2010

Primes of the form X² + nY² in function fields

Piotr Maciak

Louisiana State University and Agricultural and Mechanical College

PRIMES OF THE FORM $X^2 + nY^2$ IN FUNCTION FIELDS

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by
Piotr Maciak
M.S., Szczecin University, 2003
May 2010

Acknowledgments

This dissertation would not be possible without the help of many people. First, I would like to thank my adviser Dr. Jorge Morales for his patience, support and advice.

I would also like to thank Dr. Paweł Andrzejewski for his encouragement to pursue graduate studies in mathematics. If it was not for him, I would not be where I am today.

My family deserve special thanks for their support throughout the years. They never doubted I would make it.

This dissertation is gratefully dedicated to my mother.

Table of Contents

Notation

In this work we will use the following notation:

q - a power of an odd prime number

$\mathbb{F}$ - the finite field with q elements

$\mathcal{Z}$ - the polynomial ring $\mathbb{F}[x]$

$\mathcal{Q}$ - the field of fractions of $\mathcal{Z}$

$\mathcal{K}$ - an imaginary, quadratic extension of $\mathcal{Q}$ of the form $\mathcal{Q}(\sqrt{-n})$

$\mathcal{O}_{\mathcal{K}}$ - the integral closure of $\mathcal{Z}$ in $\mathcal{K}$

p_∞ - the prime at infinity in $\mathcal{Q}$, that is, a localization of $\mathcal{Z}$ at x^{-1}

$\mathfrak{p}_\infty$ - the unique prime in $\mathcal{K}$ lying above p_∞

$\mathrm{ord}_{p_\infty}(\cdot)$ - the valuation associated with p_∞

$\mathrm{ord}_{\mathfrak{p}_\infty}(\cdot)$ - the valuation associated with $\mathfrak{p}_\infty$

$|\cdot|_\infty$ - the multiplicative valuation of $\mathcal{Q}$ defined by $|a|_\infty = q^{-\mathrm{ord}_{p_\infty}(a)}$

$\mathcal{R}$ - the completion of $\mathcal{Q}$ with respect to $\mathrm{ord}_{p_\infty}(\cdot)$

$\mathcal{C}$ - the completion of an algebraic closure of $\mathcal{R}$ with respect to $|\cdot|_\infty$

$\mathcal{H}$ - the Hilbert class field of $\mathcal{K}$

Abstract

Let n be a square-free polynomial over $\mathbb{F}_q$, where q is an odd prime power. In this work, we determine which irreducible polynomials p in $\mathbb{F}_q[x]$ can be represented in the form $X^2 + nY^2$ with $X, Y \in \mathbb{F}_q[x]$. We restrict ourselves to the case where $X^2 + nY^2$ is anisotropic at infinity. As in the classical case over $\mathbb{Z}$ discussed in [2], the representability of p by the quadratic form $X^2 + nY^2$ is governed by conditions coming from class field theory. A necessary and almost sufficient condition is that the ideal generated by p splits completely in the Hilbert class field $\mathcal{H}$ of $\mathcal{K} = \mathbb{F}_q(x, \sqrt{-n})$ for the appropriate notion of Hilbert class field in this context. In order to get explicit conditions for p to be of the form $X^2 + nY^2$, we use the theory of sgn-normalized rank-one Drinfeld modules. We present an algorithm to construct a generating polynomial for $\mathcal{H}/\mathcal{K}$. This algorithm generalizes to all situations an algorithm of D.S. Dummit and D.Hayes for the case where $-n$ is monic of odd degree.

Introduction

This dissertation is inspired by the classical problem of Fermat about the sum of two squares and its generalizations discussed in [2]. The unfolding work considers an analogous problem in the function fields context.

Let $\mathcal{Z} = \mathbb{F}_q[x]$, where q is a power of an odd prime, and let $n \in \mathcal{Z}$ be a square-free polynomial of degree d with the leading coefficient n_d. We require that d is odd or $-n_d$ is not a square in $\mathbb{F}_q$, which means that the infinite place of $\mathcal{Q} = \mathbb{F}_q(x)$ has a unique extension $\mathfrak{p}_\infty$ in the quadratic field $\mathcal{K} = \mathcal{Q}(\sqrt{-n})$. Equivalently, the norm form $X^2 + nY^2$ is anisotropic over $\mathcal{R} = \mathbb{F}_q((x^{-1}))$, the completion of $\mathcal{Q}$ at infinity. In this exposition, we determine which irreducible polynomials p in $\mathcal{Z}$ can be represented by the form $X^2 + nY^2$.

Let $\mathcal{O}_\mathcal{K}$ denote the algebraic closure of $\mathcal{Z}$ in $\mathcal{K}$. Since the form X^2+nY^2, viewed as a function on $\mathcal{O}_\mathcal{K}$, is multiplicative, the ideal theory of this ring is a useful tool in the investigation of this problem. More specifically, if a prime $p \nmid n$ can be represented by $X^2 + nY^2$, then $p\mathcal{O}_\mathcal{K} = \mathfrak{p}\overline{\mathfrak{p}}, \mathfrak{p} \neq \overline{\mathfrak{p}}$, and $\mathfrak{p}$ is principal in $\mathcal{O}_\mathcal{K}$. Unfortunately, the converse is not quite true. If $\mathfrak{p} = (a + \sqrt{-n}b)\mathcal{O}_\mathcal{K}$ and $p\mathcal{O}_\mathcal{K} = \mathfrak{p}\overline{\mathfrak{p}}$, then $p\mathcal{O}_\mathcal{K} = (a^2 + nb^2)\mathcal{O}_\mathcal{K}$ from which it follows that $a^2 + nb^2 = up$ for some $u \in \mathcal{Z}^*$. Since the ring $\mathcal{Z}$ has $q - 1$ units, we are led to consider a notion of *weak representability.* We say that p can be *weakly represented* by the form $X^2 + nY^2$ if there is $u \in \mathbb{F}_q^*$ such that up can be represented by this form. Observe that if p can be represented by the form $X^2 + nY^2$ over $\mathcal{Z}$, then up also can be represented by this form for every square u in $\mathbb{F}_q$. In other words, if p is a monic prime that can be weakly represented, then the set of all elements $u \in \mathbb{F}_q^*$ such that up can be represented is either the whole group $\mathbb{F}_q^*$ or a coset of the subgroup $(\mathbb{F}_q^*)^2$ in $\mathbb{F}_q^*$.

The former holds if and only if n is a constant, which makes weak representability a non-trivial concept. Note that the described issue does not occur in the classical case since the ring of integers $\mathbb{Z}$ has only two units 1 and -1 and the form X^2+nY^2 can represent only positive elements of $\mathbb{Z}$ provided that $n > 0$. Using the notion of weak representability, we can now obtain the following equivalence. The prime $p \nmid n$ can be weakly represented by the form $X^2 + nY^2$ over $\mathcal{Z}$ if and only if $p\mathcal{O}_{\mathcal{K}} = \mathfrak{p}\overline{\mathfrak{p}}, \mathfrak{p} \neq \overline{\mathfrak{p}}$, and $\mathfrak{p}$ is principal in $\mathcal{O}_{\mathcal{K}}$. This rather simple fact is the first stepping stone towards solving the (weak) representation problem.

Thus, the question becomes: when does a prime p split in $\mathcal{O}_{\mathcal{K}}$ into a product of two principal ideals? Since the factorization of p in $\mathcal{O}_{\mathcal{K}}$ is governed by factorization of $X^2 + n$ over $\mathcal{Z}/p\mathcal{Z}$, the answer is immediate if $\mathcal{O}_{\mathcal{K}}$ is a principal ideal domain. In this case it happens precisely when $(\frac{-n}{p}) = 1$. However, $\mathcal{O}_{\mathcal{K}}$ typically is not a principal ideal domain. As a matter of fact, as a consequence of the Riemann Hypothesis, there are only two polynomials n of degree greater than 1 for which $\mathcal{O}_{\mathcal{K}} = \mathcal{Z}[\sqrt{-n}]$ is a principal ideal domain. Just like in the classical theory of number fields, this obstacle can be bypassed by the virtue of Hilbert class field theory. One needs to keep in mind that the usual definition of the Hilbert class field is not really suitable in this context. If K is a function field over a finite field $\mathbb{F}$, then the maximal abelian extension of K is not finite over K. However, if we define the Hilbert class field $\mathcal{H}$ of $\mathcal{K}$ as in [9], to be the maximal unramified abelian extension of $\mathcal{K}$ in which $\mathfrak{p}_\infty$ splits completely, then $\mathcal{H}$ is a finite Galois extension of $\mathcal{K}$ and $\mathrm{Cl}(\mathcal{O}_{\mathcal{K}}) \simeq \mathrm{Gal}(\mathcal{H}/\mathcal{K})$ via the Artin map. Consequently, if $\mathfrak{p}$ is a prime ideal in $\mathcal{K}$, then $\mathfrak{p}$ is principal if and only if it splits completely $\mathcal{H}$. Using the fact that $\mathcal{H}$ is also Galois over $\mathcal{Q}$, we conclude a prime $p \nmid n$ can weakly represented by the form $X^2 + nY^2$ if and only if p splits completely in $\mathcal{H}$. This fact seems to solve the (weak) representability problem. However, it is not a constructive solution. Given a concrete polynomial n, we are still lacking an effective criterion to verify which polynomials p can be written in the form $X^2 + nY^2$. Since splitting of a prime ideal in a field extension depends on the factorization of a minimal polynomial of a generator of the extension modulo the prime ideal, the next and final step is to find a polynomial which generates $\mathcal{H}$ over $\mathcal{K}$.

This final task is the least trivial part of the whole procedure. In the classical case, this is achieved via analytic methods. More specifically, if $K = \mathbb{Q}(\sqrt{-n})$, then the object of interest, the ring class field of the order $\mathbb{Z}[\sqrt{-n}]$ is generated by the j-invariant of this order. The definition of the j-invariant and computation of its minimal polynomial rely on the theory of elliptic and modular functions. In the function field context, this goal will be also achieved using analytic methods but the used technique is not a straightforward generalization of the classical case. The field of complex numbers $\mathbb{C}$, being a finitely dimensional extension of the real numbers, is complete. The situation is more complicated over function fields. The algebraic closure of $\mathcal{R}$ is incomplete and hence we define $\mathcal{C}$ to be the completion of $\overline{\mathcal{R}}$. The field $\mathcal{C}$ is known to be algebraically closed. A similar construction can be repeated for the field $\mathcal{K}$ and the prime $\mathfrak{p}_\infty$. The resulting field is both isomorphic and isometric to $\mathcal{C}$. Consequently, these two fields can be identified and regarded as the analog of the field of complex numbers. An $\mathcal{O}_\mathcal{K}$-lattice in $\mathcal{C}$ a discrete, finitely generated, $\mathcal{O}_\mathcal{K}$-submodule of $\mathcal{C}$. If $\Lambda \subset \mathcal{C}$ is a lattice, then the *rank* of Λ is the dimension of $\mathcal{K}_{\mathfrak{p}_\infty}\Lambda$ over $\mathcal{K}_{\mathfrak{p}_\infty}$. In particular, up to homothety the set of $\mathcal{O}_\mathcal{K}$-lattice of rank 1 in $\mathcal{C}$ consists precisely of fractional ideals of $\mathcal{O}_\mathcal{K}$. For every lattice $\mathcal{O}_\mathcal{K}$-lattice Γ of rank r, we define the exponential function associated to Γ by

$$e_\Gamma(x) = x \prod_{\gamma \in \Gamma \setminus \{ 0 \}} \left(1 - \frac{x}{\gamma} \right).$$

The function $e_\Gamma(x)$ is the unique entire function with simple zeros on the elements of Γ and with leading term x. It is also known to be $\mathbb{F}$-linear. Next, if $\Gamma \subset \Gamma'$ and Γ' is also a lattice of rank r, then Γ'/Γ is finite and

$$P(x;\Gamma'/\Gamma) = x \prod_{\mu \in \Gamma'/\Gamma} \left(1 - \frac{x}{e_\Gamma(\mu)}\right)$$

is $\mathbb{F}$-linear polynomial with the initial term x. If $\tau = x^q$ is the Frobenius endomorphism of $\mathcal{C}$ and $\mathcal{C}\langle\tau\rangle$ and is the subring of $\mathrm{End}_{\mathbb{F}}(\mathcal{C})$ generated by τ, then $P(x;\Gamma'/\Gamma)$ can be regarded as an element of $\mathcal{C}\langle\tau\rangle$. Consequently, $aP(x;a^{-1}\Gamma/\Gamma) \in \mathcal{C}\langle\tau\rangle$ for each $a \in \mathcal{O}_\mathcal{K} \setminus \{0\}$. If we set

$$\rho_a^\Gamma(x) = aP(x;a^{-1}\Gamma/\Gamma),$$

then $\rho^\Gamma : \mathcal{O}_\mathcal{K} \to \mathcal{C}\langle\tau\rangle$ is an $\mathbb{F}$-algebra homomorphism such that the constant term of ρ_a^Γ equals a and $\deg_\tau \rho_a = -r \operatorname{ord}_{\mathfrak{p}_\infty}(a)\, d_\infty$, where d_∞ is the degree of $\mathfrak{p}_\infty$. Any such a homomorphism is called a *Drinfeld $\mathcal{O}_\mathcal{K}$-module over $\mathcal{C}$* of rank r. Moreover, the map $\Gamma \to \rho^\Gamma$ is rank preserving bijection between the lattices and Drinfeld modules. Further, if Γ and Λ are homothetic, then ρ^Γ and ρ^Λ are isomorphic, meaning that there exists a constant $c \in \mathcal{C}^*$ such that $c\rho^\Gamma = \rho^\Lambda c$. In particular, if the correspondence $\Gamma \to \rho^\Gamma$ is restricted to the set of rank 1 lattices, we obtain a bijection between the class group $\mathrm{Cl}(\mathcal{O}_\mathcal{K})$ and the set of isomorphism classes of rank 1 Drinfeld $\mathcal{O}_\mathcal{K}$-modules.

Due to this correspondence, rank one $\mathcal{O}_\mathcal{K}$-Drinfeld modules can be considered to be analogues of elliptic curves with complex multiplication. In particular, they can be used to define the j-invariant of a fractional ideals of $\mathcal{O}_\mathcal{K}$. If ρ is a rank one $\mathcal{O}_\mathcal{K}$-Drinfeld module associated with the fractional ideal $\mathfrak{a}$, then $\rho_x = a_0 + a_1\tau + a_2\tau^2$ and we define $j(\mathfrak{a}) = a_2^{q+1}/a_1$. It turns out that the $j = j(\mathcal{O}_\mathcal{K})$ is a generator of $\mathcal{H}$ over $\mathcal{K}$. In [3], D. Hayes and D.S. Dummit present an algorithm to compute the minimal polynomial of j in the case when $-n$ is a square-free monic polynomial of odd degree. In this dissertation, we extend this algorithm to deal with the cases when $-n$ is not monic or of even degree (with the assumption that $-n_d$ is not a square in $\mathbb{F}$). If $f(X)$ denotes the minimal polynomial of j and $g(X)$ denotes the output of the modified algorithm, then $g(X)$ equals either $f(X)$ or $f(X)f(-X)$. This is however sufficient for our purpose. As we shall see the splitting of p in $\mathcal{H}$ depends on solvability of the congruence $f(X) \equiv 0 \pmod{p}$. Clearly, this congruence is solvable if and only if $g(X) \equiv 0 \pmod{p}$ is solvable. The algorithm presented by us is illustrated with some explicit computations performed using Magma Computational Algebra System [1].

The final question posed and answered in this dissertation is: *'Assuming that p can be weakly represented by the form $X^2 + nY^2$, when can p itself be represented by this form?'* In order to answer this question, we first define what it means for a polynomial p to be positive. If π is a uniformizer at $\mathfrak{p}_\infty$, that is, an element of the completion $\mathcal{K}_{\mathfrak{p}_\infty}$ such that $\mathrm{ord}_{\mathfrak{p}_\infty}\pi = 1$, then every element α of $\mathcal{K}_{\mathfrak{p}_\infty}$ can be expressed uniquely as a Laurent series

$$\sum_{k=k_0}^{\infty} c_k \pi^k,$$

where $c_k \in \mathbb{F}_{q^{d_\infty}}$ and $c_{k_0} \neq 0$. A sign function associated with the uniformizer π is given by $\mathrm{sgn}(\alpha) = c_{k_0}$. An element α is called *positive* if $\mathrm{sgn}(\alpha) = 1$. If g is the genus of $\mathcal{K}$ and $y^2 = -n$, then $\pi = \frac{x^g}{y}$ is a uniformizer at $\mathfrak{p}_\infty$. Using the sign function associated with this uniformizer, we can easily find that a prime polynomial p that can be weakly represented by the form $X^2 + nY^2$ is positive if and only if its leading coefficient is equal $(-n_d)^{\deg^* p}$, where $\deg^* p = \frac{\deg p}{d_\infty}$. If ρ is a sign normalized, rank one $\mathcal{O}_\mathcal{K}$-Drinfeld module and $\rho_x = a_0 + a_1\tau + a_2\tau^2$, then the field $\mathcal{H}^+ = \mathcal{K}(a_1, a_2)$ is a Kummer extension of $\mathcal{H}$ of degree $\frac{q^{d_\infty}-1}{q-1}$. For a positive prime p that can be weakly represented by the form $X^2 + nY^2$, we shall prove the following two results results.

Theorem. *Suppose that* $\deg^* p$ *is even or* $4 \mid q - 1$*. Then* p *can be represented by the form* $X^2 + nY^2$ *if and only if it splits completely in* $\mathcal{H}^+$*.*

Theorem. *Let* $\mathfrak{P}^+$ *be a prime in* $\mathcal{H}^+$ *above* p*. Suppose that* $\deg^* p$ *is odd and* $4 \nmid q - 1$*. Then* p *can be represented by the form* $X^2 + nY^2$ *if and only if* $f(\mathfrak{P}^+ \mid p) = 4$*.*

Chapter 1
Function Fields

In this chapter we will review elementary facts about function fields. Majority of the results presented here are well-known and discussed with details in [8]. Consequently, we shall omit most proofs.

1.1 Basic Properties of $\mathcal{Z}$

The basic object of number theory in function fields is the ring of polynomials $\mathbb{F}[x]$ over a finite field with q elements. In this work we will always assume that q is a power of an *odd* prime number. The polynomial ring $\mathbb{F}[x]$ is known to share many arithmetic properties with the ring of integers $\mathbb{Z}$. The following section shows several instances of this fact. In order to emphasize similarities between these rings, we shall use the symbol $\mathcal{Z}$ to denote the ring $\mathbb{F}[x]$.

Proposition 1.1.1. *$\mathcal{Z}$ is a principal ideal domain. The group of units of $\mathcal{Z}$ consists only of nonzero elements of the field $\mathbb{F}$.*

Definition 1.1.2. Let $m \in \mathcal{Z}$. We define the *norm* of m, denoted by $|m|$, to be $q^{\deg m}$ if $m \neq 0$. The norm of the zero polynomial is zero.

Proposition 1.1.3. *Let $m \in \mathcal{Z}$. If $m \neq 0$, then $\mathcal{Z}/m\mathcal{Z}$ is a finite ring with $|m|$ elements. Additionally, $\mathcal{Z}/m\mathcal{Z}$ is a field if and only if m is irreducible. In such a case $(\mathcal{Z}/m\mathcal{Z})^*$ is a cyclic group with $|m| - 1$ elements.*

Corollary 1.1.4. (Fermat's Little Theorem) *Let $p \in \mathcal{Z}$ be irreducible. If $a \in \mathcal{Z}$ is not divisible by p, then*

$$a^{|p|-1} \equiv 1 \pmod{p}.$$

Corollary 1.1.5. *Let $p \in \mathcal{Z}$ be irreducible. If $a \in \mathcal{Z}$ is not divisible by p, then*

$$a^{\frac{|p|-1}{2}} \equiv 1 \pmod{p} \quad \text{or} \quad a^{\frac{|p|-1}{2}} \equiv -1 \pmod{p}.$$

Proposition 1.1.6. *Let $p \in \mathcal{Z}$ be irreducible and $a \in \mathcal{Z}$ be not divisible by p. The congruence $X^2 \equiv a \pmod{p}$ is solvable if and only if*

$$a^{\frac{|p|-1}{2}} \equiv 1 \pmod{p}.$$

Definition 1.1.7. Let $p \in \mathcal{Z}$ be irreducible and $a \in \mathcal{Z}$ be not divisible by p. We define the *Legendre symbol* $(\frac{a}{p})$ to be the unique unit of $\mathcal{Z}$ such that

$$a^{\frac{|p|-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

If a is divisible by p, we set $(\frac{a}{p}) = 0$.

Proposition 1.1.8. *The Legendre symbol has the following properties:*

- *If $a \equiv b \pmod{p}$, then $(\frac{a}{p}) = (\frac{b}{p})$.*
- $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$.
- $(\frac{a}{p}) = 1$ *if and only if the congruence $X^2 \equiv a \pmod{p}$ is solvable.*

In other words, the Legendre symbol can be regarded as a group epimorphism from $(\mathcal{Z}/p\mathcal{Z})^*$ to $\{1, -1\}$ whose kernel consists of squares of $(\mathcal{Z}/p\mathcal{Z})^*$.

Theorem 1.1.9. (The Quadratic Reciprocity Law) *Let p, $r \in \mathcal{Z}$ be monic and irreducible polynomials of degrees k and l respectively. Then*

$$\left(\frac{r}{p}\right) = (-1)^{\frac{q-1}{2}kl} \left(\frac{p}{r}\right).$$

Theorem (1.1.9) can be easily generalized. If p and r are not necessarily monic, we have:

Corollary 1.1.10. *Let p, $r \in \mathcal{Z}$ be irreducible polynomials of degrees k and l respectively. Let p_k and r_l be the leading coefficients of p and q respectively. Then*

$$\left(\frac{r}{p}\right) = (-1)^{\frac{q-1}{2}kl} {r_l}^{\frac{q-1}{2}k} {p_k}^{-\frac{q-1}{2}l} \left(\frac{p}{r}\right).$$

1.2 Arithmetic of Function Fields

The field of rational functions $\mathbb{F}(x)$ is naturally the field of fractions of the ring $\mathcal{Z}$. For that reason, it will be denoted by $\mathcal{Q}$. Analogously to number fields, one can define a *function field* to be a finite extension of $\mathcal{Q}$. More generally, we have the following definition.

Definition 1.2.1. A *function field* over $\mathbb{F}$ is a field extension $K/\mathbb{F}$ containing an element x such that x is transcendental over $\mathbb{F}$ and the extension $K/\mathbb{F}(x)$ is finite. If $\mathbb{F}$ is algebraically closed in K, we say that $\mathbb{F}$ is the *constant field* of K.

Proposition 1.2.2. *Let K be a function field over $\mathbb{F}$ and $\mathbb{E}$ be the algebraic closure of $\mathbb{F}$ in K. Then $\mathbb{E}$ is a finite extension of $\mathbb{F}$, K is a function field over $\mathbb{E}$ and $\mathbb{E}$ is the constant field of K.*

From now on we will assume that if K is a function field over $\mathbb{F}$, then $\mathbb{F}$ is the constant field of K.

Definition 1.2.3. Let K be a function field over $\mathbb{F}$. A *prime* in K is a discrete valuation ring $\mathfrak{o}$ containing $\mathbb{F}$ such that K is the quotient field of $\mathfrak{o}$.

Lemma 1.2.4. *Let $\mathfrak{p}$ be the maximal ideal of $\mathfrak{o}$. The dimension of $\mathfrak{o}/\mathfrak{p}$ over $\mathbb{F}$ is finite.*

By abuse of language, the maximal ideal $\mathfrak{p}$ is often referred to as a prime in K. The quotient field $\mathfrak{o}/\mathfrak{p}$ will be denoted by $\kappa(\mathfrak{p})$. Its dimension over $\mathbb{F}$ is called the *degree* of $\mathfrak{p}$ and is denoted by $\deg \mathfrak{p}$. Similarly, the valuation associated with $\mathfrak{p}$ is denoted by $\mathrm{ord}_{\mathfrak{p}}$. Each valuation $\mathrm{ord}_{\mathfrak{p}}$ induces the *normalized multiplicative* *valuation* $|\cdot|_{\mathfrak{p}}$, which is given by

$$|\alpha|_{\mathfrak{p}} = q^{-\operatorname{ord}_{\mathfrak{p}}(\alpha)\deg\mathfrak{p}}.$$

Example 1.2.5. Let $p \in \mathcal{Z}$ be monic and irreducible or $p = \frac{1}{x}$. Then the localization $\mathcal{Z}_p$ of $\mathcal{Z}$ at p is a prime in $\mathcal{Q}$ and every prime in $\mathcal{Q}$ is of this form. If $p \in \mathcal{Z}$, the degree of $\mathcal{Z}_p$ equals the degree of the polynomial p. The degree of $\mathcal{Z}_{\frac{1}{x}}$ equals 1.

The prime $\mathcal{Z}_{\frac{1}{x}}$ is called the *prime at infinity* and is denoted by p_∞. The valuation associated with p_∞ is given by

$$\operatorname{ord}_{p_\infty}\left(\frac{f}{g}\right) = \deg g - \deg f$$

for all $f \in \mathcal{Z}$, $g \in \mathcal{Z}^*$.

Definition 1.2.6. Let K be a function field over $\mathbb{F}$. The free abelian group generated by the primes of K is called the *group of divisors of* K and is denoted by $\mathcal{D}_K$. The elements of $\mathcal{D}_K$ are called the *divisors of* K.

Thus, a divisor D of K is simply a formal $\mathbb{Z}$-linear combination of primes

$$D = \sum_{\mathfrak{p}} a(\mathfrak{p})\mathfrak{p}.$$

The *degree of* D is defined to be

$$\deg(D) = \sum_{\mathfrak{p}} a(\mathfrak{p})\deg(\mathfrak{p}).$$

Hence the degree function defined initially for primes becomes a group homomorphism from $\mathcal{D}_K$ to $\mathbb{Z}$. The kernel of this map consisting of all divisors of degree 0 is denoted by $\mathcal{D}_K^0$.

Lemma 1.2.7. *If $a \in K^*$, then $\operatorname{ord}_{\mathfrak{p}}(a) \neq 0$ for only finitely many primes $\mathfrak{p}$ of K.*

Definition 1.2.8. Let $a \in K^*$. We define the *divisor of* a to be

$$(a) = \sum_{\mathfrak{p}} \operatorname{ord}_{\mathfrak{p}}(a)\mathfrak{p}.$$

For a fixed prime $\mathfrak{p}$ set $n = \operatorname{ord}_{\mathfrak{p}}(a)$. If $n > 0$, we say that $\mathfrak{p}$ is a *zero* of a of order n. If $n < 0$, we say that $\mathfrak{p}$ is a *pole* of a of order $-n$.

It is easy to see that the map $\mathcal{P} : K^* \to \mathcal{D}_K$ defined by $\mathcal{P}(a) = (a)$ is a group homomorphism. Its image is called the *group of principal divisors* and is denoted by $\mathcal{P}_K$. The quotient $\mathcal{D}_K/\mathcal{P}_K$ is called the *group of divisor classes* and is denoted by $\mathrm{Cl}(K)$. Thus, two divisors D_1, D_2 are in the same class if they differ by a principal divisor:

$$D_1 - D_2 = (a)$$

for some $a \in K^*$. In such a case, we also say that D_1, D_2 are *linearly equivalent.*

Proposition 1.2.9. *Let $a \in K^*$. The divisor of a equals 0 if and only if $a \in \mathbb{F}^*$. Moreover, $\deg(a) = 0$. In other words, $\ker \mathcal{P} = \mathbb{F}^*$ and $\deg \mathcal{P}_K = \{ 0 \}$.*

Corollary 1.2.10. *The degree function $\deg : \mathcal{D}_K \to \mathbb{Z}$ induces a well-defined homomorphism from $\mathrm{Cl}(K)$ to $\mathbb{Z}$.*

Definition 1.2.11. The kernel of the induced homomorphism $\deg : \mathrm{Cl}(K) \to \mathbb{Z}$ is called the *group of divisors of degree zero* and is denoted by $\mathrm{Cl}^0(K)$. The cardinality of this group is called the *class number of* K and is denoted by h_K.

In order to state the Riemann-Roch theorem, we need the following definition

Definition 1.2.12. Let $D = \sum_{\mathfrak{p}} a(\mathfrak{p})\, \mathfrak{p}$ be a divisor of K and $L(D) = \{ x \in K^* \,|\, \operatorname{ord}_{\mathfrak{p}}(x) + a(\mathfrak{p}) \geq 0 \} \cup \{ 0 \}$. The *dimension of* D, denoted by $l(D)$, is the dimension of $L(D)$ over $\mathbb{F}$.

Theorem 1.2.13. (Riemann-Roch Theorem) *There is a unique nonnegative integer g and a unique divisor class $\mathfrak{C}$ such that for all divisors A and all $C \in \mathfrak{C}$*

we have

$$l(A) = \deg(A) - g + 1 + l(C - A).$$

The integer g is called the *genus* of the function field K. The class $\mathfrak{C}$ is called the *canonical class.*

Corollary 1.2.14. *If* $\deg(A) > 2g - 2$*, then* $l(A) = \deg(A) - g + 1$*.*

Example 1.2.15. The genus of $\mathcal{Q}$ is 0.

1.3 The Zeta Function of a Function Field

The zeta function $\zeta(s)$ in the context of function fields is even a more powerful tool than in the classical situation. Firstly, it can be effectively written as a rational function of q^{-s}. Additionally, an analog of the Riemann hypothesis holds true.

Definition 1.3.1. Let $D = \sum_{\mathfrak{p}} a(\mathfrak{p})\,\mathfrak{p}$ be a divisor of K. The divisor D is said to be *effective* if $a(\mathfrak{p}) \geq 0$ for all primes $\mathfrak{p}$. In such a case, we write $D \geq 0$.

Lemma 1.3.2. *Let* $n \geq 0$ *be an integer. There are only finitely many effective divisors of degree* n*.*

The number of effective divisors of degree n will be denoted by e_n.

Definition 1.3.3. Let $D \in \mathcal{D}_K$. The *norm* of the divisor D is defined to be the number

$$N(D) = q^{\deg(D)}.$$

Note that $N(D_1 + D_2) = N(D_1)N(D_2)$ for any two divisors and that $N(D)$ is a positive integer if D is an effective divisor.

Definition 1.3.4. The *zeta function* of K, denoted by $\zeta_K(s)$, is defined to be the infinite series

$$\zeta_K(s) = \sum_{D \geq 0} N(D)^{-s}.$$

If $\deg(D) = n$, then $N(D)^{-s} = q^{-ns}$. Since there are e_n effective divisors with $\deg(D) = n$, the series defining the zeta function can be rewritten as

$$\zeta_K(s) = \sum_{n=0}^{\infty} \frac{e_n}{q^{ns}}.$$

If we further set $u = q^{-s}$, we see that the zeta function is simply a power series in u. We will denote this power series by $Z_K(u)$. Thus,

$$\zeta_K(s) = Z_K(u) = \sum_{n=0}^{\infty} e_n u^n.$$

Theorem 1.3.5. *The radius of convergence of $Z_K(u)$ is q^{-1}. Equivalently, $\zeta_K(s)$ converges absolutely for all s with $\Re(s) > 1$. Moreover, there is a polynomial $L_K(u) \in \mathbb{Z}[u]$ of degree $2g$, where g is the genus of K, such that for all $|u| < 1$*

$$Z_K(u) = \frac{L_K(u)}{(1-u)(1-qu)}.$$

Additionally, $L_K(0) = 1$ and $L_K(1) = h_K$. The rational function on the right-hand side defines an analytic continuation of $\zeta_K(s)$ to all $s \in \mathbb{C}$. $\zeta_K(s)$ has simple poles at $s = 0$ and $s = 1$.

Theorem 1.3.6. (The Riemann Hypothesis for Function Fields) *All roots of $\zeta_K(s)$ lie on the line $\Re(s) = \frac{1}{2}$.*

Corollary 1.3.7. *Let g be the genus of K. Then $(\sqrt{q}-1)^{2g} \leq h_K \leq (\sqrt{q}+1)^{2g}$.*

1.4 Extensions of Function Fields

Let K be a function field over $\mathbb{F}$ and L be a finite field extension of K. Let $\mathbb{E}$ be an algebraic closure of $\mathbb{F}$ in L. It is easy to see that L is a function field over $\mathbb{E}$. Indeed, if $x \in K$ is transcendental over $\mathbb{F}$ and $K/\mathbb{F}(x)$ is a finite extension, then x is transcendental over $\mathbb{E}$ since $\mathbb{E}$ is algebraic over $\mathbb{F}$ and $[L : \mathbb{E}(x)] \leq [L : \mathbb{F}(x)] = [L : K] \cdot [K : \mathbb{F}(x)] < \infty$. Finally, $\mathbb{E}$ is algebraically closed in L being the algebraic closure of $\mathbb{F}$. The most interesting case from our point of view is when $\mathbb{F}$ is algebraically closed in L, that is, when $\mathbb{E} = \mathbb{F}$. Then L is a function field over $\mathbb{F}$. In such a case, we say that L is a *geometric extension* of K.

Definition 1.4.1. Let K be a function field over $\mathbb{F}$ and L/K be a finite extension. Let $\mathfrak{O}$ be a prime of L with the maximal ideal $\mathfrak{P}$ and $\mathfrak{o}$ be a prime of K with the maximal ideal $\mathfrak{p}$. We say that $\mathfrak{O}$ *lies above* $\mathfrak{o}$ if $\mathfrak{o} = K \cap \mathfrak{O}$ and $\mathfrak{p} = K \cap \mathfrak{P}$. In such a case, we will write $\mathfrak{O}|\mathfrak{o}$. As before, by abuse of language, we will also say that $\mathfrak{P}$ lies above $\mathfrak{p}$ and we will write $\mathfrak{P}|\mathfrak{p}$.

If $\mathfrak{P}$ lies above $\mathfrak{p}$, then $\mathfrak{O}/\mathfrak{P}$ is a vector space over $\mathfrak{o}/\mathfrak{p}$. The dimension of this space is called the *relative degree* and is denoted by $f = f(\mathfrak{P}/\mathfrak{p})$. Further, $\mathfrak{p}\mathfrak{O}$ is an ideal in $\mathfrak{O}$ and hence $\mathfrak{p}\mathfrak{O} = \mathfrak{P}^e$ for some $e \geq 1$. The number $e = e(\mathfrak{P}/\mathfrak{p})$ is called the *ramification index*. The ramification index has the following property: for all $a \in K$. $\operatorname{ord}_{\mathfrak{P}}(a) = e(\mathfrak{P}|\mathfrak{p}) \operatorname{ord}_{\mathfrak{p}}(a)$, which follows easily from the definition. Another immediate consequence of the definitions is the identity $\deg \mathfrak{P} = f(\mathfrak{P}|\mathfrak{p}) \deg \mathfrak{p}$.

Let K be a function field over $\mathbb{F}$ and L/K be a finite, separable extension. Let $\mathfrak{o}$ be a prime of K and $\mathfrak{p}$ be its maximal ideal. All primes of L lying above $\mathfrak{p}$ can be constructed as follows. Let $\mathcal{O}$ be an integral closure of $\mathfrak{o}$ in L. Since $\mathfrak{o}$ is a principal ideal domain, it follows that $\mathcal{O}$ is a Dedekind domain. Hence $\mathfrak{p}\mathcal{O}$ admits the prime factorization

$$\mathfrak{p}\mathcal{O} = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2} \dots \mathcal{P}_k^{e_n}.$$

Now, for each $1 \leq i \leq k$ define $\mathfrak{O}_i$ to be the localization of $\mathcal{O}$ at $\mathcal{P}_i$. Then $\mathfrak{O}_i$ is a prime of L. Its maximal ideal $\mathfrak{P}_i = \mathcal{P}_i\mathfrak{O}_i$ lies above $\mathfrak{p}$ and every prime above $\mathfrak{p}$ is of this form. Moreover, using basic facts about localization, we see that the notions of the ramification index and the relative degree defined above and the ones that are typically defined for extensions of Dedekind domains coincide. Thanks to that, we have the following well-known identity

$$\sum_{i=1}^{k} e_i f_i = [L : K].$$

1.5 Quadratic Extensions of $\mathcal{Q}$.

Let $n \in \mathcal{Z}$ be a square-free polynomial of degree d with the leading coefficient n_d. In this section we will study the quadratic extensions of $\mathcal{Q}$ of the form $\mathcal{K} = \mathcal{Q}(\sqrt{-n})$. Imaginary extensions (defined below) will be of special interest for us.

Lemma 1.5.1. *If $n \in \mathcal{Z}$ is a polynomial of positive degree, then $\mathcal{K}/\mathcal{Q}$ is a geometric extension, that is, $\mathbb{F}$ is the exact field of constants of $\mathcal{K}$.*

Proof. Suppose that $\alpha \in \mathcal{K}$ is algebraic over $\mathbb{F}$. We can write $\alpha = a + b\sqrt{-n}$ for some a, $b \in \mathcal{Q}$. Then $a = \frac{\alpha+\bar{\alpha}}{2}$, $-b^2 n = (\frac{\alpha-\bar{\alpha}}{2})^2$ are also algebraic over $\mathbb{F}$. Since $\mathbb{F}$ is algebraically closed in $\mathcal{Q}$, it follows that $a \in \mathbb{F}$ and $-b^2 n \in \mathbb{F}$. Since n is square-free polynomial of positive degree, it follows that $b = 0$. Thus, $\alpha = a \in \mathbb{F}$. □

Proposition 1.5.2. *$\mathcal{Z}[\sqrt{-n}]$ is the integral closure of $\mathcal{Z}$ in $\mathcal{K}$.*

Proof. Let $\mathcal{O}_{\mathcal{K}}$ be the integral closure of $\mathcal{Z}$ in $\mathcal{K}$. Since $\sqrt{-n} \in \mathcal{O}_{\mathcal{K}}$ and $\mathcal{Z} \subset \mathcal{O}_{\mathcal{K}}$, it follows that $\mathcal{Z}[\sqrt{-n}] \subset \mathcal{O}_{\mathcal{K}}$. On the other hand, if $a + b\sqrt{-n} \in \mathcal{O}_K$, then $m(X) = X^2 - 2aX + (a^2 + nb^2) \in \mathcal{Z}[X]$, which follows that $a \in \mathcal{Z}$ and $nb^2 \in \mathcal{Z}$. If $b = \frac{u}{v}$, where u, $v \in \mathcal{Z}$ are relatively prime, then $v^2 | n$. Since n is either invertible or square-free, it follows that $v \in \mathbb{F}$ and $b \in \mathcal{Z}$. □

The field of real numbers $\mathbb{R}$ is a completion of $\mathbb{Q}$ with respect to the standard absolute value. Then we can say that an imaginary extension of $\mathbb{Q}$ is simply $\mathbb{Q}(\alpha)$, where $\alpha \notin \mathbb{R}$. If n is square-free and $\alpha = \sqrt{-n}$, then an imaginary extension can be equivalently characterized by saying that n is positive or that the norm form $X^2 + nY^2$ is anisotropic over $\mathbb{R}$. It turns out that each of these conditions has a quite natural analogue in a rational function field $\mathcal{Q}$. The analogue of the field of real numbers is a completion of $\mathcal{Q}$ with respect to $|\cdot|_{p_\infty}$, the multiplicative valuation of $\mathcal{Q}$ defined by $|a|_{p_\infty} = q^{-\mathrm{ord}_{p_\infty}(a)}$. Such a completion will be further denoted by $\mathcal{R}$. Theorem (1.5.4) presents a series of equivalent conditions which we can be used to define an imaginary extension of $\mathcal{Q}$.

Lemma 1.5.3. *Let $a \in \mathcal{Z}$ be a polynomial of degree $m \geq 0$ with the leading coefficient a_m. Then $\sqrt{a} \in \mathcal{R}$ if and only if m is even and a_m is a square in $\mathbb{F}$.*

Proof. Assume that $\sqrt{a} \in \mathcal{R}$. Then $a = \lim_{k\to\infty} x_k^2$ for some sequence $(x_k) \in \mathcal{Q}^{\mathbb{N}}$. Consequently, $\lim_{k\to\infty} |x_k|_\infty^2 = |a|_\infty$, which implies that $m = \lim_{k\to\infty} \deg(x_k^2) = 2\lim_{k\to\infty} \deg x_k$. Since $(\deg x_k)_{k\in\mathbb{N}}$ is a sequence of integers, there is a number k_0 such that $m = \deg x_k^2 = 2\deg x_k$ for all $k \geq k_0$. Thus, m is even. Moreover, if $k \geq k_0$, then $x_k^2 = q_k^2 + r_k$, where q_k^2 is a polynomial of degree m and r_k is a proper rational function. Since

$$\lim_{k\to\infty} \log_q |x_k^2 - a|_\infty = \lim_{k\to\infty} \deg(x_k^2 - a) = -\infty,$$

it follows that for some $l \geq k_0$ the leading coefficient of a equals the leading coefficient of q_l^2 which clearly is a square in $\mathbb{F}$. Now assume that m is even and $a_m = b^2$ for some $b \in \mathbb{F}$. Clearly, $\sqrt{a} \in \mathcal{R}$ if and only if $f(X) = X^2 - a$ has a root in $\mathcal{R}$. By Hensel's Lemma, this is the case if

$$|f(\alpha)|_\infty < |f'(\alpha)|_\infty^2$$

for some $\alpha \in \mathcal{Z} \cap \mathcal{R}$. Set $\alpha = bx^{\frac{m}{2}}$. Then $|f(\alpha)|_\infty = q^{m-1}$ and $|f'(\alpha)|_\infty^2 = q^m$. Thus, $\sqrt{a} \in \mathcal{R}$. □

Theorem 1.5.4. *The following conditions are equivalent:*

(i) d is odd or $-n_d$ is not a square in $\mathbb{F}$.

(ii) $\sqrt{-n} \notin \mathcal{R}$.

(iii) *The norm form* $X^2 + nY^2$ *is anisotropic over* $\mathcal{R}$.

(iv) *There is a unique prime* $\mathfrak{p}_\infty$ *of* $\mathcal{K}$ *that lies over* p_∞.

Proof. Clearly, *(ii)* $\Leftrightarrow$ *(iii)*. The equivalence *(i)* $\Leftrightarrow$ *(iv)* is a part of Proposition 14.6 in [8]. *(i)* $\Leftrightarrow$ *(ii)* follows directly from (1.5.3). □

Definition 1.5.5. We say that the extension $\mathcal{K}/\mathcal{Q}$ is *imaginary* if the degree of n is positive and one of the equivalent conditions of Theorem (1.5.4) is satisfied. The degree of the unique prime $\mathfrak{p}_\infty$ above p_∞ will be denoted by d_∞.

Note that $d_\infty = f(\mathfrak{p}_\infty | \, p_\infty) \deg p_\infty = f(\mathfrak{p}_\infty | \, p_\infty)$. Hence in order to determine the degree of $\mathfrak{p}_\infty$, we need to find out when p_∞ is ramified in $\mathcal{K}$. The answer turns out to be quite simple. We have the following result.

Proposition 1.5.6. *Let* $n \in \mathcal{Z}$ *be a square-free polynomial of positive degree* d *such that* $\mathcal{K} = \mathcal{Q}(\sqrt{-n})$ *is an imaginary quadratic extension of* $\mathcal{Q}$. *If* d *is odd, then* p_∞ *is ramified in* $\mathcal{K}$. *If* d *is even, then* p_∞ *is inert.*

Proof. See Proposition (14.6) in [8]. □

Corollary 1.5.7. *If* d *is odd, then* $d_\infty = 1$. *If* d *is even, then* $d_\infty = 2$. *In any case,* $d_\infty \cdot e(\mathfrak{p}_\infty | \, p_\infty) = 2$.

Proof. By Theorem (1.5.4), $\mathfrak{p}_\infty$ is the only prime above p_∞ and hence we have $e(\mathfrak{p}_\infty | \, p_\infty) \cdot f(\mathfrak{p}_\infty | \, p_\infty) = [\mathcal{K} : \mathcal{Q}] = 2$. The result follows. □

Lemma 1.5.8. *If* $a, b \in \mathcal{Z}$ *and* $\sqrt{-n} \notin \mathcal{R}$, *then* $\deg(a^2 + nb^2) = \max\{\, 2\deg a, 2\deg b + \deg n \,\}$.

Proof. Let $a = a_k x^k + \cdots + a_1 x + a_0$, $b = b_l x^l + \cdots + b_1 x + b_0$, and $n = n_d x^d + \cdots + n_1 x + n_0$. If $\deg(a^2) \neq \deg(nb^2)$, the result follows. Otherwise, $2k = d + 2l$ and $a^2 + nb^2 = (a_k^2 + n_d b_l^2)x^{2k} + \cdots + (a_0^2 + n_0 b_0^2)$. The coefficient $a_k^2 + n_d b_l^2$ is not zero because $-n_d$ is not a square in $\mathbb{F}$. □

Proposition 1.5.9. *If* $\deg n \geq 1$*, then* $\mathcal{O}_{\mathcal{K}}^* = \mathbb{F}^*$*. Otherwise,* $\mathcal{O}_{\mathcal{K}}^* = \mathbb{F}(\sqrt{-n})^*$*.*

Proof. Suppose that $\deg n \geq 1$. Clearly, $\mathbb{F}^* \subset \mathcal{O}_{\mathcal{K}}^*$. If $a + b\sqrt{-n} \in \mathcal{O}_{\mathcal{K}}^*$, then $N(a + b\sqrt{-n}) = a^2 + nb^2 \in \mathbb{F}^*$. It follows from Lemma (1.5.8) that $a \in \mathbb{F}$ and $b = 0$. The second equality can be proven in a very similar way. □

Proposition 1.5.10. *Let* $\mathcal{K} = \mathcal{Q}(\sqrt{-n})$ *be an imaginary quadratic extension of* $\mathcal{Q}$ *and let* g *be the genus of* $\mathcal{K}$*.Then*

$$g = \left\lfloor \frac{d-1}{2} \right\rfloor = \frac{d - d_\infty}{2}$$

Proof. Let g be the genus of $\mathcal{K}$. Let $k > 2g - 2$. Then, by the Riemann-Roch theorem

$$l(k\mathfrak{p}_\infty) = \deg(k\mathfrak{p}_\infty) - g + 1 = kf(\mathfrak{p}_\infty | p_\infty) - g + 1. \tag{1.5.1}$$

Observe that $L(k\mathfrak{p}_\infty) \subset \mathcal{O}_{\mathcal{K}}$ and $a + b\sqrt{-n} \in L(k\mathfrak{p}_\infty)$ if and only if

$$\deg(a^2 + nb^2) \leq \frac{2k}{e(\mathfrak{p}_\infty | p_\infty)} = k \cdot f(\mathfrak{p}_\infty | p_\infty). \tag{1.5.2}$$

In order to prove the inequality (1.5.2), note that for all $\alpha \in \mathcal{K}$

$$\operatorname{ord}_{\mathfrak{p}_\infty}(\alpha) = \operatorname{ord}_{\mathfrak{p}_\infty}(\overline{\alpha})$$

since $\mathfrak{p}_\infty$ is the unique prime above p_∞ and hence it is fixed under conjugation. Consequently,

$$\begin{aligned}\mathrm{ord}_{\mathfrak{p}_\infty}(a+\sqrt{-n}b) &= \frac{1}{2}\mathrm{ord}_{\mathfrak{p}_\infty}(a^2+nb^2)\\ &= \frac{1}{2}e(\mathfrak{p}_\infty|\, p_\infty)\mathrm{ord}_{p_\infty}(a^2+nb^2)\\ &= -\frac{1}{2}e(\mathfrak{p}_\infty|\, p_\infty)\deg(a^2+nb^2).\end{aligned}$$

Thus, $\mathrm{ord}_{\mathfrak{p}_\infty}(a+b\sqrt{-n}) \geq -k$ if and only if the inequality (1.5.2) holds. By Lemma (1.5.8), the inequality (1.5.2) is equivalent to the following inequalities

$$\deg a \leq \frac{f(\mathfrak{p}_\infty|\, p_\infty)k}{2}$$

and

$$\deg b \leq \frac{f(\mathfrak{p}_\infty|\, p_\infty)k-d}{2}.$$

Thus, if $k \geq d$, then

$$l(k\mathfrak{p}_\infty) = \left\lfloor \frac{f(\mathfrak{p}_\infty|\, p_\infty)k}{2} \right\rfloor + \left\lfloor \frac{f(\mathfrak{p}_\infty|\, p_\infty)k-d}{2} \right\rfloor + 2.$$

If k is even, we have

$$l(k\mathfrak{p}_\infty) = f(\mathfrak{p}_\infty|\, p_\infty)k + 2 + \left\lfloor \frac{-d}{2} \right\rfloor. \tag{1.5.3}$$

Combining equalities (1.5.1) and (1.5.3), we get $g = 1 - \left\lfloor \frac{-d}{2} \right\rfloor = \left\lfloor \frac{d-1}{2} \right\rfloor$. If d is odd, then $\left\lfloor \frac{d-1}{2} \right\rfloor = \frac{d-1}{2}$. Otherwise, $\left\lfloor \frac{d-1}{2} \right\rfloor = \frac{d-2}{2}$. The result follows immediately from Corollary (1.5.7). □

Proposition 1.5.11. *$\mathcal{O}_\mathcal{K}$ is a principal ideal domain if and only if $d \leq 1$ or $n = x^3+2x+2 \in \mathbb{F}_3[x]$ or $n = 2x^3+x+2 \in \mathbb{F}_3[x]$.*

Proof. Suppose first that $d = 0$. Then by Proposition (1.5.2),

$$\mathcal{O}_\mathcal{K} = \mathcal{Z}[\sqrt{-n}] = \mathbb{F}[x][\sqrt{-n}] = \mathbb{F}[\sqrt{-n}][x] = \mathbb{F}(\sqrt{-n})[x].$$

Thus, $\mathcal{O}_{\mathcal{K}}$ is a polynomial ring over the field $\mathbb{F}(\sqrt{-n})$. The result follows.

Now, suppose that d is positive. Let $h_{\mathcal{O}_{\mathcal{K}}}$ be the class number of $\mathcal{O}_{\mathcal{K}}$ and $h_{\mathcal{K}}$ be the class number of $\mathcal{K}$. By Proposition 14.7 in [8], $h_{\mathcal{O}_{\mathcal{K}}} = h_{\mathcal{K}}$ if d is odd and $h_{\mathcal{O}_{\mathcal{K}}} = 2h_{\mathcal{K}}$ otherwise. Thus, $\mathcal{O}_{\mathcal{K}}$ is a principal ideal domain if and only if d is odd and $h_{\mathcal{K}} = 1$. By Corollary (1.3.7), we have

$$(\sqrt{q}-1)^{2g} \leq h_{\mathcal{K}} \leq (\sqrt{q}+1)^{2g},$$

which follows that

(a) $h_{\mathcal{K}} = 1$ whenever $g = 0$ and $q \geq 3$,

(b) If $g = 1$, then $h_{\mathcal{K}} = 1$ only if $q = 3$,

(c) $h_{\mathcal{K}} > 1$ for all $g > 1$ and all $q \geq 3$.

Given that d must be odd, it follows from Proposition (1.5.10) that the genus of $\mathcal{K}$ is 0 if and only if $d = 1$ and the genus of $\mathcal{K}$ is 1 if and only if $d = 3$. For every square-free polynomial of degree 3 in $\mathbb{F}_3[x]$, the zeta function $Z_{\mathcal{K}}(u)$ of $\mathcal{K}$ can be computed and then, by the virtue of Theorem (1.3.5), $h_{\mathcal{K}}$ can be found using the formula

$$h_{\mathcal{K}} = \lim_{u \to 1} 2(u-1)Z_{\mathcal{K}}(u).$$

In this way one can derive the presented list of polynomials. □

Chapter 2
Drinfeld Modules

In this dissertation, the theory of Drinfeld Modules will play a role analogue to the complex multiplication theory in the classical case. In this chapter we collect various results concerning Drinfeld Modules.

2.1 Construction of Drinfeld Modules

Definition 2.1.1. Let K be a function field over $\mathbb{F}$ and S be a non-empty finite set of primes of K. The *ring of S-integers* in K is

$$O_S = \{\, \alpha \in K \,|\, \mathrm{ord}_P(\alpha) \geq 0 \text{ for all } P \notin S \,\}.$$

Proposition 2.1.2. *Let K be a function field over $\mathbb{F}$ and S be a non-empty finite set of primes of K. There exists $x \in K$ such that S is the set of poles of x. For any x with this property O_S is the integral closure of $\mathbb{F}[x]$.*

Proof. See Theorem 14.5 in [8]. □

Let L be a field containing $\mathbb{F}$. Recall that the Frobenius endomorphism of L is the map $\tau : L \to L$ defined by $\tau(\alpha) = \alpha^q$.

Definition 2.1.3. Let L be a field containing $\mathbb{F}$ and $\mathrm{End}_{\mathbb{F}}(L)$ the ring of endomorphism of L which fix $\mathbb{F}$. The subring of $\mathrm{End}_{\mathbb{F}}(L)$ generated by the Frobenius endomorphism τ is called the *ring of skewed polynomials* over L and is denoted by $L\langle\tau\rangle$.

Note that every element of $L\langle\tau\rangle$ can be indeed written as polynomial in τ with coefficients in L. The only thing that distinguishes this ring from the regular polynomial ring $L[X]$ is that multiplication of ”variable” τ by elements of L is not commutative and subject to the relation:

$$\tau a = a^q \tau$$

for all $a \in L$. Since $L\langle \tau \rangle$ is not commutative, it cannot be Euclidean in a usual sense. However, mimicking the proof for the commutative polynomial rings, one can easily show that $L\langle \tau \rangle$ is *right Euclidean*, that is, if $f,\ g \in L\langle \tau \rangle$ and $g \neq 0$, then there exist $s,\ r \in L\langle \tau \rangle$ such that $f = sg + r$ with $\deg r < \deg g$. A simple consequence of this fact is that every left ideal in $L\langle \tau \rangle$ is principal.

Definition 2.1.4. Let K be a function field over $\mathbb{F}$ and $S = \{\infty\}$, where ∞ is a fixed prime of K of degree d_∞. Let L be a field containing $\mathbb{F}$ and A be the ring of S-integers. A *Drinfeld A-module over L* consists of an $\mathbb{F}$-algebra homomorphism $\delta : A \to L$, together with an $\mathbb{F}$-algebra homomorphism $\rho : A \to L\langle \tau \rangle$ such that the constant term of ρ_a equals $\delta(a)$ for all $a \in A$ and $\deg_\tau \rho_a \geq 1$ for at least one $a \in A$.

For a fixed map $\delta : A \to L$, the symbol $\mathrm{Drin}_A(L)$ will denote the set of all A-Drinfeld modules over L.

Proposition 2.1.5. *Let $\rho \in \mathrm{Drin}_A(L)$. There exists a positive integer r such that $\deg_\tau \rho_a = -r \operatorname{ord}_\infty(a)\, d_\infty$ for all $a \in A$.*

Proof. See Proposition 13.7 and Theorem 13.1 in [8]. □

Definition 2.1.6. Let $\rho \in \mathrm{Drin}_A(L)$. The positive integer r such that $\deg_\tau \rho_a = -r \operatorname{ord}_\infty(a)\, d_\infty$ for all $a \in A$ is called *the rank* of the Drinfeld module ρ.

Definition 2.1.7. Let $\rho,\ \rho' \in \mathrm{Drin}_A(L)$. We say that $\rho,\ \rho'$ are *isomorphic* if and only if there is a non-zero element $c \in L$ such that $c\rho_a = \rho'_a c$ for all $a \in A$. The set of isomorphism classes of Drinfeld modules will be denoted by $\mathrm{Drin}^o_A(L)$.

Even though it is not easy to give non-trivial examples of Drinfeld modules using the definition, there exist infinitely many Drinfeld modules of all ranks and they all can be constructed using analytic methods. In classical number theory, analytic methods typically rely on the theory of meromorphic functions defined on the field of complex number. The field $\mathbb{C}$ can be defined as algebraic closure of the real numbers. Since $\mathbb{C}$ is finitely dimensional over $\mathbb{R}$, it follows it is complete. The situation is more complicated over function fields. The valuation $|\cdot|_\infty$ extends uniquely to the algebraic closure of $\mathcal{R}$ in a standard way. If $\alpha \in \overline{\mathcal{R}}$ and $\mathcal{S} = \mathcal{R}(\alpha)$, we set

$$|\alpha|_\infty = |N_{\mathcal{S}/\mathcal{R}}(\alpha)|_\infty^{[\mathcal{S}:\mathcal{R}]^{-1}}.$$

However, $\overline{\mathcal{R}}$ is not complete with respect to this valuation and hence we define $\mathcal{C}$ to be the completion of $\overline{\mathcal{R}}$. The field $\mathcal{C}$ is known to be algebraically closed and it is regarded as the analog of the field of complex numbers.

If K is a function field over $\mathbb{F}$ and P is a fixed prime of K, one can repeat the described construction with K as the base field as follows. The field K is not complete with respect to the multiplicative valuation $|\cdot|_P$ so one can form the completion K_P and extend $|\cdot|_P$ uniquely to K_P. As before this valuation can be further extended to the algebraic closure of K_P in the standard way. Finally, one defines $\mathcal{C}$ to be the completion of $\overline{K_P}$.

The symbol $\mathcal{C}$ is ambiguous because the field resulting from the described procedure depends both on the base field and the choice of the prime P. This ambiguity typically does not lead to any confusion as the base field and the prime P are fixed. However, we will consider simultaneously the rational function field $\mathcal{Q}$ with the prime at infinity p_∞ and an imaginary, quadratic field $\mathcal{K} = \mathcal{Q}(\sqrt{-n})$ with the prime $\mathfrak{p}_\infty$ which lies above p_∞. Fortunately, as it will follow from the next lemma, essentially there is no confusion in this case.

Lemma 2.1.8. *Let $\mathcal{K} = \mathcal{Q}(\sqrt{-n})$ be an imaginary, quadratic field and $\mathfrak{p}_\infty$ be the unique prime above p_∞. If $|\cdot|_\infty$ is extended to $\mathcal{K}$ via*

$$|\alpha|_\infty = |N_{\mathcal{K}/\mathcal{Q}}(\alpha)|_\infty^{[\mathcal{K}:\mathcal{Q}]^{-1}}$$

and $|\cdot|_{\mathfrak{p}_\infty}$ is the normalized valuation associated with $\mathfrak{p}_\infty$, then

$$|\alpha|_{\mathfrak{p}_\infty} = |\alpha|_\infty^2$$

for all $\alpha \in \mathcal{K}$. Moreover, there is an isomorphism $i : \mathcal{R}(\sqrt{-n}) \to K_{\mathfrak{p}_\infty}$ such that

$$|i(\alpha)|_{\mathfrak{p}_\infty} = |\alpha|_\infty^2 \tag{2.1.1}$$

for all $\alpha \in \mathcal{R}(\sqrt{-n})$

Proof. Let d_∞ be the degree of $\mathfrak{p}_\infty$. Since $\mathrm{ord}_{\mathfrak{p}_\infty}(\cdot) = e(\mathfrak{p}_\infty|p_\infty) \cdot \mathrm{ord}_{p_\infty}(\cdot)$ and $e(\mathfrak{p}_\infty|p_\infty) \cdot d_\infty = 2$, we have

$$\begin{aligned}\mathrm{ord}_{p_\infty}(N_{\mathcal{K}/\mathcal{Q}}(\alpha)) &= \frac{d_\infty}{2}\mathrm{ord}_{\mathfrak{p}_\infty}(N_{\mathcal{K}/\mathcal{Q}}(\alpha))\\ &= \frac{d_\infty}{2}(\mathrm{ord}_{\mathfrak{p}_\infty}(\alpha) + \mathrm{ord}_{\mathfrak{p}_\infty}(\overline{\alpha}))\\ &= d_\infty \mathrm{ord}_{\mathfrak{p}_\infty}(\alpha)\end{aligned}$$

Thus,

$$|\alpha|_\infty^2 = |N_{\mathcal{K}/\mathcal{Q}}(\alpha)|_\infty = q^{-\mathrm{ord}_{p_\infty}(N_{\mathcal{K}/\mathcal{Q}}(\alpha))} = q^{-d_\infty \mathrm{ord}_{\mathfrak{p}_\infty}(\alpha)} = |\alpha|_{\mathfrak{p}_\infty}.$$

Since $\mathcal{Q} \subset \mathcal{K}_{\mathfrak{p}_\infty}$ and the valuations $|\cdot|_\infty$ and $|\cdot|_{\mathfrak{p}_\infty}$ are equivalent, it follows that is isomorphic to the closure of $\mathcal{Q}$ in $\mathcal{K}_{\mathfrak{p}_\infty}$. Given that $\sqrt{-n} \in \mathcal{K}_{\mathfrak{p}_\infty}$, there is an embedding $i : \mathcal{R}(\sqrt{-n}) \to \mathcal{K}_{\mathfrak{p}_\infty}$ which fixes $\mathcal{K}$. It is easy to see that i is surjective.

Finally, if $\beta \in \mathcal{K}_{\mathfrak{p}_\infty}$ and $\beta = i(\alpha)$ for some $\alpha \in \mathcal{R}(\sqrt{-n})$, then $\alpha = \lim_{k\to\infty} \alpha_k$, where $\alpha_k \in \mathcal{K}$. Since i fixes $\mathcal{K}$, we also have $i(\alpha) = \lim_{k\to\infty} \alpha_k$. Consequently,

$$|\alpha|_{\mathfrak{p}_\infty} = \lim_{k\to\infty} |\alpha_k|_{\mathfrak{p}_\infty} = \lim_{k\to\infty} |\alpha_k|_\infty^2 = |\alpha|_\infty^2.$$

□

Using basic properties of algebraic closures, we see that the map i can be extended to algebraic closures of $\mathcal{K}_{\mathfrak{p}_\infty}$ and $\mathcal{R}$. Since $[\mathcal{R}(\sqrt{-n}) : \mathcal{R}] = 2$ and the norm function behaves transitively in towers of fields, an extension of i can chosen so that the equality (2.1.1) holds for all $\alpha \in \overline{\mathcal{R}}$. Thus, i being both an isomorphism and homeomorphism can be further extended to an isomorphism between the completion of $\overline{\mathcal{K}_{\mathfrak{p}_\infty}}$ with respect to $|\cdot|_{\mathfrak{p}_\infty}$ and $\mathcal{C}$ in such a way that the equality (2.1.1) holds for all $\alpha \in \mathcal{C}$.

Now we will describe briefly how to construct Drinfeld modules of any rank which will also lead to very important correspondence between Drinfeld modules and lattices. The construction and the correspondence are somehow similar to the correspondence between elliptic curves and lattices of rank 2 in $\mathbb{C}$. Since we will be interested in both $\mathcal{Z}$- and $\mathcal{O}_\mathcal{K}$-Drinfeld modules, let us go back to a more general set up. Namely, we let K be a function field over $\mathbb{F}$ and $\mathcal{C}$ be the completion of $\overline{K_P}$, where P is a fixed prime of K. Further, let A be the ring of P-integers.

Definition 2.1.9. An *A-lattice* in $\mathcal{C}$ is defined to be a discrete, finitely generated, A-submodule of $\mathcal{C}$. If $\Lambda \subset \mathcal{C}$ is a lattice, then the *rank* of Λ is the dimension of $K_P\Lambda$ over K_P. The set of all A-lattices in $\mathcal{C}$ will be denoted by $\mathrm{Lat}_A(\mathcal{C})$.

The standard fact about A-lattices in $\mathcal{C}$ is the following.

Lemma 2.1.10. *Every A-lattice of rank r in $\mathcal{C}$ is of the form*

$$\mathfrak{a}_1 c_1 + \mathfrak{a}_2 c_2 + \cdots + \mathfrak{a}_r c_r,$$

where $\mathfrak{a}_1$*,* $\mathfrak{a}_2, \ldots, \mathfrak{a}_r$ *are fractional ideals of* A*, and* $c_1, c_2, \ldots, c_r$ *are elements of* $\mathcal{C}$ *which are linearly independent* K_P*. Conversely, any set of this form is an* A*-lattice of rank* r *in* $\mathcal{C}$*.*

Theorem 2.1.11. *There exists a rank preserving bijection between* $\mathrm{Lat}_A(\mathcal{C})$ *and* $\mathrm{Drin}_A(\mathcal{C})$*.*

Sketch of a proof. Let Γ be an A-lattice in $\mathcal{C}$ of rank r. We define the exponential function associated to Γ by

$$e_\Gamma(x) = x \prod_{\gamma \in \Gamma \setminus \{ 0 \}} \left(1 - \frac{x}{\gamma}\right).$$

$e_\Gamma(x)$ is the unique entire function with simple zeros on the elements of Γ and with leading term x. $e_\Gamma(x)$ is also known to be $\mathbb{F}$-linear. Next, if $\Gamma \subset \Gamma'$ and Γ' is also a lattice of rank r, then Γ'/Γ is finite and

$$P(x; \Gamma'/\Gamma) = x \prod_{\mu \in \Gamma'/\Gamma} \left(1 - \frac{x}{e_\Gamma(\mu)}\right)$$

is $\mathbb{F}$-linear polynomial with the initial term x. Consequently, it can be written as polynomial in τ. Thus, $aP(x; a^{-1}\Gamma/\Gamma) \in \mathcal{C}\langle\tau\rangle$ for each $a \in A \setminus \{ 0 \}$. If we set

$$\rho_a^\Gamma(x) = aP(x; a^{-1}\Gamma/\Gamma),$$

then ρ^Γ is a A-Drinfeld module of rank r. Moreover, the map $\Gamma \to \rho^\Gamma$ is rank preserving bijection between $\mathrm{Lat}_A(\mathcal{C})$ and $\mathrm{Drin}_A(\mathcal{C})$. For more details see Theorems (13.23) and (13.24) in [8]. □

2.2 Rank-One $\mathcal{O}_\mathcal{K}$-Drinfeld Modules

Clearly, every fractional ideal of $\mathcal{K}$ is an $\mathcal{O}_\mathcal{K}$-lattice of rank 1. Due to Theorem (2.1.11) rank-one $\mathcal{O}_\mathcal{K}$-Drinfeld modules become very important objects to study.

Let $S = \{\, \mathfrak{p}_\infty \,\}$, where $\mathfrak{p}_\infty$ is the unique prime above p_∞ in an imaginary quadratic, field $\mathcal{K} = \mathcal{Q}(\sqrt{-n})$. Then, by Proposition (2.1.2), $\mathcal{O}_\mathcal{K} = \mathcal{Z}[\sqrt{-n}]$ is the ring of S-integers in $\mathcal{K}$. We will discuss rank-one $\mathcal{O}_\mathcal{K}$-Drinfeld modules over $\mathcal{C}$ in this section. The structure map $\delta : \mathcal{O}_\mathcal{K} \to \mathcal{C}$ is assumed to the inclusion. In order to simplify the notation, we will fix a square root of $-n$ in $\mathcal{K}$ and denote it by y.

Lemma 2.2.1. *Let ρ be a rank-one $\mathcal{O}_\mathcal{K}$-Drinfeld module in $\mathcal{C}$. Then for every $a \in \mathcal{Z}$*

$$\deg_\tau \rho_a = 2 \deg a.$$

Proof. First, recall that $d_\infty = f(\mathfrak{p}_\infty | \, p_\infty)$ and $\mathrm{ord}_{\mathfrak{p}_\infty}(\cdot) = e(\mathfrak{p}_\infty | \, p_\infty) \cdot \mathrm{ord}_{p_\infty}(\cdot)$ on $\mathcal{Q}$. By the definition of the rank of a Drinfeld module, we have

$$\begin{aligned}\deg_\tau \rho_a &= -d_\infty \mathrm{ord}_{\mathfrak{p}_\infty}(a) \\ &= -f(\mathfrak{p}_\infty | \, p_\infty) \cdot e(\mathfrak{p}_\infty | \, p_\infty) \cdot \mathrm{ord}_{p_\infty}(a) \\ &= f(\mathfrak{p}_\infty | \, p_\infty) \cdot e(\mathfrak{p}_\infty | \, p_\infty) \cdot \deg a \\ &= 2 \deg a.\end{aligned}$$

The last equality follows from the fact that $\mathfrak{p}_\infty$ is the unique prime above p_∞. □

Corollary 2.2.2. $\deg_\tau \rho_x = 2$ *and* $\deg_\tau \rho_y = d$.

Proof. The first equality follows immediately from the lemma. The second one follows from

$$2 \deg_\tau \rho_y = \deg_\tau \rho_y^2 = \deg_\tau \rho_{y^2} = \deg_\tau \rho_{-n} = 2 \deg(-n) = 2d.$$

□

Since x, y generate $\mathcal{O}_\mathcal{K}$ as an $\mathbb{F}$-algebra, a rank-one $\mathcal{O}_\mathcal{K}$-Drinfeld module ρ in $\mathcal{C}$ is determined uniquely by two polynomials ρ_x, ρ_y. By Corollary (2.2.2), these polynomials are of degree 2 and d respectively and since ρ is an $\mathbb{F}$-algebra homomorphism, they commute. As observed in [7], these two conditions are sufficient to define a rank-one $\mathcal{O}_{\mathcal{K}}$-Drinfeld module. More specifically, we have the following result.

Lemma 2.2.3. *Let f, $g \in \mathcal{C}\langle\tau\rangle$ be twisted polynomials such that $\deg_\tau f = 2$ and $\deg_\tau g = d$. If x, y are constant terms of f, g respectively and $fg = gf$, then there exists a unique rank-one $\mathcal{O}_{\mathcal{K}}$-Drinfeld module ρ such that $\rho_x = f$, $\rho_y = g$.*

Proof (due to M. Rosen). Let $\overline{\rho} : \mathbb{F}[X,Y] \to \mathcal{C}\langle\tau\rangle$ be a unique $\mathbb{F}$-algebra homomorphism such that $\overline{\rho}_X = f$ and $\overline{\rho}_Y = g$ and let $\pi : \mathbb{F}[X,Y] \to \mathcal{O}_{\mathcal{K}}$ be the canonical projection. Note that for every $H(X,Y) \in \mathbb{F}[X,Y]$ the constant term of $H(f,g)$ is $H(x,y)$. Thus, if $H(x,y) = 0$, then the lowest degree term of $H(f,g)$ is $c_k\tau^k$ for some $c_k \in \mathcal{C}$ and $k \geq 1$. Since f, g commute, we have

$$fH(f,g) = H(f,g)f.$$

Comparing coefficients of the lowest degree terms, we get

$$xc_k = c_k x^{q^k},$$

which follows that $c_k = 0$. Consequently, $H(f,g) = 0$, which shows that $\ker\pi \subset \ker\overline{\rho}$. Thus, there is a unique $\mathbb{F}$-algebra homomorphism $\rho : \mathcal{O}_{\mathcal{K}} \to \mathcal{C}\langle\tau\rangle$ such that $\overline{\rho} = \rho \circ \pi$. It is easy to see that the for every $a \in \mathcal{O}_{\mathcal{K}}$ constant term of ρ_a is a. Finally, $\deg_\tau \rho_x = 2$ proves that ρ is in fact a rank-one $\mathcal{O}_{\mathcal{K}}$-Drinfeld module in $\mathcal{C}$. □

2.3 j-invariant

Let ϕ be a $\mathcal{Z}$-Drinfeld module of rank 2. The structural map is assumed to be the inclusion $i : \mathcal{Z} \to \mathcal{C}$. Since $\mathcal{Z}$ is a free $\mathbb{F}$-algebra generated by T, the module Drinfeld

ϕ is determined by its value at x. Since the degree of p_∞ is 1 and $\mathrm{ord}_{p_\infty}(a) = -\deg a$ for all $a \in \mathcal{Z}$, it follows from Definition (2.1.6) that $\deg_\tau \phi_a = 2 \deg a$ for all $a \in \mathcal{Z}$. In particular,

$$\phi_x(\tau) = T + f_1\tau + f_2\tau^2$$

for some $f_1 \in \mathcal{C}$ and $f_2 \in \mathcal{C}^*$. We will write $\phi = (f_1, f_2)$ in such a case.

If $\phi = (f_1, f_2)$ and $\psi = (g_1, g_2)$ are isomorphic modules, then $c \cdot \phi_x = \psi_x \cdot c$ for some $c \in \mathcal{C}^*$. But

$$(c \cdot \phi_x)(\tau) = cx + f_1 c^q \tau + f_2 c^{q^2} \tau^2$$

and

$$(\psi_x \cdot c)(\tau) = cx + cf_1\tau + cf_2\tau^2,$$

so $f_1 = c^{q-1}g_1$ and $f_2 = c^{q^2-1}g_2$, which in turns implies

$$\frac{f_1^{q+1}}{f_2} = \frac{c^{q^2-1}g_1^{q+1}}{c^{q^2-1}g_2} = \frac{g_1^{q+1}}{g_2}$$

This leads to the following definition.

Definition 2.3.1. The *j-invariant* of a Drinfeld module $\phi = (f_1, f_2)$ is defined by

$$j(\phi) = \frac{f_1^{q+1}}{f_2}.$$

Let ρ be a rank-one $\mathcal{O}_\mathcal{K}$-Drinfeld module over $\mathcal{C}$. As before the structure map $\delta : \mathcal{O}_\mathcal{K} \to \mathcal{C}$ is assumed to be inclusion. Then the restriction $\rho_{|\mathcal{Z}} : \mathcal{Z} \to \mathcal{C}\langle\tau\rangle$ is an $\mathbb{F}$-algebra homomorphism and $\delta_{|\mathcal{Z}} : \mathcal{Z} \to \mathcal{C}$ remains to be the inclusion. Clearly, the constant term of $(\rho_{|\mathcal{Z}})_a$ equals a for all $a \in \mathcal{Z}$ and by Lemma (2.2.1), $\deg_\tau(\rho_{|\mathcal{Z}})_x = 2$. Thus, $\rho_{|\mathcal{Z}}$ is a $\mathcal{Z}$-Drinfeld module. Since the degree of p_∞ is 1 and $\mathrm{ord}_{p_\infty}(x) = -1$, the equality $\deg_\tau(\rho_{|\mathcal{Z}})_x = 2$ implies also that $\rho_{|\mathcal{Z}}$ is of rank 2. Observe also that if ρ and ρ' are isomorphic, then their restrictions $\rho_{|\mathcal{Z}}$ and $\rho'_{|\mathcal{Z}}$ are also isomorphic. This motivates the following definition.

Definition 2.3.2. Let ρ be a rank-one $\mathcal{O}_{\mathcal{K}}$-Drinfeld module over $\mathcal{C}$. The j-invariant of ρ is defined to be the j-invariant of the restriction $\rho_{|\mathcal{Z}}$.

Since rank-one $\mathcal{O}_{\mathcal{K}}$-Drinfeld modules correspond to fractional ideals of $\mathcal{O}_{\mathcal{K}}$, we may also define the j-invariant of a fractional ideal.

Definition 2.3.3. Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_{\mathcal{K}}$. The j-invariant of $\mathfrak{a}$, denoted by $j(\mathfrak{a})$, is defined to be the j-invariant of the corresponding rank-one Drinfeld module $\rho^{\mathfrak{a}}$.

Just like in the classical case, we have the following result.

Theorem 2.3.4. *Let ϕ be a Drinfeld module associated with an ideal of $\mathcal{O}_{\mathcal{K}}$. Then $j(\phi)$ is integral over $\mathcal{Z}$.*

Proof. See theorem (4.3) in [4]. □

Chapter 3

Sign Normalization and Class Field Theory of $\mathcal{K}$.

3.1 The Artin Map

Let $\mathcal{K} = \mathcal{Q}(\sqrt{-n})$ be an imaginary extension of $\mathcal{K}$ and $\mathcal{K}_{sep}$ be a separable closure of $\mathcal{K}$. Let $\mathcal{L} \subset \mathcal{K}_{sep}$ be a finite, unramified Galois extension of $\mathcal{K}$ and let $\mathfrak{p} \in \mathcal{D}_{\mathcal{K}}$ be a prime of $\mathcal{K}$. If $\mathfrak{P} \in \mathcal{D}_{\mathcal{L}}$ lies above $\mathfrak{p}$, then $e(\mathfrak{P}|\mathfrak{p}) = 1$ and $\kappa(\mathfrak{P}) = \mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$ is a Galois extension of $\kappa(\mathfrak{p}) = \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$ of degree $f(\mathfrak{P}|\mathfrak{p})$. Since $\kappa(\mathfrak{p})$ is a finite field with $N(\mathfrak{p}) = q^{\deg(\mathfrak{p})}$ elements, it follows that $\mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ is a cyclic group of order $f(\mathfrak{P}|\mathfrak{p})$ and the map

$$x \mapsto x^{N(\mathfrak{p})} \tag{3.1.1}$$

is its generator. The Galois group $\mathrm{Gal}(\mathcal{L}/\mathcal{K})$ acts transitively on the set of primes of $\mathcal{L}$ that lie above $\mathfrak{p}$. Let $D_{\mathfrak{P}}$ be the stabilizer of $\mathfrak{P}$. Then we have a map $D_{\mathfrak{P}} \longrightarrow \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ given by

$$\sigma \mapsto \overline{\sigma}, \quad \text{where} \quad \overline{\sigma}(x + \mathfrak{P}) = \sigma(x) + \mathfrak{P}. \tag{3.1.2}$$

This map is onto and since $e(\mathfrak{P}|\mathfrak{p}) = 1$, it is also injective. This important isomorphism will be used to define the Artin map. The first step is the following lemma.

Lemma 3.1.1. *There is a unique element $(\mathfrak{P}, \mathcal{L}/\mathcal{K}) \in \mathrm{Gal}(\mathcal{L}/\mathcal{K})$ such that*

$$(\mathfrak{P}, \mathcal{L}/\mathcal{K})(x) \equiv x^{N(\mathfrak{p})} \quad (mod\, \mathfrak{P})$$

for all $x \in \mathcal{O}_{\mathfrak{P}}$.

Proof. Let $(\mathfrak{P}, \mathcal{L}/\mathcal{K})$ be the inverse image of the generator (3.1.1) under the map (3.1.2). In order to prove uniqueness, observe that any σ in $\mathrm{Gal}(\mathcal{L}/\mathcal{K})$ that satisfies the above congruence condition is necessarily in the stabilizer of $\mathfrak{P}$. □

Corollary 3.1.2. *Let* $\sigma \in \mathrm{Gal}(\mathcal{L}/\mathcal{K})$*. Then*

(a) $(\sigma(\mathfrak{P}), \mathcal{L}/\mathcal{K}) = \sigma(\mathfrak{P}, \mathcal{L}/\mathcal{K})\sigma^{-1}$.

(b) The order of $(\mathfrak{P}, \mathcal{L}/\mathcal{K})$ *if* $f(\mathfrak{P}|\mathfrak{p})$.

(c) $\mathfrak{p}$ *splits completely in* $\mathcal{L}$ *if and only if* $(\mathfrak{P}, \mathcal{L}/\mathcal{K}) = 1$.

Proof. Let $y \in \mathcal{O}_{\sigma(\mathfrak{P})}$. Then $y = \sigma(x)$ for some $x \in \mathcal{O}_{\mathfrak{P}}$ and $\sigma(\mathfrak{P}, \mathcal{L}/\mathcal{K})\sigma^{-1}(y)$ $= \sigma(\mathfrak{P}, \mathcal{L}/\mathcal{K})(x)$. Since $(\mathfrak{P}, \mathcal{L}/\mathcal{K})(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{P}}$, it follows that $\sigma(\mathfrak{P}, \mathcal{L}/\mathcal{K})(x) \equiv y^{N(\mathfrak{p})} \pmod{\sigma(\mathfrak{P})}$. But $(\sigma(\mathfrak{P}), \mathcal{L}/\mathcal{K})$ is the unique element of $\mathrm{Gal}(\mathcal{L}/\mathcal{K})$ having this property so we must have

$$(\sigma(\mathfrak{P}), \mathcal{L}/\mathcal{K}) = \sigma(\mathfrak{P}, \mathcal{L}/\mathcal{K})\sigma^{-1}.$$

Part (b) follows directly from the definition of $(\mathfrak{P}, \mathcal{L}/\mathcal{K})$. Finally, $\mathfrak{p}$ splits completely in $\mathcal{L}$ if and only if $e(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{p}) = 1$ since $\mathrm{Gal}(\mathcal{L}/\mathcal{K})$ acts transitively on the set of primes lie above $\mathfrak{p}$. We have $e(\mathfrak{P}|\mathfrak{p}) = 1$ since $\mathcal{L}/\mathcal{K}$ is unramified and $f(\mathfrak{P}|\mathfrak{p}) = 1$ if and only if $(\mathfrak{P}, \mathcal{L}/\mathcal{K}) = 1$ by part (b). □

If $\mathcal{L}/\mathcal{K}$ is an Abelian extension, then by part (a) of the corollary the automorphism $(\mathfrak{P}, \mathcal{L}/\mathcal{K})$ does not depend on the choice of $\mathfrak{P}$ above $\mathfrak{p}$. In such a case, it will be denoted by $(\mathfrak{p}, \mathcal{L}/\mathcal{K})$ and called the *Artin symbol.* Since $\mathcal{D}_{\mathcal{K}}$ is a free group generated by primes, we may define the Artin symbol for any divisor $D \in \mathcal{D}_{\mathcal{K}}$. If $D = \sum_{\mathfrak{p}} a(\mathfrak{p})\mathfrak{p}$, we set

$$(D, \mathcal{L}/\mathcal{K}) = \prod_{\mathfrak{p}} (\mathfrak{p}, \mathcal{L}/\mathcal{K})^{a(\mathfrak{p})}.$$

Thus, we get a group homomorphism $(\quad, \mathcal{L}/\mathcal{K}) : \mathcal{D}_{\mathcal{K}} \to \mathrm{Gal}(\mathcal{L}/\mathcal{K})$, called the *Artin map.*

In previous chapters we have seen that many concepts and techniques of the classical theory of number fields have rather natural analogues in the function field context. Unfortunately, the notion of the Hilbert class field cannot be generalized that easily. If K is a function field, then the maximal abelian unramified extension of K is not finite.

If S is a finite, non-empty set of primes of a function field K and A is the ring of S-integers of K, then following Michael Rosen [9], we define the Hilbert class field as follows.

Definition 3.1.3. *The Hilbert class field of K with respect to A*, denoted by K^A, is the maximal unramified abelian extension of K in K_{sep} in which every prime $P \in S$ splits completely.

Recall that the ring that the ring of integers $\mathcal{O}_{\mathcal{K}}$ in an imaginary extension $\mathcal{K}/\mathcal{Q}$ can be viewed as a ring of S-integers for $S = \{\, \mathfrak{p}_\infty \,\}$. Thus, the Hilbert class field of $\mathcal{K}$ with respect to $\mathcal{O}_{\mathcal{K}}$ is the maximal abelian unramified extension of $\mathcal{K}$ in $\mathcal{K}_{sep}$ in which $\mathfrak{p}_\infty$ splits completely. Since this is the only Hilbert class field we are interested in, we will call it simply the Hilbert class field of $\mathcal{K}$ and denote it by $\mathcal{H}$. We have the following fundamental result about $\mathcal{H}$.

Theorem 3.1.4. *The Artin symbol $(\quad, \mathcal{H}/\mathcal{K})$ induces isomorphism between $\mathrm{Cl}(\mathcal{O}_{\mathcal{K}})$ and $\mathrm{Gal}(\mathcal{H}/\mathcal{K})$. Consequently, $\mathcal{H}/\mathcal{K}$ is a finite extension of degree $h_{\mathcal{O}_{\mathcal{K}}}$.*

Sketch of a proof. It is known from the class field theory that the Artin map is surjective and every principal divisor is mapped into identity. Consequently, the map

$$\sum_{\mathfrak{p}} a(\mathfrak{p})[\mathfrak{p}] \longmapsto \prod_{\mathfrak{p}} (\mathfrak{p}, \mathcal{H}/\mathcal{K})^{a(\mathfrak{p})} \tag{3.1.3}$$

is a well-defined epimorphism between $\mathrm{Cl}(\mathcal{K})$ and $\mathrm{Gal}(\mathcal{H}/\mathcal{K})$. Since $\mathfrak{p}_\infty$ splits completely in $\mathcal{H}$, we have $(\mathfrak{p}_\infty, \mathcal{H}/\mathcal{K}) = 1$ by part (c) of Lemma (3.1.2). In fact, one can show that $\mathcal{N} = [\mathfrak{p}_\infty]\mathbb{Z}$ is precisely the kernel of (3.1.3). Thus,

$$\mathrm{Cl}(\mathcal{K})/\mathcal{N} \simeq \mathrm{Gal}(\mathcal{H}/\mathcal{K}).$$

On the other hand, by the virtue of Lemma 1.1 in [9]

$$\mathrm{Cl}(\mathcal{K})/\mathcal{N} \simeq \mathrm{Cl}(\mathcal{O}_\mathcal{K})$$

via

$$\sum_{\mathfrak{p}\neq\mathfrak{p}_\infty} a(\mathfrak{p})[\mathfrak{p}] \longmapsto \prod_{\mathfrak{p}\neq\mathfrak{p}_\infty} [\mathfrak{p}]^{a(\mathfrak{p})}.$$

Composition of these two maps gives an isomorphism between $\mathrm{Cl}(\mathcal{O}_\mathcal{K})$ and $\mathrm{Gal}(\mathcal{H}/\mathcal{K})$ such that

$$[\mathfrak{p}] \longmapsto (\mathfrak{p}, \mathcal{H}/\mathcal{K}).$$

For more details see Theorem 1.3 in [9] □

Just like in the classical case, the Hilbert class field is generated by the j-invariant. More precisely,we have the following result.

Theorem 3.1.5. *Let $j = j(\mathcal{O}_\mathcal{K})$. Then $\mathcal{H} = \mathcal{K}(j)$. Moreover, $[\mathcal{H} : \mathcal{K}] = [\mathcal{Q}(j) : \mathcal{Q}]$.*

Proof. See Corollary (4.5) in [4]. □

Corollary 3.1.6. *If $f(X)$ is the minimal polynomial of j over $\mathcal{K}$, then $f(X) \in \mathcal{Z}[X]$*

3.2 The Action of $\mathrm{Cl}(\mathcal{O}_\mathcal{K})$ on $\mathrm{Drin}^o_{\mathcal{O}_\mathcal{K}}(\mathcal{C}, 1)$

In this section, we shall see that the ideals of $\mathcal{O}_\mathcal{K}$ act naturally on isomorphism classes of $\mathcal{O}_\mathcal{K}$-Drinfeld modules. This action, when restricted to rank one Drinfeld modules, is faithful and transitive. This fact is the main link that joins the Hilbert class field of $\mathcal{K}$ with the theory of rank one $\mathcal{O}_\mathcal{K}$ Drinfeld modules.

Definition 3.2.1. Let ρ, $\rho' \in \mathrm{Drin}_{\mathcal{O}_\mathcal{K}}(\mathcal{C})$. An *isogeny* from ρ to ρ' is an element $f \in \mathcal{C}\langle\tau\rangle$ such that $f\rho_a = \rho'_a f$ for all $a \in \mathcal{O}_\mathcal{K}$.

Definition 3.2.2. Let $\mathfrak{a} \subset \mathcal{O}_\mathcal{K}$ be an ideal and $I_\mathfrak{a}$ be the left ideal in $\mathcal{C}\langle\tau\rangle$ generated by $\{\, \rho_a \,|\, a \in \mathfrak{a} \,\}$. Define $\rho_\mathfrak{a}$ to be the monic generator of $I_\mathfrak{a}$.

If $a \in \mathcal{O}_\mathcal{K}$, then $I_\mathfrak{a}\rho_a \subset I_\mathfrak{a}$ and hence $\rho_\mathfrak{a}\rho_a = \rho'_a\rho_\mathfrak{a}$ for some $\rho'_a \in \mathcal{C}\langle\tau\rangle$. By Proposition (13.13) in [8], the map $a \mapsto \rho'_a$ is a Drinfeld $\mathcal{O}_\mathcal{K}$-module. This module shall be denoted by $\mathfrak{a} * \rho$. Clearly, $\rho_\mathfrak{a}$ is an isogeny from $\mathfrak{a}$ to $\mathfrak{a} * \rho$. Moreover, $\mathfrak{a} * \rho$ is uniquely determined by this property.

Suppose that $\mathfrak{a} = (\alpha)$ is a principal ideal. Then $I_\mathfrak{a}$ is generated by ρ_α. Clearly, $\rho_\mathfrak{a} = c^{-1}\rho_\alpha$, where c is the leading coefficient of ρ_α. Moreover, $\mathfrak{a} * \rho$ and ρ are isomorphic:

$$\mathfrak{a} * \rho = c^{-1}\rho c. \tag{3.2.1}$$

Indeed, for every $a \in \mathcal{O}_\mathcal{K}$, we have $\rho_\mathfrak{a}\rho_a = (\mathfrak{a} * \rho)_a\rho_\mathfrak{a}$. Since $\rho_a\rho_\alpha = \rho_\alpha\rho_a$ and $\rho_\mathfrak{a} = c^{-1}\rho_\alpha$, the result follows. It is also known (see Lemma (4.5) in [6]) that

$$\mathfrak{a} * (\mathfrak{b} * \rho) = \mathfrak{a}\mathfrak{b} * \rho \tag{3.2.2}$$

for non-zero ideals $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_\mathcal{K}$. The equalities (3.2.1) and (3.2.2) imply that the operation $*$ induces an action of the class group $\mathrm{Cl}(\mathcal{O}_\mathcal{K})$ on the set $\mathrm{Drin}^o_{\mathcal{O}_\mathcal{K}}(\mathcal{C})$.

This action is especially useful when restricted to rank one Drinfeld modules as we have the following result.

Theorem 3.2.3. *The action of* $\mathrm{Cl}(\mathcal{O}_{\mathcal{K}})$ *on the set* $\mathrm{Drin}^{o}_{\mathcal{O}_{\mathcal{K}}}(\mathcal{C}, 1)$ *is faithful and transitive.*

Proof. See Theorem (13.27) in [8]. □

3.3 Sign Normalization

Let $\mathbb{F}_{\mathfrak{p}_\infty} = \mathcal{O}_{\mathfrak{p}_\infty}/\mathfrak{p}_\infty$, where $\mathcal{O}_{\mathfrak{p}_\infty}$ is the local ring of the completion $\mathcal{K}_{\mathfrak{p}_\infty}$. It is known that $[\mathbb{F}_{\mathfrak{p}_\infty} : \mathbb{F}] = \deg \mathfrak{p}_\infty = f(\mathfrak{p}_\infty \mid p_\infty)$. If $\deg n$ is odd, then p_∞ is ramified in $\mathcal{K}$ and hence $\mathbb{F}_{\mathfrak{p}_\infty} = \mathbb{F}$. Otherwise, p_∞ is inert in $\mathcal{K}$, which follows that $[\mathbb{F}_{\mathfrak{p}_\infty} : \mathbb{F}] = 2$. Since $\sqrt{-n_d} \notin \mathbb{F}$, we have $\mathbb{F}_{\mathfrak{p}_\infty} = \mathbb{F}(\sqrt{-n_d})$. In any case, if we choose a *uniformizer at* $\mathfrak{p}_\infty$, that is, an element π such that $\mathrm{ord}_{\mathfrak{p}_\infty}(\pi) = 1$, then every non-zero element α of $\mathcal{K}_{\mathfrak{p}_\infty}$ can be uniquely represented as a Laurent series

$$\alpha = \sum_{k=k_0}^{\infty} c_k \pi^k, \tag{3.3.1}$$

where $c_k \in \mathbb{F}_{\mathfrak{p}_\infty}$ and $c_{k_0} \neq 0$. Using this representation, we define a sign function as follows.

Definition 3.3.1. A *sign function associated with the uniformizer* π is given by

$$\mathrm{sgn}(\sum_{k=k_0}^{\infty} c_k \pi^k) = c_{k_0}.$$

Additionally, we set $\mathrm{sgn}(0) = 0$.

Clearly, a sign function is multiplicative. Note also that if α is a unit of the local ring $\mathcal{O}_{\mathfrak{p}_\infty}$, then $\mathrm{sgn}(\alpha) = 1$ if and only if $\alpha \equiv 1 \pmod{\mathfrak{p}_\infty}$.

Definition 3.3.2. Let $\sigma \in \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}_\infty}/\mathbb{F})$. If sgn is a sign function on $\mathcal{K}_{\mathfrak{p}_\infty}$, then the composition $\sigma \circ \mathrm{sgn}$ is called a *twisted sign function.* In this context, the automorphism σ is referred to as a *twist of the sign.*

The next lemma provides a convenient choice of the uniformizer at $\mathfrak{p}_\infty$.

Lemma 3.3.3. *Let g be the genus of $\mathcal{K}$. Then* $\mathrm{ord}_{\mathfrak{p}_\infty}(\frac{x^g}{y}) = 1$.

Proof. Since $\mathrm{ord}_{\mathfrak{p}_\infty}(\cdot) = e(\mathfrak{p}_\infty | p_\infty) \cdot \mathrm{ord}_\infty(\cdot)$ on $\mathcal{Q}$, we have

$$2\,\mathrm{ord}_{\mathfrak{p}_\infty}\left(\frac{x^g}{y}\right) = \mathrm{ord}_{\mathfrak{p}_\infty}\left(\frac{x^{2g}}{-n(x)}\right) = 2g\,\mathrm{ord}_{\mathfrak{p}_\infty}(x) - \mathrm{ord}_{\mathfrak{p}_\infty} n(x) = (d-2g)\cdot e(\mathfrak{p}_\infty | p_\infty).$$

By Proposition (1.5.10), $d-2g = d_\infty$ and by Corollary (1.5.7), $d_\infty \cdot e(\mathfrak{p}_\infty | p_\infty) = 2$. The result follows. □

Having defined a sign function, we will use it to *normalize* $\mathcal{O}_\mathcal{K}$-Drinfeld modules. This normalization will allow us to work with sgn-normalized modules instead of isomorphism classes, which will simplify certain arguments. Let ρ be a rank-one $\mathcal{O}_\mathcal{K}$-Drinfeld module over $\mathcal{C}$. For $\alpha \in \mathcal{O}_\mathcal{K}$, let $\mu_\rho(\alpha)$ be the leading coefficient of ρ_α. Since ρ is of rank one, we have $\deg_\tau(\rho_\alpha) = -d_\infty \cdot \mathrm{ord}_{\mathfrak{p}_\infty}(\alpha)$ and hence $q^{\deg_\tau(\rho_\alpha)} = N(\alpha)$. Thus,

$$\mu_\rho(\alpha\beta) = \mu_\rho(\alpha) \cdot \mu_\rho(\beta)^{N(\alpha)} \tag{3.3.2}$$

for all $\alpha, \beta \in \mathcal{O}_\mathcal{K}$. As explained in [6, Section 6], μ_ρ can be extended to $\mathcal{K}_{\mathfrak{p}_\infty}$ in such a way that the identity (3.3.2) still holds. The obtained will be denoted by the same symbol μ_ρ and referred to as the *leading coefficient map of ρ.*

Definition 3.3.4. Let ρ be a rank-one $\mathcal{O}_\mathcal{K}$-Drinfeld module over $\mathcal{C}$ and let sgn be a sign function on $\mathcal{K}_{\mathfrak{p}_\infty}$. We say that ρ is sgn-*normalized* if the leading coefficient map μ_ρ is a twisting of the sign function sgn.

Theorem 3.3.5. *Let* sgn *be a sign function on $\mathcal{K}_{\mathfrak{p}_\infty}$. Every rank-one $\mathcal{O}_\mathcal{K}$-Drinfeld module over $\mathcal{C}$ is isomorphic to a* sgn-*normalized Drinfeld module. Every isomorphism class in* $\mathrm{Drin}^o_{\mathcal{O}_\mathcal{K}}(\mathcal{C}, 1)$ *contains exactly* $\chi = \frac{q^{d_\infty}-1}{q-1}$ sgn-*normalized $\mathcal{O}_\mathcal{K}$-Drinfeld modules, and hence there are exactly $\chi \cdot h_{\mathcal{O}_\mathcal{K}}$ rank-one,* sgn-*normalized $\mathcal{O}_\mathcal{K}$-Drinfeld modules.*

Proof. See Theorem (12.3) and Corollary (13.2) in [6]. □

By Lemma (2.2.3), a rank-one Drinfeld module ρ is determined uniquely by

$$\rho_x = x + a_1\tau + a_2\tau^2,$$

$$\rho_y = y + b_1\tau + \cdots + b_d\tau^d,$$

where $d = \deg n$. If ρ is sign normalized, then $a_2, b_d \in \mathbb{F}_{\mathfrak{p}_\infty}$. More specifically, $a_2, b_d \in \mathbb{F}$ if d is odd and $a_2, b_d \in \mathbb{F}(\sqrt{-n_d})$ otherwise. Even more can be said if the normalization is with respect to the sign function associated to $\pi = \frac{x^g}{y}$.

Proposition 3.3.6. *Let* sgn *be a sign function on $\mathcal{K}_{\mathfrak{p}_\infty}$ associated to $\pi = \frac{x^g}{y}$, and let ρ be a sgn-normalized rank-one Drinfeld $\mathcal{O}_{\mathcal{K}}$-module. If a_2, b_d are the leading coefficients of ρ_x and ρ_y respectively, then $a_2^{d_\infty} = -n_d^{-1}$ and $b_d = a_2^g$.*

Proof. Let $u = (-n_d\pi^2 x^{d_\infty})^{-1}$. Then

$$\begin{aligned}\mathrm{ord}_{\mathfrak{p}_\infty}(u) &= -(\mathrm{ord}_{\mathfrak{p}_\infty}(-n_d) + 2\cdot \mathrm{ord}_{\mathfrak{p}_\infty}\pi + d_\infty \mathrm{ord}_{\mathfrak{p}_\infty} x)\\ &= -(0 + 2 - d_\infty \cdot e(\mathfrak{p}_\infty|\infty))\\ &= -2 + d_\infty \cdot e(\mathfrak{p}_\infty|\infty) = 0.\end{aligned}$$

Thus, u is a unit in $\mathcal{O}_{\mathfrak{p}_\infty}$. Now,

$$\begin{aligned}u - 1 = (-n_d\pi^2 x^{d_\infty})^{-1} - 1 &= \frac{-n(x)}{-n_d x^{2g+d_\infty}} - 1 = \frac{n(x) - n_d x^d}{n_d x^d}\\ &= \frac{n_{d-1}}{n_d}\cdot\frac{1}{x} + \frac{n_{d-2}}{n_d}\cdot\frac{1}{x^2} + \cdots + \frac{n_0}{n_d}\cdot\frac{1}{x^d},\end{aligned}$$

which follows that $u \equiv 1 \pmod{\mathfrak{p}_\infty}$. Consequently, $\mathrm{sgn}(u) = 1$. Since sgn is multiplicative and $\mathrm{sgn}(\pi) = 1$, we get

$$\mathrm{sgn}(x)^{d_\infty} = \mathrm{sgn}(-n_d^{-1}) = -n_d^{-1}. \tag{3.3.3}$$

and

$$\mathrm{sgn}(y) = \mathrm{sgn}(x)^g.$$

Now, if $\rho_x = a_2\tau^2 + a_1\tau + x$ and $\rho_y = b_d\tau^d + \cdots + b_1\tau + y$ and μ_ρ is the leading coefficient function, then

$$a_2 = \mu_\rho(x) = i_\rho(\mathrm{sgn}(x)),$$
$$b_d = \mu_\rho(y) = i_\rho(\mathrm{sgn}(y)),$$

where $i_\rho : \mathbb{F}_{\mathfrak{p}_\infty} \to \mathbb{F}_{\mathfrak{p}_\infty}$ is a twist of sgn.

If d is odd, then $\mathbb{F}_{\mathfrak{p}_\infty} = \mathbb{F}$ and i_ρ is the identity function. Consequently,

$$a_2 = -n_d^{-1}, \tag{3.3.4}$$
$$b_d = -n_d^{-g}, \tag{3.3.5}$$

If d is even, then $\mathbb{F}_{\mathfrak{p}_\infty} = \mathbb{F}(\sqrt{-n_d})$ and i_ρ is the identity on $\mathbb{F}$. Since $d_\infty = 2$, we get

$$\begin{aligned} \mathrm{sgn}(x)^2 &= -n_d^{-1} \\ i_\rho(\mathrm{sgn}(x)^2) &= i_\rho(-n_d^{-1}) \\ i_\rho(\mathrm{sgn}(x))^2 &= -n_d^{-1}, \\ a_2^2 &= -n_d^{-1}. \end{aligned} \tag{3.3.6}$$

We also have

$$\begin{aligned} \mathrm{sgn}(y) &= \mathrm{sgn}(x)^g \\ i_\rho(\mathrm{sgn}(y)) &= i_\rho(\mathrm{sgn}(x)^g) \\ b_d &= i_\rho(\mathrm{sgn}(x))^g \\ b_d &= a_2^g. \end{aligned} \tag{3.3.7}$$

□

3.4 Normalizing Field for Rank-one $\mathcal{O}_{\mathcal{K}}$-Drinfeld Modules

In the final section of this chapter, we present selected results concerning sgn-normalized rank-one $\mathcal{O}_{\mathcal{K}}$-Drinfeld modules. We follow closely the paper [6] of D. Hayes where the proofs and more detailed discussion of these results can be found.

Definition 3.4.1. Let sgn be a sign function on $\mathcal{K}_{\mathfrak{p}_\infty}$. We say that $\alpha \in \mathcal{K}_{\mathfrak{p}_\infty}$ is *positive* if $\operatorname{sgn}(\alpha) = 1$.

Definition 3.4.2. Let $\mathcal{I}(\mathcal{O}_{\mathcal{K}})$ be the set of fractional ideals of $\mathcal{O}_{\mathcal{K}}$ and $\mathcal{P}^+(\mathcal{O}_{\mathcal{K}})$ be the set of principal ideals which are generated by a positive element. The quotient group $\mathrm{Cl}^+(\mathcal{O}_{\mathcal{K}}) = \mathcal{I}(\mathcal{O}_{\mathcal{K}})/\mathcal{P}^+(\mathcal{O}_{\mathcal{K}})$ is called the *narrow class group* of $\mathcal{O}_{\mathcal{K}}$ relative to sgn. The order of this group will be denoted by $h^+_{\mathcal{O}_{\mathcal{K}}}$.

Let X be the set of sgn-normalized rank-one $\mathcal{O}_{\mathcal{K}}$-Drinfeld modules. One can check that if $\rho \in X$, then $\mathfrak{a} * \rho \in X$ for any ideal $\mathfrak{a} \subset \mathcal{O}_{\mathcal{K}}$. Furthermore, $\mathfrak{a} * \rho = \rho$ if and only if $\mathfrak{a} = \alpha\mathcal{O}_{\mathcal{K}}$ with $\operatorname{sgn}(\alpha) = 1$. If $\mathfrak{a}$ is a fractional ideal, then there is a positive element $\alpha \in \mathcal{K}$ such that $\alpha\mathfrak{a} \subset \mathcal{O}_{\mathcal{K}}$. In such a case, we define $\mathfrak{a} * \rho = (\alpha\mathfrak{a}) * \rho$. Thus, we obtain an action of $\mathcal{I}(\mathcal{O}_{\mathcal{K}})$ on X and now $\mathfrak{a} = \alpha\mathcal{O}_{\mathcal{K}}$ if and only if $\mathfrak{a} \in \mathcal{P}^+$. Consequently, the operation $*$ induces the action of the narrow class group $\mathrm{Cl}^+(\mathcal{O}_{\mathcal{K}})$ on X. By Theorem (3.3.5), $|X| = \chi \cdot h_{\mathcal{O}_{\mathcal{K}}}$, where $\chi = \frac{q^{d_\infty}-1}{q-1}$. Since sgn is multiplicative, $h^+_{\mathcal{O}_{\mathcal{K}}} = \chi \cdot h_{\mathcal{O}_{\mathcal{K}}}$. Thus, we have obtained the following result.

Theorem 3.4.3. *The action of* $\mathrm{Cl}^+(\mathcal{O}_{\mathcal{K}})$ *on* X *is faithful and transitive.*

Let ρ be a sgn-normalized rank-one $\mathcal{O}_{\mathcal{K}}$-Drinfeld module and let $\alpha \in \mathcal{O}_{\mathcal{K}} \setminus \mathbb{F}$. Set $\mathcal{H}^+_{\alpha,\rho} = \mathcal{K}(c_0, c_1, \ldots, c_k)$, where $\rho_\alpha = c_0 + c_1\tau + \cdots + c_k\tau^k$. As explained in [6, Section 14], $\mathcal{H}^+_{\alpha,\rho}$ depends neither on ρ nor on α. Thus, we can simply write $\mathcal{H}^+$ to denote this field.

Definition 3.4.4. The field $\mathcal{H}^+$ is called the *normalizing field* for rank-one $\mathcal{O}_\mathcal{K}$-Drinfeld modules over the triple $(\mathcal{K}, \mathfrak{p}_\infty, \mathrm{sgn})$.

The importance of this field stems from the next three theorems.

Theorem 3.4.5. *The normalizing field $\mathcal{H}^+$ is a Galois extension of $\mathcal{K}$. The Galois group $\mathrm{Gal}(\mathcal{H}^+/\mathcal{K})$ is isomorphic to the narrow class group $\mathrm{Cl}^+(\mathcal{O}_\mathcal{K})$ via the Artin map, and hence $[\mathcal{H}^+ : \mathcal{K}] = h^+_{\mathcal{O}_\mathcal{K}} = \chi \cdot h_{\mathcal{O}_\mathcal{K}}$.*

Proof. See Theorem (14.7) in [6]. □

Theorem 3.4.6. *The extension $\mathcal{H}^+/\mathcal{K}$ is unramified at every prime $\mathfrak{p}$ in $\mathcal{O}_\mathcal{K}$.*

Proof. See Proposition (14.4) in [6]. □

Theorem 3.4.7. *$\mathcal{H}^+/\mathcal{H}$ is a Kummer extension of degree χ.*

Proof. See Proposition 15.4 in [6]. □

Let sgn be a sign function associated to the uniformizer $\pi = \frac{x^g}{y}$ and let ρ be a rank-one sgn-normalized $\mathcal{O}_\mathcal{K}$-Drinfeld module. Then $\rho_x = x + a_1\tau + a_2\tau^2$ for some a_1, a_2. Thus, the normalizing field $\mathcal{H}^+$ can be written simply as $\mathcal{K}(a_1, a_2)$. As explained in [6, Section 15], $\mathcal{K}\mathbb{F}_{\mathfrak{p}_\infty} \subset \mathcal{H}$. Since $a_2 \in \mathbb{F}_{\mathfrak{p}_\infty}$, it follows that $a_2 \in \mathcal{H}$. On the other hand, by Theorem (3.1.5), $\mathcal{H} = \mathcal{K}(j)$. Thus, $\mathcal{H}^+ = \mathcal{H}(a_1)$ and $\mathrm{irr}(a_1, \mathcal{H}) = X^\chi - a_1^\chi$. In particular, if $\deg n$ is odd, then $\chi = 1$ and $\mathcal{H}^+ = \mathcal{H}$. Otherwise, $\chi = q+1$ and $\mathcal{H}^+/\mathcal{H}$ is a non-trivial Kummer extension of degree $q+1$ generated by a_1.

Chapter 4
Representation Problem

4.1 Some Special Cases

Let $n \in \mathcal{Z}$ be a square-free polynomial of degree d with the leading coefficient n_d such that the form $X^2 + nY^2$ is anisotropic over $\mathcal{R}$. By Theorem (1.5.4), this is equivalent with the condition that d is odd or $-n_d$ is not a square in $\mathbb{F}$. The form $X^2 + nY^2$ is the norm of the field $\mathcal{K} = \mathcal{Q}(\sqrt{-n})$ over $\mathcal{Q}$. In this final chapter, we will discuss the following representation problem:

When can a prime element of $\mathcal{Z}$ be represented by the form $X^2 + nY^2$?

Since the form $X^2 + nY^2$, viewed as a function on K, is multiplicative, it is natural to expect that the ideal theory of the ring $\mathcal{O}_K$ will be a useful tool in the investigation of this problem. More specifically, we will see in Proposition (4.1.5) that if a prime $p \nmid n$ can be represented by $X^2 + nY^2$, then $p\mathcal{O}_\mathcal{K} = \mathfrak{p}\overline{\mathfrak{p}}, \mathfrak{p} \neq \overline{\mathfrak{p}}$, and $\mathfrak{p}$ is principal in $\mathcal{O}_\mathcal{K}$. Unfortunately, the converse is not quite true. If $\mathfrak{p} = (a+\sqrt{-n}b)\mathcal{O}_\mathcal{K}$ and $p\mathcal{O}_\mathcal{K} = \mathfrak{p}\overline{\mathfrak{p}}$, then $p\mathcal{O}_\mathcal{K} = (a^2 + nb^2)\mathcal{O}_\mathcal{K}$, which follows that $a^2 + nb^2 = up$ for some $u \in \mathcal{Z}^*$. Since the ring $\mathcal{Z}$ has $q - 1$ units, we are led to consider a notion of *weak representability.*

Definition 4.1.1. Let p be a prime element of $\mathcal{Z}$. We say that p can be represented by the form $X^2 + nY^2$ over $\mathcal{Z}$ if there are $a, b \in \mathcal{Z}$ such that $p = a^2 + nb^2$. We say that p can be *weakly represented* by the form $X^2 + nY^2$ if there is $u \in \mathbb{F}^*$ such that up can be represented by this form.

Observe that if p can be represented by the form $X^2 + nY^2$ over $\mathcal{Z}$, then up also can be represented for this form for every square in $\mathbb{F}$. In other words, if p is a monic prime that can be weakly represented, then the set of all elements $u \in \mathbb{F}^*$ such that up can be represented is either the whole group $\mathbb{F}^*$ or a coset of the subgroup $(\mathbb{F}^*)^2$ in $\mathbb{F}^*$. We will see soon that the former holds if and only if n is a constant, which makes weak representability a non-trivial concept. If d is odd, a representative of this coset can be found easily as shown in Lemma (4.1.3). However, if d is even, the problem is much more delicate. We will show in section 4.5 that both for an even and odd d a representative of this coset depends on the decomposition of p in the normalizing field $\mathcal{H}^+$.

Proposition 4.1.2. *Suppose that* $\deg n = 0$. *If* $p \in \mathcal{Z}$ *is a prime that can be weakly represented by the form* $X^2 + nY^2$, *then* p *can be represented by this form.*

Proof. Let $u \in \mathbb{F}^*$ be a constant such that up can be represented by X^2+nY^2. Since this form is multiplicative, it is enough to show that u^{-1} can be represented by it. Let $f_1, f_2 : \mathbb{F} \to \mathbb{F}$ be functions defined by $f_1(X) = u^{-1} - X^2$ and $f_2(Y) = nY^2$. Since $|f_1(\mathbb{F})| = |f_2(\mathbb{F})| = \frac{q+1}{2}$, it follows that $f_1(\mathbb{F}) \cap f_2(\mathbb{F}) \neq \varnothing$, which implies that u^{-1} can be represented by $X^2 + nY^2$. □

Lemma 4.1.3. *Assume that* d *is odd and* p *is a monic prime that can be weakly represented by the form* $X^2 + nY^2$. *If* $\deg p$ *is even, then* p *can be represented by the form* $X^2 + nY^2$. *Otherwise,* $n_d p$ *can be represented by the form* $X^2 + nY^2$.

Proof. Let $u \in \mathbb{F}^*$ and suppose that $up = a^2 + nb^2$ for some $a, b \in \mathcal{Z}$. Let a_k, b_l denote the leading coefficients of a, b respectively. If the degree of p is even, it follows from Lemma (1.5.8) that $u = a_k^2$. Set $A = a_k^{-1}a$ and $B = a_k^{-1}b$. Then $p = A^2 + nB^2$. If the degree of p is odd, it follows that $u = n_d b_l^2$. Set $A = b_l^{-1}a$ and $B = b_l^{-1}b$. Then $n_d p = A^2 + nB^2$. □

Proposition 4.1.4. *Let p be a prime element of $\mathcal{Z}$ that does not divide n. The prime p can be weakly represented by the form $X^2 + nY^2$ over $\mathcal{Z}$ if and only if $p\mathcal{O}_{\mathcal{K}} = \mathfrak{p}\overline{\mathfrak{p}}, \mathfrak{p} \neq \overline{\mathfrak{p}}$, and $\mathfrak{p}$ is principal in $\mathcal{O}_{\mathcal{K}}$.*

Proof. If $up = a^2 + nb^2$, set $\mathfrak{p} = (a + b\sqrt{-n})\mathcal{O}_{\mathcal{K}}$. Then $\overline{\mathfrak{p}} = (a - b\sqrt{-n})\mathcal{O}_{\mathcal{K}}$ and clearly $p\mathcal{O}_{\mathcal{K}} = \mathfrak{p}\overline{\mathfrak{p}}$. Since $n\mathcal{Z}$ is the discriminant of $\mathcal{O}_{\mathcal{K}}|\mathcal{Z}$ and p does not divide n, it follows that p is unramified in $\mathcal{K}$. In particular, we must have $\mathfrak{p} \neq \overline{\mathfrak{p}}$.

Now, suppose that $p\mathcal{O}_{\mathcal{K}} = \mathfrak{p}\overline{\mathfrak{p}}$, $\mathfrak{p} \neq \overline{\mathfrak{p}}$, and $\mathfrak{p}$ is principal in $\mathcal{O}_{\mathcal{K}}$. Since $\mathcal{O}_{\mathcal{K}} = \mathcal{Z}[\sqrt{-n}]$, we have $\mathfrak{p} = (a+b\sqrt{-n})\mathcal{O}_{\mathcal{K}}$ for some $a, b \in \mathcal{Z}$. Thus, $p\mathcal{O}_{\mathcal{K}} = (a^2+nb^2)\mathcal{O}_{\mathcal{K}}$. Intersecting both sides of this equality with $\mathcal{Z}$, we get $p\mathcal{Z} = (a^2+nb^2)\mathcal{Z}$ and hence $up = a^2 + nb^2$ for some $u \in \mathbb{F}^*$. □

The following corollary provides a very simple condition for weak representability in the case when $\mathcal{O}_{\mathcal{K}}$ is a principal ideal domain. However, its applicability is somehow restricted because as we have seen in Proposition (1.5.11) that it happens if and only if $d \leq 1$ or $n = x^3 + 2x + 2 \in \mathbb{F}_3[x]$ or $n = 2x^3 + x + 2 \in \mathbb{F}_3[x]$.

Corollary 4.1.5. *If $\mathcal{O}_{\mathcal{K}}$ is a principal ideal domain and p does not divide n, then p can be weakly represented by $X^2 + nY^2$ if and only if $(\frac{-n}{p}) = 1$.*

Proof. By Proposition (4.1.4), p can be weakly represented if and only if $p\mathcal{O}_{\mathcal{K}}$ splits. The ideal $p\mathcal{O}_{\mathcal{K}}$ splits if and only if the polynomial $X^2 + n$ splits over $\mathcal{Z}/p\mathcal{Z}$, which in turn is equivalent with $(\frac{-n}{p}) = 1$. □

We will finish this section with several examples in which Corollary (4.1.5) can be applied effectively.

Theorem 4.1.6. *Suppose that $\deg n = 0$ and $p \in \mathcal{Z}$ is irreducible.Then p can be represented by $X^2 + nY^2$ if and only if the degree of p is even.*

Proof. By Lemma (1.5.8), only polynomials of even degree can be represented by X^2+nY^2. For a prime p of even degree, we have $\left(\frac{-n}{p}\right) = 1$, so by Corollary (4.1.5), p can be weakly represented by this form. Proposition (4.1.2) implies that p itself can be represented by $X^2 + nY^2$. □

Example 4.1.7. Let $q = 3$ and $p \in \mathcal{Z}$ be a prime different from x. Then p can be represented by the form $X^2 + xY^2$ if and only if p is monic and $p(0) = 1$.

Proof. Since the degree of x is odd, the form $X^2 + xY^2$ is anisotropic. Set $\mathcal{K} = \mathcal{Q}(\sqrt{-x})$. By Proposition (1.5.11), $\mathcal{O}_{\mathcal{K}}$ is a principal ideal domain. Consequently, by Corollary (4.1.5), p can be weakly represented if and only if $1 = \left(\frac{-x}{p}\right)$. Let p_m be the leading coefficient of p. Using the quadratic reciprocity, we get

$$1 = \left(\frac{-x}{p}\right) = \left(\frac{p}{-x}\right) p_m^{-1} = \left(\frac{p(0)}{-x}\right) p_m^{-1} = \frac{p(0)}{p_m}.$$

The result follows from Lemma (4.1.3). □

Example 4.1.8. Let $q = 3$ and $p \in \mathcal{Z}$ be a prime polynomial of degree m with the leading coefficient p_m. If $p \neq 2x^3 + x + 2$, then p can be represented by the form $X^2 + (2x^3 + x + 2)Y^2$ if and only if p is a square modulo $2x^3 + x + 2$ and $p_m = (-1)^m$.

Proof. The degree of $2x^3 + x + 2$ is odd, so the form $X^2 + (2x^3 + x + 2)Y^2$ is anisotropic. Set $\mathcal{K} = \mathcal{Q}(\sqrt{x^3 + 2x + 1})$. By Proposition (1.5.11), $\mathcal{O}_{\mathcal{K}}$ is a principal ideal domain. Suppose that p is monic. By Corollary (4.1.5), p can be weakly represented if and only if $1 = \left(\frac{x^3+2x+1}{p}\right)$. Using the quadratic reciprocity, we get

$$1 = \left(\frac{x^3 + 2x + 1}{p}\right) = \left(\frac{p}{x^3 + 2x + 1}\right) (-1)^m.$$

Combining this condition with Lemma (4.1.3) and the fact that $\left(\frac{2}{x^3+2x+1}\right) = (-1)^m$, we obtain the result. □

4.2 The General Case

In the previous section, we have obtained a complete solution of the representation problem for n of degree zero. The simplicity of the presented solution and the obtained criterium is a consequence of Proposition (1.5.11) and the fact that in that case weak representability implies the actual representability. If the degree of n is positive, the ring $\mathcal{O}_{\mathcal{K}}$ typically is not a principal ideal domain as shown in Proposition (1.5.11). The following lemma shows that a prime which can be weakly represented by the form $X^2 + nY^2$ does not need necessarily to be representable by this form.

Lemma 4.2.1. *Suppose that $p \in \mathcal{Z}$ is irreducible and $u \in \mathbb{F}^*$. If both p and $u \cdot p$ can be represented by the form $X^2 + nY^2$, then u is a square in $\mathbb{F}$.*

Proof. Suppose that $p = N(\alpha)$ and $u \cdot p = N(\beta)$ for some α, $\beta \in \mathcal{O}_{\mathcal{K}}$. Then

$$p\mathcal{O}_{\mathcal{K}} = \alpha\mathcal{O}_{\mathcal{K}} \cdot \overline{\alpha}\mathcal{O}_{\mathcal{K}}$$

and

$$p\mathcal{O}_{\mathcal{K}} = (u \cdot p)\mathcal{O}_{\mathcal{K}} = \beta\mathcal{O}_{\mathcal{K}} \cdot \overline{\beta}\mathcal{O}_{\mathcal{K}}.$$

Clearly, none of the ideals on the left-hand side of these equalities equals $\mathcal{O}_{\mathcal{K}}$. Since there are at most two primes of $\mathcal{O}_{\mathcal{K}}$ lying above $p\mathcal{Z}$, it follows that $\alpha\mathcal{O}_{\mathcal{K}}$, $\overline{\alpha}\mathcal{O}_{\mathcal{K}}$, $\beta\mathcal{O}_{\mathcal{K}}$, $\overline{\beta}\mathcal{O}_{\mathcal{K}}$ are prime and the uniqueness of the prime factorization implies that $\alpha\mathcal{O}_{\mathcal{K}} = \beta\mathcal{O}_{\mathcal{K}}$ or $\alpha\mathcal{O}_{\mathcal{K}} = \overline{\beta}\mathcal{O}_{\mathcal{K}}$. Replacing β with $\overline{\beta}$ if needed, we may assume that $\alpha\mathcal{O}_{\mathcal{K}} = \beta\mathcal{O}_{\mathcal{K}}$, which follows that $\beta = w\alpha$ for some $w \in \mathcal{O}_{\mathcal{K}}^*$. By Proposition (1.5.9), $\mathcal{O}_{\mathcal{K}}^* = \mathbb{F}^*$, which gives

$$u \cdot p = N(\beta) = N(w\alpha) = w^2 N(\alpha) = w^2 p.$$

Hence u is a square in $\mathbb{F}$. □

By Proposition (4.1.4), a prime $p \nmid n$ can be weakly represented by the form $X^2 + nY^2$ if and only if $p\mathcal{O}_\mathcal{K}$ splits completely into a product of principal ideals. Thus, the first step in solving the representation problem is find when it happens. The answer is provided by the Hilbert class field theory presented in the previous chapter.

Lemma 4.2.2. *A prime ideal $\mathfrak{p}$ of $\mathcal{O}_\mathcal{K}$ is principal if and only if $\mathfrak{p}$ splits completely in $\mathcal{H}$.*

Proof. An ideal $\mathfrak{p}$ is principal if and only if $[\mathfrak{p}]$ is the identity element in $Cl(\mathcal{O}_\mathcal{K}) \simeq \mathrm{Gal}(\mathcal{H}/\mathcal{K})$, which in turn, by part (c) of Corollary (3.1.2), happens precisely when $\mathfrak{p}$ splits completely in $\mathcal{H}$. □

Applying Galois theory to prime decomposition, we obtain the following criterion for weak representability.

Proposition 4.2.3. *Let p be an irreducible element of $\mathcal{Z}$ that does not divide n. The prime p can be weakly represented by the form $X^2 + nY^2$ over $\mathcal{Z}$ if and only if p splits completely in $\mathcal{H}$.*

Proof. By Proposition (4.1.4), p can be weakly represented by the form $X^2 + nY^2$ over $\mathcal{Z}$ if and only if it splits completely in $\mathcal{K}$ and the primes above it are principal. By Lemma (4.2.2), a prime of $\mathcal{O}_\mathcal{K}$ is principal if and only if it splits completely in $\mathcal{H}$, so p can be represented by the form $X^2 + nY^2$ if and only if it splits completely in $\mathcal{K}$ and the primes above it split completely in $\mathcal{H}$. By Lemma 2.3 in [9], $\mathcal{H}$ is Galois over $\mathcal{Q}$, so the last condition is equivalent to p splitting completely in $\mathcal{H}$. □

Let $\mathcal{S}$ be a set of monic primes in $\mathcal{Z}$. Recall that the *Dirichlet density* of $\mathcal{S}$, denoted by $\delta(\mathcal{S})$ is defined to be

$$\delta(\mathcal{S}) = \lim_{s \to 1^+} \frac{\sum_{p \in \mathcal{S}} |p|^{-s}}{\sum_{p \in \mathcal{Z}} |p|^{-s}}$$

if the limit exists.

Corollary 4.2.4. *The Dirichlet density of the set of monic primes p that can be weakly represented by the form $X^2 + nY^2$ equals $(2h_{\mathcal{O}_{\mathcal{K}}})^{-1}$. In particular, there are infinitely many primes that can be represented by the form $X^2 + nY^2$.*

Proof. Let $\mathcal{S}_{rep}$ be the set of monic primes p that can be weakly represented by the form $X^2 + nY^2$. By Proposition (4.2.3), $\mathcal{S}_{rep} \cup \{ p_\infty \}$ is precisely the set of primes that split completely in $\mathcal{H}$. Since $\mathcal{H}/\mathcal{Q}$ is a Galois extension of degree $2h_{\mathcal{O}_{\mathcal{K}}}$, it follows from Tchebotarev Density Theorem (see [8, Proposition 9.13]) that

$$\delta(\mathcal{S}_{rep}) = \delta(\mathcal{S}_{rep} \cup \{ p_\infty \}) = [\mathcal{H} : \mathcal{K}]^{-1} = (2h_{\mathcal{O}_{\mathcal{K}}})^{-1}.$$

□

We have seen in Chapter 3 that the Hilbert class field $\mathcal{H} = \mathcal{K}(j)$, where j is the j-invariant of $\mathcal{O}_{\mathcal{K}}$ and that the minimal polynomial f of j over $\mathcal{K}$ has actually coefficient in $\mathcal{Z}$. Consequently, the condition of p splitting completely in $\mathcal{H}$ can be expressed in terms of the factorization of f in the field $\mathcal{Z}/p$. This leads to the following theorem.

Theorem 4.2.5. *There exists a monic polynomial $f \in \mathcal{Z}[X]$ such that for every prime $p \in \mathcal{Z}$ that divides neither n nor the discriminant of f, p can be weakly represented by the form $X^2 + nY^2$ if and only if $(\frac{-n}{p}) = 1$ and the congruence $f(X) \equiv 0 \pmod{p}$ has a solution in $\mathcal{Z}$.*

Proof. Let f be the minimal polynomial f of $j = j(\mathcal{O}_{\mathcal{K}})$. Clearly, f is monic and by Corollary (3.1.6), $f \in \mathcal{Z}[X]$. Let $p \in \mathcal{Z}$ be a prime $p \in \mathcal{Z}$ that divides neither n nor the discriminant of f. It follows that f is separable modulo p. As we have seen in the proof of Proposition (4.2.3), p can be weakly represented by the form X^2+nY^2

if and only if p splits completely in $\mathcal{K}$ and the primes above it are principal. The ideal $p\mathcal{O}_{\mathcal{K}}$ splits if and only if the polynomial $X^2 + n$ splits over $\mathcal{Z}/p\mathcal{Z}$, which in turn is equivalent with $(\frac{-n}{p}) = 1$. Now, if p splits completely in $\mathcal{K}$ and $\mathfrak{p}$ lies above it, then $f(\mathfrak{p}|p) = 1$ and hence $\mathcal{O}_{\mathcal{K}}/\mathfrak{p} \simeq \mathcal{Z}/p$. Consequently, f is separable modulo $\mathfrak{p}$, which implies that $\mathfrak{p}$ splits completely in $\mathcal{H}$ if and only if the congruence $f(X) \equiv 0 \pmod{\mathfrak{p}}$ has a solution in $\mathcal{O}_{\mathcal{K}}$, which in turns is equivalent with solvability of $f(X) \equiv 0 \pmod{p}$ in $\mathcal{Z}$ by the virtue of the isomorphism $\mathcal{O}_{\mathcal{K}}/\mathfrak{p} \simeq \mathcal{Z}/p$. The result follows. □

Theorem (4.2.5) seems to solve the problem of weak representation provided that there exists a method to compute the polynomial f. In [3], D. Hayes and D.S. Dummit present an algorithm to compute the minimal polynomial of j in the case when $-n$ is a square-free monic polynomial of odd degree. In the following section, we extend this algorithm to deal with the cases when $-n$ is not monic or of even degree. If $g(X)$ denotes the output of the modified algorithm, then $g(X)$ equals either $f(X)$ or $f(X)f(-X)$. This is however sufficient for our purpose since $g(X)$ has a root modulo p if and only if $f(X)$ does.

4.3 The Algorithm

Let us recall several facts discussed in chapters 2 and 3. Every element of $\mathcal{K}_{\mathfrak{p}_\infty}$ can be represented uniquely as a Laurent series

$$x = \sum_{k=k_0}^{\infty} c_k \pi^k.$$

with coefficients in $\mathbb{F}_{\mathfrak{p}_\infty}$, where $\mathbb{F}_{\mathfrak{p}_\infty} = \mathcal{O}_{\mathfrak{p}_\infty}/\mathfrak{p}_\infty$ and π is a uniformizer at $\mathfrak{p}_\infty$. The associated sign function is a multiplicative map defined by $\mathrm{sgn}(x) = c_{k_0}$, where $c_{k_0} \neq 0$ is the leading coefficient of the Laurent series expansion. A twisted sign function is a function of the form $\sigma \circ \mathrm{sgn}$, where σ is an $\mathbb{F}_q$- automorphism of $\mathbb{F}_{\mathfrak{p}_\infty}$.

If the leading coefficient function μ_ρ of a module ρ happens to be a twisted sign function, then ρ is said to be sgn-normalized. If ρ is a sgn-normalized Drinfeld module and $a \in \mathcal{O}_{\mathcal{K}}$, then the *normalizing field* $\mathcal{H}^+$ is the field generated over $\mathcal{K}$ by the coefficients of ρ_a. It depends neither on the choice of the element a nor the module ρ. Moreover, the narrow class group $\mathrm{Cl}^+(\mathcal{O}_{\mathcal{K}})$ is isomorphic to the Galois group $G = \mathrm{Gal}(\mathcal{H}^+/\mathcal{K})$. If n of odd degree, then $\mathcal{H}^+$ is simply the Hilbert class field $\mathcal{H}$ and every isomorphism class of rank-one Drinfeld $\mathcal{O}_{\mathcal{K}}$-modules contains exactly one sgn-normalized representative. This corresponds to the case when $\mathfrak{p}_\infty$ is of degree 1. If the degree of n is even, then $\deg \mathfrak{p}_\infty = 2$ and $\mathcal{H}^+$ is an extension of $\mathcal{H}$ of degree $q+1$. Then every isomorphism class of rank-one Drinfeld $\mathcal{O}_{\mathcal{K}}$-modules contains $q+1$ sgn-normalized representatives. In any case, the significance of the sgn-normalization lies in the fact G acts transitively on the set of all sgn-normalized modules. Additionally, the sgn-function will useful in the discussion of strong representability.

In the following discussion, sgn-normalized refers to the sgn function is associated to the uniformizer $\pi = \frac{x^g}{y}$, where g is the genus of $\mathcal{K}$. Recall also that d_∞ denotes the degree of $\mathfrak{p}_\infty$. Every rank-one Drinfeld $\mathcal{O}_{\mathcal{K}}$-module ρ over $\mathcal{C}$ is determined completely by two polynomials

$$\rho_x = x + a_1\tau + a_2\tau^2 \tag{4.3.1}$$

$$\rho_y = y + b_1\tau + \cdots + b_d\tau^d \tag{4.3.2}$$

with coefficients in $\mathcal{C}$ such that

$$\rho_x\rho_y = \rho_y\rho_x. \tag{4.3.3}$$

As shown in Lemma (2.2.3), this commutative condition is also sufficient for polynomials ρ_x and ρ_y to define a rank-one Drinfeld $\mathcal{O}_{\mathcal{K}}$-module ρ over $\mathcal{C}$. The following computation is based on this fact.

If we write $a_0 = x$ and $b_0 = y$, then the equation (4.3.3) is equivalent with the system of $d+3$ equations:

$$\begin{gathered}
a_0 b_0 = b_0 a_0 \\
a_0 b_1 + a_1 b_0^q = b_0 a_1 + b_1 a_0^q \\
\vdots \\
\sum_{i=0}^{k} a_i b_{k-i}^{q^i} = \sum_{i=0}^{k} b_i a_{k-i}^{q^i} \\
\vdots \\
a_2 b_d^{q^2} = b_d a_2^{q^d}
\end{gathered}$$

The first equation is satisfied trivially and so is the last one if ρ is sgn-normalized since a_2, $b_d \in \mathbb{F}_{\mathfrak{p}_\infty}$ in such a case. Thus, we have $d+1$ equations with variables a_1, a_2, $b_1, \ldots, b_d$. The first $d-1$ equations define b_1, $b_2, \ldots, b_{d-1}$ recursively in terms of x, y, a_1, a_2

$$b_k = \sum_{i=1}^{k} \left(a_i b_{k-i}^{q^i} - a_i^{q^{k-i}} b_{k-i} \right) / (a_0^{q^k} - a_0). \tag{4.3.4}$$

By Proposition (3.3.6), $b_d = a_2^g$, so substituting these expressions into the last two equations, we obtain two polynomials P, Q with variables a_1, a_2 defined over the field $\mathcal{K}$. Now, if d is odd, then by (3.3.4), $a_2 = -n_d^{-1}$ and hence P, Q are in fact elements of $\mathcal{K}[a_1]$. In such a case, we define

$$\varphi = \gcd(P, Q) \in \mathcal{K}[a_1]. \tag{4.3.5}$$

If d is even, then by (3.3.6) $a_2 = \sqrt{-n_d^{-1}}$ or $a_2 = -\sqrt{-n_d^{-1}}$. In such a case, we define

$$\begin{aligned}
P^+ &= e\left(\sqrt{-n_d^{-1}}\right)(P) \\
Q^+ &= e\left(\sqrt{-n_d^{-1}}\right)(Q)
\end{aligned}$$

and

$$\begin{aligned}P^- &= e\left(-\sqrt{-n_d^{-1}}\right)(P)\\ Q^- &= e\left(-\sqrt{-n_d^{-1}}\right)(Q),\end{aligned}$$

where $e(\alpha)$ is an evaluation homomorphism defined by

$$e(\alpha)(S(a_1,a_2)) = S(a_1,\alpha).$$

Then just like in the odd case we define

$$\begin{aligned}\varphi^+ &= \gcd(P^+,Q^+) \in \mathcal{K}\left(\sqrt{-n_d^{-1}}\right)[a_1]\\ \varphi^- &= \gcd(P^-,Q^-) \in \mathcal{K}\left(\sqrt{-n_d^{-1}}\right)[a_1]\end{aligned}$$

Now, if $\sigma : \mathcal{K}(\sqrt{-n_d}) \to \mathcal{K}(\sqrt{-n_d})$ is the $\mathcal{K}$-automorphism of $\mathcal{K}(\sqrt{-n_d})$ defined by $\sigma(\sqrt{-n_d}) = -\sqrt{-n_d}$ and $\sigma^* : \mathcal{K}(\sqrt{-n_d})[a_1] \to \mathcal{K}(\sqrt{-n_d})[a_1]$ is the induced automorphism of polynomial rings, then it is easy to see that

$$e\left(-\sqrt{-n_d^{-1}}\right) = \sigma^* \circ e\left(\sqrt{-n_d^{-1}}\right).$$

Consequently, we have

$$\begin{aligned}\sigma^*(P^+) &= P^-\\ \sigma^*(Q^+) &= Q^-\\ \sigma^*(\varphi^+) &= \varphi^-,\end{aligned}$$

which in turns implies that

$$\varphi \overset{def}{=} \varphi^+\varphi^- \in \mathcal{K}[a_1]. \tag{4.3.6}$$

We see that if ρ is a sgn-normalized, rank-one, $\mathcal{O}_\mathcal{K}$-Drinfeld module, then a_1 is a root of φ. The converse is also true.

Proposition 4.3.1. *Let α be a root of φ. Set $a_1 = \alpha$ and $b_d = a_2^g$, where*

$$a_2 = \begin{cases} -n_d^{-1} & \text{if } d \text{ is odd,} \\ \sqrt{-n_d^{-1}} & \text{if } d \text{ is even and } \varphi^+(\alpha) = 0, \\ -\sqrt{-n_d^{-1}} & \text{if } d \text{ is even and } \varphi^+(\alpha) \neq 0. \end{cases}$$

If $b_1, b_2, \ldots, b_{d-1}$ are given via (4.3.4), then the rank-one $\mathcal{O}_{\mathcal{K}}$-Drinfeld module ρ defined by the equations (4.3.1) and (4.3.2) is sgn-normalized.

Proof. Suppose that the module ρ is not sgn-normalized. Then there is an isomorphic module $v\rho v^{-1}$ which is sgn-normalized. Since the leading coefficient function is determined uniquely by $a_2(v\rho v^{-1})$, d must be even and

$$a_2(v\rho v^{-1}) = -a_2(\rho).$$

On the other hand,

$$a_2(v\rho v^{-1}) = v^{1-q^2} a_2(\rho),$$

which gives

$$v^{q^2-1} = -1. \tag{4.3.7}$$

We also have

$$v^{1-q^d} b_d(\rho) = b_d(v\rho v^{-1}) = a_2(v\rho v^{-1})^g = (v^{1-q^2})^g a_2(\rho)^g,$$

which gives

$$(v^{q^2-1})^g = v^{q^d-1}.$$

Combining this equality with (4.3.7), we get

$$(-1)^g = (-1)^{\frac{q^d-1}{q^2-1}},$$

which in turns implies

$$\frac{q^d-1}{q^2-1} \equiv g \pmod 2. \tag{4.3.8}$$

If $d = 2k$, then $g = \frac{d}{2} - 1 = k - 1$ and

$$\frac{q^d - 1}{q^2 - 1} = \frac{q^{2k} - 1}{q^2 - 1} = \sum_{i=0}^{k-1} q^{2i} \equiv k \pmod 2,$$

which contradicts (4.3.8). □

Remark 4.3.2. Since $\deg \varphi^+ = \deg \varphi^- > 0$, the above argument proves also that for an even d, there are sgn-normalized $\mathcal{O}_{\mathcal{K}}$-Drinfeld modules both with $a_2 = \sqrt{-n_d^{-1}}$ and with $a_2 = -\sqrt{-n_d^{-1}}$.

Theorem 4.3.3. *The polynomial φ defined by (4.3.5) or (4.3.6) is a power of the minimal polynomial of a_1 over $\mathcal{K}$.*

Proof. Let $R = \{\alpha_1, \alpha_2, \dots, \alpha_t\}$ be the set of roots of φ and let $m(X) = (X - \alpha_1)(X - \alpha_2)\dots(X - \alpha_t)$. The Galois group $G = \mathrm{Gal}(\mathcal{H}^+/\mathcal{K})$ acts transitively on the set of sgn-normalized $\mathcal{O}_{\mathcal{K}}$-Drinfeld modules of rank-one and hence it also acts transitively on the set R. Thus, if $\sigma \in G$, then $\sigma(R) = R$ and hence $\sigma m = m$. Combining this with the fact that $\mathcal{H}^+/\mathcal{K}$ is a Galois extension, we conclude that $m(X) \in \mathcal{K}[X]$, which in turns implies that $\mathrm{irr}(a_1, \mathcal{K}) \,|\, m$. On the other hand, transitivity of the action of G on R implies that α_i is a root of $\mathrm{irr}(a_1, \mathcal{K})$ for all i and hence $\mathrm{irr}(a_1, \mathcal{K}) = m$. Let

$$\varphi = (X - \alpha_1)^{e_1}(X - \alpha_2)^{e_2}\dots(X - \alpha_t)^{e_t}.$$

and choose $\sigma \in G$ so that $\sigma(\alpha_1) = \alpha_i$. Since $\sigma\varphi = \varphi$ and σ permutes the roots of φ, it follows that $e_1 = e_i$. Consequently, $\varphi = m^{e_1}$. □

Once φ is computed, it can be used to find a polynomial f with the required property. First, we compute $\mathrm{irr}(a_1^{q+1}, \mathcal{K})$ as follows. Let $A = C(\varphi)$ be the companion matrix of φ. Then φ is the characteristic polynomial of A and m is the minimal polynomial of A. Consequently,

$$\mathcal{K}(a_1) \simeq \mathcal{K}(A) \hookrightarrow M(\mathcal{K}),$$

which follows that $\mathrm{irr}(a_1^{q+1}, K) = \mathrm{irr}(A^{q+1}, K)$. The minimal polynomial of A^{q+1} is known to be the invariant factor of A^{q+1} of the highest degree. The invariant factors of A^{q+1} are the non-constant diagonal entries of a Smith normal form of $X\mathbb{I} - A^{q+1}$ over $\mathcal{K}[X]$, which can be found using Gaussian elimination. Now, let $r = \mathrm{irr}(a_1^{q+1}, \mathcal{K})$, $f = \mathrm{irr}(j, \mathcal{K})$, and $h = h_{\mathcal{O}_\mathcal{K}}$. If d is odd, then $j = -n_d a_1^{q+1}$ and hence we can set $g(X) = f(X) = (-n_d)^h r(\frac{X}{-n_d})$. If d is even, then $j = \sqrt{-n_d} a_1^{q+1}$ and $h = 2h_\mathcal{K}$. Additionally, it follows from [6, Section 15] that $\sqrt{-n_d} \in \mathcal{H}$. Consequently, $\mathcal{K}(a_1^{q+1})$ is a subfield of $\mathcal{H}$ of degree at most 2. Define

$$g(X) = (\sqrt{-n_d})^{2h} \cdot r\left((\sqrt{-n_d})^{-1} X\right) \cdot r\left((-\sqrt{-n_d})^{-1} X\right).$$

Since g is invariant under the action of the conjugation $\sigma : \mathcal{K}(\sqrt{-n_d}) \to \mathcal{K}(\sqrt{-n_d})$, it follows that g has coefficients in $\mathcal{K}$. Moreover, both j and $-j$ are the roots of g. If $[\mathcal{H} : \mathcal{K}(a_1^{q+1})] = 2$, then $\deg g = h$ and hence $g = n_d^{h_\mathcal{K}} \cdot f$. If $[\mathcal{H} : \mathcal{K}(a_1^{q+1})] = 1$ and j and $-j$ are conjugates over $\mathcal{K}$, then $f(X) = \mathrm{irr}(-j, \mathcal{K})$. On the other hand, since h is even, it follows that $f(-X) = \mathrm{irr}(-j, \mathcal{K})$. Thus, $f(X) = f(-X)$, which in turns implies that $f(X)$ consists only of even powers of X. Consequently, if $\widetilde{f}(X) = (\sqrt{-n_d})^{-h} \cdot f(\sqrt{-n_d} X)$, then $\widetilde{f}$ is a monic polynomial of degree h with coefficients in $\mathcal{K}$ such that $\widetilde{f}(a_1^{q+1}) = 0$. Thus, $\widetilde{f} = r$, which in turns implies that

$$f(X) = (\sqrt{-n_d})^h \cdot r\left(\frac{X}{\sqrt{-n_d}}\right).$$

Moreover, it follows that r also consists only of even powers of X. Consequently,

$$g(X) = (\sqrt{-n_d})^{2h} \cdot r\left((\sqrt{-n_d})^{-1} X\right) \cdot r\left((-\sqrt{-n_d})^{-1} X\right) = f(X) \cdot f(-X).$$

If j and $-j$ are not conjugates, then $g(X) = \text{irr}(j, \mathcal{K}) \cdot \text{irr}(-j, \mathcal{K}) = f(X) \cdot f(-X)$ since the polynomials on the right-hand side are distinct, monic, irreducible polynomials dividing g and both sides are monic of the same degree.

Example 4.3.4. Let $q = 3$ and $n = x^2 + 2x$. Computation of the polynomial φ using Magma Computational Algebra System [1] resulted in

$$\varphi = X^8 + (y^9 + y^7 - y^5)X^4 + y^8.$$

By Proposition (1.5.10), the genus of $\mathcal{K} = \mathcal{Q}(\sqrt{-n})$ is 0. Consequently, $h_{\mathcal{K}} = 1$ by the virtue of Corollary (1.3.7). Since $\mathcal{H}^+$ is a Kummer extension of $\mathcal{H}$ of degree 4, it follows that $[\mathcal{H}^+ : \mathcal{K}] = 4 \cdot [\mathcal{H} : \mathcal{K}] = 4 \cdot h_{\mathcal{O}_{\mathcal{K}}} = 8$, which in turns implies that $\varphi = \text{irr}(a_1, \mathcal{K})$. Since a_1 is a root of φ, it follows that a_1^4 is a root of

$$\chi = X^2 + (y^9 + y^7 - y^5)X + y^8.$$

Note that χ must be irreducible over $\mathcal{K}$ otherwise we would have $a_1^4 = \alpha$ for some $\alpha \in \mathcal{K}$. But then we would get $\varphi \mid X^8 - \alpha^2$ which is impossible. Consequently, $\chi = \text{irr}(a_1^4, \mathcal{K})$. Thus, the output of the algorithm $g(X)$ equals

$$(\sqrt{-1})^{2h} \cdot \chi(\sqrt{-1} \cdot X)\chi(-\sqrt{-1} \cdot X) = X^4 + d_1X^2 + d_0,$$

where

$$d_1 = 2x^{18} + 2x^{16} + 2x^{15} + x^{13} + 2x^7 + 2x^6 + x^4$$

and

$$d_0 = x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8.$$

The discriminant D of g equals

$$x^{26}(x+1)^4(x+2)^{26}(x^2+1)^4(x^2+x+2)^4(x^4+x^3+x^2+1)^4. \tag{4.3.9}$$

Assuming that a prime polynomial $p \in \mathcal{Z}$ does not divide D, we obtain that p can be weakly represented by the form $X^2 + (x^2 + 2x)Y^2$ if and only if $2x^2 + x$ is a quadratic residue modulo p and the congruence $X^4 + d_1X^2 + d_0 \equiv 0 \pmod p$ has a solution in $\mathcal{Z}$.

Example 4.3.5. Let $q = 3$ and $n = x^3 + x^2 + 1$. Computation of the polynomial φ using Magma Computational Algebra System [1] resulted in $\varphi = X^2 + c_1X + c_0$, where $c_1, c_0 \in \mathcal{K}$ are given by $c_0 = x^6 + 2x^5 + x^3 + 2x^2$ and $c_1 = (x^3 + x^2)y$. Since a_1 is a root of φ, simple computation shows it is a root of $(X^4 + c_0^2)^2 - (c_1 - 2c_0)^2X^4$ as well. We have

$$(X^4 + c_0^2)^2 - (c_1 - 2c_0)^2X^4 = X^8 + d_1X^4 + d_0,$$

where $d_1, d_0 \in \mathcal{Z}$ are given by

$$d_0 = x^{24} + 2x^{23} + 2x^{18} + x^{17} + x^{15} + 2x^{14} + 2x^9 + x^8$$

and

$$d_1 = 2x^{18} + x^{15} + x^{13} + x^8 + 2x^6 + x^5 + x^4.$$

Consequently, $j = -n_2a_1^4 = -a_1^4$ is a root of $f = X^2 - d_1X + d_0$. The discriminant $\Delta = d_1^2 - d_0$ of this polynomial equals $x^{10} \cdot \delta$, where

$$\delta = x^{26}+x^{23}+x^{21}+x^{20}-x^{18}-x^{16}+x^{14}+x^{13}+x^{12}-x^{10}+x^7+x^6+2x^5-x^4-x^3+x-1.$$

Since the constant term of δ is not a square in $\mathbb{F}_3$, it follows that Δ is not a square in $\mathcal{Z}$, which in turns implies that $f = \operatorname{irr}(j, \mathcal{Q})$. Assuming that a prime polynomial $p \in \mathcal{Z}$ divides neither n nor Δ, we obtain that p can be weakly represented by the form $X^2 + (x^3 + x^2 + 1)Y^2$ if and only if $2x^3 + 2x^2 + 2$ is a quadratic residue modulo p and the congruence $X^2 + d_1X + d_0 \equiv 0 \pmod p$ has solution in $\mathcal{Z}$. Note that this congruence is solvable over $\mathcal{Z}$ if and only if $(\frac{\delta}{p}) = 1$. Thus, by the virtue of the quadratic reciprocity law, the weak representability criterion can be expressed using only linear congruences. Finally, by Lemma (4.1.3), only monic primes p can be represented by the form $X^2 + nY^2$.

Example 4.3.6. Let $q = 3$ and $n = x^4 + x + 1$. Computation of the polynomial φ using Magma Computational Algebra System [1] resulted in $\varphi = X^8 + c_1X^4 + c_0$, where $c_1, c_0 \in \mathcal{K}$ are given by

$$\begin{aligned} c_1 = (2x^{25} + 2x^{22} + 2x^{21} + x^{19} + x^{17} + 2x^{15} \\ + x^{14} + x^{12} + 2x^{11} + x^7 + x^5 + 2x^4) \cdot y \end{aligned}$$

and

$$\begin{aligned} c_0 = x^{36} + 2x^{34} + 2x^{33} + x^{32} + x^{31} + x^{30} \\ + x^{28} + 2x^{26} + 2x^{23} + x^{22} + x^{21} + x^{20} \\ + x^{17} + 2x^{16} + 2x^{14} + 2x^{13} + x^{12} \end{aligned}$$

Since a_1 is a root of φ, it follows that a_1^4 is a root of $\chi = X^2 + c_1X + c_0$. The discriminant $c_1^2 - c_0$ of χ is an element of $\mathcal{Z}$ with the leading coefficient 2, which follows that χ is irreducible over $\mathcal{K}$. Consequently, $\chi = \text{irr}(a_1^4, \mathcal{K})$. Thus, the output of the algorithm $g(X)$ equals

$$(\sqrt{-1})^{2h} \cdot \chi(\sqrt{-1} \cdot X)\chi(-\sqrt{-1} \cdot X) = X^4 + d_1X^2 + d_0,$$

where $d_1, d_0 \in \mathcal{Z}$ are given by

$$\begin{aligned} d_1 = 2x^{54} + 2x^{48} + 2x^{46} + 2x^{44} + x^{42} + 2x^{41} + x^{39} + x^{38} + x^{36} + x^{35} + 2x^{33} \\ + 2x^{32} + x^{31} + x^{30} + 2x^{27} + x^{26} + x^{25} + x^{24} + 2x^{23} + x^{22} + x^{21} + x^{20} \\ + 2x^{19} + x^{18} + 2x^{16} + 2x^{15} + 2x^{13} + x^{11} + x^{10} + x^9 + 2x^8 \end{aligned}$$

and

$$\begin{aligned} d_0 = x^{72} + x^{70} + x^{69} + x^{67} + x^{66} + 2x^{65} + 2x^{64} + 2x^{62} + 2x^{60} + 2x^{59} + 2x^{58} + 2x^{57} \\ + x^{56} + 2x^{53} + 2x^{52} + 2x^{50} + x^{48} + 2x^{47} + x^{46} + x^{44} + x^{43} + 2x^{42} + x^{38} \\ + 2x^{37} + x^{36} + 2x^{34} + x^{33} + x^{31} + x^{29} + 2x^{28} + 2x^{27} + 2x^{26} + x^{25} + x^{24}. \end{aligned}$$

Assuming that a prime polynomial $p \in \mathcal{Z}$ divides neither n nor the discriminant of g, we obtain that p can be weakly represented by the form $X^2 + (x^4 + x + 1)Y^2$ if and only if $2x^4 + 2x + 2$ is a quadratic residue modulo p and the congruence $X^4 + d_1X^2 + d_0 \equiv 0 \pmod{p}$ has solution in $\mathcal{Z}$.

4.4 Strong Representability

Theorem (4.2.5) along with the presented algorithm solves the problem of weak representation. There is one question remaining. *Assuming that p can be weakly represented by the form $X^2 + nY^2$, when can p itself be represented by this form?* In this section, we will answer this question.

Let $p(X) \in \mathcal{Z}$ be an irreducible polynomial of degree k that does not divide n and can be weakly represented by the form $X^2 + nY^2$. Note that k must be even if $d = \deg n$ is even. Consequently, regardless on parity of d, the quotient $\frac{k}{d_\infty}$ is an integer. In order to simplify some statements, we will use the symbol $\deg^* p$ to denote this number. Now, observe that

$$p(x) = p_0 + p_1x + \cdots + p_kx^k = p_kx^k\hat{p}(x^{-1}),$$

where $\hat{p} \in \mathcal{Z}$ is a polynomial of degree k. By the virtue of the equation (3.3.3), we get

$$\operatorname{sgn}(p(x)) = p_k\operatorname{sgn}(x)^k\operatorname{sgn}(\hat{p}(x^{-1})) = p_k\operatorname{sgn}(\hat{p}(x^{-1}))(-n_d)^{-\deg^* p}$$

Since $\operatorname{ord}_{\mathfrak{p}_\infty}(\hat{p}(x^{-1})) = 0$ and $\operatorname{ord}_{\mathfrak{p}_\infty}(\hat{p}(x^{-1})-1) \geq 0$, it follows that $\hat{p}(x^{-1})$ is a unit in $\mathcal{O}_{\mathfrak{p}_\infty} \subset \mathcal{K}_{\mathfrak{p}_\infty}$ and $\hat{p}(x^{-1}) \equiv 1 \pmod{\mathfrak{p}_\infty}$, which in turns implies $\operatorname{sgn}(\hat{p}(x^{-1})) = 1$. Consequently, p is positive if and only if

$$p_k = (-n_d)^{\deg^* p}. \tag{4.4.1}$$

Lemma 4.4.1. *Let $a + by \in \mathcal{K}$ and $n_0 = \operatorname{ord}_{\mathfrak{p}_\infty}(a + by)$. Then*

$$\operatorname{sgn}(a - by) = (-1)^{n_0} \cdot \operatorname{sgn}(a + by).$$

Proof. The conjugation of $\mathcal{K}$ is a continuous map with respect to $|\cdot|_\infty$. Hence if

$$a + by = \sum_{n=n_0}^{\infty} c_n \pi^n,$$

then

$$a - by = \sum_{n=n_0}^{\infty} c_n (-1)^n \pi^n,$$

and the result follows. □

Proposition 4.4.2. *Let $p \nmid n$ be a positive prime that can be weakly represented by the form $X^2 + nY^2$ and let $\mathfrak{p} = (\alpha)$ be an ideal above p.Then p can be represented by the form if and only if α can be chosen so that $\operatorname{sgn}(\alpha)^2 = (-1)^{\deg^* p}$.*

Proof. Suppose that p can be represented. Then $p = \alpha\overline{\alpha}$ for some generator α of $\mathfrak{p}$. Then $\operatorname{ord}_{\mathfrak{p}_\infty}(\overline{\alpha}) = -\deg^* p$ and hence

$$1 = \operatorname{sgn}(p) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\overline{\alpha}) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\alpha)(-1)^{-\deg^* p}$$

and the result follows.

Now, assume that α can be chosen so that $\operatorname{sgn}(\alpha)^2 = (-1)^{\deg^* p}$. Since p can be weakly represented, we have $up = \alpha\overline{\alpha}$ and hence

$$\begin{aligned} u = \operatorname{sgn}(up) &= \operatorname{sgn}(\alpha)\operatorname{sgn}(\overline{\alpha}) \\ &= \operatorname{sgn}(\alpha)\operatorname{sgn}(\alpha)(-1)^{-\deg^* p} \\ &= (-1)^{\deg^* p}(-1)^{-\deg^* p} = 1. \end{aligned}$$

□

Theorem 4.4.3. *Let $p \nmid n$ be a positive prime that can be weakly represented by the form $X^2 + nY^2$. Suppose that* $\deg^* p$ *is even or* $4 \mid q - 1$. *Then p can be represented by the form $X^2 + nY^2$ if and only if it splits completely in $\mathcal{H}^+$.*

Proof. let $\mathfrak{p}$ be a prime in $\mathcal{O}_{\mathcal{K}}$ above p. Suppose that $\deg^* p$ is even. Then, by Proposition (4.4.2), p can be represented if and only if $\mathfrak{p}$ has a generator α such that $\operatorname{sgn}(\alpha)^2 = 1$. Since for any generator α of $\mathfrak{p}$, $-\alpha$ is also a generator, the last condition is equivalent with the existence of a positive generator α. Similarly, if $\deg^* p$ is odd, then we conclude from Proposition (4.4.2) that p can be represented if and only if $\mathfrak{p}$ has a generator α such that $\operatorname{sgn}(\alpha)^2 = -1$. Since $4 \mid q-1$, it follows that there is an $u \in \mathbb{F}^*$ such that $u^2 = -1$. Since for any generator α of $\mathfrak{p}$, both $-u\alpha$ and $u\alpha$ are generators as well, the last condition is also equivalent with the existence of a positive generator α, which in turns is equivalent with the equality $[\mathfrak{p}] = 1$ in $\mathrm{Cl}^+(\mathcal{O}_{\mathcal{K}}) \simeq \mathrm{Gal}(\mathcal{H}^+/\mathcal{K})$. By Corollary (3.1.2), we have $[\mathfrak{p}] = 1$ in $\mathrm{Cl}^+(\mathcal{O}_{\mathcal{K}})$ if and only if $\mathfrak{p}$ splits completely in $\mathcal{H}^+$. Since p splits in $\mathcal{K}$ and $\mathcal{H}^+/\mathcal{Q}$ is Galois, the result follows. □

Theorem 4.4.4. *Let $p \nmid n$ be a positive prime that can be weakly represented by the form $X^2 + nY^2$, and let $m(X) = \mathrm{irr}(a_1, \mathcal{K})$. Suppose that* $\deg^* p$ *is even or* $4 \mid q - 1$.

Let

$$\omega_p(X) = \gcd(X^{|p|} - X, m_p(X)) \in (\mathcal{Z}/p)[X], \tag{4.4.2}$$

where $m_p(X)$ is the reduction of $m(X)$ modulo p. Assume also that p is relatively prime to the discriminant of $m(X)$. Then, p can be represented by the form $X^2 + nY^2$ if and only if $\deg \omega_p(X) \geq 1$.

Proof. Let $\mathfrak{p}, \mathfrak{P}, \mathfrak{P}^+$ be primes in $\mathcal{O}_\mathcal{K}, \mathcal{O}_\mathcal{H}, \mathcal{O}_{\mathcal{H}^+}$ respectively such that $p \subset \mathfrak{p} \subset \mathfrak{P} \subset \mathfrak{P}^+$. We have seen in the proof of Theorem (4.4.3) that p can be represented by the form $X^2 + nY^2$ if and only if $\mathfrak{p}$ splits completely in $\mathcal{H}^+$. Since p can be weakly represented, it follows that $\mathfrak{p}$ splits completely in $\mathcal{H}$. In particular, $f(\mathfrak{P}|\,\mathfrak{p}) = e(\mathfrak{P}|\,\mathfrak{p}) = 1$ and $\kappa(\mathfrak{P}) = \kappa(\mathfrak{p})$. By Theorem (3.4.6), $\mathcal{H}^+$ is unramified at all primes in $\mathcal{O}_\mathcal{K}$. Thus, $\mathfrak{p}$ splits completely in $\mathcal{H}^+$ if and only if $f(\mathfrak{P}^+|\,\mathfrak{P}) = 1$. Since p is relatively prime to the discriminant of $m(X)$, so is $\mathfrak{P}$. Consequently, $\mathcal{H}^+ = \mathcal{H}(a_1)$ implies $\kappa(\mathfrak{P}^+) = \kappa(\mathfrak{P})(\overline{a_1}) = \kappa(\mathfrak{p})(\overline{a_1})$. On the other hand, $[\kappa(\mathfrak{P}^+) : \kappa(\mathfrak{P})] = f(\mathfrak{P}^+|\,\mathfrak{P})$. Thus, $f(\mathfrak{P}^+|\,\mathfrak{P}) = 1$ if and only if $\overline{a_1} \in \kappa(\mathfrak{p}) = \mathcal{Z}/p$, which in turn is equivalent with $m_p(X)$ having a root in $\mathcal{Z}/p$. Since elements of $\mathcal{Z}/p$ are precisely the roots of $X^{|p|} - X$, the result follows. □

Theorem 4.4.5. *Let $p \nmid n$ be a positive prime that can be weakly represented by the form $X^2 + nY^2$ and let $\mathfrak{P}^+$ be a prime in $\mathcal{H}^+$ above p. Suppose that* $\deg^* p$ *is odd and $4 \nmid q - 1$. Then p can be represented by the form $X^2 + nY^2$ if and only if $f(\mathfrak{P}^+|\,p) = 4$.*

Proof. Let $\mathfrak{p}$ be a prime in $\mathcal{O}_\mathcal{K}$ such that $p \subset \mathfrak{p} \subset \mathfrak{P}^+$. Since $4 \nmid q - 1$, it follows that -1 is not a square in $\mathbb{F}$. Consequently, Proposition (4.4.2) implies that p can be represented if and only if $[\mathfrak{p}]$ is an element of order 4 in $\mathrm{Cl}^+(\mathcal{O}_\mathcal{K}) \simeq \mathrm{Gal}(\mathcal{H}^+/\mathcal{K})$. The image of $[\mathfrak{p}]$ in $\mathrm{Gal}(\mathcal{H}^+/\mathcal{K})$ is the Artin symbol $\left(\frac{\mathcal{H}^+/\mathcal{K}}{\mathfrak{p}}\right)$. By Corollary (3.1.2), the order of this symbol is $f(\mathfrak{P}^+|\,p)$. The result follows. □

Theorem 4.4.6. *Let $p \nmid n$ be a positive prime that can be weakly represented by the form $X^2 + nY^2$, and let $m(X) = \operatorname{irr}(a_1, \mathcal{K})$. Suppose that $\deg^* p$ is odd and $4 \nmid q - 1$. Let*

$$\omega_p(X) = \gcd(X^{2|p|} + X^2, m_p(X)) \in (\mathcal{Z}/p)[X], \tag{4.4.3}$$

where $m_p(X)$ is the reduction of $m(X)$ modulo p. Assume also that p is relatively prime to the discriminant of $m(X)$. Then, p can be represented by the form $X^2 + nY^2$ if and only if $\deg \omega_p(X) \geq 1$.

Proof. Let $\mathfrak{p}, \mathfrak{P}, \mathfrak{P}^+$ be primes in $\mathcal{O}_{\mathcal{K}}, \mathcal{O}_{\mathcal{H}}, \mathcal{O}_{\mathcal{H}^+}$ respectively such that $p \subset \mathfrak{p} \subset \mathfrak{P} \subset \mathfrak{P}^+$. By Theorem (4.4.5), p can be represented if and only if $f(\mathfrak{P}^+ | \, p) = 4$. Since p is weakly represented, it splits completely in $\mathcal{H}$ and hence $f(\mathfrak{P}^+ | \, p) = f(\mathfrak{P}^+ | \, \mathfrak{P})$. Thus, p can be represented if and only if $[\kappa(\mathfrak{P}^+) : \kappa(\mathfrak{P})] = 4$. Since p is relatively prime to the discriminant of $m(X)$, so is $\mathfrak{P}$. Consequently, $\mathcal{H}^+ = \mathcal{H}(a_1)$ implies $\kappa(\mathfrak{P}^+) = \kappa(\mathfrak{P})(\overline{a_1}) = \kappa(\mathfrak{p})(\overline{a_1})$ and hence $[\kappa(\mathfrak{P}^+) : \kappa(\mathfrak{P})] = \deg \operatorname{irr}(\overline{a_1}, \kappa(\mathfrak{p}))$. Note that if $\deg n$ is odd, then $\mathcal{H}^+ = \mathcal{H}$ and hence $[\kappa(\mathfrak{P}^+) : \kappa(\mathfrak{P})] = 1$. On the other hand, $m_p(X)$ splits completely over $\mathcal{Z}/p$. It is easy to see that none of the elements of $\mathcal{Z}/p$ is a root of $X^{2|p|} + X^2$ and hence $\omega_p(X) = 1$, which completes the proof in this case. Thus, for the rest of the proof, we may assume that $\deg n$ is even.

Let $w(X) = \operatorname{irr}(\overline{a_1}, \kappa(\mathfrak{p}))$. Suppose that $\deg w(X) = 4$. By Theorem (3.4.7), $\mathcal{H}^+/\mathcal{H}$ is a Kummer extension of degree $q+1$ and hence $w(X) | X^{q+1} - \overline{a_1}^{q+1}$, which it follows that $w(X) = (X - \overline{a_1})(X - \overline{a_1}\xi_1)(X - \overline{a_1}\xi_2)(X - \overline{a_1}\xi_3)$, where ξ_i are roots of unity of order $q + 1$. Consequently, $\overline{a_1}^4 \xi_1 \xi_2 \xi_3 \in \kappa(\mathfrak{p})$. Note that $\kappa(\mathfrak{p})$ contains all roots of unity of order $q + 1$, and so $\overline{a_1}^4 \in \kappa(\mathfrak{p})$, which in turns implies that $w(X) = X^4 - \overline{a_1}^4$. Observe that $\overline{a_1}^2 \notin \kappa(\mathfrak{p})$ due to irreducibility of $w(X)$. Since p splits completely in $\mathcal{O}_{\mathcal{K}}$, we have $\kappa(\mathfrak{p}) = \mathcal{Z}/p$ and hence the cardinality of $\kappa(\mathfrak{p})$

equals the norm of p, which follows that $\overline{a_1}$ is a root of the polynomial

$$\frac{X^{4|p|}-X^4}{X^{2|p|}-X^2}=X^{2|p|}+X^2.$$

Thus, $\overline{a_1}$ is a root of

$$\omega_p(X)=\gcd\left(X^{2|p|}+X^2, m_p(X)\right). \tag{4.4.4}$$

In particular, $\omega_p(X)$ has a positive degree. Thus, if $[\kappa(\mathfrak{P}^+):\kappa(\mathfrak{p})]=4$, then $\deg\omega_p(X)\geq 1$. It is easy to see that the converse is also true. Indeed, suppose that $\deg\omega_p(X)\geq 1$ and let α be a root of ω_p. Since $m_p(\alpha)=0$, it follows that $\alpha=\overline{a_1}$ for some root a_1 of $m(X)$. Consequently, $\kappa(\mathfrak{P}^+)=\kappa(\mathfrak{P})(\alpha)=\kappa(\mathfrak{p})(\alpha)$. We also have $\alpha^{4|p|}=\alpha^4$ and $\alpha^{2|p|}\neq\alpha^2$, which shows that $\alpha^4\in\kappa(\mathfrak{p})$ but $\alpha^2\notin\kappa(\mathfrak{p})$. Thus, $X^4-\alpha^4$ is an irreducible polynomial of α over $\mathcal{K}$ and $[\kappa(\mathfrak{P}^+):\kappa(\mathfrak{p})]=4$. □

Example 4.4.7. We have learned in Example (4.3.4) that a prime polynomial $p\in\mathcal{Z}$ different from $x, x, (x+1), (x+2), (x^2+1), (x^2+x+2), (x^4+x^3+x^2+1)$ can be weakly represented by the form $X^2+(x^2+2x)Y^2$ if and only if $2x^2+x$ is a quadratic residue modulo p and the congruence $X^4+d_1X^2+d_0\equiv 0 \pmod{p}$, where

$$d_1=2x^{18}+2x^{16}+2x^{15}+x^{13}+2x^7+2x^6+x^4,$$

and

$$d_0=x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8,$$

has a solution in $\mathcal{Z}$. Let $p=2x^{10}+2x^7+x^4+2x^3+2x+1$. Then $\deg^{*}p=5$ and p is positive. Set also $u=x^9+2x^8+x^6+2x^5+x^4+2x^3+x+2$, and $v=x^9+x^8+x^7+x$. Then $u^2\equiv 2x^2+x \pmod{p}$ and $v^4+d_1v^2+d_0\equiv 0 \pmod{p}$, which follows that p can be weakly represented by the form $X^2+(x^2+2x)Y^2$. We will apply Theorem (4.4.6) to decide whether p can be actually represented by the form $X^2+(x^2+2x)Y^2$.

Recall that $\mathrm{irr}(a_1, \mathcal{K}) = X^8 + (y^9 + y^7 - y^5)X^4 + y^8$. Its discriminant equals

$$x^{28}(x+1)^8(x+2)^{28}(x^4+x^3+x^2+1)^8,$$

which is relatively prime to p. Using the fact that u is a square root of $-n$ modulo p, we can compute the reduction of $\mathrm{irr}(a_1, \mathcal{K})$ modulo p. We obtain

$$m_p(X) = X^8 + (2x^8 + x^7 + 2x^5 + 2x^4 + x^3 + x^2 + 2)X^4 + (x^8 + 2x^7 + 2x^5 + x^4).$$

Since $\deg p = 10$, it follows that $|p| = 3^{10} = 59049$. Thus,

$$\omega_p(X) = \gcd\left(X^{118098} + X^2, m_p(X)\right).$$

Using the division algorithm, we see that $m_p(X)|X^{118098} + X^2$ in $(\mathcal{Z}/p)[X]$ and hence $\deg \omega_p(X) \geq 1$. Thus, by Theorem (4.4.6), the polynomial p can be represented by the form $X^2 + (x^2 + 2x)Y^2$. Indeed, we have

$$p = (x^5 + 2x^4 + 2x^3 + x^2 + 2)^2 + (x^2 + 2x) \cdot (x^4 + 2x^2 + x + 1)^2.$$

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235-265, 1997

[2] David A. Cox, *Primes of the form $x^2 + ny^2$*, John Wiley & Sons, New York, 1989

[3] D. S. Dummit and David Hayes, *Rank-One Drinfeld Modules on Elliptic Curves*, Mathematics of Computation, Vol. 62, No. 206, (Apr., 1994), pp. 875-883, American Mathematical Society

[4] Ernst-Ulrich Gekeler, *Zur Arithmetik von Drinfeld-Moduln*, Math. Ann. 262 (1983), no. 2, 167-182.

[5] David Goss, *Basic structures of function field arithmetic*, Springer-Verlag, Berlin, 1996

[6] David R. Hayes, *A Brief Introduction to Drinfeld Modules*, The Arithmetic of function fields; Proceedings of the workshop at the Ohio State University, June 17-26, 1991, Pages 1-32, 1992

[7] David R. Hayes, *On the reduction of rank-one Drinfeld modules*, Math. Comp. 57 (1991), 339-349.

[8] Michael Rosen, *Number Theory in Function Fields*, Graduate Texts in Mathematics, vol 210, Springer-Verlag, New York, 2002

[9] Michael Rosen, *The Hilbert class field in function fields*, Expo. Math. 5 (1987), 365378.

Vita

Piotr Maciak was born in January 1980, in Szczecin, Poland. He earned a master of science degree in mathematics from Szczecin University in July 2003. In August 2004 he came to Louisiana State University to pursue graduate studies in mathematics. He is currently a candidate for the degree of Doctor of Philosophy in mathematics, which will be awarded in May 2010.