The class number one problem in function fields

John-Paul Harper

Thesis presented in partial fulfilment of the requirements for the degree of
Master of Commerce at the University of Stellenbosch

Supervisor: Professor B.W. Green
December 2003

Declaration

I, the undersigned, hereby declare that the work contained in this thesis is my own original work and that I have not previously in its entirety or in part submitted it at any university for a degree.

Abstract

In this dissertation I investigate the class number one problem in function fields. More precisely I give a survey of the current state of research into extensions of a rational function field over a finite field with principal ring of integers. I focus particularly on the quadratic case and throughout draw analogies and motivations from the classical number field situation. It was the "Prince of Mathematicians" C.F. Gauss who first undertook an in depth study of quadratic extensions of the rational numbers and the corresponding rings of integers. More recently however work has been done in the situation of function fields in which the arithmetic is very similar.

I begin with an introduction into the arithmetic in function fields over a finite field and prove the analogies of many of the classical results. I then proceed to demonstrate how the algebra and arithmetic in function fields can be interpreted geometrically in terms of curves and introduce the associated geometric language. After presenting some conjectures, I proceed to give a survey of known results in the situation of quadratic function fields. I present also a few results of my own in this section. Lastly I state some recent results regarding arbitrary extensions of a rational function field with principal ring of integers and give some heuristic results regarding class groups in function fields.

Opsomming

In hierdie tesis ondersoek ek die klasgetal een probleem in funksieliggame. Meer spesifiek ondersoek ek die huidige staat van navorsing aangaande uitbreidings van 'n rasionale funksieliggaam oor 'n eindige liggaam sodat die ring van heelgetalle 'n hoofidealgebied is. Ek kyk in besonder na die kwadratiese geval, en deurgaans verwys ek na die analoog in die klassieke getalleliggaam situasie. Dit was die beroemde wiskundige C.F. Gauss wat eerste kwadratiese uitbreidings van die rasionale getalle en die ooreenstemende ring van heelgetalle in diepte ondersoek het. Onlangs het wiskundiges hierdie probleme ook ondersoek in die situasie van funksieliggame oor 'n eindige liggaam waar die algebraïese struktuur baie soortgelyk is.

Ek begin met 'n inleiding tot die rekenkunde in funksieliggame oor 'n eindige liggaam en bewys die analogie van baie van die klassieke resultate. Dan verduidelik ek hoe die algebra in funksieliggame geometries beskou kan word in terme van kurwes en gee 'n kort inleiding tot die geometriese taal. Nadat ek 'n paar vermoedes bespreek, gee ek 'n oorsig van wat alreeds vir quadratiese funksieliggame bewys is. In hierdie afdeling word 'n paar resultate van my eie ook bewys. Dan vermeld ek 'n paar resultate aangaande algemene uitbreidings van 'n rasionale funksieliggaam oor 'n eindige liggaam waar die van ring heelgetalle 'n hoofidealgebied is. Laastens verwys ek na 'n paar heurisitiese resultate aangaande klasgroepe in funksieliggame.

Acknowledgements

I would firstly like to thank my supervisor Professor B.W. Green for all his support, insight and suggestions into the topic of my research. His guidance and encouragement have indeed been invaluable in the presentation of this thesis. I would also like to thank my dear parents, Paul and Cecile Harper, for supporting me throughout the years and giving me an enjoyment of intellectual endeavours. I would in fact like to thank my whole family for their fond devotion and inspiration. Thank you also to all my friends.

During 2002 and 2003 I have been supported by a NRF grantholder bursary through Professor Green as well as by the NRF Scarce Skills bursary[1]. I would like to thank the National Research Foundation for making such bursaries available and for continuing to encourage research and development in our country. I would also like to thank the Department of Mathematics at Stellenbosch University for being supportive and helpful in many regards. Particularly in that for the last two years I could serve as a part-time research assistant. Finally as many before me I would like to state my conviction - Soli Deo Gloria.

[1]In accordance with the condition of the NRF scholarship I received I would like to state that opinions expressed and conclusions arrived at are those of myself and are not necessarily to be attributed to the NRF.

Contents

Chapter 1

Introduction

It has long been of interest to number theorists to know when an extension of the ring of integers $\mathbb{Z}$ is a unique factorization domain. The classic example where this is not the case is $\mathbb{Z}[\sqrt{-5}]$ in which $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ and all factors are irreducible. The natural questions are: why does unique factorization fail, is there some kind of 'measure' as to how far a ring is from a UFD, and is there some algorithmic method for determining whether a ring is a UFD. These questions led mathematicians like Dedekind to study so called 'ideal' numbers, which in modern terminology are simply ideals of rings. Thus the above questions are answered in the theory of Dedekind domains which have certain desirable properties allowing us to better understand their arithmetic. With any Dedekind domain one can form the class group, whose order (the class number) gives a mysterious measure of how far it is from being a UFD. The class group being trivial, i.e. the ring having class number one, implies that the ring is a PID and hence also a UFD.

We ask ourselves how the above problem of unique factorization in extensions of $\mathbb{Z}$ arises. It is natural to consider these extensions as the integral closure of $\mathbb{Z}$ in a number field. Such extensions of $\mathbb{Z}$ will always be Dedekind domains and due to a celebrated result will always have finite class number. Of particular interest in this context, perhaps because of their very simplicity, are number fields which arise from adjoining the square root of some integer to $\mathbb{Q}$. Such extensions are called real if the square root of a positive number is adjoined and imaginary otherwise. C.F. Gauss was the first who undertook an in depth study of such extensions and it is a well known conjecture of his which I am, amongst other things, studying in an analogous context. This conjecture of Gauss, although stated slightly differently in its original context, is

essentially the following:

Conjecture 1.1 *There are infinitely many real quadratic number fields of class number one.*

To date, however, it is not even known if there are infinitely many general number fields of class number one, the so called Weak Gauss Conjecture. There does however seem to be a great deal of heuristic evidence to support these conjectures. In this classical situation there is another class number problem of a slightly different nature also attributed to Gauss. This problem is to determine all imaginary quadratic number fields of a given class number. There will always be only a finite number of such fields by a well known result of Heilbronn. One can even extend this problem to more general (not necessarily quadratic) imaginary extensions of $\mathbb{Q}$ and ask the same determination problem.

Having explained these classical problems in algebraic number theory, we move towards our topic of number theory in function fields over a finite field. It is well known that there is a very close link between the arithmetic of the integers and that of polynomials over finite fields. For example, both are Dedekind domains and have finite residue rings. Here the analogue of the rationals $\mathbb{Q}$ is the rational function field over a finite field $\mathbb{F}_q(x)$. Throughout this dissertation I will draw on this rich analogy giving motivation and analogies for many of the results from their classical context in algebraic number theory. Thus we can ask precisely the same question as above in this context: Are there infinitely many 'real' (a notion we will make precise later) quadratic extensions of $\mathbb{F}_q(x)$ whose associated ring of integers has class number one. Although this problem is unsolved, the Weak Gauss Conjecture in this context has been shown over certain constant fields $\mathbb{F}_q$ by Lachaud and Vladut and I will in the last chapter explain their precise result. We can also ask the determination problem of all imaginary quadratic extensions of $\mathbb{F}_q(x)$ with a given class number. In this dissertation we will focus primarily on the class number problem in quadratic function fields. It was the great mathematician Emil Artin who in his doctoral thesis first undertook an in depth study of these quadratic extensions of $\mathbb{F}_q(x)$.

In the function field context there are two approaches to the class number problem, the algebraic and the geometric. Roughly speaking, the algebraic approach focuses on the study of ideals whilst the geometric approach focuses on the properties of the curves associated with the function fields. For example quadratic extensions of $\mathbb{F}_q(x)$ correspond to hyperelliptic curves over $\mathbb{F}_q$. These two approaches have come together beautifully with the advent of

modern algebraic geometry, and one tends to use the language most appropriate in a particular situation.

In the Appendix A we give some basic definitions and results regarding algebraic function fields which will be used throughout. We begin in Chapter 2 by laying the groundwork for studying quadratic extensions of $\mathbb{F}_q(x)$. We will prove for example the finiteness of the class number and the analogue of the Dirichlet unit theorem. Moreover we will present a formula for computing the class number of a quadratic function field as well as introducing continued fractions which play an important role in the study of real quadratic fields. We also develop some well known ideal theory in quadratic function fields as well as giving a formulation of results such as the Hasse-Weil theorem which will be used in the later chapters.

In Chapter 3 we introduce the geometric language of varieties and curves and briefly explain how this relates to the algebraic language of function fields. We also translate some of the results of Chapter 2 into this new language. Several conjectures regarding global field extensions are also presented in the more general context of global fields so as to draw on the close analogy between global fields in positive characteristic and those in characteristic 0.

Chapter 4 attempts to cover the most important results in the theory of quadratic extensions of $\mathbb{F}_q(x)$. We draw on work done on both real and imaginary quadratic function fields over the last 30 odd years. In this chapter we also give a brief account of how the theory of quadratic function fields has been applied to modern applications such as Cryptography. I also present some of my own original work regarding real quadratic function fields in Section 4.3.

Finally in Chapter 5 we briefly explain the results of Lachaud and Vladut regarding infinitely many Galois extensions of $\mathbb{F}_q(x)$ with principal rings of integers. We also present some recent results regarding more general imaginary extensions of $\mathbb{F}_q(x)$ with principal rings of integers. We then proceed to look briefly at some heuristic results regarding class numbers in function fields. These heuristics give motivation to continue in this avenue of research until satisfactory proofs of the many conjectures are given. We end this chapter with a brief outlook on the class number one problem in function fields.

I note that all numerical and computational investigations were done using the MAGMA computational algebra package.

Chapter 2

Preliminaries and background

In this chapter we will develop the necessary background in order to discuss the deeper results in the theory of quadratic function fields. We will mainly be following the algebraic approach of Chevalley and the school of Roquette (Deuring, Stichtenoth) although in Chapter 3 we will introduce some geometric language. As a matter of notation, the symbols $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ denote respectively the natural numbers, the natural numbers inclusive of 0, the integers, the rational numbers, and the real numbers. We will denote by R_p the localization of the ring R at some prime ideal p. In the Appendix A we present basic definitions and results regarding algebraic function fields which we will use throughout.

2.1 S-Integers, S-Units and the S-Class Group

Here we will develop the necessary groundwork to study the behaviour of quadratic extensions of $\mathbb{F}_q(x)$. We will do so by approaching the problem slightly more generally. Let F/k be a function field in one variable over a perfect field k. We are interested in the analogy between classical algebraic number theory and number theory in function fields. This analogy becomes particularly clear when we choose some non-constant $x \in F$. The rings $k[x] \subset k(x)$ then play the role of the pair $\mathbb{Z} \subset \mathbb{Q}$. The analogue of the ring of integers would be the integral closure of $k[x]$ in F which we will denote by $\mathcal{O}$. It is a well known result that the integral closure of a Dedekind domain in some finite extension of its quotient field is again a Dedekind domain, consequently $\mathcal{O}$ is a Dedekind domain. The results of this section are well known and can be found in [Ro, Ch 8]

The ring $\mathcal{O}$ can be thought of in another perhaps more insightful way. Let ∞ denote the prime at infinity (place defined by the usual degree) in the subfield $k(x)$ of F and let S be the set of finitely many primes in F lying above ∞. We will show that the ring $\mathcal{O}$ is the intersection of all valuation rings $\mathcal{O}_P$ where $P \in S(F/k)\backslash S$. This being the case, let $S \subset S(F/k)$ be any finite set of primes. The *ring of S-integers* is defined to be:

$$\mathcal{O}_S := \{z \in F : v_P(z) \geq 0,\ \forall P \notin S\}$$

The units of the ring of S-integers will be called the *S-unit group* and are naturally characterized by:

$$\mathcal{O}_S^* = \{z \in F^* : v_P(z) = 0,\ \forall P \notin S\}$$

It is clear that $k^* \subseteq \mathcal{O}_S^*$ and we will in fact see that $\mathcal{O}_S^*/k^*$ is a finitely generated, free abelian group. This is the analogue of the famous Dirichlet unit theorem. The ring of S-integers is a holomorphy ring and consequently a Dedekind domain (see Appendix A).

Since the function field F will be fixed for this section, we will denote by $\mathcal{D}$ its divisor group, by $\mathcal{P}$ the subgroup of principal divisors and by $Cl = \mathcal{D}/\mathcal{P}$ the group of divisor classes. The *group of S-divisors*, $\mathcal{D}_S$, is defined to be the subgroup of $\mathcal{D}$ generated by the primes in $S(F/k)\backslash S$. Given an element $z \in F^*$, its S-divisor is defined to be

$$(z)_S = \sum_{P \notin S} v_P(z)P$$

A divisor which is of the form $(z)_S$ for some $z \in F^*$ is called a *principal S-divisor*. The principal S-divisors form a subgroup of $\mathcal{D}_S$ which is denoted by $\mathcal{P}_S$. The quotient group $Cl_S = \mathcal{D}_S/\mathcal{P}_S$ is called the *S-class group*. Later we will show that Cl_S is in fact isomorphic to the ideal class group of the Dedekind domain $\mathcal{O}_S$.

Additionally, we define $\mathcal{D}(S)$ to be the subgroup of $\mathcal{D}$ generated by the primes in S and $\mathcal{P}(S) = \mathcal{P} \cap \mathcal{D}(S)$. As usual a superscript 0 will imply that we only consider divisors (or divisor classes) of degree 0.

Consider the degree map $\deg : \mathcal{D} \to \mathbb{Z}$, which is a group homomorphism with respect to the additive operation on $\mathbb{Z}$. The image of this map is a principal ideal $i\mathbb{Z}$ where $i = \gcd\{\deg P : P \in S(F/k)\}$. When k is a finite field a theorem of F.K. Schmidt ensures that $i = 1$. The image of $\mathcal{D}(S)$ under the degree map is also a principal ideal in $\mathbb{Z}$ which we will denote $d\mathbb{Z}$ where

$d = \gcd\{\deg P : P \in S\}$. Clearly $i \mid d$. We will now prove the analogues of the Dirichlet unit theorem and the finiteness of the class number.

Proposition 2.1 *The following sequences are exact:*

(a) $(0) \to k^* \to \mathcal{O}_S^* \to \mathcal{P}(S) \to (0)$,

(b) $(0) \to \mathcal{D}(S)^0/\mathcal{P}(S) \to Cl^0 \to Cl_S \to G \to (0)$, *where* G *is a cyclic group of order* d/i.

Proof. The map from $\mathcal{O}_S^*$ to $\mathcal{P}(S)$ is given by taking an S-unit to its divisor. It is an onto map by definition of $\mathcal{P}(S)$. If an S-unit e goes to the zero divisor, then $v_P(e) = 0$ for all $P \in S(F/k)$ and hence must be a constant. This proves the exactness of (a).

To deal with the second exact sequence we first define a map $\tau : \mathcal{D} \to \mathcal{D}_S$ as follows:

$$\tau(D) = \sum_{P \notin S} v_P(D)P$$

This map is an epimorphism with kernel $\mathcal{D}(S)$. We obtain the following exact sequence:

$$(0) \to \mathcal{D}(S) \to \mathcal{D} \to \mathcal{D}_S \to (0)$$

Now the preimage under τ of $\mathcal{P}_S$ is $\mathcal{P} + \mathcal{D}(S)$. We therefore obtain the exact sequence:

$$(0) \to \frac{\mathcal{P} + \mathcal{D}(S)}{\mathcal{P}} \to \frac{\mathcal{D}}{\mathcal{P}} \to \frac{\mathcal{D}_S}{\mathcal{P}_S} \to (0)$$

Using the second isomorphism theorem we have:

$$(0) \to \frac{\mathcal{D}(S)}{\mathcal{P} \cap \mathcal{D}(S)} \to \frac{\mathcal{D}}{\mathcal{P}} \to \frac{\mathcal{D}_S}{\mathcal{P}_S} \to (0) \qquad (*)$$

Now since $\mathcal{D}^0(S) = \mathcal{D}(S) \cap \mathcal{D}^0$ and $\mathcal{P}(S) = \mathcal{P} \cap \mathcal{D}(S) = \mathcal{P} \cap \mathcal{D}^0(S)$ we have:

$$(0) \to \mathcal{D}(S)^0/\mathcal{P}(S) \to Cl^0 \to Cl_S$$

Unfortunately the right hand morphism need not be onto. We will show that the cokernel of the right hand morphism is a cyclic group of order d/i.

To do this, we again use the fact that τ induces an isomorphism from $\mathcal{D}/(\mathcal{P} + \mathcal{D}(S))$ to Cl_S (From the third isomorphism theorem and the exact sequence $(*)$ above). The group we are interested in can also be described as the cokernel of the natural map from $Cl^0 = \mathcal{D}^0/\mathcal{P}$ to $\mathcal{D}/(\mathcal{P} + \mathcal{D}(S)) \cong Cl_S$. This cokernel is isomorphic to $\mathcal{D}/(\mathcal{D}^0 + \mathcal{D}(S))$ (using the fact that $\mathcal{P} \subseteq \mathcal{D}^0$). The degree map provides an isomorphism of $\mathcal{D}/(\mathcal{D}^0 + \mathcal{D}(S))$ with $i\mathbb{Z}/d\mathbb{Z} \cong \mathbb{Z}/(d/i)\mathbb{Z}$.

■

Corollary 2.2 *The group $\mathcal{O}_S^*/k^*$ is a finitely generated free group of rank at most $|S|-1$, where $|S|$ is the cardinality of S.*

Proof. By the exact sequence (a) we have $\mathcal{O}_S^*/k^* \cong \mathcal{P}(S)$, which is a subgroup of the free abelian group $\mathcal{D}(S)^0$. By the degree map we have the following exact sequence:

$$(0) \to \mathcal{D}(S)^0 \to \mathcal{D}(S) \to d\mathbb{Z} \to (0)$$

Hence $\mathcal{D}(S)/\mathcal{D}(S)^0 \cong d\mathbb{Z} \cong \mathbb{Z}$. Now since $\mathcal{D}(S)$ is free on $|S|$ generators, it follows that $\mathcal{D}(S)^0$ is free on $|S|-1$. Thus, $\mathcal{P}(S)$ is free on at most $|S|-1$ generators. ∎

Corollary 2.3 *Cl_S is a finite group if Cl^0 is a finite group. Also, Cl_S is a torsion group if Cl^0 is a torsion group.*

Proof. Both statements are a consequence of the exact sequence Proposition 2.1 (b). ∎

Proposition 2.4 *Let $F/\mathbb{F}_q$ be a function field over the finite field $\mathbb{F}_q$. Then, for all finite subsets $S \subset S(F/\mathbb{F}_q)$, we have that Cl_S is a finite group and $\mathcal{O}_S^*/\mathbb{F}_q^*$ is a free abelian group on $|S|-1$ generators.*

Proof. It is a well known result that a function field over a finite field has a finite number of divisor classes of degree 0, i.e. Cl^0 is a finite group. Now finiteness of Cl_S follows from the result above.

By the exact sequence (b) we see that $\mathcal{D}(S)^0/\mathcal{P}(S)$ is finite. This shows that $\mathcal{P}(S) \cong \mathcal{O}_S^*/k^*$ is free on $|S|-1$ generators. ∎

We now look at an important invariant of the function field, namely the S-regulator. To define this, we begin by choosing a set of S-units $\{e_1, ..., e_{s-1}\}$ whose projection to $\mathcal{O}_S^*/k^*$ is a basis. Consider the $(s-1) \times s$ matrix M whose ij'th entry is $\ln |e_i|_{P_j}$, where $S = \{P_1, ..., P_s\}$. We claim that the sum of the columns of this matrix is zero. To see this, note that for any $z \in F^*$ we have

$$-\sum_P \ln |z|_P = -\sum_P \ln(q^{-\deg(P)v_P(z)}) = \sum_P (v_P(z) \deg P) \ln q = \deg(z) \ln q = 0$$

For any S-unit, the only primes occurring in the sum are the primes in S and the assertion follows.

Hence the determininants of the $(s-1)\times(s-1)$ minors of M are all the same up to sign. The absolute value of any one of these determinants is taken as the definition of the S-regulator which we will denote R_S. It can be shown that this definition is independent of the choice of basis for $\mathcal{O}_S^*/k^*$.

An associated regulator $R_S^{(q)}$ has the same definition as R_S except that one uses $\log_q(*)$ instead of the natural logarithm $\ln(*)$. By examining the determininants of the $(s-1)\times(s-1)$ minors one sees that the factor $\ln(q)$ can be taken out and consequently the two regulators are related as follows:

$$\ln(q)^{s-1}R_S^{(q)} = R_S$$

We note that $R_S^{(q)}$ is in fact an integer as any entry in the matrix M defined above had the following form:

$$\log_q |z|_P = \log_q(q^{-\deg(P)v_P(z)}) = -\deg(P)v_P(z)$$

which is an integer. The following proposition relates the regulator to the index $[\mathcal{D}(S)^0 : \mathcal{P}(S)]$ and will be important for determining the relationship between the regulator and other key invariants.

Proposition 2.5

$$[\mathcal{D}(S)^0 : \mathcal{P}(S)] = \frac{dR_S^{(q)}}{\prod_{P\in S}\deg P}$$

Proof. We begin by defining a map $\theta : \mathcal{D}(S) \to \mathbb{Z}^s$. If $D \in \mathcal{D}(S)$, we set $\theta(D) = (..., -v_P(D)\deg P, ...)$, where P varies over S. Note that θ is a homomorphism and that if $e \in \mathcal{O}_S^*$, then $\theta((e)) = (..., \log_q |e|_P, ...)$. We also see from the definition that $[\mathbb{Z}^s : \theta(\mathcal{D}(S))] = \prod_{P\in S}\deg P$. Consider the elements of $\mathbb{Z}^s$ as row vectors and define $H^0 \subset \mathbb{Z}^s$ to be the subgroup consisting of all row vectors whose sum of coordinates is zero.

We have $\theta(\mathcal{P}(S)) \subseteq \theta(\mathcal{D}(S)^0) \subseteq H^0$. It is easy to see that θ is one to one. It follows that

$$[\mathcal{D}(S)^0 : \mathcal{P}(S)] = [\theta(\mathcal{D}(S)^0) : \theta(\mathcal{P}(S))] = \frac{[H^0 : \theta(\mathcal{P}(S))]}{[H^0 : \theta(\mathcal{D}(S)^0)]}$$

We now calculate the numerator and denominator of this expression. First we compute the index $[H^0 : \theta(\mathcal{P}(S))]$. Let $\epsilon_s \in \mathbb{Z}^s$ be the vector with zeros everywhere except for a 1 at the s'th place. Then $\mathbb{Z}^s$ is the direct sum of H^0 and $\mathbb{Z}\epsilon_s$. It follows that the index of $\theta(\mathcal{P}(S))$ in H^0 is the same as the index of $\theta(\mathcal{P}(S)) + \mathbb{Z}\epsilon_s$ in $\mathbb{Z}^s$. A free basis for this subgroup is $\{\theta((e_1)), ..., \theta((e_{s-1})), \epsilon_s\}$. Let $M^{(q)}$ be the $s-1\times s$ matrix whose i'th row is $\theta((e_i))$ and M' be

the $s \times s$ matrix obtained from $M^{(q)}$ by adjoining ϵ_s as the bottom row. By application of the elementary divisors theorem [La1, Th 7.8], the index we are looking for is the absolute value of the determinant M'. Expanding this determinant in cofactors along the bottom row shows the index in question is $R_S^{(q)}$.

To compute $[H^0 : \theta(\mathcal{D}(S)^0)]$, consider the exact sequence

$$(0) \to H^0/\theta(\mathcal{D}(S)^0) \to \mathbb{Z}^s/\theta(\mathcal{D}(S)) \to \mathbb{Z}/d\mathbb{Z} \to (0)$$

The second arrow is induced by inclusion and the third arrow by the sum of coordinates map from $\mathbb{Z}^s \to \mathbb{Z}$. From this exact sequence, we deduce

$$[H^0 : \theta(\mathcal{D}(S)^0)] = \frac{\prod_{P \in S} \deg P}{d}$$

The result now follows. ■

Corollary 2.6 *Suppose all primes in S have degree 1. Then, $[\mathcal{D}(S)^0 : \mathcal{P}(S)] = R_S^{(q)}$.*

Now putting together this last result and the exact sequence (b) in Proposition 2.1 we arrive at the following result first shown by F.K. Schmidt. Writing the exact sequence (b) in the following way:

$$\mathcal{D}(S)^0/\mathcal{P}(S) \hookrightarrow Cl^0 \overset{\phi}{\twoheadrightarrow} \mathrm{Im}(\phi) \subseteq Cl_S \twoheadrightarrow G$$

we see that $Cl_S/\mathrm{Im}(\phi) \cong G$. Also $Cl^0/(\mathcal{D}(S)^0/\mathcal{P}(S)) \cong \mathrm{Im}(\phi)$ hence

$$\begin{aligned} |Cl_S| &= |G|\,|\mathrm{Im}(\phi)| \\ &= |G|\,\left|Cl^0\right| / \left|\mathcal{D}(S)^0/\mathcal{P}(S)\right| \\ &= (\frac{d}{i} h_F) \cdot \frac{\prod_{P \in S} \deg P}{d R_S^{(q)}} \\ &= \frac{h_F \prod_{P \in S} \deg P}{i R_S^{(q)}} \end{aligned}$$

In particular if all primes in S have degree 1 and the constant field k is finite we have:

$$|Cl_S|\, R_S^{(q)} = h_F$$

Now that we have exhibited the above relationship, we wish to relate the S-Class group Cl_S to the class group of the Dedekind domain $\mathcal{O}_S$. We have the following result:

Theorem 2.7 *Let F/k be a function field over k and let S be a non-empty, finite set of primes. There exist elements $x \in F$ such that the poles of x consist precisely of the elements of S. For any such element x, the integral closure of $k[x]$ in F is $\mathcal{O}_S$. $\mathcal{O}_S$ is a Dedekind domain and there is a 1-1 correspondence between the non-zero prime ideals of $\mathcal{O}_S$ and the primes of F not in S given by*

$$P \mapsto M_P := P \cap \mathcal{O}_S \quad \textit{(for any } P \in S(F/k) \backslash S\textit{)}.$$

moreover, the map

$$\varphi : \left\{ \begin{array}{c} \mathcal{O}_S/M_P \to \mathcal{O}_P/P \\ x + M_P \mapsto x + P \end{array} \right\}$$

is an isomorphism. Finally the class group $Cl(\mathcal{O}_S)$ is isomorphic to Cl_S.

Proof. Let $S = \{P_1, ..., P_s\}$. Consider the vector spaces $\mathcal{L}(mP_i) = \{x \in F^* : (x) + mP_i \geq 0\}$ for some positive integer m. We suppose that m is large enough (say, $m > 2g - 2$) so that $\mathcal{L}(mP_i) = m \deg P_i - g + 1$. It follows that $\mathcal{L}(mP_i)$ is properly contained in $\mathcal{L}((m+1)P_i)$. Pick an element $x_i \in \mathcal{L}((m+1)P_i) \backslash \mathcal{L}(mP_i)$. Then x_i has a pole of order $m+1$ at P_i and no other poles. Now consider $x = x_1 x_2 \cdots x_s$. Then x has each element of S as a pole, and no other poles.

Now let R be the integral closure of $k[x]$ in F. It is well known that the ring R is a Dedekind domain even if $F/k(x)$ is an inseparable extension. If P is a prime of F not in S, then $x \in \mathcal{O}_P$ and it follows that $R \subseteq \mathcal{O}_P$. Thus,

$$R \subseteq \bigcap_{P \notin S} \mathcal{O}_P = \mathcal{O}_S$$

We will show that $R = \mathcal{O}_S$. Let $P \notin S$ be a prime of F and consider $P \cap R$. It cannot be that $P \cap R = (0)$ since otherwise the quotient field of R, namely F, would inject into the residue field $\mathcal{O}_P/P$ and $\mathcal{O}_P/P$ is of finite degree over k. Thus $P \cap R = p$ is a maximal ideal of R, and $R_p \subseteq \mathcal{O}_P$. This must be an equality as R_p is a d.v.r and so is a maximal subring of F. On the other hand, if p is a maximal ideal of R then R_p is a d.v.r and pR_p is a prime of F containing x. This shows that $p \to pR_p$ is a 1-1 correspondence between the maximal ideals of R and the primes of F not in S. Again using the fact that R is a Dedekind domain, we have:

$$R = \bigcap_{p \subset R} R_p = \bigcap_{P \notin S} \mathcal{O}_P = \mathcal{O}_S$$

Hence it follows that $Cl(R) \cong Cl(\mathcal{O}_S) \cong Cl_S$. Finally we note that

$$R/p \cong R_p/pR_p$$

which implies that the map φ given above is indeed an isomorphism. ■

2.2 Application to quadratic function fields

In our case we are primarily interested in quadratic extensions of $\mathbb{F}_q(x)$. I will use the terminology quadratic instead of hyperelliptic, as some authors require that the genus be strictly larger than one in the latter case whilst we are interested in all cases. For simplicity and in the spirit of Artin, we will for the most part not deal with the even characteristic case although I will mention a few results in that case as well. We define a quadratic function field as follows:

Definition 2.8 *A quadratic function field over $\mathbb{F}_q$ is an algebraic function field $F/\mathbb{F}_q$ of genus $g \geq 1$ which contains a rational subfield $\mathbb{F}_q(x) \subseteq F$ with $[F : \mathbb{F}_q(x)] = 2$.*

Note that we do not consider the case $g = 0$ since any such quadratic function field over $\mathbb{F}_q$ is rational and the arithmetic well understood.

We have the following characterization of quadratic function fields in odd characteristic which can be found in [St, Ch VI]. Let $k = \mathbb{F}_q$ be of odd characteristic.

Proposition 2.9 *(a) Let F/k be a quadratic function field of genus g. Then there exist $x, y \in F$ such that $F = k(x, y)$ and*

$$y^2 = D(x) \in k[x]$$

for a square-free polynomial $D(x)$ of degree $2g + 1$ or $2g + 2$.

(b) Conversely, if $F = k(x, y)$ and $y^2 = f(x) \in k[x]$ for a square-free polynomial f of degree $m > 2$, then F/k is quadratic of genus

$$g = \left\{ \begin{array}{l} (m-1)/2 \text{ if } m \equiv 1 (\mathrm{mod}\, 2) \\ (m-2)/2 \text{ if } m \equiv 0 (\mathrm{mod}\, 2) \end{array} \right\}$$

I will usually denote the function field F in (a) above as $F = k(x, \sqrt{D})$, i.e. $F = k(x, y)$ where $y^2 - D(x) = 0$. In this case F is a Galois extension of $k(x)$ with the non-identity automorphism σ characterized by $\sigma(\sqrt{D}) = -\sqrt{D}$. For any $z \in F$, we will denote its conjugate by $\bar{z} = \sigma(z)$.

We now come to the even characteristic case. The following characterization can be found in [Lb1]. Let $k = \mathbb{F}_q$ be of even characteristic and let us recall the form of an Artin-Schreier extension in this case:

Proposition 2.10 *(a) Let F/k be a quadratic function field of genus g. Then there exist x and y in F such that $F = k(x, y)$ and*

$$y^2 + h(x)y + f(x) = 0 \tag{2.1}$$

with polynomials h, $f \in k[x]$ such that all zeros of h in $\bar{k}$ are simple zeros of f and

$$\deg(h) \leq g \text{ and } \deg(f) = 2g + 1$$

or

$$\deg(h) = g + 1 \text{ and } \deg(f) \leq 2g + 2$$

(b) Conversely, let g be an integer such that $g \geq 2$. If $F = k(x, y)$ and $y^2 + h(x)y + f(x) = 0$ with polynomials f and h as in (2.1), then F/k is a quadratic function field of genus g.

Once again under the above conditions F/k is Galois. In this case the non-identity automorphism σ is characterized by $\sigma(y) = y + h(x)$. We note that that above extension can also be transformed into the so called *Hasse normalized* equation $y^2 + y = g(x)$ for some $g(x) \in k(x)$, but we present it as above in order to simplify the later description of the decomposition of primes.

We have the following characterization of the integral closure of $\mathbb{F}_q[x]$ in a quadratic function field $F/\mathbb{F}_q$ when $\mathbb{F}_q$ is of odd characteristic. Unlike in classical quadratic number fields where the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ depends upon the congruence class of $d \bmod 4$, the integral closure of $\mathbb{F}_q[x]$ in $\mathbb{F}_q(x, \sqrt{D})$ has only one form, that being:

Proposition 2.11 *The integral closure of $\mathbb{F}_q[x]$ in $F = \mathbb{F}_q(x, \sqrt{D})$ is $\mathcal{O} = \mathbb{F}_q[x, \sqrt{D}]$*

Proof. Let $f \in F$ be integral over $\mathbb{F}_q[x]$. We can write $f = (g + h\sqrt{D})/r$ where $g, h, r \in \mathbb{F}_q[x]$. Since f is integral we have $f^2 + a_1 f + a_0 = 0$ for some $a_0, a_1 \in \mathbb{F}_q[x]$. By multiplying through by r^2 we obtain $(g + h\sqrt{D})^2 + a_1 r(g + h\sqrt{D}) + a_0 r^2 = 0$. Hence

$$g^2 + h^2 D + a_1 rg + a_0 r^2 + h(2g + a_1 r)\sqrt{D} = 0 \tag{$*$}$$

Hence $h(2g + a_1 r) = 0$. Hence $h = 0$ or $2g + a_1 r = 0$ ($\mathbb{F}_q[x]$ is an integral domain). Suppose $h = 0$. Then

$$\begin{aligned} g^2 + a_1 rg + a_0 r^2 &= 0 \\ g^2 &= r(-a_1 g + -a_0 r) \\ \text{therefore } r &\mid g \end{aligned}$$

Suppose $h \neq 0$. Then $2g + a_1 r = 0$, so that $g = (-a_1/2)r$ and hence $r \mid g$. Now from $(*)$

$$\begin{aligned} g^2 + h^2 D + a_1 rg + a_0 r^2 &= 0 \\ (\frac{-a_1}{2} r)^2 + h^2 D + a_1 r(\frac{-a_1}{2} r) + a_0 r^2 &= 0 \\ h^2 D &= r^2(\frac{-a_1^2}{2} - a_0 - \frac{a_1^2}{4}) \end{aligned}$$

but $r^2 \nmid D$ since D is square-free. Hence $r \mid h$. The result follows. ■

Hence $\alpha_1 = 1$, $\alpha_2 = \sqrt{D}$ form an integral basis for $\mathcal{O}$. The discriminant of the function field F is

$$\begin{aligned} d_F &= (\det(\sigma_i \alpha_j))^2 \\ &= \begin{vmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{vmatrix}^2 \\ &= (-2\sqrt{D})^2 \\ &= 4D \end{aligned}$$

Since the discriminant is only defined up to multiplication by a unit, we will refer to the discriminant of F simply as D. We recall that the above integral closure can also be seen as the ring of S-integers $\mathcal{O}_S$, where S is chosen to be the primes in F lying above ∞.

Convention 2.12 *For convenience we will simply write $\mathcal{O}$ instead of $\mathcal{O}_S$. Similarly we will simply write R for the regulator $R_S^{(q)}$ as it is convenient to use the associated regulator.*

We recall that a real quadratic number field is of the form $\mathbb{Q}(\sqrt{d})$ for some square-free positive integer d. Another way of characterizing the above extension is according to whether or not the archimedean valuation $|\cdot|_\infty$ splits. In the real case we obtain two distinct valuations $v_1 : a + b\sqrt{d} \mapsto \left|a + b\sqrt{d}\right|$ and $v_2 : a + b\sqrt{d} \mapsto \left|a - b\sqrt{d}\right|$ which both give us $|\cdot|_\infty$ on restriction.

However with an imaginary extension, i.e. d a negative integer, the two valuations given above are equivalent as the norm of a complex number is the same as that of its conjugate. Hence in the imaginary case the archimedean valuation does not split.

This provides motivation for how we ought (and how Emil Artin did indeed) characterize quadratic extensions of $\mathbb{F}_q(x)$, i.e. by how the prime at infinity ∞ behaves. The following theorem will aid us in this task. Recall that for an element $f \in \mathbb{F}_q[x]$, $v_\infty(f) = -\deg(f)$. Let $u = \frac{1}{x}$, then $v_\infty(u) = 1$, i.e. u is a uniformizing parameter at infinity. Let $d = \deg D$ and rewrite $D(x)$ in terms of u as:

$$D(x) = \sum_{i=0}^{d} a_i x^i = x^d \sum_{i=0}^{d} a_i x^{i-d} = u^{-d} \sum_{i=0}^{d} a_i u^{d-i} = u^{-d} D^*(u)$$

where $D^*(u) \in \mathbb{F}_q[u]$ and its constant term $a_d \neq 0$ is the leading term of $D(x)$.

Theorem 2.13 *Let $F = \mathbb{F}_q(x, \sqrt{D})$, where $D \in \mathbb{F}_q[x]$ is square-free. Let $d = \deg(D)$ and a_d be the leading coefficient of D.*

(1) If d is odd, then ∞ is ramified in F,

(2) if d is even and a_d is not a square in $\mathbb{F}_q^*$, then ∞ remains prime in F,

(3) if d is even and a_d is a square in $\mathbb{F}_q^*$, then ∞ splits in F.

Proof. Suppose d is odd. Since u is a uniformizing parameter at infinity we know that $D(x) = u^{-d}D^*(u)$ where $D^*(u) \in \mathcal{O}_\infty^*$. Suppose P_∞ is a prime of F lying above ∞. Then, setting e equal to the ramification index of P_∞ over ∞ we obtain:

$$v_{P_\infty}(\sqrt{D(x)}) = \frac{1}{2} v_{P_\infty} D(x) = \frac{e}{2} v_\infty(u^{-d}D^*(u)) = -\frac{ed}{2}$$

Since this must be an integer, and d is assumed odd, it follows that $2 \mid e$. Thus $e = 2$, and ∞ is ramified in $F/\mathbb{F}_q$.

Now suppose d is even. Then F is generated over $\mathbb{F}_q$ by $\sqrt{D^*(u)}$. Since $D^*(u)$ is square-free as a polynomial in u, it follows that the integral closure, B, of $A = \mathbb{F}_q[u]$ in F is $A + A\sqrt{D^*(u)}$. Now from [La2, Ch 1, Prop 15], the prime decomposition of ∞ follows from that of the irreducible polynomial $x^2 - D^*(u)$ reduced modulo u. The reduction is simply $x^2 - a_d \in \mathbb{F}_q[x]$. This either splits or is irreducible according to whether or not a_d is a square in $\mathbb{F}_q^*$. ∎

In the even characteristic we have the following analogue of the above theorem (see [Lb1]):

Theorem 2.14 *Let $F/\mathbb{F}_q$ be a quadratic function field of genus g over $\mathbb{F}_q$ where $2 \mid q$. Then $F = \mathbb{F}_q(x, y)$ where x and y satisfy equation (2.1).*

(1) The infinite prime ∞ ramifies if and only if $\deg(f) = 2g + 1$ and $\deg(h) \leq g$,

(2) ∞ is inert if and only if $\deg(h) = g + 1$ and $x^2 + ax + b$ is an irreducible polynomial in $\mathbb{F}_q[x]$, where $a, b \in \mathbb{F}_q$ are the leading coefficients of h and f respectively,

(3) ∞ splits if and only if $\deg(h) = g + 1$ and $x^2 + ax + b$ is a reducible polynomial in $\mathbb{F}_q[x]$, where $a, b \in \mathbb{F}_q$ are the leading coefficients of h and f respectively.

We use the above two theorems to characterize quadratic extensions of $\mathbb{F}_q(x)$.

Definition 2.15 *F is called real quadratic if ∞ splits and imaginary quadratic otherwise. For distinction between the two imaginary cases we will sometimes refer to the inert or ramified case.*

Since we have not developed all the necessary theory yet, we will not now describe the decomposition of the finite primes. We will see in Section 2.5 that in the case of quadratic fields there exist elegant formulae for the decomposition of the finite primes. The next result characterizes the units $\mathcal{O}^*$ in a quadratic function field and is simply an application of Proposition 2.4.

Proposition 2.16 *If F is imaginary quadratic, then $\mathcal{O}^* = \mathbb{F}_q^*$. If F is real quadratic, then $\mathcal{O}^* = \mathbb{F}_q^* \langle \epsilon \rangle$.*

Proof. In the first case there is only one prime lying above ∞, i.e. $|S| = 1$. Since $\mathbb{F}_q^* \subseteq \mathcal{O}^*$, this implies immediately that $\mathcal{O}^* = \mathbb{F}_q^*$ (there are no generators for the free part). In the second case ∞ splits, i.e. $|S| = 2$. Hence $\mathcal{O}^* = \mathbb{F}_q^* \langle \epsilon \rangle$ (is free on one generator). This generator ϵ is known as a *fundamental unit* of $\mathcal{O}^*$. ■

We are now interested in the relationship between the class number h_F of the function field, i.e. the number of the divisor classes of degree 0, and the class number of the ring of integers $\mathcal{O}$. This is simply an application of Schmidt's formula which we derived above.

Proposition 2.17 *Let $h_{\mathcal{O}}$ denote the class number of $\mathcal{O}$.*

(1) If ∞ is ramified, $h_{\mathcal{O}} = h_F$,

(2) if ∞ is inert, $h_{\mathcal{O}} = 2h_F$,

(3) if ∞ splits, $h_{\mathcal{O}} = h_F/R$.

Proof. Schmidt's formula tells us:

$$h_{\mathcal{O}} = \frac{h_F \prod_{P \in S} \deg P}{iR}$$

Since our constants are $\mathbb{F}_q$ another result of F.K. Schmidt tells us that $i = 1$. In the first two cases $R = 1$. Now we need only note that if ∞ is inert, $\deg P_\infty = 2$ where P_∞ is the prime above ∞. In the real case let $\{P_\infty, \bar{P}_\infty\}$ be the primes above ∞. Then $\deg(P_\infty) = \deg(\bar{P}_\infty) = 1$ and moreover $R = \left|\log_q |\epsilon|_{P_\infty}\right|$ where ϵ is a fundamental unit of $\mathcal{O}$. ∎

Remark 2.18 When $\mathbb{F}_q$ is of odd characteristic, the expression $R = \left|\log_q |\epsilon|_{P_\infty}\right|$ can be simplified in the following way. Let $\epsilon = g + h\sqrt{D}$, $g, h \in \mathbb{F}_q[x]$ be a fundamental unit. Then $\epsilon + \bar{\epsilon} = 2g$, which implies $v_\infty(g) = v_{P_\infty}(g) = v_{P_\infty}(\epsilon + \bar{\epsilon}) = v_{P_\infty}(\hat{\epsilon}) = -\log_q |\hat{\epsilon}|_{P_\infty}$, where $\hat{\epsilon}$ equals either ϵ or $\bar{\epsilon}$ (the absolute value however makes it unimportant whether $\hat{\epsilon}$ equals ϵ or its conjugate). Since $v_\infty(g) = -\deg(g)$, we arrive at $h_{\mathcal{O}} = h_F/\deg(g)$.

The regulator is hence a very important invariant for our purposes. The result above tells us that in the case of imaginary extensions of $\mathbb{F}_q(x)$ the problem of finding the class number of the ring of integers $\mathcal{O}$ is precisely the same as that of finding the class number h_F of the function field. For this reason one can in a certain sense say that more is known in the imaginary case, for example all imaginary quadratic extensions of $\mathbb{F}_q(x)$ with principal ring of integers have been determined (see [Mr]). The situation in the real case is different however as the class number $h_{\mathcal{O}}$ depends not only on h_F but also on the regulator R. We will present algorithms for computing both h_F and R.

2.3 Continued fractions in real quadratic function fields

We will in this section introduce the theory of continued fractions in function fields analogous to that of classical number theory. The high-point of this section will be the computation of

the fundamental unit and regulator by means of continued fractions, a method first shown in the function field case in [Ar]. A more recent treatment of this subject can be found in [St2]. Once again we deal here only with the odd characteristic case, although very similar results hold in the even characteristic case as well. See R. Zuccherato's paper [Zu], where the even characteristic theory is developed and where it is also shown that continued fraction algorithm yields the fundamental unit and regulator.

2.3.1 Definitions and basic results

We keep the notation as above. $F = \mathbb{F}_q(x, \sqrt{D})$ is a real quadratic function field where we assume that $2 \nmid q$. Let $\mathcal{O} = \mathbb{F}_q[x, \sqrt{D}]$ denote the ring of integers and $\mathcal{O}^* = \mathbb{F}_q^* \langle \epsilon \rangle$, with ϵ a fundamental unit. Let $\{P_\infty, \bar{P}_\infty\}$ be the primes lying above ∞ and let v_{P_∞} and $v_{\bar{P}_\infty}$ denote the corresponding valuations. The classical way of computing the regulator is based on the continued fraction expansion of $\alpha = \sqrt{D}$. We let $L := \mathbb{F}_q(x)_\infty$ be the completion of $\mathbb{F}_q(x)$ with respect to the prime at infinity. Because F is real, it will be a subfield of L just as in the classical case. Since $\frac{1}{x}$ is a uniformizing parameter at ∞, L will be the field of Laurent series in $\frac{1}{x}$. Moreover we have the following:

$$F_{P_\infty} \cong F_{\bar{P}_\infty} \cong \mathbb{F}_q(x)_\infty = \mathbb{F}_q((\frac{1}{x})) = L$$

For an element $\alpha \in L = \mathbb{F}_q((\frac{1}{x}))$ such that $0 \neq \alpha = \sum_{i=-\infty}^{m} c_i x^i$ and $c_m \neq 0$, we define

$$\left\{ \begin{array}{l} \deg(\alpha) := m \\ |\alpha| := q^m \\ sgn(\alpha) := c_m \\ \lfloor \alpha \rfloor := \sum_{i=0}^{m} c_i x^i \text{ ('polynomial part')} \end{array} \right\} \tag{2.2}$$

If m is negative, then naturally the polynomial part $\lfloor \alpha \rfloor = 0$. For completeness, we set $\deg(0) = -\infty$ and $|0| = 0$.

Now we introduce continued fraction expansions in L in the sense of Artin. Let $\alpha \in L$, define

$$\left\{ \begin{array}{ccc} \alpha_0 = \alpha & ; & a_0 = \lfloor \alpha_0 \rfloor \\ \alpha_{i+1} = 1/(\alpha_i - a_i) \text{ if } \alpha_i \neq a_i & ; & a_{i+1} = \lfloor \alpha_{i+1} \rfloor \end{array} \right\}$$

We call α_i the i'th *iterate* of α and a_i the i'th *partial quotient*. It is easily seen that this sequence terminates if and only if α is a rational element. If this sequence does not terminate we will call α an *irrational* element. The analogy with classical continued fractions is clear, for example $\lfloor \cdot \rfloor$ is analogous to the floor function for a real number. Because $\lfloor \alpha \rfloor$ is the unique polynomial such that $|\alpha - \lfloor \alpha \rfloor| < 1$, we note that for each $i \in \mathbb{N}$:

$$\begin{aligned} |\alpha_i| &= |a_i| \text{ (by definition of } a_i \text{ and } |\cdot|) \\ &\geq q \text{ (since } |\alpha_{i+1}| = \frac{1}{|\alpha_i - a_i|} = \frac{1}{q^{-n}} = q^n, n \geq 1) \end{aligned} \tag{2.3}$$

Thus α has the following representation

$$\alpha := [a_0, a_1, ...] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

As in the classical case, we define:

$$\left\{ \begin{array}{ccc} p_{-2} := 0 & ; & q_{-2} := 1 \\ p_{-1} := 1 & ; & q_{-1} := 0 \\ p_i := a_i p_{i-1} + p_{i-2} & ; & q_i := a_i q_{i-1} + q_{i-2} \ (i \in \mathbb{N}_0) \end{array} \right\}$$

By induction we derive the following well known properties:

$$|q_i| > |q_{i-1}| \text{ and } |q_i| \geq q^i \ (i \in \mathbb{N}_0) \tag{2.4}$$

$$\frac{p_i}{q_i} = [a_0, a_1, ..., a_i]$$

$$\alpha = \frac{p_i\alpha_{i+1} + p_{i-1}}{q_i\alpha_{i+1} + q_{i-1}}, \text{ equivalently } \alpha_{i+1} = -\frac{q_{i-1}\alpha - p_{i-1}}{q_i\alpha - p_i} \ (i \geq -1) \tag{2.5}$$

$$q_ip_{i-1} - p_iq_{i-1} = (-1)^i \ (i \geq -1) \tag{2.6}$$

$$\alpha - \frac{p_i}{q_i} = \frac{(-1)^i}{q_i(q_i\alpha_{i+1} + q_{i-1})} \ (i \geq -1) \tag{2.7}$$

$$\left|\alpha - \frac{p_i}{q_i}\right| = \frac{1}{|q_iq_{i+1}|} \ (i \geq -1) \tag{2.8}$$

$$|p_{i+1} - q_{i+1}\alpha| < |p_i - q_i\alpha| \ (i \geq -1) \tag{2.9}$$

For example let us show that (2.5) holds. For $i = -1$, we have:

$$\frac{p_i\alpha_{i+1} + p_{i-1}}{q_i\alpha_{i+1} + q_{i-1}} = \frac{p_{-1}\alpha_0 + p_{-2}}{q_{-1}\alpha_0 + q_{-2}} = \frac{\alpha_0 + 0}{0 + 1} = \alpha_0 = \alpha$$

Suppose that (2.5) holds for a fixed k, i.e.

$$\begin{aligned}
\alpha &= \frac{p_k\alpha_{k+1} + p_{k-1}}{q_k\alpha_{k+1} + q_{k-1}} \\
&= \frac{p_k\frac{1+\alpha_{k+2}a_{k+1}}{\alpha_{k+2}} + p_{k-1}}{q_k\frac{1+\alpha_{k+2}a_{k+1}}{\alpha_{k+2}} + q_{k-1}} \text{ (by definition of } \alpha_{k+2}) \\
&= \frac{p_k + p_k\alpha_{k+2}a_{k+1} + p_{k-1}\alpha_{k+2}}{q_k + q_k\alpha_{k+2}a_{k+1} + q_{k-1}\alpha_{k+2}} \text{ (by definition of } p_{k+1} \text{ and } q_{k+1}) \\
&= \frac{p_k + \alpha_{k+2}(p_ka_{k+1} + p_{k-1})}{q_k + \alpha_{k+2}(q_ka_{k+1} + q_{k-1})} \\
&= \frac{p_{k+1}\alpha_{k+2} + p_k}{q_{k+1}\alpha_{k+2} + q_k} \text{ (by definition of } p_{k+1})
\end{aligned}$$

Therefore by induction the result holds for all $k \geq -1$.

For an $\alpha \in L$, we define the following useful sequence:

$$\theta_1 = 1 \ , \ \theta_{i+1} = \prod_{j=1}^{i} \frac{1}{\alpha_j}, \text{ or recursively by:} \tag{2.10}$$

$$\theta_{i+1} = \frac{\theta_i}{\alpha_i} \ (i \in \mathbb{N}) \tag{2.11}$$

and we derive by induction that:

$$\theta_{i+1} = (-1)^i(p_{i-1} - \alpha q_{i-1}) \ (i \in \mathbb{N}_0) \tag{2.12}$$

The following two results relate arbitrary polynomials $A, B \in \mathbb{F}_q[x]$ to the continued fraction expansion of a monic irrational $\alpha \in L$.

Lemma 2.19 *Let $\alpha \in L$ be a monic irrational. If $A, B \in \mathbb{F}_q[x]$ and $n \geq 0$ such that*

$$|\alpha B - A| < |\alpha q_n - p_n|$$

then $|B| \geq |q_{n+1}|$

Proof. We see that (2.6) implies that there exist $X, Y \in \mathbb{F}_q[x]$ such that

$$\begin{aligned} Xq_n + Yq_{n+1} &= B \\ Xp_n + Yp_{n+1} &= A \end{aligned}$$

If $|Xq_n| \neq |Yq_{n+1}|$ then $|B| = \max(|Xq_n|, |Yq_{n+1}|) \geq |q_{n+1}|$ and we are done. Else we have $|Xq_n| = |Yq_{n+1}|$ which implies $|X| > |Y|$. We now write

$$|\alpha B - A| = |X(\alpha q_n - p_n) + Y(\alpha q_{n+1} - p_{n+1})|$$

Using (2.9) together with $|X| > |Y|$

$$|\alpha B - A| = |X(\alpha q_n - p_n)| \geq |\alpha q_n - p_n|$$

which is a contradiction. This concludes the proof. ■

Lemma 2.20 *Let $\alpha \in L$ be a monic irrational. If $A, B \in \mathbb{F}_q[x]$ are relatively prime elements satisfying*

$$\left|\alpha - \frac{A}{B}\right| < \frac{1}{|B^2|}$$

then $A = ap_n$ and $B = aq_n$ for some $n \geq 0$ and some $a \in \mathbb{F}_q^*$ where p_n, q_n arise out of the continued fraction expansion of α.

Proof. Let $A, B \in \mathbb{F}_q[x]$ be relatively prime elements satisfying the above inequality. Fix n so that $|q_n| \leq |B| < |q_{n+1}|$ (This is possible from (2.4)). Then the contrapositive of Lemma 2.19 above requires that

$$|\alpha B - A| \geq |\alpha q_n - p_n|$$

By assumption we have

$$|\alpha B - A| < \frac{1}{|B|}$$

and combining the above two equations and dividing by q_n we obtain

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{|Bq_n|}$$

Suppose now the conclusion doesn't hold. Then since (2.6) forces p_n and q_n to be relatively prime, it follows that $Bp_n - Aq_n$ is non-zero and we have

$$\begin{aligned}
\frac{1}{|Bq_n|} &\leq \frac{|Bp_n - Aq_n|}{|Bq_n|} \\
&= \left|\frac{p_n}{q_n} - \frac{A}{B}\right| \\
&\leq \max\left(\left|\alpha - \frac{p_n}{q_n}\right|, \left|\alpha - \frac{A}{B}\right|\right) \\
&< \max\left(\frac{1}{|Bq_n|}, \frac{1}{|B^2|}\right) \\
&\Rightarrow |B| < |q_n|
\end{aligned}$$

and this contradiction proves the lemma. ■

In contrast to real quadratic function fields where the computation of the period of the continued fraction expansion plays the most important role, the so called quasi-period plays a more important role for reasons which will become apparent later. We distinguish between two forms of periodic behaviour. Let $\alpha \in L$. We say the continued fraction expansion of α is *quasi-periodic* if there exist integers $\gamma > \gamma_0 \geq 0$ and a constant $c \in \mathbb{F}_q^*$ such that

$$\alpha_\gamma = c\alpha_{\gamma_0} \tag{2.13}$$

The smallest positive integer $\gamma - \gamma_0$ for which the above holds is called the *quasi-period* of the continued fraction expansion of α. The continued fraction expansion is called *periodic* if the above holds for $c = 1$. In that case the smallest integer $\gamma - \gamma_0$ for which it holds is known as the *period*.

We have the following well known relationship between the period and the quasi-period:

Proposition 2.21 *If the continued fraction expansion of $\alpha \in L$ is periodic with period n, then it is quasi-periodic with period m, and $m \mid n$. Moreover the period and quasi-period start at the same index γ_0, i.e. γ_0 is the minimal non-negative integer such that $\alpha_{\gamma_0+m} = c\alpha_{\gamma_0}$ and $\alpha_{\gamma_0+n} = \alpha_{\gamma_0}$.*

Using the above proposition, we obtain by induction the following helpful lemma:

Lemma 2.22 *If the continued fraction expansion of $\alpha \in L$ is quasi-periodic with quasi- period m, then with γ_0 and c chosen as above, we have that:*

$$\alpha_{i+\lambda m} = c_i^{1+(-1)^m+\ldots+(-1)^{(\lambda-1)m}} \alpha_i \ (i \geq \gamma_0,\ \lambda \geq 0)$$

where $c_i := c^{(-1)^{i-\gamma_0}}$.

To obtain more information about the relation between the period and the quasi-period we distinguish between even and odd periods. The above results immediately give the following:

Corollary 2.23 *Let $\alpha \in L$.*

(1) If the continued fraction expansion of α is quasi-periodic with odd quasi-period m, then it is periodic with period n, and $n = m$ or $n = 2m$.

(2) If the continued fraction expansion of α is periodic with odd period n, then it is quasi-periodic with period $n = m$.

Proof. (1) Choosing $i = \gamma_0$ in the above Lemma we obtain:

$$\begin{aligned} \alpha_{\gamma_0+\lambda m} &= c_{\gamma_0}^{1+(-1)^m+\ldots+(-1)^{(\lambda-1)m}} \alpha_{\gamma_0} \ (\lambda \geq 0) \\ &= c^{1+(-1)^m+\ldots+(-1)^{(\lambda-1)m}} \alpha_{\gamma_0} \end{aligned}$$

If $c = 1$ already then by definition the period is $n = m$. Otherwise with $\lambda = 2$ we have $\alpha_{\gamma_0+2m} = c^{1+(-1)^m}\alpha_{\gamma_0} = c^0\alpha_{\gamma_0} = \alpha_{\gamma_0}$ (since m is odd). And this is the smallest λ for which it holds.

(2) n odd $\Rightarrow$ m odd since $m \mid n$. Now from (1) we must have $n = m$. ■

2.3.2 Real quadratic irrationalities and reduction

We will now consider the continued fraction expansion of expressions of the form:

$$\alpha = \frac{P + \sqrt{\Delta}}{Q} \ (0 \neq Q, P, \Delta \in \mathbb{F}_q[x]) \tag{2.14}$$

where $\alpha \in L \backslash \mathbb{F}_q(x)$, $0 < \deg(\Delta)$ even, Δ square-free in $\mathbb{F}_q[x]$ and $Q \mid (\Delta - P^2)$. We call such an element a *real quadratic irrationality*. In this situation, we set $Q_0 = Q$, $P_0 = P$, $\alpha_0 = \alpha$, $Q_{-1} = (\Delta - P^2)/Q$ and $d = \left\lfloor \sqrt{\Delta} \right\rfloor$. For $i \in \mathbb{N}_0$ we use the recursions:

$$\left\{ \begin{array}{c} P_{i+1} = a_i Q_i - P_i \\ Q_{i+1} = (\Delta - P_{i+1}^2)/Q_i \end{array} \right\} \tag{2.15}$$

We see by induction that:

$$\alpha_i = \frac{P_i + \sqrt{\Delta}}{Q_i} \ (i \in \mathbb{N}_0) \tag{2.16}$$

where $0 \neq Q_i, P_i \in \mathbb{F}_q[x]$ and $Q_i \mid (\Delta - P_i^2)$. We compute $a_i = \lfloor \alpha_i \rfloor$ by

$$a_i = (P_i + d)/Q_i \ (i \in \mathbb{N}_0)$$

From the above recursion we see that:

$$Q_{i+1} = Q_{i-1} + a_i(P_i - P_{i+1}) \ (i \in \mathbb{N}_0)$$

Define $r_i := (P_i + d) \bmod Q_i$, i.e.

$$P_i + d = a_i Q_i + r_i, \text{ where } 0 \leq \deg(r_i) < \deg(Q_i) \ (i \in \mathbb{N}_0) \tag{2.17}$$

We then optimize the formulae as follows:

$$\begin{aligned} P_{i+1} &= d - r_i \ (i \in \mathbb{N}_0) \\ Q_{i+1} &= Q_{i-1} + a_i(r_i - r_{i-1}) \ (i \in \mathbb{N}) \\ a_i &= (P_i + d)/Q_i \ (i \in \mathbb{N}_0) \\ r_i &= (P_i + d) \bmod Q_i \ (i \in \mathbb{N}_0) \end{aligned} \tag{2.18}$$

Also by applying (2.16) to (2.5) and comparing rational and irrational parts we obtain for $i \in \mathbb{N}_0$:

$$\begin{aligned} \Delta q_{i-1} &= P_i(p_{i-1}Q_0 - P_0 q_{i-1}) + Q_i(p_{i-2}Q_0 - P_0 q_{i-2}) \\ Q_0 p_{i-1} &= q_{i-1}P_i + q_{i-2}Q_i + P_0 q_{i-1} \end{aligned}$$

Now taking $\alpha = \sqrt{\Delta}$, i.e. $P_0 = 0$, $Q_0 = 1$, in the above two equations we obtain for $i \in \mathbb{N}_0$:

$$\begin{aligned} \Delta q_{i-1} &= P_i p_{i-1} + Q_i p_{i-2} \\ p_{i-1} &= q_{i-1}P_i + q_{i-2}Q_i \end{aligned}$$

Now using the above two equations we obtain for $i \in \mathbb{N}_0$:

$$\begin{aligned} p_{i-1}^2 - \Delta q_{i-1}^2 &= Q_i(p_{i-1}q_{i-2} - q_{i-1}p_{i-2}) \\ &= Q_i(-1)^i \text{ (from (2.6))} \end{aligned} \tag{2.19}$$

Finally using (2.12), we deduce that

$$N(\theta_{i+1}) = \theta_{i+1}\bar{\theta}_{i+1} = (-1)^i \frac{Q_i}{Q_0} \ (i \in \mathbb{N}_0) \tag{2.20}$$

The following powerful result uses the theory of real quadratic irrationalities to generalize Lemma 2.20.

Theorem 2.24 *Let $\Delta \in \mathbb{F}_q[x] \backslash \mathbb{F}_q$ be monic, square-free and of even degree. Let $N \in \mathbb{F}_q[x]$ satisfy $|N| < \left|\sqrt{\Delta}\right|$. If the equation*

$$A^2 - \Delta B^2 = N$$

has a solution in relatively prime $A, B \in \mathbb{F}_q[x]$ then $N = a^2(-1)^n Q_n$ for some $a \in \mathbb{F}_q^*$ and $n \geq 1$ where Q_n arises from the expansion of $\alpha = \sqrt{\Delta}$.

Proof. Let $A, B \in \mathbb{F}_q[x]$ satisfy $A^2 - \Delta B^2 = N$. Taking norms leads to the equality

$$\left|\sqrt{\Delta} - \frac{A}{B}\right| \left|\sqrt{\Delta} + \frac{A}{B}\right| = \frac{|N|}{|B^2|}$$

At least one of the two norms on the left must be $\geq \left|\sqrt{\Delta}\right|$ (since their sum has norm equal to $\left|\sqrt{\Delta}\right|$) and by adjusting the sign of A we may assume w.l.o.g that $\left|\sqrt{\Delta} + A/B\right| \geq \left|\sqrt{\Delta}\right|$ and hence

$$\left|\sqrt{\Delta} - \frac{A}{B}\right| \leq \frac{|N|}{|B^2|} \frac{1}{\left|\sqrt{\Delta}\right|} < \frac{1}{|B^2|}$$

Now applying Lemma 2.20 with $\alpha = \sqrt{\Delta}$ we see that $A = \pm a p_{n-1}$ and $B = a q_{n-1}$ for some $n \geq 1$ and $a \in \mathbb{F}_q^*$, where the $\pm$ arises out of the possible adjustment to the sign of A. We apply (2.19) to see that

$$A^2 - \Delta B^2 = (\pm a p_{n-1})^2 - \Delta(a q_{n-1})^2 = a^2(-1)^n Q_n$$

■

Definition 2.25 *A real quadratic irrationality α is called reduced if $|\bar{\alpha}| < 1 < |\alpha|$. If $\alpha = (P + \sqrt{\Delta})/Q$ we see that this is the case if and only if*

$$\left|P - \sqrt{\Delta}\right| < |Q| < \left|P + \sqrt{\Delta}\right|$$

Lemma 2.26 *If the real quadratic irrationality α is reduced, then we have*

(1) $|P| = \left|\sqrt{\Delta}\right| = |d|$

(2) $sgn(P) = sgn(\sqrt{\Delta}) = sgn(d)$

(3) $|Q| < \left|\sqrt{\Delta}\right| = \left|P + \sqrt{\Delta}\right|$

The proof of the above Lemma can be found in [Ar], where he also shows that if α_i is reduced for some $i \in \mathbb{N}_0$, then α_j is reduced for $j \geq i$. Combining this with our recursion formula above we obtain the following:

Proposition 2.27 *If in the continued fraction expansion of a real quadratic irrationality α it happens that α_{i_0} is reduced for some $i_0 \geq 0$, then it follows for $i \geq i_0$ that:*

(1) $|P_i| = \left|P_i + \sqrt{\Delta}\right| = \left|\sqrt{\Delta}\right| = |d|$

(2) $sgn(P_i) = sgn(\sqrt{\Delta}) = sgn(d)$

(3) $|a_i Q_i| = \left|\sqrt{\Delta}\right|$. *In particular* $1 < |a_i| \leq \left|\sqrt{\Delta}\right|, 1 \leq |Q_i| < \left|\sqrt{\Delta}\right|$.

It is well known that the continued fraction algorithm can be interpreted as a reduction process. By this we mean that in the expansion of a real quadratic irrationality α there exists an index $i_0 \geq 0$ such that α_i is reduced for all $i \geq i_0$. The next result gives an explicit bound for this index i_0.

Theorem 2.28 *Let α be a real quadratic irrationality. Then α_i is reduced for:*

$$i > i_0 := \max\{0, \frac{1}{2}\deg(Q_0) - \frac{1}{4}\deg(\Delta) + 1\}$$

Proof. Let $i \in \mathbb{N}$ be chosen such that $i > i_0$. First we note that from (2.3) we know that $|\alpha_i| > 1$. Also note now that by definition of i_0 we have that $i > i_0$ is equivalent to:

$$\frac{|Q_0|}{\left|\sqrt{\Delta}\right|} < q^{2i-2}$$

From (2.4) we know that $|q_{i-1}| \geq q^{i-1}$ and therefore

$$|\alpha_0 - \bar{\alpha}_0| = \left|\frac{P_0 + \sqrt{\Delta}}{Q_0} - \frac{P_0 - \sqrt{\Delta}}{Q_0}\right| = \frac{\left|\sqrt{\Delta}\right|}{|Q_0|} > \frac{1}{|q_{i-1}|^2}$$

On the other hand from (2.7) we get that for $i \in \mathbb{N}_0$:

$$(-1)^i(\alpha - \bar{\alpha}) = \frac{1}{q_{i-1}(q_{i-1}\bar{\alpha}_i + q_{i-2})} - \frac{1}{q_{i-1}(q_{i-1}\alpha_i + q_{i-2})}$$

Assuming that α_i is not reduced, i.e. $|\bar{\alpha}_i| \geq 1$, we have that

$$|q_{i-1}\alpha_i + q_{i-2}| = |q_{i-1}\alpha_i| \text{ and } |q_{i-1}\bar{\alpha}_i + q_{i-2}| = |q_{i-1}\bar{\alpha}_i|$$

Hence

$$\begin{aligned} |\alpha_0 - \bar{\alpha}_0| &\leq \max\{\frac{1}{|q_{i-1}|\,|q_{i-1}\bar{\alpha}_i + q_{i-2}|}, \frac{1}{|q_{i-1}|\,|q_{i-1}\alpha_i + q_{i-2}|}\} \\ &= \frac{1}{|q_{i-1}|^2}\max\{\frac{1}{|\bar{\alpha}_i|}, \frac{1}{|\alpha_i|}\} \\ &\leq \frac{1}{|q_{i-1}|^2} \ (|\alpha_i| > 1 \text{ and by assumption } |\bar{\alpha}_i| \geq 1) \end{aligned}$$

A contradiction. ■

The next theorem together with the previous results will assert the periodicity of the continued fraction expansion.

Theorem 2.29 *Let α be a real quadratic irrationality and let $i \in \mathbb{N}_0$. Then α_{i+1} is reduced if and only if $|Q_i| < \left|\sqrt{\Delta}\right|$.*

Proof. ($\Rightarrow$) If α_{i+1} is reduced, then by definition $|\bar{\alpha}_{i+1}| < 1 < |\alpha_{i+1}|$. From (2.16) we see that

$$\bar{\alpha}_{i+1} = \frac{P_{i+1} - \sqrt{\Delta}}{Q_{i+1}} \cdot \frac{P_{i+1} + \sqrt{\Delta}}{P_{i+1} + \sqrt{\Delta}} = \frac{-Q_i}{P_{i+1} + \sqrt{\Delta}}$$

Together with Proposition 2.27 this implies

$$\begin{aligned} |Q_i| &= |\bar{\alpha}_{i+1}|\left|P_{i+1} + \sqrt{\Delta}\right| \\ &= |\bar{\alpha}_{i+1}|\left|\sqrt{\Delta}\right| \\ &< \left|\sqrt{\Delta}\right| \end{aligned}$$

($\Leftarrow$) Let $i \in \mathbb{N}_0$ with $|Q_i| < \left|\sqrt{\Delta}\right|$. By Definition 2.25 we have to show that $|\bar{\alpha}_{i+1}| < 1$ or, equivalently, that $\left|P_{i+1} - \sqrt{\Delta}\right| < |Q_{i+1}|$. From (2.18) we have that $P_{i+1} = d - r_i$, and by (2.17) we then obtain that

$$0 \leq |r_i| < |Q_i| < \left|\sqrt{\Delta}\right| = |d|$$

Now because the characteristic of $\mathbb{F}_q$ is odd, we deduce that

$$\left|P_{i+1} + \sqrt{\Delta}\right| = \left|\sqrt{\Delta}\right| = |P_{i+1}|$$

Now substituting into (2.15), we get

$$\begin{aligned} |Q_{i+1}| &= \frac{\left|\Delta - P_{i+1}^2\right|}{|Q_i|} = \frac{\left|\sqrt{\Delta} + P_{i+1}\right|}{|Q_i|} \cdot \left|\sqrt{\Delta} - P_{i+1}\right| \\ &= \frac{\left|\sqrt{\Delta}\right|}{|Q_i|} \cdot \left|\sqrt{\Delta} - P_{i+1}\right| \\ &> \left|\sqrt{\Delta} - P_{i+1}\right| \end{aligned}$$

This completes the proof. ■

This above result together with Proposition 2.27 place bounds on the degree of P_i and Q_i and hence these sequences must repeat at some point ($\mathbb{F}_q$ is finite) which implies that the sequence α_i must repeat since $\alpha_i = (P_i + \sqrt{\Delta})/Q_i$, $i \in \mathbb{N}_0$ (2.16).

We note the following well known fact which is the function field analogue of what can be found in [Pe]:

Theorem 2.30 *The continued fraction expansion of the real quadratic irrationality α is pure periodic, i.e. the period begins at $v_0 = 0$, if and only if α is reduced.*

Finally, we develop properties of the polynomials P_i and Q_i in view of their periodic behaviour. Using Lemma 2.22 applied to (2.16) we obtain:

Proposition 2.31 *If the continued fraction expansion of the real quadratic irrationality α is quasi-periodic with quasi-period m and $v_0 \geq 0$, then we have for $i \geq v_0$ and $\lambda \geq 1$ that*

$$\begin{aligned} P_i &= P_{i+\lambda m} \\ Q_i &= c_i^{1+(-1)^m+\ldots+(-1)^{(\lambda-1)m}} Q_{i+\lambda m} \end{aligned}$$

where $c_i := c^{(-1)^{i-v_0}}$ and $c \in \mathbb{F}_q^*$ is defined as (2.13).

2.3.3 The real quadratic irrationality $\sqrt{\Delta}$

The real quadratic irrationality $\alpha = \sqrt{\Delta}$ plays a particularly important role in the computation of the fundamental unit and regulator of a real quadratic function field. Of course $\alpha = \sqrt{\Delta}$ is a real quadratic irrationality by simply choosing $P = 0$ and $Q = 1$ in (2.14) (Δ is once again assumed square-free). We observe that $\alpha = \sqrt{\Delta}$ is clearly not reduced as $\left|-\sqrt{\Delta}\right| = \left|\sqrt{\Delta}\right|$. Thus from Theorem 2.30 it follows that the period n (and hence also the quasi-period m) of the expansion of α starts at $v_0 = 1$ since α_1 is reduced. We also note the well known fact that $Q_{\lambda n} = Q_n = Q_0 = 1$ for all $\lambda \geq 0$ which will be used in the theorem below.

We have the following important result:

Theorem 2.32 *If the continued fraction expansion of $\alpha = \sqrt{\Delta}$ is periodic with period n and quasi-period m, then $Q_s \in \mathbb{F}_q^*$ if and only if $s = \lambda m$ for some $\lambda \geq 0$.*

Proof. ($\Leftarrow$) Let $s = \lambda m$. If $\lambda = 0$ or $n = m$, then there is nothing to show. Let $n = lm$ where $l \geq 2$. Defining $c_m = c^{(-1)^{m-1}}$, we see from Proposition 2.31 that

$$Q_m = c_m^{1+(-1)^m+\ldots+(-1)^{(\lambda-2)m}} Q_{\lambda m} \ (\lambda \geq 2)$$

Therefore we need only show that $Q_m \in \mathbb{F}_q^*$. But the assertion now follows by choosing $\lambda = l$ which implies $Q_{lm} = Q_n = 1$.

($\Rightarrow$) Let $Q_s \in \mathbb{F}_q^*$. If $s = 0$, then the assertion is true. Therefore let $s \geq 1$. We must show $m \mid s$. First, we know that $P_0 = 0$, $Q_0 = 1$, $a_0 = d = \left\lfloor \sqrt{\Delta} \right\rfloor$, $P_1 = d$, and $Q_1 = \Delta - d^2$. Furthermore, $\alpha_s = (P_s + \sqrt{\Delta})/Q_s = (P_s + \sqrt{\Delta})/c$ is reduced. This means that $|\bar{\alpha}_s| = \left|P_s - \sqrt{\Delta}\right| < 1$. Consequently $P_s = \left\lfloor \sqrt{\Delta} \right\rfloor = d$ and $a_s = 2d/c$. Also $P_{s+1} = d = P_1$ and $Q_{s+1} = Q_1/c$. We get $\alpha_{s+1} = c\alpha_1$ which implies that $m \mid s$. ■

Corollary 2.33 *In the situation of the above theorem we have that*

$$N(\bar{\theta}_{\lambda m+1}) = \bar{\theta}_{\lambda m+1}\theta_{\lambda m+1} = p_{\lambda m-1}^2 - \Delta q_{\lambda m-1}^2 \in \mathbb{F}_q^* \ (\lambda \geq 1)$$

Proof. This follows from (2.12) and (2.19). ■

The following lemma will aid us in the proof of the fact that the continued fraction expansion of $\alpha = \sqrt{\Delta}$ indeed yields the fundamental unit and hence also the regulator.

Lemma 2.34 *Let the continued fraction expansion of $\alpha = \sqrt{\Delta}$ be periodic with period n and quasi-period m. Then for every $\lambda \geq 1$ there exists a constant $c_\lambda \in \mathbb{F}_q^*$ such that*

$$\bar{\theta}_{\lambda m+1} = c_\lambda \bar{\theta}_{m+1}^{\lambda}$$

Proof. From Lemma 2.22 we get for $i \in \mathbb{N}$ that

$$\alpha_{i+\lambda m} = c_i^{1+(-1)^m+\ldots+(-1)^{(\lambda-1)m}} \alpha_i$$

where $c_i := c^{(-1)^{i-1}}$. By (2.10) we derive that

$$\prod_{j=\lambda m+1}^{\lambda m+m} \frac{1}{\bar{\alpha}_j} = \prod_{j=1}^{m} \frac{1}{\bar{\alpha}_{\lambda m+j}} = \hat{c}\bar{\theta}_{m+1}$$

where

$$\hat{c} = \prod_{j=1}^{m} c_j^{-1-(-1)^m-\ldots-(-1)^{(\lambda-1)m}}$$

and the assertion follows by induction. ■

2.3.4 Computation of the fundamental unit and regulator

In this section we use the above theory to demonstrate how we can use the continued fraction expansion of $\alpha = \sqrt{D}$ to compute the fundamental unit and regulator in the real quadratic function field $F = \mathbb{F}_q(x, \sqrt{D})$.

We will make use of the following well known fact from the theory of Dedekind domains:

Remark 2.35 Let A be a Dedekind domain with quotient field k. Let B be the integral closure of A in some finite separable extension F of k. Then $\eta \in B^*$ if and only if $N(\eta) \in A^*$.

Theorem 2.36 *Let $D \in \mathbb{F}_q[x]$ be a monic, square-free polynomial of even degree. Then the continued fraction expansion of $\alpha = \sqrt{D}$ is periodic and quasi-periodic. If m denotes the quasi-period, then*

$$\epsilon = p_{m-1} + q_{m-1}\sqrt{D}$$

is a fundamental unit of $F = \mathbb{F}_q(x, \sqrt{D})$ and

$$\mathcal{O}^* = \mathbb{F}_q^* \left\langle \bar{\theta}_{m+1} \right\rangle = \mathbb{F}_q^* \left\langle p_{m-1} + q_{m-1}\sqrt{D} \right\rangle$$

Proof. The fact that $\bar{\theta}_{m+1} = \pm(p_{m-1} + q_{m-1}\sqrt{D})$ comes from (2.12). We must show that $\mathcal{O}^* = \mathbb{F}_q^* \langle \bar{\theta}_{m+1} \rangle$.

($\supseteq$) From Corollary 2.33 we have that $N(\bar{\theta}_{m+1}) \in \mathbb{F}_q^*$ and hence from the above remark that $\bar{\theta}_{m+1} \in \mathcal{O}^*$.

($\subseteq$) Now let $\eta = U + V\sqrt{D}$, where $U, V \in \mathbb{F}_q[x]$ be an arbitrary unit. If $|\eta| = 1$ the result follows immediately. Suppose firstly that $|\eta| > 1$. Then $N(\eta) = (U + V\sqrt{D})(U - V\sqrt{D}) = c \in \mathbb{F}_q^*$. Hence

$$\begin{aligned} \left|U - V\sqrt{D}\right| &= \frac{|c|}{\left|U + V\sqrt{D}\right|} \text{ or} \\ \left|\frac{U}{V} - \sqrt{D}\right| &= \frac{|c|}{\left|UV + V^2\sqrt{D}\right|} \\ &= \frac{1}{\left|UV + V^2\sqrt{D}\right|} \\ &< \frac{1}{|V^2|} \end{aligned}$$

Now from Lemma 2.20 there exists a $c_0 \in \mathbb{F}_q^*$ and an index $j \geq 1$ such that

$$U = c_0 p_{j-1}, \; V = c_0 q_{j-1}.$$

Thus we obtain:

$$N(\eta) = U^2 - V^2 D = c_0^2(p_{j-1}^2 - q_{j-1}^2 D) = c_0^2(-1)^j Q_j = c \text{ by (2.19)}$$

This means that $Q_j \in \mathbb{F}_q^*$. Hence $j = tm$ for some $t \geq 1$ by Theorem 2.32. Lemma 2.34 now implies that

$$\eta = \hat{c}\bar{\theta}_{m+1}^t$$

with $\hat{c} \in \mathbb{F}_q^*$ and $t \in \mathbb{N}$. If $|\eta| < 1$, then $|\bar{\eta}| = |1/\eta| > 1$, and we use $1/\eta$ instead of η. ■

We now do an explicit calculation of the fundamental unit and regulator of real quadratic function fields of a very specific form.

Example 2.37 The form is the following: The function field $F = \mathbb{F}_q(x, \sqrt{D})$ with $D = A^2 + b$, $A \in \mathbb{F}_q[x]$ and $b \in \mathbb{F}_q^*$. We will say that F is of Chowla type. We show that the regulator of F equals $\deg(A)$. We compute the continued fraction expansion of the real quadratic irrationality $\alpha = \sqrt{D} = \sqrt{A^2 + b}$.

$$\alpha_0 = \sqrt{A^2 + b} \text{ and } a_0 = \left\lfloor \sqrt{A^2 + b} \right\rfloor = A$$

Now

$$\alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{1}{\sqrt{A^2+b} - A} = \frac{\sqrt{A^2+b}+A}{A^2+b-A^2} = \frac{\sqrt{A^2+b}+A}{b}$$

We now see that

$$a_1 = \lfloor \alpha_1 \rfloor = \left\lfloor \frac{\sqrt{A^2+b}+A}{b} \right\rfloor = \frac{2A}{b}$$

Now

$$\alpha_2 = \frac{1}{\alpha_1 - a_1} = \frac{1}{(\sqrt{A^2+b}+A)/b - 2A/b} = \frac{b}{\sqrt{A^2+b}-A} = \frac{b(\sqrt{A^2+b}+A)}{b} = \sqrt{A^2+b}+A$$

and

$$a_2 = \lfloor \alpha_2 \rfloor = \left\lfloor \sqrt{A^2+b}+A \right\rfloor = 2A$$

Finally

$$\alpha_3 = \frac{1}{\alpha_2 - a_2} = \frac{1}{\sqrt{A^2+b}+A-2A} = \frac{\sqrt{A^2+b}+A}{b} = \alpha_1$$

Thus the continued fraction expansion of α is periodic with period $n = 2$. The quasi-period of the expansion is $m = 1$, since $\alpha_2 = (1/b)\alpha_1$. Consequently a fundamental unit of this function field is

$$\epsilon = p_0 + q_0\sqrt{D} = a_0 + \sqrt{D} = A + \sqrt{D}$$

This makes sense as $N(\epsilon) = (A+\sqrt{D})(A-\sqrt{D}) = A^2 - D = b \in \mathbb{F}_q^*$ and it is clear that this ϵ is a non-trivial unit of lowest possible degree. Hence the regulator of F is equal to $\deg(A)$.

We have only developed the basic theory here and have not taken into account computational considerations. See A. Stein's paper [St2] for a more complete overview of this subject. In Section 2.5.3 we will also briefly mention the infrastructure method which is in most cases a more efficient algorithm for the computation of the regulator.

2.4 The Reciprocity law in $\mathbb{F}_q[x]$

In this section we will state the reciprocity law which will aid us in understanding the decomposition of primes in quadratic function fields. In [Ar] a proof of the quadratic reciprocity law in $\mathbb{F}_q[x]$ is given, but we will in fact state the more general d'th power reciprocity law. Elementary proofs following Carlitz can be found in [Ro, Ch 3].

If $0 \neq h \in \mathbb{F}_q[x]$ we define $|h| = q^{\deg(h)}$ and $|0| = 0$. Let $P \in \mathbb{F}_q[x]$ be an irreducible polynomial and $d \in \mathbb{N}$ a divisor of $q-1$. We have the following definition:

Definition 2.38 *If P does not divide h, let $\left(\frac{h}{P}\right)_d$ be the unique element of $\mathbb{F}_q^*$ such that*

$$h^{\frac{|P|-1}{d}} \equiv \left(\frac{h}{P}\right)_d \pmod{P}$$

If $P \mid h$ define $\left(\frac{h}{P}\right)_d = 0$. The symbol $\left(\frac{h}{P}\right)_d$ is called the d'th power residue symbol.

Remark 2.39 Since we will be working mainly with quadratic reciprocity I will make the convention that if the d is omitted, $d = 2$ is assumed. In this case we also assume that q is odd. Then $\left(\frac{h}{P}\right)$ is just like the classical Legendre symbol. We also note that since $h^{(|P|-1)/2}$ is an element of order dividing 2 in $(\mathbb{F}_q[x]/P(x)\mathbb{F}_q[x])^* \cong \mathbb{F}_{q^{\deg(P)}}^*$ it follows that $\left(\frac{h}{P}\right) = \pm 1$ or $\left(\frac{h}{P}\right) = 0$ since -1 is the only element of order 2 in $\mathbb{F}_{q^{\deg(P)}}^*$.

We now come to some of the beautiful properties of the d'th power residue symbol.

Theorem 2.40 *Let $h, g, P \in \mathbb{F}_q[x]$ with P a monic irreducible. The following properties hold:*

(1) $\left(\frac{h}{P}\right)_d = \left(\frac{g}{P}\right)_d$ *if* $h \equiv g \pmod{P}$

(2) $\left(\frac{hg}{P}\right)_d = \left(\frac{h}{P}\right)_d \left(\frac{g}{P}\right)_d$

(3) $\left(\frac{h}{P}\right)_d = 1$ *if and only if* $X^d \equiv h \pmod{P}$ *is solvable*

(4) Let $\zeta \in \mathbb{F}_q^*$ be an element of order dividing d. There exists an $h \in \mathbb{F}_q[x]$ such that $\left(\frac{h}{P}\right)_d = \zeta$

(5) Let $\alpha \in \mathbb{F}_q$. Then $\left(\frac{\alpha}{P}\right)_d = \alpha^{\frac{q-1}{d}\deg(P)}$

(6) Let $P, Q \in \mathbb{F}_q[x]$ be monic irreducible polynomials of degree δ and ν respectively. Then we have the following reciprocity law:

$$\left(\frac{Q}{P}\right)_d = (-1)^{\frac{q-1}{d}\delta\nu} \left(\frac{P}{Q}\right)_d$$

Remark 2.41 We can extend the above definition to arbitrary polynomials $M, N \in \mathbb{F}_q[x]$. If M and N have a common divisor define $\left[\frac{M}{N}\right] = 0$ otherwise we define $\left[\frac{M}{N}\right]$ to be multiplicative in both variables M and N. In this way we obtain the analogue of the classical Jacobi symbol.

2.5 Ideal Theory in quadratic function fields

In this section we develop some of the basic ideal theory in quadratic function fields. Much of the theory, for example the decomposition of primes, is similar to that of quadratic number fields. We will also highlight the important relationship between certain places of a function field and the maximal ideals of holomorphy rings of the function field.

2.5.1 Definitions and basic results

Once again we let $F/\mathbb{F}_q$ be a quadratic function field over $\mathbb{F}_q$ and $\mathcal{O}$ the corresponding be the ring of integers. The first part of this discussion is general and holds in odd and even characteristic. We will make it clear when we come to results which are dependent upon the characteristic. We have remarked several times already that $\mathcal{O}$ is a Dedekind domain and from Proposition 2.4 has finite class number. We will begin by stating the relationship between the prime (hence maximal) ideals of $\mathcal{O}$ and the finite places of F. As we have already remarked the ring $\mathcal{O}$ can be thought of as the ring of S-integers, where S is the set of primes lying above infinity. The relationship of which we are speaking is that there is a 1-1 correspondence between the finite primes of F and the maximal ideals of $\mathcal{O}$ as was shown in Theorem 2.7. This tells us that knowledge of decomposition of primes in the Dedekind domain $\mathcal{O}$ translates to knowledge of decomposition of the primes in the function field F. We will also point out the important correspondence between the fractional ideals of $\mathcal{O}$ and divisors of the function field F. Before we do this we have a few basic definitions. As usual we define:

Definition 2.42 *A fractional ideal of F is a finitely generated $\mathcal{O}$-submodule $\mathfrak{a} \neq 0$ of F.*

Since $\mathcal{O}$ is Noetherian, an $\mathcal{O}$-submodule $\mathfrak{a} \neq 0$ of F is a fractional ideal if and only if there exists a $c \in \mathcal{O}$, $c \neq 0$ such that, $c\mathfrak{a} \subseteq \mathcal{O}$ is an ideal of $\mathcal{O}$. For distinction, when c can be chosen as 1, we will call $\mathfrak{a}$ an *integral ideal.* As usual if $\mathfrak{a} = (\alpha) = \alpha\mathcal{O}$ for some $\alpha \in F^*$, we will call $\mathfrak{a}$ a *principal ideal.* We define the *conjugate ideal* $\bar{\mathfrak{a}}$, to be $\bar{\mathfrak{a}} = \{\bar{\alpha} : \alpha \in \mathfrak{a}\}$. As usual we define the equivalence relation $\mathfrak{a} \sim \mathfrak{b} \Leftrightarrow \exists \alpha \in F^*$ such that $\mathfrak{a} = (\alpha)\mathfrak{b}$. Now by definition we have:

$$Cl(\mathcal{O}) := J_F/\sim = J_F/P_F$$

where J_F, P_F denote the group of fractional ideals and principal ideals of the F respectively.

Let $P(x)$ be a prime (irreducible) of $\mathbb{F}_q[x]$. Then $P(x)\mathcal{O} = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}$, $e_1, e_2 \in \mathbb{N}_0$. We will use the notation $\mathfrak{P} \mid P(x)$ to mean that $\mathfrak{P} \cap \mathbb{F}_q[x] = P(x)$, or simply say that $\mathfrak{P}$ *lies over* $P(x)$. As usual, we define the exponent e_i to be the *ramification index* of $\mathfrak{P}_i$ and the degree of the field extension

$$f_i := [\mathcal{O}/\mathfrak{P}_i : \mathbb{F}_q[x]/P(x)]$$

to be the *inertia degree* or *relative degree.* We recall also the fundamental identity which in the quadratic case says the following:

$$\sum_{i=1}^{m} e_i f_i = 2$$

where m is the number of primes lying above $P(x)$. We note that $m = 1$ or $m = 2$. In the former case, either $e = 1$ and $f = 2$ ($P(x)$ *is inert*), or $e = 2$ and $f = 1$ ($P(x)$ *is ramified*). In the latter case, we will say that $P(x)$ *splits* and naturally $e_i = f_i = 1$, $i = 1, 2$. In the next section we will give precise conditions to determine the behaviour of a prime $P(x)$.

Let $\mathfrak{a}$ be a fractional ideal of F. Then we can write $\mathfrak{a} = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_r^{e_r}$, $e_i \in \mathbb{Z}$ for $i = 1, ..., r$. Using the correspondence of Theorem 2.7, to each prime ideal $\mathfrak{P}_i$ in decomposition of $\mathfrak{a}$, we can associate a prime P_i of F. Then to the ideal $\mathfrak{a}$ we associate the divisor $D = \sum_{i=1}^{r} e_i P_i$. This is the correspondence of which we spoke above. We note that not all divisors D come from fractional ideals, for example the divisor $D = P_\infty$ where P_∞ is an infinite prime.

We note that for each integral $\mathcal{O}$-ideal $\mathfrak{a} \neq (0)$, the order of the finite quotient ring $\mathcal{O}/\mathfrak{a}$ is a q'th power since if $\mathfrak{a} = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_r^{e_r}$, $e_i \in \mathbb{N}$ for $i = 1, ..., r$, then by the Chinese remainder theorem $\mathcal{O}/\mathfrak{a} \cong \oplus_{i=1}^{r}(\mathcal{O}/\mathfrak{P}_i)^{e_i}$ and $|\mathcal{O}/\mathfrak{P}_i| = q^{n_i}$ (since $\mathcal{O}/\mathfrak{P}_i$ is a finite extension of $\mathbb{F}_q[x]/(\mathfrak{P}_i \cap \mathbb{F}_q[x])$) for each $i = 1, ..., r$. When $|\mathcal{O}/\mathfrak{a}| = q^m$ we define the *degree* or *absolute norm* of $\mathfrak{a}$ to be

$$\deg \mathfrak{a} := \log_q |\mathcal{O}/\mathfrak{a}| = m$$

This coincides with the definition of the degree of the divisor associated to $\mathfrak{a}$, as by Theorem 2.7 we know that $\mathcal{O}/(P \cap \mathcal{O}) \cong \mathcal{O}_P/P$ for any finite prime P.

We now come to some properties and results regarding ideals of $\mathcal{O}$ shown in [Ar]. These results are specific to the odd characteristic case, and hence we suppose that $2 \nmid q$ for the rest of this section. Firstly every $\mathbb{F}_q[x]$-basis for an integral ideal $\mathfrak{a}$ consists of two elements $\{\omega_1, \omega_2\}$. A non-zero subset $\mathfrak{a}$ of $\mathcal{O}$ is an integral ideal if and only if there exist $S, P, Q \in \mathbb{F}_q[x]$ with $Q \mid D - P^2$ such that:

$$\mathfrak{a} = [SQ, SP + S\sqrt{D}]$$

We say that an integral $\mathcal{O}$-ideal $\mathfrak{a}$ is *primitive* if S can be chosen to be 1, i.e. if:

$$\mathfrak{a} = [Q, P + \sqrt{D}]$$

and $Q \mid D - P^2$. An $\mathbb{F}_q[x]$-basis can be chosen in so called *adapted* form, meaning that

$$\mathfrak{a} = [T, R + S\sqrt{D}] \ (T, R, S \in \mathbb{F}_q[x])$$

where $\deg(R) < \deg(T)$. If $sgn(T) = sgn(S) = 1$, then the adapted representation is unique.

We define the *norm* of $\mathfrak{a} = [\omega_1, \omega_2]$, $N(\mathfrak{a}) \in \mathbb{F}_q[x]$, via

$$\begin{vmatrix} \omega_1 & \omega_2 \\ \bar{\omega}_1 & \bar{\omega}_2 \end{vmatrix}^2 = c^2 (N(\mathfrak{a}))^2 D$$

where $c \in \mathbb{F}_q^*$ is chosen so that $sgn(N(\mathfrak{a})) = 1$, i.e. we have $N(\mathfrak{a}) = (\omega_1\bar{\omega}_2 - \omega_2\bar{\omega}_1)/c\sqrt{D}$ and $N(\mathfrak{a})$ is monic. This definition is independent of the $\mathbb{F}_q[x]$-basis chosen for $\mathfrak{a}$. By definition of the norm of an ideal, we have that

$$\deg \mathfrak{a} = \deg(N(\mathfrak{a}))$$

Morever, for two integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ we have that:

$$\mathfrak{a}\bar{\mathfrak{a}} = (N(\mathfrak{a})) \tag{2.21}$$

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$$

$$N(\mathfrak{a}) = cN(\alpha), \ c \in \mathbb{F}_q^* \text{ when } \mathfrak{a} = \alpha\mathcal{O} \text{ is principal} \tag{2.22}$$

An integral $\mathcal{O}$-ideal $\mathfrak{a}$ is called *reduced* if there exists an $\mathbb{F}_q[x]$-basis $\{Q, P + \sqrt{D}\}$ of $\mathfrak{a}$ with $Q, P \in \mathbb{F}_q[x]$, $Q \mid D - P^2$ and

$$\left|P - \sqrt{D}\right| < |Q| = |N(\mathfrak{a})| < \left|P + \sqrt{D}\right|$$

We note that it is always true that $|Q| = |N(\mathfrak{a})|$ since

$$N(\mathfrak{a}) = \frac{Q(P - \sqrt{D}) - Q(P + \sqrt{D})}{c\sqrt{D}} = -\frac{2}{c}Q$$

Moreover from Definition 2.14 it follows that $\mathfrak{a}$ being reduced is equivalent to $(P + \sqrt{D})/Q$ being a reduced real quadratic irrationality. It also follows from the definition that a reduced ideal is primitive. In this case the $\mathbb{F}_q[x]$-basis $\{Q, P + \sqrt{D}\}$ is called a *reduced basis* for $\mathfrak{a}$. If $sgn(Q) = 1$, then this reduced basis is unique.

2.5.2 Decomposition of primes

The decomposition of primes in our situation is analogous to the decomposition of primes in the ring of integers of a quadratic number field. Recall that we have already characterized how the infinite primes decompose, so we deal here only with the finite primes. We begin with the odd characteristic case, so suppose the $k = \mathbb{F}_q$ is of odd characteristic. We have the following characterization found in [Ar]:

Theorem 2.43 *Let $P(x) \in k[x]$ be a monic irreducible.*

(1) $P(x)$ ramifies in F if and only if $P(x) \mid D(x)$. Thus $P(x)\mathcal{O} = \mathfrak{P}^2$.

(2) If $P(x) \nmid D(x)$ and $\left(\frac{D}{P}\right) = 1$ then $P(x)$ splits. Moreover, since the extension is Galois, we know that σ actss transitively on the set of primes lying above $P(x)$ (see [St, Th. III.7.1]). Thus $P(x)\mathcal{O} = \mathfrak{P}\bar{\mathfrak{P}}$.

(3) If $P(x) \nmid D(x)$ and $\left(\frac{D}{P}\right) = -1$ then $P(x)$ remains prime (inert) in F. Thus $P(x)\mathcal{O} = \mathfrak{P}$.

We now come to the even characteristic case, so suppose the $k = \mathbb{F}_q$ is of even characteristic. See [Lb1] for a proof of the following result:

Theorem 2.44 *Let $F = k(x, y)$ be a quadratic function field where x, y satisfy $y^2 + h(x)y + f(x) = 0$. Let k_r denote the extension of degree r of k and set $k_0 = \mathbb{F}_2$. Denote by tr_{k_r/k_0} the usual trace of k_r over k_0. Let $P(x) \in k[x]$ be some monic irreducible.*

(1) $P(x)$ ramifies in F if and only if $P(x) \mid h(x)$. Thus $P(x)\mathcal{O} = \mathfrak{P}^2$.

(2) If $P(x) \nmid h(x)$, suppose that $P(x)$ is of degree r and c is a root of $P(x)$ in k_r. Then $P(x)$ splits if and only if

$$tr_{k_r/k_0}\left(\frac{f(c)}{h(c)^2}\right) = 0$$

Moreover, since the extension is Galois, we know that σ acts transitively on the set of primes lying above $P(x)$ (see [St, Th. III.7.1]). Thus $P(x)\mathcal{O} = \mathfrak{P}\bar{\mathfrak{P}}$.

(3) If $P(x) \nmid h(x)$, suppose that $P(x)$ is of degree r and c is a root of $P(x)$ in k_r. $P(x)$ remains prime (inert) in F if and only if

$$tr_{k_r/k_0}\left(\frac{f(c)}{h(c)^2}\right) = 1$$

Thus $P(x)\mathcal{O} = \mathfrak{P}$.

2.5.3 The Minkowski bound and Infrastructure

Let $F = \mathbb{F}_q(x, \sqrt{D})$ be a real quadratic function field where we assume once again that $2 \nmid q$. We come now to a result which may be interpreted as the Minkowski bound in real quadratic function fields. When one proves the finiteness of the class number of a number field $K/\mathbb{Q}$ we rely on the fact that every integral ideal $\mathfrak{a}$ is equivalent to an integral ideal $\mathfrak{b}$ with $N(\mathfrak{b}) \leq M = \frac{n!}{n^n}(\frac{4}{\pi})^s\sqrt{|d_K|}$ (M the Minkowski bound). It is shown in [St1] that every integral $\mathcal{O}$-ideal $\mathfrak{a}$ is equivalent to a reduced $\mathcal{O}$-ideal $\mathfrak{b}$, which together with the following result can be used to give another proof of the finiteness of the class number in the real quadratic case.

Theorem 2.45 *A primitive $\mathcal{O}$-ideal $\mathfrak{a}$ is reduced if and only if*

$$|N(\mathfrak{a})| < \left|\sqrt{D}\right|$$

Proof. ($\Rightarrow$) If $\mathfrak{a}$ is reduced, then $\mathfrak{a} = [Q, P + \sqrt{D}]$ with $P, Q \in \mathbb{F}_q[x], Q \mid D - P^2$ and

$$\left|P - \sqrt{D}\right| < |Q| = |N(\mathfrak{a})| < \left|P + \sqrt{D}\right|$$

This can only happen if $|P| = \left|\sqrt{D}\right|$ and even their leading coefficients must be equal. Thus

$$|N(\mathfrak{a})| < \left|P + \sqrt{D}\right| = \left|\sqrt{D}\right|$$

($\Leftarrow$) Suppose $\mathfrak{a}$ is primitive with $|N(\mathfrak{a})| < \left|\sqrt{D}\right|$, then $\mathfrak{a} = [Q, P+\sqrt{D}]$ with $P, Q \in \mathbb{F}_q[x], Q \mid D - P^2$. We set

$$P' := P - \left\lfloor \frac{P - \sqrt{D}}{Q} \right\rfloor Q$$

Clearly also $\mathfrak{a} = [Q, P'+\sqrt{D}]$ since $\left\lfloor (P - \sqrt{D})/Q \right\rfloor Q$ lies in the ideal. Moreover $\left|P' - \sqrt{D}\right| < |Q|$ since

$$\left|\frac{P' - \sqrt{D}}{Q}\right| = \left|\frac{P - \sqrt{D}}{Q} - \left\lfloor \frac{P - \sqrt{D}}{Q} \right\rfloor\right| < 1$$

Finally, using our assumption

$$\left|P' + \sqrt{D}\right| = \left|(P' - \sqrt{D}) + 2\sqrt{D}\right| = \left|\sqrt{D}\right| > |Q|$$

We also easily see that $Q \mid D - (P')^2$ and hence that $\{Q, P' + \sqrt{D}\}$ is a reduced $\mathbb{F}_q[x]$-basis for $\mathfrak{a}$. ■

Since F is real quadratic, $\deg(D) = 2d$ for some $d \in \mathbb{N}$. As an immediate consequence of the above result, we have the following.

Corollary 2.46 *$h_{\mathcal{O}} = 1$ if and only if all prime ideals of $\mathcal{O}$ with degree $< d$ are principal.*

Proof. This follows from what was mentioned above, namely that every integral $\mathcal{O}$-ideal $\mathfrak{a}$ is equivalent to a reduced $\mathcal{O}$-ideal $\mathfrak{b}$. ■

If the above primitive $\mathcal{O}$-ideal is principal we can in fact say more, namely:

Theorem 2.47 *If a principal $\mathcal{O}$-ideal $\mathfrak{a}$ without factors in $\mathbb{F}_q[x]\backslash\mathbb{F}_q$ satisfies $|N(\mathfrak{a})| < \left|\sqrt{D}\right|$, then $N(\mathfrak{a}) = aQ_i$ for some $a \in \mathbb{F}_q^*$ and $i \geq 1$.*

Proof. $\mathfrak{a}$ being principal implies $\mathfrak{a} = (P+Q\sqrt{D})\mathcal{O}$ for some $P, Q \in \mathbb{F}_q[x]$. Then from (2.22) we see that $N(\mathfrak{a}) = c(P^2 - DQ^2)$ for some $c \in \mathbb{F}_q^*$. Now the assumption implies that

$$\left|P^2 - DQ^2\right| < \left|\sqrt{D}\right|$$

and in order to apply Theorem 2.24 we need only show that P and Q are relatively prime. Suppose $H \in \mathbb{F}_q[x]$ divides both P and Q, then it also divides $P + Q\sqrt{D}$. But this contradicts the fact that $\mathfrak{a}$ was without factors in $\mathbb{F}_q[x]\backslash\mathbb{F}_q$ so H must be an element of $\mathbb{F}_q^*$. Hence P and Q are relatively prime and Theorem 2.24 declares that

$$P^2 - DQ^2 = b^2(-1)^i Q_i$$

for some $i \geq 1$ and $b \in \mathbb{F}_q^*$. Hence $N(\mathfrak{a}) = aQ_i$ for some $i \geq 1$ and $a = b^2c(-1)^i \in \mathbb{F}_q^*$ as required. ■

The process of reducing ideals is very similar to that of reduction of real quadratic irrationalities. Reduction of a primitive ideal $\mathfrak{a}$ is done by applying the continued fraction algorithm to the real quadratic irrationality $\alpha = (P + \sqrt{D})/Q$ (where $\{Q, P + \sqrt{D}\}$ is an $\mathbb{F}_q[x]$-basis for the ideal $\mathfrak{a}$). It is shown in [St1] that the continued fraction algorithm applied to a reduced ideal produces all equivalent, reduced ideals. Therefore in each $\mathcal{O}$-ideal class we have precisely one cycle of reduced ideals. Since $\mathbb{F}_q$ is finite, this cycle will be finite. The continued fraction algorithm applied to any primitive $\mathcal{O}$-ideal class yields a reduced $\mathcal{O}$-ideal in the same class after a finite number of steps and then produces all reduced ideals in that class. In this way each ideal class can be represented by exactly one cycle of reduced ideals. Basically one has a structure (the cycle of reduced ideals) within a structure (the ideal class group). This concept is called the *infrastructure* in real quadratic function fields and is due to D. Shanks [Sh]. These considerations correspond to the observations made in real quadratic number fields, see for

example [Co]. We can then define a distance function δ between equivalent, reduced, integral $\mathcal{O}$-ideal's. Now using Shank's baby-step giant-step idea we obtain an efficient algorithm for computing the regulator of $\mathcal{O}$. See [St1] for an overview of the infrastructure method in odd characteristic and [Zu] for the even characteristic case. I will touch on this again in Chapter 4.

2.6 The function field Riemann hypothesis

I will state several results here for completeness as they will be used in several places later on. Concise proofs following Bombieri can be found in [St, Ch V]. I will first give several other useful results before that of the Hasse-Weil theorem itself. Let $F/\mathbb{F}_q$ be a function field of genus g over $\mathbb{F}_q$. We define the numbers

$$A_n := |\{A \in \mathcal{D}_F : A \geq 0 \text{ and } \deg(A) = n\}|$$

For example, $A_0 = 1$ and A_1 is the number of places $P \in S(F/\mathbb{F}_q)$ of degree 1. We have the following helpful lemma:

Lemma 2.48 *(1) For a fixed divisor class $[C] \in Cl_F$, we have*

$$|\{A \in [C] : A \geq 0\}| = \frac{1}{q-1}(q^{\dim[C]} - 1)$$

(2) For any integer $n > 2g - 2$,

$$A_n = \frac{h}{q-1}(q^{n+1-g} - 1)$$

Finally we have the celebrated:

Theorem 2.49 (Hasse-Weil) *The zeta function of F,*

$$Z_F(t) = \sum_{A \in \mathcal{D}_F, A \geq 0} \mathcal{N}(A)^{-t} = \sum_{A \in \mathcal{D}_F, A \geq 0} q^{-t \deg(A)}$$

has the following properties:

(1) $Z_F(t) = (1-t)^{-1}(1-qt)^{-1}L_F(t) = (1-t)^{-1}(1-qt)^{-1}\prod_{i=1}^{2g}(1-\alpha_i t)$ where $\alpha_1, ..., \alpha_{2g}$ are algebraic integers and they can be arranged such that $\alpha_i \alpha_{g+i} = q$.

(2) $L_F(t) = 1 + (N - (q+1))t + ... + q^g t^{2g}$ where $N = |\{P \in S(F/\mathbb{F}_q) : \deg P = 1\}|$

(3) $L_F(1) = h$, *the class number of* $F/\mathbb{F}_q$.

(4) $|\alpha_i| = q^{\frac{1}{2}}$ *for* $i = 1, ..., 2g$.

Let $F_r = F\mathbb{F}_{q^r}$ *be the constant field extension and let* $Z_r(t)$ *and* $L_r(t)$ *be the respective zeta function and L-polynomials. Then*

(5) $Z_r(t) = (1-t)^{-1}(1-q^r t)^{-1} L_r(t) = (1-t)^{-1}(1-q^r t)^{-1} \prod_{i=1}^{2g}(1-\alpha_i^r t)$

An immediate consequence of this is the following useful result:

Theorem 2.50 (Hasse-Weil Bound) *The number* $N = N(F)$ *of places of* $F/\mathbb{F}_q$ *of degree one can be estimated by*

$$|N - (q+1)| \leq 2gq^{\frac{1}{2}}$$

2.7 The class number of a quadratic function field

It was Artin who in his thesis first gave an analytic formula for the class number of a quadratic function field. We will shortcut most of his work by using the deep results of the previous section on the Hasse-Weil theorem. It was in fact Artin who first saw hints that the Hasse-Weil theorem may hold in quadratic function fields from some of his computational results. Let $F = \mathbb{F}_q(x, \sqrt{D})$ be a quadratic function field of genus g over $\mathbb{F}_q$ where $2 \nmid q$. Let $Z(t) := Z_F(t)$ be the Zeta function of F. We will make use the well known Euler product representation of $Z(t)$:

$$Z(t) = \prod_{P \in S(F/\mathbb{F}_q)} (1 - t^{\deg P})^{-1}$$

Now we wish to express $Z(t)$ as a product ranging over all monic irreducibles P in $\mathbb{F}_q[x]$. We will do so by making use of our knowledge of the decomposition of primes (Theorem 2.43). By examining the prime lying beneath P for each $P \in S(F/\mathbb{F}_q)$ we derive the following:

$$Z(t) = G(t) \prod_{P \in \mathbb{F}_q[x] \text{ monic, prime}} (1 - t^{\deg P})^{-1}(1 - \left(\frac{D}{P}\right) t^{\deg P})^{-1}$$

the factor $G(t)$ coming from the prime at infinity. The product of the first factors is:

$$\prod_{P\in\mathbb{F}_q[x]}(1-t^{\deg P})^{-1}=\sum_{M\in\mathbb{F}_q[x]\text{ monic}}t^{\deg M}=\sum_{m\geq 0}q^m t^m=\frac{1}{1-qt}$$

The product of the remaining factors is:

$$\begin{aligned}\prod_{P\in\mathbb{F}_q[x]}(1-\left(\frac{D}{P}\right)t^{\deg P})^{-1} &= \sum_{M\in\mathbb{F}_q[x]\text{ monic}}\left[\frac{D}{M}\right]t^{\deg M} \quad (\left[\frac{D}{M}\right]\text{ the Jacobi symbol})\\ &= \sum_{m\geq 0}\sigma_m t^m \quad \text{where } \sigma_m=\sum_{\deg M=m}\left[\frac{D}{M}\right]\end{aligned}$$

We must now investigate the factor $G(t)$ which will be dependent on the prime at infinity, i.e. on whether or not F is real or imaginary. We have three cases to consider:

(1) $D(x)$ is of odd degree (F ramified imaginary)

In this case $G(t)=(1-t)^{-1}$ since the prime at infinity is ramified. Now

$$L(t)=(1-t)(1-qt)Z(t)=\sum_{m\geq 0}\sigma_m t^m$$

Since we know that $\deg(L(t))=2g$, we conclude that $\sigma_m=0$ if $m\geq 2g+1$. Hence we have the following elegant formula for the class number:

$$h_F=L(1)=\sum_{m=0}^{2g}\sigma_m$$

(2) $D(x)$ is of even degree with the leading coefficient of D a square in $\mathbb{F}_q^*$ (F real)

In this case $G(t)=(1-t)^{-2}$ since the prime at infinity splits. Now

$$\begin{aligned}L(t) &= (1-t)(1-qt)Z(t)\\ &= \frac{1}{1-t}\sum_{m\geq 0}\sigma_m t^m\\ &= \sum_{m\geq 0}t^m\sum_{m\geq 0}\sigma_m t^m\\ &= \sum_{m\geq 0}(\sum_{i=0}^{m}\sigma_i)t^m\\ &= \sum_{m=0}^{2g}(\sum_{i=0}^{m}\sigma_i)t^m \ (\deg(L(t))=2g)\end{aligned}$$

Hence,

$$\begin{aligned} h_F &= L(1) \\ &= (2g+1)\sigma_0 + 2g\sigma_1 + \ldots + \sigma_{2g} \\ &= (2g+1)\sum_{m=0}^{2g}\sigma_m - \sum_{m=1}^{2g} m\sigma_m \\ &= -\sum_{m=1}^{2g+1} m\sigma_m \end{aligned}$$

Where the terms are arranged so as to coincide with Artin's formula.

(3) $D(x)$ is of even degree with the leading coefficient of D a non-square in $\mathbb{F}_q^*$ (F inert imaginary)

In this case $G(t) = (1-t)^{-1}(1+t)^{-1}$ since the prime at infinity is inert. Now

$$\begin{aligned} L(t) &= (1-t)(1-qt)Z(t) \\ &= \frac{1}{1+t}\sum_{m=0}^{2g}\sigma_m t^m \ (\deg(L(t)) = 2g) \end{aligned}$$

Hence,

$$\begin{aligned} h_F &= L(1) \\ &= \frac{1}{2}\sum_{m=0}^{2g}\sigma_m \end{aligned}$$

We note that we can simplify the computation of h_F by making use of the symmetries given by the functional equation. We also note that the coefficient of t in $L(t)$ equals $N-(q+1)$ where N is the number of places $P \in S(F/\mathbb{F}_q)$ of degree one. This gives us a method for computing the number of places of degree one of F in terms of sums of Jacobi symbols.

Chapter 3

A Geometric perspective and Conjectures

We will now introduce the geometric language of curves and their Jacobians instead of the algebraic language of function fields and ideal class groups. Some of the results in Chapter 2 will be translated into this new language. There are many excellent books describing this dictionary between algebra and geometry, see for example R. Hartshorne's classic [Ha]. We have mainly been following the algebraic approach of Stichtenoth [St]. See for example Fulton [Fu] or Silverman's good introduction [Si] for a more geometric approach to curves. After this brief geometric perspective, we will put forward some very general conjectures regarding extensions of global fields. Using the algebraic geometric dictionary we will be able to formulate the conjectures both algebraically and geometrically.

3.1 Varieties

We will start our geometric exposition with a brief account of affine and projective varieties and will mainly follow the notation and development of ideas in [Si]. Let k, $\bar{k}$ and $G_{\bar{k}/k}$ denote a perfect field, an algebraic closure of k and the Galois group of $\bar{k}$ over k respectively. The assumption that k is perfect does not concern us unduly since we are primarily interested in the case of k being a finite field.

We define $\mathbb{A}^n = \mathbb{A}^n(\bar{k}) = \{P = (x_1, ..., x_n) : x_i \in \bar{k}\}$ to be *affine n-space over* k. The set of

k-rational points in $\mathbb{A}^n$ can be characterized by

$$\mathbb{A}^n(k) = \{P \in \mathbb{A}^n : P^\sigma = P \text{ for all } \sigma \in G_{\bar{k}/k}\}$$

Let $\bar{k}[X] = \bar{k}[X_1, ...X_n]$ be a polynomial ring in n variables, and let $I \subset \bar{k}[X]$ be an ideal. To each such I we associate a subset of $\mathbb{A}^n$,

$$V_I = \{P \in \mathbb{A}^n : f(P) = 0 \text{ for all } f \in I\}$$

We consequently define an *affine algebraic set* to be any set of the form V_I for some ideal I. If V is an affine algebraic set, *the ideal of* V is given by

$$I(V) = \{f \in \bar{k}[X] : \ f(P) = 0 \text{ for all } P \in V\}$$

An affine algebraic set V is *defined over* k if its ideal $I(V)$ can be generated by polynomials in $k[X]$. We denote this by V/k. This being the case, the *set of k-rational points of* V is given by

$$V(k) = V \cap \mathbb{A}^n(k)$$

We also denote by $I(V/k) = I(V) \cap k[x]$ the ideal of V defined over k. We note that by the Hilbert basis theorem all ideals in $\bar{k}[X]$ and $k[X]$ are finitely generated.

An affine algebraic set V is called an *affine variety* if $I(V)$ is a prime ideal in $\bar{k}[X]$. The fact that $I(V)$ is a prime ideal ensures that V is *irreducible*. Let V/k be a variety (defined over k). Then the *affine coordinate ring* of V/K is defined to be

$$k[V] = \frac{k[X]}{I(V/k)}$$

It is an integral domain; and its quotient field, denote $k(V)$, is called the *function field* of V/k. Similarly $\bar{k}[V]$ and $\bar{k}(V)$ are defined by replacing k with $\bar{k}$. Let V be a variety. The *dimension of* V, denoted $\dim(V)$, is the transcendence degree of $\bar{k}(V)$ over $\bar{k}$.

Let V be a variety and $P \in V$. We define an ideal M_P of $\bar{k}[V]$ by

$$M_P = \{f \in \bar{k}[V] : f(P) = 0\}$$

It can be shown that M_P is a maximal ideal and the quotient M_P/M_P^2 is a finite dimensional $\bar{k}$-vector space. A point $P \in V$ is called *non-singular* if and only if $\dim_{\bar{k}} M_P/M_P^2 = \dim V$.

The variety V is called *non-singular* if every point $P \in V$ is non-singular. The *local ring of* V *at* P denoted $\bar{k}[V]_P$ is the localization of $\bar{k}[V]$ at M_P. In other words

$$\bar{k}[V]_P = \{F \in \bar{k}(V) : F = \frac{f}{g} \text{ for some } f, g \in \bar{k}[V] \text{ with } g(P) \neq 0\}$$

Notice that if $F = f/g \in \bar{k}[V]_P$, then $F(P) = f(P)/g(P)$ is well defined. The functions in $\bar{k}[V]_P$ are said to be *regular* (or *defined*) at P.

Working in affine space however has some drawbacks in that we miss 'points at infinity'. For that reason we introduce projective space and projective varieties. We define *projective n-space* over k to be

$$\mathbb{P}^n = \mathbb{P}^n(\bar{k}) = \{(x_0, ..., x_n) \in \mathbb{A}^{n+1} : \text{at least one } x_i \neq 0\} \ / \ \sim$$

where the equivalence relation $\sim$ is given by: $(x_0, ..., x_n) \sim (y_0, ..., y_n)$ if there exists a $\lambda \in \bar{k}^*$ with $x_i = \lambda y_i$ for all i. Such an equivalence class is denoted by $[x_0, ..., x_n]$. The set of *k-rational points in* $\mathbb{P}^n$ is defined to be

$$\mathbb{P}^n(k) = \{[x_0, ..., x_n] \in \mathbb{P}^n : x_i \in k, \ i = 0, ..., n\}$$

A polynomial $f \in \bar{k}[X] = \bar{k}[X_0, ..., X_n]$ is *homogeneous of degree* d if

$$f(\lambda X_0, ..., \lambda X_n) = \lambda^d f(X_0, ..., X_n)$$

for all $\lambda \in \bar{k}$. An ideal $I \subset \bar{k}[X]$ is *homogeneous* if it is generated by homogeneous polynomials. To each homogenous ideal I we associate a subset of $\mathbb{P}^n$,

$$V_I = \{P \in \mathbb{P}^n : f(P) = 0 \text{ for all homogeneous } f \in I\}$$

We define a *projective algebraic set* to be any set of the form V_I for some homogeneous ideal I. If V is a projective algebraic set, the *homogeneous ideal of* V, denoted $I(V)$, is the ideal in $\bar{k}[X]$ generated by

$$\{f \in \bar{k}[X] : f \text{ is homogeneous and } f(P) = 0 \text{ for all } P \in V\}$$

Such a V *is defined over* k, denoted V/k, if its ideal $I(V)$ can be generated by homogeneous polynomials in $k[X]$. This being the case, the set of *k-rational points of* V is the set

$$V(k) = V \cap \mathbb{P}^n(k)$$

A projective algebraic set is called a *projective variety* if its homogeneous ideal $I(V)$ is a prime ideal in $\bar{k}[X]$. Once again, the fact that $I(V)$ is a prime ideal ensures that V is *irreducible*. It is clear that $\mathbb{P}^n$ contains many copies of $\mathbb{A}^n$. For example, for each $0 \leq i \leq n$, there is an inclusion

$$\begin{aligned} \phi_i \quad &: \quad \mathbb{A}^n \to \mathbb{P}^n \\ (x_1, ..., x_n) \quad &\to \quad [x_1, x_2, ..., x_{i-1}, 1, x_i, ..., x_n] \end{aligned}$$

Now let V be an affine algebraic set with ideal $I(V)$, and consider V as a subset of $\mathbb{P}^n$ via the map

$$V \subset \mathbb{A}^n \xrightarrow{\phi_i} \mathbb{P}^n$$

The *projective closure* of V, denoted $\bar{V}$, is the projective algebraic set whose homogeneous ideal $I(\bar{V})$ is generated by

$$\{f^*(X) : f \in I(V)\}$$

where

$$f^*(X_0, ..., X_n) = X_i^d f(\frac{X_0}{X_i}, \frac{X_1}{X_i}, ..., \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, ..., \frac{X_n}{X_i})$$

and $d = \deg(f)$ is the smallest integer for which f^* is a polynomial. We say that f^* *is the homogenization of* f *with respect to* X_i.

We have the following well known result:

(1) Let V be an affine variety. Then $\bar{V}$ is a projective variety and

$$V = \bar{V} \cap \mathbb{A}^n$$

(2) Conversely let V be a projective variety. Then $V \cap \mathbb{A}^n$ is an affine variety, and either

$$V \cap \mathbb{A}^n = \emptyset \text{ or } V = \overline{V \cap \mathbb{A}^n}$$

Finally if an affine (respectively projective) variety V is defined over k, then $\bar{V}$ (respectively $V \cap \mathbb{A}^n$) is also defined over k.

By the above correspondence, most of the important properties of a projective variety V may now be defined in terms of the affine subvariety $V \cap \mathbb{A}^n$. Let V/k be a projective variety. We choose $\mathbb{A}^n \subset \mathbb{P}^n$ so that $V \cap \mathbb{A}^n \neq \emptyset$. Then the *dimension of* V is the dimension of $V \cap \mathbb{A}^n$. Similarly the *function field of* V, denoted $k(V)$, is the function field of $V \cap \mathbb{A}^n$. It can also be

shown that for different choices of embeddings of $\mathbb{A}^n$ in $\mathbb{P}^n$, the different $k(V)$'s are canonically isomorphic.

Now let V be a projective variety, $P \in V$, and choose $\mathbb{A}^n \subset \mathbb{P}^n$ with $P \in \mathbb{A}^n$. Then V is *non-singular* at P if $V \cap \mathbb{A}^n$ is non-singular at P. Like in the affine case, a projective variety V is called *non-singular* if every point $P \in V$ is non-singular. The *local ring of* V at P, denoted $\bar{k}[V]_P$, is the local ring of $V \cap \mathbb{A}^n$ at P. A function $F \in \bar{k}(V)$ is *regular* (or *defined*) at P if it is in $\bar{k}[V]_P$.

3.2 Curves

We are now in a position to define what we mean by a curve.

Definition 3.1 *A curve over k, denoted C/k, is a projective variety of dimension one over k.*

For our purposes we will only consider non-singular curves. Let C/k be such a non-singular curve. In this case the points on C/k are in a 1-1 correspondence with the discrete valuations of the function field $\bar{k}(C)$. Let $P \in C$. The valuation corresponding to P is given by:

$$\begin{aligned} v_P &: \bar{k}[C]_P \to \mathbb{N}_0 \cup \{\infty\} \\ v_P(f) &= \max\{d \in \mathbb{Z} : f \in M_P^d\} \end{aligned}$$

where $v_P(0) = \infty$. Now using $v_P(f/g) = v_P(f) - v_P(g)$, we extend v_P to $\bar{k}(C)$,

$$v_P : \bar{k}(C) \to \mathbb{Z} \cup \{\infty\} \qquad (*)$$

Let's see how these ideas correspond with the intuitive definition of a point as a zero of a given polynomial and a curve as the set of the zero's plus maybe some additional points at infinity.

Example 3.2 To demonstrate this more clearly, suppose that k is an algebraically closed field. Let $G \in k[x, y]$ be an irreducible polynomial of degree > 1 and monic in y. Let F be the function field obtained as the quotient field of $k[x, y]/(G)$. First of all we establish a bijection between the maximal ideals of $k[x, y]/(G)$ and the tuples $(a, b) \in k^2$ with $G(a, b) = 0$. Note

that the maximal ideals in $k[x,y]/(G)$ correspond to maximal ideals in $k[x,y]$ containing G.
Let $a,b \in k$ with $G(a,b)=0$. $P=(x-a,y-b)$ is a maximal ideal in $k[x,y]/(G)$ as $k[x,y]/P$ is isomorphic to k and $G \in P$ since $G(a,b)=0$.
Conversely, let M be a maximal ideal of $k[x,y]/(G)$ and let $\tilde{M}$ be the corresponding maximal ideal in $k[x,y]$ containing G. Set $P=\tilde{M}\cap k[x]$. P is a non-zero prime ideal of $k[x]$, and as k is algebraically closed we have $P=(x-a)$ for some $a \in k$. Consider the image of $\tilde{M}$ in $k[x,y]/(x-a) \cong k[y]$. It is given by $(y-b)$ for some $b \in k$, hence $\tilde{M}=(x-a,y-b)$. As $G \in \tilde{M}$ we have that $G(a,b)=0$ and $M=(x-a,y-b)$.
Now we can associate to the maximal ideal $M=(x-a,y-b)$ the local ring $\mathcal{O}_M=\{\alpha \in F : \alpha$ is defined at $(a,b)\}$ with maximal ideal $\mathcal{M}_M=\{\alpha \in \mathcal{O}_M : \alpha(a,b)=0\}$. The maximal ideal M leads to a discrete valuation if and only if $\mathcal{M}_M$ is a principal ideal. These (a,b) are the non-singular points. If all points are non-singular, i.e. $\mathcal{O}_M$ is a local principal Noetherian domain for all (a,b) with $G(a,b)=0$, then $k[x,y]/(G)$ is a Dedekind domain. Now using $(*)$ above we can associate to each maximal ideal of $k[x,y]/(G)$ a discrete valuation and conversely to each valuation v, a maximal ideal $\mathcal{M}_v=\{\alpha \in F : v(\alpha)>0\}$. Putting this together implies that to each zero of $G(x,y)$ we can associate a maximal ideal, and hence a discrete valuation on the function field F. The set of these valuations is an example of an affine curve. But we are missing some valuations of F, namely those that do not result from $k[x,y]/(G)$ but from other rings contained in F.
Classically, we add points 'at infinity' by considering the solutions of $\tilde{G}(t,y)$ at $t=0$ after the change of variables $t=1/x$. Considering the polynomial ring $k[t,y]/(\tilde{G})$ one obtains the corresponding valuations in the same way as above.

The simplest example of a curve is the projective line $\mathbb{P}^1$ over k. If k is algebraically closed, the finite points on $\mathbb{P}^1$ are in a 1-1 correspondence with k itself. The remaining point at infinity corresponds to the degree valuation on $k(\mathbb{P}^1)=k(x)$.

In our introduction above we have not discussed maps between varieties as we do not need such generality. We are however interested in maps between non-singular curves.

Definition 3.3 *Let C/k and C'/k be two non-singular curves over k. A morphism $\varphi : C \to C'$ of non-singular curves over k is a map given by a homomorphism of k-algebras $\varphi^* : k(C') \to k(C)$ in the following way: if $P \in C$ corresponds to the valuation v_P then $\varphi(P)$ corresponds in C' to the unique discrete valuation attached to the valuation $v_P \circ \varphi^*$.*

The degree of φ is defined to be $[k(C) : \varphi^*(k(C'))]$. If $\varphi^* : k(C') \to k(C)$ is an isomorphism of k-algebras, then the corresponding morphism of curves is called an isomorphism.

We now come to our area of study, namely function fields and their associated curves over a finite field. Let $k = \mathbb{F}_q$ be a finite field, and C/k be a non-singular curve defined over k. In this situation, all the important invariants and properties of the curve C/k are in fact given by those of the function field $k(C)$. For example, the divisor group of the curve is equal to the divisor group of the function field $k(C)$ and the genus of the curve is given by that of the function field. We must take care however in these correspondences as k is not algebraically closed. The *Jacobian* of the curve C/k, which we will denote $\operatorname{Jac} C$, is given by the divisor classes of degree 0 of the function field $\bar{k}(C)$. $\operatorname{Jac} C$ can in fact be given the structure of an *abelian variety* which is canonically isomorphic to $\operatorname{Pic}^0(C)$, but for our purposes the above definition suffices. We will be working primarily with the group of k-rational points of the abelian variety $\operatorname{Jac} C$, which we will denote $\operatorname{Jac} C(k)$. This group is given by the group of divisor classes of degree 0 of the function field $F = k(C)$. We will sometime abuse notation and simply refer to $\operatorname{Jac} C(k)$ as the Jacobian of C. In terms of Definition A.6 we have

$$\operatorname{Jac} C(k) = Cl_F^0$$

and hence

$$h_F = |\operatorname{Jac} C(k)|$$

where h_F is finite since k is finite.

Let S be a finite non-empty subset of $C(k)$ (the set of k-rational points of C). Geometrically, the ring $\mathcal{O}_S = \cap_{P \notin S} \mathcal{O}_P$ of S-integers of F defined in Section 2.1 can be thought of as the ring of functions which are regular on the set $U = C(k) \backslash S$. Define

$$h_S = |Cl(\mathcal{O}_S)|$$

It is well known that if C/k is a non-singular projective curve of genus $g \geq 1$, then there exists an injection $j : C \hookrightarrow \operatorname{Jac} C$, called the *Jacobian embedding* of C. If C has a k-rational point this embedding can be defined over k (see [Mi]). We are in fact interested in an embedding of the k-rational points of C into $\operatorname{Jac} C(k)$. If we assume that C/k has a k-rational point, this embedding can be given explicitly in the following way. Fix a point $P_0 \in C(k)$. Then the map

$$\theta : \left\{ \begin{array}{c} C(k) \to \operatorname{Jac} C(k) \\ P \mapsto [P - P_0] \end{array} \right\}$$

where $[D]$ denotes the class of the divisor D in $\operatorname{Jac} C(k)$, is the desired embedding. We note that in general $C(k)$ is not a group, hence by an embedding we simply mean an injective map. In the case of C being an elliptic curve, the above map becomes an isomorphism (the group law). θ is injective since if $[P - P_0] = [P' - P_0]$, then $P - P' = (z)$ for some $z \in F$. Hence the pole divisor of z, $(z)_\infty$, equals P'. This implies $[F : k(z)] = \deg(z)_\infty = 1$ (see [St, Th. I.4.11]) and therefore $F = k(z)$. We assumed however that $g \geq 1$ so that F is not rational, hence we must have $P = P'$. In the above situation $\theta(S) \subseteq \operatorname{Jac} C(k)$ and one can consider the finite subgroup, denoted $\operatorname{Jac} C_S(k)$, of the group $\operatorname{Jac} C(k)$ generated by $\theta(S)$. Define

$$\rho_S = |\operatorname{Jac} C_S(k)|$$

3.3 Translation of results

Since $S \subset C(k)$ we have that $d = \gcd\{\deg P : P \in S\}$ defined in Section 2.1 equals one. We also see that the subgroup $\operatorname{Jac} C_S(k)$ defined above is in terms of the definitions in Section 2.1 equal to $\mathcal{D}(S)^0/\mathcal{P}(S)$. Hence, the following result is the consequence of the exact sequences obtained in Proposition 2.1.

Proposition 3.4 *If S is a finite non-empty subset of $C(k)$, there is an exact sequence*

$$0 \to \operatorname{Jac} C_S(k) \to \operatorname{Jac} C(k) \to Cl(\mathcal{O}_S) \to 0$$

In particular Schmidt's formula holds

$$h_F = \rho_S h_S$$

This immediately implies:

Corollary 3.5 *The ring $\mathcal{O}_S$ is principal if and only if* $\operatorname{Jac} C(k) = \operatorname{Jac} C_S(k)$, *i.e. the image of S generates* $\operatorname{Jac} C(k)$.

We now describe extensions of a pair (F_0, S_0), where F_0 is a function field over k and S_0 a finite subset of $S(F_0/k)$. A pair (F, S) is called an extension of (F_0, S_0) if F is an extension of F_0

and S is exactly the set of places of F lying over S_0. Let C_0 be the unique (up to isomorphism) non-singular projective curve over k which corresponds to F_0. Then an extension (F, S) of (F_0, S_0) corresponds to a morphism $\pi : C \to C_0$ where C is the curve corresponding to F, in such a way that $\pi^{-1}(S_0) = S$. Such a pair (C, S) together with the map $\pi : C \to C_0$ satisfying the above conditions is called a *covering* of (C_0, S_0).

To demonstrate this new language let us translate some of our knowledge of real quadratic function fields into geometric knowledge of a hyperelliptic curve over k.

Example 3.6 Let $F = k(x, \sqrt{D})$ be a real quadratic function field over k (where we assume k is of odd characteristic). Let $\mathbb{P}^1$ be the projective line over k (the curve corresponding to the rational function field $k(x)$) and let C/k be the non-singular curve corresponding to F. Since F is real we know that there are two primes P_1 and P_2 lying over P_∞. Let $S = \{P_1, P_2\}$. Then there exists a morphism $\pi : C \to \mathbb{P}^1$ such that $\pi^{-1}(P_\infty) = S$ defined by the homomorphism of k-algebras given by $\pi^* : k(x) \hookrightarrow F$. In this way (C, S) becomes a covering of $(\mathbb{P}^1, P_\infty)$. In this specific case the above exact sequence becomes

$$0 \to \langle [P_1 - P_2] \rangle \to \operatorname{Jac} C(k) \to Cl(\mathcal{O}_S) \to 0$$

since $\operatorname{Jac} C_S(k) = \langle \theta(S) \rangle$. From this it immediately follows that the ring of integers $\mathcal{O}_S$ is principal if and only if the Jacobian $\operatorname{Jac} C(k)$ is a cyclic group generated by the class $[P_1 - P_2]$. We also note by the exactness that $\operatorname{Jac} C(k) / \langle [P_1 - P_2] \rangle \cong Cl(\mathcal{O}_S)$, which implies that the order of $Cl(\mathcal{O}_S)$ equals h_F divided by the order of the class $[P_1 - P_2]$. Thus the order of the class $[P_1 - P_2]$ is none other than the regulator of F. We also note that the class $[P_1 - P_2]$ is therefore a torsion point inside $\operatorname{Jac} C(k)$ and the torsion in question is the regulator of F (or of C/k).

3.4 General conjectures in global fields

Recall that algebraic number fields are global fields in characteristic 0, while function fields in one variable over $\mathbb{F}_q$ are global fields in positive characteristic. We focus on global fields in positive characteristic, but examine the more general situation as it is useful to relate problems and conjectures to their original contexts in algebraic number theory. When considering this relationship it is helpful to keep the following diagram in mind:

$$\begin{array}{ccc} \mathcal{O} \subset K & & \mathcal{O} \subset F \\ | & & | \\ \mathbb{Z} \subset \mathbb{Q} & & \mathbb{F}_q[x] \subset \mathbb{F}_q(x) \end{array}$$

Where $\mathcal{O}$ denotes the respective rings of integers. Let us consider pairs (F, S) where F is a global field and S is a finite non-empty set of places of F. In the case of algebraic number fields, we also assume that S contains the set S_∞ of archimedean places of F. The ring of S-integers in any global field F is defined in precisely the same way as Section 2.1, namely

$$\mathcal{O}_S = \{z \in F : v_P(z) \geq 0, \forall P \notin S\} = \bigcap_{P \notin S} \mathcal{O}_P$$

For global fields in characteristic 0 it is a classical result that $\mathcal{O}_S$ is a Dedekind domain with finite class group. In Chapter 2 we showed that the same holds for global fields in positive characteristic. For a fixed pair (F_0, S_0) we will call a pair (F, S) an extension of (F_0, S_0) is F is a field extension of F_0 and S is the exact set of places of F lying above the places in S_0. We start by stating a very general conjecture on global field extensions suggested in [LV].

Conjecture 3.7 *For any pair (F_0, S_0) with $\mathcal{O}_{S_0}$ principal, there are infinitely many extensions (F, S) such that*

(1) All the places of S_0 split completely in K.

(2) The extension F/F_0 is of degree two.

(3) The ring $\mathcal{O}_S$ principal.

If we choose $F_0 = \mathbb{Q}$ and $S_0 = \{P_\infty\}$ where P_∞ is the archimedean place of $\mathbb{Q}$ we obtain the classical conjecture of Gauss since in this case $\mathcal{O}_S$ is nothing other than the ring of integers of the number field F. One can observe that conditions 1 and 3 in the above conjecture are antinomicals: meaning that as S increases there are more and more extensions satisfying condition 3, but it is less and less probable that they will satisfy condition 1. Condition 1 should be thought of as the 'realness' condition, recalling that in the specific case of $S_0 = \{P_\infty\}$ the splitting of P_∞ implies that F is a 'real' field.

3.5 Conjectures in positive characteristic

For the remaining conjectures we will give both an algebraic and geometric formulation using the corresponce determined in the previous section. The following conjecture which is as yet unproved is the exact analogue of the classical Gauss conjecture. Choosing $F_0 = \mathbb{F}_q(x)$ and $S_0 = \{P_\infty\}$ in Conjecture 3.7 we obtain:

Conjecture 3.8 *(Algebraic) For a fixed constant field $\mathbb{F}_q$, there are infinitely many real quadratic function fields $F/\mathbb{F}_q$ whose ring of integers is principal.*

(Geometric) For a fixed constant field $\mathbb{F}_q$, there are infinitely many coverings (C, S) of $(\mathbb{P}^1, \infty)$ such that:

(1) $S = \{P_1, P_2\}$ and $S \subset C(\mathbb{F}_q)$

(2) The covering π is hyperelliptic

(3) The group $\operatorname{Jac} C(k)$ is cyclic, generated by the class $[P_1 - P_2]$.

The above conjecture is believed by most researchers to be out of reach at present (just as its analogy in characteristic 0). It is an example of what is known as a 'vertical' class number problem since we are looking for infinitely many extensions for a fixed constant field $\mathbb{F}_q$, which implies that were such a family $\{F_i : i \in \mathcal{I}\}$ to be found, it would contain function fields F_i of arbitrarly large genus.

We can also formulate what is known as a 'horizontal' class number problem. In this case we begin with a fixed hyperelliptic curve C over $\mathbb{Q}$ given by $y^2 = D(x)$, $D(x) \in \mathbb{Z}[x]$. The conjecture is the following:

Conjecture 3.9 *(Algebraic) There are infinitely many odd primes p for which $\mathbb{F}_p[x, \sqrt{D}]$ has class number one.*

(Geometric) There are infinitely many odd primes p for which

$$\langle [P_1 - P_2] \rangle = \operatorname{Jac} C_p(\mathbb{F}_p)$$

where C_p is the reduction of $C/\mathbb{Q}$ to $\mathbb{F}_p$, and P_1 and P_2 are the points lying above infinity, i.e. the group of $\mathbb{F}_p$-rational points on the Jacobian of C_p is generated by the class $[P_1 - P_2]$.

We will not go into more detail than that given above as it is a divergence from the central theme of this dissertation. A more in depth exposition of the above conjecture can be found in Jing Yu's paper [Yj].

Since Conjecture 3.7 seems to be inaccessible at present, we follow [LV] and formulate some related problems which are a series of weaker versions of that conjecture.

Problem 3.10 *Let (F_0, S_0) be a fixed pair with F_0 an algebraic function field over $\mathbb{F}_q$ and S_0 a non-empty, finite set of places of degree one of F_0, such that the ring $\mathcal{O}_S$ is principal. Then construct infinitely many extensions (F, S) of (F_0, S_0) satisfying the following conditions:*

(1) Either:

A. The places in S are $\mathbb{F}_q$-rational, or

B. All the places in S_0 split completely in F.

(2) We have one of the following:

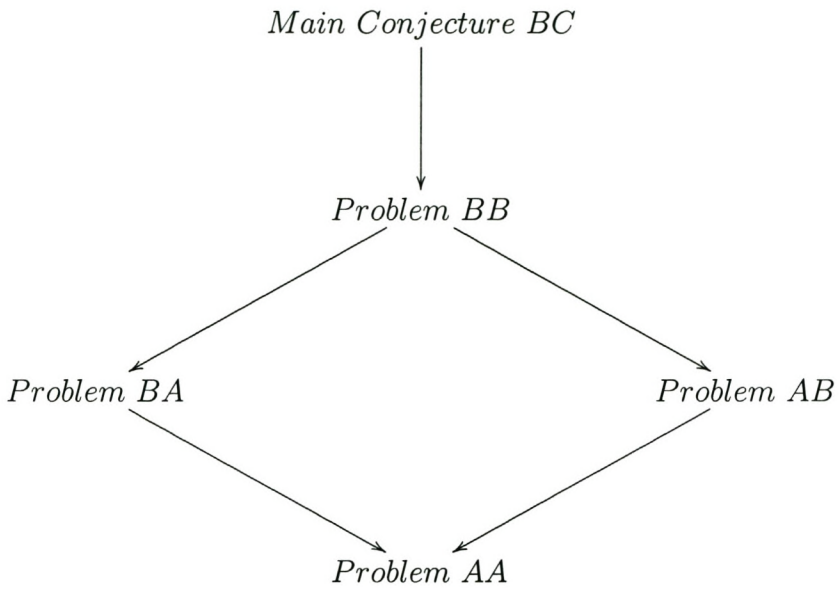
A. The extension F/F_0 is arbitrary (i.e. Galois or not), but the genus of F is positive.

B. The extension F/F_0 is Galois.

C. The extension F/F_0 is of degree two.

(3) The ring $\mathcal{O}_S$ is principal.

We say that Problem XY for (F_0, S_0) has a solution if we are able to construct infinitely many extensions (F, S) satifying conditions $1.X$, $2.Y$ and condition 3. It is clear that Problem BC is precisely that of Conjecture 3.7. Note that the above problem can also easily be translated into geometric language. We have the following diagram of implications:



We will see in Chapter 5 that Problem BB has been solved over certain constant fields. In Chapter 4 we will investigate results which are a step towards solving the more difficult BC Problem.

Chapter 4

Quadratic Function Fields over $\mathbb{F}_q$

In this section I will investigate some deeper results in the arithmetic of quadratic function fields both real and imaginary. We will see that the class number one problem has in fact been solved for imaginary quadratic fields. As far as real quadratic function fields are concerned I will highlight what I believe to be the most important results of the last 30 years. Included amongst these will be a few small results of my own, not because I regard them as the most important by any means, but simply because they are my own. A great deal of work has been done in this area and I apologize for any important results which I may quite easily have omitted. We will begin with a few general results.

4.1 General results

We begin by demonstrating how in certain situations we can move via a birational transformation between real quadratic and imaginary quadratic function fields. This is of particular interest when it comes to computational and numerical considerations. First we examine how a ramified imaginary field can be transformed to a real field:

Proposition 4.1 *Let $F/\mathbb{F}_q$ be a ramified imaginary quadratic function field over $\mathbb{F}_q$, where q is odd. Then $F = \mathbb{F}_q(x, \sqrt{D})$ for some $D(x) = x^{2g+1} + a_{2g}x^{2g} + ... + a_o \in \mathbb{F}_q[x]$, where g is the genus of F. If $q^{\frac{1}{2}} \geq 2g$ then F can be represented as a real quadratic function field over the same constants via the birational transformation:*

$$t = \frac{1}{x - \beta}, \ \tilde{D}(t) = t^{2g+2} D(\beta + \frac{1}{t})$$

for an appropriate $\beta \in \mathbb{F}_q$.

Proof. It is clear that the above transformation is birational. Recalling Theorem 2.13, we need to check that $\tilde{D}(t) = t^{2g+2}D(\beta + \frac{1}{t})$ is of even degree with leading coefficient a square in $\mathbb{F}_q^*$. Now, by the Hasse-Weil bound, the number of $\mathbb{F}_q$-rational points N on $y^2 = D(x)$ is bounded below by:

$$N \geq q + 1 - 2gq^{\frac{1}{2}}$$

if $N \geq 1$, then it is clear that we can find a β such that $\beta^{2g+1} + a_{2g}\beta^{2g} + ... + a_0$ is a square in $\mathbb{F}_q^*$ since the curve $y^2 = D(x)$ has an $\mathbb{F}_q$-rational point. Therefore we want:

$$\begin{aligned} q + 1 - 2gq^{\frac{1}{2}} &\geq 1 \\ q &\geq 2gq^{\frac{1}{2}} \\ q^{\frac{1}{2}} &\geq 2g \end{aligned}$$

which is what we assumed about the relationship between q and the genus. Moreover, we see that:

$$\begin{aligned} \tilde{D}(t) &= t^{2g+2}D(\beta + \frac{1}{t}) \\ &= t^{2g+2}\left[(\beta + \frac{1}{t})^{2g+1} + a_{2g}(\beta + \frac{1}{t})^{2g} + ... + a_0\right] \\ &= (\beta^{2g+1} + a_{2g}\beta^{2g} + ... + a_0)t^{2g+2} + ... + t \end{aligned}$$

and it is clear the $\tilde{D}(t)$ is of even degree. Also, β was chosen above in such a way that the leading coefficient of $\tilde{D}(t)$ is a square in $\mathbb{F}_q^*$. ■

Conversely we now begin with a real quadratic field and show how if we make a certain assumption about the discriminant we can transform the field into an imaginary field. More precisely:

Proposition 4.2 *Let* $F/\mathbb{F}_q$ *be a real quadratic function field over* $\mathbb{F}_q$, *where* q *is odd. Then* $F = \mathbb{F}_q(x, \sqrt{D})$ *for some* $D(x) = x^{2g+2} + a_{2g+1}x^{2g+1} + ... + a_o \in \mathbb{F}_q[x]$, *where* g *is the genus of* F. *If* $D(x)$ *has a root* $\alpha \in \mathbb{F}_q$, *i.e.* F *has a ramified prime of degree one, then* F *can be represented as a ramified imaginary quadratic function field over the same constants via the birational transformation:*

$$t = \frac{1}{x - \alpha}, \ \tilde{D}(t) = t^{2g+2}D(\alpha + \frac{1}{t})$$

Proof. It is clear that the above transformation is birational. Recalling Theorem 2.13, we need to check that $\tilde{D}(t) = t^{2g+2}D(\alpha + \frac{1}{t})$ is of odd degree. We see that:

$$\begin{aligned}
\tilde{D}(t) &= t^{2g+2}D(\alpha + \frac{1}{t}) \\
&= t^{2g+2}\left[(\alpha + \frac{1}{t})^{2g+2} + a_{2g+1}(\alpha + \frac{1}{t})^{2g+1} + ... + a_0\right] \\
&= (\alpha^{2g+2} + a_{2g+1}\alpha^{2g+1} + ... + a_0)t^{2g+2} + ... + 1 \\
&= b_{2g+1}t^{2g+1} + b_{2g}t^{2g} + ... + 1 \text{ (since } D(\alpha) = 0)
\end{aligned}$$

for some $b_i \in \mathbb{F}_q$, $i = 1, ..., 2g+1$. Moreover:

$$\begin{aligned}
b_{2g+1} &= (2g+2)\alpha^{2g+1} + a_{2g+1}(2g+1)\alpha^{2g} + ... + a_1 \\
&= D'(\alpha) \neq 0 \text{ (since } D \text{ is square-free)}
\end{aligned}$$

This proves the result. ■

Let $F = \mathbb{F}_q(x, \sqrt{D})$ be a quadratic function field (real or imaginary) in odd characteristic. The following theorem gives us a condition under which the ideal class group of the ring of integers $\mathcal{O}$ has an element of order n. This useful result was first shown by K. Wang and X. Zhang [WZ2]. We will call a pair $(X, Y) \in \mathbb{F}_q[x] \times \mathbb{F}_q[x]$ *proper* if X and Y are relatively prime.

Theorem 4.3 *The ideal class group of $\mathcal{O} = \mathbb{F}_q[x, \sqrt{D}]$ has a cyclic subgroup of order $n \geq 2$ if and only if the equation*

$$X^2 - DY^2 = cZ^n$$

has a proper solution (X, Y) ($c \in \mathbb{F}_q^*$, $Z \in \mathbb{F}_q[x] \backslash \mathbb{F}_q$), and the equation

$$X^2 - DY^2 = bZ^j$$

has no proper solution (X, Y) ($b \in \mathbb{F}_q^*$, $1 \leq j \mid n$, $j < n$).

Proof. ($\Leftarrow$) Suppose the equation $X^2 - DY^2 = cZ^n$ has a proper solution $X = A$ and $Y = B$. Set $\theta = A + B\sqrt{D}$, then

$$\theta\bar{\theta} = A^2 - DB^2 = cZ^n$$

Suppose that $Z = cP_1^{e_1}...P_r^{e_r}$ is the factorization of Z in $\mathbb{F}_q[x]$ into distinct monic irreducibles, $c \in \mathbb{F}_q^*$. Then for any particular irreducible factor P of Z we have $A^2 \equiv DB^2 (\mathrm{mod}\, P)$. Since D is square-free, $(A, B) = 1$ and $n \geq 2$, we quite easily see that $P \nmid A, P \nmid B$ and $P \nmid D$.

For example if $P \mid A$, then $P \nmid B$ and $P \mid D$; Now from $A^2 - DB^2 \equiv cZ^n (\mathrm{mod}\, P^2)$ we obtain $0 - DB^2 \equiv 0 (\mathrm{mod}\, P^2)$ a contradiction since D is square-free. Therefore we have:

$$\left(\frac{D}{P}\right) = \left(\frac{B^2 D}{P}\right) = \left(\frac{A^2}{P}\right) = 1$$

in other words P is completely split in F. Hence for each $P_i \mid Z$, $i = 1, ..., r$, we have

$$(P_i) = \mathcal{P}_i \bar{\mathcal{P}}_i$$

Therefore we have the following ideal equation

$$(\theta\bar{\theta}) = (Z^n) = (P_1^{e_1} ... P_r^{e_r})^n = (\mathcal{P}_1^{e_1} \bar{\mathcal{P}}_1^{e_1} ... \mathcal{P}_r^{e_r} \bar{\mathcal{P}}_r^{e_r})^n$$

We note that the principal ideal (θ) is relatively prime to $(\bar{\theta})$ since if $(P) \mid (\theta, \bar{\theta})$, then $(P) \mid (\theta + \bar{\theta}, \theta - \bar{\theta}) = (A, BD) = (A, D)$ (since $(A, B) = 1$) which implies that $P \mid D$. But this implies that P ramifies which is contradictory with the fact that all factors of (θ) are splitting. Hence we have

$$(\theta) = I^n$$

where $I = (\hat{\mathcal{P}}_1 ... \hat{\mathcal{P}}_r)$ where $\hat{\mathcal{P}}_i = \mathcal{P}_i$ or $\hat{\mathcal{P}}_i = \bar{\mathcal{P}}_i$ for each $i = 1, ..., r$. Thus I^n is a principal ideal. If $j \mid n$ and I^j is principal, then

$$I^j = (\alpha)$$

for some $\alpha = X_1 + Y_1\sqrt{D} \in \mathcal{O}$. Then

$$(Z)^j = I^j \bar{I}^j = (\alpha\bar{\alpha}) = (X_1^2 - Y_1^2 D)$$

in other words,

$$X_1^2 - Y_1^2 D = c' Z^j$$

for some $c' \in \mathbb{F}_q^*$. Since we have assumed that $X_1^2 - Y_1^2 D = c' Z^j$ $(1 \leq j \mid n,\ j < n)$ has no proper solutions, it follows that I^j is not principal. In other words I generates a cyclic subgroup of order n in the ideal class group of $\mathcal{O}$.

$(\Rightarrow)$ On the other hand if the ideal class group of $\mathcal{O}$ contains a cyclic subgroup of order n, we may assume that it is generated by $[I]$, the ideal class represented by some integral ideal I. Thus we have

$$(I^n) = (\theta)$$

where $\theta = A + B\sqrt{D} \in \mathcal{O}$. Therefore

$$(A^2 - B^2\sqrt{D}) = (\theta\bar{\theta}) = (I\bar{I})^n = (Z^n)$$

where $Z \in \mathbb{F}_q[x]$ is the norm of the ideal I. This simply implies that

$$A^2 - B^2\sqrt{D} = cZ^n$$

for some $c \in \mathbb{F}_q^*$. We also know that $X^2 - Y^2D = c'Z^j$ $(1 \leq j \mid n, j < n)$ has no proper solution for otherwise $[I]$ would generate a subgroup of order j, a contradiction. ■

4.2 The Imaginary case

The imaginary case is divided into three sections. In the first section we present several results which determine all imaginary fields of class number one and two respectively, as well as giving a general outlook on this area of research. In the second section we do some general constructions of imaginary function fields with elements of a specified order in the ideal class group. In the final section we briefly mention some class number relations.

4.2.1 Fields of a given class number

We know that in the classical case of imaginary quadratic number fields the order of the ideal class group grows with the order of the discriminant. This was conjectured by Gauss, but only shown by Heilbronn in 1934. It therefore follows that there are only a finite number of imaginary quadratic fields of a given class number. The problem is now the precise determination of these fields. In the classical case it is known that there are precisely 9 imaginary quadratic number fields with principal ring of integers, the last one being $\mathbb{Q}(\sqrt{-163})$. It is interesting that these 9 examples were given by Gauss, although it was only shown (about which there is some controversy) in 1952 by Heegner that these are the only ones. See [Oe] for a review of that subject. Here we present the analogous situation for function fields.

We recall that a quadratic function field F is called imaginary if the prime at infinity is either inert or ramified in F. In the situation of function fields the class number also tends towards infinity as the order of the discriminant tends towards infinity. This can be seen using the Hasse-Weil theorem which tells us that for a function field F with ring of integers $\mathcal{O}$, the following bound holds

$$h_{\mathcal{O}} = \delta h_F \geq (\sqrt{q} - 1)^{2g}$$

where $\delta = 1$ or $\delta = 2$ depending on whether F is inert or ramified. In either case if $q \geq 5$, the right hand side tends toward infinity as the discriminant (or genus) grows. For $q < 5$ similar bounds can be obtained through other constructions.

The inert imaginary case is not of consequence when examining the class number one problem, as by recalling Proposition 2.17 it is impossible for the ring of integers to be principal. In the ramified case however it is possible for the ideal class number $h_{\mathcal{O}}$ to be one and we will describe precisely when this happens. An important ingredient in this regard will be the function field Riemann hypothesis. To give an idea of how the proof works we will show here the impossibility in the imaginary case of $h_{\mathcal{O}} = h_F = 1$ when $q > 4$. We exclude the trivial case $g = 0$. The proof is as follows:

Theorem 4.4 *Let $F/\mathbb{F}_q$ be a ramified imaginary quadratic function field and $q > 4$. Then $h_{\mathcal{O}} = h_F > 1$.*

Proof. From the function field Riemann hypothesis (Theorem 2.49) we can write

$$L_F(t) = 1 + (N - (q+1))t + ... + q^g t^{2g} = \prod_{i=1}^{2g}(1 - \alpha_i t)$$

Hence

$$h_F = L_F(1) = \prod_{i=1}^{2g}(1 - \alpha_i)$$

Suppose now that $q > 4$. Then for any algebraic integer α with $|\alpha| = q^{\frac{1}{2}}$ we have

$$|1 - \alpha| \geq ||1| - |\alpha|| = \left|1 - q^{\frac{1}{2}}\right| > 1 \text{ (since } \sqrt{q} > 2)$$

Hence $h_F > 1$. ■

The details can be found in [Mr] where all imaginary quadratic fields of class number one are determined using most importantly the beautiful bounds given by the Hasse-Weil theorem. I will list these fields here for completeness:

Theorem 4.5 (MacRae) *There are only four imaginary quadratic extensions $F/\mathbb{F}_q$ of $\mathbb{F}_q(x)$ whose ideal class number is one. These being:*

(1) $q = 4$, $g = 1$: F generated by $y^2 + y + x^3 + a = 0$ where $\langle a \rangle = \mathbb{F}_q^*$,

(2) $q = 3$, $g = 1$: F generated by $y^2 - (x^3 - x - 1) = 0$,

(3) $q = 2$, $g = 2$: *F generated by* $y^2 + y + (x^5 + x^3 + 1) = 0$,

(4) $q = 2$, $g = 1$: *F generated by* $y^2 + y + (x^3 + x + 1) = 0$.

The above result was shown by R.E. Macrae in 1971, but he only determined fields F with class number one having a prime of degree one. A year later M. Madan and C.S. Queen [MQ] showed that up to isomorphism there is exactly one imaginary quadratic field F with class number one having no prime of degree one. This is their result:

Theorem 4.6 *There is up to isomorphism only one imaginary quadratic extension $F/\mathbb{F}_q$ of $\mathbb{F}_q(x)$ having no prime of degree one and whose ideal class number is one. This being:*

$$q = 2,\ g = 2\text{: } F \text{ generated by } y^2 + y = \frac{x^3 + x^2 + 1}{x^3 + x + 1}$$

We now come to the class number 2 problem. In the classical number field case there are exactly 18 imaginary quadratic extensions of $\mathbb{Q}$ with ideal class number 2, a result proved independently by H.M. Stark [Sk] and H.L. Montgomery-P.J. Weinberger [MWe]. The analogous situation in function fields was studied by D. Le Brigand [Lb1]. She determined that there are 13 imaginary quadratic extensions of $\mathbb{F}_q(x)$ having ideal class number 2. By recalling Proposition 2.17 we see that it is possible in the inert imaginary case for the ideal class number to equal 2 (the class number of the function field must then be 1). This is the precise result:

Theorem 4.7 (Le Brigand) *Let $F/\mathbb{F}_q$ be a quadratic function field, n_i the number of places of degree i in F. Up to isomorphism there are 13 imaginary quadratic extensions F such that the class number of the ring of integers of F equals 2. They are obtained for $F = \mathbb{F}_q(x, y)$ where*

(1) in the inert case, $h_F = 1$

g	q		n_1	n_2
1	2	$y^2 + y = (x^3 + x^2 + 1)/(x^3)$	1	
	3	$y^2 = (2x^3 + 2x^2 + 1)/(x^3)$	1	
	4	$y^2 + y = (ax^3 + 1)/(x^3)$ *where* $\langle a \rangle = \mathbb{F}_q^*$	1	
2	2	$y^2 + y = (x^5 + x^2 + 1)/(x^5)$	1	2
		$y^2 + y = (x^3 + x^2 + 1)/(x^3 + x + 1)$	0	3

(2) in the ramified case, $h_F = 2$

g	q		n_1	n_2	n_3
1	2	$y^2 + xy = x^3 + x^2 + 1$	2		
	3	$y^2 = x^3 + 2x + 2$	2		
	4	$y^2 + xy = x^3 + ax + 1$ *where* $\langle a \rangle = \mathbb{F}_q^*$	2		
	5	$y^2 = x^3 + 2x$	2		
2	2	$y^2 + y = (x^3 + x + 1)/(x^2 + x + 1)$	1	3	
		$y^2 + y = (x^4 + x + 1)/x$	2	1	
3	2	$y^2 + y = (x^4 + x^3 + x^2 + x + 1)/(x^3 + x + 1)$	1	2	1
		$y^2 + y = (x^5 + x^2 + 1)/(x^2 + x + 1)$	1	3	0

The general problem of determining all imaginary quadratic number fields with a given class number has been solved in principle by Goldfeld-Gross-Zagier. The most recent advance is by M. Watkins who determined a complete list of all imaginary quadratic fields with class number ≤ 100. See a recent survey by D. Goldfeld [Go] for a review on this subject. The analogue of some of these results have been shown in the function field case. See for example the paper by H.-G. Rück and U. Tipp [RT] which presents a Gross-Zagier formula for function fields.

4.2.2 Construction of fields with an element of order n

We now present a specific form of imaginary quadratic function fields which will always have an element of order n in the ideal class group of $\mathcal{O}$. We will do so by using Theorem 4.3 proved in the previous section.

Theorem 4.8 *Let* $D = B^2 + M^n$, $\deg(B^2) < \deg(M^n)$ *where* B, $M \in \mathbb{F}_q[x]$, $\deg(M)$ *odd,* $(B, M) = 1$, *and* n *is odd. If* D *is square-free, then* $F = \mathbb{F}_q(x, \sqrt{D})$ *is imaginary quadratic and the ideal class group of* $\mathcal{O}$ *contains a cyclic subgroup of order* n.

Proof. By the conditions given it is clear that $\deg(D)$ is odd and consequently F is ramified imaginary quadratic. It is clear that $(X, Y) = (B, 1)$ is a proper solution to

$$X^2 - DY^2 = -M^n$$

By Theorem 4.3 it is sufficient to show that $X^2 - DY^2 = cM^j$ ($c \in \mathbb{F}_q^*$, $1 \leq j \mid n$, $j < n$) has no proper solution. Now for any $X, Y \in \mathbb{F}_q[x]$ we have that

$$\begin{aligned} \deg(X^2 - DY^2) &\geq \deg(D) \text{ (since } \deg(D) \text{ is odd)} \\ &= \deg(M^n) \text{ (by assumption)} \end{aligned}$$

hence it is not possible that $\deg(X^2 - DY^2) = \deg(M^j)$ for any $1 \leq j \mid n$, $j < n$. This completes the proof. ■

The above example is interesting although somewhat lacking in that one does not know how often the discriminant D of the above form will be square-free. In a recent paper Murty [Mu] showed that if $n \geq 3$ is a fixed integer then the number of imaginary quadratic number fields whose absolute discriminant is $\leq m$ and whose class group has an element of order n is at least $m^{\frac{1}{2}+\frac{1}{n}}$. I will state without proof the result of D. Cardon and Murty [CM] which is the analogue in the function field case. As we saw above it is relatively easy to construct function fields whose ideal class group will have an element of order n, but is more difficult to count how often a specific form of discriminant will give us a new field, i.e. how often the discriminant is square-free. The authors apply some interesting counting techniques to achieve a lower bound on the number of square-free discriminants of a particular form. This is their precise result:

Theorem 4.9 *Let $q \geq 5$ be a power of an odd prime and let $n \geq 3$ be a fixed integer. There are at least $q^{m(\frac{1}{2}+\frac{1}{n})}$ imaginary quadratic extensions $F = \mathbb{F}_q(x, \sqrt{D})$ of $\mathbb{F}_q(x)$ with $\deg(D) \leq m$ whose class group has an element of order n.*

4.2.3 Class number relations

Classically, one of the most effective ways to compute tables of class numbers for imaginary quadratic fields is through a beautiful formula of Hurwitz [Hu]. This formula, derived using information from the moduli space of elliptic curves, gives relations between class numbers of different imaginary quadratic fields. See a brief survey of this topic in [Co]. This story has its counterpart in our setting of imaginary quadratic function fields over $\mathbb{F}_q$. The moduli space of elliptic curves is replaced by the moduli space of rank 2 Drinfeld $\mathbb{F}_q[x]$-modules introduced by Drinfeld [Dr]. The analogue of the Hurwitz class number relation was first established by Jiu-Kang Yu [Yu1] in the odd characteristic case, and then by Julie T.-Y. Wang and Jing Yu [WY] in even characteristic. The resulting formula gives interesting relationships between the number of $\mathbb{F}_q$-rational points of the Jacobians of different imaginary hyperelliptic curves. See the cited papers for a more in depth exposition.

4.3 The Real case

Let $F/\mathbb{F}_q$ be a real quadratic function field over $\mathbb{F}_q$. Most of the results in this section are only applicable in the odd characteristic case, so suppose henceforth that $2 \nmid q$ unless stated otherwise. The real case is divided into four sections. The first section gives some very general results on the divisibility of the ideal class number of real quadratic function fields of different forms. We also present explicit formulae for the regulator of fields of a few different forms. It is in this section that some of my own results will also be presented. In the second section we determine all real quadratic function fields of Chowla type having ideal class number one. The third section contains a result of T.A. Schmidt on infinitely many real quadratic function fields of genus two with ideal class number one (where the constant field $\mathbb{F}_q$ is naturally allowed to vary). The last section is the analogue in the function field case of a conjecture by Ankeny-Artin-Chowla regarding the fundamental unit and discriminant in real quadratic number fields.

4.3.1 Class Number divisibility and explicit regulator computation

We will firstly introduce a useful result of X. Zhang [Zh1] which determines the 2-rank of the ideal class group. This was done by calculating the number of 'ambiguous' ideal classes (ideal classes for which $\mathfrak{a} \sim \bar{\mathfrak{a}}$).

Theorem 4.10 *Let $F = \mathbb{F}_q(x, \sqrt{D})$ be as above and let $Cl(\mathcal{O})$ denote the ideal class group of $\mathcal{O}$. Let $r = \dim_{\mathbb{F}_2} Cl(\mathcal{O})/Cl(\mathcal{O})^2$ be the 2-rank of $Cl(\mathcal{O})$, m the number of monic irreducible factors of D. Then $r = m - 2$ if D has an irreducible factor of odd degree, and $r = m - 1$ otherwise.*

Corollary 4.11 *We have that $2 \nmid h_{\mathcal{O}} = |Cl(\mathcal{O})|$ if and only if*

(1) D is irreducible, or

(2) $D = P_1 P_2$ where P_1 and P_2 are irreducible polynomials of odd degree.

Moreover if ϵ is a fundamental unit of F, then for case (1) it is shown in [Ar] that $N(\epsilon) = g$ where $\langle g \rangle = \mathbb{F}_q^*$ and in case (2) we have $N(\epsilon) = 1$.

Proof. Clearly $2 \nmid h_{\mathcal{O}}$ if and only if $r = 0$. In other words either $m = 1$ and D itself is irreducible, or if $m = 2$, it is necessary that one of the irreducible factors of D is of odd degree

(but since $\deg(D)$ is even it follows that both factors are of odd degree). Let $\epsilon = A + B\sqrt{D}$, and P be an irreducible factor of D with odd degree. If $N(\epsilon) = g = A^2 - DB^2$, we have that $A^2 \equiv g (\mathrm{mod}\, P)$ and hence $\left(\frac{g}{P}\right) = 1$. But $2 \nmid \deg(P)$ implies $\left(\frac{g}{P}\right) = -1$ by one of the reciprocity properties, a contradiction. Moreover it is also shown in [Ar] that $N(\epsilon) = g$ for some generator g of $\mathbb{F}_q^*$ or $N(\epsilon) = 1$, and consequently we must have that $N(\epsilon) = 1$. ■

In the classical number field case we have the following interesting result shown in 1985 by Hong Wen Lu [Hw]: Let $d = 4m^{2n} + 1$ be square-free, where $m, n \in \mathbb{Z}$ are such that $n > 0$ and $m \geq 2$. Then n divides the ideal class number of $\mathbb{Q}(\sqrt{d})$.

We will prove the analogue of the above result in the function field case, a result shown in 1992 by C. Friesen [Fr2]. I will present my own proof of the result using results which we have already shown. The two essential results in this regard will be Theorem 2.24 and Theorem 4.3. The natural analogue of the form $d = 4m^{2n}+1$ is $D = Z^{2n}+a^2$ where $Z \in \mathbb{F}_q[x]\backslash\mathbb{F}_q$ and $a \in \mathbb{F}_q^*$. This is the result:

Theorem 4.12 *Let $\mathbb{F}_q$ be a finite field of odd characteristic and $n \geq 2$. Let $Z \in \mathbb{F}_q[x]\backslash\mathbb{F}_q$ and let $a \in \mathbb{F}_q^*$. We let $D = Z^{2n} + a^2$. If D is monic and square-free then n divides the ideal class number of $\mathbb{F}_q(x, \sqrt{D})$.*

Proof. We see that $(X, Y) = (a, 1)$ is a proper (i.e. X and Y are relatively prime) solution to the equation

$$X^2 - DY^2 = -Z^{2n}$$

We now examine the continued fraction expansion of the real quadratic irrationality $\alpha = (0 + \sqrt{D})/1$. We have that $P_0 = 0$, $Q_0 = 1$. A simple investigation shows that $P_i = Z^n$ for all $i \in \mathbb{N}$ and that $Q_i = 1$ if i is even and $Q_i = a^2$ if i is odd, where these recursive sequences are defined by 2.15. Now from Theorem 2.24 we see that if the equation

$$X^2 - DY^2 = N$$

has a proper solution (X, Y) for some $N \in \mathbb{F}_q[x]$ with $\deg(N) < \frac{1}{2}\deg(Z^{2n}) = \deg(Z^n)$ then it follows that $N = b^2(-1)^i Q_i$ for some positive integer i and $b \in \mathbb{F}_q^*$. But because of what was observed above about the Q_i sequence, it follows that $N = c$ for some $c \in \mathbb{F}_q^*$, but we know that $c \neq c'Z^j$ for any $c \in \mathbb{F}_q^*$, $1 \leq j \mid 2n$, $j < 2n$ since $\deg(Z) \geq 1$. It follows that the above equation can only have a solution when $\deg(N) \geq \deg(Z^n)$. Now it follows from Theorem 4.3 that the

ideal class group of $\mathcal{O}$ has a cyclic subgroup of order either n or $2n$ (depending on whether or not $X^2 - DY^2 = cZ^n$ has a proper solution). In both cases we have that n divides $h_{\mathcal{O}}$. ■

We now wish to apply the above theorem in order to determine infinite families $\mathbb{F}_q(x, \sqrt{D})$ for which $n \mid h_{\mathcal{O}}$ for any $n \in \mathbb{N}$. We are able to do this for any n relatively prime to the characteristic p of $\mathbb{F}_q$. The condition that D must be monic does not pose a problem as we can simply choose for example Z to be monic. The condition that D must be square-free is slightly more troublesome. We display two families for which D is indeed monic and square-free:

Lemma 4.13 *Let $\mathbb{F}_q$ be of odd characteristic. Fix a positive integer n which is relatively prime to the characteristic p of $\mathbb{F}_q$ and an element $a \in \mathbb{F}_q^*$. Let $Z \in \mathbb{F}_q[x] \backslash \mathbb{F}_q$ be such that $D = Z^{2n} + a^2$ is monic. Then D is also square-free if Z has one of the following two forms:*

(1) $Z(x) = G(x^p) + bx^m$: $\quad (p, m) = 1$, $G(x) \in \mathbb{F}_q[x]$, $b \in \mathbb{F}_q^*$, $G(0)^{2n} \neq -a^2$.

(2) $Z(x) = G(x^p) + bx$: $\quad G(x) \in \mathbb{F}_q[x]$, $b \in \mathbb{F}_q^*$.

Proof. $D = Z^{2n} + a^2$ is square-free if and only if it shares no factors with its derivative $2nZ^{2n-1}Z'$. Since $a \neq 0$ and $p \nmid 2n$ we have that $Z^{2n} + a^2$ is square-free if and only if $Z^{2n} + a^2$ and Z' are relatively prime. For the first form we note that $Z'(x) = bmx^{m-1}$ can have zeros only at $x = 0$. But the condition $G(0)^{2n} \neq -a^2$ prevents $x = 0$ from being a root of $Z^{2n} + a^2$ and so $D = Z^{2n} + a^2$ is square-free. For the second form we simply note that $Z' = b \neq 0$ has no roots. ■

Corollary 4.14 *Let $\mathbb{F}_q$ be a finite field of odd characteristic and fix a positive integer n relatively prime to the characteristic p of $\mathbb{F}_q$. There are infinitely many square-free, even-degree monics $D \in \mathbb{F}_q[x]$ such that n divides the ideal class number of $\mathbb{F}_q(x, \sqrt{D})$.*

Once again, using Theorem 2.24 and Theorem 4.3 as we did in Theorem 4.12 we can obtain many different types of real quadratic function fields whose ideal class group has an element of order n. We have the following general result:

Theorem 4.15 *Let $D = (Z^n + aF - b)^2 + 4abF$ where $a, b \in \mathbb{F}_q^*$, $Z \in \mathbb{F}_q[x] \backslash \mathbb{F}_q$, $F \mid Z^n - b$ and $\deg(F) < \deg(Z^n)$. If D is monic and square-free, then the ideal class group of $\mathbb{F}_q(x, \sqrt{D})$ contains a cyclic subgroup of order n.*

Proof. We see firstly that $(X, Y) = (Z^n + aF + b, 1)$ is a proper solution to

$$X^2 - DY^2 = 4bZ^n$$

What remains to show according to Theorem 4.3 is that

$$X^2 - DY^2 = cZ^j$$

has no proper solution for ($c \in \mathbb{F}_q^*$, $1 \leq j \mid n$, $j < n$). Let us now investigate the continued fraction expansion of the real quadratic irrationality $\alpha = \sqrt{D}$. We have that $P_0 = 0$ and $Q_0 = 1$. We easily see that $P_i = Z^n + aF - b$ for all $i \geq 1$ and that $Q_i = 1$ if i is even and $Q_i = 4abF$ is i is odd. From Theorem 2.24 we know that if

$$X^2 - DY^2 = N$$

has a proper solution with $\deg(N) < \frac{1}{2}\deg(D) = \deg(Z^n)$, then $N = f^2(-1)^i Q_i$ for some $i \geq 1$ and $f \in \mathbb{F}_q^*$. Now suppose that $X^2 - DY^2 = cZ^j$ has a solution ($c \in \mathbb{F}_q^*$, $1 \leq j \mid n$, $j < n$). Then either $cZ^j = a^2(-1)^i$ which is not possible since $\deg(Z^j) \geq 1$ or $cZ^j = a^2(-1)^i 4abF$. The latter case implies that $Z^n = c'FZ^{j'}$ (where $j'j = n$ and $c' \in \mathbb{F}_q^*$) but this contradicts $F \mid Z^n - b$. Hence the ideal class group of $\mathcal{O}$ has a cyclic subgroup of order n. ■

Both the above result and Theorem 4.10 were relatively easy to prove as the discriminant D had the desirable property that when it was written as $D = h^2 + r$, then $r \mid h$ (where $h, r \in \mathbb{F}_q[x]$, $\deg(h) = \frac{1}{2}\deg(D)$ and $\deg(r) < \frac{1}{2}\deg(D)$). If D has this property we will say that the function field $F = \mathbb{F}_q(x, \sqrt{D})$ is of *ERD* type (extended Richaud-Degert type). Function fields F of this type are analogous to the classical case $\mathbb{Q}(\sqrt{d})$ where $d = N^2 + n$ with $n \mid 4N$ or $n \mid 2^m N$ ($m \geq 2$). We now do an explicit calculation of the regulator of a real quadratic function field of this form. This is interesting as in general it is difficult to find an analytic formula for the regulator of an infinite family of real quadratic function fields.

Theorem 4.16 *Let $F = \mathbb{F}_q(x, \sqrt{D})$ be of ERD type, where $D = h^2 + r$ is square-free,* $\deg(h) = \frac{1}{2}\deg(D)$ *and $r \mid h$. Then the regulator of F equals*

(1) $\frac{1}{2}\deg(D)$ *if* $r \in \mathbb{F}_q^*$,

(2) $\deg(D) - \deg(r)$ *if* $r \notin \mathbb{F}_q^*$.

Proof. If $r \in \mathbb{F}_q^*$, then F is of Chowla type and we determined in Example 2.37 that the regulator of F is in this case equal to $\deg(h)$. Suppose now that $r \notin \mathbb{F}_q^*$. We compute the

continued fraction expansion of the real quadratic irrationality $\alpha = (0 + \sqrt{D})/1$. We see that $P_0 = 0$ and $Q_0 = 1$. By using the recursion 2.15 we see $P_i = h$, $i \geq 1$ and $Q_i = 1$ if i is even and $Q_i = r$ if i is odd. Now recalling that $\alpha_i = (P_i + \sqrt{D})/Q_i$ (2.16) we observe that $\alpha_1 = \alpha_3$ and that the quasi-period m equals the period n, equals two (since $\deg(r) \geq 1$). Now using Theorem 2.36 we see that a fundamental unit of F is

$$\begin{aligned} \epsilon &= p_{m-1} + q_{m-1}\sqrt{D} = p_1 + q_1\sqrt{D} \\ &= \frac{2h^2}{r} + 1 + (\frac{2h}{r})\sqrt{D} \end{aligned}$$

Consequently recalling Remark 2.18 we see that $R = \deg(2h^2/r+1) = \deg(2h^2/r) = \deg(2h^2) - \deg(r) = \deg(D) - \deg r$. ■

We now present an infinite family of real quadratic function fields which are not of ERD type, but whose ideal class group has an element of order n. We first compute the regulator of function fields of this type. This explicit computation of the regulator is my own result although this construction is given in [WZ1]. I will give a general discussion of these results after the next two theorems.

Theorem 4.17 *Suppose $A \in \mathbb{F}_q[x] \backslash \mathbb{F}_q$ is monic. Let $h = \frac{1}{2}A - \frac{1}{2}$. If $D = (A^d + h)^2 + A$ $(d \geq 2)$ is square-free, then $F = \mathbb{F}_q(x, \sqrt{D})$ is not of ERD type and the regulator of F equals $d^2 \deg(A)$. Moreover the quasi-period of the expansion of $\alpha = \sqrt{D}$ equals $2d - 1$.*

Proof. Firstly it is clear that F is not of ERD type since $A \nmid A^d + h$. We compute the continued fraction expansion of $\alpha = \sqrt{D}$. As usual $P_0 = 0$ and $Q_0 = 1$. We follow the algorithm defined in Section 2.3.2. Our first observation is that $a_0 = \left\lfloor \sqrt{D} \right\rfloor = A^d + h$ and that $r_0 = 0$. Now $P_1 = a_0 Q_0 - P_0 = a_0 = A^d + h$ and $Q_1 = (D - P_1^2)/Q_0 = A$. By definition

$$a_1 = (P_1 + a_0)/Q_1 = (2A^d + A - 1)/A = 2A^{d-1} + 1$$

and $r_1 = -1$. Now $P_2 = a_1Q_1 - P_1 = A(2A^{d-1} + 1) - (A^d + h) = A^d + A - h$ and $Q_2 = (D - P_2^2)/Q_1 = -2A^{d-1}$. Continuing with the algorithm we obtain the following:

i	P_i	Q_i	a_i	r_i
0	0	1	$A^d + h$	0
1	$A^d + h$	A	$2A^{d-1} + 1$	-1
2	$A^d + A - h$	$-2A^{d-1}$	$-A$	A
3	$A^d - A + h$	$-A^2$	$-2A^{d-2}$	-1
4	$A^d + A - h$	$2A^{d-2}$	A^2	A
5	$A^d - A + h$	A^3	$2A^{d-3}$	-1
6	$A^d + A - h$	$-2A^{d-3}$	$-A^3$	A
7	$A^d - A + h$	$-A^4$	$-2A^{d-4}$	-1
8	$A^d + A - h$	$2A^{d-4}$	A^4	A
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

(supposing in order to see the pattern that $d > 4$). This pattern continues until the index $i = 2d - 2$ (this index is found by examining the decreasing powers of A in the Q sequence). Observe that $P_{2d-2} = A^d + A - h$ and $Q_{2d-2} = \pm 2A^{d-(\frac{2d-2}{2})} = \pm 2A$ where the $\pm$ is dependent on whether d is even or odd. Also $a_{2d-2} = \pm(A^{d-1} + \frac{1}{2})$ and $r_{2d-2} = 0$. Continuing for a few more iterations yields:

i	P_i	Q_i	a_i	r_i
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$2d-2$	$A^d + A - h$	$\pm 2A$	$\pm(A^{d-1} + \frac{1}{2})$	0
$2d-1$	$A^d + h$	$\pm\frac{1}{2}$	$\pm(4A^d + 2A - 2)$	0
$2d$	$A^d + h$	$\pm 2A$	$\pm(A^{d-1} + \frac{1}{2})$	-1

From this we see that

$$\alpha_1 = \frac{P_1 + \sqrt{D}}{Q_1} = \frac{A^d + h + \sqrt{D}}{A} = \pm 2 \cdot \frac{A^d + h + \sqrt{D}}{\pm 2A} = \pm 2 \cdot \frac{P_{2d} + \sqrt{D}}{Q_{2d}} = \pm 2\alpha_{2d}$$

In other words the quasi-period of the expansion of $\alpha = \sqrt{D}$ is $m = 2d - 1$ since $\alpha_1 = c\alpha_{2d}$ for some $c \in \mathbb{F}_q^*$. Since $c = \pm 2$ (depending on whether d is odd or even) we know from Corollary 2.23 that the period of the expansion must be $2m = 4d - 2$. Now from Theorem 2.36 we know that a fundamental unit of F is $\epsilon = p_{2d-2} + q_{2d-2}\sqrt{D}$. We also know from Remark 2.18 that the regulator R of F equals $\deg(p_{2d-2})$. Recalling that $p_0 = a_0$, $p_1 = a_1a_0 + 1$, $p_2 = a_2(a_1a_0 + 1) + a_0$ and in general that $p_i = a_ip_{i-1} + p_{i-2}$ we see that:

$$\deg(p_{2d-2}) = \deg(\prod_{i=0}^{2d-2} a_i) = \sum_{i=0}^{2d-2} \deg(a_i)$$

(since $a_i \neq 0$ for any $i \geq 0$). Observing the pattern in the sequence a_i, we see that

$$\sum_{i=0}^{2d-2} \deg(a_i) = \deg(A)(\sum_{i=0}^{d-1}(d-i) + \sum_{i=0}^{d-1} i) = \deg(A) \sum_{i=0}^{d-1} d = \deg(A)d^2$$

Hence the regulator of F equals $\deg(p_{2d-2}) = d^2 \deg(A)$. ■

We now examine the ideal class group of function fields of the above type more closely. More precisely:

Theorem 4.18 *Suppose $A = Z^n$ $(n \geq 2)$ is monic for some $Z \in \mathbb{F}_q[x] \backslash \mathbb{F}_q$. Let $h = \frac{1}{2}A - \frac{1}{2}$. If $D = (A^d + h)^2 + A$ $(d \geq 2)$ is square-free, then the ideal class group of $F = \mathbb{F}_q(x, \sqrt{D})$ has an element of order n.*

Proof. Firstly we note that $(X, Y) = (A^d + h, 1)$ is a proper solution to the equation

$$X^2 - Y^2 D = -A = -Z^n$$

What remains to show according to Theorem 4.3 is that

$$X^2 - DY^2 = cZ^j$$

has no proper solution for $(c \in \mathbb{F}_q^*,\ 1 \leq j \mid n,\ j < n)$. From Theorem 2.24 we know that if

$$X^2 - DY^2 = N$$

has a proper solution with $\deg(N) < \frac{1}{2}\deg(D) = \frac{1}{2}\deg(A^{2d}) = 2d\deg(Z^n)$, then $N = a^2(-1)^i Q_i$ for some $i \geq 1$ and some $a \in \mathbb{F}_q^*$. We will make use the continued fraction expansion of $\alpha = \sqrt{D}$ determined in the theorem above. Now suppose that $X^2 - DY^2 = cZ^j$ has a solution $(c \in \mathbb{F}_q^*,\ 1 \leq j \mid n,\ j < n)$. Then either $cZ^j = a^2(-1)^i b$ $(b = 1$ or $b = \pm\frac{1}{2})$ which is not possible since $\deg(Z^j) \geq 1$ or $cZ^j = a^2(-1)^i bA^k$ $(b \in \mathbb{F}_q^*$ and $k \in [1, 2, ..d-1])$. The latter case implies that $cZ^j = c'Z^{nk}$ $(c, c' \in \mathbb{F}_q^*)$ which is not possible if $j < n$. Hence the ideal class group of $\mathcal{O}$ has a cyclic subgroup of order n. ■

The construction of the function fields in Theorem 4.15 and the Theorem above can be found in [WZ1]. They do not however find an explicit formula for the regulator, but simply note that function fields of that form have an element of order n in their ideal class group. The authors also present three other types of function fields F which are not of ERD type but have a subgroup of order n in their ideal class group. These being:

(1) $D = (A^d - h)^2 + A$,

(2) $D = (A^d + h + 1)^2 - A$,

(3) $D = (A^d - h - 1)^2 - A$.

where the situation is the same as that of the above theorem. These three forms lead to essentially the same continued fraction expansion of $\alpha = \sqrt{D}$ and the formula for the quasi-period and regulator of these function fields are the same as those given in Theorem 4.17. Once again it is a difficult problem to determine exact conditions under which D will be square-free and the authors do not address this issue. It would indeed be interesting if we could show conditions under which the discriminant D of the above form would be square-free since it would give us an explicit construction a function field F with a given odd quasi-period (for the expansion of $\sqrt{D}$). To this end I was able to construct such a field F having quasi-period congruent to -1 modulo $2p$, where p is the characteristic of $\mathbb{F}_q$. This is the precise result:

Theorem 4.19 *Let $G \in \mathbb{F}_q[x]$. Suppose $A(x) = G(x^p) + cx + d \in \mathbb{F}_q[x]$, $c, d \in \mathbb{F}_q^*$ is monic and let $h = \frac{1}{2}A - \frac{1}{2}$. Then $D = (A^d + h)^2 + A$ is square-free if $d = np$ for any $n \geq 1$, where p is the characteristic of $\mathbb{F}_q$.*

Proof. D is square-free if and only if it shares no common factors with its derivative D'. Let $B = A^d + h$. We have:

$$\begin{aligned} D' &= 2B(dA^{d-1}A' + h') + A' \\ &= 2B(0 + \frac{1}{2}A') + A' \\ &= A'B + A' \\ &= A'(B + 1) \end{aligned}$$

Now suppose there exists a monic irreducible $P \in \mathbb{F}_q[x] \backslash \mathbb{F}_q$ dividing both D and D'. Then since $P \mid D'$ and $A' \in \mathbb{F}_q^*$, it follows that $P \mid B + 1$, i.e. $P \mid A^d + \frac{1}{2}A + \frac{1}{2}$. Moreover since $P \mid D$ it also follows that

$$\begin{aligned} P &\mid BD' - A'D = B^2A' + BA' - A'(B^2 + A) = A'(B - A) \text{ i.e.} \\ P &\mid A'(A^d - \frac{1}{2}A - \frac{1}{2}) \end{aligned}$$

Hence since $A' \in \mathbb{F}_q^*$, we have $P \mid (A^d - \frac{1}{2}A - \frac{1}{2})$. But this implies that $P \mid (A^d - \frac{1}{2}A - \frac{1}{2}) + (A^d + \frac{1}{2}A + \frac{1}{2}) = 2A^d$. So that $P \mid A$. A contradiction. Hence D is indeed square-free. ∎

Now recalling Theorem 4.17, we know that the quasi-period of the expansion of $\sqrt{D}$ of the above form equals $2d-1 = 2(np)-1$. Hence over the finite field $\mathbb{F}_q$ of characteristic p, we have an explicit construction of a function field $F = \mathbb{F}_q(x, \sqrt{D})$ such that the expansion of $\sqrt{D}$ will be quasi-periodic for any given quasi-period congruent to -1 modulo $2p$. In particular we can construct a real quadratic function field $F = \mathbb{F}_q(x, \sqrt{D})$ over any finite field of odd characteristic, whose continued fraction expansion of $\sqrt{D}$ has arbitrarily long period. Note that it also follows that we can construct F with arbitrarily large regulator from the above results.

We now ask ourselves whether we can find an infinite family of real quadratic function fields with a given even quasi-period. I found the following construction which yields even quasi-periods which are multiples of 4 when the discriminant is square-free:

Theorem 4.20 *Suppose $A \in \mathbb{F}_q[x]\backslash\mathbb{F}_q$ is monic. Let $h = \frac{1}{2}A - \frac{1}{2}$. If $D = (A^d + A^{d-1} + h)^2 + A$ $(d \geq 3)$ is square-free, then $F = \mathbb{F}_q(x, \sqrt{D})$ is not of ERD type and the regulator of F equals $(2d^2 - 2d + 1)\deg(A)$. Moreover the quasi-period of the expansion of $\alpha = \sqrt{D}$ equals $4(d-1)$.*

Proof. Firstly it is clear once again that F is not of ERD type since $A \nmid A^d + A^{d-1} + h$. We compute the continued fraction expansion of $\alpha = \sqrt{D}$. As usual $P_0 = 0$ and $Q_0 = 1$. We follow the algorithm defined in Section 2.3.2. Our first observation is that $a_0 = \left\lfloor \sqrt{D} \right\rfloor = A^d + A^{d-1} + h$ and that $r_0 = 0$. Now $P_1 = a_0Q_0 - P_0 = a_0 = A^d + A^{d-1} + h$ and $Q_1 = (D - P_1^2)/Q_0 = A$. By definition

$$a_1 = (P_1 + a_0)/Q_1 = (2A^d + A^{d-1} + A - 1)/A = 2(A^{d-1} + A^{d-2}) + 1$$

and $r_1 = -1$. Now $P_2 = a_1Q_1 - P_1 = A(2(A^{d-1}+A^{d-2})+1) - (A^d+A^{d-1}+h) = A^d+A^{d-1}+(h+1)$ and $Q_2 = (D - P_2^2)/Q_1 = -2(A^{d-1} + A^{d-2})$. Continuing with the algorithm we obtain the

following:

i	P_i	Q_i	a_i	r_i
0	0	1	$A^d + A^{d-1} + h$	0
1	$A^d + A^{d-1} + h$	A	$2(A^{d-1} + A^{d-2}) + 1$	-1
2	$A^d + A^{d-1} + (h+1)$	$-2(A^{d-1} + A^{d-2})$	$-A$	A
3	$A^d + A^{d-1} - (h+1)$	$-A^2$	$-2(A^{d-2} + A^{d-3})$	-1
4	$A^d + A^{d-1} + (h+1)$	$2(A^{d-2} + A^{d-3})$	A^2	A
5	$A^d + A^{d-1} - (h+1)$	A^3	$2(A^{d-3} + A^{d-4})$	-1
6	$A^d + A^{d-1} + (h+1)$	$-2(A^{d-3} + A^{d-4})$	$-A^3$	A
7	$A^d + A^{d-1} - (h+1)$	$-A^4$	$-2(A^{d-4} + A^{d-5})$	-1
8	$A^d + A^{d-1} + (h+1)$	$2(A^{d-4} + A^{d-5})$	A^4	A
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

(supposing in order to see the pattern that $d > 4$). This pattern continues until the index $i = 2d - 2$ (this index is found by examining the decreasing powers of A in the Q sequence). Observe that $P_{2d-2} = A^d + A^{d-1} + (h+1)$ and $Q_{2d-2} = \pm 2(A+1)$ where the $\pm$ is dependent on whether or not d is even or odd. Since the sign does not essentially change the expansion, we suppose that d is odd in order to see the general pattern. Also $a_{2d-2} = A^{d-1} + \frac{1}{2}$ and $r_{2d-2} = -1$. Continuing for a few more iterations yields:

i	P_i	Q_i	a_i	r_i
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$2d-2$	$A^d + A^{d-1} + (h+1)$	$2(A+1)$	$A^{d-1} + \frac{1}{2}$	-1
$2d-1$	$A^d + A^{d-1} + (h+1)$	$-A^{d-1}$	$-2(A+1)$	A
$2d$	$A^d + A^{d-1} - (h+1)$	$-2(A^2 + A)$	$-A^{d-2}$	-1
$2d+1$	$A^d + A^{d-1} + (h+1)$	A^{d-2}	$2(A^2 + A)$	A
$2d+2$	$A^d + A^{d-1} - (h+1)$	$2(A^3 + A^2)$	A^{d-3}	-1
$2d+3$	$A^d + A^{d-1} + (h+1)$	$-A^{d-3}$	$-2(A^3 + A^2)$	A
$2d+4$	$A^d + A^{d-1} - (h+1)$	$-2(A^4 + A^3)$	$-A^{d-4}$	-1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

This pattern continues until the index $i = 4d - 6$ (this index is again found by examining the decreasing powers of A). Observe that $P_{4d-6} = A^d + A^{d-1} - (h+1)$ and $Q_{4d-6} = -2(A^{d-1} + A^{d-2})$.

Also $a_{4d-6} = -A$ and $r_{4d-6} = -1$. Continuing for a few more iterations yields:

i	P_i	Q_i	a_i	r_i
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$4d-6$	$A^d + A^{d-1} - (h+1)$	$-2(A^{d-1} + A^{d-2})$	$-A$	-1
$4d-5$	$A^d + A^{d-1} + (h+1)$	A	$2(A^{d-1} + A^{d-2}) + 1$	0
$4d-4$	$A^d + A^{d-1} + h$	1	$2(A^d + A^{d-2} + a)$	0
$4d-3$	$A^d + A^{d-1} + h$	A	$2(A^{d-1} + A^{d-2}) + 1$	-1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

From this we see that

$$\alpha_1 = \frac{P_1 + \sqrt{D}}{Q_1} = \frac{A^d + A^{d-1} + h + \sqrt{D}}{A} = \frac{P_{4d-3} + \sqrt{D}}{Q_{4d-3}} = \alpha_{4d-3}$$

In other words the quasi-period of the expansion of $\alpha = \sqrt{D}$ is $m = 4d-3-1 = 4(d-1)$. Now from Theorem 2.36 we know that a fundamental unit of F is $\epsilon = p_{4d-5} + q_{4d-5}\sqrt{D}$. We also know from Remark 2.18 that the regulator R of F equals $\deg(p_{4d-5})$. Recalling that $p_0 = a_0$, $p_1 = a_1a_0 + 1$, $p_2 = a_2(a_1a_0 + 1) + a_0$ and in general that $p_i = a_ip_{i-1} + p_{i-2}$ we see that:

$$\deg(p_{4d-5}) = \deg(\prod_{i=0}^{4d-5} a_i) = \sum_{i=0}^{4d-5} \deg(a_i)$$

(since $a_i \neq 0$ for any $i \geq 0$). Observing the pattern in the sequence a_i, we see that

$$\begin{aligned}
\sum_{i=0}^{4d-5} \deg(a_i) &= \deg(A)(d + 3(d-1) + 4\sum_{i=0}^{d-2} i) \\
&= \deg(A)(4d - 3 + 4\frac{d-2}{2}(d-2+1)) \\
&= \deg(A)(2d^2 - 2d + 1)
\end{aligned}$$

Hence the regulator of F equals $\deg(p_{2d-2}) = (2d^2 - 2d + 1)\deg(A)$. ■

Once again with the above type if we assume that $A = Z^n$ for some $Z \in \mathbb{F}_q[x] \backslash \mathbb{F}_q$, $n \geq 2$, we can see in a similar manner to Theorem 4.18 that if $D = (A^d + A^{d-1} + h)^2 + A$ is square-free then ideal class group of $F = \mathbb{F}_q(x, \sqrt{D})$ has an element of order n. Once again it is a non-trivial task to determine infinite families for which the discriminant of the above form will be square-free. I was unable to find such a family, although from numerical investigations it seems probable that there are infinitely many discriminants of this form which are square-free.

From these results it becomes clear that it is no real art to construct function fields with elements of a given order in the ideal class group. This is indeed to be expected. Rather, as a

step towards Gauss' conjecture, we wish to find infinite families of function fields such that the ideal class number of the ring of integers is small.

It has been my idea to search for infinite families of real quadratic function fields for which I could explicitly compute the regulator. I have been looking in particular for families for which the order of the regulator grows 'quickly' as the genus of the function field grows (or indeed the order of the discriminant grows). The motivation behind this is Schmidt's formula: $h_{\mathcal{O}} = h_F/R$. In other words if we can show that the order of R grows with the order of h_F, we will obtain function fields with small ideal class numbers. In one of the constructions above (Theorem 4.17), if A is chosen to be of degree one, we have that $R = d^2 = (\frac{1}{2}\deg(D))^2 = \frac{1}{4}\deg(D)^2$. Which shows that R grows with the square of the degree of the discriminant. I note at this point a useful bound on the ideal class number $h_{\mathcal{O}}$ which is achieved by a well known construction using constant field extensions done in Theorem 4.30. This bound is the following:

$$\begin{aligned} h_{\mathcal{O}} &\geq (q-1)\frac{q^{2g-1}+1-2gq^{\frac{2g-1}{2}}}{R(2g-1)(q^g-1)} \\ &= (q-1)\frac{q^{2d-3}+1-2(d-1)q^{\frac{2d-3}{2}}}{R(2d-3)(q^{d-1}-1)} \end{aligned}$$

where $d = \frac{1}{2}\deg(D) = g+1$ (where g is the genus). An easy calculation shows that the quadratic growth of the regulator mentioned above is not fast enough to ensure a lower bound less than or equal to 1. Indeed for all the constructions in this section the above bound ensures that $h_{\mathcal{O}}$ tends towards infinity as the degree of the discriminant tends towards infinity. For this reason it would be desirable to find families for which the order of the regulator's growth is dependent on the field $\mathbb{F}_q$ over which we work and preferably some type of exponential growth.

As we know, the regulator of a function field equals the degree of the polynomial p_{m-1} where m denotes the quasi-period of the expansion of the root of the discriminant. The degree of p_{m-1} can also be expressed as $\sum_{i=0}^{m-1}\deg(a_i)$ as was used in the above constructions. Hence if we are looking for families with large regulators, it makes sense to look for families with long quasi-periods for the expansion of $\sqrt{D}$. I have done several numerical investigations into the maximum quasi-period which can be obtained for the expansion of $\sqrt{D}$ over different constants $\mathbb{F}_q$ and different genus. These investigations have led me to make the following conjecture:

Conjecture 4.21 *Let $\mathbb{F}_q$ be a fixed finite field of odd characteristic and let $g \geq 1$ be a fixed genus. Let m_D respectively R_D denote the quasi-period of the expansion of $\sqrt{D}$ and the regulator of $\mathbb{F}_q(x,\sqrt{D})$. Set $\mu = \max\{m_D : D \in \mathbb{F}_q[x]$ monic, square-free and $\deg(D) = 2g+2\}$ and*

$\gamma = \max\{R_D : D \in \mathbb{F}_q[x]$ *monic, square-free and* $\deg(D) = 2g+2\}$. *I conjecture that the set of discriminants* D *for which* $m_D = \mu$ *equals the set of discriminants* D *for which* $R_D = \gamma$.

This conjecture being true would imply that to characterize those function fields with maximal regulators for a given genus we need only characterize those function fields with maximal quasi-periods. I have attempted without success to characterize these families, and it seems that this determination is in itself a difficult problem. The proof of this conjecture in the genus 1 case is not difficult and follows from the following strong relationship between the quasi-period and the regulator. After proving this I have subsequently seen that it is well known.

Theorem 4.22 *Let* $F = \mathbb{F}_q(x, \sqrt{D})$ *be a real quadratic function field of genus* 1 *over a finite field of odd characteristic. The regulator of* F *equals* $m_D + 1$, *where* m_D *is defined as above.*

Proof. Since F is of genus 1, we know that $\deg(D) = 4$ and that the degree of $a_0 = d = \lfloor \sqrt{D} \rfloor$ equals 2. Now from Proposition 2.27 we know that $1 < \deg(a_i) \leq 2$ and $0 \leq \deg(Q_i) < 2$ for all $i \geq 1$ (recalling that α_i is reduced for all $i \geq 1$ where $\alpha = \sqrt{D}$). Also from Proposition 2.27 we have that $|a_i Q_i| = |d|$ for $i \geq 1$. This implies that $\deg(a_i) + \deg(Q_i) = 2$ for all $i \geq 1$. I claim that for $1 \leq i < m_D$, $\deg(Q_i) = 1$. For suppose that $\deg(Q_j) = 0$ for some index $1 \leq j < m_D$, then $Q_j = c \in \mathbb{F}_q^*$. Therefore $P_{j+1} = d$ and $Q_{j+1} = (1/c)(D - d^2) = (1/c)Q_1$. This implies that

$$\alpha_1 = \frac{d + \sqrt{D}}{Q_1} = \frac{1}{c} \cdot \frac{d + \sqrt{D}}{Q_{j+1}} = \alpha_{j+1}$$

or in other words that the quasi-period of the expansion of $\sqrt{D}$ equals j. This is a contradiction since $j < m_D$.

Now since $\deg(Q_i) = 1$ for $1 \leq i < m_D$ it follows that $\deg(a_i) = 1$ for $1 \leq i < m_D$ (since $\deg(a_i) + \deg(Q_i) = 2$ for all $i \geq 1$). We therefore have that the regulator of F equals

$$\begin{aligned} \deg(p_{m_D-1}) &= \sum_{i=0}^{m_D-1} \deg(a_i) \\ &= \deg(a_0) + \sum_{i=1}^{m_D-1} \deg(a_i) \\ &= 2 + \sum_{i=1}^{m_D-1} 1 \\ &= m_D + 1 \end{aligned}$$

■

It is now clear from the above theorem that the conjecture holds in the genus 1 case since the regulator is related to the quasi-period in such a simple way. It is important to note that the above conjecture does not follow trivially in higher genus since there do exist discriminants D and D' such that $m_D < m_{D'}$, but $R_D > R_{D'}$. Take for example the genus 2 case over $\mathbb{F}_3$ with $D = x^6 + x^5 + x - 1$ and $D' = x^6 + x^5 - x^3 - x^2 + x + 1$. Then

$$\begin{aligned} m_D &= 5,\ R_D = 9,\ \text{but} \\ m_{D'} &= 6,\ R_{D'} = 8 \end{aligned}$$

It seems that the focus in the study of continued fractions in real quadratic function fields has been on improved algorithmic methods for computing the regulator. Therefore there seems to be room for a more in depth study of the structure and investigation of such phenomena as presented in the conjecture above. There are also certainly results in the classical theory of continued fractions which are waiting to be translated into the function field context. In general there seem from numerical investigations to be some very interesting phenomena in the study of continued fractions in real quadratic function fields. This makes this area of research exciting and possibly very rewarding.

4.3.2 All quadratic fields of Chowla type with class number one

Let $d = a^2 + 1 \geq 2$ be a square-free integer. R.A. Mollin [Mo] presented several equivalent conditions for the class number of the real quadratic number field $K = \mathbb{Q}(\sqrt{d})$ to be one. S. Chowla conjectured that there are exactly 6 such fields. R.A. Mollin and H.C. Williams [MW] proved this conjecture under the assumption of the Generalized Riemann Hypothesis for $\zeta_K(s)$.

We will prove the analogue of this in the function field context, following the method in [FH]. We recall from Example 2.37 that a real quadratic function field of the form $F = \mathbb{F}_q(x, \sqrt{D})$ with $D = A^2 + b$, $A \in \mathbb{F}_q[x]$ and $b \in \mathbb{F}_q^*$ is said to be of Chowla type. Let $2d := \deg(D)$. We need a few preliminary results.

Definition 4.23 *Let $E \in \mathbb{F}_q[x], E \neq 0$. A solution (U, V) of the equation*

$$X^2 - DY^2 = E \tag{4.1}$$

in $\mathbb{F}_q[x]$ is called trivial if $E = aM^2, a \in \mathbb{F}_q^*$, and $M \mid U$, $M \mid V$.

Lemma 4.24 *Let $\epsilon = A + B\sqrt{D}$ $(A, B \in \mathbb{F}_q[x])$ be a fundamental unit of F. If the equation 4.1 has a non-trivial solution in $\mathbb{F}_q[x]$, then* $\deg(E) \geq \deg(A) - 2\deg(B)$.

Proof. Let (U, V) be a non-trivial solution of equation 4.1, then $V \neq 0$ (otherwise the solution is trivial). We can assume w.l.o.g that (U, V) is a non-trivial solution with minimal $\deg(V)$. We have

$$\begin{aligned} N(\epsilon)E &= N[(A + B\sqrt{D})(U \pm V\sqrt{D})] \\ &= (AU \pm BDV)^2 - D(BU \pm AV)^2 \end{aligned}$$

We claim that the solutions $(AU + BDV, BU + AV)$ and $(AU - BDV, BU - AV)$ are non-trivial. If one of them is trivial, then $E = aM^2, a \in \mathbb{F}_q^*$ and

$$AU + BDV \equiv 0 (\mathrm{mod}\, M) \tag{1}$$

$$BU + AV \equiv 0 (\mathrm{mod}\, M) \tag{2}$$

or

$$AU - BDV \equiv 0 (\mathrm{mod}\, M) \tag{3}$$

$$BU - AV \equiv 0 (\mathrm{mod}\, M) \tag{4}$$

But

$$\begin{aligned} B(1) - A(2) &\Rightarrow A^2V - DB^2V \equiv 0 (\mathrm{mod}\, M) \Rightarrow V \equiv 0 (\mathrm{mod}\, M) \\ B(3) - A(4) &\Rightarrow A^2U - DB^2U \equiv 0 (\mathrm{mod}\, M) \Rightarrow U \equiv 0 (\mathrm{mod}\, M) \end{aligned}$$

This implies (U, V) is trivial, a contradiction. Hence $(AU + BDV, BU + AV)$ and $(AU - BDV, BU - AV)$ are non-trivial. Since $\deg(V)$ is minimal, we know that

$$\min\{\deg(BU + AV), \deg(BU - AV)\} \geq \deg(V) \tag{5}$$

Moreover,

$$\begin{aligned} \deg(E) &= \deg(U^2 - DV^2) = \deg(B^2U^2 - B^2DV^2) - 2\deg(B) \\ &= \deg(B^2U^2 - A^2V^2 + V^2N(\epsilon)) - 2\deg(B) \end{aligned} \tag{6}$$

If $\deg(BU) > \deg(AV)$,then

$$\begin{aligned} \deg(E) &= \deg(B^2U^2) - 2\deg B \\ &> \deg(A^2V^2) - 2\deg B \\ &> 2\deg A - 2\deg B \end{aligned}$$

If $\deg(BU) < \deg(AV)$,then

$$\begin{aligned} \deg(E) &= \deg(A^2V^2) - 2\deg B \\ &> 2\deg(A) - 2\deg B \end{aligned}$$

Finally if $\deg(BU) = \deg(AV)$, then

$$\max\{\deg(BU + AV), \deg(BU - AV)\} = \deg(AV)$$

From (5) we see that $\deg(B^2U^2 - A^2V^2) \geq \deg(AV^2)$ which together with (6) gives us $\deg(E) \geq \deg(AV^2) - 2\deg(B) \geq \deg(A) - 2\deg(B)$. ■

Lemma 4.25 *Let k be a positive integer. The following conditions are equivalent.*

(1) For each monic irreducible $P \in \mathbb{F}_q[x]$ with $\deg(P) \leq k$, we have $\left(\frac{D}{P}\right) = -1$ (i.e. P is inert in F).

(2) For each $A \in \mathbb{F}_q[x]$ and monic irreducible $P \in \mathbb{F}_q[x]$ satisfying $\deg(A) < \deg(P) \leq k$ we have $A^2 - D \not\equiv 0 (\mathrm{mod}\, P)$

Proof. This follows directly from the reciprocity law. ■

Corollary 4.26 *The conditions of the above lemma can only be satisfied if $k \leq d - 1$ ($2d = \deg D$). In other words there exists a monic irreducible P such that $\deg(P) \leq d$ and $\left(\frac{D}{P}\right) = 1$.*

Proof. D can always be expressed as $D = A^2 + B$ with $\deg A = d$ and $\deg(B) \leq d - 1$. If $\deg(B) \geq 1$, we choose P to be an irreducible factor of B, then $D \equiv A^2 (\mathrm{mod}\, P)$, i.e. $\left(\frac{D}{P}\right) = 1$. If $B = b \in \mathbb{F}_q^*$, it is easy to see that there exists an $a \in \mathbb{F}_q$ such that $a^2 + b$ is a square in $\mathbb{F}_q$ (The curve defined by $X^2 - Y^2 = b$ has at least one $\mathbb{F}_q$-rational point by the Hasse-Weil bound). Then $D = A^2 + b = A^2 - a^2 + a^2 + b = (A - a)(A + a) + a^2 + b \equiv a^2 + b (\mathrm{mod}\, A - a)$. We choose P to be an irreducible factor of $A - a$. Then $D \equiv a^2 + b (\mathrm{mod}\, P)$, and $\left(\frac{D}{P}\right) = 1$ since $a^2 + b$ is a square in $\mathbb{F}_q^*$. ■

We now come to one of the main results which shows that each condition in Lemma 4.25 with $k = d - 1$ is equivalent to $h_{\mathcal{O}} = 1$ and F of Chowla type.

Theorem 4.27 *Let $F = \mathbb{F}_q(x, \sqrt{D})$ be a real quadratic function field with, $\deg D = 2d \geq 2$. The following conditions are equivalent.*

(1) For each monic irreducible $P \in \mathbb{F}_q[x]$ *with* $\deg(P) \leq d-1$, *we have* $\left(\frac{D}{P}\right) = -1$ *(i.e.* P *is inert in* F*).*

(2) For each $A \in \mathbb{F}_q[x]$ *and monic irreducible* $P \in \mathbb{F}_q[x]$ *satisfying* $\deg(A) < \deg(P) \leq d-1$ *we have* $A^2 - D \not\equiv 0 (\mathrm{mod}\, P)$

(3) For any $A \in \mathbb{F}_q[x]$ *with* $\deg(A) \leq d-1, D - A^2$ *is either irreducible or a product of two irreducible polynomials with degree* d.

(4) $h_{\mathcal{O}} = 1$ *and* F *is of Chowla type:* $D = A^2 + b, A \in \mathbb{F}_q[x], b \in \mathbb{F}_q^*$.

Proof. (1)⇔(2): By the above lemma.

(2)⇒(3): If $\deg(A) \leq d-1$ and $D - A^2$ has an irreducible factor P with $\deg(P) \leq d-1$, we can assume that $\deg(A) < \deg(P)$ by replacing A if necessary by its residue mod P. Therefore $\deg(A) < \deg(P) \leq d-1$ and $D - A^2 \equiv 0 (\mathrm{mod}\, P)$ which contradicts (2).

(3)⇒(2): If $\deg(A) < \deg(P) \leq d-1$ and $D - A^2 \equiv 0 (\mathrm{mod}\, P)$, then $D - A^2$ has the irreducible factor P with $\deg(P) \leq d-1$ which contradicts (3).

(4)⇒(1): We have $\epsilon = A + \sqrt{D}$, $\deg(A) = d \geq 1$. We do this by contradiction. Suppose there exists an irreducible P with $\deg(P) \leq d-1$ and $\left(\frac{D}{P}\right) \neq 1$ then either $P\mathcal{O} = \mathfrak{P}\bar{\mathfrak{P}}$ or $P\mathcal{O} = \mathfrak{P}^2$. In both cases $P\mathcal{O} = \mathfrak{P}\bar{\mathfrak{P}}$ since $\mathfrak{P} = \bar{\mathfrak{P}}$ in the latter case. Since by assumption $h_{\mathcal{O}} = 1$, $\mathfrak{P}$ is principal: $\mathfrak{P} = (U + V\sqrt{D})$ and $\bar{\mathfrak{P}} = (U - V\sqrt{D})$. Hence

$$U^2 - V^2 D = cP \ (c \in \mathbb{F}_q^*)$$

The solution (U, V) of the equation $X^2 - DY^2 = cP$ is non-trivial since $E = cP$ is not of the form aM^2. From Lemma 4.24 is follows that $\deg(P) \geq \deg(A) - 0 = d$, which contradicts $\deg(P) \leq d-1$.

(1)⇒(4): Now by recalling Corollary 2.46 it is clear that $h_{\mathcal{O}} = 1$ since for each monic irreducible $P \in \mathbb{F}_q[x]$ with $\deg(P) \leq d-1$ we have $\left(\frac{D}{P}\right) = -1$ (i.e. P remains prime in $\mathcal{O}$). Moreover from the above remark, we have the expression $D = A^2 + B$ with $\deg(A) = d$ and $\deg(B) \leq d-1, B \neq 0$. If $\deg(B) \geq 1$, then B has an irreducible factor P with $\deg(P) \leq d-1$. We have $A^2 \equiv D (\mathrm{mod}\, P)$, i.e. $\left(\frac{D}{P}\right) = 1$ which contradicts (1). Therefore $B \in \mathbb{F}_q^*$ and F is of Chowla type. ■

We can in fact say slightly more than the previous theorem, namely:

Corollary 4.28 *If* $F = \mathbb{F}_q(x, \sqrt{D})$ *is of Chowla type with* $h_{\mathcal{O}} = 1$, *then either:*

(I) $D = A^2 - a$ *is irreducible and* a *is not a square in* $\mathbb{F}_q^*$; *or*

(II) $D = (A-b)(A+b) = A^2 - b^2$ *and* $A \pm b$ *are irreducible of odd degree* d.

Proof. The above Theorem asserts that $D = A^2 - a, a \in \mathbb{F}_q^*$ and $\deg(A) = d$. From condition (1), (2), or (3) we know that D has no irreducible factor P with $\deg(P) \leq d-1$. Therefore either D is irreducible (and a is not a square in $\mathbb{F}_q^*$) or $D = P_1 P_2$ with $\deg(P_1) = \deg(P_2) = d$. Since $h_{\mathcal{O}} = 1$, Theorem 4.10 asserts that $2 \nmid d$ in the second case. Now from Remark 4.11 we have that $N(\epsilon) = (A + \sqrt{D})(A - \sqrt{D}) = A^2 - D = 1$ (if D is monic). In general if D is not monic, then $D = A^2 - b^2$ for some $b \in \mathbb{F}_q^*$. ■

The following theorem presents a better bound for $h_{\mathcal{O}}$.

Theorem 4.29 *Suppose* $F = \mathbb{F}_q(x, \sqrt{D})$ *is a real quadratic function field either of the form (I) or (II) in the above Corollary. If there exists an irreducible* P *with* $\deg(P) \leq d-1$ *and* $\left(\frac{D}{P}\right) = 1$. *Then* $h_{\mathcal{O}} \geq \left\langle \frac{d}{\deg(P)} \right\rangle$ *where* $\langle \alpha \rangle$ *denotes the smallest odd integer larger than or equal to* α.

Proof. Because of the form of D and Theorem 4.10 we know that $h_{\mathcal{O}}$ is odd. From $\left(\frac{D}{P}\right) = 1$ we know that $P\mathcal{O} = \mathfrak{P}\bar{\mathfrak{P}}$. Let n be the order of the ideal class $[\mathfrak{P}]$, then $2 \nmid n$ and $n \mid h_{\mathcal{O}}$. $\mathfrak{P}^n$ is a principal ideal by definition of n, so suppose $\mathfrak{P}^n = U + V\sqrt{D}, U, V \in \mathbb{F}_q[x]$. Then $U^2 - V^2 D = cP^n$ for some $c \in \mathbb{F}_q^*$. Since $2 \nmid n$ we know that (U, V) is a non-trivial solution and hence Lemma 4.24 tells us that $\deg(P^n) \geq d$. Therefore $h_{\mathcal{O}} \geq n \geq \frac{d}{\deg(P)}$. Since $2 \nmid h_{\mathcal{O}}$ it follows that $h_{\mathcal{O}} \geq \left\langle \frac{d}{\deg(P)} \right\rangle$. ■

We are now in a position to determine all real quadratic function fields of Chowla type with class number one. The task is accomplished by bounds provided by the Hasse-Weil theorem as well as the Riemann-Roch theorem. It is also essential to the result below that we have an elegant formula for the regulator of these function fields (determined in Example 2.37).

Theorem 4.30 *Let* $F = \mathbb{F}_q(x, \sqrt{D})$ *be a real quadratic function field. Suppose* $2 \nmid q$, $D = A^2 + a$, $a \in \mathbb{F}_q^*$, $\deg(A) = d \geq 1$. *If* $h_{\mathcal{O}} = 1$, *then* $q = 3$, $d \leq 4$; $q = 5$, $d \leq 2$; *or* $q \geq 7$, $d = 1$.

Proof. The proof is based on a fairly standard argument using constant field extensions. The regulator of F as determined in Example 2.37 is $d = \deg(A)$. The genus of F is $g_F = d - 1$.

Let $n = 2g_F - 1$ and $F' = \mathbb{F}_{q^n} F$ a function field with constants $\mathbb{F}_{q^n}$ and genus $g_{F'} = d - 1$ (the genus is invariant under constant field extensions). Let N_1' be the number of prime divisors

of F' with degree 1. The Hasse-Weil bound give us

$$N_1' \geq q^n + 1 - 2g_{F'}q^{\frac{n}{2}}$$

F'/F is a constant field extension of degree n. Now let $Q \in S(F'/\mathbb{F}_{q^n})$ be a place of degree 1 of F', and P the unique place of F lying under Q. As Q has degree 1 we have that the residue field $\bar{F}_Q' = \mathbb{F}_{q^n}$, and hence

$$n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\bar{F}_Q' : \mathbb{F}_q] = [\bar{F}_Q' : \bar{F}_P][\bar{F}_P : \mathbb{F}_q] = f(Q \mid P)\deg(P)$$

which implies that $\deg(P)$ divides n. It follows that $(n/\deg(P))P$ is an integral divisor of degree n of F. As there are at most n places Q above P, we see that in this way we have constructed at least N_1'/n integral divisors of degree n of F. On the other hand Lemma 2.48 tells us that there are exactly

$$\frac{h_F}{q-1}(q^{n+1-g} - 1)$$

such places (n was chosen in this way). Hence we obtain

$$\frac{h_F}{q-1}(q^{n+1-g} - 1) \geq \frac{N_1'}{n} \geq \frac{q^n + 1 - 2g_{F'}q^{\frac{n}{2}}}{n}$$

or rearranging

$$\begin{aligned} h_F &\geq (q-1)\frac{q^n + 1 - 2(d-1)q^{\frac{n}{2}}}{n(q^{n+1-(d-1)} - 1)} \\ &= (q-1)\frac{q^{2d-3} + 1 - 2(d-1)q^{\frac{2d-3}{2}}}{(2d-3)(q^{d-1} - 1)} \end{aligned}$$

Now Schmidt's formula tells us that $h_{\mathcal{O}} = h_F/R = h_F/d$ and hence we obtain

$$h_{\mathcal{O}} \geq (q-1)\frac{q^{2d-3} + 1 - 2(d-1)q^{\frac{2d-3}{2}}}{d(2d-3)(q^{d-1} - 1)}$$

A simple calculation now confirms the statement of the theorem. ■

We note from the bounds obtained above that only a finite number of cases have to be checked. Since we know what the regulator is in each case and have a formula from Section 2.7 for the class number of the function field this is a relatively easy task. I will not provide the details here, but simply state the final result. When $d = 1$, we always have that $g_F = 0$ and $h_{\mathcal{O}} = 1$ hence we don't consider this case in the theorem below.

Theorem 4.31 (All fields of Chowla type with $h_{\mathcal{O}} = 1$) *Let $F = F_q(x, \sqrt{D})$, $D = A^2 + a$, $a \in \mathbb{F}_q^*$, $A \in \mathbb{F}_q[x]$ monic with $\deg(A) = d \geq 2$. There are precisely six such fields with $h_{\mathcal{O}} = 1$, namely:*

$$\begin{aligned} q &= 3: \quad D = A^2 + 1 \text{ with } A = x^3 - x \pm 1,\ x^2 + 1,\ x^2 \pm x - 1 \\ q &= 5: \quad D = x^4 + 2. \end{aligned}$$

4.3.3 Infinitely many real quadratic fields with class number one

The title of this section can be misleading as it implies that the Gauss conjecture has been solved in the function field case. This is however not the case as our construction allows the field of constants $\mathbb{F}_p$ to vary. The precise result is that for all sufficiently large primes p, there is a polynomial $D_p(x)$ of degree six with distinct roots, such that the ring of integers $\mathcal{O} = \mathbb{F}_p[x, \sqrt{D_p}]$ in $F = \mathbb{F}_p(x, \sqrt{D_p})$ is principal (where F is real quadratic). The result of this section was first pointed out by T.A Schmidt [Sa]. It is important to note that the construction here is also not a solution to Conjecture 3.9 since the polynomials $D_p(x)$ obtained do not come from the reduction of some fixed hyperelliptic curve over $\mathbb{Q}$.

The result follows relatively easily from the work done by L.M Adleman and M.-D.A Huang [AH], where they study the moduli space of genus 2 curves over the finite field $\mathbb{F}_p$. It relies upon Schmidt's formula (Proposition 2.17) which we recall says the following in the real quadratic case:

$$h_F = h_{\mathcal{O}} \cdot R, \text{ where } R \text{ is the regulator of } F$$

Now noting that if $\epsilon = A + B\sqrt{D}$ is a fundamental unit of F, then $|\epsilon| = R \geq \frac{1}{2}\deg(D)$ we can say the following: Suppose the class number of F, h_F is prime (The Jacobian of F has a prime number of $\mathbb{F}_p$-rational points) then since $R \geq \frac{1}{2}\deg(D)$, it follows that $R = h_F$ and consequently $h_{\mathcal{O}} = 1$. This is the essence of the proof. Of course the hard work lies in finding the function fields F with a prime number of $\mathbb{F}_p$-rational points on their Jacobians.

We have the following key theorem:

Theorem 4.32 ([AH, Prop. 1, pg. 15]) *For all sufficiently large primes p, there exists $D(x) = D_p(x)$ of degree 6 in $\mathbb{F}_p[x]$ with distinct roots such that h_F is prime for the function field $F = \mathbb{F}_p(x, \sqrt{D})$.*

All that remains to show by the above remarks is that F can be chosen to be real. Since D is by construction of even degree we need only show that we can choose its leading coefficient to be a square in $\mathbb{F}_p$. Given $f(x) = \prod_{i=1}^{n}(x - \alpha_i)$ in $\mathbb{F}_p[x]$ and $M = \begin{pmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{pmatrix}$ in $SL_2(\mathbb{F}_p)$, define

$$f^M(x) = \prod_{i=1}^{n}(x - \frac{M_{11}\alpha_i + M_{12}}{M_{21}\alpha_i + M_{22}})$$

Lemma 4.33 ([AH, Lemma 31, pg. 101]) *Let p be an odd prime and $D(x) = a_6x^6 + ... + a_0 \in \mathbb{F}_p[x]$. Suppose that $D(x) = a_6 f_D(x)$ has distinct roots. If $\tilde{D}(x) = a_6 f_D(\frac{A_{11}}{A_{21}}) f_D^{A^{-1}}(x)$ for some $A \in SL_2(\mathbb{F}_p)$, then the curves of the equations $y^2 - D(x)$ and $y^2 - \tilde{D}(x)$ are isomorphic over $\mathbb{F}_p$.*

Thus given a specific $D(x)$ as in the main theorem above, if a_6 is a non-square it suffices to find some $A \in SL_2(\mathbb{F}_p)$ such that $f_D(\frac{A_{11}}{A_{21}})$ is also a non-square (the product of two non-square's is a square in $\mathbb{F}_p^*$ since both must have odd order and consequently their product hence has even order). Clearly it suffices to show that f_D does take on some non-square value. Unfortunately this is not guaranteed by the fact that f_D has distinct roots. For example if $p = 11$ then $D(x) = x^5 + 4$ has distinct roots, but takes all of $\mathbb{F}_p$ to squares. On the other hand, if the degree of f is small enough, then having distinct roots does imply that f must take on non-square values. L. Carlitz seems to have been the first to attack this problem. We have the following Lemma (see [Ca]) due to him:

Lemma 4.34 *Let p be an odd prime. If $f(x) \in \mathbb{F}_p[x]$ has degree less than or equal to $\sqrt{p} - 1$ and f takes on only square values, then f is a square in $\mathbb{F}_p[x]$.*

The result now follows since $D(x)$ given by the main theorem is square-free and hence we can find an $A \in SL_2(\mathbb{F}_p)$ such that $f_D(\frac{A_{11}}{A_{21}})$ is a non-square.

4.3.4 Ankeny-Artin-Chowla's conjecture

A well known conjecture of Ankeny-Artin-Chowla [AAC] states that if $K = \mathbb{Q}(\sqrt{p})$ is a real quadratic number field with prime discriminant p, then the conductor of the fundamental unit

of K is not divisible by p. In this section we show that the analogous conjecture is true in the function field case without any hypothesis on the discriminant. It was Jing Yu and Jiu-Kang Yu [YY] who proved this interesting property in the function field case.

Essential in the proof of this result will be a theorem of R.C Mason. A simple proof of this result was found by N. Snyder [Sn].

Theorem 4.35 (Mason's Theorem) *Let a, b, and c be relatively prime polynomials in $k[x]$ for some algebraically closed field k. Suppose that $a + b = c$ and a', b', and c' are not all zero (where the prime indicates the derivative). Then $\deg(c) \leq n_0(abc) - 1$ where $n_0(abc)$ denotes the number of distinct roots of the polynomial abc.*

Let $\mathbb{F}_q$ be a finite field of odd characteristic. The following theorem is the main result:

Theorem 4.36 *Let $F = \mathbb{F}_q(x, \sqrt{D})$ be a real quadratic function field. Let $u = r + s\sqrt{D}$ be a unit of the ring of integers $\mathcal{O}^*$ of F. Then $\deg(\gcd(D, s)) \leq g$ where $g = \deg(D)/2 - 1$ is the genus of F.*

Proof. Let $\bar{\mathbb{F}}_q$ be an algebraic closure of $\mathbb{F}_q$. Let $\tilde{D} = \gcd(D, s)$, $s = \tilde{D}\tilde{s}$, $\deg(\tilde{D}) = \tilde{g}$, $\deg(\tilde{s}) = m$, then $\deg(r^2 - Ds^2) = 0$ which implies that $\deg(r) = m + g + \tilde{g} + 1$. Let $a = r^2, b = -D(\tilde{D}\tilde{s})^2$, and $c = N_{F/\mathbb{F}_q(x)}(u) \in \bar{\mathbb{F}}_q^*$. Then $a + b = c$ and $\gcd(a, b, c) = 1$. Now from Mason's Theorem above it follows that

$$\max \deg\{a, b, c\} \leq n_0(abc) - 1$$

Now in our case $n_0(abc) \leq \deg(rD\tilde{s}) = 2m + 3g + \tilde{g} + 3$. Consequently:

$$\begin{aligned} \deg(a) &= \deg(r^2) \\ &= 2\deg(r) \\ &= 2m + 2g + 2\tilde{g} + 2 \\ &\leq 2m + 3g + \tilde{g} + 3 - 1 \\ \text{or } \tilde{g} &\leq g \end{aligned}$$

which is what we wanted to prove. ■

Corollary 4.37 *Let $D \in \mathbb{F}_q[x]$ be monic, square-free, and of even degree ≥ 2. Let $\epsilon = r + s\sqrt{D}$ be a fundamental unit of $\mathcal{O} = \mathbb{F}_q[x, \sqrt{D}]$. Then D does not divide s. In other words, the discriminant D does not divide the conductor of the order $\mathbb{F}_q[x, \epsilon]$. Where the conductor of $\mathbb{F}_q[x, \epsilon]$ is defined to be the largest ideal of $\mathcal{O}$ which is contained in $\mathbb{F}_q[x, \epsilon]$.*

Proof. Clear from the above theorem. ■

Above we have dealt with the odd characteristic case. The even characteristic case can also be found in [YY].

4.4 Computation and Application

Interest in quadratic function fields over a finite field has increased in recent years in the search for secure cryptosystems. Initially elliptic curves cryptosystems were considered (the genus 1 case), but more recently higher genus (hyperelliptic) curves have also been considered. Originally pursued mainly for purely aesthetic reasons, elliptic curves have recently become an essential tool in several important areas of application including coding theory, pseudo-random number generation, number theory algorithms and public key cryptography. On the other hand hyperelliptic curves have not received as much attention by the research community. Recently however, applications of hyperelliptic curves have been found to areas outside algebraic geometry. Hyperelliptic curves were a key ingredient in Adleman and Huang's [AH] random polynomial-time algorithm for primality proving (as well as proving the result in Section 4.3.3). Hyperelliptic curves have also been considered in the design of error-correcting codes (e.g. [Lb2]), in integer factorization algorithms [LPP], and in public key cryptography [Ko2].

For this reason we would like efficient algorithms for working out the arithmetic in the Jacobians of hyperelliptic curves as well as computing key invariants such as the number of rational points and the divisor class number. A fair amount of work has been done in this area, much of it at the Centre for Applied Cryptographic Research, University of Waterloo. See [MWZ] for an introduction to hyperelliptic curves over a finite field and an efficient algorithm for working out the sum of points on the Jacobian in terms of reduced divisors. We can also ask ourselves whether it is computationally more efficient to work in real quadratic or imaginary quadratic function fields, since we saw in Section 4.1 that in certain cases we can move between

the two by a birational transformation. This question was studied by S. Paulus and H.-G. Rück [PR] and A. Stein [St3]. The conclusion of the former paper is that imaginary representations should be used whenever possible, whereas the latter seems to indicate that the complexity is essentially identical. It also appears (quite naturally) that working in characteristic 2 is the most computationally effective.

We come now specifically to the use of quadratic function fields in cryptography. In 1989 hyperelliptic curve cryptosystems where first introduced by N. Koblitz [Ko2] as a natural extension of the existing elliptic curve cryptosystems (see [Me], [Ko1]). The Jacobians of hyperelliptic curves turned out to be a rich source of finite abelian groups for defining one-way functions. N. Koblitz's initial scheme was based on imaginary quadratic function fields although subsequently real quadratic function fields have also been used. See for example [SSW], where a secure key exchange protocol was suggested based on the infrastructure in the principal ideal class of real quadratic function fields. There are however several avenues of research which have to be further pursued before hyperelliptic curve cryptosystems can be adopted in practical applications. These being:

(1) The most important issue is with regards to the security of hyperelliptic curve cryptosystems. More precisely, the security relies upon the complexity of the hyperelliptic curve discrete logarithm problem (HCDLP) which is the following: given a hyperelliptic curve C over a finite field k, and given reduced divisors $D_1, D_2 \in \operatorname{Jac} C(k)$, determine a positive integer n such that $D_1 = nD_2$, provided such an integer exists. If the order of the divisor D_1 is divisible by a large prime r, then the best known algorithm for the HCDLP is an exponential one and takes $O(\sqrt{r})$ steps. However for special hyperelliptic curves it may be possible to reduce the HCDLP to the discrete logarithm problem (DLP) in a small extension finite field. Since there are subexponential-time algorithms known for the DLP, hyperelliptic curves of this type would offer no additional security over finite fields. Such a reduction was accomplished for elliptic curves by Menezes, Okamoto and Vanstone [MOV]. Frey and Rück [FR] extended this reduction to more general abelian varieties. This reduction is efficient for some classes of hyperelliptic curves but needs to be explored more fully. Adleman, DeMarais and Huang [ADH] recently discovered an algorithm for HCDLP which takes subexponential time if the genus g of the curve is large. More precisely if the curve is defined over $\mathbb{F}_p$, then the genus g should satisfy $\log p \leq (2g+1)^{0.98}$. Their algorithm works only in odd characteristic and it would be interesting to extend it to the even characteristic case as well.

(2) Classification of the isomorphism classes of hyperelliptic curves over a finite field. This was done for the genus 2 case in [AH].

(3) Further research into the efficient implementation of the addition rule in the Jacobian of a hyperelliptic curve. In this line see for example the recent thesis by T. Lange [La] which investigates efficient arithmetic on low genus hyperelliptic curves.

For a further review on this subject see N. Koblitz's book [Ko3]. The ideas expounded above demonstrate that the study of quadratic function fields are rewarding not only from a purely mathematical perspective, but also from an applications based perspective.

Chapter 5

General Function Fields over $\mathbb{F}_q$ and Heuristics

The focus of this dissertation has indeed been that of quadratic function fields over $\mathbb{F}_q$ for which we developed much of the important theory in Chapter 2. The theory required to understand the results in this chapter is however rather vast and a divergence from our main theme. I therefore chose to simply state results giving some idea of the methods used to obtain them. We will in this chapter present the results of Lachaud and Vladut [LV] which give solutions to some of the problems set out in Chapter 3. The most important result being an analogue of the number field Weak Gauss Conjecture. Hereafter we present some results regarding general imaginary extensions of $\mathbb{F}_q(x)$. We then proceed to examine some heuristic results regarding class numbers in function fields. Finally we present an outlook on the class number problem in function fields and present some ideas for future research in this direction.

5.1 The Weak Gauss Theorem

The solution to Problem BB as set out in Problem 3.10 utilizes many deep results in the theory of classical modular curves such as ramification structure and reduction properties. Geometrically speaking we are searching for infinitely many Galois coverings of the projective line $\mathbb{P}(\bar{\mathbb{F}}_q)$ (which correspond to Galois extensions of the rational function field $\mathbb{F}_q(x)$) such that the ring of S-integers is principal. This covering is provided by the j-invariant of a modular curve. The details can be found in [LV]. This is their main result:

Theorem 5.1 *Let $q = 4, 9, 25, 49,$ or 169. Let $P \in S(\mathbb{F}_q(x)/\mathbb{F}_q)$ be a prime of degree one. Then there are infinitely many extensions (K, S) of the pair $(\mathbb{F}_q(x), \{P\})$ such that:*

(1) The prime P splits completely in K.

(2) The field K is a Galois extension of $\mathbb{F}_q(x)$.

(3) The ring $\mathcal{O}_S$ is principal.

The proof of this result is a step towards the analogue of Gauss' conjecture, although it would appear that new methods are needed in order to attack Gauss' long standing conjecture. The reason I say this is that it is quite rare that the coverings found in the theorem are hyperelliptic. We note that the theorem above holds for five different constant fields $\mathbb{F}_q$, where $q = p^2$ for some prime p. It would be interesting to find more constant fields $\mathbb{F}_q$ for which we could solve this problem, and perhaps even some where q is not a square.

We note that since Problem BB is stronger than for example Problem AB, it is possible using the theorem above to also give solutions to that problem. The authors also apply Drinfeld modular curves to solve the Problem BA in a specific case. This is an exciting area of research with many open problems. It is also a triumph of algebraic geometry in that it demonstrates how an algebraic problem can be solved using geometric techniques.

5.2 General Imaginary extensions of $\mathbb{F}_q(x)$

We begin with the situation of imaginary bicyclic biquadratic function fields over $\mathbb{F}_q$. By this we simply mean quartic extensions of the rational function field $\mathbb{F}_q(x)$ with Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. By imaginary in this situation we mean that the prime at infinity in $\mathbb{F}_q(x)$ does not split completely. This situation also has its counterpart in the classical case where we are interested in quartic extensions of $\mathbb{Q}$ with Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and in which the archimedean valuation does not split completely. In 1974 E. Brown and C.J. Parry [BP] determined that there are exactly 47 such number fields with principal ring of integers. More recently this situation has been studied in function fields. This was done by X. Zhang [Zh2] in the odd characteristic case and by Y. Aubry and D. Le Brigand [AL] in the even characteristic case. The techniques and methods used for studying such function fields are derived from

results in quadratic function fields, since such quartic extensions can be represented as the compositum of two quadratic extensions of $\mathbb{F}_q(x)$. In [AL] it is shown that up to isomorphism there are 7 such fields in the even characteristic with principal ring integers.

We now come to another situation, namely that of cyclotomic extensions of $\mathbb{F}_q(x)$ with principal ring of integers. In the classical case of number fields, K. Yamamura [Ya] showed in 1994 that there are exactly 172 imaginary abelian number fields with class number one. Of course this result is inclusive of imaginary cyclic extensions of $\mathbb{Q}$ with class number one. To the best of my knowledge such a complete determination has not been made in the function field situation. We do however have a determination of all imaginary cyclotomic function fields over $\mathbb{F}_q$ having principal ring of integers. This determination was done in two papers by S. Sémirat. The first paper [Se1] which appeared in 2000 deals with the case of the extension being of prime power degree. One year after the above result he proceeds to determine all imaginary cyclotomic function fields over $\mathbb{F}_q$ having principal ring of integers. His result which can be found in [Se2] is that there are up to isomorphism exactly 17 such function fields.

5.3 Heuristics

In Section V of *Disquisitiones Arithmeticae*, C.F. Gauss writes at art. 304:

> It is a curious question and it would not be unworthy of a geometer's talent to investigate the law in accordance with which [positive non-square] determinants having one class in a genus becoming increasingly rare. Up to the present we cannot decide theoretically nor conjecture with any certainty by observation whether there are only a finite number of them (this hardly seems probable), or that they occur infinitely rarely, or that their frequency tends more and more to a fixed limit. The average number of classes increase by a ratio that is hardly greater than that of the number of genera and far more slowly than the square root of the determinants.

Gauss was speaking above in the language of binary quadratic forms. In modern language this question can be reformulated as follows: The above mentioned determinants are the discriminants of real quadratic fields. If $D > 0$ is such a discriminant, then we denote by $Cl(D)$ the class group of the corresponding real quadratic field $K = \mathbb{Q}(\sqrt{D})$, and by $\mathcal{O}_K$ its ring of integers. Then $|Cl(D)| = 1$ if and only if $\mathcal{O}_K$ is a PID. Let $Cl_0(D) \subset Cl(D)$ be the subgroup

of elements of odd order; then $|Cl_0(D)|$ equals the number of classes in each genus of which Gauss speaks. Let $\triangle$ be the set of discriminants D for which $|Cl_0(D)| = 1$. Gauss says that "It hardly seems probable" that $\triangle$ is finite and also asks if $\triangle$ has a natural density.

In 1983 Cohen-Lenstra [CL] introduced a very interesting heuristic assumption to explain the distribution of class numbers of number fields. They made observations like the fact that the odd part of the class group of imaginary quadratic fields is quite rarely non-cyclic. The scarcity of non-cyclic groups was attributed by H.W. Lenstra to the fact that they have many automorphisms. This leads to the heuristic assumption that a finite abelian group G appears as a class group with a frequency inversely proportional to the order of the automorphism group of G. This principle succeeded in explaining a number of puzzling empirical observations which had been made over the years. There heuristics predict that the density of the set $\triangle$ described above does exist and equals:

$$1/\prod_{n=2}^{\infty}(1-\frac{1}{2^n})\zeta(n) = 0,7544...$$

where $\zeta(n)$ is the Riemann zeta function. This and other predictions have been confirmed by numerous calculations.

We however are here interested in heuristics explaining the orders of class groups of function fields over a finite field. Four years after the famous Cohen-Lenstra paper, E. Friedman and L. Washington [FW] address this issue. It seems that the basis for the assumptions of the Cohen-Lenstra heuristics are clearer in the situation of function fields. Friedman and Washington propose a natural conjecture that predicts and explains the Cohen-Lenstra heuristic principle for the function field analogue of the set of imaginary quadratic fields. This new conjecture amounts to an equidistribution statement for the Frobenius map acting on various Jacobian varieties and is explicit enough that one may try to prove it. This would suggest that instead of regarding class groups as a random abelian group G with weight $1/|Aut(G)|$, we can think of class groups as cokernels of large random matrices. To date neither assumption can be placed on a rigorous basis, but they do explain empirical observations very accurately.

The situation in real quadratic function fields is slightly different however as the order of the ideal class group depends upon both the class number of the function field as well as the regulator. The Cohen-Lenstra heuristics predict in this situation that class groups ought to behave as the quotient of a random abelian group (once again weighted by the inverse of its

number of automorphisms) by a cyclic subgroup generated by a random point. In the function field case this can be interpreted as follows: Recalling Example 3.6 the above heuristics assume that divisor class $[P_1 - P_2]$, where P_1 and P_2 are the point lying above ∞, should behave as a random $\mathbb{F}_q$-rational point on the Jacobian. The predictions of the Cohen-Lenstra heuristics in the situation in real quadratic function fields are therefore precisely the same as those of real quadratic number fields although the geometric interpretation is somewhat more intuitive. For example we once again have that the probability that the odd part of the ideal class group of a real quadratic field over $\mathbb{F}_q$ is trivial is roughly $0,7544$.

As stated above the Cohen-Lenstra conjectures in the function field situation are more reachable than those in number fields and are supported not merely by empirical evidence but also by strong theoretical evidence. In fact, in 1994 Jiu-Kang Yu [Yu2] proved theorems in this direction where the exact values predicted by the Cohen-Lenstra heuristics came out. To state one of his results, let q be odd and p be an odd prime relatively prime to q (in this case p is not the characteristic of $\mathbb{F}_q$). Let $\hat{\mathbb{Z}}_p$ be the ring of p-adic integers and G be a finite abelian p-group. Moreover for any $n \geq 1$, let $X_n(\mathbb{F}_q)$ be the set consisting of $D \in \mathbb{F}_q[x]$, monic, square-free and of degree n. Given $D \in X_n(\mathbb{F}_q)$, let Cl_D denote the ideal class group of $\mathcal{O} = \mathbb{F}_q[x, \sqrt{D}]$. The following theorem of his concerns the probability that the p-part of an ideal class group of an imaginary quadratic function field is isomorphic to a given p-group. We recall that when we tensor a finite group such as the class group Cl_D with the ring of p-adic integers $\hat{\mathbb{Z}}_p$ and view the decomposition into a product of cyclic groups, all primes other than p vanish.

Theorem 5.2 *For any $n \geq 3$ odd, as q ranges over odd prime powers such that $\gcd(p, q) = 1$ and $p \nmid q - 1$, the limit*

$$\lim_{q \to \infty} \frac{\#\{D \in X_n(\mathbb{F}_q) : Cl_D \otimes \hat{\mathbb{Z}}_p \cong G\}}{\#X_n(\mathbb{F}_q)} = d_n(G)$$

exists. Furthermore

$$\lim_{n \to \infty,\ n \text{ odd}} d_n(G) = \frac{c_p}{\#Aut(G)}$$

where $c_p = \prod_{n=1}^{\infty}(1 - p^{-n})$.

Yu's theorem should be compared with the following strong conjectures based on the Cohen-Lenstra heuristics, where q is not allowed to vary:

Conjecture 5.3 *Given q odd and prime p with* $\gcd(p,q) = 1$. *Then*

$$\lim_{n\to\infty,\ n\ odd} \frac{\#\{D \in X_n(\mathbb{F}_q) : Cl_D \otimes \hat{\mathbb{Z}}_p \cong G\}}{\#X_n(\mathbb{F}_q)} = \frac{c_p}{\#Aut(G)}$$

Yu also proved other theorems in this direction, see [Yu2] for the details. The proofs of his results are based on Weil's Conjecture as proved by Deligne and rely on some deep algebraic geometry.

Another strong result in this area is due to C. Friesen [Fr1]. He in fact proves one of the predictions of the Cohen-Lenstra heuristics in the genus one real quadratic case. To state his result: Let $D(x) \in \mathbb{F}_q[x]$ be a monic irreducible quartic, where $\mathbb{F}_q$ is of odd characteristic. Let $\Omega(D)$ denote the odd part of the divisor class group of degree 0 of the function field $\mathbb{F}_q(x, \sqrt{D})$. Let G be a finite abelian group of odd order and define S_G to be the set of monic irreducible quartics D such that $\Omega(D) = G$. We say that D belongs to G if $D \in S_G$.

His main result is that under the above conditions the distribution of the class groups for those D belonging to G is identical to the distribution of $G/\langle\sigma\rangle$, where σ is a random element of G. This is precisely what the Cohen-Lenstra heuristics predict. From these and other results there seem to be many possibilities and exciting avenues of research in this topic of heuristics of class groups in function fields.

5.4 Conclusion

Thus experimental evidence and heuristics indeed seem to show that Gauss' long standing conjecture is true in both the classical context and in the context of function fields. This is indeed a great motivation to continue investigation into this area of number theory as a mathematician ought never to be satisfied until a satisfactory proof of a claim is given. The class number one problem in function fields therefore remains an open area of research. Firstly we would like a satisfactory proof that there are indeed infinitely many real quadratic function fields with ideal class number one. It is my opinion that a significant step towards this will be a better understanding of continued fraction expansions and the regulator in quadratic function fields. In the case of real quadratic number fields Cohen [Co, Ch. 5] also suggests that the regulator is "the main source of our ignorance about real quadratic fields". Secondly there is the problem of the determination of all general imaginary extensions of $\mathbb{F}_q(x)$ with ideal class

number one. Finally there is the less interesting problem of determining a complete list of imaginary quadratic function fields of class number 3 or higher as has been done in the classical situation.

In the function field situation there seem to be more tools available for studying these problems than in its classical counter part. For example the Riemann hypothesis is often assumed in order to prove many of the classical results, whereas in the function field situation we already have a proof thereof. We also have tools such as the d'th power reciprocity law with a remarkably elegant formulation not found in the classical case. These and other results give us hope that some of these class number problems in function fields may indeed sometime in the near future be solved. Let us labour in that vein.

Appendix A

Algebraic function field basics

The following definitions and results are standard and can be found in Stichtenoth [St]. We begin with the definition of an algebraic function field in one variable over a field k, which we will simply refer to as a function field over k.

Definition A.1 *An algebraic function field F/k in one varaible over k is an extension field $F \supseteq k$ such that F is a finite algebraic extension of $k(x)$ for some element $x \in F$ which is transcendental over k.*

We will always assume that k is algebraically closed in F (or that k is the full constant field of F). By this we mean that k is the exact set of elements of F which are algebraic over k.

Essential in the study of function fields is the definition of a *valuation ring.*

Definition A.2 *A valuation ring of the function field F/k is a ring $\mathcal{O} \subseteq F$ with the following properties:*

(1) $k \subsetneq \mathcal{O} \subsetneq F$, and

(2) for any $z \in F$, $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

A valuation ring $\mathcal{O}$ of F/k turns out to be a local ring and a principal ideal domain. Let P denote the unique maximal ideal of $\mathcal{O}$. We will call such a P a *place* or a *prime* of F/k. We will denote by $S(F/k)$ the set of all primes of F/k. Note that $\mathcal{O}$ is uniquely determined by P since $\mathcal{O} = \{z \in F : z^{-1} \notin P\}$. Hence $\mathcal{O}_P := \mathcal{O}$ is called *the valuation ring of the place P*. Since $\mathcal{O}$ is a PID, we can find an element $t \in P$ such that $P = t\mathcal{O}$. Such an element is called a *prime*

element, or a *uniformizing parameter* for P. We define the *degree* of a prime P to be the index $[\mathcal{O}_P/P : k]$.

We now come to the definition of a discrete valuation function.

Definition A.3 *A discrete valuation of F/k is a function $v : F \to \mathbb{Z} \cup \{\infty\}$ with the following properties:*

(1) $v(x) = \infty \Leftrightarrow x = 0$.

(2) $v(xy) = v(x) + v(y)$ *for any* $x, y \in F$.

(3) $v(x + y) \geq \min\{v(x), v(y)\}$ *for any* $x, y \in F$.

(4) There exists an element $z \in F$ *with* $v(z) = 1$.

(5) $v(a) = 0$ *for all* $0 \neq a \in k$.

To each prime P we can associate a discrete valuation v_P in the following way: choose a uniformizing parameter t for P. Then every $0 \neq z \in F$ has a unique representation as $z = t^n u$ with $u \in \mathcal{O}_P^*$ and $n \in \mathbb{Z}$. Define $v_P(z) := n$ and $v_P(0) := \infty$. Conversely for any discrete valuation v of F/k, we obtain a prime $P = \{z \in F : v(z) > 0\}$ with associated valuation ring $\mathcal{O}_P = \{z \in F : v(z) \geq 0\}$. Hence there exists a bijection between the primes of F/k and the discrete valuation functions on F/k.

We now define the divisor group of the function field F/k.

Definition A.4 *The free abelian group which is generated by the primes of F/k is denoted by $\mathcal{D}_F$ and is called the divisor group of F/k.*

To each $x \in F$ we can associate a divisor (x) in the following way:

$$(x) = \sum_{P \in S(F/k)} v_P(x) P$$

This definition makes sense since any $x \in F$ has only finitely many zeros and poles. We define the *degree* of a divisor $D = \sum_{P \in S(F/k)} n_P P \in \mathcal{D}_F$ to be

$$\deg(D) := \sum_{P \in S(F/k)} n_P \deg P$$

We now define an important subgroup of $\mathcal{D}_F$.

Definition A.5 *The group* $\mathcal{P}_F = \{(x) : 0 \neq x \in F\}$ *is called the group of principal divisors of* F/k.

Since the sum of two principal divisors is again a principal divisor this becomes a subgroup of $\mathcal{D}_F$. Consequently we can define the factor group

$$Cl_F := \mathcal{D}_F/\mathcal{P}_F$$

called the *divisor class group*. Moreover we also define the following subgroups of $\mathcal{D}_F$ and Cl_F respectively.

Definition A.6 *The group*

$$\mathcal{D}_F^0 = \{A \in \mathcal{D}_F : \deg(A) = 0\}$$

is called the group of divisors of degree 0, *and*

$$Cl_F^0 = \{[A] \in Cl_F : \deg[A] = 0\}$$

is called the group of divisor classes of degree 0. *We define the class number of the function field* F/k *to be*

$$h_F = \left|Cl_F^0\right|$$

We are frequently interested in studying special subrings of a function field F/k, for example valuation rings. We come now to a special class of subrings known as *holomorphy rings*.

Definition A.7 *Let* $\emptyset \neq S \subsetneq S(F/k)$. *Let*

$$\mathcal{O}_S := \{z \in F : v_P(z) \geq 0,\ \forall P \notin S\}$$

Any ring $R \subseteq F$ which is of the form $R = \mathcal{O}_S$ for some $\emptyset \neq S \subsetneq S(F/k)$ is called a holomorphy ring. Note that our definition of $\mathcal{O}_S$ differs slightly from that in [St]. The relationship is simply that our $\mathcal{O}_S$ is for him $\mathcal{O}_{S(F/k)\setminus S}$. We do this in order that our notation coincides with the standard definition of the ring of S-integers, which are a special class of holomorphy rings in which S is chosen to be finite.

Using the Strong Approximation Theorem it is possible to show that that any holomorphy ring is in fact a Dedekind domain which we define as to be:

Definition A.8 *A Dedekind domain is a Noetherian, integrally closed integral domain in which every non-zero prime ideal is maximal.*

Let B be a Dedekind domain. We can form the well known *ideal class group* of B which is the quotient of the fractional ideals of B by the principal ideals. We will denote this class group by $Cl(B)$. The order of this group, the *ideal class number*, plays an important role in number theory. In particular a Dedekind domain is a PID if and only if the class number equals one.

References

[ADH] L.M. Adleman, J. DeMarais, M.-D. A. Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields, Algorithmic Number Theory, Lecture Notes in Computer Science, **877** (1994), 28-40.

[AH] L.M. Adleman, M.-D. A. Huang. *Primality Testing and Abelian Varieties over Finite Fields*, Lecture Notes in Math., Vol 1512, Springer-Verlag, Berlin, 1992.

[AAC] N.C. Ankeny, E. Artin, S.Chowla. The class number of real quadratic fields, Annals of Math. **56** (1953), 479-492.

[Ar] E. Artin. Quadratische Körper im Gebiet der hoheren Kongruenzen I, II, *Math. Zeitschrift* **19** (1924) 153-246.

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

[BP] E. Brown, C. Parry. The imaginary bicyclic biquadratic fields with class number 1, *J. reine angew. math.* **226** (1974), 118-120.

[CM] David Cardon and M. Ram Murty. Exponents of class groups of quadratic functions fields over finite fields, *Canad. Math. Bull.* Vol 44 (4), 2001, 398-407.

[Ca] L. Carlitz. A problem of Dickson's, *Duke Math. J.* **14** (1947) 1139-1140.

[Co] H. Cohen. *A Course in Computational Algebraic Number Theory*, Springer-Verlag, Berlin, 1993.

[CL] H. Cohen, H.W. Lenstra. Heuristics on class groups of number fields, in "Number Theory, Noordwijkerhout, 1983", Notes in Math., Vol. 1068, 33-62, Springer-Verlag, New York, 1984.

[Dr] V.G. Drinfeld. *Elliptic modules* (Russian), Math. Sbornik (N.S.) **94** (136) (1974) 594-627, 656.

[FH] K. Feng, W. Hu. On real quadratic function fields of Chowla type with ideal class number one, *Proc. Amer. Math. Soc.* **127** (1999) 1301-1307.

[FR] G. Frey, H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves, *Mathematics of Computation*, **62** (1994), 865-874.

[FW] E. Friedman and L.C. Washington. On the distribution of divisor class groups of curves over a finite field, in "Théorie des Nombres, Québec, 1987", 227-239, De Gruyter, Berlin, 1989.

[Fr1] C. Friesen. A special case of Cohen-Lenstra heuristics in function fields, Number theory (Ottawa, ON, 1996), 99105, CRM Proc. Lecture Notes, 19, Amer. Math. Soc., Providence, RI, 1999.

[Fr2] C. Friesen. Class Number Divisibility in Real Quadratic Function Fields, *Canad. Math. Bull.* **35** (1992) 361-370.

[Fu] W. Fulton. *Algebraic curves: an introduction to Algebraic Geometry*, Benjamin 1969.

[Go] D. Goldfeld. The Gauss class number problem for imaginary quadratic fields, Preprint.

[Ha] R. Hartshorne. *Algebraic Geometry*, Springer-Verlag, 1977.

[Hw] Hong Wen Lu. Divisibility of the Class Number of some real quadratic fields, *Acta Math. Sinica* **28** (1985) 756-762.

[Hu] A. Hurwitz. *Über Relationen zwischen Klassenzahlen binärer quadratischer Formen von negativer Determinante*, Math. Ann. **25** (1885), 157-196.

[Ko1] N. Koblitz. Elliptic curve cryptosystems, *Mathematics of Computation*, **48** (1987), 203-209.

[Ko2] N. Koblitz. Hyperelliptic cryptosystems, *Journal of Cryptology*, **1** (1989), 139-150.

[Ko3] N. Koblitz. *Algebraic aspects of Cryptography*, Springer-Verlag, 1998.

[LV] G. Lachaud, S. Vlădut. Gauss Problem for Function Fields, *J. Number Theory* **85** (2000), 109-129.

[La1] S. Lang. *Algebra* (3rd edition), Addison-Wesley, Reading, MA, 1993.

[La2] S. Lang. *Algebraic Number Theory*, GTM 110, Springer-Verlag, New York, 1986.

[La] T. Lange. Efficient Arithmetic on Hyperelliptic Curves, PhD thesis, Essen 2001.

[LPP] H.W. Lenstra, J. Pila, C. Pomerance. "A hyperelliptic smoothness test. I", *Philosophical Transactions of the Royal Society of London A*, **345** (1993), 397-408.

[Lb1] D. Le Brigand. Quadratic algebraic function fields with ideal class number two, in "Arithmetic, Geometry and Coding Theory, Proceedings International Conference, Luminy, 1993." 105-126, De Gruyter, Berlin, 1996.

[Lb2] D. Le Brigand. Decoding of codes on hyperelliptic curves, Eurocode '90, Lecture Notes in Computer Science, **514** (1991), Springer-Verlag, 126-134.

[Mr] R.E. MacRae. On unique factorization in certain rings of algebraic functions, *J. Algebra* **17** (1971), 243-261.

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

[Me] A. Menezes. *Elliptic curve public key cryptosystems*, Kluwer Academic Publisher, 1993.

[Mi] J. Milne. Abelian varieties. In *Arithmetic Geometry*, Cornell, Silverman, eds., Springer-Verlag, 1986, 103-150.

[MOV] A. Menezes, T. Okamoto, S. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field, *IEEE Transactions on Information Theory*, **39** (1993), 1639-1646.

[MWZ] A. Menezes, Y. Wu, R. Zuccherato. "An elementary introduction to hyperelliptic curves", appendix in *Algebraic aspects of Cryptography* by N. Koblitz, Springer-Verlag, 1998, 155-178.

[Mo] R.A. Mollin. Necessary and sufficient conditions for the class number of a real quadratic field to be one, and a conjecture of S. Chowla, Proc. Amer. Math. Soc. 102 (1988), 17-21.

[MW] R.A. Mollin, H.C. Williams. A conjecture of S. Chowla via the generalized Riemann hypothesis, Ibid, 102(1988), 794-796.

[MWe] H. Montgomery, P. Weinberger. Notes on Small Class Numbers, *Acta. Arith.* **24** (1974), 529-542.

[Mu] M. Ram Murty. Exponents of class groups of quadratic fields, Topics in Number Theory (University Park, PA, 1997), 229-239, Math. Appl., 467, Kluwer Acad. Publ., Dordrecht, 1999.

[Oe] J. Oesterlé. Nombres de classes des corps quadratiques imaginaires, *Astérisque* **121-122** (1985), 309-323.

[PR] S. Paulus, H.-G. Rück. Real and Imaginary quadratic representations of Hyperelliptic function fields, *Math Comp.* **68** (1999), 1233-1241.

[Pe] O. Perron. *Die Lehre von den Kettenbrüchen*, Teubner, Leipzig, 1913.

[Ro] M. Rosen. *Number Theory in Function Fields*, GTM 210, Springer-Verlag, 2002.

[RT] H.-G. Rück, U. Tipp. Heegner points and L-series of automorphic cusp forms of Drinfeld type, *Doc. Math.* **5** (2000), 365-444.

[SSW] R. Scheidler, A. Stein, H.C. Williams. Key exchange in real quadratic congruence function fields, *Designs, Codes and Cryptography*, **7** (1996), 153-174.

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

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

[Se1] S. Sémirat. Class number one problem for imaginary function fields: the cyclic prime power case, *J. Number Theory* **84** (2000), no. 1, 166-183.

[Se2] S. Sémirat. Cyclotomic function fields with ideal class number one, *J. Algebra* **236** (2001), no. 1, 376–395.

[Sh] D. Shanks. The infrastructure of a real quadratic field and its applications, *In Proc. 1972 Number Theory Conference, Boulder, Colorado*, pages 217-224, 1972.

[Si] J.H. Silverman. *The Arithmetic of elliptic curves*, Springer, 1986.

[Sn] N. Snyder. An Alternate Proof of Mason's Theroem, *Elemente de Mathematik* **55** (2000) 93-94.

[Sk] H.M. Stark. On Complex Quadratic Fields with Class-Number two, *Math. Comput.* **29** (1975), 289-302.

[St1] A. Stein. Infrastructure in real quadratic function fields. Technical Report CORR 99-17, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, 1999. 19 pages.

[St2] A. Stein. Introduction to continued fraction expansions in real quadratic function fields. Technical Report CORR 99-16, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, 1999. 23 pages.

[St3] A. Stein. Sharp upper bounds for arithmetics in hyperelliptic function fields. Technical Report CORR 99-23, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, 1999. 68 pages.

[St] H. Stichtenoth. *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 1993.

[Ya] K. Yamamura. The determination of the imaginary abelian number fields with class number one, *Math. of. Comp.*, 62(206) 1994, 899-921.

[Yj] J. Yu. On arithmetic of hyperelliptic curves, to appear in Aspects of Mathematics 1998.

[YY] J. Yu, J.-K. Yu. A note of a geometric analogue of Ankeny-Artin-Chowla's conjecture, Contempory Math. A.M.S 210(1998), 101-105.

[Yu1] J.-K. Yu. A class number relation over function fields, *J. Number Theory* **54** (1995), 318-340.

[Yu2] J.-K. Yu. Toward a proof of the Cohen-Lenstra conjecture in the function field case, Preprint (1997).

[WY] J. T.-Y. Wang, J. Yu. On class number relations over function fields, *J. Number Theory* **69** (1998), 181-196.

[WZ1] K. Wang, X. Zhang. Ideal class groups and subgroups of real quadratic function fields, *Tsinghua Science and Technology*, 5 (2000.12), No.4: 372-373.

[WZ2] K. Wang, X. Zhang. Subgroups of class groups of algebraic quadratic function fields, *Chinese Annals of Mathematics*, Vol. 24, No. 3 (2003) 315-322

[Zh1] X. Zhang. Ambiguous classes and the 2-rank of class group of quadratic function field, *Jour. of China Univ. of Sci. & Tech.*,19 (1987), 425-431.

[Zh2] X. Zhang. Determination of algebraic function fields of type (2,2,...,2) with class number one, *Scientia Sinica* **A 31**, n. 8 (1998), 908-915.

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