (A_1, n_2) satisfy the properties of the proposition. From this we see that

$$A_1 + \bar{A}_2 - (n_2 + \deg(A_2) - n_1)P_1 - (n_1 + \deg(A_1) - n_2)P_2 = (f)$$

is a principal divisor in K. (Here $^-$ denotes the involution of $K/k(t)$.) Since f has only poles at P_1 or P_2, it is of the form $f = h(t) + g(t)\sqrt{D(t)}$ with polynomials $h(t), g(t) \in k[t]$. We get

$$\nu_1(f) = -(n_2 + \deg(A_2)) + n_1 \geq -g,$$

and analogously

$$\nu_1(\bar{f}) = \nu_2(f) \geq -g.$$

This gives

$$-g \leq \nu_1(f - \bar{f}) = \nu_1(2g(t)\sqrt{D(t)}),$$

which induces $-g \leq -(g+1) + \nu_1(g(t))$ if $g(t) \neq 0$. So obviously $g(t) = 0$ and $f = h(t) \in k(t)$. Then $A_1 + \bar{A}_2$ is a conorm. Since A_1 and A_2 do not contain any conorm by assumption, we get $A_1 = A_2$. Moreover, we must have

$$n_2 + \deg(A_2) - n_1 = n_1 + \deg(A_1) - n_2,$$

which shows that $n_1 = n_2$. □

Now we proceed as in Section 3. We consider the ring $O_K^{(t)}k[t][\sqrt{D(t)}]$, which is the integral closure of $k[t]$ in K. Any ideal $\mathfrak{a} \subset O_K^{(t)}$ can be given in the form

$$\mathfrak{a} = S(t)(Q(t)k[t] + (\tilde{P}(t) + \sqrt{D(t)})k[t])$$

with $S(t), Q(t), \tilde{P}(t) \in k[t]$, where $Q(t)$ divides $D(t) - \tilde{P}(t)^2$. If $\deg \tilde{P}(t) < \deg Q(t)$ and if the leading coefficients of $Q(t)$ and $S(t)$ are 1, then this representation is unique. The degree of $\mathfrak{a}$ satisfies $\deg(\mathfrak{a}) = \deg(Q(t)S(t)^2)$. If $S(t) = 1$, we call $\mathfrak{a}$ a *primitive ideal*. Again we get a canonical isomorphism from the group of ideals of $O_K^{(t)}$ onto the group of divisors of K which are prime to P_1 and P_2.

An ideal $\mathfrak{a} \subset O_K^{(t)}$ which corresponds to a divisor A with the properties of Proposition 4.1 is called a *reduced ideal*. It is an ideal $\mathfrak{a}$ with $\deg(\mathfrak{a}) \leq g$ which is not divisible by an ideal of the form $S(t)O_K^{(t)}$ with $S(t) \in k[t]$, and it is therefore uniquely represented by the pair $(Q(t), \tilde{P}(t))$.

We want to formulate Proposition 4.1 in terms of reduced ideals as in Section 3. We add two divisor classes given as in Proposition 4.1 and represent the sum again in the form

$$\begin{aligned}[A_1 - \deg(A_1)P_2] + n_1[P_1 - P_2] + [A_2 - \deg(A_2)P_2] + n_2[P_1 - P_2] \\ = [A_3 - \deg(A_3)P_2] + n_3[P_1 - P_2].\end{aligned}$$

It follows that

$$A_1 + A_2 - A_3 + (n_1 + n_2 - n_3)P_1 + mP_2 = (f)$$

is a principal divisor in K. This yields, for the corresponding reduced ideals $\mathfrak{a}_i$,

$$\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3^{-1} = fO_K^{(t)}$$

and $\nu_1(f) = n_1 + n_2 - n_3$.

We now give a link to the infrastructure as defined in [7, 9]. We consider the following ideal in $\mathbb{Z}$:

$$\{m \in \mathbb{Z} \mid m(P_1 - P_2) \text{ is a principal divisor}\} = R\mathbb{Z},$$

where the generator R with $R \geq 0$ is called the *regulator* of $O_K^{(t)}$. It is not difficult to see (cf. the end of the proof of Proposition 4.1) that either $R = 0$ or $R \geq g + 1$. If $\mathfrak{a}\mathfrak{b}^{-1} = fO_K^{(t)}$, we define the *distance* between $\mathfrak{a}$ and $\mathfrak{b}$ as

$$d(\mathfrak{b}, \mathfrak{a}) := \nu_1(f) \bmod R\mathbb{Z}.$$

We want to compute with small representatives of the residue class $d(\mathfrak{b}, \mathfrak{a})$; therefore we define for $\lambda \in \mathbb{R}$

$$d(\mathfrak{b}, \mathfrak{a}, \lambda) := \max\{n \in d(\mathfrak{b}, \mathfrak{a}) \mid n \leq \lambda\}.$$

With this notation we see that $\mathfrak{a}_1\mathfrak{a}_2$ and $\mathfrak{a}_3$ are in the same ideal class of $O_K^{(t)}$ with $d(\mathfrak{a}_3, \mathfrak{a}_1\mathfrak{a}_2, n_1+n_2) = n_1+n_2-n_3$. In the next theorem we will see how the distance determines $\mathfrak{a}_3$ and n_3 uniquely.

Theorem 4.2. *There is a canonical bijection between the divisor class group $Cl_0(K)$ and the set of pairs $\{(\mathfrak{a}, n)\}$, where $\mathfrak{a}$ is a reduced ideal of $O_K^{(t)}$ and n is an integer with $0 \leq \deg(\mathfrak{a}) + n \leq g$. This bijection induces the following group law $(\mathfrak{a}_1, n_1) * (\mathfrak{a}_2, n_2) = (\mathfrak{a}_3, n_3)$ on the set of these pairs: multiply the ideals $\mathfrak{a}_1$ and $\mathfrak{a}_2$, find in the ideal class of $\mathfrak{a}_1\mathfrak{a}_2$ a reduced ideal $\mathfrak{a}_3$ such that $d(\mathfrak{a}_3, \mathfrak{a}_1\mathfrak{a}_2, n_1 + n_2)$ is maximal, and define $n_3 = n_1 + n_2 - d(\mathfrak{a}_3, \mathfrak{a}_1\mathfrak{a}_2, n_1 + n_2)$.*

Proof. The bijection follows immediately from Proposition 4.1 and the remarks preceding this theorem. We have to show that the group law is indeed given by this rule.

Let A_3 and n_3 be the representatives of the sum given in Proposition 4.1. They satisfy in particular $\deg(A_3) + n_3 \leq g$. Suppose that the rule in the theorem gives a reduced ideal $\tilde{\mathfrak{a}}_3$ and an integer $\tilde{n}_3$. Note that the maximality condition implies $\tilde{n}_3 \leq n_3$. Let $\tilde{A}_3$ be the corresponding divisor.

We compare the equation of the definition of A_3 and n_3

$$A_1 + A_2 - A_3 + (n_1 + n_2 - n_3)P_1 + mP_2 = (f)$$

with the one coming from the rule in the theorem

$$A_1 + A_2 - \tilde{A}_3 + (n_1 + n_2 - \tilde{n}_3)P_1 + \tilde{m}P_2 = (\tilde{f}),$$

and we evaluate that

$$A_3 + \tilde{\tilde{A}}_3 + (-\tilde{n}_3 + n_3 - \deg(\tilde{A}_3))P_1 + (-n_3 + \tilde{n}_3 - \deg(A_3))P_2 = (h)$$

is a principal divisor with

$$\nu_1(h) = -\deg(\tilde{A}_3) + (n_3 - \tilde{n}_3) \geq -g$$

and

$$\nu_2(h) = -(\deg(A_3) + n_3) + \tilde{n}_3 \geq -g.$$

Analogous calculations as in the proof of Proposition 4.1 show that $h \in k(t)$. This only occurs if $\tilde{A}_3 = A_3$ and $\tilde{n}_3 = n_3$. □

We remark that we did not use the ideal class group of $O_K^{(t)}$ to represent the divisor class group. Here two different reduced ideals in the same ideal class group determine different elements in $Cl_0(K)$.

In [7] and [9] the authors considered only a special subset of $Cl_0(K)$, namely the set $\{(\mathfrak{a},0)\}$, where $\mathfrak{a}$ are reduced ideals in $O_K^{(t)}$. This so-called "infrastructure" describes only a part of $Cl_0(K)$ which is not a subgroup. Theorem 4.2 shows how to extend this theory to recover all of $Cl_0(K)$ for any genus.

We show now how the group law can be computed in practice (cf. [7]). First, modify the basis of a reduced ideal $\mathfrak{a}$ by changing $\tilde{P}(t)$ modulo a multiple of $Q(t)$ to $P(t)$ such that

$$-\nu_1(P(t)-\sqrt{D(t)}) < -\nu_1(Q(t)) = \deg Q(t) < -\nu_1(P(t)+\sqrt{D(t)}).$$

One calls the (unique) pair $(Q(t),P(t))$ with these properties the *reduced basis* of $\mathfrak{a}$.

We explain the *ideal multiplication*. Let $\mathfrak{a}_1$ and $\mathfrak{a}_2$ be two primitive ideals given by bases $(Q_1(t),P_1(t))$ and $(Q_2(t),P_2(t))$ respectively. We compute

$$\begin{aligned} S_3(t) &= \gcd(Q_1(t),Q_2(t),P_1(t)+P_2(t)) \quad \text{and} \quad A(t),B(t),C(t) \\ &\quad \text{such that} \quad S_3(t) = A(t)Q_1(t)+B(t)Q_2(t)+C(t)(P_1(t)+P_2(t)), \\ Q_3(t) &= Q_1(t)Q_2(t)/S_3(t)^2, \\ P_3(t) &= P_1(t)+\frac{Q_1(t)}{S_3(t)}\left(A(t)(P_2(t)-P_1(t))+C(t)\frac{D(t)-P_1(t)^2}{Q_1(t)}\right) \bmod Q_3(t). \end{aligned}$$

Then $(S_3(t),Q_3(t),P_3(t))$ is a basis of $\mathfrak{a}_1\mathfrak{a}_2$.

We explain the *ideal reduction*. The ideal reduction procedure is closely related to the computation of continued fractions. Let $\mathfrak{a}_0$ be a primitive ideal given by a basis $(Q_0(t),P_0(t))$. Compute for $i\in\mathbb{N}$

$$\begin{aligned} P_i(t) &= \lfloor\sqrt{D(t)}\rfloor - \left((P_{i-1}(t)+\lfloor\sqrt{D(t)}\rfloor) \bmod Q_{i-1}(t)\right), \\ Q_i(t) &= \left(D(t)-P_i(t)^2\right)/Q_{i-1}(t), \end{aligned}$$

where $\lfloor\sqrt{D(t)}\rfloor$ denotes the "polynomial part" of the expansion of $\sqrt{D(t)}$ in the completion $K_{P_1}k((t^{-1}))$. Then $(Q_i(t),P_i(t))$ is a basis of a primitive ideal $\mathfrak{a}_i$ equivalent to $\mathfrak{a}_{i-1}$. We write $\mathfrak{a}_i=\mathrm{red}(\mathfrak{a}_{i-1})$. There is $l\in\mathbb{N}$ with

$$l \le \max\{0, 1/2\deg\mathfrak{a}_0 - (g+1)/2 + 1$$

such that $\mathfrak{a}_l$ is reduced. In this case $(Q_{l+1}(t),P_{l+1}(t))$ is the reduced basis of $\mathfrak{a}_{l+1}$.

Denote $f_{\mathfrak{a}_i}=f_i=(P_i(t)-\sqrt{D(t)})/Q_i(t)$ for $i>0$. We have $f_i\mathfrak{a}_i=\mathfrak{a}_{i-1}$ and $\nu_1(f_i)>0$ iff $\mathfrak{a}_{i-1}$ is reduced.

Given a reduced ideal $\mathfrak{a}$, there is a unique reduced ideal $\mathfrak{b}$ such that $\mathrm{red}(\mathfrak{b})=\mathfrak{a}$. The formulas for computing the reduced basis of $\mathfrak{b}$ from the reduced basis of $\mathfrak{a}$ are easily deduced from the formulas above. We write $\mathrm{red}^{-1}(\mathfrak{a})$ for $\mathfrak{b}$. For every reduced ideal $\mathfrak{b}$ equivalent to a given reduced ideal $\mathfrak{a}$ there is $i\in\mathbb{Z}$ such that $\mathfrak{b}=\mathrm{red}^i(\mathfrak{a})$. If $R=0$ this number is unique.

Let $\mathfrak{b}=\mathrm{red}^i(\mathfrak{a})$ for $i\in\mathbb{Z}$. We define the *distance covered by reduction* to be $\mathfrak{d}(\mathfrak{b},\mathfrak{a}) := \sum_{j=1}^{i}\nu_1(f_{\mathrm{red}^j(\mathfrak{a})})$ if $i\ge 0$ and $\mathfrak{d}(\mathfrak{b},\mathfrak{a}) := \sum_{j=i+1}^{0}-\nu_1(f_{\mathrm{red}^j(\mathfrak{a})})$ if $i<0$. We clearly have $\mathfrak{d}(\mathfrak{b},\mathfrak{a})\in d(\mathfrak{b},\mathfrak{a})$.

Let $\mathfrak{a}_0$ be a primitive ideal given by $(Q_0(t), P_0(t))$. Let $l_0 > 0$ be minimal such that $\mathrm{red}^{l_0}(\mathfrak{a})$ is reduced. Then

$$-\deg Q_0(t) \leq \mathfrak{d}(\mathrm{red}^{l_0}(\mathfrak{a}_0), \mathfrak{a}_0) \leq 0.$$

Let $(\mathfrak{a}_1, n_1)$ and $(\mathfrak{a}_2, n_2)$ be two representations of divisor classes and $(\mathfrak{a}_3, n_3)$ its product as defined in Theorem 4.2. Let the product of $\mathfrak{a}_1$ and $\mathfrak{a}_2$ be represented by $(S(t), Q(t), P(t))$. Let $l \geq 0$ be maximal such that

$$\mathfrak{d}(\mathrm{red}^{l}(\mathfrak{a}_1\mathfrak{a}_2/S(t)), \mathfrak{a}_1\mathfrak{a}_2/S(t)) \leq \deg S(t) + n_1 + n_2.$$

Now it is easy to see that

$$\mathfrak{a}_3 = \mathrm{red}^{l}(\mathfrak{a}_1\mathfrak{a}_2/(S(t)))$$

and

$$\mathfrak{d}(\mathrm{red}^{l}(\mathfrak{a}_1\mathfrak{a}_2/S(t)), \mathfrak{a}_1\mathfrak{a}_2/S(t)) = d(\mathfrak{a}_3, \mathfrak{a}_1\mathfrak{a}_2, n_1 + n_2).$$

Thus we showed how to compute the product in Theorem 4.2. One also sees that the number of reduction steps $l = l_0 + l_1$ is bounded by

$$l \leq \frac{5g+1}{2},$$

since $l_0 \leq (g+1)/2$ and $l_1 \leq 2g$. Similar considerations lead to the evaluation of the inverse of a divisor class.

5. Imaginary versus real quadratic representation

In this section we want to compare the imaginary quadratic and the real quadratic representation of the function field K.

As in Section 4, let $K = k(t)(\sqrt{D(t)})$ with a monic, separable polynomial $D(t)$ of degree $2g+2$. We suppose in addition that $K/k(t)$ has a ramified prime divisor P_∞ which is rational over k. To P_∞ there corresponds a root $\alpha \in k$ of $D(t)$.

We set $x = (t-\alpha)^{-1}$ and get $k(x) = k(t)$. The divisor of x equals $P_1 + P_2 - 2P_\infty$. An easy calculation shows that $F(x) := D(x^{-1} + \alpha)x^{2g+2}$ is a polynomial in $k[x]$ of degree $2g+1$, and that $K = k(x)(\sqrt{F(x)})$.

Now we relate the representations of Theorem 3.2 and Theorem 4.2. Let $[D]$ be a divisor class of K which is given by a pair $(\mathfrak{a}^{(t)}, n)$ as in Theorem 4.2. Let $(Q(t), P(t))$ be the reduced basis of the reduced ideal $\mathfrak{a}^{(t)}$ of $O_K^{(t)}$. We want to evaluate the corresponding reduced ideal $\mathfrak{a}^{(x)}$ of $O_K^{(x)}$ which represents $[D]$ by Theorem 3.2. We calculate

$$\begin{aligned}[D] &= [A^{(t)} - \deg(A^{(t)})P_2] + n[P_1 - P_2] \\ &= [A^{(t)} - \deg(A^{(t)})P_\infty] + n[P_1 - P_\infty] - (n + \deg(A^{(t)}))[P_2 - P_\infty].\end{aligned}$$

It suffices to evaluate the reduced ideals $\mathfrak{a}_i^{(x)}$ and their reduced basis $(U_i(x), V_i(x))$ for the summands $[A^{(t)} - \deg(A^{(t)})P_\infty]$, $[P_1 - P_\infty]$ and $[P_2 - P_\infty]$. The reduced basis $(U(x), V(x))$ of $\mathfrak{a}^{(x)}$ corresponding to the sum can then be evaluated using the Cantor algorithm (cf. Section 3).

We start with $[A^{(t)} - \deg(A^{(t)})P_\infty]$. If P_∞ divides $A^{(t)}$, then $Q(t)$ and $P(t)$ have a simple zero at α, and the reduced basis corresponding to the divisor class $[(A^{(t)} - P_\infty) - \deg(A^{(t)} - P_\infty)P_\infty]$ is $(Q(t)(t-\alpha)^{-1}, P(t)(t-\alpha)^{-1})$. Hence we assume that $Q(\alpha) \neq 0$, and define

$$U_1(x) := Q(\alpha)^{-1}x^{\deg Q(t)}Q(x^{-1} + \alpha)$$

and

$$V_1(x) := x^{g+1}P(x^{-1}+\alpha).$$

$U_1(x)$ and $V_1(x)$ are polynomials in $k[x]$; $U_1(x)$ is monic of degree $\deg U_1(x) = \deg Q(t) = \deg(A^{(t)})$. Let P be any prime divisor of K (with corresponding valuation ν_P) which is different from P_1, P_2 and P_∞. Since $\nu_P(x) = 0$, we calculate

$$\nu_P(U_1(x)) = \nu_P(Q(t))$$

and

$$\nu_P(V_1(x) + \sqrt{F(x)}) = \nu_P(P(t) + \sqrt{D(t)}).$$

Hence $(U_1(x), V_1(x))$ is a basis of the reduced ideal $\mathfrak{a}_1^{(x)}$ corresponding to the class $[A^{(t)} - \deg(A^{(t)})P_\infty]$. Finally one has to reduce $V_1(x)$ modulo $U_1(x)$ to get the reduced basis of $\mathfrak{a}_1^{(x)}$.

The reduced bases corresponding to $[P_1 - P_\infty]$ and $[P_2 - P_\infty]$ depend on the power series expansion of $\sqrt{D(t)}$ in the completion $K_{P_1} = k((t^{-1}))$ of K at P_1. We choose $\sqrt{D(t)}t^{-g-1} + ...$ in K_{P_1}; then $(U_2(x), V_2(x)) = (x, -1)$ corresponds to $[P_1 - P_\infty]$ and $(U_3(x), V_3(x)) = (x, 1)$ to $[P_2 - P_\infty]$. This establishes the calculation of $\mathfrak{a}^{(x)}$.

On the other hand, if one starts with the representation

$$[D] = [A^{(x)} - \deg(A^{(x)})P_\infty]$$

as in Theorem 3.2, then similar calculations yield the representation

$$[D] = [A^{(t)} - \deg(A^{(t)})P_2] + n[P_1 - P_2].$$

An explicit realization of this procedure in the case of $g = 1$ produces the formulas in [1].

Finally, we compare the complexity of the multiplications in Theorem 3.2 and Theorem 4.2. All polynomials involved have degree $\leq g + 1$. We assume that multiplication and division with remainder of two polynomials $F(x)$ and $G(x)$ require $2 \deg F(x) \deg G(x)$ operations in k. Every reduction step applied to nonreduced ideals either in the Cantor algorithm [4] or in the algorithm presented in Section 4 can then be computed in $32g^2 + O(g)$ operations in k, whereas a reduction step applied to reduced ideals in the algorithm presented in Section 4 requires $6g^2 + O(g)$ operations in k.

It follows that the computation of a basis of the primitive ideal $\mathfrak{a}_1\mathfrak{a}_2/S(t)$ requires $4g^3 + O(g^2)$ operations in k and the computation of the (first) reduced ideal $\mathrm{red}^{l_0}(\mathfrak{a}_1\mathfrak{a}_2/S(t))$ equivalent to $\mathfrak{a}_1\mathfrak{a}_2/S(t)$ requires $16g^3 + O(g^2)$ operations in k, since one needs at most $g/2 + 2$ reduction steps to reduce $\mathfrak{a}_1\mathfrak{a}_2/S(t)$. In the imaginary quadratic case, we have $\mathfrak{a}_3 = \mathrm{red}^{l_0}(\mathfrak{a}_1\mathfrak{a}_2/S(t))$, and thus the complexity of computing the product of two elements of the divisor class group is $20g^3 + O(g^2)$ operations in k, given an imaginary quadratic representation.

In the real quadratic case, we have to execute first $l_0 \leq (g+1)/2$ reduction steps to get from $\mathfrak{a}_1\mathfrak{a}_2/S(t)$ to a reduced ideal and additionally $l_1 \leq 2g$ reduction steps to get to $\mathfrak{a}_3$ as explained above. Thus the complexity of computing the product of two elements of the divisor class group is at most $32g^3 + O(g^2)$ operations in k, given a real quadratic representation.

Let us remark that this analysis is far from being optimal and should not induce one to prefer the imaginary over the real representation. Indeed, a few practical experiments show that both arithmetics seem to be equally fast.

Concluding, the arithmetic in the divisor class group of a hyperelliptic function field can be performed using either an imaginary quadratic representation whenever there is a ramified prime divisor in $K/k(t)$ rational over k, or a real quadratic representation when there is no such prime divisor. In the latter case, the new method described in Section 4 is definitely preferable to the imaginary quadratic representation over a suitable constant field extension.

References

1. W. W. Adams, M. J. Razar: *Multiples of points on elliptic curves and continued fractions*. Proc. London Math. Soc. **41** (1980). pp. 481 – 498. MR **82c:**14031
2. E. Artin: *Quadratische Körper im Gebiete der höheren Kongruenzen I*. Mathematische Zeitschrift **19** (1924). pp. 153 – 206; reprinted in S. Lang, J. Tate (eds.): *The collected papers of Emil Artin*. Reading, Mass.: Addison Wesley 1965. MR **31:**1159
3. I. Biehl, J. Buchmann, C. Thiel: *Cryptographic protocols based on discrete logarithms in real quadratic orders*. Proceedings of CRYPTO '94. New York: Springer 1995.
4. D. G. Cantor: *Computing in the Jacobian of a hyperelliptic curve*. Mathematics of Computation **48** (1987). pp. 95 – 101. MR **88f:**11118
5. H. W. Lenstra, Jr.: *On the calculation of regulators and class numbers of quadratic fields*. Number Theory Days (Exeter, 1980; J. V. Armitage, ed.), London Math. Soc. Lecture Note Ser., vol. 56, Cambridge Univ. Press, 1982, pp. 123 – 150. MR **86g:**11080
6. D. Mumford: *Tata Lectures on Theta I, II*. Boston: Birkhäuser Verlag 1983/84. MR **85h:**14026; MR **86b:**14017
7. R. Scheidler, A. Stein, H. C. Williams: *Key-exchange in real quadratic congruence function fields*. Designs, Codes and Cryptography **7** (1996). pp. 153 – 174. MR **97d:**94009
8. D. Shanks: *The infrastructure of a real quadratic field and its applications*. Proc. Number Theory Conf., Univ. of Colorado, Boulder, CO, 1972, pp. 217 – 224. MR **52:**10672
9. A. Stein: *Equivalences between elliptic curves and real quadratic congruence function fields*. Journal de Théorie des Nombres de Bordeaux **9**. 1997. pp. 79 – 95. MR **98d:**11144
10. H. Stichtenoth: *Algebraic Function Fields and Codes*. Berlin; Heidelberg: Springer 1993. MR **94k:**14016

Institut für Theoretische Informatik, TU Darmstadt, Alexanderstrasse 10, 64283 Darmstadt (Germany)

E-mail address: sachar@cdc.informatik.th-darmstadt.de

Institut für Experimentelle Mathematik, Universität GH Essen, Ellernstr.29, 45326 Essen (Germany)

E-mail address: rueck@exp-math.uni-essen.de