The Lang-Trotter conjecture for Drinfeld modules

by

David Tweedle

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Pure Mathematics

Waterloo, Ontario, Canada, 2011

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

In 1986, Gupta and Murty proved the Lang-Trotter conjecture in the case of elliptic curves having complex multiplication, conditional on the generalized Riemann hypothesis. That is, given a non-torsion point $P \in E(\mathbb{Q})$, they showed that $P \pmod{p}$ generates $E(\mathbb{F}_p)$ for infinitely many primes p, conditional on the generalized Riemann hypothesis. We demonstrate that Gupta and Murty's result can be translated into an unconditional result in the language of Drinfeld modules. We follow the example of Hsu and Yu, who proved Artin's conjecture unconditionally in the case of sign normalized rank one Drinfeld modules. Further, we will cover all necessary background information.

Acknowledgements

I would like to thank my lovely wife Kemba for her love, support and encouragement. I would like to thank my parents Terry and Bonnie Tweedle for all their help over the years. I would like to thank my supervisor, Professor Wentang Kuo, for his patience and guidance. I would like to thank Professors Yu-Ru Liu, Kevin Hare, David McKinnon for being helpful and wise. I would like to thank Jesse for being a good brother and friend. My thanks go to Professors Kumar Murty, David Jao and my entire committee for all their hard work and helpful comments on my thesis, your comments are greatly appreciated. Thank you to Mrs. Yvonne Thomas for welcoming me into your family and for your unending support. My thanks go to Mr. Enos Thomas for sharing his advice and experience with me. My thanks also to my aunts Karen and Donna, my uncle Frank, my cousins Kim, Kelly, Mark and Scott and my grandma Shirley.

Dedication

To Kemba!

Table of Contents

Nomenclature

$\delta_a, \delta_E(a), \delta_\phi(a), \delta_E(\Gamma), \delta_\phi(\Gamma)$	Densities of primes for Artin-like problems
Γ	A finitely generated torsion-free submodule of either $E(\mathbb{Q})$ or $\phi(F)$
∞	A fixed rational prime of F
$\mathbb{F}_r$	The finite field with r elements
τ	The r-power Frobenius map, $\tau(X) = X^r$
A	The ring of elements of F which are regular everywhere except possibly ∞
a	A non-torsion point of $E(\mathbb{Q})$ or $\phi(F)$
E	An elliptic curve defined over $\mathbb{Q}$
F	A function field, i.e. an extension of $\mathbb{F}_r$ having transcendence degree 1 over $\mathbb{F}_r$ with $F \cap \mathbb{F}_r = \mathbb{F}_r$
$F\{\tau\}$	The twisted polynomial ring $F\{\tau\}$
k	This refers to either a quadratic imaginary extension of $\mathbb{Q}$ or an extension of F where ∞ does not split
$K_m^a = \mathbb{Q}(a^{1/m}, \zeta_m), \mathbb{Q}(m^{-1}a, E[m])$	The particular extension we are talking about will be clear from context
$N_a(x), N_\Gamma(x), \tilde{N}_\Gamma(x)$	Prime counting functions for Artin-like problems
$P, \mathfrak{P}, \mathfrak{p}, \mathfrak{q}$	Finite primes in various function fields
p, q	Rational primes

Chapter 1

Introduction

1.1 Artin's primitive root conjecture

We say that an integer a is a primitive root mod p if the class of a mod p generates the multiplicative group $\mathbb{F}_p^*$, where p is prime. In [2], Artin conjectured that an integer a, which is not equal to ±1 or any square, should be a primitive root for infinitely many primes p. He further conjectured that the set of primes p for which a is a primitive root mod p should have a natural density $A(a) > 0$ which is given by an Euler product. These conjectures are called Artin's primitive root conjecture and have been a continuing subject of study to this date.

We need algebraic number theory to investigate the density $A(a)$. For each positive integer m, let $K_m^a = \mathbb{Q}(a^{1/m}, \zeta_m)$, where ζ_m is a primitive mth root of unity. By examining the behaviour of the prime ideal p in the extensions K_q for q prime, we get that a is a primitive root mod p if and only if p does not split completely in any extension K_q^a, for q prime. The Chebotarev density theorem then tells us that the density of primes which split completely in K_q^a is $[K_q^a : \mathbb{Q}]^{-1}$. (For an effective version see [19]) This heuristic allows us to guess that

$$A(a) = \prod_{q \text{ prime}} \left(1 - \frac{1}{[K_q^a : \mathbb{Q}]}\right).$$

By incorporating inclusion-exclusion into our heuristic, we obtain the more accurate formula

$$A(a) = \sum_{m \geq 1} \frac{\mu(m)}{[K_m^a : \mathbb{Q}]},$$

where $\mu(m) = (-1)^j$ if m is the product of j distinct primes for some j, and 0 otherwise.

In 1967, Hooley[16] proved Artin's primitive root conjecture conditionally on the generalized Riemann Hypothesis for the number fields $K_m^a, \;\; m \geq 1$. Recall that the generalized Riemann Hypothesis is for K_m^a is the assumption that the analytic continuation of the function

$$\zeta_{K_m^a}(s) = \sum_{I \text{ an ideal of } O_{K_m^a}} N_{K_m^a/\mathbb{Q}}(I)^{-s},$$

has all of its non-trivial zeroes lying on the line $\mathrm{Re}(s) = 1/2$.

Now, let

$$N_a(x) = \#\{p \text{ prime} : p \leq x, a \text{ is a primitive root mod } p\}.$$

Theorem 1.1.1 ([16], Theorem, pp. 219-220)**.** *Suppose that a is a non-square and not equal to ± 1. Further, assume that the generalized Riemann Hypothesis holds for the extensions $K_m^a, m \geq 1$. Then*

$$N_a(x) = A(a)x/\log x + \mathrm{O}(x \log\log x/(\log x)^2),$$

with

$$A(a) = \sum_{m \geq 1} \frac{\mu(m)}{[K_m^a : \mathbb{Q}]} > 0.$$

We can broadly think of Hooley's proof as being organized into several steps, which we can imitate when thinking of similar questions. First, restate "a is a primitive root mod p" as "p splits completely in no field K_m^a". Next, determine a bound for the discriminant of K_m^a for each $m \geq 1$, and determine bounds for $[K_m^a : \mathbb{Q}]$ for each $m \geq 1$. One then observes that

$$N_a(x) = N(x, y) + \mathrm{O}(M(y, x)),$$

where $N(x, y)$ is the number of primes which do not split completely in K_q^a with $q \leq y$, and $M(y, x)$ is the number of primes which split completely in some K_q^a with $y < q \leq x$. Then see that y can be chosen so that $N(x, y) = A(a)x/\log x + \mathrm{O}(x \log\log x/(\log x)^2)$. Then the error term $M(y, x)$ is dealt with by a combination of sieving techniques. Finally, further investigation of $[K_m^a : \mathbb{Q}]$ gives that $A(a)$ has an Euler product, which leads to the fact that $A(a) > 0$.

After Hooley's success, it is natural to ask whether the concept of a primitive root can be generalized to (abelian) algebraic groups defined over $\mathbb{Q}$. One particular example is elliptic curves.

1.2 The Lang-Trotter Conjecture

Suppose that the algebraic curve $E(\mathbb{C}) = \{(x,y) \in \mathbb{C}^2 : y^2 = x^3 + ax + b\} \bigcup \{\infty\}$ is smooth (this is the same as requiring that $f(x) = x^3 + ax + b$ has no repeated roots). Suppose also that $a, b \in \mathbb{Q}$. Then we say that E is an elliptic curve defined over $\mathbb{Q}$. The set of rational points of $E(\mathbb{Q}) = \{(x,y) \in \mathbb{Q}^2 : y^2 = x^3 + ax + b\} \bigcup \{\infty\}$ forms an abelian group. An endomorphism of E is a map $(x,y) \to (f(x), g(y))$ such that f, g are fractions of polynomials which can be extended to be defined everywhere on $E(\mathbb{C})$, and which takes $\infty \to \infty$ when extended. The set of endomorphisms is a commutative ring which contains $\mathbb{Z}$ under the map $n \to \{P \to n \cdot P)$. If it is strictly larger than $\mathbb{Z}$ then we say that E has complex multiplication (abbreviated CM).

For a point $a \in E(\mathbb{Q})$ which is non-torsion, and a prime p, we say that a is a primitive point mod p if E has good reduction at p and $\overline{a} \in E(\mathbb{F}_p)$ generates $E(\mathbb{F}_p)$ as an abelian group. Obviously, if a is a primitive point for E mod p, then $E(\mathbb{F}_p)$ must be cyclic. This leads us to ask whether or not $E(\mathbb{F}_p)$ is cyclic for infinitely many primes p. The answer to this question is given by Serre in [29] in the affirmative giving a positive density of such primes, assuming the generalized Riemann hypothesis. This was later refined by Gupta and Murty in [12] to an unconditional result, but at the cost of losing the natural density.

Therefore, it makes sense to consider an elliptic curve version of Artin's primitive root conjecture. In fact, Lang and Trotter [20] made the relevant conjecture, along with computational evidence and heuristics based on the Chebotarev density theorem.

Let E be an elliptic curve defined over $\mathbb{Q}$, and $a \in E(\mathbb{Q})$. For a prime p of good reduction for E, let $i(p) = [E(\mathbb{F}_p) : \langle \overline{a} \rangle]$, where $\overline{a}$ is the point in $E(\mathbb{F}_p)$ corresponding to a mod p and $\langle \overline{a} \rangle$ represents the subgroup of $E(\mathbb{F}_p)$ generated by the reduction of $\overline{a}$. Let $K_m^a = \mathbb{Q}(E[m], m^{-1}a)$, for m a square-free integer. Lang and Trotter show that there is a union of conjugacy classes $\mathscr{C}_m \subset \mathrm{Gal}(K_m^a/\mathbb{Q})$ such that $q \mid i(p)$ if and only if $\sigma_p \subset \mathscr{C}_q$. Here, σ_p denotes the union of all the Frobenius' automorphisms for p' lying above p. Further, let $\delta(m) = |\mathscr{C}_m|/[K_m^a : \mathbb{Q}]$. Then Lang and Trotter [20] conjectured that

$$\sum_{m \geq 1} \mu(m)\delta(m)$$

is equal to the density of primes p for which a is a primitive root mod p.

There is one main obstacle towards proving the Lang-Trotter by following Hooley's argument. That is for q large enough $|\mathscr{C}_q| \sim q^4$ if E does not have complex multiplication or q^2 when E does have complex multiplication, and $[K_q^a : \mathbb{Q}] \sim q^6$ if E does not have complex multiplication or q^4 if E does have complex multiplication. These larger degrees for $|\mathscr{C}_q|$ and $[K_q^a : \mathbb{Q}]$ as well as increased discriminant values conflict with the error terms in the Chebotarev density theorem, even if we assume the generalized Riemann hypothesis. There is no obvious way around this obstacle. Luckily Gupta and Murty [11] circumvented these difficulties in the case where E has complex multiplication.

1.3 Gupta's and Murty's work

Gupta and Murty first assume that they are in the case where E has complex multiplication by the full ring of integers O_k, where k is a quadratic imaginary extension of $\mathbb{Q}$. Put simply, Gupta and Murty aim to make the Lang-Trotter conjecture tractable by splitting the condition that $q \mid i(p)$ into two independent conditions, each of which is equivalent to a condition of the form "p splits completely in an extension field (depending on q)". Now, our main term becomes a double sum and since we are looking for primes which split completely, the error term coming from the Chebotarev density theorem is more manageable. Unfortunately, this method only deals with the primes p which split completely in k, so even in this case, a density result remains elusive.

Let

$$N_a(x) = \{p \text{ prime} \mid p \leq x,\ p \text{ splits completely in } k,\ a \text{ is a primitive point mod } p\}.$$

Theorem 1.3.1 ([11],Theorem 1)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by O_k, and let $a \in E(\mathbb{Q})$ be a point of infinite order. Under the GRH for each number field K_m^a,*

$$N_a(x) = \delta_E(a)\frac{x}{\log x} + \mathrm{O}\left(\frac{x \log\log x}{(\log x)^2}\right),$$

as $x \to \infty$.

Further, they gave conditions [11, Theorem 2] which imply that $\delta_E(a) > 0$, hence giving a conditional proof of the Lang-Trotter conjecture in these cases. Although they were not able to resolve the Lang-Trotter conjecture if E has no complex multiplication, by considering finitely generated torsion-free subgroups $\Gamma \subset E(\mathbb{Q})$, they were able to make progress.

Let Γ be a freely generated subgroup of $E(\mathbb{Q})$, generated by t elements. Denote the reduction of Γ mod p by Γ_p for those p where E has good reduction. Let $N_\Gamma(x)$ be the number of primes of good reduction for E, less than or equal to x for which $\Gamma_p = E(\mathbb{F}_p)$.

Theorem 1.3.2 ([11], Theorem 3)**.** *Suppose that E has no complex multiplication and* $\operatorname{rank}(\Gamma) = t \geq 18$*. Then, under GRH, there is a constant $\delta_E(\Gamma)$ such that*

$$N_\Gamma(x) = \delta_E(\Gamma)x/\log x + \mathrm{o}(x/\log x),$$

as $x \to \infty$.

If we suppose that E has complex multiplication and let $\tilde{N}_\Gamma(x)$ be the number of primes which split completely in k, of good reduction for E and satisfy $\Gamma_p = E(\mathbb{F}_p)$.

Let $1/2 \leq \eta < 1$. The term η-GRH means that the Dedekind zeta functions for ζ_L have no zeroes in the region $Re(s) > \eta$, where L runs over the number fields K_m^Γ, with m squarefree.

Theorem 1.3.3 ([11], Theorem 4)**.** *Suppose that E has complex multiplication by an order in k and that* $\operatorname{rank}(\Gamma) = t$*. Assuming an $t/(t+1)$-GRH, we have*

$$\tilde{N}_\Gamma(x) = \delta_E(\Gamma)x/\log x + \mathrm{o}(x/\log x),$$

as $x \to \infty$.

The main goal of this thesis is to formulate and prove analogous results to these, where we consider Drinfeld modules over function fields with constant field $\mathbb{F}_r$, where r is a power of a prime.

1.4 The Carlitz module and Drinfeld modules

For an introduction to function fields see [27, Chapters 2,5,12,13] and for more detailed information see [8, Chapters 2,3,4,6]. For a comprehensive treatment of Drinfeld modules see [10, Chapter 4]. For now, we will be as brief as possible with our treatment, leaving the details for later.

In this thesis, a function field F will be an extension of $\mathbb{F}_r$, where r is a power of a prime, such that the transcendence degree of F over $\mathbb{F}_r$ is 1 and $F \cap \overline{\mathbb{F}_r} = \mathbb{F}_r$. For a fixed rational prime ∞, let A be the ring of elements of F for which $v_\ell(x) \geq 0$ for any $x \in A$, and place $\ell \neq \infty$.

Example 1.4.1. *Let $F = \mathbb{F}_r(T)$ with T an indeterminate. Let $A = \mathbb{F}_r[T]$ be the polynomial ring with coefficients in $\mathbb{F}_r$. For $f(T) \in \mathbb{F}_r[T]$, define* $\deg f = [A/f(T) : \mathbb{F}_r]$*. The primes of A are the monic, irreducible and non-constant polynomials in A.*

The A defined above is well-known to be similar to the integers in many ways. For example, let

$$\pi_{\mathbb{F}_r[T]}(x) = \#\{P(t) \in \mathbb{F}_r[T] | P \text{ is a prime}, \deg P = x.\}$$

Then a counting argument [27, Theorem 2.2] gives

$$\pi_{\mathbb{F}_r[T]}(x) = \frac{r^x}{x} + \mathrm{O}\left(\frac{r^{x/2}}{x}\right),$$

as $x \in \mathbb{N}$, $x \to \infty$. When A and F are more general, we can use [27, Theorem 5.12].

Compare this to the regular prime number theorem, by considering x above as $\log x$ in the prime number theorem and r^x above as x in the prime number theorem. In fact, in these terms, the prime number theorem for $\mathbb{F}_r[T]$ is as strong as the Riemann Hypothesis in the classical case. A general program of study is therefore to convert classical results which are conditional on GRH to results for function fields which are unconditional.

Two other papers which we will follow for our results are [17] and [18], which state and prove the analogue to Artin's conjecture for the Carlitz module and rank 1 sgn-normalized Drinfeld modules respectively. Before we can state these results, we must introduce the Carlitz module and Drinfeld modules in general.

For the original paper by Carlitz see [5]. The idea of the Carlitz module is to provide F with an additional A-module structure. Since in this case $A = \mathbb{F}_r[T]$, let us first define the T action. Let $C_T : F \to F$ be defined by $C_T(X) = X^r + TX$. Then C_T is $\mathbb{F}_r$-linear. When we want to multiply x in the module F by T, we can apply C_T to x. Now, we want a homomorphism from A to the $\mathbb{F}_r$-linear endomorphisms of F, which extends $T \to C_T$ This implies that $C_b = bX$ for $b \in \mathbb{F}_r$, and $C_{T^n} = C_T(C_{T^{n-1}})$, which associates to each element of $\mathbb{F}_r[T]$ an $\mathbb{F}_r$-linear polynomial.

Notice as well that the action of A by C is well-defined for any field extension of F. Further, if P is a monic irreducible, the action induced by C turns $\mathbb{F}_r[T]/P$ into an $\mathbb{F}_r[T]$-module as well. Compare this to the action of the integers on the multiplicative group $\mathbb{Q}^*$. Building on this analogy, Hayes [13],[14] and Drinfeld [6],[7] somewhat independently developed class field theory for function fields over finite fields.

We need slightly more language to talk about Drinfeld modules in general.

Define $\tau : F \to F$ by the following formula,

$$\tau(X) = X^r$$

for $X \in F$. Another way to state this is $\tau \in \mathrm{End}_{\mathbb{F}_r}(G_a(F))$, where G_a is the functor which associates to each field its underlying additive group. That is, $\tau(x+y) = \tau(x) + \tau(y)$ and $\tau(\alpha x) = \alpha\tau(x)$ for $x, y \in F, \alpha \in \mathbb{F}_r$. Then set $F\{\tau\}$ to be the ring generated by τ and F, with the natural relations inherited by the definition of τ. That is, $\tau^n\tau^m = \tau^{n+m}, \tau{\cdot}x = x^r\tau$, for $x \in k$.

If F is infinite then $\mathrm{End}_{\mathbb{F}_r}(G_a(F)) = F\{\tau\}$, by [10, Proposition 1.1.5].

We say that K is an A-field if it is equipped with a homomorphism $i : A \to K$.

Definition 1.4.1. *Let $\phi : A \to K\{\tau\}$ be a homomorphism of $\mathbb{F}_r$-algebras. For $a \in A$, the image of a under ϕ is denoted ϕ_a. Write*

$$\phi_a = \phi_{a,n}\tau^n + \cdots + \phi_{a,1}\tau + \phi_{a,0}\tau^0,$$

with $\phi_{a,n} \neq 0$, and $\phi_{a,i} \in F$. We say that ϕ is a Drinfeld module if $\phi_{a,0} = i(a)$ for all $a \in A$ and $\phi_{a^*} \neq i(a^*)\tau^0$ for some $a^* \in A$. We will set ϕ_a to be the image of a in $K\{\tau\}$ under ϕ. For fixed a, the number $d := \deg_\tau \phi_a / \deg a$ is a positive integer which is independent of a. The positive integer d is called the rank of the Drinfeld module.

1.5 Artin's conjecture for Drinfeld modules

As before, by reducing the coefficients of C_f modulo P, for a monic, irreducible $P \in \mathbb{F}_r[T]$, we obtain an action $\overline{C_f}$ on $A/P \equiv \mathbb{F}_{r^{\deg P}}$. When we are talking about A/P as an A-module via C, we will refer to it as $C(A/P)$. Now, fix $a \in \mathbb{F}_r[T]$ and let $A \cdot \overline{a}$ denote the submodule of $C(A/P)$ generated by the reduction of a mod P. Let

$$N_a(x) = \#\{P \in \mathbb{F}_r[T] : P \text{ is monic, irreducible with } \deg P = x, \text{ and } A \cdot \overline{a} = C(A/P)\},$$

for $x \in \mathbb{N}$. As usual, for a polynomial $m \in A$,we define the m-torsion of C to be

$$C[m] = \{x \in \overline{F} \mid C_m(x) = 0\}.$$

Let α be a particular root of $C_m(X) = a$. Then, just as in the classical case, the extensions $K_m^a = F(C[m], \alpha)$ play an integral role in the proof.

Theorem 1.5.1 ([17], Theorem 4.6)**.** *Suppose that $0 \neq a \in \mathbb{F}_r[T]$. Then there exists a constant δ_a such that*

$$N_a(x) = \delta_a \frac{r^x}{x} + \mathrm{o}\left(\frac{r^x}{x}\right),$$

for $x \in \mathbb{N}$ as $x \to \infty$, with $\delta_a > 0$ except for when $r = 2$ and $a \in \{1\} \cup C_T(A) \cup C_{1+T}(A)$.

If $r \neq 2$, we have

$$\delta(a) = \prod_{q \in \mathbb{F}_r[T],\ monic,\ irreducible} \left(1 - \frac{1}{[K_q^a : k]}\right).$$

The proof of this proceeds similarly to that of Hooley's result, the main difficulties arising from ramification at the prime at ∞ (corresponding to $(1/t)$), as well as proving that $[K_{mn}^a : k] = [K_m^a : k][K_n^a : k]$, for $(m, n) = 1$. That is, because we are not working over the integers, working out the multiplicative nature of these field extension degrees requires more work than the classical case.

Later, Hsu and Yu [18] were able to extend this result to a class of rank 1 Drinfeld modules, called sgn-normalized rank 1 Drinfeld modules. We will state their result here. Let F be a function field, and ∞ a rational prime of F. Set O to be the subring of F consisting of all elements which are regular everywhere except possibly ∞. Let H_O be the Hilbert class field of O, (i.e., the maximal unramified extension of F such that ∞ splits completely). Let O' be the integral closure of O in H_O. Let ψ be a rank 1, sgn normalized Drinfeld module with coefficients in O'. For prime ideals $\mathfrak{P}$ of O', we say that a is a primitive root mod $\mathfrak{P}$ if $\overline{a}$ generates $\psi(O'/\mathfrak{P})$ as an A-module.

Theorem 1.5.2 ([18], Theorem 4.6)**.** *Suppose that $r \neq 2$ and $0 \neq a \in O'$. The set of primes $\mathfrak{P}$ of O' for which a is a primitive root mod $\mathfrak{P}$ has density $\delta_\psi(a) > 0$, which is given by an Euler product.*

The notion of sgn-normalized rank 1 Drinfeld modules arises naturally from the class field theory of F, and we will address all notation in **Chapter 3**.

1.6 Lang-Trotter for rank 2 Drinfeld modules

Earlier, we saw that the Lang-Trotter conjecture is a natural elliptic curve analogue of Artin's conjecture. Further, Hsu and Yu's result is a function field analogue for Artin's conjecture. Actually, Bilharz [4] proved a function field analogue for Artin's conjecture as well. That is, let K be a global function field, and let $a \in K$. Given a prime $P = (O_P, R_P)$ of K, if the reduction of a modulo P generates $(O_P/R_P)^*$ multiplicatively, then we say that a is a primitive root modulo P. Briefly, under suitable conditions on the field K and $a \in K$, Bilharz proved that a is a primitive root modulo P for infinitely many primes

P. This is the most direct generalization of Artin's Conjecture to the function field case. Bilharz assumed the Riemann Hypothesis for function fields which was later proved by Weil. Further, Bilharz obtained a Dirichlet density for the set of primes in question, but not a natural density.

One of the goals of this thesis is to prove a function field analogue for the result of Gupta and Murty. During this proof, we will expose some of the deep similarities between the arithmetic of elliptic curves, the functor $G_m(\cdot)$ which assigns to every field its multiplicative group of non-zero elements, and Drinfeld modules.

Let $\phi : A \to K\{\tau\}$ be a Drinfeld module of generic characteristic, where the fraction field of A is F and $[K : F] < \infty$. Let P be a prime of K (a local sub-ring O_P and corresponding maximal ideal R_P) which does not lie above ∞. For all but finitely many P, the coefficients of ϕ_a will be elements of O_P for all $a \in A$. We can reduce them modulo P to obtain a Drinfeld module $\phi(\mathbb{F}_P)$ (where $\mathbb{F}_P = O_P/R_P$). If we again exclude finitely many P, we can insist that $\phi(\mathbb{F}_P)$ has the same rank as ϕ.

If $a \in F$ is such that $a \in O_P$, then we can ask whether or not $a + R_P$ generates $\phi(\mathbb{F}_P)$ as an A-module. Let $A \cdot \overline{a}$ be the submodule of $\phi(\mathbb{F}_P)$ which is generated by $a + R_P$. If it so happens that ϕ has "good reduction" at P, and $a \in O_P$, and $\phi(\mathbb{F}_P)$ is generated by $\overline{\alpha}$, then we say α is a primitive point mod P.

Conjecture 1.6.1. *Let a be a non-torsion point for ϕ, a rank 2 Drinfeld module defined over K, with $[K : F]$ finite. Suppose that $\mathrm{tor}(\phi)$ is cyclic (the submodule of rational torsion). Then a is a primitive point mod P for infinitely many primes P of K.*

We now make assumptions that correspond to CM. Let k be an extension of F such that ∞ ramifies and $[k : F] = 2$. Further suppose that $\mathrm{End}(\phi)$ is the integral closure of A in k, say that $\mathrm{End}(\phi) \cong O(= O_k)$. The case that ∞ does not ramify is not covered in this thesis. If ∞ is inert, there are two possibilities. The first is that $k = F(\mathbb{F}_{r^2})$ is a constant field extension. One example of this is $F = \mathbb{F}_r(T), k = \mathbb{F}_{r^2}(T)$. The second case is if k has $\mathbb{F}_r$ as its constant field, and then ∞ is of degree 2 in k. In the first case, the constant field complicates the splitting behaviour of primes, as well as the Chebotarev density theorem. Thus, the difficulty lies with resolving the peculiarities of constant field extension, rather than generalizing the work of Gupta and Murty. To solve the second case, we would have to attempt to generalize Hsu and Yu's work for Artin's conjecture for rank 1 Drinfeld modules. Again, this is worth doing, but it is outside of the scope of this thesis. We expect that the constant field extension case will be solved in the future.

Let ψ be the rank 1 Drinfeld module such that $\psi : O \to H_O$, and ψ restricted to A is ϕ. Assume that H_O is the Hilbert class field of k, and that H_O has constant field equal to $\mathbb{F}_r$.

Finally, assume that ψ is a sgn-normalized Drinfeld module, for some sign function sgn. A sign function for us is a homomorphism $\mathrm{sgn} : F_\infty^* \to \mathbb{F}_r^*$ which fixes $\mathbb{F}_r^*$. We set $\mathrm{sgn}(0) = 0$. The Drinfeld module ψ is sgn-normalized if the leading coefficient of ψ_x is $\mathrm{sgn}(x)$.

Let $a \in K, x \in \mathbb{N}$, then we let

$$N_\alpha(x) = \# \left\{ P \text{ a prime of } K \;\middle|\; \begin{array}{l} \deg P = x, P \text{ splits completely in } H_O \\ a \text{ is a primitive root mod } P \end{array} \right\}$$

Theorem 5.1.1. *Let $\phi : A \to K\{\tau\}$ be a rank 2 Drinfeld module, with CM by a* sgn-*normalized Drinfeld module ψ of rank 1, $\psi : O \to O'\{\tau\}$. Suppose that* $\mathrm{tor}(\phi)$ *is cyclic. Let $a \in K$ be a non-torsion element for ϕ, then there exists $\delta_\phi(a) > 0$ such that*

$$N_a(x) = \delta_\phi(a)\frac{r^x}{x} + \mathrm{O}\left(\frac{r^x \log x}{x^2}\right)$$

as x tends to infinity.

For our second theorem, let $A = \mathbb{F}_r[T]$ and $K = F = \mathbb{F}_r(T)$.

Let $\phi : A \to F\{\tau\}$ be a Drinfeld Module of rank 2, defined by

$$\phi_T = \Delta\tau^2 + g\tau + T,$$

for some $D, g \in F, D \neq 0$. Suppose further that ϕ has no complex multiplication over any extension field.

Let Γ be a finitely generated free A submodule of F (see [24] for the structure of F). That is $\Gamma = A \cdot \{a_1, \ldots, a_s\}$ and the a_i's are independent over A (remember that the A action is given by ϕ).

A prime P of A will be a monic irreducible. These correspond to the prime ideals of A.

For all but finitely many primes P of F, we may reduce Γ modulo P to obtain a submodule Γ_P of the Drinfeld Module $\phi(\mathbb{F}_P)$, where $\mathbb{F}_P$ is the residue field of A modulo P.

Theorem 5.1.2. *Let $F = \mathbb{F}_r(T), A = \mathbb{F}_r[T], \phi_T = D\tau^2 + g\tau + T, \Gamma = A \cdot \{a_1, \ldots, a_t\}$ and N_Γ denote the number of primes of A of degree x with $\Gamma_P = \phi(\mathbb{F}_P)$. If $t \geq 18$ then,*

$$N_\Gamma(x) = \delta_\phi(\Gamma)\frac{r^x}{x} + \mathrm{O}\left(\frac{r^x \log x}{x^2}\right)$$

as $x \to \infty$ for $x \in \mathbb{N}$, if we assume that the Kummer extension fields associated to Γ have constant field equal to $\mathbb{F}_r$.

Notice that in the above result, as well as [11, Theorem 4], we require the 18 independent generators in Γ. This is very unlikely to happen for elliptic curves, but for Drinfeld modules, we can find many examples of Γ, by [24, Theorem 1].

1.7 An overview of the rest of the thesis

In order to understand our motivation for the method of Gupta and Murty, we give a summary of their work [11] in **Chapter 2**. This will provide our general program for the rest of the thesis. We will be able to see the motivation behind our work for the Drinfeld module case. Further, we will see how Gupta and Murty overcame the main obstacles of the Lang-Trotter conjecture. There are three results which are interesting because we are able to prove an analogue for Drinfeld modules. These results are [11, Theorems 1,2,3]. We are able to prove a more general result than would be expected, in part because of the explicit class field theory available in the function field case.

In **Chapter 3**, we will explore the theory of Drinfeld modules in detail. There is much to define and prove before one can start talking about the arithmetical properties of Drinfeld modules. We will not prove everything, but we will prove some of the results which are fundamental to the later sections. First, we will see the theory of additive functions over a field of finite characteristic. Then we review some non-archimedean analysis, especially important is the theory of Newton polygons. We then give the definition of Drinfeld modules and look at some of the basic theory of the subject. The main areas to note are the theory of endomorphisms, reduction theory, analytic uniformization theorems and class field theory.

In **Chapter 4**, we have compiled all of the algebraic number theory results. That is, the Kummer theory which is hybridized from [17, 18, 25, 26]. Further, we need many discriminant bounds, which are compiled here as well. Finally, we review the relevant sections of [18] which we need for our CM theory.

In **Chapter 5**, we prove our main results, drawing on all previous chapters as well as prime counting theorems.

Finally, in **Chapter 6**, we give some future work directions, as well as any difficulties towards future goals.

Chapter 2

Overview of the Lang-Trotter conjecture and Gupta's and Murty's work

2.1 Elliptic Curves review

For a background reference on elliptic curves, see [33].

Let E be an elliptic curve defined over $\mathbb{Q}$. The curve E is defined by an equation $y^2 = x^3 + ax + b$, such that $a, b \in \mathbb{Q}$ and the resulting projective curve is smooth. This is true if we require $f(x) = x^3 + ax + b$ to have no repeated roots. Let $E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 + ax + b\} \bigcup \{\infty\}$, where ∞ refers to the point at infinity when we look at this curve as being embedded in $\mathbb{P}^2$. It is well-known that $E(\mathbb{Q})$ is a group. In fact, let K be a field with $\mathbb{Q} \subset K$; then the set of points with coefficients in K is also a group, denoted $E(K)$ (again we are including the point at infinity).

We are interested in what happens to this group when we reduce the coefficients of E modulo various primes. Let $\Delta = \mathrm{disc}(f(x))$ (where $\mathrm{disc}(f(x))$ is the discriminant of f). We will give a very crude treatment of the reduction theory. Let $O_p = \{x \in \mathbb{Q} \mid v_p(x) \geq 0\}$. We may assume that $a, b \in O_p$ and $\Delta \in O_p^\times$ for all but finitely many p. For these p, we see that by reducing the equation $y^2 = f(x)$ modulo p, we obtain an elliptic curve defined over $\mathbb{F}_p$. If this is the case then we say that E has good reduction at p. So we see that E has good reduction modulo all primes with only finitely many exceptions.

Let $n \in \mathbb{Z}$, and

$$E[n] = \{P \in E(\mathbb{C}) \mid n \cdot P = \infty\}.$$

Then, as an abstract group $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$. If E is a curve defined over a field of positive characteristic, say p, then $E[p^n]$ is isomorphic to either $\mathbb{Z}/p^n\mathbb{Z}$ or 0. For n coprime to p, we have that $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$, as before.

The structure of the K-points of E is determined by the following theorem.

Theorem 2.1.1 ([33], Theorem 6.7, Mordell-Weil Theorem)**.** *Let K be a finite extension of $\mathbb{Q}$ and E/K be an elliptic curve. Then there exists a non-negative integer t, called the rank of E (over K), such that*

$$E(K) \cong \mathbb{Z}^t \oplus E_{\text{tors}},$$

where E_{tors} is the torsion subgroup of $E(K)$. Further E_{tors} is finite.

Let p be a prime where E has good reduction. Then since $E(\mathbb{F}_p)$ is a finite group it is torsion, hence we may write

$$E(\mathbb{F}_p) \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z},$$

with $m_1 \mid m_2$. Thus, in general, the finite abelian group $E(\mathbb{F}_p)$ may or may not be cyclic.

Finally, an important aspect of Gupta's and Murty's work is that it requires complex multiplication theory for one of the main results. A map $f : E \to E$ which is defined by rational functions is called an endomorphism if it takes ∞ to ∞, and is defined everywhere. It is called an isogeny if it is not the constant map $f(P) = \infty$. Then f respects the group law, see [33, Chapter 1, Section 3 and Chapter 3, Section 4]. One example of such an endomorphism is the multiplication by n map, denoted $[n]$. Let K be a field such that $\mathbb{Q} \subset K$. Then the endomorphisms defined over K form an integral domain, called $\mathrm{End}_K(E)$, with product given by composition, and addition given by pointwise addition. Denote by $\mathrm{End}(E)$ the ring of all endomorphisms of E. Then $k = \mathrm{End}(E) \otimes \mathbb{Q}$ is either $\mathbb{Q}$ or a quadratic imaginary extension of $\mathbb{Q}$. Further $\mathrm{End}(E)$ is an order in k. For clarification, we mean that $\mathrm{End}(E)$ is contained in the integral closure of $\mathbb{Z}$ in k, it is finitely generated as an abelian group, and it satisfies $\mathrm{End}(E) \otimes \mathbb{Q} = k$. There is a finite extension K of $\mathbb{Q}$ such that $\mathrm{End}_K(E) = \mathrm{End}(E)$.

We want to see that all endomorphisms of E are defined over k. Let $G := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then, for $\phi \in \mathrm{End}(E), g \in G$ define $g \cdot \phi = g\phi g^{-1}$, which gives an action of G on $\mathrm{End}(E)$ which satisfies

$$gh(\phi) = g(h(\phi)),$$

$$g(\phi\psi) = (g\phi)(g\psi),$$

and

$$g(\psi + \phi) = g\psi + g\phi.$$

Further, we have that $g \cdot [n] = [n]$, where n is the multiplication by n map (since E is defined over $\mathbb{Q}$).

Let $x \in O_k$ such that $k = \mathbb{Q}(x)$, and there exists $\phi \in \mathrm{End}(E)$ such that ϕ satisfies the same equation over $\mathbb{Z}$ that x does. Thus, the polynomial f splits in the field k. Further $g(\phi) + \phi = g(x) + x$ and so ϕ is fixed by g if and only if x is fixed by g, for any $g \in G$. Let $P \in E(k)$, then $g(P) = P$ for $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/k)$, let $\phi \in \mathrm{End}(E)$, then $g(\phi) = \phi$, so $\phi(P) = g(\phi(g^{-1}(P))) = g(\phi(P))$, so $\phi(P) \in E(k)$.

2.2 Main Results

We want to investigate the structure of $E(\mathbb{F}_p)$ for various primes p. It is natural to ask whether or not $E(\mathbb{F}_p)$ is cyclic for infinitely many primes p.

Theorem 2.2.1 ([29], Theorem 1.1)**.** *Assume the generalized Riemann hypothesis for the number fields K_m, where K_m is $\mathbb{Q}$ adjoined by the coordinates of all the m-torsion points for E. Then $E(\mathbb{F}_p)$ is cyclic for infinitely many primes p. Further, let*

$$N_E(x) = \#\{p \textit{ prime} \mid E \textit{ has good reduction at } p, E(\mathbb{F}_p) \textit{ is cyclic}\}.$$

Then there exists a constant δ_E such that

$$N_E(x) = \delta_E \frac{x}{\log x} + \mathrm{o}\left(\frac{x}{\log x}\right),$$

with $\delta_E > 0$ if and only if E has an irrational 2-torsion point.

Theorem 2.2.2 ([12], Theorem 1)**.** *Let $E, N_E(x)$ be as above. If E has an irrational 2-torsion point, then*

$$N_E(x) \gg \frac{x}{(\log x)^2}.$$

Now, given a point $a \in E(\mathbb{Q})$ of infinite order and a prime p of good reduction, we may reduce the coordinates of a modulo p. That is, if $a = (x, y)$, then in projective coordinates $a = [x : y : 1]$, so rewrite a as $[x' : y' : z]$ where all coordinates are integers and $\gcd(x', y', z) = 1$. By reducing x', y' and z modulo p we obtain a point $\overline{a} \in E(\mathbb{F}_p)$. If $\overline{a}$ generates $E(\mathbb{F}_p)$ then we say that a is a primitive point modulo p. If Γ is generated by

n points which are independent over $\mathbb{Z}$, then we denote the reduction of Γ modulo p by Γ_p and we get that Γ_p is a subgroup of $E(\mathbb{F}_p)$.

Let

$$N_a(x) = \#\{p \leq x,\ \text{prime} \mid p \text{ splits in } k,\ a \text{ is a primitive point modulo } p\}.$$

Theorem 2.2.3 ([11], Theorem 1)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by O_k and let a be a rational point of infinite order. Under the GRH,*

$$N_a(x) = \delta_E(a)\frac{x}{\log x} + \mathrm{O}\left(\frac{x \log\log x}{(\log x)^2}\right),$$

as $x \to \infty$.

Gupta and Murty are able to give conditions which imply $\delta_E(a) > 0$.

Theorem 2.2.4 ([11], Theorem 2)**.** *If 2 and 3 are inert in k or $k = \mathbb{Q}(\sqrt{-11})$, then $\delta_E(a) > 0$. Therefore, on the GRH,*

$$N_a(x) \gg \frac{x}{\log x}$$

in these cases.

Unfortunately, their method is only able to treat the primes that split in k.

By considering multiple generators, i.e. a subgroup generated by n elements, Gupta and Murty were able to make some progress in the non-CM case. Let Γ be a free subgroup of $E(\mathbb{Q})$ of rank t. For a prime p of good reduction, denote by Γ_p the subgroup of $E(\mathbb{F}_p)$ generated by the reduction of each generator of Γ modulo p. Let

$$N_\Gamma(x) = \#\{p \leq x, \quad p \text{ prime} \mid p \text{ is of good reduction}, \Gamma_p = E(\mathbb{F}_p)\}.$$

Theorem 2.2.5 ([11], Theorem 3)**.** *Suppose that E has no complex multiplication and* $\operatorname{rank}(\Gamma) = t \geq 18$*. Then, under GRH, there is a constant $\delta_E(\Gamma)$ such that*

$$N_\Gamma(x) = \delta_E(\Gamma)\frac{x}{\log x} + \mathrm{o}\left(\frac{x}{\log x}\right)$$

as $x \to \infty$.

A similar result is derived for the case when E has complex multiplication, but we only need to assume that the corresponding Dedekind zeta functions have no zeroes in the region $\mathrm{Re}(s) > (t/(t+1))$. We call this assumption $t/(t+1)$-GRH. This method again only deals with those primes that split completely in k. Let

$$\tilde{N}_\gamma(x) = \#\{p \text{ prime}, p \leq x \mid p \text{ splits in } k, \Gamma_p = E(\mathbb{F}_p)\}.$$

Theorem 2.2.6 ([11], Theorem 4)**.** *Suppose that E has complex multiplication by an order in k and recall that the rank of Γ is t. Assuming a $t/(t+1)$-GRH, we have*

$$\tilde{N}_\Gamma(x) = \tilde{\delta}_E(\Gamma)\frac{x}{\log x} + \mathrm{o}\left(\frac{x}{\log x}\right)$$

as $x \to \infty$.

Using sieve theory, Gupta and Murty also showed

Theorem 2.2.7 ([11], Theorem 5)**.** *If E has complex multiplication and $t \geq 6$, where t is the rank of Γ, then*

$$N_\Gamma(x) \gg \frac{x}{(\log x)^2}.$$

Our focus is on the paper [11] but it should be noted that [12] contains several related results.

2.3 The Lang-Trotter condition

Let $a \in E(\mathbb{Q})$ be a non-torsion point. For a prime p of good reduction, let $\langle \overline{a} \rangle$ be the subgroup of $E(\mathbb{F}_p)$ generated by the reduction of a modulo p, and let $i(p) = [E(\mathbb{F}_p) : \langle \overline{a} \rangle]$. We want to formulate a condition for $q \mid i(p)$ in terms of the behaviour of p in an extension field, similar to Artin's conjecture.

We have that $q \mid i(p)$ if and only if either

- $E[q] \subset E(\mathbb{F}_p)$ for $q \neq p$.
- The q primary part of $E(\mathbb{F}_p)$ is cyclic and there exists $b \in E(\mathbb{F}_p)$ such that $q \cdot b = \overline{a}$.

These conditions motivate the definition of the fields $K_q^a = \mathbb{Q}(E[q], q^{-1}a)$, just as in the classical case.

Let $A_q = \mathrm{Gal}(K_q^a/\mathbb{Q})$. For $\sigma \in A_q$, we may represent σ as (γ, χ), where $\gamma \in \mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z})$ and $\chi \in E[q]$. The action of σ can be given in terms of γ and χ. Since σ permutes the

q-torsion, we may denote this action by γ. Also, let u_0 be a particular point such that $q \cdot u_0 = a$. Since $\sigma u_0 - u_0 \in E[q]$, write $\sigma u_0 - u_0 = \chi$. Let u be an arbitrary point such that $q \cdot u = a$. Then $\sigma(u - u_0) = \gamma(u - u_0)$. Thus

$$\sigma(u) = u_0 + \chi + \gamma(u - u_0).$$

Thus, we see that $\sigma(u) = u$ if and only if

$$(\gamma - 1)(u_0 - u) = \chi.$$

Next, we formulate a condition such for $q \mid i(p)$ whenever $p \nmid q\Delta$, where Δ is the discriminant of the curve.

Lemma 2.3.1 ([20], Lang-Trotter condition, pp. 289-290)**.** *Suppose $p \nmid q\Delta$. Fix a member $\sigma_p = (\gamma_p, \tau_p)$ in $\mathrm{Gal}(K_q^a/\mathbb{Q})$ in the conjugacy class of the Frobenius at p. Then $q \mid i(p)$ if and only if either*

1. $\gamma_p = 1$
2. *γ_p has eigenvalue 1, $\ker(\gamma_p - 1)$ is cyclic and $\tau_p \in \mathrm{Im}(\gamma_p - 1)$.*

Remark 2.3.1. The set $\mathscr{C}_q$ corresponding to elements (γ, τ) of $\mathrm{Gal}(K_q^a/\mathbb{Q})$ such that either $\gamma = 1$ or γ has eigenvalue 1 and $\tau \in \mathrm{Im}(\gamma - 1)$ is a union of conjugacy classes.

For $p > 5$, if $p \mid i(p)$ then it is clear that $\#E(\mathbb{F}_p) = p$. Hence, by Serre's result [32, Theorem 21], we have that the number of such primes is $\mathrm{o}(x/\log x)$, whether or not E has CM.

We now refine the Lang-Trotter condition to the case when p splits completely in k. Let $\mathrm{End}(E) = O_k$ be the ring of integers of k, where k is a quadratic imaginary extension of $\mathbb{Q}$. Since E is defined over $\mathbb{Q}$, we have that the class number of O_k is equal to 1. This is because the j invariant of E is rational, and the class number of O_k is bounded by $[\mathbb{Q}(j(E)) : \mathbb{Q}]$. For an ideal $\mathfrak{a} = (\alpha)$ of O_k, let $\mathfrak{a}^{-1}a$ denote a point $b \in E(\mathbb{C})$ such that $\alpha \cdot b = a$. This choice is unique up to translation by $E[\mathfrak{a}]$ and multiplication by a unit in O_k.

For $\mathfrak{q}$ a prime ideal of first degree (i.e. the norm of $\mathfrak{q}$ must be a rational prime), define

$$K_{\mathfrak{q}}^a = k(E[\mathfrak{q}], \mathfrak{q}^{-1}a).$$

Then $K_{\mathfrak{q}}^a$ is independent of the choice of $\mathfrak{q}^{-1}a$ and is Galois over k. If q is a rational prime set

$$K_q = k(E[q]).$$

Lemma 2.3.2 ([11], Lemma 3)**.** *Suppose that p splits in k and $p \nmid q\Delta$. Let $\mathfrak{p}$ be such that $p = \mathfrak{p}\overline{\mathfrak{p}}$ in k, and $\mathfrak{p}$ gives the Frobenius endomorphism of E mod $\mathfrak{p}$.*

1. *If q is inert in k, then $q \mid i(p)$ if and only if p splits completely in K_q.*
2. *If q ramifies or splits in k, let $q = \mathfrak{q}_1\mathfrak{q}_2$ be its factorization in k. Then $q \mid i(p)$ if and only if $(\mathfrak{p})$ splits completely in $K_{\mathfrak{q}_1}^a$ or $K_{\mathfrak{q}_2}^a$ or K_q.*

2.4 Algebra, Kummer and Discriminants

Let $\mathfrak{a}$ be a square-free ideal of O_k which is only divisible by prime ideal factors of first degree and let s be a square-free integer. Define

$$K_{\mathfrak{a}}^a = \prod_{\mathfrak{q}|\mathfrak{a}} K_{\mathfrak{q}}^a, \;\; n(\mathfrak{a}) = [K_{\mathfrak{a}}^a : k].$$

Notice that $K_{\mathfrak{a}}^a = k(E[\mathfrak{a}], \mathfrak{a}^{-1}a)$. Also, the group $\mathrm{Gal}(K_{\mathfrak{a}}^a/k)$ is a subgroup of

$$\left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \in \mathrm{GL}_2(O_k/\mathfrak{a}) \right\}.$$

Set

$$K_s = \prod_{q|s} K_q, \quad m(s) = [K_s : k],$$

and

$$K_{\mathfrak{a},s}^a = K_{\mathfrak{a}}^a \cdot K_s = k(E[l(\mathfrak{a}, s)], \mathfrak{a}^{-1}a),$$

where $l(\mathfrak{a}, s)$ is the least common multiple ideal of $\mathfrak{a}, s$ in O_k.

Let $n(\mathfrak{a}, s)$ be the degree of $K_{\mathfrak{a},s}^a$ over k and $d(\mathfrak{a}, s)$ be the discriminant of $K_{\mathfrak{a},s}^a$ over $\mathbb{Q}$. The following lemmas estimate the numbers $n(\mathfrak{a}, s)$ and $d(\mathfrak{a}, s)$.

Lemma 2.4.1 ([11], Lemma 6)**.** *We have that*

$$\log n(\mathfrak{a}, s) \ll \log N(\mathfrak{a}) + \log s.$$

Lemma 2.4.2 ([11], Lemma 7)**.** *We have that*

$$\frac{\log |d(\mathfrak{a}, s)|}{n(\mathfrak{a}, s)} \ll \log N(\mathfrak{a}) + \log s.$$

Remark 2.4.1. We will see several similar results in **Chapter 4**.

Now, in order to estimate the density $\delta_E(a)$ we need to find a way to calculate $n(\mathfrak{a}, s)$ in terms of $n(\mathfrak{a})$ and $m(s)$.

Lemma 2.4.3 ([11], Lemma 8)**.** *If* $\mathfrak{a}$ *and* s *are coprime to* 6Δ*, where* Δ *is the discriminant of* E*, then*

$$n(\mathfrak{a}, s) = \frac{n(\mathfrak{a})m(s)}{\phi(\mathfrak{a}, s)},$$

where $(\mathfrak{a}, s)$ *is the gcd of* $\mathfrak{a}$ *and* s *in* O_k*, and* $\phi(\mathfrak{a}, s)$ *is* $\#(O_k/(\mathfrak{a}, s))^*$.

2.5 Analysis overview of CM case

Let

$$N(x, y) = \#\left\{ \begin{array}{l} \mathfrak{p} \text{ a first degree prime of } k \\ N(\mathfrak{p}) \leq x \end{array} \middle| \begin{array}{l} \mathfrak{p} \text{ does not split completely in any} \\ K_q \text{ or } K_{\mathfrak{q}}^a \text{ for } q \leq y, N(\mathfrak{q}) \leq y \end{array} \right\}$$

Let S be the set of first degree prime ideals of k. Let T be the set of all rational primes. Let S_y (resp. T_y) denote those elements of S (resp. T) such that $N(\mathfrak{q}) \leq y$ (resp. $q \leq y$). Let S^*, T^*, S_y^*, T_y* denote the set of all square-free products of elements of S, T, S_y, T_y.

Now, let $M(y_1, y_2)$ denote the number of primes $p \leq x$ such that $\mathfrak{p}$ splits completely in some $K_{\mathfrak{q}}^a$ or K_q for $y_1 < q < y_2$ or $y_1 < N(\mathfrak{q}) < y_2$.

Proposition 2.5.1 ([11], p. 23)**.** *We have that*

$$N_a(x) = \frac{1}{2}N(x, y) + \mathrm{O}(M(y, 2x)).$$

The analysis is therefore broken up into parts. First we show that $N(x, y)$ (the main term) tends to $\delta_E(a)\,\mathrm{li}(x)$ as $x \to \infty$ for an appropriate choice of y in terms of x. Then we must show that $M(y, 2x)$ is small compared to the main term. We will do this by splitting up this term into three chunks, each of which is handled separately.

We choose $y = \frac{1}{12}\log x$ and let $\pi(x, \mathfrak{a}, s)$ be the number of first degree primes $\mathfrak{p}$ of k with $N(\mathfrak{p}) \leq x$ which split completely in $K^a_{\mathfrak{a},s}$. By the inclusion-exclusion principle, we have

$$N(x,y) = \sum_{(\mathfrak{a},s)\in S^*_y \times T^*_y} \mu(\mathfrak{a})\mu(s)\pi(x,\mathfrak{a},s).$$

To estimate $\pi(x, \mathfrak{a}, s)$ we use an effective Chebotarev density theorem.

Lemma 2.5.1 ([19], Theorem 1.1)**.** *Let L'/L be a normal extension of number fields with $n = [L' : L]$. Let $d = \operatorname{disc}(L'/\mathbb{Q})$. Let $\pi_{\mathscr{C}}(x, L')$ be the number of prime ideals of first degree of L whose Frobenius automorphism lies in a given conjugacy class $\mathscr{C}$ of* $\operatorname{Gal}(L'/L)$*. If the Dedekind zeta function of L' satisfies the Riemann hypothesis, then*

$$\left|\pi_{\mathscr{C}}(x,L') - \frac{|\mathscr{C}|}{n}\operatorname{li}(x)\right| \ll |\mathscr{C}|x^{1/2}(\log x + \delta(L')),$$

where the implied constant depends only on L and $\delta(L') = \frac{\log|d|}{n}$.

We set $L = k$, $L' = K^a_{\mathfrak{a},s}$ and $\mathscr{C} = \{1\}$, and apply the theorem directly.

Proposition 2.5.2 ([11], pp. 23-24)**.**

$$\left|N(x,y) - \sum_{(\mathfrak{a},s)\in S^*_y\times T^*_y} \frac{\mu(s)\mu(\mathfrak{a})}{n(\mathfrak{a},s)}\operatorname{li}(x)\right| = \mathrm{O}(x^{3/4+\epsilon})$$

for any $\epsilon > 0$.

Proposition 2.5.3 ([11], pp. 24-26)**.** *The sum*

$$\delta = \sum_{(\mathfrak{a},s)\in S^*\times T^*} \frac{\mu(s)\mu(\mathfrak{a})}{n(\mathfrak{a},s)}$$

is absolutely convergent, where $S^* \times T^*$ is the set of all pairs $(\mathfrak{a}, s)$ where s is any square-free positive integer and $\mathfrak{a}$ is square-free and any prime ideal dividing $\mathfrak{a}$ must be of first degree. The constant δ is equal to $2\delta_E(a)$.

Further, as $x \to \infty$, we have

$$N(x,y) = \delta\operatorname{li}(x) + \mathrm{O}\left(\frac{x\log\log x}{\log^2 x}\right).$$

Now, we need to estimate $M(y, 2x)$. We do this by breaking up the interval $(y, 2x)$ into three parts $(y, x^{1/2}/(\log^2 x))$, $(x^{1/2}/(\log^2 x), x^{1/2}\log^2 x)$ and $(x^{1/2}\log^2 x, 2x)$. We will handle the first interval with the Chebotarev density theorem [19, Theorem 1.1]. For the second interval we use an analogue of the Brun-Titchmarsh theorem. For the last interval we use the earlier result on the size of the coefficients of g_β and a counting argument.

Proposition 2.5.4 ([11], p. 26)**.** *Assuming the GRH, we have*

$$M(y, x^{1/2}/(\log^2 x)) = \mathrm{O}(x/(\log^2 x)).$$

Using the large sieve in Schaal [28, Theorem 6], we can get a Brun-Titchmarsh type result. Applying this result along with special considerations for the fields K_q, we get the following proposition.

Proposition 2.5.5 ([11], pp. 26-27)**.** *We have*

$$M(x^{1/2}/\log^2 x, x^{1/2}\log^2 x) = \mathrm{O}\left(\frac{x\log\log x}{\log^2 x}\right).$$

Using a similar idea as [16, p. 211-212], we complete the estimation of the remainder terms.

Proposition 2.5.6 ([11], pp. 27-28)**.** *We have*

$$M(x^{1/2}\log^2 x, 2x) = \mathrm{O}\left(\frac{x}{\log^2 x}\right).$$

Then combining the above propositions, we obtain

$$N_a(x) = \frac{\delta}{2}\,\mathrm{li}(x) + \mathrm{O}\left(\frac{x\log\log x}{\log^2 x}\right).$$

Let $\delta_E(a) = 2\delta$, and the only thing to check is that $\delta_E(a) > 0$.

2.6 Free subgroups of high rank

Let $\Gamma \subset E(\mathbb{Q})$ be a free subgroup of rational points, with Γ_p the reduction of Γ modulo p. Let Γ be freely generated by t rational points $a_1, \ldots, a_r$. Let $\langle\cdot,\cdot\rangle$ be the canonical height pairing, and $H(b) = \langle b, b\rangle$, for $b \in E(\mathbb{Q})$.

Lemma 2.6.1 ([11], Lemma 13). *The number of t-tuples $(n_1, \ldots, n_t)$ satisfying*

$$H(n_1a_1 + \cdots + n_ta_t) \leq x$$

is

$$\frac{(\pi x)^{t/2}}{\sqrt{R}\Gamma\left(\frac{t}{2}+1\right)} + \mathrm{O}(x^{(t-1)/2+\epsilon}),$$

where $R = \det(\langle a_i, a_j \rangle) > 0$

The following lemma has a Drinfeld module analogue given in [1, Proposition 5.1].

Lemma 2.6.2 ([11], Lemma 14). *The number of primes p satisfying $|\Gamma_p| \leq y$ is $\mathrm{O}(y^{(t+2)/t})$.*

Consider the extensions $K_q^\Gamma = \mathbb{Q}(E[q], q^{-1}a_1, \ldots, q^{-1}a_t)$. These extensions are Galois over $\mathbb{Q}$ and their Galois group is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{F}_q) \rtimes E[q]^t$. In [25],[26], Ribet showed that for almost all q, the group $\mathrm{Gal}(K_q^\Gamma/\mathbb{Q}(E[q]))$ is isomorphic to $E[q]^t$ under the map

$$(b_1, \ldots, b_t) \mapsto \{(q^{-1}a_1, \ldots, q^{-1}a_t) \to (q^{-1}a_1 + b_1, \ldots, q^{-1}a_t + b_t)\},$$

for $(b_1, \ldots, b_t) \in E[q]^t$. So each $\sigma \in \mathrm{Gal}(K_q^\Gamma/\mathbb{Q})$ can be written as (γ, χ) where $\gamma \in \mathrm{GL}_2(\mathbb{F}_q)$ and $\chi \in E[q]^t$. Denote by $\chi(\Gamma)$ the subgroup of $E[q]$ generated by the coordinates of χ.

Lang and Trotter also proved the following result.

Lemma 2.6.3 ([20], p. 291). *Let $\mathscr{C}_q$ consist of elements $\sigma = (\gamma, \chi)$ of $\mathrm{Gal}(K_q^\Gamma/\mathbb{Q})$ such that*

1. $\ker(\gamma - 1) = E[q]$ *and* $\mathrm{rank}(\chi(\Gamma)) = 0$ *or* 1
2. $\ker(\gamma - 1)$ *is a non-trivial cyclic group and* $\chi(\Gamma) \subset \mathrm{Im}(\gamma - 1)$.

For $p \nmid q\Delta$, we have $q \mid [E(\mathbb{F}_p) : \Gamma_p]$ if and only if $\sigma_p \in \mathscr{C}_q$ where σ_p denotes the Frobenius element of p in $\mathrm{Gal}(K_q^\Gamma/\mathbb{Q})$.

As before, the number of primes p such that $p \mid [E(\mathbb{F}_p) : \Gamma_p]$ are at most $\mathrm{o}(x/\log x)$.

For s square-free, let

$$K_s^\Gamma = \prod_{q|s} K_q^\Gamma.$$

Let $\mathscr{C}_s$ be the conjugacy class of K_s^Γ determined by the $\mathscr{C}_q$'s, and let $\pi(x,s)$ be the number of primes $p \leq x$ such that $\sigma_p(K_s^\Gamma/\mathbb{Q}) \in \mathscr{C}_s$, let $G_s = \mathrm{Gal}(K_s^\Gamma/\mathbb{Q})$. Let

$$\delta(s) = \frac{|\mathscr{C}_s|}{|G_s|}.$$

Proposition 2.6.1 ([11], p. 35)**.** *We have that* $\delta(s) = \mathrm{O}(s^{-t-1})$.

Let T_y denote the primes less than or equal to y, T the set of all primes and T_y^*, T^* the square-free products of elements of T_y and T respectively. Define $N_\Gamma(x,y)$, $N_\Gamma(x)$ and $M_\Gamma(y,2x)$ analogously to $N(x,y)$, $N_a(x)$ and $M(x,y)$ respectively.

Proposition 2.6.2 ([11], p. 36)**.** *We have that*

$$N_\Gamma(x) = N_\Gamma(x,y) + \mathrm{O}(M_\Gamma(y,2x)).$$

Proposition 2.6.3 ([11], p. 36)**.** *Choose* $y = (\frac{1}{4}\log x)^{1/(t+2)}$. *For some* $\epsilon > 0$, *we get*

$$N_\Gamma(x,y) = \sum_{s \in T_y^*} \mu(s)\delta(s)\,\mathrm{li}(x) + \mathrm{O}(x^{1-\epsilon}).$$

Proposition 2.6.4 ([11], p. 36)**.** *The infinite sum*

$$\delta_E(\Gamma) = \sum_s \mu(s)\delta(s),$$

is absolutely convergent.

Let

$$V_q^{(i)} = \mathbb{Q}(E[q], q^{-1}a_i),$$

and notice that $\sigma_p(K_q^\Gamma/\mathbb{Q})$ must satisfy the Lang-Trotter condition as before. The restriction of $\mathscr{C}_q$ to $V_q^{(i)}$ is of size $\mathrm{O}(q^4)$ for all i.

Proposition 2.6.5 ([11], p. 37)**.** *Let*

$$\alpha = \frac{1}{10}\log x - \frac{2}{5}\log\log x.$$

Then,

$$M_\Gamma(y, x^\alpha) = \mathrm{o}(x/\log x).$$

Using **Lemma 2.6.2** we can get the following bound.

Proposition 2.6.6 ([11], p. 37). *If $t \geq 18$ and A is large enough, we get*

$$M_\Gamma(x^\alpha \log^A x, 2x) = \mathrm{o}(x/\log x).$$

Using a Brun-Titchmarsh theorem again, we can obtain the following proposition.

Proposition 2.6.7 ([11], p. 37). *We have that*

$$M_\Gamma(x^\alpha, x^\alpha \log^A x) = \mathrm{o}(x/\log x),$$

Therefore, assuming the GRH,

$$N_\Gamma(x) = \delta_E(\Gamma)x/\log x + \mathrm{o}(x/\log x),$$

if $t \geq 18$.

2.7 Density calculation

A quick note on the density $\delta_E(\Gamma)$. If we take "Serre curves" for E, and Γ such that for $l \neq 2$ the natural map $\Gamma/l\Gamma \to E(\mathbb{Q})/lE(\mathbb{Q})$ is injective, then $\delta_E(\Gamma) > 0$, since $\delta_E(\Gamma) = \delta_1 - \delta(2)\delta_1 = (1-\delta(2))\delta_1$, and δ_1 has an Euler product, and $\delta(2) \neq 1$. This works, because the curves satisfy $\mathrm{Gal}(K_q^\Gamma/\mathbb{Q}) \cong E[q]^t \rtimes \mathrm{GL}_2(\mathbb{F}_q)$ for $q \neq 2$ and $K_2^\Gamma \neq \mathbb{Q}$. If we can find a curve satisfying the above and Γ with $\mathrm{rank}(\Gamma) \geq 18$, then we will have an example for which to apply [11, Theorem 3].

Now, let us calculate the density $\delta = \sum \mu(\mathfrak{a})\mu(s)n(\mathfrak{a}, s)^{-1}$.

Lemma 2.7.1 ([11], Lemma 11). *Let $\mathfrak{a} = \mathfrak{a}_1\mathfrak{b}$ and $s = s_1 b$ where $(\mathfrak{a}_1, 6\Delta) = (s_1, 6\Delta) = 1$ and $\mathfrak{b}, b \mid 6\Delta$. Then*

$$n(\mathfrak{a}, s) = n(\mathfrak{a}_1, s_1)n(\mathfrak{b}, b).$$

Now,

$$\delta = \sum_{\substack{\mathfrak{a}_1, s_1 (\mathfrak{a}_1, 6\Delta) = (s_1, 6\Delta) = 1 \\ \mathfrak{b}, b \mid 6\Delta}} \frac{\mu(\mathfrak{a}_1)\mu(s_1)}{n(\mathfrak{a}_1, s_1)} \cdot \frac{\mu(\mathfrak{b})\mu(b)}{n(\mathfrak{b}, b)},$$

So that,

$$\delta = \sum_{\mathfrak{b}, b \mid 6\Delta} \frac{\mu(\mathfrak{b})\mu(b)}{n(\mathfrak{b}, b)} \cdot \sum_{\mathfrak{a}_1, s_1} \frac{\mu(\mathfrak{a}_1)\mu(s_1)}{n(\mathfrak{a}_1, s_1} = \delta_0\delta_1.$$

Let us now see that $\delta_1 > 0$.

$$\begin{aligned}\delta_1 &= \sum_{\mathfrak{a}_1, s_1} \frac{\mu(\mathfrak{a}_1)\mu(s_1)}{n(\mathfrak{a}_1)m(s_1)} \cdot \varphi(\mathfrak{a}_1, s_1) \\ &= \sum_{s_1} \frac{\mu(s_1)}{m(s_1)} \prod_{\mathfrak{q}} \left(1 - \frac{\varphi(\mathfrak{q}, s_1)}{n(\mathfrak{q})}\right).\end{aligned}$$

Now,

$$\begin{aligned}\delta_1 &= \prod_{\mathfrak{q}} \left(1 - \frac{1}{n(\mathfrak{q})}\right) \sum_{s_1} \frac{\mu(s_1)}{m(s_1)} \prod_{\mathfrak{q}|s_1} \left(1 - \frac{1}{N(\mathfrak{q})}\right) \left(1 - \frac{1}{n(\mathfrak{q})}\right)^{-1} \\ &= \prod_{\substack{q \text{inert in } k \\ (q,6\Delta)=1}} \left(1 - \frac{1}{q^2 - 1}\right) \\ &\cdot \prod_{\substack{q \text{ splits in } k \\ (q,6\Delta)=1}} \left(1 - \frac{2}{q(q-1)} - \frac{1}{(q-1)^2} + \frac{2}{q(q-1)^2}\right).\end{aligned}$$

In fact, we have to replace the above factor by $(1 - (q-1)^{-1})^2$ for the finitely many q such that $q^{-1}a \in E(\mathbb{Q})$. In any case, it is now clear that $\delta_1 > 0$.

We note that δ_0 represents the density of primes π_p which do not split completely in any $K^a_{\mathfrak{b},b}$, $\mathfrak{b}, b \mid 6\Delta$. Now consider the density θ of primes $\mathfrak{p}$ which do not split completely in any K_q or $k(E[\mathfrak{q}])$ for $\mathfrak{q}, q \mid 6\Delta$. Then $\delta_0 \geq \theta$. Class field theory will imply that if 2 and 3 are inert in k then $\theta > 0$ (this works for $k = \mathbb{Q}(\sqrt{-19}), \mathbb{Q}(\sqrt{-43}), \mathbb{Q}(\sqrt{-67}), \mathbb{Q}(\sqrt{-163})$). If $k = \mathbb{Q}(\sqrt{-11}), \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-2})$, then we must work harder to see when $\theta > 0$.

Chapter 3

Function Fields and Drinfeld Modules

In this chapter, we explore some of the basic properties of function fields and Drinfeld modules. Drinfeld modules are a function field analogue of the multiplicative group of $\mathbb{C}$ and elliptic curves with complex multiplication. That is, the torsion points of $\mathbb{C}^*$ tell us a lot about the class field theory of the rational numbers. The torsion points of an elliptic curve with complex multiplication can tell us about the class field theory of a particular quadratic imaginary extension of the rational numbers. For function fields, we know the class field theory explicitly for all function fields, just like we know it for $\mathbb{Q}$ and k a quadratic imaginary extension of $\mathbb{Q}$. This theory was first developed by Hayes [13] and Drinfeld [6] independently, using what are now known as Drinfeld modules.

This important discovery illustrates a connection between the arithmetic of function fields and classical groups such as the multiplicative group of the rational numbers and an elliptic curve defined over the rational numbers.

3.1 Number theory in function fields

Let F be a field such that $\mathbb{F}_r \subset F$ and $F \cap \overline{\mathbb{F}_r} = \mathbb{F}_r$, where $\overline{\mathbb{F}_r}$ is an algebraic closure of $\mathbb{F}_r$. Let $y \in F$ be a non-constant, that is $y \notin \mathbb{F}_r$. If $[F : \mathbb{F}_r(y)]$ is finite, then we say that F is a global function field. In other words, a global function field is a field of transcendence degree one over $\mathbb{F}_p$ with constant field $\mathbb{F}_r$. Here r is a power of $p = \mathrm{Char}(F)$.

A prime ℓ of F is defined to be a pair (O_ℓ, R_ℓ) where $O_\ell \subset F$ is a discrete valuation ring and R_ℓ its maximal ideal such that the field of fractions of O_ℓ is F. Equivalently, we may associate to ℓ a surjective homomorphism $v_\ell : F^* \to \mathbb{Z}$ such that $v_\ell(x+y) \geq \inf(v_\ell(x), v_\ell(y))$ for all $x, y \in F^*$. With v_ℓ in hand, we set $O_\ell = \{x \in F \mid v_\ell(x) \geq 0\} \cup \{0\}$ and $R_\ell = \{x \in F \mid v_\ell(x) > 0\} \cup \{0\}$. The homomorphism v_ℓ is called a valuation. For convenience, we sometimes use the convention that $v_\ell(0) = \infty$. Given a valuation v on F, we may form a (normalized) absolute value $|\cdot|_v$ by the rule

$$|x|_v = r^{-v(x)}.$$

We need to briefly mention some algebraic geometry. We can then discuss the Riemann-Roch theorem. See [27, Chapters 2 and 5]. For a prime ℓ, we set $\deg \ell = [O_\ell/R_\ell : \mathbb{F}_r]$. A divisor of F is a formal sum

$$D = \sum_{\ell \text{ prime}} n_\ell \cdot \ell,$$

where $n_\ell \in \mathbb{Z}$, and all but finitely many $n_\ell = 0$. The degree of D is

$$\deg D = \sum_{\ell \text{ prime}} n_\ell \cdot \deg \ell.$$

Further, set $v_\ell(D) = n_\ell$.

For $x \in F$, define $\operatorname{div}(x)$ by the formula

$$\operatorname{div}(x) = \sum_{\ell \text{ prime}} v_\ell(x) \cdot \ell,$$

which is well-defined, see [27] for details.

Also, note that $\operatorname{div}(x) = 0$ if and only if $x \in \mathbb{F}_r$.

For a divisor D of F, define an $\mathbb{F}_r$-vector space $L(D)$ by the following

$$L(D) = \{x \in F \mid v_\ell(\operatorname{div}(x) + D) \geq 0 \text{ for all primes } \ell\} \cup \{0\},.$$

Let $l(D) = [L(D) : \mathbb{F}_r]$, which is finite.

Now let us state the Riemann-Roch theorem. A divisor class of F is an equivalence class of divisors, under the equivalence that $D' \equiv D$ if $D - D' = \operatorname{div}(y)$ for some $y \in F$.

Theorem 3.1.1 ([27], Theorem 5.4, Riemann-Roch Theorem)**.** *There exists a divisor class $\mathfrak{C}$, called the canonical divisor class and a non-negative integer g, called the genus, such* *that for any divisor A of F and $C \in \mathfrak{C}$, we have*

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

The Riemann-Roch theorem allows one to prove the following two results. Again, see [27, Chapter 5] for more details. Let h_F be the number of divisor classes of degree 0. Then h_F is finite if F is a global function field. Let a_N be the number of primes of F of degree N, then

$$a_N = \frac{r^N}{N} + \mathrm{O}\left(\frac{r^{N/2}}{N}\right).$$

The fields F as above are seen to be analogous to number fields. If we take $F = \mathbb{F}_r(T)$ for an indeterminate T, then F is similar to the rational numbers. The integers are analogous to the ring $A = \mathbb{F}_q[T] \subset F$. In general, let us fix a rational prime ∞ of F. Actually, the prime ∞ need not be rational, but it simplifies things a bit, and we will not need to consider the case where ∞ is not rational in this thesis. Let $A \subset F$ be defined by

$$A = \{x \in F \mid v_\ell(x) \geq 0 \text{ for all } \ell \text{ such that } \ell \neq \infty\}.$$

Let A be the ring of functions of F that are regular everywhere except possibly ∞. The units of A are exactly equal to $\mathbb{F}_r^*$. The prime ∞ is called the infinite prime of F; all others are called finite primes. For a divisor D of F, set D_0 to be the divisor such that $v_\ell(D_0) = v_\ell(D)$ for all $\ell \neq \infty$ and $v_\infty(D_0) = 0$.

For $f \in A$, set $\deg f = [A/f : \mathbb{F}_r]$. Then because ∞ is rational $\deg f = \deg(\mathrm{div}(f))_0$. Finite primes ℓ of F are in one to one correspondence with prime ideals of A.

Example 3.1.1. *Let $A = \mathbb{F}_r[T]$ and $F = \mathbb{F}_r(T)$, for an indeterminate T.*

Example 3.1.2. *Let $F = \mathbb{F}_r(x)[y]/(y^2 - f(x))$, where $\deg f = n \geq 3$ and f has n distinct roots, and $2 \nmid r, \deg f$. In this case, the Dedekind domain $A = \mathbb{F}_r[x, y]$ is a suitable choice. In this case, the field F is a quadratic extension of $\mathbb{F}_r(x)$ and the integral closure of $\mathbb{F}_r[x]$ in F is A.*

We may think of $\mathbb{F}_r[T]$ as the function field version of $\mathbb{Z}$. The second example we may think of being like the ring of integers of a quadratic imaginary extension of $\mathbb{Q}$. In this way, we get many good candidates for complex multiplication. These two examples will give many examples of Drinfeld modules for which we may apply our theorems, yet they are relatively uncomplicated.

3.2 Additive polynomials

Let L be a field of characteristic p. Let $f(x) \in L[x]$ be a polynomial in one variable over L. We say $f(x)$ is additive if $f(a+b) = f(a) + f(b)$ for all $a, b \in L$. The set of additive polynomials of L is a ring, where addition is given by addition of polynomials and multiplication is given by $(f \cdot g)(x) = f(g(x))$.

Let $\tau_p \in L[x]$ be the polynomial x^p. Then τ_p is an additive polynomial, and it generates a subring of the ring of additive polynomials, which we denote by $L\{\tau_p\}$. If L is a finite field, then this ring is not the full ring of additive polynomials. For example, take $g(x) = (x^p - x)^n$ for a non-negative integer n. Then g is additive but g is not always in $L\{\tau_p\}$. Let $\overline{L}$ be an algebraic closure of L. We say that $f \in L[x]$ is absolutely additive if $f(a+b) = f(a) + f(b)$ for all $a, b \in \overline{L}$.

Proposition 3.2.1 ([10], Proposition 1.1.5)**.** *Let L be a field with infinitely many elements. Then the ring of additive polynomials of L is equal to $L\{\tau_p\}$.*

Thus, the ring of absolutely additive polynomials of L is equal to $L\{\tau_p\}$ for any L of characteristic p. If L is infinite, the notions of absolutely additive and additive coincide. From now on, we only consider absolutely additive polynomials (even if L is finite).

Now suppose that $\mathbb{F}_r \subset L$. Let τ be the map $x \to x^r$. Then the subring of $L\{\tau_p\}$ generated by τ consists of polynomials which are $\mathbb{F}_r$-linear. This is because $\tau a = a^r \tau$ for $a \in L$.

Let $f \in L\{\tau\}$, then we may interpret the coefficients of f in two different ways. First, the twisted polynomial f may be represented as a polynomial in $L[x]$, in this case as

$$f(x) = a_0 x + a_1 x^r + a_2 x^{r^2} + \cdots + a_n x^{r^n},$$

so that $\deg f = r^n$ for some integer n. If we represent f in this way, we will write $f(x)$. Secondly, we may represent f as a polynomial in $L\{\tau\}$, in which case write

$$f(\tau) = a_0 \tau^0 + a_1 \tau + \cdots + a_n \tau^n.$$

If we think of it this way, then we will write $\deg_\tau(f) = n$, so that $\deg f = r^{\deg_\tau(f)}$.

Proposition 3.2.2 ([10], Theorem 1.2.1)**.** *Let $f(x)$ be a separable polynomial. Then f is absolutely additive if and only if the zeroes of f form a subgroup of $\overline{L}$. Further, we have that f is $\mathbb{F}_r$-linear if and only if the zeroes of f form an $\mathbb{F}_r$-subspace of $\overline{L}$.*

Let us study the polynomials f_W further [10, Section 1.3]. We want to describe how the polynomial f_W behaves when replacing W by $\mathbb{F}_r$ subspaces. To do this we will use the Moore determinant, which is a τ version of the classical Vandermonde determinant. In particular, Goss [10, p. 9] says "It would be amusing to know the mechanics of transforming the computation of the Moore determinant (i.e., Corollary 1.3.7) into the usual Vandermonde computation." We give the computation in this way.

Define a vector $v(x)$ by $v(x) = (1, x, x^2, \ldots, x^{n-1})^t$, where v^t means the transpose of the vector v. Define

$$A(x_1, \ldots, x_n) = (v(x_1), \ldots, v(x_n)).$$

Then

$$\det(A(x_1, \ldots, x_n)) = \prod_{j<i}(x_i - x_j).$$

For now, let us consider $W \subset L$, a field with $\mathbb{F}_r \subset L$, and W a $\mathbb{F}_r$ subspace of L.

Lemma 3.2.1 ([10], Lemma 1.3.1)**.** *Let $\{w_1, \ldots, w_n\} \subset W$. The set $\{w_1, \ldots, w_n\}$ is linearly independent over $\mathbb{F}_r$ if and only if, for every $i \geq 0$, the set*

$$\{\tau^i(w_1), \ldots, \tau^i(w_n)\}$$

is also linearly independent over $\mathbb{F}_r$.

We now define a determinant which should tell us when a set is linearly independent over $\mathbb{F}_r$.

Definition 3.2.1. *Set*

$$\begin{aligned}
\Delta(w_1, \ldots, w_n) &:= \Delta_r(w_1, \ldots, w_n) \\
&:= \det\begin{pmatrix} w_1 & \cdots & w_n \\ w_1^r & \cdots & w_n^r \\ \vdots & & \vdots \\ w_1^{r^{n-1}} & \cdots & w_n^{r^{n-1}} \end{pmatrix} \\
&= \det\begin{pmatrix} \tau^0(w_1) & \cdots & \tau^0(w_n) \\ \vdots & & \vdots \\ \tau^{n-1}(w_1) & \cdots & \tau^{n-1}(w_n) \end{pmatrix}.
\end{aligned}$$

We call $\Delta(w_1, \ldots, w_n)$ the Moore determinant.

Consider the ring $L\{\tau_1, \ldots, \tau_n\}$ where $\tau_i(x_1, \ldots, x_n) = \tau(x_i)$ for indeterminates $x_1, \ldots$. Then $\tau_i\tau_j = \tau_j\tau_i$ and $\tau_j\alpha = \alpha^r\tau_j$. The Vandermonde determinant above has coefficients in $\mathbb{F}_r$, so the Moore determinant satisfies

$$\Delta(x_1, \ldots, x_n) = V(\tau_1, \ldots, \tau_n)(x_1, \ldots, x_n).$$

We therefore have the identity

$$\Delta(x_1, \ldots, x_n) = \left(\prod_{i<j}(\tau_i - \tau_j)\right)(x_1, \ldots, x_n).$$

To study the Moore determinant in terms of the Vandermonde determinant, let us define maps $\tau_i : L^m \to L$ by $\tau_i(x_1, \ldots, x_m) = x_i^r$. Then the pointwise product gives us a ring $L\{\tau_1, \ldots, \tau_m\}$ of additive polynomials from L^m to L, and the τ_i's commute with each other. Also, we have that $L\{\tau_i\} \subset L\{\tau_1, \ldots, \tau_m\}$ is a copy of $L\{\tau\}$. Now, the Moore determinant can be thought of as

$$\det(\tau_i^{j-1}(\vec{x})_{1\leq i,j\leq m})$$

Now, the regular Vandermonde matrix will give us that this determinant is equal to (because the τ_i's commute).

$$\prod_{i<j}(\tau_i - \tau_j),$$

which defines an additive function from k^m to k. In fact it is $\mathbb{F}_r$-linear.

We have that $\Delta(x_1, \ldots, x_m, x_{m+1}) = (\prod_{i=1}^m(\tau_{m+1} - \tau_i))\Delta(x_1, \ldots, x_m)$. Using this form we can prove that if $\{w_1, \ldots, w_m\}$ is a basis of some subspace W of L, over $\mathbb{F}_r$ then $\Delta(w_1, \ldots, w_m, x)$ is an additive polynomial of degree r^m. But r^m different roots of the polynomial are given by $\alpha_1 w_1 + \cdots + \alpha_m w_m$ (this is easy to check). Let

$$f_W(x) = \prod_{w\in W}(x - w).$$

Thus, we have the equality $\Delta(w_1, \ldots, w_m, x) = f_W(x)c$ for some constant c. Now f_W is monic and the leading term of $\Delta(w_1, \ldots, w_m, x)$ is $\Delta(w_1, \ldots, w_m)$. Now, this implies that $\Delta(w_1, \ldots, w_m) = 0$ if and only if $w_1, \ldots, w_m$ are linearly dependent vectors over $\mathbb{F}_r$.

We will use the following proposition later.

Proposition 3.2.3 ([10], Proposition 1.3.5 part 3)**.** *Let W be a finite dimensional $\mathbb{F}_r$*

subspace of L. Let $\{w_1, \ldots, w_m\}$ be a basis of W, and set W_i be the span of $\{w_1, \ldots, w_i\}$ over $\mathbb{F}_r$. Let $f_{W_i} = \prod_{w \in W_i}(x-w)$, and $f_W = f_{W_m}$. Let $\overline{W_i}$ be the span of $f_{W_i}(w_{i+1}), \ldots, f_{W_i}(w_m)$. Then

$$f_W(\tau) = f_{\overline{W_i}}(\tau) f_{W_i}(\tau).$$

Proof. Both polynomials have the same set of roots, as well as the same leading term. □

Definition 3.2.2. *Let $f, g \in L\{\tau\}$.*

1. *We say that $f(\tau)$ is right divisible by $g(\tau)$ if there exists $h(\tau) \in L\{\tau\}$ such that $f(\tau) = h(\tau) \cdot g(\tau)$.*
2. *We say that $f(\tau)$ is left divisible by $g(\tau)$ if there exists $h(\tau) \in L\{\tau\}$ such that $f(\tau) = g(\tau)h(\tau)$.*

Proposition 3.2.4 ([10], Proposition 1.6.2)**.** *Let $f, g \in L\{\tau\}$ with $g(\tau) \neq 0$. Then there exists $h, r \in L\{\tau\}$ such that $\deg_\tau r < \deg_\tau g$ and*

$$f(\tau) = h(\tau)g(\tau) + r(\tau).$$

Moreover, the polynomials h and r are uniquely determined.

Proof. Proceed just as in the classical division algorithm for polynomials. □

Corollary 3.2.1 ([10], Corollary 1.6.3)**.** *Every left ideal of $L\{\tau\}$ is principal.*

Definition 3.2.3. *We say that L is perfect if and only if $\tau(L) = L$.*

Proposition 3.2.5 ([10], Proposition 1.6.5)**.** *Let L be perfect and let $f, g \in L\{\tau\}$ with $g \neq 0$. Then there exists $h, r \in L\{\tau\}$ with $\deg_\tau r < \deg_\tau g$ and*

$$f(\tau) = g(\tau) \cdot h(\tau) + r(\tau).$$

Further, the polynomials h and r are uniquely determined.

Proof. The perfectness of L allows us to solve for h in the usual way. □

Corollary 3.2.2 ([10], Corollary 1.6.5)**.** *If L is perfect, then every right ideal of $L\{\tau\}$ is principal.*

Definition 3.2.4. *Let $f, g \in L\{\tau\}$. The left ideal generated by f, g has a monic generator $(f(\tau), g(\tau)) \in L\{\tau\}$, called the greatest common divisor of f and g.*

3.3 Valued fields and Newton polygons

For a global function field F and valuation v_ℓ of F, it is often useful to consider the completion of F at v_ℓ, denoted by F_ℓ. In this section, we provide a brief overview of non-archimedean analysis. We want to focus on the theory of Newton polygons, taken from [10].

Let L be a field of characteristic p, equipped with a (non-archimedean) valuation v such that L is complete with respect to v. Let $O_v = \{x \in L \mid v(x) \geq 0\} \cup \{0\}$ and $R_v = \{x \in L \mid v(x) > 0\} \cup \{0\}$. Now assume that O_v/R_v is a finite field with $\#O_v/R_v = r$. We define an absolute value $|\cdot|$ on L by $|x| = r^{-v(x)}$, for $0 \neq x \in L$ and $|0| = 0$. Set $v(0) = \infty$.

If L'/L is any finite extension of L, we may define a unique extension of v to L' by the following formula

$$v(x) = \frac{1}{[L' : L]} v(N_L^{L'}(x)).$$

In this way, we may extend the valuation v to a fixed algebraic closure $\overline{L}$ of L.

Proposition 3.3.1 ([10], Proposition 2.1)**.** *Let $\overline{L}$ be a fixed algebraic closure of L together with the canonical extension of v. Let $\hat{\overline{L}}$ be its completion with respect to v. Then $\hat{\overline{L}}$ remains algebraically closed.*

Let $\{a_j\}_{j\geq 0}$ be a sequence in L. For the infinite sum $\sum_{j\geq 0} a_j$, we define the Nth partial sum as $S_N = \sum_{j=0}^{N} a_j$, and we say the sum $\sum_{j\geq 0} a_j$ converges if $\lim_{N\to\infty} S_N$ exists and equals S. We then put $\sum_{j\geq 0} a_j = S$.

Proposition 3.3.2 ([10], Proposition 2.2)**.** *The infinite sum $\sum_{j\geq 0} a_j$ converges to an element of L if and only if $\lim_{j\to\infty} a_j = 0$.*

Proof. The "only if" is just like the proof from calculus. The "if" part follows because $|S_n| \leq \max |a_i| \to 0$. □

Until the end of this section assume that L is complete and algebraically closed.

Now, let us consider the power series $f(x) = \sum_{j\geq 0} a_j x^j$. Then f converges at $x = \alpha$ if and only if

$$\lim_{j\to\infty} a_j x^j = 0,$$

or in terms of v,

$$\lim_{j\to\infty} v(a_j) + jv(x) = \infty.$$

Definition 3.3.1. *Let*

$$\rho(f) = -\lim_{j\to\infty} v(a_j)/j.$$

The limit $\rho(f)$ is called the order of convergence of f.

Proposition 3.3.3 ([10], Proposition 2.4)**.** *Let $\alpha \in L$. Then f converges at α if $v(\alpha) > \rho(f)$ and diverges at α if $v(\alpha) < \rho(f)$.*

Definition 3.3.2. *Let $f(x) = \sum_{j\geq 0} a_j x^j \in L[[x]]$. Let $S = \bigcup_{i\geq 0} A_i$, where $A_i = \{(i, y) \subset \mathbb{R}^2 \mid y \geq v(a_i)\}$. The Newton polygon of f is defined to be the convex hull of S.*

Proposition 3.3.4 ([10], Proposition 2.8)**.** *Let $\{m_i\}$ be the sequence of slopes of the Newton polygon of $f(x) = \sum_{j\geq 0} a_j x^j$. Then $\{m_i\}$ is monotonically increasing and*

$$-\lim_{i\to\infty} m_i = \rho(f).$$

Proposition 3.3.5 ([10], Proposition 2.9)**.** *Let $t > \rho(f)$. There are two possibilities.*

1. *If no side of the Newton Polygon of $f(x)$ has slope $-t$, then there are no zeroes of $f(x)$ on the circle $v(x) = t$.*

2. *If the Newton Polygon of $f(x)$ has a side with slope $-t$, then $f(x)$ has exactly m zeroes on $v(x) = t$.*

Here, the number m refers to the length of the projection of the side of the Newton polygon of slope $-t$ onto the x-axis.

Definition 3.3.3. *We say that $f(x) = \sum_{j\geq 0} a_j x^j$ is entire if it converges for all $x \in L$, or equivalently if $\rho(f) = -\infty$.*

Proposition 3.3.6 ([10], Proposition 2.13)**.** *If f is an entire function with no zeroes, then f is constant.*

Proof. This follows from looking at the Newton polygon of f (if f is non-trivial, then there is a non-trivial side of the Newton polygon). □

Theorem 3.3.1 ([10], Theorem 2.14). *Let $f(x)$ be an entire function and let*

$$\{\lambda_1, \ldots, \lambda_t, \ldots\}$$

be its non-zero roots in L. Then

$$\lim_{t\to\infty} v(\lambda_t) = -\infty,$$

and

$$f(x) = cx^n \prod_t (1 - x/\lambda_t),$$

where $n = \mathrm{ord}_{x=0}(f)$.

Conversely, if $\{\lambda_t\}$ is as above and $c \in L$, then the above product defines an entire function.

Proof. The above product defines an entire function. If f is an entire function not equal to the above product, then the quotient defines a non-constant entire function with no zeroes, a contradiction. □

3.4 Drinfeld modules

Let F be a global function field, with fixed rational prime ∞, and A the ring of functions of F regular everywhere except possibly ∞.

A field K equipped with an $\mathbb{F}_r$-homomorphism $i : A \to K$ is called an A-field. In particular, the field K has characteristic p. As any A-field has the same characteristic, we say that $\ker(i) \subset A$ is the characteristic of K as an A-field. If $\ker(i) = 0$, then K has generic characteristic, otherwise it has finite characteristic.

Example 3.4.1. *Let $A = \mathbb{F}_r[T]$ and let K be any field containing A. By setting $i : A \to K$ to be the injection map, we make K into an A-field of generic characteristic. That is, we have $\ker(i) = 0$.*

Example 3.4.2. *Let $A = \mathbb{F}_r[T]$ and let $K = \mathbb{F}_{r^n}$. Let P be a monic irreducible of A of degree n. Then $i : A \to K$ given by $x \to x \pmod{P}$ turns $\mathbb{F}_{r^n}$ into an A-field with finite characteristic. Further, we have $\ker(i) = (P)$.*

Recall that $K\{\tau\}$ is the ring of (absolutely) $\mathbb{F}_q$-linear polynomials over K. For each $f \in K\{\tau\}$, write $f = \tau^0 a_0 + \cdots + \tau^n a_n$, set $D(f) = a_0$.

Definition 3.4.1. *A Drinfeld module defined over K is an $\mathbb{F}_q$-linear homomorphism $\phi : A \to K\{\tau\}$ such that*

1. *$D(\phi_x) = i(x)$ for all $x \in A$, and*
2. *$\phi_x \neq i(x)\tau^0$ for some $x \in A$.*

From now on, we use the standard convention that for a Drinfeld module $\phi : A \to K\{\tau\}$, $\phi_x \in K\{\tau\}$ is the image of x under the homomorphism ϕ

Thus a Drinfeld module gives us an A-module action on the field K. In fact, any field L with $K \subset L$ becomes a Drinfeld module via ϕ, we denote this Drinfeld module by $\phi(L)$. It is often helpful to think of the A-action on K similar to the $\mathbb{Z}$ action on the points of an elliptic curve E.

3.5 Fundamental structures for Drinfeld modules

Let ϕ, ψ be two Drinfeld modules defined over K. Let $f \in K\{\tau\}$. We say that f is a morphism from ϕ to ψ if $f \cdot \phi_a = \psi_a \cdot f$, as polynomials in $K\{\tau\}$, for all $a \in A$. Non-zero morphisms are called isogenies.

Let I be an ideal of A. Let $\overline{K}$ be a fixed algebraic closure of K. The I-torsion of ϕ is given by

$$\phi[I] = \{x \in \overline{K} \mid \phi_a(x) = 0 \text{ for all } a \in I\}.$$

Let $I^{h_A} = (a)$, where h_A is the class number of F. Then $\phi[I]$ is a subset of the zeroes of ϕ_a, which is a finite set. Therefore, the torsion $\phi[I]$ is a finite $\mathbb{F}_q$ vector space, and so is the zero set of a monic, $\mathbb{F}_q$-linear polynomial, say $\phi_I \in K\{\tau\}$. For $a \in A$, define $\phi[a] = \phi[(a)]$. To compute ϕ_I, write $I = (i_1, i_2)$ (because A is Dedekind). Then set ϕ_I to be the monic generator of the left ideal of $K\{\tau\}$ generated by ϕ_{i_1} and ϕ_{i_2}. This works because $K\{\tau\}$ has a right division algorithm.

In the theory of elliptic curves, the kernel of the multiplication by n map has a very strict structure. We will see that this is true for Drinfeld modules as well. Recall that if E/K is an elliptic curve with n coprime to $\mathrm{Char}(K)$, we have

$$E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2.$$

Proposition 3.5.1 ([10], Proposition 4.5.3)**.** *There is a positive integer d such that if an ideal I is coprime to the characteristic of K, denoted by* $\ker(i)$*, we have that $\phi[I] \cong (A/I)^d$.*

Definition 3.5.1. *The positive integer d appearing above is called the* rank *of the Drinfeld module ϕ.*

It remains to deal with the case that $\ker(i) = \mathfrak{p} \neq 0$.

Proposition 3.5.2 ([10], Proposition 4.5.7)**.** *Suppose that* $\ker(i) \neq 0$*, then there exists a positive integer h such that*

$$\phi[\mathfrak{p}^j] \cong (A/\mathfrak{p}^j)^{d-h}.$$

Definition 3.5.2. *The positive integer d appearing in the above propositions is called the* rank *of the Drinfeld module ϕ. If* $\ker(i) \neq 0$*, then the positive integer h is called the height of ϕ, otherwise ϕ is said to have height $h = 0$.*

Definition 3.5.3. *Let ϕ, ψ be two Drinfeld modules over K. If $f \in K\{\tau\}$ satisfies*

$$f\phi_a = \psi_a f.$$

then we say that f is a morphism from ϕ to ψ defined over K.

If f is non-zero then ϕ and ψ must have the same rank, say d. Let the set of all such morphisms be denoted $\mathrm{Hom}_K(\phi, \psi)$. If $\phi = \psi$, we denote the set $\mathrm{End}_K(\phi)$. The set of all morphisms defined over $\overline{K}$ is denoted $\mathrm{Hom}(\phi, \psi)$, and when $\phi = \psi$ we have $\mathrm{End}(\phi)$.

3.6 Complex Multiplication

The main reference for this section is [10, Chapter 4.7].

Proposition 3.6.1 ([10], Proposition 4.7.1)**.** *Let $f \in K\{\tau\}$ be a morphism from ϕ to ψ. Then f is an isomorphism if and only if* $\deg_\tau f(\tau) = 0$.

Proposition 3.6.2 ([10], Proposition 4.7.2)**.** *Let $f \in K\{\tau\}$ be a morphism from ϕ to ψ, $a \in A$, and $\alpha \in \overline{K}$ be an a-division point of ϕ. Then $f(\alpha)$ is an a-division point of ψ.*

Corollary 3.6.1 ([10], Corollary 4.7.3)**.** *Let $f \in K\{\tau\}$ be a morphism form ϕ to ψ, $I \subset A$ be an ideal, and let $\alpha \in \phi[I]$. Then $f(\alpha) \in \psi[I]$.*

Proposition 3.6.3 ([10], Proposition 4.7.4)**.** *Let $L \supset \overline{K}$ be algebraically closed. Then the natural inclusion* $\mathrm{Hom}_{\overline{K}}(\phi, \psi) \hookrightarrow \mathrm{Hom}_L(\phi, \psi)$ *is an equality.*

Proposition 3.6.4 ([10], Proposition 4.7.6)**.** *Suppose that K has generic characteristic, so that $F \subset K$. Then* $\mathrm{End}_K(\phi)$ *is commutative.*

Theorem 3.6.1 ([10], Theorem 4.7.8)**.** *The set of morphisms* $\mathrm{End}_K(\phi)$ *is a projective* A*-module of rank at most* d^2*.*

Proposition 3.6.5 ([10], Proposition 4.7.13)**.** *Let* $f : \phi \to \psi$ *be an isogeny. Then there exists an isogeny* $\hat{f} : \psi \to \phi$ *such that*

$$\hat{f}f = \phi_a,$$

for some non-zero $a \in A$*.*

Corollary 3.6.2 ([10], Corollary 4.7.14)**.** *1.* $f\hat{f} = \psi_a$*.*

2. Isogeny gives rise to an equivalence relation on Drinfeld modules over K*.*

Corollary 3.6.3 ([10], Corollary 4.7.15)**.** *The tensor product* $\mathrm{End}_K(\phi) \otimes_A F$ *is a finite dimensional division algebra over* F*.*

Corollary 3.6.4 ([10], Corollary 4.7.16)**.** *Let* $f : \phi \to \psi$ *be an isogeny. Then* $\mathrm{End}_K(\phi)$ *and* $\mathrm{End}_K(\psi)$ *have the same rank as* A*-modules.*

Proposition 3.6.6 ([10], Proposition 4.7.17)**.** *The tensor product* $\mathrm{End}_K(\phi) \otimes_A F_\infty$ *is a finite dimensional division algebra over* F_∞*.*

Let L be a field containing F. Let $O \subset L$ be an order above A. That is, the field of fractions of O is equal to L, all elements of O are integral over A and O contains A. Let $\tilde{O}$ be the ring of A integers. The conductor of O, denoted by $\mathfrak{c}$, is the largest ideal of $\tilde{O}$ which is also an ideal of O.

Proposition 3.6.7 ([10], Proposition 4.7.19)**.** *Let* K *be an* A*-field and* ϕ *a Drinfeld module over* K*. Let* O *inject into* $\mathrm{End}_K(\phi)$ *over* A*. Then there is a Drinfeld module* ψ *over* K *which is isogenous to* ϕ *and such that* $\tilde{O} \cong \mathrm{End}_K(\psi)$*.*

3.7 Reduction of Drinfeld modules

The main reference for this section is [10, Chapter 4.10].

Let K be an A-field equipped with a non-trivial valuation v. We assume that $v(x) \geq 0$ for all $x \in A$. This is because we want to talk about reduction modulo v, and that cannot happen if v lies above ∞.

Let $O_v = \{x \in K \mid v(x) \geq 0\}$ and R_v the maximal ideal of O_v. We know that $i(A) \subset O_v$. Set $F_v = O_v/R_v$. Let ϕ be a Drinfeld module of fixed rank $d > 0$.

Definition 3.7.1. *1. We say that ϕ has integral coefficients if the coefficients of ϕ_a are in O_v for all $a \in A$ and the reduction modulo R_v of these coefficients defines a Drinfeld module of some rank d_1, where $0 < d_1 \leq d$, over F_v. Denote the reduced Drinfeld module (our notation) by $\phi(F_v)$.*

2. *We say that ϕ has stable reduction at v if there exists a Drinfeld module ψ over K with ψ isomorphic to ϕ over K and ψ has integral coefficients.*
3. *We say that ϕ has good reduction at v if it has stable reduction at v and in addition $\phi(F_v)$ has rank d.*
4. *We say that ϕ has potential stable (resp. potential good) reduction at v if there exists an extension (L, w) of (K, v) such that ϕ has stable (resp. good) reduction at w.*

Let $f(\tau) = \sum_{j=0}^{t} c_j \tau^j \in K\{\tau\}$. We set

$$v(f(\tau)) = \min\{v(c_j)/(r^j - 1) \mid j > 0\}.$$

Lemma 3.7.1 ([10], Lemma 4.10.2). *Let $u \in K^*$. Then the Drinfeld module $u\phi u^{-1}$ has integral coefficients at v if and only if*

$$v(u) = \min\{v(\phi_a) \mid a \in A \backslash \mathbb{F}_r\}.$$

Proposition 3.7.1 ([10], Proposition 4.10.3). *Let ϕ be a Drinfeld module over K as above. Then there is a natural number $e_v(\phi)$ which is prime to p such that the following two properties are equivalent for a finite extension (L, w) of (K, v):*

1. *ϕ has stable reduction at w.*
2. *The index of ramification of w over v is divisible by $e_v(\phi)$.*

In fact, we can take w to be tamely ramified over v, which is very important in different calculations.

Corollary 3.7.1 ([10], Corollary 4.10.4). *Every ϕ has potential stable reduction in a tamely ramified extension. Further if the rank of ϕ is 1, then ϕ has potential good reduction everywhere.*

Actually, we can say more about rank 1 Drinfeld modules. Let $\eta_\phi(x)$ be the leading coefficient of ϕ_x for $x \in A$.

Corollary 3.7.2 ([14], Corollary 7.4). *Suppose ψ has rank 1, and $\eta_\psi(x)$ is a unit of O_v for all $x \in A$. Then ψ has integral coefficients.*

3.8 Analytic theory

Let F_∞ be the completion of F at ∞. Let C_∞ be the completion of the algebraic closure of F_∞.

For a prime $\ell \neq \infty$, let F_ℓ be the completion of F at ℓ and C_ℓ be the completion of the algebraic closure of F_ℓ.

Let L be a complete subfield of C_∞ or C_ℓ which contains either F_ℓ or F_∞.

Theorem 3.8.1 ([10], Theorem 4.6.9)**.** *Let ϕ be a Drinfeld module over $L \subset C_\infty$ of rank $d > 0$. Then there is an L-lattice $\Lambda := \Lambda_\psi$ which is $\mathrm{Gal}(L^{\mathrm{sep}}/L)$ invariant and of rank d such that ϕ is the associated Drinfeld module to the lattice Λ. Moreover, the association $\phi \to L_\phi$ gives rise to an equivalence of categories between the category of Drinfeld modules of rank d over L and the category of L-lattices of rank d (equipped with L morphisms of L-lattices).*

Theorem 3.8.2 ([6], Proposition 7.2)**.** *The isomorphism classes of rank d Drinfeld modules defined over $L \subset C_\ell$ are in one-to-one correspondence with the isomorphism classes of pairs (ϕ, Λ), where ϕ is a Drinfeld module over L of rank d_1 ($d_1 \leq d$) with potentially good reduction, and Λ is a lattice in L of rank $d - d_1$ which is $\mathrm{Gal}(L^{\mathrm{sep}}/L)$ invariant.*

Remark 3.8.1. *The L-lattices of rank 1 are in correspondence to the set of fractional ideals of A under the equivalence $C\ D$ if $C = xD$ for some $x \in F$. Thus, the above result says that there are h_A (the class number of A) isomorphism classes of Drinfeld modules, for each isomorphism class of ideals $\mathfrak{U}$, we may associate a Drinfeld module $\phi^{\mathfrak{U}}$.*

We will first consider the exponential function of a lattice in a local non-archimedean field. Let L be a local field, with discrete valuation v. That is L is complete and locally compact with respect to v. Suppose also that $A \subset L$. Let $\hat{\bar{L}}$ be the completion of the algebraic closure of L. Suppose that $F \subset L$.

Definition 3.8.1. *Let Λ be an A-submodule of $\hat{\bar{L}}$. We say that Λ is a L lattice if there is a norm $|\cdot|$ on Λ which satisfies $|a \cdot \lambda| = r^{\deg a}|\lambda|$ for $a \in A, \lambda \in \Lambda$ and such that*

1. *Λ is finitely generated as an A-module*

2. *Λ is discrete w.r.t. the norm $|\cdot|$.*

3. *$\Lambda \subset L^{\mathrm{sep}}$ and is $\mathrm{Gal}(L^{\mathrm{sep}}/L)$ stable.*

Definition 3.8.2. *Let Λ be as above. Set*

$$e_\Lambda(x) = x \prod_{\substack{\alpha\in\Lambda \\ 0\neq\alpha}} \left(1 - \frac{x}{\alpha}\right).$$

Proposition 3.8.1 ([10], Proposition 4.2.4)**.** *The function e_Λ is entire and has a Taylor expansion around $x = 0$ with coefficients in L.*

Proof. That e_Λ is entire follows from the discreteness of Λ. Proving that the coefficients are in L results from the $\mathrm{Gal}(M^{\mathrm{sep}}/M)$ action on Λ. One can also look at e_Λ as being the limit of polynomials with coefficients in L (for example, consider a polynomial whose newton polygon approximates that of e_Λ). □

Proposition 3.8.2 ([10], Proposition 4.2.5)**.** *The function e_Λ is $\mathbb{F}_r$-linear.*

Proof. Since e_Λ is the limit of $\mathbb{F}_r$-linear polynomials, we have that e_Λ is $\mathbb{F}_r$-linear. □

Let d be the rank of Λ as a finitely generated projective A-module. Let $0 \neq a \in A$.

Theorem 3.8.3 ([10], Theorem 4.3.1)**.** *We have the following equality of entire functions*

$$e_\Lambda(ax) = ae_\Lambda(x) \prod_{0\neq\alpha\in a^{-1}\Lambda/\Lambda} (1 - e_\Lambda(x)/e_\Lambda(\alpha)).$$

Proof. Let

$$f(x) = x \prod_{0\neq\alpha\in a^{-1}\Lambda/\Lambda} (1 - x/e_\Lambda(\alpha)).$$

Then we can check that f is $\mathbb{F}_r$-linear, so $f'(x) \equiv 1$. The entire functions $af(e_\Lambda(x))$ and $e_\Lambda(ax)$ have the same roots and the same derivative, so they are equal. □

Up until now we have not specified the field L. We need the above theory for two related uses. If we set $L \subset C_\infty$, then we will be able to obtain the uniformization theory for **Theorem 3.8.1**. If we take $L \subset C$, then we can obtain the uniformization theory for **Theorem 3.8.2**. We will also return to these ideas when we review Gardeyn's paper [9], in **Chapter 4**.

3.9 Class field theory

We give an overview [14]. Also, see [10, Chapter 7],[7],[15].

First, let us determine the minimal field of definition for a rank 1 Drinfeld module. We will see that this field is an abelian extension of F, for which ∞ splits, and with Galois group equal to $\mathrm{Pic}(A)$.

Then we will develop the cyclotomic theory for sgn-normalized rank 1 Drinfeld modules, where ∞ is assumed to be rational. Notice that in this case, the sgn-normalized treatment summarised in [10, Chapter 7] corresponds to the treatment given by Hayes in [14]. If ∞ is not rational, then it is necessary to follow [10, Chapter 7] or Hayes [15]. The theory of Drinfeld modules can even be developed for O an order of A, as done by Hayes [14].

Let ϕ be a Drinfeld module $\phi : A \to C_\infty\{\tau\}$.

Definition 3.9.1. *Let K be a subfield of C_∞ containing F. We say that ϕ is defined over K or that K is a field of definition for ϕ if ϕ is isomorphic over C_∞ to a Drinfeld module $\phi' : A \to C_\infty$such that ϕ'_x has coefficients in K for every $x \in A$.*

Proposition 3.9.1 ([14], Theorem 6.6)**.** *There is a field $I(\phi)$ contained in every field of definition of ϕ. The field $I(\phi)$ is itself a field of definition for ϕ.*

Definition 3.9.2. *Let $\mathfrak{A}$ be an ideal of A. The following equation defines a Drinfeld module $(\mathfrak{A} * \phi)$:*

$$\phi_{\mathfrak{A}} \cdot \phi_x = \phi'_x \phi_{\mathfrak{A}}.$$

Corollary 3.9.1 ([14], Corollary 6.7)**.** *If B is an ideal of A, then $I(B * \phi) = I(\phi)$.*

Let ϕ be a rank 1 Drinfeld module defined over F_∞ and let H_A be the field of definition $I(\phi)$. Let σ be an automorphism of C_∞ which fixes F. Then $\sigma\phi$ defined by $(\sigma\phi)_x = \sigma(\phi_x)$ is a Drinfeld module of the same rank as ϕ. Further

$$\sigma(B * \phi) = B * (\sigma\phi).$$

Proposition 3.9.2 ([14], Proposition 8.1)**.** *The automorphism σ acts naturally on the isomorphism classes of rank d Drinfeld modules defined over C_∞, denoted by $\mathrm{Isom}_{C_\infty}(d)$. In particular, we can take $d = 1$. Further, this action commutes with that of $\mathrm{Pic}(A)$ given by the star operator.*

From now on, we are interested only in rank 1 Drinfeld modules. From now on ψ denotes a rank 1 Drinfeld module. This is because in **Chapter 4**, we will set ψ to be a rank 1 Drinfeld module which is CM for some ϕ of rank 2.

Proposition 3.9.3 ([14], Proposition 8.4)**.** *The extension H_A/F is finite and and Galois. Further, the prime ∞ splits completely in H_A.*

Proof. We know that $H_A \subset F_\infty$. Further, the field $I(\psi^B)$ remains invariant under the action of $*$, and hence it is generated by the coefficients of ψ_y^B for any choice of y non-constant and B. Therefore, H_A is finite, and any finite extension of F contained in F_∞ is separable. □

Let $G_A = \mathrm{Gal}(H_A/F)$, then we can see that G_A acts faithfully on $\mathrm{Isom}_{C_\infty}(1)$ and so G_A can be viewed as a subgroup of $\mathrm{Pic}(A)$, and is therefore abelian.

Theorem 3.9.1 ([14], Theorem 8.8)**.** *We have that the group G_A is isomorphic to* $\mathrm{Pic}(A)$*. A prime P of A splits completely in H_A/F if and only if P is principal.*

Theorem 3.9.2 ([14], Theorem 8.10)**.** *The field H_A is unramified of degree h_A over F and has field of constants $\mathbb{F}_r$.*

Definition 3.9.3. *Two Drinfeld modules ψ, ψ' defined over H_A are said to be equivalent if there exists $w \in \overline{H_A}$ such that $w^{q-1} \in H_A$ and $\psi' = w^{-1}\psi w$.*

Proposition 3.9.4 ([14], Proposition 10.4)**.** *In our setting, that is* $\deg \infty = 1$*, any rank* 1 *Drinfeld module defined over H_A is equivalent to a Drinfeld module with coefficients in O' which is the integral closure of A in H_A. Recall that a Drinfeld module has coefficients in O' if the leading coefficient of each ψ_y is in $\mathbb{F}_r = O'^{\times}$ and all other coefficients are in O'.*

Proposition 3.9.5 ([14], Proposition 10.7)**.** *Every ideal B of A generates a principal ideal in O'.*

From now on, let ψ be a Drinfeld module defined over H_A which has coefficients in O' (recall that this means that the leading coefficient of ψ_y is in $\mathbb{F}_r$ and all other coefficients are in O').

Let $G_B = \mathrm{Gal}(H_A(\psi[B])/H_A)$, then we have a natural map

$$\psi : G_B \to (A/B)^*.$$

Let $\varphi(B) = \#(A/B)^*$.

Proposition 3.9.6 ([14], Proposition 9.1)**.** *Suppose $B = P^e$, where P is a prime of A. Let $\mathfrak{P}$ be a prime of H_A which sits over P. Then $H_A(\psi[B])/H_A$ is totally ramified at $\mathfrak{P}$ and its degree equals $\varphi(B)$.*

Theorem 3.9.3 ([14], Theorem 9.2)**.** *Let B be an ideal of A. Then*

$$\Psi : \mathrm{Gal}(H_A(\psi[B])/H_A) \to (A/B)^*$$

is an isomorphism.

3.10 Drinfeld modules over global function fields

Let us define our frames of reference for the rest of the paper. We will be considering two types of Drinfeld modules of rank 2. For the first type, we have a function field F, rational point ∞ and A such that $F \subset k$ with $[k : F] = 2$, k/F separable, and ∞ ramifies in k. Further, the field of constants of k and F are equal to $\mathbb{F}_r$ and finally the characteristic of F is not equal to 2. Set O to be the integral closure of A in k.

Under these assumptions, let ϕ be a rank 2 Drinfeld module defined over $K \subset H_O$, with $\mathrm{End}_{H_O}(\phi) \cong O$, with action given by a rank 1 Drinfeld module $\psi : O \to O'\{\tau\}$ with coefficients in O' (again the leading coefficient of ψ_y is in $\mathbb{F}_r$), where O' is the integral closure of O in H_O. Certainly, any Drinfeld module of rank 2 that has complex multiplication by a sgn-normalized Drinfeld module ψ defined over H_O can also be defined over H_O. In case that it is defined over a strictly smaller subfield, we let $K \subset H_O$ be the minimal field of definition for ϕ.

Our second possible situation is that $A = \mathbb{F}_q[T]$ and $F = \mathbb{F}_q(T)$ and ϕ is a rank 2 Drinfeld module defined over F. Further $\mathrm{End}(\phi) = A$.

In the first case, the class field theory developed by Drinfeld and Hayes provides a powerful tool towards solving our formulation of the Lang-Trotter conjecture. This is also seen in [18].

In the second case, we take the method of higher rank free submodules of the module of rational points, as in [11],[1]. To do this we need to use the theorem of Pink and Rutsche[23, Theorem 0.1] and the Kummer theory given by Ribet in [25],[26]. Further, Poonen's theorem,[24, Theorem 1] will give us the structure of the module of rational points.

For a prime ideal P of A, let $P^h = (a)$ for some h, a, and let

$$T_P(\phi) = \lim_{\leftarrow i} \phi[a^i] = \lim_{\leftarrow j} \phi[P^j]$$

be the P-adic Tate-module of ϕ. Let A_P be the completion of A at P (the same as the

P-adic integers). Then $T_P(\phi)$ is a free A_P module of rank d (the rank of ϕ) if P is coprime to the characteristic of L.

Let $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$, then there is a continuous Galois representation

$$\rho_P : G_K \to \mathrm{Aut}_{A_P}(T_P(\phi)) \cong \mathrm{GL}_r(A_P).$$

Theorem 3.10.1 ([34], Theorem 0.1)**.** *The G_K module $T_P(\phi)$ is semi-simple.*

Let $\mathbb{A}_F^f$ be the ring of finite adeles of F and consider the adelic representation

$$\rho_{ad} : G_K \to \prod_{P \neq \infty} \mathrm{GL}_r(A_P) \subset \mathrm{GL}_r(\mathbb{A}_F^f).$$

Theorem 3.10.2 ([23], Theorem 0.1)**.** *Let ϕ be a Drinfeld A-module of rank d over a finitely generated field K of generic characteristic. Assume that* $\mathrm{End}_{\overline{K}}(\phi) = A$*. Then the image of the adelic representation*

$$\rho_{ad} : G_K \to \prod_{P \neq \infty} \mathrm{GL}_r(A_P) \subset \mathrm{GL}_r(\mathbb{A}_F^f)$$

is open.

This is basically a Drinfeld analogue of Serre's result [30] for elliptic curves without complex multiplication.

The following result is proved by Poonen as [24, Theorem 1] by developing a theory of local heights for Drinfeld modules. We can see that although there is no Mordell-Weil rank for Drinfeld modules, they are still pretty nicely behaved.

Theorem 3.10.3 ([24], Theorem 1)**.** *Let L/F be a finite extension, and ϕ a Drinfeld module $\phi : A \to L\{\tau\}$. Then under the action of ϕ, the field L is isomorphic to the direct sum of its torsion submodule, and a free A-module of countably infinite rank. Further, the torsion submodule of L is finite.*

Chapter 4

Number Theory

4.1 Lang-Trotter conditions

First, we must formulate a purely algebraic condition which will turn the question of "Does $\overline{a}$ generate $\phi(\mathbb{F}_P)$?" into two questions. First, "Does $\overline{a}$ generate $\psi(\mathbb{F}_P)$ as an $\mathrm{End}(\phi)$ module, where P splits completely in $H := H_O$?" Second, "Is $\phi(\mathbb{F}_P)$ cyclic?" It is easy to see that these conditions are both necessary for $\overline{a}$ to generate $\phi(\mathbb{F}_P)$, but in fact they are sufficient as well.

Our next goal will be to follow the work of Gupta-Murty and Hsu-Yu, by formulating the extensions $K_q = H(\phi[q])$, and $K_{\mathfrak{q}}^a = H(\phi[\mathfrak{q}], \mathfrak{q}^{-1}a)$. Then we see that $\overline{a}$ generates $\phi(\mathbb{F}_P)$ if and only if P does not split completely in any extension K_q or $K_{\mathfrak{q}}^a$, as q varies over finite primes of A, and $\mathfrak{q}$ varies over finite primes of $O = \mathrm{End}(\phi)$.

Let A be a Dedekind domain and let F be the fraction field of A. Let k be a field such that $[k : F] < \infty$ and let O be the integral closure of A in k. If M is any (left)O-module, then M has a natural A-module structure, by restricting the left-multiplication by O to A. If $S \subset M$, then let $A \cdot S$ be the smallest A-submodule of M which contains S, and let $O \cdot S$ be the smallest O-submodule of M which contains S. Clearly $A \cdot S \subset O \cdot S$.

Our main interest is finite modules.

Definition 4.1.1. *If I is an ideal of A and N is an A-module.*

$$N[I] = \{a \in N \mid x \cdot a = 0, \text{ for every } x \in I\}.$$

Similarly, define for $\mathfrak{I}$ an ideal of O, and N' an O-module

$$N'[\mathfrak{I}] = \{b \in N' \mid x \cdot b = 0, \text{ for every } x \in \mathfrak{I}\}.$$

Lemma 4.1.1. *Let I be an ideal of A, with $\mathfrak{I} = O \cdot I$. Then $A \cdot S[I] \subset O \cdot S[\mathfrak{I}]$*

Proof. Without loss of generality, we assume that $S = A \cdot S[I]$. We must show that $O \cdot S$ is entirely $\mathfrak{I}$-torsion. Let $b_1, b_2 \in O$, $s \in S$ and $a \in I$, then

$$(b_1 a)(b_2 s) = b_1 a b_2 s = b_1 b_2 (as) = b_1 b_2 0 = 0$$

Therefore $O \cdot S$ is annihilated by $b_1 a$ for any $a \in I$ and $b_1 \in B$. Hence $O \cdot S$ is annihilated by $\mathfrak{I}$ as required. □

Lemma 4.1.2. *Suppose M is a finite O-module, which is also a cyclic A-module. Let $a \in M$. Then $A \cdot a = M$ if and only if $O \cdot a = M$.*

Proof. If $A \cdot a = M$ then $O \cdot a \supset A \cdot a \supset M$. Suppose that $O \cdot a = M$. Write $a = c \cdot m$, where $c \in A$, and m is the element which generates M as an A-module. We can write $m = b \cdot a$ for some $b \in B$. For $x \in B$, let Φ_x denote the multiplication by x map from M to M. Since $a = c \cdot m = c \cdot b \cdot a$, we have that Φ_{bc} is the identity map on M. Hence, the map $\Phi_c \in \mathrm{Aut}(M)$, so $\Phi_c^n = 1$, for some n. Hence, the map $\Phi_{c^{n-1}}$ is the inverse map of Φ_c on M, that is $c^{n-1} a = m$. Hence $A \cdot a = M$.

□

Now, suppose we are in the situation that ϕ is a rank 2 Drinfeld module with CM by a rank 1 Drinfeld module $\psi : O \to O'\{\tau\}$ with leading coefficient of ψ_x always an element of $\mathbb{F}_r^*$.

This is exactly the situation where we can apply **Lemma 4.1.2**.

Before we see this, we must go over what is happening for ψ as in [18].

Definition 4.1.2. *An element $x \in O$ is positive if $\eta(x) = 1$, where $\eta(x)$ is the leading coefficient of ψ_x.*

Let $\mathfrak{P}$ be a finite prime of $H := H_O$. Then $N_{H/k}(\mathfrak{P})$ is always a principal ideal in O **Theorem 3.9.5**. There exists a positive element $\beta = \beta(\mathfrak{P}) \in O$ with $(\beta) = N_{H/k}(\mathfrak{P})$.

Proposition 4.1.1 ([18], Proposition 2.1). *We have*

$$\psi(O/\mathfrak{P}) \cong O/(\beta(\mathfrak{P}) - 1),$$

where the isomorphism is as O-modules.

Proof. Since ψ is rank 1, we know that $\psi(O'/\mathfrak{P})$ is cyclic. If we let $\mathfrak{p} = \mathfrak{P} \cap O$, then we know that the reduction of ψ at $\mathfrak{P}$ has height one at $\mathfrak{p}$. Hence, by [14], the polynomial $\psi_{\mathfrak{p}}$ is completely inseparable mod $\mathfrak{P}$, so $\psi_{\mathfrak{p}} \equiv x^{r^{\deg \mathfrak{p}}} \pmod{\mathfrak{P}}$. Now $\beta(\mathfrak{P}) = \mathfrak{p}^{\deg \mathfrak{P}/\deg \mathfrak{p}}$, so that

$$\psi_{\beta(\mathfrak{P})}(b) \equiv b \pmod{\mathfrak{P}},$$

for all $b \in O'$. This completes the proof since both sides have the same number of elements.

□

Proposition 4.1.2 ([18], Proposition 2.2). *Suppose that $a \in O'$, $\mathfrak{P}$ is a prime ideal in O' and $N_{H/L}(\mathfrak{P}) = (\beta)$ for some positive element $\beta \in O$. Then $\overline{a}$ generates $\psi(O'/\mathfrak{P})$ if and only if $\psi_{(\beta-1)\mathfrak{p}^{-1}}(\overline{a}) \neq 0$ for all prime ideals $\mathfrak{p} \subseteq O$ such that $\mathfrak{p}$ divides $(\beta - 1)$.*

Proof. Follows from the above proposition. □

Consider the set of $\mathfrak{a}$-torsion of ψ $\psi[\mathfrak{a}]$, and the field $K_{\mathfrak{a}} = H(\psi[\mathfrak{a}])$. The extensions $K_{\mathfrak{a}}/H$ are unramified outside of $\mathfrak{a}$ and ∞, and are abelian. We have $\mathrm{Gal}(K_{\mathfrak{a}}/H) \cong (O/\mathfrak{a})^*$. Thus, there is no rational torsion as long as $r \neq 2$, which we have assumed to be the case.

Further the Artin symbol at a prime $\mathfrak{p}$ of O not dividing $\mathfrak{a}$ is given by

$$\sigma_{\mathfrak{p}}(\lambda) = \psi_{\mathfrak{p}}(\lambda) \text{ for all } \lambda \in \psi[\mathfrak{a}].$$

Set $K_{\mathfrak{a}}^a = K_{\mathfrak{M}}(x)$, where x is a solution to $\psi_{\mathfrak{a}}(x) = a$.

Proposition 4.1.3 ([18], Proposition 2.3). *Let $\mathfrak{p}$ be a prime ideal in O, and let $\mathfrak{P}$ be a prime ideal in O' with $N_{H/k}(\mathfrak{P}') = (\beta)$ for some positive $\beta \in O$. Then $\mathfrak{P}$ splits completely in $K_{\mathfrak{p}}^a$ if and only if $\mathfrak{p} \mid (\beta - 1)$ and $\psi_{(\beta-1)\mathfrak{p}^{-1}}(\overline{a}) = 0$.*

Proof. Suppose that $\mathfrak{P}$ splits completely in $K_{\mathfrak{p}}^a$. The Artin symbol $\sigma_{(\beta)}$ is the identity in $\mathrm{Gal}(H(\psi[\mathfrak{p}])/H)$. Thus,

$$\sigma_{(\beta)}(\lambda) = \psi_{\beta}(\lambda) = \lambda.$$

So, $\psi_{\beta-1}(\lambda) = 0$ for all $\lambda \in \psi[\mathfrak{p}]$. Thus, the prime $\mathfrak{p}$ divides the principal ideal $(\beta - 1)$ in O. Since $\mathfrak{P}$ splits completely in $K_{\mathfrak{p}}^a$, there is a root $\overline{\alpha}$ of $\psi_{\mathfrak{p}}(x) \equiv a \pmod{\mathfrak{P}}$ in $\psi(O'/\mathfrak{P})$. From the above proposition, we obtain that $\psi_{(\beta-1)\mathfrak{p}^{-1}}(\overline{a}) = \psi_{(\beta-1)}(\alpha) = 0$ in $\psi(O'/\mathfrak{P}')$.

Now, suppose that $\mathfrak{p}$ divides $(\beta - 1)$ and $\psi_{(\beta-1)\mathfrak{p}^{-1}}(\overline{a}) = 0$. Let $\sigma_{\mathfrak{P}}$ be the Artin symbol in $\mathrm{Gal}(H(\psi[\mathfrak{p}])/H)$. Since $N_{H/k}(\mathfrak{P}) = (\beta)$, we know that $\sigma_{(}\beta) = \sigma_{\mathfrak{P}}$. Since $\mathfrak{p} \mid (\beta - 1)$, we get that $\sigma_{\mathfrak{P}}(\lambda) = \sigma_{(}\beta)(\lambda) = \psi_{\beta-1}(\lambda) + \lambda = \lambda$, for all $\lambda \in \psi[\mathfrak{p}]$. That is, the prime $\mathfrak{P}$ splits completely in $H(\psi[\mathfrak{p}])$. To show that it splits completely in $K^a_{\mathfrak{p}}$, we need to find a solution to the equation $\psi_{\mathfrak{p}}(x) = \overline{a}$ in $O'/\mathfrak{P}$. Let α be a root of the equation in a fixed algebraic closure of $O'/\mathfrak{P}$. Then $\psi_{\beta-1}(\alpha) = \psi_{(\beta-1)\mathfrak{p}^{-1}}(a) = 0$.

Let $\mathfrak{q} = \mathfrak{P} \cap O$. Then $\psi_{\mathfrak{q}}(x)$ is Eisenstein at $\mathfrak{P}$. So, reducing modulo P gives that $\psi_{\mathfrak{q}}(x) \equiv x^{r^{\deg \mathfrak{q}}} \pmod{\mathfrak{P}}$, for $x \in \mathscr{O}'$. Now, write $(\beta) = \mathfrak{q}^l$ where l is a positive integer (l is the dimension of $O'/\mathfrak{P}$ over $O/\mathfrak{q}$) Then $\psi_\beta(x) \equiv x^{r^{\deg \beta}} \pmod{\mathfrak{P}}$. Thus, $\alpha^{r^{\deg p}} \equiv \beta \pmod{\mathfrak{P}}$.

Since $\deg \beta = \deg \mathfrak{P}$, we have that $\alpha \in O'/\mathfrak{P}$, completing the proof.

□

Theorem 4.1.1 ([18], Theorem 2.4)**.** *The element $\overline{a}$ is a generator of $\psi(O'/\mathfrak{P})$ if and only if the prime ideal $\mathfrak{P}$ does not split completely in any of the fields $K^a_{\mathfrak{P}}$ where $\mathfrak{P}$ runs through prime ideals in O.*

Let P be a finite prime of F which lies over a prime ideal of A, say p^*, and assume that p^* splits completely in H. Let $\mathfrak{p}$ be a prime of O' lying above P. The index module at P, denoted $i(P)$, is used to keep track of whether or not the residue $\overline{a}$ generates the module $\phi(\mathbb{F}_P)$. It is defined by

$$i(P) = \phi(\mathbb{F}_P)/(A \cdot \{\overline{a}\}),$$

where $A \cdot \{\overline{a}\}$ is the A-submodule of $\phi(\mathbb{F}_P)$ generated by the reduction of a modulo P, $(\overline{a})$.

Notice that $\phi(\mathbb{F}_P)$ is generated by $\overline{a}$ if and only if $i(P)[q] = \{0\}$ for every prime q of A.

Lemma 4.1.3. *The A-module $\phi(\mathbb{F}_P)$ is cyclic if and only if $\phi[q] \subsetneq \phi(\mathbb{F}_P)$ for every $q \neq p^*$.*

Proof. Suppose $\phi(\mathbb{F}_P)$ is cyclic, then it is isomorphic to A/m for some ideal m. Since ϕ is rank 2, for every q except $q = p^*$, we have $\phi[q] \cong (A/q)^2$. Sufficiency follows.

Now, write $\phi(\mathbb{F}_P) \cong A/m_1 \oplus A/m_2$ for $m_1 \mid m_2$. If $q \mid m_1$ then $\phi[q] \subset \phi(\mathbb{F}_P)$, therefore $m_1 = 1$. The prime p^* cannot divide m_1 since either $\phi[p^*] = A/p^*$ or $\phi[p^*] = 0$. Necessity follows. □

Lemma 4.1.4. *We have that $\phi(\mathbb{F}_P) = A \cdot \{\overline{a}\}$ if and only if*

1. *$\phi[q] \subsetneq \phi(\mathbb{F}_P)$, for every prime q of A with $q \neq p^*$*

2. $\psi(\mathbb{F}_{\mathfrak{p}}) = O \cdot \{\overline{a}\}$

Proof. Combining **Lemma 4.1.2** and **Lemma 4.1.3**, we see that if $A \cdot \{\overline{a}\} = \phi(\mathbb{F}_P)$ then both conclusions hold. Conversely by **Lemma 4.1.3**, we know that $\phi(\mathbb{F}_P)$ must be cyclic, and so we can apply **Lemma 4.1.2** to finish. □

Just as in the case of the Lang-Trotter condition,

Lemma 4.1.5. *Let q be a prime of A with $q \neq p^*$. Then $\phi[q] \subset \phi(\mathbb{F}_P)$ if and only if P splits completely in the field $K(\phi[q])$.*

Proof. Let

$$f(X) = \prod_{0 \neq s \in \phi[q]} (X - s)\,.$$

The polynomial f is separable with coefficients in K, since $\phi_b(X)$ is a separable polynomial for $b \notin p^*$, and $0 \neq b \in q$ implies that f divides ϕ_b. So we see that $F(\phi[q])$ is the splitting field for f, and $\phi[q] \subset \phi(\mathbb{F}_P)$ if and only if $\overline{f}$ factors over $\mathbb{F}_P$. This is equivalent to the condition of P splitting completely in $F(\phi[q])$ from principles in number theory. □

For q a prime of A, let $K_q = H(\phi[q])$.

Lemma 4.1.6. *Suppose that p^* splits completely in the field H. Let q be a prime of A with $q \neq p^*$, then $\phi[q] \subset \phi(\mathbb{F}_P)$ if and only if P splits completely in the field K_q.*

Proof. By **Lemma 4.1.5**, we just have to show that P splits completely in $K(\phi[q])$ if and only if P splits completely in the field K_q, under the given conditions. If p^* splits completely in H then P splits completely in H. Also, we remark that $K_q = H * K(\phi[q])$. Thus, we have that P splits completely in K_q if and only if P splits completely in $K(\phi[q])$ (see for example [8, Proposition 3.5.2]). □

Proposition 4.1.4 (Modified Lang-Trotter)**.** *Let $P, \mathfrak{p}, p^*, a$ be as above. Then $A \cdot \overline{a} = \phi(\mathbb{F}_P)$ if and only if P does not split completely in any field $K^a_{\mathfrak{q}}$ or K_q, for q,$\mathfrak{q}$ prime ideals that do not divide p^*.*

Just as in the CM-case for elliptic curves, we need only consider $K^a_{\mathfrak{a}}$ such that $\mathfrak{a}$ is only divisible by primes of first degree. Let $\mathfrak{q}$ be a prime ideal of O. Set $q = \mathfrak{q} \bigcap A$. We say $\mathfrak{q}$ is of first-degree if $[O/\mathfrak{q} : A/q] = 1$.

Then for a square-free ideal s of A, let $K_s = \prod_{q|s} K_q$. Similarly, for $\mathfrak{a}$ a square-free ideal of O which is a product of first-degree primes of O, define $K^a_{\mathfrak{a}} = \prod_{\mathfrak{q}|\mathfrak{a}} K^a_{\mathfrak{q}}$. Then set

$K^a_{\mathfrak{a},s} = K^a_{\mathfrak{a}} \cdot K_s$. Then if P is a prime for which p^* splits completely in H, $\mathbb{F}_P = A \cdot \{\overline{a}\}$ if and only if P does not split completely in any $K^a_{\mathfrak{a},s}$.

Now, assume that $A = \mathbb{F}_r[T]$, and $F = \mathbb{F}_r(T)$. In this situation a prime of A will simply mean a monic irreducible polynomial. Let $\phi : A \to F\{\tau\}$ be a Drinfeld module of generic characteristic such that $\mathrm{End}(\phi) = A$. Let $a_1, \ldots, a_t \in F$ generate a free A-submodule of F, by Poonen's theorem [24, Theorem 1], we can take t as large as we want. Let Γ be the A-submodule generated by $a_1, \ldots, a_t$. Let Γ_P be the reduction of Γ modulo P for primes P such that ϕ has good reduction at P and $v_P(P_i) \geq 0$ for each i.

We want to describe completely the situation that $\phi(\mathbb{F}_P)/\Gamma_P[q] \neq 0$. First of all, this condition implies that $\phi(\mathbb{F}_P[q]) \cong A/q$ or $(A/q)^2$. Secondly, there must exist $\alpha_1, \ldots, \alpha_t \in \mathbb{F}_P$ with $\overline{\phi_q}(\alpha_i) = \overline{a_i}$.

Then we know that $\phi(\mathbb{F}_P)/\Gamma_P[q] \neq 0$ if and only if $\phi(\mathbb{F}_P)[q] \neq 0$ and there exists $\alpha_i \in \mathbb{F}_P$ such that $\overline{\phi_q}(\alpha_i) = \overline{a_i}$.

This leads us to define

$$K^\Gamma_q = k(\phi[q], \alpha_1, \ldots, \alpha_t)$$

where α_i is a root of $\phi_q(X) = P_i$.

Let $G_q = \mathrm{Gal}(K^\Gamma_q/F)$.

Proposition 4.1.5. *The Galois group G_q is isomorphic to a subset of $\mathrm{GL}_2(\mathbb{F}_q) \rtimes \phi[q]^t$. Let $\sigma_P \in G_q$ be the Frobenius corresponding to P, and write $\sigma_P = (\gamma_P, \xi_P)$. Then*

$$\phi(\mathbb{F}_P)/\Gamma_P[q] \neq 0,$$

if and only if either

1. *$\gamma_P = \mathrm{id}_{\phi[q]}$ and $\langle(\xi_{a_1}), \ldots, (\xi_{a_t})\rangle$ generates a cyclic or trivial submodule of $\phi[q]$, or*
2. *$\ker(\gamma_P - 1) \cong A/q$ and $(\xi_{a_i}) \in \mathrm{Im}(\gamma_P - 1)$.*

Denote the resulting conjugacy class by $\mathscr{C}_q \subset G_q$.

Let s be a square-free monic polynomial in A, and let $K^\Gamma_s = \prod_{q|s} K^\Gamma_q$, $G_s = \mathrm{Gal}(K^\Gamma_s/k)$, and $\mathscr{C}_s$ be the conjugacy class in G_s determined by all $\mathscr{C}_q$ for $q \mid s$.

Then $\Gamma_P = \phi(\mathbb{F}_P)$ if and only if $\sigma_P \in G_s$ does not lie in $\mathscr{C}_s$ for any square-free s.

4.2 Basic discriminant overview

We will work from the following references:[8], [31].

We recall the machinery of the different, for more details see [8, Chapter 3, Section 6]. Let (L, v) and (L', w) be two complete fields with discrete valuations v, w such that L' is a finite separable extension of L. Set

$$\begin{array}{rcl} O_{L'} & = & \{x \in L' \mid w(x) \geq 0\} \\ R_{L'} & = & \{x \in L' \mid w(x) > 0\} \end{array}$$

and let $\beta_{L'}$ be a generating element for the principal ideal $R_{L'}$. The complementary module $O'_{L'/L}$ of $O_{L'}$ over L is defined by

$$O'_{L'/L} = \{x \in L' \mid \mathrm{trace}_{L'/L}(xO_{L'}) \subset O_L\},$$

where trace takes fractional ideals of L' to fractional ideals of L.

The complementary module $O'_{L'/L}$ contains $O_{L'}$ and is a fractional ideal of $O_{L'}$, so $O'_{L'/L} = \beta_{L'}^{-d_{L'/L}} O_{L'}$ for some non-negative exponent $d_{L'/L}$, called the different exponent. Note that $d_{L'/L} > 0$ if and only if L'/L is a ramified extension.

If we know that $\mathrm{trace}_{L'/L}(\beta_{L'}^{-m} O_{L'}) \subsetneq O_L$ for some non-negative integer m, then $d_{L'/L} \leq m$. Likewise, if $\mathrm{trace}_{L'/L}(\beta_{L'}^{-m} O_{L'}) \subset O_L$, then $d_{L'/L} \geq m$.

For our purposes, consider L'/L a finite, separable extension of global function fields. Let $\mathfrak{P}$ be a prime of L', lying over a prime P of L. Set $(\hat{L}', v_{\mathfrak{P}}), (\hat{L}, v_P)$ to be the completions of L, K at $\mathfrak{P}$ and P, respectively. Let $d_{L'/L}(\mathfrak{P})$ be the different exponent of $\hat{L}/\hat{K}$.

The different of the extension L'/L is a divisor of L', denoted $\mathrm{Diff}(L'/L)$, defined by

$$\mathrm{Diff}(L'/L) = \sum_{\mathfrak{P}} d_{L'/L}(\mathfrak{P}) \cdot \mathfrak{P}.$$

The degree of the different appears in the Riemann-Hurwitz formula [27, Theorem 7.16] to determine the genus of L' in terms of the genus of L. The genera of L' and L both appear in an effective Chebotarev density theorem for L'/L. Thus, we must compute the different of various fields. More specifically for fields L' over some fixed field L, we must determine a bound for $\deg \mathrm{Diff}(L'/L)/[L' : L]$.

The different is additive over towers of extensions. That is, let $L \subset M \subset N$ be a tower of function fields. Then $\mathrm{Diff}(N/L) = \mathrm{Diff}(N/M) + \mathrm{Diff}(M/L)$ where the second summand is the appropriate divisor of N. Now, the degree of $\mathrm{Diff}(M/L)$ as a divisor of N is not necessarily the same as the degree of $\mathrm{Diff}(M/L)$ as a divisor of M. Assume that the constant fields of N, M, L are all equal to $\mathbb{F}_r$. Then $\deg_N \mathrm{Diff}(M/L) = [N : M] \deg_M \mathrm{Diff}(N/M)$, so that

$$\frac{\deg \mathrm{Diff}(M/L)}{[N : L]} = \frac{\deg \mathrm{Diff}(N/M)}{[N : M]} + \frac{\deg \mathrm{Diff}(M/L)}{[M : L]}.$$

The different exponent of tamely ramified primes are also very predictable. That is if $\mathfrak{P}$ is a prime of L', with ramification degree $e_{\mathfrak{P}}$ coprime to p, the characteristic of N, then $d_{L'/L}(\mathfrak{P}) = e_{\mathfrak{P}} - 1$. If $\mathfrak{P}$ is wildly ramified, then we have $d_{L'/L}(\mathfrak{P}) \geq e_{\mathfrak{P}} - 1$.

4.3 All discriminant results

We begin with the results of Gardeyn[9].

To find out the (possibly wild) ramification over various primes, we must complete at the primes in question, then use Drinfeld's analytization results.

This section is from [9, Propositions 4 and 6]. Here we set $A = \mathbb{F}_r[T]$, $F = \mathbb{F}_r(T)$ and K to be a finite extension of F. The map $\phi : A \to K\{\tau\}$ is a Drinfeld module of rank d.

For a place v of K, let K_v be the completion of K at v and O_v the ring of integers of K_v with residue field F_v. Let $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K), G_v = \mathrm{Gal}(K_v^{\mathrm{sep}} s/K_v) \subset G_F$ and I_v be the inertia group at v. Let C_v be the completion of the algebraic closure of K_v, with v extended in the usual way. The place v is called infinite if it lies over ∞.

Theorem 4.3.1 ([10], Theorem 4.6.9)**.** *For an infinite place v of K, there exists an entire C_v-homomorphism $e_v^{\phi} : C_v \to C_v$ defined over K_v such that*

$$e_v^{\phi}(ax) = \phi_a(e_v^{\phi}(x))$$

for all $a \in A$ and $x \in C_v$. The kernel of e_v^{ϕ}, Λ_v, is an A-lattice which is G_v-invariant in C_v of rank d.

Theorem 4.3.2 ([6], Proposition 7.2)**.** *Let P be a prime of K such that the reduction of ϕ mod P is rank $\overline{d}$. Then there exists an entire homomorphism $e_P^{\phi} : C_P \to C_P$ and a Drinfeld module ψ of rank $\overline{d}$ which has good reduction at P such that*

$$e_P^{\phi}(\psi_a(x)) = \phi_a(e_P^{\phi}(x)).$$

Let $\Lambda_P = \ker(e_P^{\phi})(C_P)$. *Then* Λ_P *is a* G_P*-invariant* A*-lattice of rank* $d - \overline{d}$.

Also, recall the following:

$$v_P(\psi_a(\lambda)) = |a|_\infty^{\overline{d}} v_P(\lambda),$$

and $v_P(\lambda) < 0$ for all $\lambda \neq 0, \lambda \in \Lambda_P$, where $|a|_\infty = (\#F_v)^{-v_\infty(a)}$.

Let us therefore define a norm on Λ_v such that

$$\|a \cdot \lambda\|_v = |a|_\infty \|\lambda\|_v.$$

For v a finite place, choose $\|\cdot\|_v = (-v(\cdot))^{1/\overline{d}}$ and for v an infinite place, choose the unique extension to $C_{\overline{\infty}}$ of $|\cdot|_\infty$.

Let n be the rank of Λ_v and K_v^Λ be the field extension of K_v by Λ_v.

Let

$$B_\kappa = \{\lambda \in \Lambda_v : \|\lambda\| \leq \kappa\},$$

for $\kappa \in \mathbb{R}$. Notice that B_κ is a finite set. Let v_i be the minimum κ such that B_κ contains i elements linearly independent over k. Notice that $v_1 \leq v_2 \leq \cdots \leq v_n$.

We say that a basis $\{\lambda_1, \ldots, \lambda_n\}$ is minimal if $\|\lambda_i\| = v_i$ for each i. We have the following equality for $(a_i) \in A^n$:

$$\left\| \sum_{i=1}^n a_i \cdot \lambda_i \right\|_v = \max_{1 \leq i \leq n}\{\|a_i \cdot \lambda_i\|_v\}.$$

Following [34], suppose that we have a strict inequality above.

Then there exists $s > 1$ such that

$$\|a_{i_1}\lambda_{i_1}\| = \cdots = \|a_{i_s}\lambda_{i_s}\| = \left\| \sum_{i=1}^n a_i \cdot \lambda_i \right\|_v .$$

Then

$$\left\| \sum_{j=1}^s a_{i_j}\lambda_{i_j} \right\| < \|a_{i_s}\lambda_{i_s}\|$$

which follows since we may remove any $a_i\lambda_i$ from the sum if $\|a_i\lambda_i\| < \|a_{i_s}\lambda_{i_s}\|$. But now,

$$\left\| \sum_{j=1}^{s} \frac{a_{i_j}}{a_{i_s}} \lambda_{i_j} \right\| < v_{i_s}.$$

By choosing a minimal basis, $\deg a_{i_j} \geq \deg a_{i_s}$ for all j, so that for $1 \leq j < s-1$ we can write $a_{i_j}/a_{i_s} = b_j + c_j$ where $b_j \in A$ and $|c_j| < 1$. Thus,

$$\left\| \sum_{j=1}^{s-1} b_j \lambda_{i_j} + \lambda_{i_s} \right\| < v_{i_s},$$

hence our assumption that $s > 1$ is false. Hence there is a unique subscript for which $\|a_i\lambda_i\|$ is maximal, and the equality follows from the ultrametric property.

Proposition 4.3.1 ([9], Proposition 4)**.** *1. The degree of the field extension K_v^Λ/K_v is bounded by g_v, which we define to be*

$$g_v := \#\,\mathrm{GL}_n(\mathbb{F}_r) \prod_{i=1}^{n} \prod_{u=1}^{i} \frac{v_i}{v_u}$$

2. The different $D(K_v^\Lambda/K_v)$ is bounded by: $\mathrm{ord}_v(D(K_v(\Lambda)/K_v)) \leq 1 + D_v^\Lambda$*, defined by*

$$D_v^\Lambda := 2\sum_{i=1}^{n} \left(r^{i-1} v\left(\frac{\lambda_1}{\lambda_i}\right) \prod_{u=1}^{i} \frac{v_i}{v_u} \right).$$

Proof of 1. Set $G_\Lambda := \mathrm{Gal}(K_v^\Lambda/K_v)$. Since Λ_v is a discrete subset of C_v, the orbit under G_v of any basis of Λ_v is a finite set. Hence $G_v = [K_v^\Lambda : K_v]$ is finite. We obtain a representation of G_v by letting it act on Λ_v:

$$\rho_\Lambda : G_v \to \mathrm{Aut}_A(\Lambda_v) \cong \mathrm{GL}_n(A).$$

Fix a minimal basis (λ_i) for Λ_v. Let $v^1 < v^2 < \cdots < v^s$ be the distinct values of $v_1, \ldots, v_n$. Suppose that v^1 appears with multiplicity m_1, v^2 with multiplicity m_2 and so on. For $i \leq n$, let $j(i)$ be the unique index such that $v^{j(i)} = v_i$. Also, for each $\sigma \in G_\Lambda$ and $1 \leq i \leq n$ write

$$\sigma(\lambda_i) = \sum_{1\leq u\leq n} \sigma_{i,u}\lambda_u,$$

with $(\sigma_{i,u})_u \in A^n$. By the properties of minimal bases,

$$v_i = \|\sigma(\lambda_i)\| = \max_{1\leq u\leq n}\{|\sigma_{i,u}|v_u\}.$$

This implies that $\sigma_{i,u} = 0$ if $j(u) > j(i)$ and $\sigma_{i,u} \in \mathbb{F}_r$ if $j(i) = j(u)$. Let

$$\Lambda^j = \oplus^n_{\substack{i=1\\ j(i)\leq j}} A \cdot \lambda_i \text{ and } \Lambda_j = \Lambda^j/\Lambda^{j-1}$$

are G_v-invariant. Further, the image of the representation

$$\rho_j : G_v \to \mathrm{Aut}_A(\Lambda_j),$$

is isomorphic to a subgroup of $\mathrm{GL}_{m_j}(\mathbb{F}_r)$.

Let H_Λ be a p-Sylow subgroup of G_Λ (where r is a power of p), and let K_v^1 be the sub-field of K_v^Λ fixed by H_Λ. We can see that the maximal divisor which is prime to p of the order of a finite index subgroup of $\#\,\mathrm{GL}_n(A)$ is $\prod_{i=1}^n(q^i - 1)$. Thus,

$$[K_v^1 : K_v] \leq \prod_{i=1}^n (q^i - 1)$$

Now let us construct a minimal basis which behaves very nicely with respect to our representations ρ_j when restricted to H_Λ. Since H_Λ is a p-group and $\rho_j(H_\Lambda) \subset \mathrm{GL}_{m_j}(\mathbb{F}_r)$, we know that $\rho_j(H_\Lambda)$ is a unipotent subgroup. Therefore, there exists change of basis matrices $\gamma_j \in \mathrm{GL}_{m_j}(\mathbb{F}_r)$ for which $\rho_j(H_\Lambda)$ is upper-triangular. Now set

$$(\lambda_1', \ldots, \lambda_n') = (\lambda_1, \ldots, \lambda_n) \cdot (\gamma_1 \oplus \cdots \oplus \gamma_s),$$

which is a new minimal basis.

For each $1 \leq i \leq n$ set

$$K_v^i = K_v^1(\lambda_1', \ldots, \lambda_i'),$$

and notice that $\lambda_1' \in K_v^1$ (since it is fixed by H_Λ). Hence, the ramification degree of λ_1' must be coprime to p. This means that the ramification degree of λ_1 must also be coprime to p (they have the same valuation) and hence $\lambda_1 \in K_v^1$.

Now, we have a tower of Galois extensions

$$K_v^1 \subset K_v^2 \subset \cdots \subset K_v^n = K_v^\Lambda$$

such that $\mathrm{Gal}(K_v^n/K_v^1) = H_\Lambda$. For each $i > 1$ and $\sigma \in \mathrm{Gal}(K_v^i/K_v^{i-1})$ we can write

$\sigma(\lambda'_i) = \sum_{1<u\leq i} \sigma_{i,u} \cdot \lambda'_u$ with $\sigma_{i,u} \in A$. Further, we have that $\sigma_{i,u} = 0$ if $u > i$ and $\sigma_{i,i} = 1$. Thus, we have $|\sigma_{i,u}| \leq \frac{v_i}{v_u}$ for $u < i$.

The number of choices for $\sigma_{i,u}$ is at most $r \cdot v_i/v_u$. Thus

$$[K_v^i : K_v^{i-1}] \leq r^{i-1} \prod_{u=1}^{i} v_i/v_u.$$

Combining this with the bound for $[K_v^1 : K_v]$ and the size of $\# \operatorname{GL}_n(\mathbb{F}_r)$ gives the required bound.

□

Proof of 2. Let $L_v := K_v^{nr}$ be the maximal unramified extension of K_v in K_v^{sep}. Set $L_v^i = L_v K_v^i$ with ring of integers U_v^i. Set $I^i = \operatorname{Gal}(L_v^i/L_v^{i-1})$. Finally, set $L_v^\Lambda = K_v^\Lambda L_v$. By [31], we have $D(L_v^\Lambda/L_v) = D(K_v^\Lambda/K_v)$. Further, since L_v^1/L_v is tamely ramified $\operatorname{ord}_v(D(L_v^1/L_v)) < 1$.

For $i \geq 2$, let $\pi_i = \lambda'_1/\lambda'_i \in U_v^i$. Since $U_v^{i-1}[\pi_i]$ is an order in U_v^i, we have

$$D(L_v^i/L_v^{i-1}) \mid \prod_{1\neq\sigma\in I^i} (\sigma(\pi_i) - \pi_i).$$

Notice that $\|\lambda'_1\| \leq \|\sigma(\lambda'_i) - \lambda'_i\|$ for $\sigma \in I^i \setminus \{1\}$, by definition of a minimal basis. In other words, $v(\lambda'_1) \geq v(\sigma(\lambda'_i) - \lambda'_i)$. Thus,

$$v(\sigma(\pi_i) - \pi_i) \leq 2v(\pi_i) = 2(v(\lambda'_1) - v(\lambda'_i)) = 2(v(\lambda_1) - v(\lambda_i)).$$

So we get

$$\operatorname{ord}_v D(L_v^i/L_v^{i-1}) \leq \sum_{1\neq\sigma\in I^i} v(\sigma(\pi_i) - \pi_i) \leq 2\# I^i v(\lambda_1/\lambda_i).$$

From the proof of 1, we know that $\# I^i \leq r^{i-1} \prod_{u=1}^{i} v_i/v_u$. Thus,

$$\operatorname{ord}_v(D(L_v^i/L_v^{i-1})) \leq 2r^{i-1} v(\lambda_1/\lambda_i) \prod_{u=1}^{i} v_i/v_u.$$

Since, by [31, Chapter III, Section 4, Proposition 8] we know that

$$D(L_v^\Lambda/L_v) = \prod_{i=1}^{n} D(L_v^i/L_v^{i-1}),$$

the result follows. □

Definition 4.3.1. *For ϕ a rank d Drinfeld module over A define a divisor Δ_ϕ of K as follows.*

1. *If v lies above ∞ then set $\operatorname{ord}_v(\Delta_\phi) = 1 + D_v^\Lambda$ where Λ is the kernel of e_v^ϕ as defined previously.*
2. *If v is a finite place of F such that ϕ has good reduction, set $\operatorname{ord}_v(\Delta_\phi) = 0$. If ϕ has potential good reduction over an tamely ramified extension of K, set $\operatorname{ord}_v(\Delta_\phi) = 1$.*
3. *If v is finite and ϕ has stable reduction over a tamely ramified extension K_v'/K_v: let Λ_v be the A-lattice of rank $d - \overline{d}$ associated to e_v^ϕ with minimal basis $(\lambda_1, \ldots, \lambda_{d-\overline{d}})$, set*
$$\operatorname{ord}_v(\Delta_\phi) = 1 + D_p^\Lambda + 2\sum_{j=1}^{d-\overline{d}}(-v(\lambda_j)).$$

Denote by $[a]$ the divisor of K corresponding to the finite part of the divisor (a).

Proposition 4.3.2 ([9], Proposition 6)**.** *Let a be a non-constant element of A. Then*

$$D(K(\phi[a]), K) \leq r[a] + \Delta_\phi$$

as divisors of $K(\phi[a])$.

Proof. We split the proof according to the three cases of the above definition.

For v an infinite place, we see that

$$\phi[a] = e_v^\phi(a^{-1}\Lambda_v),$$

thus $K_v(\phi[q]) \subset K_v^\Lambda$. Thus, this part follows from the previous proposition and the definition of Δ_ϕ.

For v a finite place of good reduction, let $0 \neq s \in \phi[a]$. The minimal polynomial of s, denoted by f_s, divides ϕ_a and so

$$v(\partial f_s(s)) \leq v_p(\partial\phi_a) = \operatorname{ord}_v(a).$$

Thus, we have that $\operatorname{ord}_v(D(K(s)/K)) \leq v(\partial f_s(s)) = \operatorname{ord}_v(a)$. Since we need to adjoin d such roots, linearly independent over A, we obtain

$$\operatorname{ord}_v D(K(\phi[a])/K) \leq r \operatorname{ord}_v(a).$$

If ϕ has potential good reduction at v' over F'_v/F_v, then the argument above gives us that

$$\operatorname{ord}_v(D(K'_v(\phi[a])/K'_v)) \leq r \operatorname{ord}_p(a),$$

and [31, Chapter III, Section 6, Proposition 13] gives us that $\operatorname{ord}_p(D(K'_v/K_v)) < 1$. Combining gives the result in this case.

Finally, suppose that v is a finite place of potential stable reduction, over K'_v. Then the corresponding rank $\overline{d}$ Drinfeld module ψ has good reduction over K'_v. Set

$$K^0_v = K'_v(\Lambda_v, \psi[a]),$$

and so $\operatorname{ord}_p(D(K^0_v/K_v)) \leq \overline{r} \operatorname{ord}_v(a) + 1 + D^\Lambda_v$.

Fix a minimal basis $\lambda_1, \ldots, \lambda_{d-\overline{d}}$ for Λ_v. For each $1 \leq j \leq d - \overline{d}$, choose a root s_j of the equation $\psi_a(X) = \lambda_j$. Each conjugate $\sigma(s_j)$ over K^0_v lies in the set $s_j + \psi[a]$. Thus $K^0_v(s_j)/K^0_v$ is Galois and let the inertia group be $I^j = \operatorname{Gal}(L_v(s_j)/L_v)$, where L_v is the maximal unramified extension of K^0_v. Set U_v (resp. U^i_v) to be the ring of integers of L_v (resp. L^i_v).

Since $\sigma(s_j) - s_j \in \psi[a]$, we have

$$\prod_{1 \neq \sigma \in I^j} (\sigma(s_j) - s_j) \mid \partial \psi_a$$

and so

$$\sum_{1 \neq \sigma \in I^j} v(\sigma(s_j) - s_j) \leq \operatorname{ord}_v(a).$$

Since $v(s_j) + q^{-\overline{d} \deg a} v(\lambda_j) < 0$, we have that $\pi_j = s_j^{-1} \in U^j_v$ and $\# I^j \leq r^{\overline{d} \deg a}$. Since $U_p[\pi_j]$ is a rank $[L_p(s_j) : L_p]$ U_v module, we obtain

$$\operatorname{ord}_p(D(K^0_v(s_j)/K^0_v)) = \operatorname{ord}_v(D(L_v(s_j)/L_v)) \leq \sum_{1 \neq \sigma \in I^j} v(\sigma(\pi_j) - \pi_j).$$

But, we know that $v(\sigma(\pi_j) - \pi_j) \leq v(\sigma(s_j) - s_j) - 2v(s_j)$, so

$$\sum_{1 \neq \sigma \in I^j} v(\sigma(\pi_j) - \pi_j) \leq \operatorname{ord}_v a - 2\#I^j v(s_j) \leq \operatorname{ord}_v(a)_2 v(\lambda_j).$$

Noticing that $K_v^0(\psi_a^{-1}(\Lambda_v))$ is obtained by adjoining $s_1, \dots, s_{d-\overline{d}}$ and $\phi[a] = e_v^\phi(\psi_a^{-1}(\Lambda_v))$ we obtain

$$\operatorname{ord}_v(D(K_v(\phi[a]))/K_v^0) \leq (d - \overline{d}) \operatorname{ord}_v(a) - 2\sum_j v(\lambda_j),$$

which proves the proposition by [31, Chapter III, Section 6, Proposition 13]. □

This completes our review of the main result of Gardeyn in [9]. We must continue along these lines if we want to determine the different of K_s^Γ. From now on, we only consider $K = F = \mathbb{F}_r(T)$. The different of K_s^Γ/K will be denoted $D(s, \Gamma) := D(K_s^\Gamma/K)$.

We again need to separate the classes of valuations of $K_s^\Gamma = K(s^{-1}\Gamma, \phi[s])$. Let us briefly consider the possibilities.

Lemma 4.3.1. *Let P be a non-torsion point and v any place of K. Let Y_0 be a particular solution to $e_v^\phi(X) = P$. Then there exists a constant N_0, depending on ϕ, P, such that if v lies over ∞*

$$\operatorname{ord}_v D(K_v(\Lambda_v, Y_0)/K_v(\Lambda_v)) \leq N_0$$

and if v is a finite place of bad reduction, then

$$\operatorname{ord}_v D(K_v(\Lambda_v, Y_0, \phi[a])/K_v(\Lambda_v, \phi[a])) \leq N_0.$$

Proof. In both cases, we examine the Newton polygon of the function $e_v^\phi(X) - P$. The function e_v^ϕ is entire, thus so is the function $e_v^\phi - P$. By considering the different of each of the finitely many extensions considered above, each of which is finite, we get an upper bound for the different as required. An exact bound depends upon P and the coefficients of e_v^ϕ. □

If v lies above ∞, then we will proceed similar to [18].

Definition 4.3.2. *We will define a divisor of K, denoted $\Delta_{\alpha,\phi}$ in the following way, by defining $\operatorname{ord}_v(\Delta_{\Gamma,\phi})$ depending on v and Γ, where Γ is freely generated over A by t elements.*

1. *v is a place of K which lies above ∞. Let $\operatorname{ord}_v(\Delta_{\Gamma,\phi}) = t \cdot N_0$*

2. *v is a place of K for which $v(\Gamma) \geq 0$ and ϕ has good reduction at v. Then set* $\mathrm{ord}_v(\Delta_{\Gamma,\phi}) = 0$.

3. *v is a place of K for which either $v(\alpha) < 0$ for some $\alpha \in \Gamma$ or ϕ has potential good reduction at v. Then set* $\mathrm{ord}_v(\Delta_{\Gamma,\phi}) = 1$.

4. *v is a place of K_s^Γ where ϕ has bad reduction, then set* $\mathrm{ord}_v(\Delta_{\Gamma,\phi}) = t \cdot N_0 + 1$.

Theorem 4.3.3. *The different of K_s^Γ over K, denoted by $D(s, \Gamma)$ satisfies*

$$D(s, \Gamma) \leq \Delta_\phi + \Delta_{\phi,\Gamma} + d \cdot [s] + t \cdot [s].$$

Thus the degree of the above divisor, denoted by $d(s, \Gamma)$ satisfies

$$d(s, \Gamma)/n(s, \Gamma) \ll (t + d) \cdot \deg s,$$

where $n(s, \Gamma) = [K_s^\Gamma : K]$.

Proof. By [31, Chapter III, Section 4, Proposition 8], the first part follows by the work of Gardeyn as well as the definition of $\Delta_{\Gamma,\phi}$. The second part follows by taking degrees and noticing that the only part on the right hand side that depends on s is $(t + d)[s]$. □

Now, let us review the case in which ϕ has rank 2 with complex multiplication by ψ. We want to determine the different of the fields $K_{\mathfrak{a},s}^a$ over H. We will give an overview of different results contained in [18], as well as slight adaptations needed for our case. This includes (sometimes wild) ramification at finite primes as well as at the infinite primes.

4.4 Kummer theory of Hsu and Yu

In this section $a \in K \cap O'$ is a fixed non-torsion element. We examine the Kummer extensions related to $\mathfrak{q}$th roots of a.

Lemma 4.4.1 ([18], Theorem 2.6, part (1))**.** *Let $\mathfrak{a}, \mathfrak{b}$ be ideals of O with $\mathfrak{a}$ square free and $\mathfrak{a} \mid \mathfrak{b}$. Then* $\mathrm{Gal}(H(\psi[\mathfrak{b}], \mathfrak{a}^{-1}a)/H(\psi[\mathfrak{b}]))$ *is an O-submodule of* $\mathrm{Gal}(H(\psi[\mathfrak{a}], \mathfrak{a}^{-1}a)/H(\psi[\mathfrak{a}]))$.

Proof. As in [18], the group $\mathrm{Gal}(H(\psi[\mathfrak{b}])/H)$ acts on $\mathrm{Gal}(H(\psi[\mathfrak{b}], \mathfrak{a}^{-1}a)/H(\psi[\mathfrak{b}]))$ by conjugation. We want to extend the action of

$$\mathrm{Gal}(H(\psi[\mathfrak{b}])/H) \cong (O/\mathfrak{b})^\times$$

to turn

$$\mathrm{Gal}(H(\psi[\mathfrak{b}], \mathfrak{a}^{-1}a)/H(\psi[\mathfrak{b}]))$$

into an O-module. This is a consequence of an approximation lemma in [31]. □

Lemma 4.4.2 ([18], Theorem 2.6, part (1))**.** *Let $\mathfrak{q}$ be a prime ideal of O of first degree. Let $\mathfrak{b}$ be an ideal of O with $\mathfrak{q}$ dividing $\mathfrak{b}$. Then*

$$[H(\psi[\mathfrak{b}], \mathfrak{p}^{-1}a) : H(\psi[\mathfrak{b}])] = [H(\psi[\mathfrak{p}], \mathfrak{p}^{-1}a) : H(\psi[\mathfrak{p}])]$$

Proof. If $H(\psi[\mathfrak{p}], \mathfrak{p}^{-1}a) = H(\psi[\mathfrak{p}])$, then the lemma follows. Therefore, assume that

$$\mathrm{Gal}(H(\psi[\mathfrak{p}], \mathfrak{p}^{-1}a)/H(\psi[\mathfrak{p}])) \cong O/\mathfrak{p}.$$

By **Lemma 4.4.1**, we know that $\mathrm{Gal}(H(\psi[\mathfrak{b}, \mathfrak{p}^{-1}a)/H(\psi[\mathfrak{b}]))$ is either the trivial O-module, or isomorphic to $O/\mathfrak{p}$. But if the Galois group is trivial then $\mathfrak{p}^{-1}a \in H(\psi[\mathfrak{b}])$. Therefore, the non-abelian extension $H(\psi[\mathfrak{p}], \mathfrak{p}^{-1}a)/H$ is contained in the abelian extension $H(\psi[\mathfrak{b}])/H$. Therefore, we must have that $\mathfrak{p}^{-1}a \notin H(\psi[\mathfrak{b}])$. □

Lemma 4.4.3 ([18], Theorem 2.6, part (3))**.** *Let $\mathfrak{a}$ be a square free ideal of O only divisible by primes of first degree, and $\mathfrak{b}$ be an ideal of O such that $\mathfrak{a}$ divides $\mathfrak{b}$. Then*

$$[H(\psi[\mathfrak{b}], \mathfrak{a}^{-1}a) : H(\psi[\mathfrak{b}])] = [H(\psi[\mathfrak{a}], \mathfrak{a}^{-1}a) : H(\psi[\mathfrak{a}])]$$

Proof. We know that

$$M := \mathrm{Gal}(H(\psi[\mathfrak{b}], \mathfrak{a}^{-1}a)/H(\psi[\mathfrak{b}]))$$

is a submodule of

$$N := \mathrm{Gal}(K_{\mathfrak{a}}/H(\psi[\mathfrak{a}])).$$

Let $\mathfrak{p}$ be a prime of O such that $\mathfrak{p} \mid \mathfrak{a}$. We can consider the projections $M_{\mathfrak{p}}$ (resp. $N_{\mathfrak{p}}$) of M (resp. N) onto the $\mathfrak{p}$-primary part. Clearly, we have that $M_{\mathfrak{p}} \subset N_{\mathfrak{p}}$. We need to eliminate the possibility that $\{0\} = M_{\mathfrak{p}} \neq N_{\mathfrak{p}}$. Consulting [18, Theorem 2.6(3)], we see that this implies that $\mathfrak{p}^{-1}a \in H(\psi[\mathfrak{b}])$ but $\mathfrak{p}^{-1}a \notin H(\psi[\mathfrak{a}])$. This implies that the non-abelian extension $K_{\mathfrak{a}}^{a}/H$ is contained in the abelian extension $H(\psi[\mathfrak{b}])/H$, which is a contradiction. So $N_{\mathfrak{p}} \cong M_{\mathfrak{p}}$ for each $\mathfrak{p} \mid \mathfrak{a}$ and hence $M = N$.

□

Lemma 4.4.4. *For $\mathfrak{a}$ an ideal of O only divisible by primes of first degree and s an ideal of A, we have $n(\mathfrak{a}, s) = \frac{n(\mathfrak{a})m(s)}{\varphi((\mathfrak{a},s))}$, where $(\mathfrak{a}, s)$ denotes the gcd ideal of $\mathfrak{a}$ and s and $\varphi(\mathfrak{m}) = \#(O/\mathfrak{m})^{\times}$.*

Proof. Set $n_1 = [K_{\mathfrak{a}} : H]$ and $n_2 = [K_s : H]$. Set $\mathfrak{b} = \mathrm{lcm}(\mathfrak{a}, s)$ and $\mathfrak{b}' = \gcd(\mathfrak{a}, s)$ then we see that

$$K^a_{\mathfrak{a},s} = H(\psi[\mathfrak{b}], \mathfrak{a}^{-1}a),$$

and by **Lemma 4.4.3**, we have

$$[K^a_{\mathfrak{a},s} : H(\psi[\mathfrak{b}])] = [K^a_{\mathfrak{a}} : H(\psi[\mathfrak{a}])]$$

Furthermore,

$$\begin{aligned} n(\mathfrak{a}, s) &= [K^a_{\mathfrak{a}} : H(\psi[\mathfrak{a}])] \cdot [H(\psi[\mathfrak{b}]) : H] \\ &= [K^a_{\mathfrak{a}} : H(\psi[\mathfrak{a}])] \cdot [H(\psi[\mathfrak{a}]) : H] \cdot [H(\phi[s]) : H]/[H(\psi[\mathfrak{b}']) : H] \\ &= [K^a_{\mathfrak{a}} : H] \cdot [K_s : H]/\varphi(\mathfrak{b}') \\ &= n_1 \cdot n_2/\varphi(\mathfrak{b}') \end{aligned}$$

□

The goal of this section is to bound the degree of the different of $K^a_{\mathfrak{a},s}/H$.

Let $\mathfrak{p}'$ be a finite prime of $K^a_{\mathfrak{a},s}$. Let $\mathfrak{m}$ be the least common multiple ideal of $\mathfrak{a}$ and s.

Proposition 4.4.1. *The different exponent $d_{K^a_{\mathfrak{a},s}/H}(\mathfrak{p}') \leq 2e_{\mathfrak{p}'}(K^a_{\mathfrak{a},s}/H)$, as long as $\mathfrak{p}'$ does not lie above a prime of A which ramifies in O. If $\mathfrak{p}'$ does lie above a prime of A which ramifies in O, then $d_{K^a_{\mathfrak{a},s}/H}(\mathfrak{p}') \leq 4e_{\mathfrak{p}'}(K^a_{\mathfrak{a},s}/H)^2$.*

Proof. Let $\mathfrak{p}''$ be a prime of $H(\psi[\mathfrak{m}])$ which sits below $\mathfrak{p}'$, such that the ramification index of $\mathfrak{p}'$ over $\mathfrak{p}''$ is e. Let $d(\mathfrak{p}'')$ denote $d_{H(\psi[\mathfrak{m}])/H}(\mathfrak{p}'')$, and $d(\mathfrak{p}')$ denote $d_{K^a_{\mathfrak{a},s}/H(\psi[\mathfrak{m}])}$. The additivity of the different over towers is equivalent to the fact

$$d_{K^a_{\mathfrak{a},s}/H}(\mathfrak{p}') = ed(\mathfrak{p}'') + d(\mathfrak{p}').$$

By the principal ideal theorem [14], or **Theorem 3.9.5**, we have that the τ^0 term of $\psi_{\mathfrak{a}}$, say u, generates $\mathfrak{a}O'$ in O'. Note that $\psi_{\mathfrak{a}}$ is monic with all coefficients in O'. Let λ be such that $\psi_{\mathfrak{a}}(\lambda) = a$. Then $H(\psi[\mathfrak{m}], \lambda) = K^a_{\mathfrak{a},s}$. Therefore,

$$\begin{aligned} d(\mathfrak{p}') &\leq v_{\mathfrak{p}'}(\partial(\psi_{\mathfrak{a}}))(\lambda) \\ &= v_{\mathfrak{p}'}(u) \\ &= v_{\mathfrak{p}'}(\mathfrak{a}). \end{aligned}$$

Now, let P be the prime of A which sits below $\mathfrak{p}''$. Suppose that P does not ramify in O, so that $H(\psi[P])/H$ is tamely ramified at P. Further, the prime P is unramified in $H(\psi[M])/H$, if M is coprime to P. Therefore, the prime $\mathfrak{p}''$ is tamely ramified in $H(\psi[\mathfrak{m}])/H$. Hence, we have that $d(\mathfrak{p}') = e_{\mathfrak{p}''}(H(\psi[\mathfrak{m}])/H) - 1$. Ramification degrees are multiplicative in towers, so that

$$d_{K^a_{\mathfrak{a},s}/H}(\mathfrak{p}') \leq e_{\mathfrak{p}'}(K^a_{\mathfrak{a},s}) + v_{\mathfrak{p}'}(\mathfrak{a}).$$

Further, the extension H/k is unramified. Using this fact, we can see that $v_{\mathfrak{p}'}(\mathfrak{m}) = e_{\mathfrak{p}'}(K^a_{\mathfrak{a},s}/H)$, which gives the first statement of the proposition.

Suppose that P does ramify in O. We know that $e \leq d_{K^a_{\mathfrak{a},s}/H(\psi[\mathfrak{m}])}(\mathfrak{p}') + 1$. In this case,

$$d_{K^a_{\mathfrak{a},s}/H}(\mathfrak{p}') \leq v_{\mathfrak{p}'}(\mathfrak{m})^2 + 2v_{\mathfrak{p}'}(\mathfrak{m}).$$

Now, remember that Δ is the product of all primes of A which ramify in O. If $\mathfrak{m}$ is the lcm of $\mathfrak{a}$ and s, then $v_{\mathfrak{p}'}(\mathfrak{m}) \leq v_{\mathfrak{p}'}(\Delta)$ if $\mathfrak{p}' \mid \Delta$. So, we have $v_{\mathfrak{p}'}(\mathfrak{m}) \leq 2e_{\mathfrak{p}'}(K^a_{\mathfrak{a},s}/H)$, which gives the second part of the proposition.

□

We notice that $K^a_{\mathfrak{a},s}/H$ is unramified at any prime not dividing ∞ or $\mathfrak{m}$.

Proposition 4.4.2. *Let ∞' be a prime of $K^a_{\mathfrak{a},s}$ which lies above ∞. Then $d_{K^a_{\mathfrak{a},s}/H}(\infty')$ is bounded by a constant independent of $\mathfrak{a}$ and s.*

Let k_∞ be the completion of k at ∞. Let Ω be a fixed algebraic closure of k_∞.

A rank 1 O-lattice is a discrete O-submodule $\Lambda \subset \Omega$ such that $k\Gamma$ is a 1 dimensional vector space over k. Given such a $\Lambda \subset \Omega$ there exists an ideal $\mathfrak{D} \subset O$ and a non-zero element $\xi \in \Omega$ such that $\Lambda = \mathfrak{D}\xi$.

We define the exponential function associated to Λ by

$$e_\Lambda(z) = z \prod_{0 \neq r \in \Lambda} \left(1 - \frac{z}{r}\right),$$

for $z \in \Omega$. The function $e_\Lambda(z) : \Omega \to \Omega$ is entire, onto and $\mathbb{F}_r$-linear. It is periodic with group of periods Λ.

By [10, Theorem 7.2.15], such lattices are in correspondence with rank 1 sgn normalized Drinfeld modules defined over H. That is given such a Drinfeld module ψ, there exists a lattice Λ for which

$$\psi_b(e_\Lambda(z)) = e_\Lambda(bz),$$

for all $b \in O$ and

$$e_\Lambda(z) = \sum_{i=1}^{\infty} a_i z^{q^i},$$

with $a_i \in H$.

Let π be a uniformizing element for k_∞, so that $\mathrm{ord}_\infty(\pi) = 1$. Extend ord_∞ to Ω in the usual way.

Proposition 4.4.3 ([18], Proposition 3.2)**.** *Let $\mathfrak{a}$ be a non-zero ideal in O. Then*

1. *There exists a constant C_0 (may be negative) which depends only on k and on the* sgn-*normalized Drinfeld module ψ such that* $\mathrm{ord}_\infty(\lambda) \geq C_0$*, for any* $0 \neq \lambda \in \psi[\mathfrak{a}]$.

2. *We have*

$$\mathrm{ord}_\infty(\lambda) = \mathrm{O}(\deg \mathfrak{a})$$

   for any $0 \neq \lambda \in \psi[\mathfrak{a}]$, where the implied constant depends only on k and ψ.

3. *There exists a constant C_1 (may be negative), which depends only on ψ and a such that if α is any root of $\psi_{\mathfrak{a}}(x) - a = 0$, then*

$$\mathrm{ord}_\infty(\alpha) \geq C_1.$$

4. *Suppose that ∞_1 is any prime divisor of $H(\psi[\mathfrak{a}])$ sitting over ∞. Then the ramification index $e_{\infty_1}(K_{\mathfrak{a}}^a/L) = \mathrm{O}(1)$, where the implied constant only depends on ψ and a.*

Proof. Let $h = [H : k]$ be the class number of O. Then write $\mathfrak{a}^h = (\beta)$ for some positive element β. We will show $\mathrm{ord}_\infty(\lambda) \geq C_0$ for $0 \neq \lambda \in \psi[p]$.

Find the lattice Λ and ideal $\mathfrak{D}$ and element $\xi \in \Omega$ with $\Gamma = \mathfrak{D}\xi$ and e_Γ satisfies the functional equation corresponding to ψ. Given $\lambda \in \psi[\beta]$, there exists $d \in \mathfrak{D}$ with $\lambda = e_\Lambda(d\xi/\beta)$. By the Riemann-Roch theorem, **Theorem 3.1.1**, we can always find an element $d' \in \mathfrak{D}$ such that $d' \equiv d \pmod{\beta\mathfrak{D}}$ and $\mathrm{ord}_\infty(d') \geq \mathrm{ord}_\infty(\beta) - \deg \mathfrak{D} - 2g + 1$, 3.1.1.

This implies that $\zeta = d'\xi/\beta \in \Omega$ is such that $\lambda = e_\Lambda(\zeta)$ and $\mathrm{ord}_\infty(\zeta) \geq C_1$. Applying the exponential function to ζ, we obtain $\mathrm{ord}_\infty(\lambda) \geq C_0$.

This follows since e_Λ is an entire function so $\mathrm{ord}_\infty(\lambda)$ is bounded by the first n terms of $e_\Lambda(\zeta)$ for some n, and the existence of C_0 follows.

For an upper bound, we have

$$\lambda = \frac{d'\xi}{\beta} \prod_{0\neq c\in\mathfrak{D}} \left(1 - \frac{d'\xi/\beta}{c\xi}\right) = \frac{d'\xi}{\beta} \prod_{0\neq c\in\mathfrak{D}} \left(1 - \frac{d'}{\beta c}\right).$$

Since $\mathrm{ord}_\infty(\beta) = -h \deg \mathfrak{a}$, and $\mathrm{ord}_\infty(d') \leq 0$, we have

$$\mathrm{ord}_\infty(\lambda) \leq \mathrm{O}(\deg \mathfrak{a}) + \mathrm{ord}_\infty \left(\prod_{\substack{0\neq c\in\mathfrak{D} \\ \mathrm{ord}_\infty(d'/(\beta c))=0}} \left(1 - \frac{d'}{\beta c}\right) \right).$$

There are only finitely many choices of $0 \neq c \in \mathfrak{D}$ with $\mathrm{ord}_\infty(d'/(\beta c)) = 0$ because $\mathrm{ord}_\infty(c) = \mathrm{ord}_\infty(d') - \mathrm{ord}_\infty(\beta) \geq C_2$. Moreover, the number of these c is bounded by a constant depending only on $\mathfrak{D}$. To be sure, the number of such c is bounded by

$$\#\{c \in \mathfrak{D} \mid \mathrm{ord}_\infty(c) \geq -\deg \mathfrak{D} - 2g + 1\}$$

which is a finite number only depending on $\mathfrak{D}$.

For each such c, we have

$$\mathrm{ord}_\infty \left(1 - \frac{d'}{\beta c}\right) \leq \mathrm{ord}_\infty \left(\frac{1}{\beta c}\right) \leq \mathrm{O}(\deg \mathfrak{a}).$$

Let us now assume that $\mathrm{ord}_\infty(\alpha) < \mathrm{ord}_\infty(\lambda)$ for $\lambda \in \psi[\mathfrak{a}]$. Since

$$\psi_\mathfrak{a}(x) = x \prod_{0\neq\lambda\in\psi[\mathfrak{a}]} (x - \lambda)$$

we have

$$\mathrm{ord}_\infty(a) = \mathrm{ord}_\infty(\alpha) + \sum_{0\neq\lambda\in\psi[\mathfrak{a}]} \mathrm{ord}_\infty(\alpha - \lambda).$$

Now,

$$\mathrm{ord}_\infty(\alpha - \lambda) = \mathrm{ord}_\infty(\alpha),$$

for all $\lambda \in \psi[\mathfrak{a}]$. Thus,

$$\operatorname{ord}_\infty(\alpha) = \operatorname{ord}_\infty(a)/q^{\deg \mathfrak{a}}$$

Now, let us construct a finite extension of k_∞ which will contain $K_\mathfrak{a}^a$ as $\mathfrak{a}$ runs through all ideals of O.

This will imply our last statement of the theorem. We will also use this fact later.

Let $b \in O$ be a fixed positive element with $\deg(b) \geq 1$, and let α be a root of $\psi_b(x) = a$. Since e_Λ is surjective, let $\eta \in \Omega$ be such that $e_\Lambda(\eta) = \alpha$. Then

$$\psi_{\beta b} e_\Lambda(\eta/\beta) = \psi_b(\alpha) = a,$$

and so,

$$\psi_\mathfrak{a}(\psi_{\beta b/\mathfrak{a}}(e_\Lambda(\eta/\beta))) = a.$$

Now, $\psi_{\beta b/\mathfrak{a}}(e_\Lambda(\eta/\beta))$ is in the finite extension $k_\infty(\eta)/k_\infty$. Hence, all roots of the equation $\psi_\mathfrak{a}(x) = a$ lie in the extension $k_\infty(\eta, \xi)/k_\infty$. Hence $e_{\infty_1}(K_\mathfrak{a}^a/k)$ is bounded by the ramification index of $k_\infty(\eta, \xi)/k_\infty$ which is independent of $\mathfrak{a}$. □

Lemma 4.4.5. *Let H_∞ be the completion of H at ∞. There exists a finite extension H^* of H_∞ such that $K_{\mathfrak{a},s}^a \subset H^*$ for all $\mathfrak{a}, s$.*

Proof. Consider the field $H_\infty(\eta, \xi)$ from the proof of [18, Proposition 3.2, part (4)]. It is then clear that $H_\infty(\eta, \xi)$ contains fields of the form $K_\mathfrak{M}$. By setting $\mathfrak{M} = \mathfrak{a}s$, we see that $H_\infty(\eta, \xi)$ contains the required fields. □

Proposition 4.4.4. *We have the bound*

$$\frac{\deg \operatorname{Diff}(K_{\mathfrak{a},s}^a/H)}{n(\mathfrak{a}, s)} \ll \deg \mathfrak{a} + \deg s.$$

Proof. Let $\mathfrak{P}$ be a prime of H and write $\mathfrak{P} = \prod(\mathfrak{p}_i^{e_i})$, a product of primes of $K_{\mathfrak{a},s}^a$, and further such that $\sum_i f_i e_i = n(\mathfrak{a}, s)$ and $f_i = [\mathbb{F}_{\mathfrak{p}_i} : \mathbb{F}_\mathfrak{P}]$.

Now, since the constant fields of $K_{\mathfrak{a},s}^a$ and H are equal, we may write

$$\deg \mathfrak{p}_i = f_i \deg \mathfrak{P}.$$

Again, we may reduce the complexity of our problem by noticing that $K_{\mathfrak{a},s}^a/H$ is a Galois extension, and so f_i,e_i do not depend on i, and we write

$$n(\mathfrak{a}, s) = g_\mathfrak{P} f_\mathfrak{P} e_\mathfrak{P},$$

for each prime $\mathfrak{P}$ of H.

Therefore

$$\begin{aligned}
\frac{\deg \operatorname{Diff}(K^a_{\mathfrak{a},s}/H)}{n(\mathfrak{a},s)} &= \sum_{\mathfrak{P}\nmid\infty\Delta}\sum_{\mathfrak{p}|\mathfrak{P}} \frac{d_{K^a_{\mathfrak{a},s}/H}(\mathfrak{p})\deg\mathfrak{p}}{n(\mathfrak{a},s)} \\
&\quad + \sum_{\mathfrak{P}|\Delta}\sum_{\mathfrak{p}|\mathfrak{P}} \frac{d_{K^a_{\mathfrak{a},s}/H}(\mathfrak{p})\deg\mathfrak{p}}{n(\mathfrak{a},s)} \\
&\quad + \sum_{\mathfrak{P}|\infty}\sum_{\mathfrak{p}|\mathfrak{P}} \frac{d_{K^a_{\mathfrak{a},s}/H}(\mathfrak{p})\deg\mathfrak{p}}{n(\mathfrak{a},s)} \\
&= S_1 + S_\Delta + S_\infty
\end{aligned}$$

Now,

$$\begin{aligned}
S_1 &= \sum_{\mathfrak{P}|\mathfrak{a}s,\mathfrak{P}\nmid\Delta} \frac{g_\mathfrak{P} f_\mathfrak{P} 2 e_\mathfrak{P}\deg\mathfrak{P}}{g_\mathfrak{P} f_\mathfrak{P} e_\mathfrak{P}} \\
&\ll \sum_{\mathfrak{P}|\mathfrak{a}s} \deg\mathfrak{P} \\
&= \sum_{P|\mathfrak{a}s} f_P g_P \deg P \\
&\ll \deg\mathfrak{a} + \deg s.
\end{aligned}$$

The other terms are all bounded by a constant depending only on a, ϕ. To see this,

$$S_\Delta \le \sum_{\mathfrak{P}|\Delta}\sum_{\mathfrak{p}|\mathfrak{P}} \frac{4e^2_\mathfrak{P} f_\mathfrak{P}\deg\mathfrak{P}}{e_\mathfrak{P} f_\mathfrak{P} g_\mathfrak{P}}$$

which is bounded by the degree of the different of the field $K^a_{\Delta',\Delta}$ where $\Delta = \Delta'^2$ as ideals of O. This is because the extension $K^a_{\mathfrak{a},s}\cdot K^a_{\Delta',\Delta}/K^a_{\Delta',\Delta}$ is unramified at primes dividing Δ' or Δ by [14].

Finally,

$$S_\infty \le \sum_{\mathfrak{P}|\infty} \frac{C g_\mathfrak{P} f_\mathfrak{P}\deg\mathfrak{P}}{e_\mathfrak{P} f_\mathfrak{P} g_\mathfrak{P}} \ll \sum_{\mathfrak{P}|\infty}\deg\mathfrak{P} = O(1)$$

□

4.5 Kummer theory of Ribet and Bashmakov

We give a summary of the introduction to [26], which gives an overview of "Bashmakov's method" for showing that $\mathrm{Gal}(M_q/k(E[q]))$ are isomorphic to $E[q]^s$ for q large enough. To put things in context, we assume that V is an abelian variety defined over some number field k, V_n is the group of n-torsion, and $P_1, \ldots, P_s$ are points of V defined over k. We want to determine $\mathrm{Gal}(k(V_n, 1/nP_1, \ldots, 1/nP_s)/k(V_n)) \subset V_n^s$. The goal is to see that this group is equal to V_n^s for n coprime to some number M. Set G to be the absolute Galois group of k, then we have a representation $\rho : G \to \mathrm{Aut}(V_n)$, let H_n be its kernel and G_n be its image. Set O to be the ring of k endomorphisms of V.

Now, we have four axioms which form the framework for Bashmakov's method.

1. For almost all l, O/lO is equal to the commutant of G_l in $\mathrm{End}(V_l)$.
2. V_l is a semisimple G_l module, for almost all l.
3. For almost all l, the cohomology group $H^1(G_l, V_l)$ vanishes.
4. For each finitely generated subgroup Γ of $V(k)$, the division group
$$\Gamma' = \{Q \in V(k) \mid lQ \in \Gamma\},$$
is such that Γ'/Γ has finite exponent.

The usual consequence of these four axioms is that $\mathrm{Gal}(k(l^{-1}P_1, \ldots, l^{-1}P_n, V_l)/k(V_l))$ should be as large as possible for l large enough. The statement of theorems of this type depends on the structure of V. Two examples that work are:

1. V is an elliptic curve with or without CM.
2. V is an abelian variety of CM type.

Now, let us show how we hope to establish analogous facts for Drinfeld modules. The fourth condition will follow from [24, Theorem 1]. The third condition can be established by following Ribet's work, or Bashmakov's work,[25],[26],[3]. The first two axioms can be proved as in [25],[3], where we basically use the theorem of Pink and Rutsche [23, Theorem 0.1] as the analogue to the theorem of Serre [30]. We carry out this basic plan in the next section. We also have hope to calculate the Galois groups of Kummer extensions for higher rank Drinfeld modules in the future, as well as possibly Anderson's T-modules.

4.6 Kummer theory for Drinfeld modules

Note that the case of a completely singular Drinfeld module has been done in [22].

Following [25] and [26] we establish the following algebraic result. Then using cohomology and the work of Pink and Rutsche [23] will establish that $\mathrm{Gal}(K_q^\Gamma/K(\phi[q])) \cong \phi[q]^t$ for $\deg q$ large enough. In fact, [26] can be adapted to our case as well, but we will essentially prove a simpler result that works for our case.

Lemma 4.6.1. *Let V be an n-dimensional $\mathbb{F}_r$-vector space. Let $B = V^t$. Let $G = \mathrm{End}(V)$ and for $g \in G$ let $g \cdot (v_1, \ldots, v_t) = (gv_1, \ldots, gv_t)$. Let π_i be the projection from B to the ith component of B. Let C be a G submodule of B such that the restriction of π_i to C is onto V, and the restrictions of π_i are linearly independent over $\mathbb{F}_q$. Then $C = B$.*

Proof. By induction on t, the base case being trivial. Let

$$C' = \{(x_1, \ldots, x_t) : (x_1, \ldots, x_t, 0) \in C\}.$$

We want to show that C' satisfies the hypotheses of the lemma, with $B' = V^t$. The map $\pi_i : C' \to V$ is either surjective or zero for $1 \le i \le t$. Since we are allowed to multiply by G, if it is not zero, then it is onto. So suppose that $\pi_i = 0$. Without loss of generality take $i = 1$. Then $(x_1, \ldots, x_t, 0) \in C$ implies that $x_1 = 0$. Thus, we get an invertible matrix M such that $M\pi_{t+1} = \pi_1$. Now, we want to show that the G action implies that M is a multiple of the identity, which would be a contradiction to the assumption that π_i's are independent. For $b \in C$, let $N_b \in \mathrm{End}(V)$ be such that $\ker(N_b) = \mathrm{span}\{\pi_{t+1}(b)\}$. Now, multiplication by N_b gives that $(N_b\pi_1(b), \ldots, N_b\pi_{t+1}(b)) \in C$. So $N_b\pi_1(b) = 0$, and thus, $\pi_1(b) \in \mathrm{span}(\pi_{t+1}(b))$ for all b. Since π_{t+1} is onto π_1 must be dependent on π_{t+1}, which is a contradiction. Therefore π_1 is onto. The other conditions of the lemma are already satisfied. Thus $C' = B'$. But this implies that $C = B$ as required.

□

We want to show that $H_q = \mathrm{Gal}(K_q^\Gamma/k(\phi[q]))$ satisfies the conditions of **Lemma 4.6.1**. Just as in [25, Sections 2 and 3], there are several steps. Let $G = \mathrm{Gal}(K^{\mathrm{sep}}/K), H = \mathrm{Gal}(K^{\mathrm{sep}}/K(\phi[q]))$. For any element $a \in K$, let $R \in K^{\mathrm{sep}}$ be such that $\phi_q(R) = a$ and let

$$\xi_a(\sigma) = \sigma(R) - R,$$

so that $\xi_a : H \to \phi[q]$.

We must investigate the G action induced by ξ_a on $\phi[q]$. Certainly, for $g \in G$, we have $g(\sigma(R) - R) = \gamma \in \phi[q]$. Thus,

$$\xi_a(g\sigma g^{-1}) = g(\sigma(g^{-1}R) - g^{-1}R) = g(\sigma(R) - R) = g \cdot \xi_a(\sigma),$$

which makes sense because for $x \in K(\phi[q])$, we have $g^{-1}x \in K(\phi[q])$ and so is fixed by σ and so $g\sigma g^{-1}x = x$, so that $g\sigma g^{-1} \in H$. To complete the reasoning, notice that $\sigma(R - g^{-1}R) = R - g^{-1}R$ since σ fixes $K(\phi[q])$.

Notice that $g \cdot \xi_a(\cdot)$ only depends on the image of g when restricted to the field $K(\phi[q])$. From now on, assume that $\mathrm{Gal}(K(\phi[q])/K) \cong \mathrm{Aut}(\phi[q])$. We claim that the action of $\mathrm{Aut}(\phi[q])$ can be extended to $\mathrm{End}(\phi[q])$ (where $\phi[q]$ is regarded as an A/q vector space).

To see this, let $g, h \in G$ and $\mathrm{res}(g), \mathrm{res}(h)$ be their restrictions to $K(\phi[q])$. Define $(\mathrm{res}(g) + \mathrm{res}(h))\xi_a(\sigma) = g \cdot \xi_a(\sigma) + h \cdot \xi_a(\sigma)$. Now, since $\mathrm{Gal}(K(\phi[q])/K) \cong \mathrm{Aut}(\phi[q])$, we get an $\mathrm{End}(\phi[q])$ action on the image of ξ_a.

Lemma 4.6.2. *The cohomology group $H^1(\mathrm{Gal}(K(\phi[q])/K), \phi[q])$ is zero for almost all q.*

Proof. By [23, Theorem 0.1], we know that $\mathrm{Gal}(K(\phi[q])/K) \cong \mathrm{Aut}(\phi[q])$. We may also take q such that $\#(A/q) > 2$. Let $\gamma \in \mathrm{Aut}(\phi[q])$ be equal to $\theta\,\mathrm{id}_{\phi[q]}$, where $\theta \in A/q, \theta \neq 0, 1$. Then γ is in the center of $\mathrm{Aut}(\phi[q])$ and is such that the map $\gamma x - x$ is an automorphism of $\phi[q]$. Hence, by Sah's Lemma [21, Chapter 6, Lemma 10.2], the cohomology $H^1(\mathrm{Gal}(K(\phi[q])/K), \phi[q])$ is zero for almost all q. □

Let ξ be the map which takes $a \in K$ to $\xi_a : H \to \phi[q]$. Since H acts trivially on $\phi[q]$, we have that $\xi : K \to H^1(H, \phi[q])$, by abuse of notation. Further the map ξ is A-linear. That is, suppose that $g \in G$ restricts to $\theta\,\mathrm{id}_{\phi[q]}$, where $\theta \in A$ and $\theta \not\equiv 0 \pmod{q}$. We want to show that

$$g \cdot \xi_a(\sigma) = \xi_{\phi_\theta(a)}(\sigma), \text{ for all } a \in K, \sigma \in H.$$

Let $R \in K^{\mathrm{sep}}$ be such that $\phi_q(R) = a$, and $R' \in K^{\mathrm{sep}}$ be such that $\phi_q(R') = \phi_\theta(a)$. Then

$$\begin{aligned} g \cdot \xi_a(\sigma) &= \xi_a(g\sigma g^{-1}) \\ &= g \cdot (\sigma(R) - R) \\ &= \phi_\theta(\sigma(R) - R) \\ &= \sigma(\phi_\theta(R)) - \phi_\theta(R) \\ &= \xi_{\phi_\theta(a)}(\sigma) \end{aligned}$$

Now, consider the short exact sequence,

$$0 \to \phi[q] \to K^{\text{sep}} \to K^{\text{sep}} \to 0,$$

where the second map is inclusion, and the third is ϕ_q. Taking cohomology gives an injection

$$\phi(K)/\phi_q(\phi(K)) \hookrightarrow H^1(G, \phi[q]).$$

We also have a restriction map

$$H^1(G, \phi[q]) \hookrightarrow H^1(H, \phi[q]),$$

which is injective for almost all l because of the Serre-Hochschild spectral sequence, and because $H^1(G/H, \phi[q]) = 0$. Let us briefly write down the relevant exact sequence for general G, H and G-module A.

$$0 \to H^1(G/H, A^H) \to H^1(G, A) \to H^1(H, A)^{G/H} \to H^2(G/H, A^H) \to H^2(G, A)$$

But the first cohomology group is 0 (since $H^1(\text{Aut}(\phi[q]), \phi[q]) = 0$), and the third is a subset of $H^1(H, \phi[q])$.

Further, the map that ξ induces from $\phi(K)/\phi_q(\phi(K))$ to $H^1(H, \phi[q])$ is given by the composition of these two maps, and so is injective for almost all q.

Let $\varphi_i = \xi_{a_i}$ and let $\varphi : H \to \phi[q]^n$ be given by

$$\sigma \to (\varphi_1(\sigma), \varphi_2(\sigma), \ldots, \varphi_t(\sigma)).$$

The map φ induces another map, which we also denote by φ, from H_q to $\phi[q]^t$.

Let $C = \text{Im}(\varphi)$ and $B = \phi[q]^n$. Then C is an $\text{End}(\phi[q])$-invariant submodule of B. Now, consider the natural map $\Gamma/\phi_q(\Gamma) \to \Gamma/\phi_q(\phi(K)) \to \phi(K)/\phi_q(\phi(K))$. We need for the first map to be an injection for all but finitely many q. Let

$$\Gamma' = \{x \in K \mid \phi_m(x) \in \Gamma \text{ for some } m \in A\}.$$

By Poonen's theorem, there exists an infinite sequence $Q_1, Q_2, \ldots$ which generates the module $\phi(K)/\operatorname{tor}(\phi)$ freely. By our assumption that $\text{Gal}(K(\phi[q])K) = \text{Aut}(\phi[q])$, we know that $\operatorname{tor}(\phi)[q]$ is trivial. Let N be such that $\Gamma \subset A \cdot \{Q_1, \ldots, Q_n\}$. But then

$$\Gamma' \subset A \cdot \{Q_1, \ldots Q_n\}.$$

There exists $M \in A$ such that $\phi_M(\Gamma') \subset \Gamma$. Taking q coprime to M implies that each projection $\varphi_i(\cdot)$ is independent over A/q.

Finally, each projection is onto $\phi[q]$, again by taking $\deg q$ large enough.

Theorem 4.6.1. *The group* $\mathrm{Gal}(K_q^\Gamma/K(\phi[q]))$ *is isomorphic to* $\phi[q]^t$ *for all but finitely many primes* q*.*

Let $\mathfrak{q}$ be a prime of $K(\phi[q])$. We want to see that $K_q^\Gamma/K(\phi[q])$ is totally ramified at $\mathfrak{q}$ for the primes for which K_q^Γ/K is maximal (i.e. for almost all primes q). Let K_0 be the maximal extension of $K(\phi[q])$ in K_q^Γ which is unramified at $\mathfrak{q}$. Then $G_0 = \mathrm{Gal}(K_0/k(\phi[q]))$ is a $\mathrm{End}(\phi[q])$ stable submodule of $\phi[q]^t = \mathrm{Gal}(K_q^\Gamma/K(\phi[q]))$. If $G_0 \neq \{1\}$, then viewing $G_0 \subset \phi[q]^t$, we must have that the projection onto each component is either surjective or trivial. By reducing t if necessary, we may assume that each projection is surjective. It is clear that $G_0 \neq \phi[q]^t$, so by **Lemma 4.6.1**, the projections must be dependent over $\mathbb{F}_r$. That is, there exists $x_1, \ldots, x_t \in A$ such that

$$\begin{aligned} 0 &= x_1\pi_1(\sigma) + \cdots + x_t\pi_t(\sigma) \\ 0 &= \sigma(R) - R \end{aligned}$$

where $\phi_q(R) = a$ and $a = x_1a_1 + \cdots + x_ta_t$ and $R = x_1R_1 + \cdots + x_tR_t$. This implies that $a \in \phi_q(K)$ and so $a_1, \ldots, a_t$ is not linearly independent in $\Gamma/q\Gamma$, which is a contradiction. Therefore $M_0 = K(\phi[q])$. Therefore $K_q^\Gamma/K(\phi[q])$ is totally ramified at primes sitting above q.

This implies that there exists $m \in A$ such that $(s, m) = 1$ implies that $\mathrm{Gal}(K_s^\Gamma/K) \cong \phi[s]^t \rtimes \mathrm{Aut}(\phi[s])$, as well as the constant field of K_s^Γ must be $\mathbb{F}_r$ for these s.

Chapter 5

Analysis and proof of main results

5.1 Main Results

Let F be a global function field with constant field $\mathbb{F}_r$, $2 \nmid r$, and a fixed rational prime ∞ of F. Suppose that there is a field extension k/F such that k has constant field $\mathbb{F}_r$ and ∞ totally ramifies in k. Let A be the ring of functions of F regular everywhere except possibly ∞, and O the integral closure of A in k, which is therefore the ring of functions of k regular everywhere except possibly ∞', the unique prime lying above ∞. Let H be the Hilbert class field of O, so that H is the maximal unramified abelian extension of k such that ∞ splits in H.

Let $\phi : A \to C_\infty\{\tau\}$ be a rank 2 Drinfeld module with $\mathrm{End}(\phi) \neq A$ (this implies that k/F is degree 2). Then there is an isogenous Drinfeld module ϕ' with $\mathrm{End}(\phi') = O$. Let us assume that $\mathrm{End}(\phi) = O$ and let ψ be the associated rank 1 Drinfeld module $\psi : O \to C_\infty\{\tau\}$. Let η_x be the leading coefficient of ψ_x for each $x \in O$. Then there exists ψ' such that $\psi' : O \to O'\{\tau\}, \quad \eta_x \in \mathbb{F}_r$ and ψ is isomorphic to ψ' over $\overline{k}$. Let us replace ψ with ψ'. Denote by $K \subset H$, such that $\phi : A \to F\{\tau\}$. There are many examples of such global function fields k, F with rational prime ∞. Let us consider these situations as similar to the situation of [11]. In some ways, our situation is more general.

For a finite prime P of K of good reduction for ϕ, and $a \in K$ such that $a \in O_P$, the local ring at P, we may ask whether $a + R_P$ generates the field O_P/R_P as an A-module (given by the reduction of ϕ). If it does, then we say that a is a primitive point or root mod P. Let $x \in \mathbb{N}$, and let

$$N_a(x) = \#\left\{ P \text{ a finite prime of } K \;\middle|\; \begin{array}{l} \deg P = x, P \text{ splits completely in } H \\ a \text{ is a primitive root mod } P \end{array} \right\}.$$

Theorem 5.1.1. *Let $\phi : A \to K\{\tau\}$ be a Drinfeld module of rank 2. Let* $\mathrm{End}(\phi) = O$, *the integral closure of A in k which is a quadratic imaginary extension of F. Let H be the Hilbert class field corresponding to O and suppose that H/K is Galois. Suppose that ∞ ramifies in k, and suppose that $\psi : O \to O'\{\tau\}$ is a* sgn*-normalized rank 1 Drinfeld module corresponding to* $\mathrm{End}(\phi)$. *Let $a \in K \cap O'$, then there exists $\delta_\phi(a) > 0$ such that*

$$N_a(x) = \delta_\phi(a)\frac{r^x}{x} + \mathrm{O}\left(\frac{r^x \log x}{x^2}\right)$$

as x tends to infinity. Furthermore, the constant $\delta_\phi(a)$ can be expressed as an Euler product.

Let us now describe the situation of **Theorem 5.1.2**. Let $A = \mathbb{F}_r[T]$,$K = \mathbb{F}_r(T)$. Let $\phi_T = \Delta\tau^2 + g\tau + T\tau^0$ define the Drinfeld module $\phi : A \to K\{\tau\}$, where $g, \Delta \in A$ are chosen so that ϕ does not have complex multiplication (so $\mathrm{End}(\phi) = A$). Then K has infinite rank when considered as an A-module, so let $a_1, \ldots, a_t$ be t elements of K, which generate a free A-submodule of K. Let Γ be this submodule. Also, assume that all the fields $K_q^\Gamma = K(\phi[q], q^{-1}\Gamma)$ are geometric, where q runs over all monic irreducibles of A. For P a monic irreducible of A, such that ϕ has good reduction at P and $a_i \in O_P$ for all $1 \le i \le t$, let Γ_P be the submodule of $\phi(\mathbb{F}_P)$ generated by $a_1 + R_P, \ldots, a_t + R_P$. We say that $\phi(\mathbb{F}_P) = \Gamma_P$ to mean that P is as above and $\Gamma_P = \phi(\mathbb{F}_P)$ as sets. For $x \in \mathbb{N}$, define

$$N_\Gamma(x) = \#\{P \text{ prime} \mid \deg P = x, \quad \Gamma_P = \phi(\mathbb{F}_P)\}.$$

Theorem 5.1.2. *Let $x \in \mathbb{N}$, Γ be a rank t submodule of the rational points of ϕ and $\phi : \mathbb{F}_r[T] \to \mathbb{F}_r(T)\{\tau\}$. Suppose that $t \ge 18$. If all the fields K_q^Γ are geometric then there exists $\delta_\phi(\Gamma)$, such that*

$$N_\Gamma(x) = \delta_\phi(\Gamma)\frac{r^x}{x} + \mathrm{O}\left(\frac{r^x \log x}{x^2}\right)$$

as $x \to \infty$.

Otherwise there exists $r_0 \in \mathbb{N}$ and constants $\delta_\phi^1(\Gamma), \delta_\phi^2(\Gamma), \ldots, \delta_\phi^{r_0}(\Gamma)$ such that as $x \to \infty$ and $x \equiv j \pmod{r_0}$ then

$$N_\Gamma(x) = \delta_\phi^j(\Gamma)\frac{r^x}{x} + \mathrm{O}\left(\frac{r^x \log x}{x^2}\right).$$

Definition 5.1.1. *An extension of global function fields K/F is called geometric whenever they have the same constant field. That is if* $\overline{\mathbb{F}_p} \cap K = \overline{\mathbb{F}_p} \cap F$, *where* $\mathrm{Char}(K) = \mathrm{Char}(F) = p$.

Our intuition is that extensions of the constant field do not change the underlying geometry of the function field. Therefore, if the constant field stays the same in the extension field, this implies a fundamental change in the geometric object underlying the function fields.

5.2 Effective Chebotarev Density Theorem

For a more complete description see [8, Chapter 6].

Let L and L' be two global function fields with $\mathbb{F}_r \subset L \subset L'$. Let $G = \mathrm{Gal}(L'/L)$. Let $\mathbb{F}_L, \mathbb{F}_{L'}$ denote the constant fields of L and L' respectively.

Let $\sigma_{\mathfrak{P}}$ be the Artin symbol (which denotes a conjugacy class of G) for $\mathfrak{P}$ with respect to L'/L, and $d_L = [\mathbb{F}_L : \mathbb{F}_r]$, and $r_{L'} = [\mathbb{F}_{L'} : \mathbb{F}_L]$.

Also, for $\mathscr{C} \subset G$ a conjugacy class, define

$$\pi_{\mathscr{C}}(x) = \{\mathfrak{P} \mid \deg \mathfrak{P} = x, \mathfrak{P} \text{ is a prime unramified in } L'/L, \text{ and } \sigma_{\mathfrak{P}} \subset \mathscr{C}\}.$$

Theorem 5.2.1 ([8], Chapter 6, Section 4)**.** . *Let L'/L be a finite Galois extension with Galois group G. Let $\mathscr{C} \subset G$ be a conjugacy class whose restriction to $\mathbb{F}_{L'}$ is the a-th power of the Frobenius automorphism of $\mathbb{F}_L$. Then for $x \in \mathbb{N}$, if $x \not\equiv a \pmod{r_L}$, we have*

$$\pi_{\mathscr{C}}(x) = 0.$$

If $x \equiv a \pmod{r_L}$,

$$\left| \pi_{\mathscr{C}}(x) - r_L \frac{|\mathscr{C}|}{|G|} \frac{r^{d_L x}}{x} \right| \leq$$

$$\frac{2|\mathscr{C}|}{x|G|}((|G| + g_{L'} r_{L'})(r^{d_L x})^{1/2} + |G|(2g_L + 1)(r^{d_L x})^{1/4} + g_{L'} r_{L'} + |G|d/d_L),$$

where $g_{L'}, g_L$ denote the genus of L' and L respectively, and d is a constant depending on L($d = [L : \mathbb{F}_r(T)]$ where T is a separating element for $L/\mathbb{F}_r$).

Although the effective version is not explicitly listed as a theorem, one can trace through [8, Chapter 6, Section 4] to find all the constants.

5.3 Main term of Theorem 5.1.1

Let $N_a(x)$ be the number of primes of F of degree x which split completely in H and which satisfy Artin's conjecture; that is, they do not split completely in any $K^a_{\mathfrak{a},s}$. Say that a prime $\mathfrak{P}$ of H is of first degree if it lies over a prime P and the residue field extension is of degree 1. Note this is the same as the previous definition of a prime being first degree, except we have replaced K with F and k with H.

Let $N(x,y)$ be the number of primes of first degree of H with degree equal to x which do not split completely in any $K^a_{\mathfrak{a},s}$ with $\deg \mathfrak{a}, \deg s \leq y$.

Let $M_x(y_1, y_2)$ be the number of first degree primes of H of degree x which split completely in some $K^a_{\mathfrak{q}}$ or K_q with $y_1 \leq \deg \mathfrak{q} \leq y_2$ or $y_1 \leq \deg q \leq y_2$.

Proposition 5.3.1.

$$N_a(x) = [H:K]^{-1} N(x,y) + \mathrm{O}(M(y,x)).$$

Proof. We have that $N_a(x) \geq [H:K]^{-1} N(x,y) - M_x(y,x)$. This is because if $\phi[q] \subset \mathbb{F}_{\mathfrak{p}}$ implies that $2 \deg q \leq \deg x$, and $\psi[\mathfrak{q}] \subset \mathbb{F}_{\mathfrak{p}}$ implies that $\deg \mathfrak{q} \leq x$.

Now $N_a(x) \leq [H:K]^{-1} N(x,y)$ because any prime counted by the left hand side must split completely in H (and hence be a product of $[H:K]$ distinct primes of H, none of which split completely in any field $K^a_{\mathfrak{q}}$ or K_q). Hence, these primes certainly do not split completely in any field $K^a_{\mathfrak{q}}$ with $\deg \mathfrak{q} \leq y$ or K_q with $\deg q \leq y$.

□

To estimate $N(x,y)$, which we expect to be the main term, we use the effective Chebotarev density theorem **Theorem 5.2.1**.

Let us fix $\mathfrak{a}, s$, and take $L' = K^a_{\mathfrak{a},s}$ and $L = H$. We know that we may take $r_{L'} = d_L = 1$. Since we are interested in the primes which split completely, we let $\mathscr{C} = \{1\}$, and write let $\pi_{\mathfrak{a},s}$ denote π_C for this particular choice of L' and L. Let the genus of $K^a_{\mathfrak{a},s}$ be $g(\mathfrak{a}, s)$.

Proposition 5.3.2. *There exists a positive constant C' independent of $x, \mathfrak{a}, s$ such that*

$$\left| \pi_{\mathfrak{a},s}(x) - \frac{r^x}{n(\mathfrak{a},s)x} \right| \leq \frac{C' r^{x/2}}{x} \left(\deg \mathfrak{a} + \deg s \right).$$

Proof. Applying **Theorem 5.2.1** to our special case, we get

$$\left| \pi_{\mathfrak{a},s}(x) - \frac{q^x}{n(\mathfrak{a},s)x} \right| \leq$$

$$\frac{2}{xn(\mathfrak{a},s)}\left((n(\mathfrak{a},s)+g(\mathfrak{a},s))r^{x/2}+n(\mathfrak{a},s)(2g_H+1)r^{x/4}+g(\mathfrak{a},s)+n(\mathfrak{a},s)d\right),$$

where d is the degree of $H/\mathbb{F}_r(t)$ for some fixed separating transcendence element t.

We can use the Riemann-Hurwitz formula [27, Theorem 7.16] to bound the genus of $K^a_{\mathfrak{a},s}$ in terms of the different of $K^a_{\mathfrak{a},s}/H$ and g_H:

$$2g(\mathfrak{a},s)-2=n(\mathfrak{a},s)(2g_H-2)+d(\mathfrak{a},s)$$

Using this our formula becomes

$$\left|\pi_{\mathfrak{a},s}(x)-\frac{r^x}{n(\mathfrak{a},s)x}\right|\leq\frac{|C|}{xn(\mathfrak{a},s)}\left((n(\mathfrak{a},s)+d(\mathfrak{a},s))r^{x/2}+n(\mathfrak{a},s)r^{x/4}+d(\mathfrak{a},s)\right),$$

where C is a constant independent of $\mathfrak{a}, s$.

Write $\pi_1\leq\pi_{\mathfrak{a},s}(x)\leq\pi_1+\pi_2$. Let $2\leq d\leq n(\mathfrak{a},s)$. Let us count the primes of degree x with residue degree d. These correspond to a subset of primes of degree x/d in some subfield of H. Thus π_2 is bounded by $r^{x/2}$. Thus, we can take $\pi_{\mathfrak{a},s}(x)$ to count only the primes of first degree which split completely in $K^{\mathfrak{a}}_{\mathfrak{a},s}$.

Using **Proposition 4.4.4**, we obtain

$$\left|\pi_{\mathfrak{a},s}(x)-\frac{r^x}{n(\mathfrak{a},s)x}\right|\leq\frac{|C'|r^{x/2}}{x}\left(\deg\mathfrak{a}+\deg s\right).$$

□

Let

$$\begin{aligned}S&=\{\mathfrak{q}\subset O\mid\mathfrak{q}\text{ is a prime ideal of }O\text{ of first-degree}\}\\T&=\{q\subset A\mid q\text{ is a prime ideal of }A\}\\S_y&=\{\mathfrak{q}\in S\mid\deg\mathfrak{q}\leq y\}\\T_y&=\{q\in T\mid\deg q\leq y\}\end{aligned}$$

Let S^*, S^*_y be the set of ideals of O which are square-free products of ideals from S (resp. S_y), including 1. Define T^* and T^*_y similarly.

Proposition 5.3.3. *Let $y = \frac{\ln x - \ln 2}{\ln r}$ and let $x \to \infty$. Then*

$$\left| N(x,y) - \sum_{\substack{\mathfrak{a} \in S_y^* \\ s \in T_y^*}} \frac{\mu(\mathfrak{a})\mu(s) r^x}{n(\mathfrak{a}, s) x} \right| = \mathrm{O}\left(\frac{(r^{(3/4+\epsilon)x}}{x} \right),$$

for any $\epsilon > 0$.

Proof. Using the inclusion-exclusion principle we obtain that

$$N(x,y) = \sum_{\substack{\mathfrak{a} \in S_y^* \\ s \in T_y^*}} \mu(\mathfrak{a})\mu(s)\pi_{\mathfrak{a},s}(x).$$

Thus, we have the following estimate for $N(x,y)$

$$\left| N(x,y) - \sum_{\substack{\mathfrak{a} \in S_y^* \\ s \in T_y^*}} \frac{\mu(\mathfrak{a})\mu(s) r^x}{n(\mathfrak{a}, s) x} \right| \leq \frac{|C_3| r^{x/2}}{x} \left(\sum_{\substack{\mathfrak{a} \in S_y^* \\ s \in T_y^*}} \deg s + \deg \mathfrak{a} \right) \leq C_5 \frac{r^{x/2}}{x} \frac{r^{2y}}{y} (2^{C_4 r^y / y})$$

where the last inequality comes from counting

$$\begin{aligned} \#S_y &\leq C_1 r^y / y \\ \#T_y &\leq C_2 r^y / y, \end{aligned}$$

using the analogue of the prime number theorem [27, Theorem 5.12]. Taking x (and hence y) as large as we need, we can guarantee that $2^{C_4 r^y/y} \leq r^{x/4}$ for x large enough. Thus the remainder term is at most

$$C_6 r^{(3/4+\epsilon)x},$$

for any $\epsilon > 0$. □

Proposition 5.3.4. *The sum*

$$\delta = \sum_{\substack{\mathfrak{a} \in S^* \\ s \in T^*}} \frac{\mu(\mathfrak{a})\mu(s)}{n(\mathfrak{a}, s)},$$

converges absolutely. Further, as $x \to \infty$ we have

$$\left| N(x,y) - \delta \frac{r^x}{x} \right| = \mathrm{O}\left(\frac{r^x}{x^2} \right)$$

Proof. We see,

$$\sum_{\mathfrak{a} \in S^*, s \in T^*} n(\mathfrak{a}, s)^{-1} = \sum_{\mathfrak{a} \in S^*, s \in T^*} \frac{\varphi(\mathfrak{a}, s)}{n(\mathfrak{a}) m(s)}.$$

Thus

$$\sum_{\mathfrak{a} \in S^*, s \in T^*} \frac{\varphi(\mathfrak{a}, s)}{n(\mathfrak{a}) m(s)} = \sum_{\mathfrak{a} \in S^*} n(\mathfrak{a})^{-1} \prod_{q \in T} \left(1 + \frac{\varphi(\mathfrak{a}, q)}{m(q)} \right).$$

Now, the possible values for $m(q)$ are

$$m(q) = \begin{cases} r^{2 \deg q} - 1 & \text{if } q \text{ is inert in } O \\ r^{2 \deg q} - 2 \cdot r^{\deg q} + 1 & \text{if } q \text{ splits in } O \\ r^{2 \deg q} - r^{\deg q} & \text{if } q \text{ ramifies in } O \end{cases}$$

Since the number of q such that $\deg q = d$ is $\mathrm{O}(r^d/d)$, we see that the infinite product $\prod_{q \in T} (1 + m(q)^{-1})$ converges. Thus

$$\sum_{\mathfrak{a} \in S^*} n(\mathfrak{a})^{-1} \prod_{q \in T} \left(1 + \frac{\varphi(\mathfrak{a}, s)}{m(s)} \right) \ll \sum_{\mathfrak{a} \in S^*} n(\mathfrak{a})^{-1} \prod_{\substack{q \in T \\ (q, \mathfrak{a}) \neq 1}} \left(1 + \frac{\varphi(\mathfrak{a}, q)}{m(q)} \right).$$

Continuing

$$\sum_{\mathfrak{a} \in S^*} n(\mathfrak{a})^{-1} \prod_{q \in T} \left(1 + \frac{\varphi(\mathfrak{a}, q)}{m(q)} \right) \ll \sum_{\mathfrak{a} \in S^*} \frac{2^{\nu(\mathfrak{a})}}{n(\mathfrak{a})},$$

where $\nu(\mathfrak{a})$ is the number of prime divisors of $\mathfrak{a}$.

The latter product converges because $\sum n(\mathfrak{q})^{-1}$ converges by [18, Theorem 4.5], because our sum is over square free ideals which are products of first-degree primes, and the sum in [18] is over all square free ideals.

Exactly as in [18], we have

$$\sum_{\mathfrak{P} \in S} n(\mathfrak{P})^{-1} \ll \sum_{i=1}^{\infty} \frac{1}{i(r^i - 1)} < \infty,$$

because of the prime number theorem for O and $n(\mathfrak{P}) = r^{\deg \mathfrak{P}}(r^{\deg \mathfrak{P}} - 1)$ for $\deg \mathfrak{P}$ large enough.

Thus, let

$$\delta = \sum_{\substack{\mathfrak{a} \in S^* \\ s \in T^*}} \frac{\mu(\mathfrak{a})\mu(s)}{n(\mathfrak{a}, s)}$$

Consider

$$\left| \sum_{\substack{\mathfrak{a} \in S_y^* \\ s \in T_y^*}} \frac{\mu(\mathfrak{a})\mu(s)}{n(\mathfrak{a}, s)} - \delta \right| \leq \sum_{\substack{\mathfrak{a} \in S^* \backslash S_y^* \text{ or} \\ s \in T^* \backslash T_y^*}} n(\mathfrak{a}, s)^{-1} \leq \sum_{\substack{\mathfrak{a} \in S^* \backslash S_y^* \\ s \in T^*}} \frac{\varphi(\mathfrak{a}, s)}{n(\mathfrak{a}) m(s)} + \sum_{\substack{\mathfrak{a} \in S^* \\ s \in T^* \backslash T_y^*}} \frac{\varphi(\mathfrak{a}, s)}{n(\mathfrak{a}) m(s)}$$

By a similar argument the above estimate is bounded by a constant times the following,

$$\sum_{\mathfrak{a} \in S^* \backslash S_y^*} n(\mathfrak{a})^{-1} + \sum_{s \in T^* \backslash T_y^*} m(s)^{-1}.$$

But then we see that

$$\sum_{s \in T^* \backslash T_y^*} m(s)^{-1} \ll \sum_{q \in T \backslash T_y} m(q)^{-1} \prod_{\ell \in T} (1 + m(l)^{-1}).$$

Since the product appearing above converges, and because $m(q)^{-1} \leq (r^{\deg q} - 1)^{-2}$ for $\deg q$ large enough, we obtain that

$$\sum_{s \in T^* \backslash T_y^*} m(s)^{-1} \ll \sum_{j \geq y} \frac{r^j}{(r^j - 1)^2} \ll (r^y - 1)^{-1},$$

by the integral test and the Riemann hypothesis for function fields. A similar argument shows that

$$\sum_{\mathfrak{a} \in S^* \backslash S_y^*} n(\mathfrak{a})^{-1} \ll 1/x.$$

Thus,

$$|N(x, y) - \delta r^x / x| = \mathrm{O}\left(\frac{r^x}{x^2}\right)$$

□

Let $z = \frac{x}{2} - \nu \log x$, where ν is a constant to be chosen later such that $\nu \geq 1/\log r$.

$$M_x(y, x) \leq M_x(y, z) + M_x\left(z, x\right)$$

Proposition 5.3.5.

$$M_x(y, z) = \mathrm{O}\left(\frac{r^x}{x^2}\right).$$

Proof. Consider

$$M_x\left(y, z\right) \ll \sum_{\mathfrak{q} \in S_z \setminus S_y} \left(\frac{r^x}{n(\mathfrak{q})x} + \mathrm{O}\left(\deg \mathfrak{q} \frac{r^{x/2}}{x}\right)\right) + \sum_{q \in T_z \setminus T_y} \left(\frac{r^x}{m(q)x} + \mathrm{O}\left(\frac{r^{x/2}}{x} \deg q\right)\right)$$

Since $\nu \geq 1/\log r$, we have $r^z \leq r^{x/2}/x$. Thus, the sum of all the error terms above is bounded by

$$\frac{r^{x/2}}{x} \sum_{y \leq i \leq x/2 - \nu \log x} r^i \cdot i/i \ll r^{x/2+z}/x \ll r^x/x^2.$$

Now,

$$\sum_{q \in T_z \setminus T_y} m(q)^{-1} \ll \sum_{y < i \leq z} \frac{r^i}{(r^i - 1)^2} \ll \frac{1}{x}.$$

As before, a similar bound applies to the sum over $\mathfrak{q} \in S_z \setminus S_y$. Thus,

$$M_x\left(y, z\right) = \mathrm{O}\left(\frac{r^x}{x^2}\right).$$

□

To take care of both of the sums, we will require the use of a Brun-Titchmarsh type result, from [17, Theorem 4.3]. Let us state the result. Let $\mathfrak{U}$ be an ideal of O and b be an element in O with $\bar{b} \in (O/\mathfrak{U})^*$. Let $\pi(N; b, \mathfrak{U})$ denote the number of prime ideals $\mathfrak{P}'$ in O' such that if $N_{H/L}(\mathfrak{P}') = (\beta)$ for some positive element (i.e., $\mathrm{sgn}(\beta) = 1$), then $\beta \equiv b \pmod{\mathfrak{U}}$ and $\deg \beta = N$.

Theorem 5.3.1 ([17], Theorem 4.3)**.** *There exists effective constants C_7 and C_8, depending only on the genus g of L and the class number $h = [H : L]$, such that if $N > \deg \mathfrak{U} + C_7 +$*

$C_8 \log \deg \mathfrak{U}$, *then we have*

$$\pi(N; b, \mathfrak{U}) \leq \frac{C_9 h q^N}{\varphi(\mathfrak{U})(K_1 + 1 - 2g)},$$

where $\varphi(\mathfrak{U})$ *is the order of* $(O/\mathfrak{U})^*$ *and* K_1 *is equal to*

$$min\left\{\left[\frac{N-1}{h}\right], \left[\frac{N - \deg \mathfrak{U} - C_7 - C_8 \log \deg \mathfrak{U} + 4g}{2}\right]\right\},$$

and C_9 *is a positive effective constant depending only on* L.

Now,

$$M_x\left(z, x\right) \leq \sum_{\mathfrak{q} \in S \setminus S_z} \pi_{\mathfrak{q},1}(x) + \sum_{q \in T \setminus T_z} \pi_{1,q}(x)$$

Proposition 5.3.6.

$$\sum_{q \in T \setminus T_z} \pi_{1,q}(x) = \mathrm{O}\left(r^{x/2}\right).$$

Proof. For $q \in T \setminus T_z$, let $\mathfrak{U} = qO$. Apply the Brun-Titchmarsh theorem above to $\pi(x; 1, \mathfrak{U})$. To check the condition,

$$\deg \mathfrak{U} + C_7 + C_8 \log \deg \mathfrak{U} \leq x/2 + C_7 + C_8 \log x - C_8 \log 2 < x,$$

for x large enough. Now, if P splits completely in $K_{1,q}$ then $P \equiv 1 \pmod{q}$ by our work in the rank 1 case. If we allow h to be absorbed into the implicit constant, we see that

$$K_1 + 1 - 2g \gg N,$$

so that

$$\pi(x; 1, \mathfrak{U}) \ll \frac{q^x}{\varphi(\mathfrak{U})x}.$$

Now, by our choice of $\mathfrak{U}$, we have that $\varphi(\mathfrak{U}) \gg r^x/x$.

Thus,

$$\sum_{q \in T \setminus T_z} \pi_{1,q}(x) \leq \sum_{q \in T \setminus T_z} \pi(x; 1, qO) \ll \sum_{i \geq z} \frac{r^i}{(r^i - 1)^2} \ll r^{-z}.$$

Hence,

$$\sum_{q \in T \setminus T_z} \pi_{1,q}(x) \ll r^{x-z}/x = \mathrm{O}(r^{x/2}).$$

□

Proposition 5.3.7.

$$\sum_{\mathfrak{q}\in S\setminus S_z} \pi_{\mathfrak{q},1}(x) = \mathrm{O}\left(\frac{r^x \log x}{x^2}\right).$$

Proof. Let us write

$$\sum_{\mathfrak{q}\in S\setminus S_z} \pi_{\mathfrak{q},1}(x) = \sum_{\mathfrak{q}\in S\setminus S_{x/2+\log x}} \pi_{\mathfrak{q},1}(x) + \sum_{\mathfrak{q}\in S_{x/2+\log x}\setminus S_z} \pi_{\mathfrak{q},1}(x).$$

Consider first the sum $\sum_{\mathfrak{q}\in S\setminus S_{x/2+\log x}} \pi_{\mathfrak{q},1}(x)$. Let $\mathfrak{P}'$ be a prime of H which splits completely in $K_{\mathfrak{q},1}$ with $x/2+\log x < \deg \mathfrak{q} \leq x$. Then, write $N_{H/L}(\mathfrak{P}') = (\beta)$ for positive $\beta \in O$, with (β) prime. By 4.1.3, we have $\mathfrak{q} \mid (\beta - 1)$, and $\psi_{(\beta-1)\mathfrak{q}^{-1}}(a) \in \mathfrak{P}'$. Also, we have that $\deg \mathfrak{P}' = \deg \beta = \deg(\beta - 1)$. Hence

$$0 \leq \deg((\beta-1)\mathfrak{q}^{-1}) \leq x/2 - \log x$$

. Hence, the prime $\mathfrak{P}'$ divides the ideal in O generated by

$$\prod_{\substack{\mathfrak{M}\subset O \text{ an ideal} \\ 0\leq \deg \mathfrak{M} \leq x/2-\log x}} \psi_{\mathfrak{M}}(a).$$

Recall that

$$\psi_{\mathfrak{M}}(a) = \prod_{\lambda\in\psi[\mathfrak{M}]} (a-\lambda) \neq 0$$

since a is non-torsion. Also,

$$\begin{aligned} \deg \psi_{\mathfrak{M}}(a) &= -\operatorname{ord}_\infty(\psi_{\mathfrak{M}}(a)) \leq \deg a + \sum_{0\neq\lambda\in\psi[\mathfrak{M}]} \max\{\deg a, -\operatorname{ord}_\infty(\lambda)\} \\ &\leq r^{\deg \mathfrak{M}}(\deg a + C) \end{aligned}$$

where C is a positive constant, by **Proposition 4.4.3**.

The number of divisors of the above element of O of degree x is therefore less than

$$\deg\left(\prod_{\substack{\mathfrak{M}\subset O \text{ an ideal} \\ 0\leq \deg \mathfrak{M}\leq x/2-\log x}} \psi_{\mathfrak{M}}(a)\right)/x.$$

The number of ideals of O of degree i is $\mathrm{O}(r^i)$ (by the Riemann-Roch theorem **Theorem 3.1.1**[27, Theorem 5.4]). Thus, the number of primes we are interested in is bounded by

$$\mathrm{O}\left(\sum_{i=0}^{x/2-\log x} r^{2i}(\deg a + C)\right)/x = \mathrm{O}\left(\sum_{i=0}^{x/2-\log x} r^{2i}\right)/x = r^x/x^{2\log r+1} = \mathrm{O}\left(\frac{r^x}{x^2}\right).$$

We now want to bound the sum

$$\sum_{\mathfrak{q}\in S_{x/2+\log x}\setminus S_z} \pi_{\mathfrak{q},1}(x).$$

For $\mathfrak{q}$ in this range, we know that

$$\pi_{\mathfrak{q},1}(x) \leq \pi(x;1,\mathfrak{q}) \ll \frac{r^x}{r^{\deg\mathfrak{q}}\cdot x}.$$

Thus,

$$\sum_{\mathfrak{q}\in S_{x/2+\log x}\setminus S_z} \pi_{\mathfrak{q},1}(x) \ll \frac{r^x}{x}\sum_{\mathfrak{q}\in S_{x/2+\log x}\setminus S_z} \frac{1}{r^{\deg\mathfrak{q}}}$$

Using the prime number theorem [27, Theorem 5.12] for O we obtain

$$\sum_{\mathfrak{q}\in S_{x/2+\log x}\setminus S_z} \pi_{\mathfrak{q},1}(x) \ll \frac{r^x}{x}\cdot \sum_{z<i\leq x/2+\log x}\frac{1}{i} = \mathrm{O}\left(\frac{r^x\log x}{x^2}\right).$$

Thus, we conclude the proposition. □

Proposition 5.3.8. *If a is non-torsion then*

$$\delta_\phi(a) = \frac{1}{2}\sum_{\substack{\mathfrak{a}\in S \\ q\in T}} \frac{\mu(\mathfrak{a})\mu(s)}{n(\mathfrak{a},s)} > 0.$$

Proof. The sum converges absolutely, so we may write

$$\delta = \sum_{s \in T} \frac{\mu(s)}{m(s)} \sum_{\mathfrak{a} \in S} \frac{\mu(\mathfrak{a})\varphi((\mathfrak{a}, s))}{n(\mathfrak{a})}$$

But

$$\begin{aligned} \sum_{\mathfrak{a} \in S^*} \frac{\mu(\mathfrak{a})\varphi((\mathfrak{a}, s))}{n(\mathfrak{a})} &= \prod_{\mathfrak{q} \in S} \left(1 - \frac{\varphi((\mathfrak{q}, s)}{n(\mathfrak{q})}\right) \\ &= \prod_{\mathfrak{q} \in S} \left(1 - \frac{1}{n(\mathfrak{q})}\right) \prod_{\mathfrak{q} | s} \left(1 - [K_{\mathfrak{q}} : H(\psi[\mathfrak{q}])]^{-1}\right) \left(1 - n(\mathfrak{a})^{-1}\right)^{-1} \end{aligned}$$

For finitely many q, b we will have $\phi_q(b) = a$. We can adjust the terms for this, just as in [11],[18]. Multiply all such q to form the ideal Σ. Then

$$\begin{aligned} \delta \;=\; & \prod_{\mathfrak{q}} \left(1 - n(\mathfrak{a})^{-1}\right) \prod_{(q,\Sigma)=1, q \text{ inert}} \left(1 - m(q)^{-1}\right) \\ & \prod_{(q,\Sigma)=1, q=\mathfrak{q}_1\mathfrak{q}_2} \left(1 - m(q)^{-1}\right) \left(1 - [K_{\mathfrak{q}_1} : H(\psi[\mathfrak{q}_1])]^{-1}\right)^2 \left(1 - n(\mathfrak{q}_1)^{-1}\right)^{-2} \\ & \prod_{(q,\Sigma)=1, q|\Delta} \left(1 - m(q)^{-1}\right) \left(1 - [K_{\mathfrak{q}} : H(\psi[\mathfrak{q}])]^{-1}\right) \left(1 - n(\mathfrak{q})^{-1}\right)^{-1} \end{aligned}$$

Thus, we have $\delta > 0$, and since $\delta = \delta_\phi(a) \cdot 2$ the proposition follows. □

This concludes the proof of **Theorem 5.1.1**.

5.4 Proof of Theorem 5.1.2

Let $\pi(x, s)$ be the number of primes P of F of degree x with $\sigma_P \in \mathscr{C}_s$. Let $S = \{q \subset A \mid q \text{ is a prime ideal of } A\}$, S^* be the ideals which are square-free products of the ideals in S, $S_y = \{q \in S \mid \deg q \leq y\}$ and S_y^* be defined similarly to S^*.

Then

$$N(x, y) = \sum_{s \in S_y^*} \mu(s)\pi(x, s)$$

Proposition 5.4.1. *Let $q \in A$ be such that $[K_q^\Gamma : F] = |\phi[q]|^t \cdot \# \operatorname{Aut}(\phi[q]) = r^{2t \deg q} \cdot (r^{2\deg q} - 1)(r^{2\deg q} - r^{\deg q})$. Then*

$$|\mathscr{C}_q| \ll r^{\deg q(t+3)}$$

Proof. We want to count the number of pairs $(\chi, \gamma) \in \phi[q]^t \rtimes \operatorname{Aut}(\phi[q])$ such that either $\ker(\gamma - 1)$ is cyclic and $\chi(\Gamma) \subset \operatorname{Im}(\Gamma)$ or $\ker(\gamma-1) = \phi[q]$, and the rank of $\chi(\Gamma)$ is 0 or 1. The latter condition happens $\mathrm{O}(r^{\deg q(t+1)})($ times and the former condition happens $\sim r^{\deg q(3+t)}$ and combining both we get that $|\mathscr{C}_q| = r^{\deg q(3+t)} + \mathrm{O}(r^{\deg q(t+2)})$. These estimates are similar to the classical case for elliptic curves and are carried out by counting arguments for $\mathbb{F}_r$-vector spaces. □

Proposition 5.4.2.

$$\frac{|\mathscr{C}_s|}{n(s,\Gamma)} \ll r^{-\deg s(t-2)} \cdot \prod_{q|s} (r^{\deg q} - 1)^{-3},$$

as $\deg s \to \infty$.

Proof. Write

$$\frac{|\mathscr{C}_s|}{n(s,\Gamma)} = \frac{|\mathscr{C}_{s'}|}{n(s',\Gamma)} \frac{|\mathscr{C}_{s_0}|}{n(s_0,\Gamma)}.$$

Thus, since s_0 has at most finitely many possibilities, there exists constants C_7, C_8 such that $0 < C_7 \leq \frac{|\mathscr{C}_{s_0}|}{n(s_0,\Gamma)} \leq C_8 \leq 1$. Also,

$$\frac{|\mathscr{C}_{s'}|}{n(s',\Gamma)} \ll r^{\deg s'(t-2)} \prod_{q|s'} (r^{\deg q} - 1)^{-3} \leq r^{\deg s(t-2)} \prod_{q|s} (r^{\deg q} - 1)^{3},$$

hence the result. □

Proposition 5.4.3. *Let the constant field of K_s^Γ be $\mathbb{F}_s$ and let $r_s = [\mathbb{F}_s : \mathbb{F}_r]$. There exists constants $\delta(s,j) \geq 0$ for $j = 1, \ldots, r_s$ such that if $x \equiv j \pmod{r_s}$*

$$\left| \pi(x,s) - \delta(s,j) \frac{r^x}{x} \right| = \mathrm{O}\left(\frac{r^{x/2}}{x} \deg s \right).$$

Further, there exists a polynomial $M \in A$ such that if s is coprime to M, there exists a constant $\delta(s)$ such that

$$\left| \pi(x,s) - \delta(s) \frac{r^x}{x} \right| = \mathrm{O}\left(\frac{r^{x/2 + \deg s(t+3)}}{x} \deg s \right).$$

Proof. There are conjugacy classes $\mathscr{C}_1, \dots, \mathscr{C}_u$ of G_s such that

$$\mathscr{C}_s = \bigcup_{i=1}^{u} \mathscr{C}_i.$$

Let a_i be the integer such that $\mathscr{C}_i$ is the a_ith power of the Frobenius automorphism of $\mathbb{F}_s$.

Let

$$\delta(s,j) = r_s \left(\sum_{i, a_i \equiv j \pmod{r_s}} \mathscr{C}_i \right) n(s,\Gamma)^{-1}.$$

Let $g(s,\Gamma)$ be the genus of K_s^Γ. By the Riemann-Hurwitz formula [27, Theorem 7.16] and **Theorem 4.3.3**, we get that

$$g(s,\Gamma) \ll \frac{n(s,\Gamma)}{r_s}(2g_F - 2) + (t+2)\deg s.$$

Now, applying the Chebotarev density theorem **Theorem 5.2.1**, we get that

$$\left| \pi(x,s) - \delta(s,j)\frac{r^x}{x} \right| \ll \frac{\delta(s,j)}{x} n(s,\Gamma)(t+2)\deg s r^{x/2}$$

By **Proposition 5.4.2**, we know $\delta(s,j) \ll r^{\deg s(t+3)}$, so

$$\left| \pi(x,s) - \delta(s,j)\frac{r^x}{x} \right| \ll r^{\deg s(t+3)}(t+2)\deg s r^{x/2}.$$

□

Proposition 5.4.4. *Let $y = (\log x - \log C_9 - \log 4)/2$, and let r_0 be the degree of the constant field extension of K_M^Γ/K. With the understanding that $\delta(s,j)$ only depends on the residue class of $j \pmod{r_s}$ where r_s is the constant field extension degree of K_s^Γ/K, then as $x \equiv j \pmod{r_0}$ and $x \to \infty$,*

$$\left| N(x,y) - \sum_{s \in S_y^*} \mu(s)\delta(s,j)\frac{r^x}{x} \right| = \mathrm{O}(r^{x(1-\epsilon)}),$$

where N is the maximum of r_s for any s, and $\delta(s,j)$ is the corresponding density coming *from the Chebotarev density theorem.*

Proof. Summing over all $s \in S_y^*$, we get

$$\begin{aligned}
\left| N(x,y) - \sum_{s\in S_y^*} \mu(s)\delta(s,j)\frac{r^x}{x} \right| &= \mathrm{O}\left(\frac{r^{x/2}}{x} \sum_{s \in S_y^*} \deg s r^{\deg s(t+3)} \right) \\
&= \mathrm{O}\left(\frac{r^{x/2}}{x} x \prod_{q \text{ prime}, \deg q \leq y} (1 + r^{\deg q(t+3)}) \right) \\
&= \mathrm{O}\left(r^{x/2} 2^{C_4 r^y / y} r^{y r^y} \right) \\
&= \mathrm{O}\left(r^{x/2} r^{C_9 r^y y} \right)
\end{aligned}$$

Now, choose $y = (\log x - \log C_9 - \log 4)/2$ so that $r^{C_9 r^y y} \leq r^{x/4}$.

□

Proposition 5.4.5.

$$\delta_\phi^j(\Gamma) = \sum_{s \in S^*} \mu(s)\delta(s,j)$$

converges absolutely.

Proof. By taking the logarithms, we need only check the convergence of

$$\sum_{q \in S} \delta(q,j) \ll \sum_{i=0}^{\infty} \frac{r^i}{r^{i(t-2)}(r^i - 1)^3},$$

which does converge.

□

Proposition 5.4.6.

$$\left| \sum_{s \in S^*} \mu(s)\delta(s,j) r^x/x - \sum_{s \in S_y^*} \mu(s)\delta(s,j) r^x / x \right| = \mathrm{O}(r^x/x^2).$$

Proof. As usual,

$$\sum_{s \in S^* \setminus S_y^*} \delta(s,j) \ll \sum_{i \geq y} \frac{r^i}{r^{i(t-2)}(r^i-1)^3} \ll r^{-y(t+1)} = \mathrm{O}(x^{-(t+1)/2}).$$

so the difference we want is $\mathrm{O}(r^x/x^2)$ for $t \geq 3$. □

Consider the following bound from [1]. We restate it as follows

Proposition 5.4.7 ([1], Proposition 5.1)**.** *Let $l \geq 1$ be an integer, and let*

$$T_l := \{P \textit{ of good reduction for } \Gamma \textit{ such that } [\Gamma_P : \mathbb{F}_r] \leq l\}.$$

Then

$$\# T_l \leq C \cdot r^{l(1+2/t)}.$$

Now, if $\phi(\mathbb{F}_P)/\Gamma_P[q] \neq 0$ then $[\Gamma_P : \mathbb{F}_r] < x - z$ for any q with $\deg q > z$.

We will split the interval $(y, x]$ into $(y, \alpha x]$, $(\alpha x, \alpha x + A \log x]$, and $(\alpha x + A \log x, x]$ for a suitable choice of α and A. The first interval is handled by Chebotarev density theorem. The second interval is handled by the Brun-Titchmarsh theorem and the third is handled by the use of the proposition from [1]. Let us concentrate on the first interval which will determine the choice of α.

Proposition 5.4.8. *Let $\alpha = 1/10 - 2\log_r(x)/x$, then as $x \to \infty$*

$$M(y, \alpha x) = \mathrm{O}\left(\frac{r^x}{x^2}\right).$$

Proof. If we consider the restriction of $\sigma_P \in \mathscr{C}_q$ to $\mathrm{Gal}(K(\phi[q], q^{-1}a_1)/K)$ there are at most $\mathrm{O}(r^{4\deg q})$ possibilities for σ_P. The size of the Galois group is $r^{6\deg q} + \mathrm{O}(r^{5\deg q})$, so that using the Chebotarev density theorem again we obtain

$$M(y, \alpha x) \leq \sum_{q \in S_{\alpha x} \setminus S_y} \frac{r^{x - 2\deg q}}{x} + \mathrm{O}(r^{4\deg q} \cdot r^{x/2} x)$$

The sum of the error terms is $\mathrm{O}(r^{x(4\alpha + \alpha + 1/2)}) = \mathrm{O}(r^{x(1-\epsilon)})$. Then the error term is $\mathrm{O}(r^x/x^2)$. Now, the number of q with $\deg q = i$ is $\mathrm{O}(\frac{r^i}{i})$, thus the first summand is bounded by a constant times

$$\sum_{i \geq y} \frac{r^{x-i}}{xi} \ll r^{-y}\frac{r^x}{x^2} = \mathrm{O}\left(\frac{r^x}{x^2}\right).$$

□

Proposition 5.4.9. *Suppose that $t \geq 18$, then there exists $A > 0$ such that for $z = \alpha x + A \log x$,*

$$M(z, x) = \mathrm{O}(r^x/x^2),$$

as $x \to \infty$.

Proof. By **Proposition 5.4.7**[1, Proposition 5.1], the number of P's such that $\sigma_P \in \mathscr{C}_q$ with $\deg q > z$, and $\deg P = x$, is bounded by $\mathrm{O}(r^{(x-z)(1+2/t)})$.

Notice that $x - z = (9/10)x - (A - 2/\log r)\log x$.

This error is bounded by $\mathrm{O}(r^{0.9x(1+2/t)}x^{-(A\log r - 2)(1+2/t)}$. Notice that if we want r^x on top, we need that $t \geq 18$. As long as A is sufficiently large, we get an overall bound of

$$\mathrm{O}\left(\frac{r^x}{x^2}\right).$$

□

Proposition 5.4.10.

$$M(\alpha x, \alpha x + A\log x) = \mathrm{O}(r^x \log x/x^2)$$

as $x \to \infty$.

Proof. We now apply the Brun-Titchmarsh theorem along the interval $(\alpha x, \alpha x + A\log x]$. Suppose that $\sigma_P \in \mathscr{C}_q$ for some q with $\alpha x < \deg q \leq \alpha x + A\log x$. This now implies that $P \equiv 1 \pmod{q}$, because ϕ_{P-1} and ϕ_q must share a common root not equal to 0. Therefore, after reducing modulo q, the polynomial ϕ_{P-1} must not be separable. Therefore $q \mid P - 1$. Hence, we may apply the Brun-Titchmarsh theorem to get that

$$M(\alpha x, \alpha x + A\log x) \ll \sum_{\alpha x \leq i \leq \alpha x + A\log x} \frac{r^x r^i}{(r^i - 1)ix} = \mathrm{O}\left(\frac{r^x \log x}{x^2}\right).$$

□

Now, to examine the density

$$\sum \mu(s)\delta(s, j),$$

we note that for q large enough K_q^Γ/K is totally ramified at q and unramified outside $q\infty\Delta$. This implies that there exists $N_0 \in A$ and $r_0 \in \mathbb{N}$ such that for each $j = 1, \ldots, r_0$

$$\sum \mu(s)\delta(s, j) = \sum_{m|N_0} \mu(m)\delta(m, j) \prod_{(q,N_0)=1} (1 - \delta(q)).$$

If all the extensions K_q^Γ are geometric (corresponding to $r_0 = 1$) this leads to a constant as in the first part of **Theorem 5.1.2**. Otherwise, the densities corresponding to m for various $m \mid M$ may be zero or non-zero corresponding to different constants depending on the residue class of the degree, where r_0 is the degree of the constant field of K_M^Γ over $\mathbb{F}_r$.

Chapter 6

Future work

Very briefly, we can extend our work in several ways. Firstly, we hope to extend **Theorem 5.1.2** to include Drinfeld modules defined over more complex A, not just $A = \mathbb{F}_r[t]$. Also, we want to consider the problem of changing ϕ to having a higher rank but being completely singular (having CM by a rank 1 Drinfeld module). Another challenge would be to increase the rank of ϕ, with no additional assumptions. Finally, the most difficult part is to consider a situation where ϕ is rank $l \cdot d$, and has CM by ψ of rank d (which would combine knowledge of all situations).

Conjecture 6.0.1. *Let K have finite A-characteristic and let*

$$\phi : A \to K\{\tau\}$$

be a Drinfeld module.

Then given $a \in K, \overline{a}$ generates $\phi(\mathbb{F}_P)$ for infinitely many P, under suitable conditions on K, A, ϕ.

Conjecture 6.0.2. *Let $\phi : A \to K$ be a rank d Drinfeld module with CM by ψ which is of rank $\ell \mid d$. Let Γ be a free submodule of the rational points of ϕ. Assuming that the rank of Γ is sufficiently large, there exists $\delta_\Gamma(\phi)$ such that*

$$N_\Gamma(x) = \delta_\Gamma(\phi)\frac{r^x}{x} + \mathrm{o}\left(\frac{r^x}{x}\right).$$

Conjecture 6.0.3. *Let $E/\mathbb{Q}$ have CM by O_k. Then $E(\mathbb{F}_\mathfrak{p}) = O_k \cdot P$ for infinitely many primes $\mathfrak{p}$ of k.*

This is very similar to Artin's conjecture. If we can link the above conjecture to the Lang-Trotter conjecture, that would be interesting.

Let p be a rational prime which is inert in k, of good reduction for E. What is the relation between $E(O_k/pO_k)$ and $E(\mathbb{Z}/p\mathbb{Z})$. Of course the sizes of these sets are well-known to be related. The endomorphism ring of $E(O_k/pO_k)$ is large, so what more can be said?

Of course to do this there are several obstacles, which we will list below.

1. $(\phi(\mathbb{F}_P)/\Gamma_P)[q] = 0$ if and only if P lies in some conjugacy class $\mathscr{C}_s$ (in particular for more general A).

2. We need to determine the size of $\mathscr{C}_q$, or at least an asymptotic. To carry out these calculations for Drinfeld modules of higher rank than 2 may be more complicated (here "rank" does not mean the rank of the free subgroup Γ, but the rank of $\phi[a]$).

3. We need to know bounds for the number of P such that $\Gamma_P < y$, among other things. For guidance see [1]. This could get quite complicated if ψ is non-trivial, but ϕ is not completely singular.

4. We need to determine bounds for the degree of the different of K_q^Γ/K, $D(K_q^\Gamma/K)$. In particular, what if we take more general A? Gardeyn [9] only deals with $A = \mathbb{F}_q[T]$. Perhaps there is an easy trick to bypass this problem?

5. We need to develop the Kummer theory in this more general case. More general A may cause problems. If we keep track of ϕ, ψ it seems doable. In the case where ψ is rank 1, this has been done in [22].

References

[1] Amir Akbary and Dragos Ghioca. Periods of orbits modulo primes. *J. Number Theory*, 129(11):2831–2842, 2009.

[2] Emil Artin. *The collected papers of Emil Artin.* Edited by Serge Lang and John T. Tate. Addison–Wesley Publishing Co., Inc., Reading, Mass.-London, 1965.

[3] M. I. Bašmakov. Cohomology of Abelian varieties over a number field. *Uspehi Mat. Nauk*, 27(6(168)):25–66, 1972.

[4] Herbert Bilharz. Primdivisoren mit vorgegebener Primitivwurzel. *Math. Ann.*, 114(1):476–492, 1937.

[5] L. Carlitz. A set of polynomials. *Duke Math. J.*, 6:486–504, 1940.

[6] V. G. Drinfel′d. Elliptic modules. *Mat. Sb. (N.S.)*, 94(136):594–627, 656, 1974.

[7] V. G. Drinfel′d. Elliptic modules. II. *Mat. Sb. (N.S.)*, 102(144)(2):182–194, 325, 1977.

[8] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics].* Springer-Verlag, Berlin, third edition, 2008. Revised by Jarden.

[9] Francis Gardeyn. Une borne pour l'action de l'inertie sauvage sur la torsion d'un module de Drinfeld. *Arch. Math. (Basel)*, 79(4):241–251, 2002.

[10] David Goss. *Basic structures of function field arithmetic*, volume 35 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)].* Springer-Verlag, Berlin, 1996.

[11] Rajiv Gupta and M. Ram Murty. Primitive points on elliptic curves. *Compositio Math.*, 58(1):13–44, 1986.

[12] Rajiv Gupta and M. Ram Murty. Cyclicity and generation of points mod p on elliptic curves. *Invent. Math.*, 101(1):225–235, 1990.

[13] D. R. Hayes. Explicit class field theory for rational function fields. *Trans. Amer. Math. Soc.*, 189:77–91, 1974.

[14] David R. Hayes. Explicit class field theory in global function fields. In *Studies in algebra and number theory*, volume 6 of *Adv. in Math. Suppl. Stud.*, pages 173–217. Academic Press, New York, 1979.

[15] David R. Hayes. A brief introduction to Drinfel′d modules. In *The arithmetic of function fields (Columbus, OH, 1991)*, volume 2 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 1–32. de Gruyter, Berlin, 1992.

[16] Christopher Hooley. On Artin's conjecture. *J. Reine Angew. Math.*, 225:209–220, 1967.

[17] Chih-Nung Hsu. The Brun-Titchmarsh theorem in function fields. *J. Number Theory*, 79(1):67–82, 1999.

[18] Chih-Nung Hsu and Jing Yu. On Artin's conjecture for rank one Drinfeld modules. *J. Number Theory*, 88(1):157–174, 2001.

[19] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464. Academic Press, London, 1977.

[20] S. Lang and H. Trotter. Primitive points on elliptic curves. *Bull. Amer. Math. Soc.*, 83(2):289–292, 1977.

[21] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[22] Anly Li. A note on Kummer theory of division points over singular Drinfeld modules. *Bull. Austral. Math. Soc.*, 64(1):15–20, 2001.

[23] Richard Pink and Egon Rütsche. Adelic openness for Drinfeld modules in generic characteristic. *J. Number Theory*, 129(4):882–907, 2009.

[24] Bjorn Poonen. Local height functions and the Mordell-Weil theorem for Drinfel′d modules. *Compositio Math.*, 97(3):349–368, 1995.

[25] Kenneth A. Ribet. Dividing rational points on Abelian varieties of CM-type. *Compositio Math.*, 33(1):69–74, 1976.

[26] Kenneth A. Ribet. Kummer theory on extensions of abelian varieties by tori. *Duke Math. J.*, 46(4):745–761, 1979.

[27] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[28] Werner Schaal. On the large sieve method in algebraic number fields. *J. Number Theory*, 2:249–270, 1970.

[29] J.-P. Serre. "Résumé des cours de l'année scolaire," 1977-78. In *Œuvres. Vol. III*, pages 67–70. Springer-Verlag, Berlin, 1986.

[30] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[31] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[32] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.

[33] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[34] Yuichiro Taguchi. Semi-simplicity of the Galois representations attached to Drinfel′d modules over fields of "infinite characteristics". *J. Number Theory*, 44(3):292–314, 1993.