Torsion bounds for Drinfeld modules with complex multiplication

by

Andry Nirina Rabenantoandro

Dissertation presented for the degree of Doctor of Philosophy in the Faculty of Science at Stellenbosch University

Supervisor:	Co-supervisor:
Prof. F. Breuer	Prof. S. Wagner

March 2020

Declaration

By submitting this dissertation electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: March 2020

Abstract

Torsion bounds for Drinfeld modules with complex multiplication

A.N. Rabenantoandro

Department of Mathematical Sciences,
University of Stellenbosch,
Private Bag X1, Matieland 7602, South Africa.

Dissertation: PhD

March 2020

The main objective of the present thesis is to prove an analogue for Drinfeld modules of a theorem due to Clark and Pollack. The cardinality of the group of K-rational torsion points of an elliptic curve $E_{|K}$ with complex multiplication defined over a number field K of degree d is uniformly bounded by $Cd \log\log d$ for some absolute and effective constant $C > 0$, i.e. the constant $C > 0$ depends neither on E nor on K. Let F be a global function field over $\mathbb{F}_q$ and A the ring of elements of F regular away from a fixed prime ∞. Let $r \geq 1$ be an integer. We prove that there exists a positive constant $C_{A,r} > 0$ depending only on A and r such that for any field extension L of degree d over F and any Drinfeld A-module $\varphi_{|L}$ of rank r with complex multiplication defined over L and such that the endomorphism ring of φ is the maximal order in its CM field, the cardinality of the A-module of L-rational torsion points of φ is bounded by $C_{A,r} d \log\log d$. The constant depends neither on φ nor on L. For a given A and r the constant $C_{A,r}$ is effective and we get an explicit formula for it. The above result is not the full analogue of Clark and Pollack's theorem but rather a weaker version since it requires the endomorphism ring of φ to be the maximal order in its CM field. However, when $A = \mathbb{F}_q[T], F = \mathbb{F}_q(T)$ and $r = 2$ we obtain the full analogue of Clark and Pollack's result by proving the analogue of what they called the Isogeny Torsion Theorem in [CP15].

Uittreksel

Beperking van torsiepunte op Drinfeld-modules met komplekse multiplikasie

("Torsion bounds for Drinfeld modules with complex multiplication")

A.N. Rabenantoandro

Department van Wiskundige Wetenskappe,
Universiteit van Stellenbosch,
Privaatsak X1, Matieland 7602, Suid Afrika.

Proefskrif: PhD

Maart 2020

Die hoofdoel van hierdie tesis is om 'n analoog vir Drinfeld modules te bewys van 'n stelling te danke aan Clark en Pollack wat die volgende beweer. Die kardinaliteit van die groep K-rasionale torsiepunte van 'n elliptiese kromme $E_{|K}$ met komplekse vermenigvuldiging gedefinieÃńr oor 'n getalveld K van graad d is eenvormig begrens deur $Cd \log \log d$ vir 'n absolute en effektiewe konstante $C > 0$, dit wil sê die konstante $C > 0$ hang nie van E of van K af nie. Laat F 'n globale funksieveld oor $\mathbb{F}_q$ wees en A die ring van elemente van F reëlmatig weg vanaf 'n vaste priem ∞. Laat $r \geq 1$ 'n heelgetal wees. Ons bewys dat daar 'n positiewe konstante $C_{A,r} > 0$ is afhangende slegs van A en r sodanig dat vir enige velduitbreiding L van graad d oor F en enige Drinfeld A-module $\varphi_{|L}$ van rang r met ingewikkelde vermenigvuldiging gedefinieer oor L en sodanig dat die endomorphism ring van φ is die maksimale orde in sy CM-veld, die kardinaliteit van die A-module van L-rasionale torsiepunte van φ begrens word deur $C_{A,r}d \log \log d$. Die konstante hang nie van φ of van L af nie. Vir 'n gegewe A en r die konstante $C_{A,r}$ is effektief en ons kry 'n eksplisiete formule daarvoor. Die bogenoemde resultaat is nie die volledige analoog van Clark en Pollack se stelling nie, maar eerder 'n swakker weergawe, aangesien dit vereis dat die endomorfisme van φ die maksimale orde in sy CM-veld. Wanneer $A = \mathbb{F}_q[T], F = \mathbb{F}_q(T)$ en $r = 2$, verkry ons die volledige analoog van Clark en Pollack se resultaat deur die analoog te bewys van wat hulle die Isogeny Torsion Stelling in [CP15] genoem het.

Acknowledgements

First and foremost, I would like to express my utmost gratitude to my supervisor Prof. Florian Breuer for his guidance and support throughout the years of my PhD studies. Thank you for suggesting really interesting topics. Thank you for letting me be independent, for being such an inspiration and most importantly for your kindness. To Prof. Stephan Wagner, thank you for taking over the role of supervisor since Florian moved to Newcastle. I would also like to thank Dr. Gerard Razafimanantsoa (Baina) for being not only a mentor but also a very good friend. I wouldn't have gone this far without your help. To Dr. Luca Demangos, thank you for all the discussions we had, the patient explanations and for answering my questions. I am grateful to Prof. Marcel Wild for translating the abstract into afrikaans.

A word of thanks to Prof. Pete Clark and Prof. Paul Pollack for making their unpublished work available to me. It provided me with the last piece of the puzzle, so to speak, to finish up this thesis. I particularly appreciate the generosity with which Prof. Clark shared his ideas with me and his answering to my questions however naive they seemed to be.

For the time I spent in Muenster during the winter semester 2012-2013, I am grateful for the AIMS-DAAD funding. I have had the pleasure to meet and learn from Prof. Dr. Urs Hartl and his team: Rajneesh, Esmail, Anna, Tim and Simon.

I would like to thank the AIMS South Africa community. I hereby also acknowledge the support through the AIMS-DAAD scholarship during the first three years of my PhD.

My deepest appreciation goes to all my friends.

Last but not least, I wouldn't have been able to do any of this without the unconditional love and support of my family. Thank you dear Dad and Mom for all that you have done for me and for all the love. To my sister Hanitra and her husband Gabin, you guys are the best. Thank you for our little Anaïs. A few words of thanks also go to my second Dad Max, Mahery, Namby, Mialy, Manana, Mahenina, Ngola and our little treasures: Aro, Kanto, Manohy, Lango and Ranto. Most importantly, there are no words to express how grateful I am to my dear wife Mihaja for her love, patience, encouragement and support in difficult times. All I can say is: kilome.

Dedications

To mom and my late dad.

To Anaïs, my little ray of light.

Contents

Notations

Chapter 1: Preliminaries

§1.1 Drinfeld modules

$\mathbb{F}_q$: the finite field with q elements where q is a power of an odd prime p.

$\mathscr{C}$: a smooth, geometrically irreducible projective algebraic curve over $\mathbb{F}_q$.

F: the function field of $\mathscr{C}$.

h_F: the class number of F.

∞ a chosen closed point of $\mathscr{C}(\overline{\mathbb{F}_q})$ of degree d_∞ over $\mathbb{F}_q$.

$A = \Gamma(\mathscr{C} \setminus \{\infty\}, \mathscr{O}_{\mathscr{C}})$: the ring of functions on $\mathscr{C}$ regular away from ∞.

$\mathbf{Pic}(A)$: the class group of A.

v_∞: the normalized valuation associated to ∞.

F_∞: the completion of F at ∞.

$\mathbb{C}_\infty$: the completion of the algebraic closure of F_∞.

$\deg(\cdot)$: $-d_\infty v_\infty(\cdot)$.

$|\cdot|$: the normalized absolute value associated to ∞.

$\rho : A \to K$: the structure morphism of the A-field K.

τ : the q-th power Frobenius.

$K\{\tau\}$: the ring of twisted polynomials in τ.

$\mathbb{G}_{a,K}$: the additive group scheme over the field K.

φ: a Drinfeld A-module.

$\varphi(L)$: the Drinfeld A-module structure defined by φ extended to the field extension L/F.

$\mathrm{Drin}^r_A(K)$: the category of rank r Drinfeld A-modules over K.

$\hat{P}$: a dual of the isogeny P.

$\mathrm{End}_K(\varphi)$: the endomorphism ring of φ over K.

$\mathrm{End}(\varphi)$: the endomorphism ring of φ over $\overline{F}$.

φ/H: the quotient of φ by the finite A-submodule H of $\overline{K}$.

$\mathscr{O}_K$: the ring of integers of K.

$\varphi(L)_{\mathrm{tors}}$: the submodule of L-rational torsion points of φ.

$\varphi[\mathfrak{a}]$: the $\mathfrak{a}$-torsion points of φ, where $\mathfrak{a} \subseteq A$ is an ideal.

e_Λ : the exponential function associated to the lattice Λ.

φ^Λ: the Drinfeld module associated to the lattice Λ.

§1.2 On quadratic and Gorenstein orders

M_{tors}: the torsion submodule of the A-module M, where A is a Dedekind domain.

$\mathrm{Cl}(A)$: the class group of A.

$\mathrm{Ann}_A(M)$: the annihilator of the A-module M.

$\mathscr{O}_{\mathfrak{f}}$: the order of conductor $\mathfrak{f}$ in the quadratic extension K/F.

$R_{\mathfrak{m}}$: the localization of the A-module R at the maximal ideal $\mathfrak{m}$ of A.

$\mathrm{MaxSpec}(A)$: the maximal spectrum of A.

Chapter 2: Complex multiplication for Drinfeld modules

A, F, ∞ are as in Chapter 1.

§2.1 Orders and Picard groups

$I(\mathscr{O})$: the group of invertible fractional ideals of the order $\mathscr{O}$ in F.

$P(\mathscr{O})$: the group of principal fractional ideals of the order $\mathscr{O}$ in F.

$\mathbf{Pic}(\mathscr{O}) = I(\mathscr{O})/P(\mathscr{O})$: the Picard group of $\mathscr{O}$.

§2.2 Hayes theory of Drinfeld modules

τ_p: the p-th power Frobenius.

$\varphi : \mathscr{O} \to L\{\tau_p\}$: a Drinfeld $\mathscr{O}$-module over L.

$\mathrm{Drin}^r_{\mathscr{O}}(L)$: the category of rank r Drinfeld $\mathscr{O}$-modules over L.

$\mathscr{M}^r_{\mathscr{O}}(L)$: the set of isomorphism classes of rank r Drinfeld $\mathscr{O}$-modules over L.

$\mathscr{L}_r(\mathscr{O})$: the set of isomorphism classes of rank r $\mathscr{O}$-lattices in $\mathbb{C}_\infty$.

§2.4 Field of invariants

$F[\mathbf{X}]$: the polynomial ring over F with infinitely many indeterminates $\mathbf{X} = \{X_i\}_{i\geq 1}$.

$\mathrm{grad}(\cdot)$: a graduation defined on $F(\mathbf{X})$.

$F(\mathbf{X})_0$: the field of formal invariants, i.e. the homogeneous elements of $F(\mathbf{X})$ of grade 0.

$I_a(\varphi)$: the field of invariants of φ at a.

$I(\varphi)$: the smallest field of definition for φ.

§2.5 The main theorem of complex multiplication

$H_{\mathscr{O}}$: the common field of invariants of the $I(\varphi^{\mathfrak{a}})$'s for any invertible $\mathscr{O}$-ideal $\mathfrak{a}$, it coincides with the ring class field associated to the order $\mathscr{O}$.

$G_\infty := \mathrm{Aut}(\mathbb{C}_\infty/F)$: the group of F-automorphisms of $\mathbb{C}_\infty$.

$\mathscr{M}_{\mathscr{O}}^{r,*}(\mathbb{C}_\infty)$: the set of isomorphism classes in $\mathscr{M}_{\mathscr{O}}^{r}(\mathbb{C}_\infty)$ that contain some $\varphi^{\mathfrak{a}}$ for some invertible $\mathscr{O}$-ideal $\mathfrak{a}$.

$G_{\mathscr{O}} := \mathrm{Gal}(H_{\mathscr{O}}/F)$: the Galois group of $H_{\mathscr{O}}/F$.

$\sigma_{\mathfrak{p}}$: the Frobenius automorphism associated to the prime $\mathfrak{p}$ of $\mathscr{O}$.

$\mathfrak{C}$: the conductor of $\mathscr{O}$ in A.

Chapter 3: Torsion bounds for CM Drinfeld modules

$A, F, \infty, d_\infty, v_\infty, F_\infty, \mathbb{C}_\infty$ are as in Chapter 1.

d_F: the degree of the field extension $F/\mathbb{F}_q(T)$ where T is a fixed transcendental element of F over $\mathbb{F}_q$.

§3.3 Ray class field containment

$K^{(\mathfrak{a})}$: the $\mathfrak{a}$-ray class field of the field K associated to the ideal $\mathfrak{a}$ of $\mathscr{O}_K$.

$|\mathfrak{a}|_K := \#\mathscr{O}_K/\mathfrak{a}$: the norm of $\mathfrak{a}$ in K.

$\mathbb{P}_K$: the set of primes of K.

$\Phi_{\mathscr{O}_K}(\cdot)$: the analogue of the Euler totient function for K.

h_R: the class number of the Dedekind domain R.

$H_{\mathscr{O}_K}$: the hilbert class field of K.

$G_{\mathfrak{a}}$: the Galois group of $H_{\mathscr{O}_K}(\varphi[\mathfrak{a}])$ over $H_{\mathscr{O}_K}$ where φ is a rank one Drinfeld $\mathscr{O}_K$-module over $H_{\mathscr{O}_K}$.

§3.4 Uniform lower bound for the Euler function

$\mathscr{C}$ is as in Chapter 1

g: the genus of $\mathscr{C}$.

$|\mathscr{C}|$: the set of closed points, or primes, of $\mathscr{C}$.

Φ_{q^n}: the set of primes of $\mathscr{C}$ of degree n.

$\zeta_{\mathscr{C}}(s)$: the arithmetic zeta function associated to $\mathscr{C}$.

§3.5 Proof of the main result and the case $r = 1$

$\mathscr{D}_K^0$: the group of degree 0 divisors of K.

$\mathscr{P}_K$: the group principal divisors of K.

g_F: the genus of F.

$\mathscr{D}_F$: the group of divisors of F.

$\mathscr{L}(A)$: the Riemann-Roch space associated to A.

(A): the dimension of $\mathscr{L}(A)$.

(x): the principal divisor associated to $x \in F$.

$(x)_\infty$: the pole divisor of x.

§3.6 Uniform torsion bound for CM Drinfeld $\mathbb{F}_q[T]$-modules of rank 2

Λ_z: the lattice $< z, 1 >$ in the quadratic function field K.

D_z: the discriminant of z.

$\varphi_{|L}$: a rank 2 Drinfeld $\mathbb{F}_q[T]$-module over L with CM by an order $\mathscr{O}$ in the quadratic function field K.

$\mathrm{GL}_2(\mathbb{F}_q[T])$: the group of 2x2 invertible matrices with entries in $\mathbb{F}_q[T]$.

$\mathfrak{g}_L$: the absolute Galois group of L, $\mathrm{Gal}(L^{\mathrm{sep}}/L)$.

$\mathrm{Aut}(\varphi[g])$: the automorphism group of $\varphi[g]$ as an A-module, where $g \in \mathbb{F}_q[T]$.

$\mathrm{Aut}_{\mathscr{O}}(\varphi[g])$: the automorphism group of $\varphi[g]$ as an $\mathscr{O}$-module, where $g \in \mathbb{F}_q[T]$.

Introduction

Motivation

It is well known that there is a strong analogy between number fields and function fields. The later often serves as ground for testing open conjectures such as the famous Riemann hypothesis in the former and it is mostly easier to work in the function fields setting. But the investigations also go the other way around. Since this analogy has been discovered, mathematicians worked on establishing analogues of results in the number fields world to function fields. The main motivation of our work is to establish the analogue of a theorem due to Clark and Pollack [CP15] concerning uniform boundedness of rational torsions for elliptic curves with complex multiplication defined over number fields of fixed degree. The role of elliptic curves in the function field world is played by Drinfeld modules.

To put things in context it is essential to say something about the *strong uniform boundedness conjecture* for elliptic curves. For elliptic curves, the uniform boundedness conjecture has been proved by Mazur [Maz78] ($K = \mathbb{Q}$, i.e. $d = 1$), Kamienny [Kam92] ($d = 2$), Mazur and Kamienny ($d \leq 8$) and Abramovich [Abr95] ($d \leq 14$). Building on Mazur and Kamienny's works the full conjecture has finally been established by Merel in 1994, namely:

Theorem 0.1 ([Mer96], strong uniform boundedness conjecture)**.** *For all $d \in \mathbb{Z}, d \geq 1$ there exists a constant $B(d) \geq 0$ such that for all elliptic curves E over a number field K of degree d we have:*

$$\#E(K)_{\text{tors}} \leq B(d).$$

To the best of our knowledge this conjecture is still open for Drinfeld modules except for the rank 1 case due to Poonen [Poo97], and special instances for the rank 2 case, due to works of Schweizer [Sch03], Pal [Pal10] and Armana [Arm12].

Remark 0.2. Unfortunately, the method used by Merel in his proof of Theorem 0.1 is not effective. However, an effective bound which is exponential in d was later given by Parent [Par99].

A strong form of Theorem 0.1 is conjectured and it is still an open problem:

Conjecture 1. *The bound $B(d)$ in Theorem 0.1 can be made polynomial. More precisely $B(d)$ can be of the form $Cd \log \log d$ where C is an absolute positive constant.*

An even stronger bound is conjectured for the class of all elliptic curves without complex multiplication defined over number fields of fixed degree:

Conjecture 2. *There exists an absolute constant $C > 0$ such that for all number fields K of degree $d \geq 1$ and all elliptic curves $E_{|K}$ without complex multiplication (or non-CM),*

$$\#E(K)_{\text{tors}} \leq C\sqrt{d \log \log d}.$$

Breuer [Bre10] established the following result:

Theorem 0.3. *Let K be a finitely generated field of characteristic 0, E be an elliptic curve over K and $\gamma = \text{rank}_{\mathbb{Z}}(\text{End}_{\overline{K}}(E))/2$. Then, there exists a constant $C > 0$ depending on E and K such that for any finite extension L/K,*

$$\#E(L)_{\text{tors}} \leq C([L : K] \log \log [L : K])^{\gamma}.$$

When K is a number field, the bounds in Theorem 0.3 correspond to those in Conjectures 1 and 2 for CM and non-CM elliptic curves respectively, but with constant depending on the curve which makes the result substantially weaker than the said conjectures.

In light of Conjectures 1 and 2, it is natural to investigate what happens for the class of all elliptic curves with complex multiplication defined over fixed degree number fields. In fact, there are very few elliptic curves with complex multiplication defined over number fields (such curves have integral j-invariants and there are only finitely many of them, up to isomorphism, over fixed degree number fields). The remainder of this section will be devoted to explaining Clark and Pollack's result which confirms Conjecture 1 for the class of CM curves.

In [HS99], Hindry and Silverman give a uniform upper bound on the size of the set of rational torsion points of elliptic curves defined over number fields of fixed degree and with integral j-invariants, namely:

Theorem 0.4. *For all number fields K of degree $d \geq 2$ and all elliptic curves $E|_K$ with integral j-invariant $j(E)$ (i.e. $j(E) \in \mathscr{O}_K$), we have:*

$$\#E(K)_{\text{tors}} \leq 1977408\, d \log d.$$

One can easily see that the bound is uniform and polynomial. However, it is of order $d \log d$ which is higher than the order of the conjectured bound. Clark and Pollack, [CP15], give a bound on the size of the torsion subgroup of an elliptic curve with complex multiplication over a degree d number field up to an absolute constant factor. More precisely:

Theorem 0.5. *There is an absolute, effective constant C such that for all number fields K of degree $d \geq 3$ and all elliptic curves $E_{|K}$ with complex multiplication,*

$$\#E(K)_{\mathrm{tors}} \leq Cd \log\log d.$$

On one hand, the bound is stronger than that of Theorem 0.4, with an improvement of $d \log\log d$ over $d \log d$. On the other hand, it is weaker in the sense that Theorem 0.4 holds for a larger class of elliptic curves. Indeed, CM elliptic curves have integral j-invariants. However, Theorem 0.5 is interesting in view of Breuer's result [Bre10]:

Theorem 0.6. *Let $E|_F$ be an elliptic curve over a number field. Then there exists a constant $C(E, F) > 0$, a sequence of positive integers $3 \leq d_1 < d_2 < \cdots < d_n < \cdots$ and number fields $F_n \supset F$ with $[F_n : F] = d_n$ such that for all $n \in \mathbb{Z}^+$ we have*

$$\#E(F_n)_{\mathrm{tors}} \geq \begin{cases} C(E,F)d_n \log\log d_n \text{ if } E \text{ has CM} \\ C(E,F)\sqrt{d_n \log\log d_n} \text{ otherwise.} \end{cases}$$

Let $T_{\mathbf{CM}}(d)$ be the maximum size of the torsion subgroup of a CM elliptic curve defined over a degree d number field. Combining Theorem 0.5 and Theorem 0.6 yields:

Theorem 0.7. *$T_{\mathbf{CM}}(d)$ has upper order $d \log\log d$, that is:*

$$0 < \limsup_{d\to\infty} \frac{T_{\mathbf{CM}}(d)}{d \log\log d} < \infty.$$

This value has been computed in [CP17]:

Theorem 0.8.

$$\limsup_{d\to\infty} \frac{T_{\mathbf{CM}}(d)}{d \log\log d} = \frac{e^{\gamma}\pi}{\sqrt{3}}.$$

Clark and Pollack point out that this is the first instance of an upper order result for torsion points on a class of abelian varieties over number fields of varying degree.

Outline of the thesis

In this work, we aim to establish the analogue of Theorem 0.5 for CM Drinfeld modules, though we only fully achieve this for CM Drinfeld $\mathbb{F}_q[T]$-modules of rank 2. Assume that we always equip a field extension L of F with the inclusion homomorphism $A \to L$. Since we know that $\#\varphi(L)_{\mathrm{tors}}$ is finite it is natural to ask how it changes as a function of φ, L. The following conjectures are the analogues of the *Uniform Boundedness Conjectures*, see [Poo97].

Conjecture 3 (Weak form). *For fixed $A, r \geq 1$, and finite extension L of F, there is a uniform bound on $\#\varphi(L)_{\mathrm{tors}}$ as φ ranges over rank r Drinfeld A-modules over L.*

Conjecture 4 (Strong form). *For fixed $A, r \geq 1$ and $d \geq 1$, there is a uniform bound on $\#\varphi(L)_{\mathrm{tors}}$ as L ranges over finite extensions of F of degree less than or equal to d, and φ ranges over rank r Drinfeld A-modules over L.*

We will focus our attention and effort on Conjecture 4 which is the strongest form one can establish in the sense that d and r have to be fixed to get a uniform bound. Indeed, for any Drinfeld A-module φ over any finite extension L/F, the torsion submodule $\varphi(\overline{L})$ is infinite and this explains why we have to fix the degree d. On the other hand, suppose $\mathscr{C} = \mathbb{P}^1, F = \mathbb{F}_q(T)$. For any positive integer r, the roots of the polynomial $\varphi_T(X) = TX + a_1X^q + a_2X^{q^2} + \cdots + a_rX^{q^r} \in F[X]$ define a sub-vector space of $\overline{F}$ over $\mathbb{F}_q$ and any finite subspace of F over $\mathbb{F}_q$ arise in this manner. Each of these polynomials defines a Drinfeld $\mathbb{F}_q[T]$-module with F-rational torsion points of size at least the cardinality of the corresponding sub-vector space of roots. We can easily see that if r is allowed to vary, the submodule of F-rational torsion points is not bounded (even if d is fixed, here $d = 1$).

Although partial results were obtained by various authors around the uniform boundedness conjectures, they are still open as far as we know. The present thesis is concerned with the following type of questions:

How does $\#\varphi(L)_{\mathrm{tors}}$ vary with the degree $d = [L : K]$? with φ?

It is unreasonable to expect exact formulas for $\#\varphi(L)_{\mathrm{tors}}$ in terms of d in general. However, one can give an explicit bound on its size in terms of the degree d. The next natural question is that of uniformity if we allow the Drinfeld module to vary within a given family. Our interest lies in Drinfeld modules with complex multiplication and our strategy follows closely that in [CP15].

Chapter 1 introduces Drinfeld modules and their basic properties along with some results on quadratic and Gorenstein orders. Theorem 1.34 gives the structure of a quadratic order over a Dedekind domain and Theorem 1.44 shows that those orders are Gorenstein. Both the above mentioned results were privately communicated by Pete Clark to the author. The author filled in the details of the proofs.

Chapter 2 is an exposition about complex multiplication for Drinfeld modules based on [Hay79].

Chapter 3 constitutes the main body of our work. The proofs in this chapter are the author's with the following exceptions: the core results in Section 3.6.2, which were kindly provided by Pete Clark during our private communications and with the proofs expanded by the author to fill in the details, and the proof of Theorem 3.21 taken from [Ros02]. The two main results are Theorem 3.31 and Theorem 3.53. Theorem 3.31 gives a uniform torsion bound for Drinfeld A-modules of rank r with complex multiplication and integrally closed endomorphism rings. The strategy of proof consists roughly of the following steps:

- Start with a CM Drinfeld A-module of rank r defined over a degree d field extension L/F.
- Section 3.1: reduce to the rank one case and assume that the endomorphism ring is integrally closed in its CM-field.
- Section 3.2: identify a field over which the reduced module is defined.
- Section 3.3: prove a ray class field containment result and deduce a lower bound for the degree d in terms of the class number of the endomorphism ring and some value of the Euler totient function associated to it.
- Section 3.4: bound the Euler totient function uniformly from below basically by using a generalized version of Mertens theorem due to Lebacque, [Leb07]. The main task here is to make Lebacque's theorem explicit, Theorem 3.20, and deduce some useful inequalities. The main result is given by Theorem 3.28.
- Section 3.5: prove Theorem 3.31 and deduce a result of Poonen [Poo97].

Theorem 3.53 is the full analogue of Theorem 0.5 for CM Drinfeld $\mathbb{F}_q[T]$-modules of rank 2. The idea is to reduce to Theorem 3.31 by proving an analogue of the Isogeny Torsion Theorem, Theorem 3.40.

The constants in our results are all explicit. For the case of elliptic curves, making Clark and Pollack's results explicit is a bit delicate and is the subject of an ongoing investigation by some of our colleagues.

Chapter 1

Preliminaries

The main purposes of this first chapter are to give some results on Gorenstein orders, which will be useful later on, and to introduce the main objects of study: Drinfeld modules. The emphasis will be on studying the torsion parts so we will adjust our exposition accordingly. There are several wonderful sources from which one can read about the basics on Drinfeld modules, we only give a non-exhaustive list: [Gos98] treats the basics and further introduces two generalisations, namely T-modules and shtukas. For more arithmetical flavour, one can consult [Ros02]. In [Sal06], Drinfeld modules are introduced in view of their applications to class field theory for global function fields as in [Hay79] but with more modern notations.

1.1 Drinfeld modules

Throughout the thesis we are going to work in the setting of global function fields, i.e. finite extensions of fields of rational functions over a finite field of one independent variable. This type of fields has a geometric realization as function fields of projective algebraic curves that makes their study suitable for algebraic geometric approach. Our main references for global function fields are [Ros02] and [Sti09].

Let $\mathscr{C}$ be a smooth, geometrically irreducible projective algebraic curve over the finite field $\mathbb{F}_q$, where $q = p^s$ with p an odd prime number and $s > 0$ an integer. Fix a closed point $\infty \in \mathscr{C}(\overline{\mathbb{F}}_q)$ of degree d_∞ over $\mathbb{F}_q$. We denote by F the function field of $\mathscr{C}$ and by $A = \Gamma(\mathscr{C} \setminus \{\infty\}, \mathscr{O}_{\mathscr{C}})$ the ring of functions on $\mathscr{C}$ regular away from ∞. Rings that arise in such a way are called *Drinfeld rings*. It is well known that A is a Dedekind domain with finite class number $|\text{Pic}(A)| = d_\infty h_F$ where h_F is the class number of F.

The closed point ∞ gives rise to a normalized valuation v_∞ (d_∞ is the degree of the residue field of ∞ over $\mathbb{F}_q$). We denote by F_∞ the completion of F with respect to v_∞, and $\mathbb{C}_\infty = \widehat{\overline{F}}_\infty$ is the completion of a fixed algebraic closure of F_∞ which is also algebraically closed (Krasner's lemma).

For $x \in F_\infty$ we set $\deg(x) = -d_\infty v_\infty(x)$ which gives rise to an absolute value $|x| = q^{\deg(x)}$ that extends to $\mathbb{C}_\infty$. For $a \in A$ we have $|a| = \#(A/aA) = q^{\deg(a)}$.

This setting is in analogy with the characteristic zero world where A plays the role of $\mathbb{Z}$, F the role of $\mathbb{Q}$, F_∞ and $\mathbb{C}_\infty$ respectively the role of $\mathbb{R}$ and $\mathbb{C}$. Many of the differences that break the analogy between number fields and global function fields come from the fact that F_∞ is an infinite extension of $\mathbb{C}_\infty$ but $[\mathbb{R} : \mathbb{C}] = 2$.

In 1974, Vladimir Drinfeld introduced what he called Elliptic Modules [Dri74] (due to their similarities with elliptic curves) in order to prove the Langlands conjecture for function fields in dimension 2. The aim of this section is to introduce Drinfeld Modules which is now the standard name of these objects. A good introduction to Drinfeld modules can be found in [Bre02].

1.1.1 Definition

We know that for a field K there exists a canonical map $\rho : \mathbb{Z} \to K$ that sends 1 to 1_K and the characteristic of K is either 0 (if ρ is an embedding) or a prime p (the generator of $\ker \rho$). If we replace $\mathbb{Z}$ by A we get the notion of an A-field.

Definition 1.1. *An A-field is a pair (ρ, K) where $\rho : A \to K$ is a non-zero ring morphism and K a field. The morphism ρ is called the* structure homomorphism *of K. The prime ideal $\mathfrak{p} =: \ker \rho$ is called the* A-characteristic *of K. We say that K has generic characteristic if $\mathfrak{p} = (0)$. Otherwise, we say that K has finite or special characteristic.*

For the rest of this chapter we fix an A-field (ρ, K) where K is a subfield of $\mathbb{C}_\infty$ and we will write K instead of (ρ, K). Note also that the condition saying that ρ is non-zero forces K to be of characteristic p.

Denote by $\tau : \mathbb{C}_\infty \to \mathbb{C}_\infty$, $x \mapsto x^q$ the q^{th}-power Frobenius. The ring of *twisted polynomials* in τ over K, $K\{\tau\}$, is the non-commutative ring of polynomials in τ subject to the multiplication rule:

$$\tau a = a^q \tau, \ \forall a \in K. \tag{1.1.1}$$

Proposition 1.2. *The ring $K\{\tau\}$ has a right division algorithm and every left ideal of $K\{\tau\}$ is principal which makes it into a left principal ideal domain (PID).*

Proof. See section 1.6 of the first chapter of [Gos98]. Essentially such type of rings has a right division algorithm. □

If K is perfect, i.e $\tau(K) = K$, then $K\{\tau\}$ also admits a left division algorithm.

We let $\mathbb{G}_{a,K}$ be the additive group scheme of K. The endomorphism ring $\operatorname{End}\mathbb{G}_{a,K}$ of $\mathbb{G}_{a,K}$ is the ring of $\mathbb{F}_q$-linear polynomials in $K[X]$ equipped with addition and composition of polynomials, these are exactly the polynomials of the form $f(X) = \sum\limits_{i=0}^{n} a_i X^{q^i}$, $a_i \in K$. The ring $K\{\tau\}$ is naturally isomorphic to $\operatorname{End}\mathbb{G}_{a,K}$ by the isomorphism $\sum\limits_{i=0}^{n} a_i\tau^i \longmapsto \sum\limits_{i=0}^{n} a_i X^{q^i}$.

Definition 1.3. *A* Drinfeld A-module *over K is an $\mathbb{F}_q$-algebra homomorphism:*

$$\begin{aligned} \varphi : A &\longrightarrow K\{\tau\} = \operatorname{End}\mathbb{G}_{a,K} \\ a &\longmapsto \varphi_a \end{aligned}$$

satisfying the following conditions:

1. *There exists $a \in A$ such that $\varphi_a \notin K$. (Non triviality)*
2. *The constant term of φ_a is $\rho(a)$ for all $a \in A$. (Normalization)*

The definition of a Drinfeld module depends a priori on a choice of an A-field. We will say that φ has generic or special characteristic if its underlined A-field has the corresponding property.

Note that φ endows K with an A-module structure: $a.x := \varphi_a(x)$ for $a \in A$ and $x \in K$. This can be thought of as a deformation of the usual action of A on K. This action extends to any A-algebra and in particular to any extension L of K in the obvious way and we denote the resulting module $\varphi(L)$.

Furthermore, if φ has generic characteristic, F is a subfield of K and we can talk about Drinfeld modules over extensions L of F and L-rational torsion points.

Remark 1.4. It is important to note that for $a \in A$ and $x \in K$ we obtain $\varphi_a(x)$ by evaluating the powers of the Frobenius in $\varphi_a(\tau)$ at x but not just merely replacing any occurrence of τ by x.

We now define the most important invariant of a Drinfeld module:

Theorem 1.5 (Rank of a Drinfeld module). *Let $\varphi : A \to K\{\tau\}$ be a Drinfeld module. Then there exists a positive integer r, called the* rank *of φ, such that for all $a \in A$, $\deg_\tau(\varphi_a) = r\deg(a)$.*

One can consult any of the above mentioned references for the proof. Rank one Drinfeld modules are called Carlitz modules and they provide an analogue of the cyclotomic theory in characteristic 0. On the other hand, the rank two case corresponds to elliptic curves.

Since every φ_a has positive degree in τ for $\deg(a) > 0$, by Theorem 1.5 we have

Proposition 1.6. *Let $\varphi : A \to K\{\tau\}$ be a Drinfeld module. Then φ is an embedding.*

We now define another integer attached to a Drinfeld module φ. Assume that $\mathrm{char}(\varphi) = \mathfrak{p} \neq (0)$ and let $v_\mathfrak{p}$ be the normalized valuation on F associated to $\mathfrak{p}$. For a non zero $a \in A$, denote by $\mathrm{ord}(\varphi_a)$ the smallest integer $t \geq 0$ such that τ^t occurs in φ_a with non zero coefficient.

Theorem 1.7 (Height of a Drinfeld module). *There exists a positive integer h_φ, called the* height *of φ, such that*

$$\mathrm{ord}(a) = h_\varphi v_\mathfrak{p}(a)\deg(\mathfrak{p})$$

for all $a \in A$.

If $\mathrm{char}(\varphi) = (0)$, we define $h_\varphi = 0$. We can easily see that Carlitz modules are of height 0 or 1 depending on whether the characteristic of K is generic or special, Drinfeld modules of generic characteristic have height 0.

Remark 1.8. It is not at all clear from the definition that Drinfeld modules exist, but they do. There is also an analytic theory of Drinfeld modules over $\mathbb{C}_\infty$ that parallels that of elliptic curves.

1.1.2 Morphisms

In this section we describe the category $\mathrm{Drin}^r_A(K)$ of rank r Drinfeld A-modules over a field K. Let $\varphi : A \to K\{\tau\}$ and $\psi : A \to K\{\tau\}$ be two Drinfeld modules of rank r over K.

Definition 1.9. *A* morphism *from φ to ψ over K is an element P of $K\{\tau\}$ such that:*

$$P\varphi_a = \psi_a P, \textit{ for all } a \in A.$$

A non zero morphism is called an isogeny.

In other words, an isogeny between φ and ψ is an $\mathbb{F}_q$-linear polynomial such that for all $a \in A$ the diagram

$$\begin{tikzcd}
\mathbb{G}_{a,K} \arrow[r, "\varphi_a"] \arrow[d, "P"'] & \mathbb{G}_{a,K} \arrow[d, "P"] \\
\mathbb{G}_{a,K} \arrow[r, "\psi_a"'] & \mathbb{G}_{a,K}
\end{tikzcd}$$

commutes. We see that an isogeny P acts on $\mathbb{G}_{a,K}$ and we define the kernel of P, denoted $\operatorname{Ker} P$, to be the geometric kernel of this action. Hence $\operatorname{Ker} P$ is the A-module formed by the roots of $P(x)$ in $\overline{K}$. An isogeny is actually a surjective morphism with finite kernel, i.e., an isogeny between algebraic groups. Note that two *isogenous* Drinfeld modules must have the same rank and characteristic.

We use the notation $P : \varphi \to \psi$ to mean that P is an isogeny from φ to ψ. The set of morphisms from φ to ψ over K is denoted $\operatorname{Hom}_K(\varphi, \psi)$, it forms an A-module via the action of ψ: $a'.P = \psi_{a'}P$ for $a' \in A$ and $P \in K\{\tau\}$. If $\varphi = \psi$, then we write $\operatorname{End}_K(\varphi)$ for $\operatorname{Hom}_K(\varphi, \varphi)$, the endomorphism ring of φ over K. When considered over $\overline{K}$, we will simply write $\operatorname{Hom}(\varphi, \psi)$ and $\operatorname{End}(\varphi)$. We see that $\operatorname{End}_K(\varphi)$ is the centralizer of $\varphi(A)$ in $K\{\tau\}$. An *isomorphism* is an invertible morphism.

The following proposition gives a correspondence between isogenies and their kernels in the case of generic characteristic. This is a particular case of [Gos98, Proposition 4.7.11].

Proposition 1.10. *Let φ be a Drinfeld module of generic characteristic over K and H be a finite A-submodule of $\overline{K}$ via φ. Then there exists a Drinfeld module φ' defined over K and an isogeny $P : \varphi \to \varphi'$ such that* $\operatorname{Ker} P = H$.

The Drinfeld module φ' is also written as φ/H and is called the quotient of φ by H. The isogeny P is also referred to as the projection map $\varphi \to \varphi/H$. These notations are suggestive since isogenies are surjective morphisms.

Proposition 1.11. *A morphism $P : \varphi \to \psi$ in $K\{\tau\}$ is an isomorphism if and only if* $\deg_\tau P = 0$ *(if and only if $P \in K^*\{\tau\} = K^*$). If there exists an isomorphism $P \in K$ between φ and ψ then we say φ and ψ are isomorphic over K and we write $\varphi \simeq \psi$.*

We know that an isogeny between two abelian varieties admit a dual isogeny. This is also the case for Drinfeld modules.

Proposition 1.12. *Let $P : \varphi \to \psi$ be an isogeny. There exists an isogeny $\hat{P} : \psi \to \varphi$ such that*

$$\hat{P}P = \varphi_a \text{ and } P\hat{P} = \psi_a$$

for some non zero $a \in A$. Such an isogeny $\hat{P}$ is called a dual *of P and is not unique.*

Proof. See [Gos98, Proposition 4.7.13 and Proposition 4.7.14]. □

This tells us that isogenies give rise to equivalence relations on Drinfeld modules over K so that we can talk about isogeny classes.

The following proposition describes the endomorphism ring of a Drinfeld module.

Proposition 1.13. *Let φ be a Drinfeld module of rank r over K. Then:*

1. $\mathrm{End}_K(\varphi)$ *is a finitely generated projective A-module of rank $\leq r^2$;*
2. *If K has generic characteristic, then* $\mathrm{End}_K(\varphi)$ *is a commutative A-algebra of rank $\leq r$;*
3. $\mathrm{End}_K(\varphi) \otimes_A F$ *is a finite dimensional division algebra over F;*
4. $\mathrm{End}_K(\varphi) \otimes_A F_\infty$ *is a finite dimensional division algebra over F_∞.*

Proof. See [Gos98, section 4.7] □

1.1.3 Complex multiplication

In the generic characteristic case, in analogy with elliptic curves, we have the theory of complex multiplication for Drinfeld modules. The theory is stronger in the function field case in the sense that it gives an explicit class field theory of arbitrary function fields over $\mathbb{F}_q[T]$, not just quadratic extensions.

Definition 1.14 (Complex multiplication)**.** *A rank r Drinfeld A-module φ of generic characteristic over L is said to have* complex multiplication (or CM) *if* $\mathrm{End}(\varphi)$ *has rank r. The complex multiplication is said to be L-* rationally defined *if* $\mathrm{End}(\varphi) = \mathrm{End}_L(\varphi)$.

Definition 1.15. *A finite extension K/F is said to be* purely imaginary *or* totally imaginary *if there is exactly one prime of K above the prime at infinity ∞.*

Recall that an *order* in K is a subring of the integral closure $\mathcal{O}_K$ of A in K which contains 1 and has field of fractions K.

Proposition 1.16. *If φ is a rank r CM Drinfeld A-module of generic characteristic then* $\operatorname{End}(\varphi)$ *is an order in a degree r purely imaginary extension K/F, namely* $K = \operatorname{End}(\varphi) \otimes_A F$.

Proof. From Proposition 1.13 part 2, $\operatorname{End}(\varphi)$ is clearly an order in K. Now, Proposition 1.13 part 4 tells us that $\operatorname{End}(\varphi) \otimes_A F_\infty$ is a finite field extension of F_∞, as an F_∞-algebra it is isomorphic to $K \otimes_F F_\infty$. Since φ has generic characteristic, K/F is a separable extension so that $K \otimes_F F_\infty \simeq \prod_{v|\infty} K_v$, where the product runs through the primes v of K above ∞ and K_v the corresponding completions. Therefore there is exactly one prime of K above ∞ since the above product is a field. □

Since φ has generic characteristic, $\mathcal{O} = \operatorname{End}(\varphi)$ is commutative so $K = \operatorname{End}(\varphi) \otimes_A F$ is indeed a field and in this case we say φ is a K-CM Drinfeld module or an $\mathcal{O}$-CM Drinfeld module and we call K the *CM-field* of φ.

1.1.4 Torsion submodules

Let L/F be a finite extension and φ be a Drinfeld A-module over L. Recall that the additive group $(L, +)$ is equipped with the A-module structure: $a.x = \varphi_a(x)$. This A-module is denoted $\varphi(L)$ and can be seen as the analogue of the Mordell-Weil group $E(L)$ of L-rational points of an elliptic curve E defined over the number field L.

Definition 1.17. *The submodule of the L-rational torsion points of φ is*

$$\varphi(L)_{\text{tors}} := \{x \in L |\, \operatorname{Ann}_A(x) \neq \{0\}\}.$$

Poonen proved an analogue of the Mordell-Weil theorem for abelian varieties using local height functions. For a finite extension L/F, the module of L-rational torsion points is not finitely generated but tame, i.e. every submodule of finite rank is finitely generated.

Theorem 1.18 ([Poo95, Theorem 1.])**.** *Let L/F be a finite extension and φ a Drinfeld A-module of any rank. Then $\varphi(L)$ is the direct sum of its torsion submodule $\varphi(L)_{\text{tors}}$, which is finite, with a free A-module of rank $\aleph_0 := \#\mathbb{N}$.*

The torsion part $\varphi(L)_{\text{tors}}$ is a finite module over a Dedekind domain the structure of which is well understood. Unlike the situation in the elliptic curves case the torsion-free part of $\varphi(L)$ always has infinite rank as a free A-module. The naive analogue of the Mordell-Weil rank of an elliptic curve defined over a number field is not available for Drinfeld modules.

Poonen also described the Drinfeld module structure over $\overline{L}$ and L^{sep}.

Proposition 1.19 ([Poo95] Proposition 7.). *Each of the A-modules $\varphi(\overline{L})$ and $\varphi(L^{\text{sep}})$ is the direct sum of a F-vector space of dimension $\aleph_0$ with a torsion module isomorphic to $(F/A)^r$ where r is the rank of φ.*

Let $\mathfrak{a} \subseteq A$ be an ideal. The set of $\mathfrak{a}$-torsion points of φ is defined as:

$$\varphi[\mathfrak{a}] := \{x \in \overline{F} | \varphi_a(x) = 0 \; \forall a \in \mathfrak{a}\}.$$

If we consider the ideal $I_{\varphi,\mathfrak{a}} := \{\varphi_a | a \in \mathfrak{a}\}$ in $L\{\tau\}$, then we can write $I_{\varphi,\mathfrak{a}} = L\{\tau\} \cdot \varphi_{\mathfrak{a}}$ for a unique monic twisted polynomial $\varphi_{\mathfrak{a}} \in L\{\tau\}$ since $L\{\tau\}$ is a left PID. In this case $\varphi[\mathfrak{a}] = \text{Ker}(\varphi_{\mathfrak{a}})$.

Theorem 1.20. *Let $\mathfrak{a} \subseteq A$ be an ideal coprime to the A-characteristic of φ. Then we have an isomorphism of A-modules*

$$\varphi[\mathfrak{a}] \simeq (A/\mathfrak{a}A)^r.$$

Proof. See [Ros02] corollary of Theorem 13.1. □

1.1.5 Analytic theory of Drinfeld modules

For more details about the materials in this section we may consult [Ros02, Chapter 13], [Gos98, Chapter 4]. For a rapid introduction, see [Poo17]. Proofs will not be given, we refer to one of the above mentioned sources.

Drinfeld modules admit an analytic theory over $\mathbb{C}_\infty$ that parallels that of elliptic curves. They can be realised as "complex tori" via analytic uniformization. An elliptic curve $E(\mathbb{C})$ over $\mathbb{C}$ is isomorphic to a torus $\mathbb{C}/\Lambda$ where Λ is a complex lattice, i.e a $\mathbb{Z}$-submodule of rank 2 (generated by two $\mathbb{R}$-linearly independent elements), and every such torus defines an elliptic curve. The analytic isomorphism is given by the Weierstrass $\mathscr{P}$-function associated to Λ, that is $\mathbb{C}/\Lambda \to E(\mathbb{C}), z \mapsto (\mathscr{P}(z), \mathscr{P}'(z))$. This is called the uniformization theorem. A similar phenomena holds for Drinfeld modules over $\mathbb{C}_\infty$. Instead of $\mathbb{Z}$-submodules, lattices in this context will be certain A-submodules of finite rank. The $\mathbb{Z}$-submodules of $\mathbb{C}_\infty$ of finite rank are exactly the $\mathbb{F}_p$-subspaces, which are finite.

We start with some analysis on $\mathbb{C}_\infty$. An analogue of the theory of entire (or holomorphic) functions over the complex numbers can be developped over function fields, or $\mathbb{C}_\infty$. Many of the theorems still hold and even manifest in a stronger form. A striking example of that is the *"freshman's dream"* which is true over non-archimedian spaces. A function $\mathbb{C}_\infty \to \mathbb{C}_\infty$ is *entire* if it can be represented by an everywhere convergent power series $\sum a_n z^n$.

A non constant entire function over $\mathbb{C}_\infty$ has at least one zero and is surjective [Ros02, Proposition 13.19.]. Moreover, an entire function is almost determined by its zeroes.[1]

Theorem 1.21 (Weierstrass preparation theorem). *Let f be an entire function on $\mathbb{C}_\infty$, let $\lambda_1, \lambda_2, \cdots$ be its zeroes with 0 excluded if $f(0) = 0$ and $m_1, m_2, \cdots$ their corresponding multiplicities. Then $\lim\limits_{i\to\infty} \lambda_i = \infty$ and there is a constant $c \neq 0$ such that*

$$f(x) = cx^n \prod_{i=1}^{\infty} \left(1 - \frac{x}{\lambda_i}\right)^{m_i}$$

where n is the order of 0. Conversely, if $\lim\limits_{i\to\infty} \lambda_i = \infty$, then the above infinite product defines an entire function on $\mathbb{C}_\infty$.

Now, we will define lattices in $\mathbb{C}_\infty$. We will see that there are far more lattices in $\mathbb{C}_\infty$ than in $\mathbb{C}$ due to the fact that $[\mathbb{C}_\infty : F_\infty] = \infty$ whereas $[\mathbb{C} : \mathbb{R}] = 2$.

Definition 1.22. *A subset $S \subseteq \mathbb{C}_\infty$ is said to be* strongly discrete *if its intersection with any ball of finite radius centered at the origin is finite.*

For instance, the zeroes of an entire function $f(z) = \sum_{n=0}^{\infty} a_n z^n$ form a strongly discrete subset.

Definition 1.23. *An A-lattice of rank r in $\mathbb{C}_\infty$ is a strongly discrete projective A-submodule of rank r (in our setting projective is equivalent to finitely generated). The rank of Λ is defined as the dimension of the vector space $F_\infty\Lambda$ over F_∞.*

Let Λ_1, Λ_2 be two rank r lattices in $\mathbb{C}_\infty$ and let $c \in \mathbb{C}_\infty$ such that $c\Lambda_1 \subseteq \Lambda_2$. The multiplication by c map defines an A-module morphism $\Lambda_1 \to \Lambda_2$. We define

$$\operatorname{Hom}(\Lambda_1, \Lambda_2) := \{c \in \mathbb{C}_\infty | c\Lambda_1 \subseteq \Lambda_2\}.$$

To an A-lattice Λ we can associate an *exponential* function which can be seen as the analogue of the Weierstrass $\wp$-function for the complex elliptic curves.

Definition 1.24. *The exponential function associated to the lattice Λ is defined as:*

$$e_\Lambda(z) := z \prod_{\lambda \in \Lambda \setminus \{0\}} \left(1 - \frac{z}{\lambda}\right) \ \forall\, z \in \ \mathbb{C}_\infty.$$

[1] This is not the case in $\mathbb{C}$, take the exponential function.

The fact that Λ is strongly discrete ensures the convergence of the infinite product by Theorem 1.21. The function $e_\Lambda(z)$ can be characterized, by Theorem 1.21, as the unique entire function with simple zeroes on the points of Λ with leading term z. The following are the main properties of the exponential function

Proposition 1.25. *Let Λ be a lattice in $\mathbb{C}_\infty$. Then for all $w, z \in \mathbb{C}_\infty$ and $\alpha \in \mathbb{F}_q$ we have*

(i) $e_\Lambda(w+z) = e_\Lambda(w) + e_\Lambda(z)$.

(ii) $e_\Lambda(\alpha z) = \alpha e_\Lambda(z)$.

(iii) *e_Λ is entire, surjective and its zeroes are exactly the points of Λ.*

We can see that $e_\Lambda : \mathbb{C}_\infty/\Lambda \to \mathbb{C}_\infty$ is an isomorphism (analytically and also of abelian groups, but not of A-modules). The set $\mathbb{C}_\infty/\Lambda$ inherits the natural A-module structure of $\mathbb{C}_\infty$, and transporting that structure across to $\mathbb{C}_\infty$ via e_Λ defines a new A-module structure on $\mathbb{C}_\infty$, a Drinfeld A-module structure.

For $a \in A$, the multiplication-by-a map $a : \mathbb{C}_\infty/\Lambda \to \mathbb{C}_\infty/\Lambda$ corresponds to a map $\varphi_a^\Lambda : \mathbb{C}_\infty \to \mathbb{C}_\infty$ under the above isomorphism, i.e. the following diagram commutes

$$\begin{tikzcd}
\mathbb{C}_\infty/\Lambda \arrow[r, "a"] \arrow[d, "e_\Lambda"', "\wr"] & \mathbb{C}_\infty/\Lambda . \arrow[d, "e_\Lambda"', "\wr"] \\
\mathbb{C}_\infty \arrow[r, dashed, "\varphi_a^\Lambda"] & \mathbb{C}_\infty
\end{tikzcd}$$

Proposition 1.26. *The map φ_a^Λ is an $\mathbb{F}_q$-linear polynomial, i.e. it is an element of $\mathbb{C}_\infty\{\tau\}$. More precisely*

$$\varphi_a^\Lambda(z) = az \prod_{\lambda \in (a^{-1}\Lambda/\Lambda)\setminus\{0\}} \left(1 - \frac{z}{e_\Lambda(\lambda)}\right).$$

Furthermore, it satisfies the following

$$e_\Lambda(az) = \varphi_a^\Lambda(e_\Lambda(z)).$$

Proof. See [Poo17, Proposition 2.3.] and [Ros02, Proposition 13.22.]. □

Theorem 1.27. *Let $\Lambda \subseteq \mathbb{C}_\infty$ be a lattice of rank r. The map $\varphi^\Lambda : A \to \mathbb{C}_\infty\{\tau\}$ that sends 0 to 0 and a to φ_a^Λ for $a \neq 0$ defines a Drinfeld A-module of rank r.*

Proof. See [Ros02, Theorem 13.23.]. □

It is now clear that a rank r lattice gives rise to a rank r Drinfeld module. One can even say more.

Theorem 1.28 (Analytic uniformization)**.** *Let φ be a Drinfeld A-module of rank r over $\mathbb{C}_\infty$. Then there exists a rank r lattice Λ such that $\varphi = \varphi^\Lambda$. Moreover, the assignment*

$$\{A-\text{lattices of rank } r \text{ in } \mathbb{C}_\infty\} \longrightarrow \{\text{Drinfeld } A-modules\ over\ \mathbb{C}_\infty \text{ of rank } r\}$$

that sends Λ to φ^Λ and $0 \neq c \in \operatorname{Hom}(\Lambda_1, \Lambda_2)$ to the morphism $f_c(z) = cz \prod_{\lambda \in (a^{-1}\Lambda_2/\Lambda_1)\backslash\{0\}} \left(1 - \frac{z}{e_{\Lambda_1}(\lambda)}\right)$ is an equivalence of categories.

Proof. See [Gos98, Theorem 4.6.9.]. □

1.2 On quadratic and Gorenstein orders

The content and results in the current subsection were communicated privately to the author by Pete Clark.

Endomorphism rings of CM Drinfeld modules arise as orders of some Dedekind domain. In our investigation we come to consider a class of orders called Gorenstein orders which comprises the maximal orders and the quadratic orders. This is especially useful when going from a non-maximal order to the maximal order by means of an isogeny as in subsection 3.6.2.

1.2.1 Quadratic orders

For a Dedekind domain A, we characterize quadratic A-orders that are finitely generated as an A-module. A standard example is the orders of a quadratic number field. Finitely generated modules over a Dedekind domain have a nice structure theorem that generalizes the case of PID.

Theorem 1.29 (Structure theorem for finitely generated modules over a Dedekind domain)**.** *Let A be a Dedekind domain and M a finitely generated A-module. Then $M \simeq M_{\text{tors}} \oplus P$ where M_{tors} is the torsion submodule of M and $P = I_1 \oplus \cdots \oplus I_n$ a finite direct sum of rank one projective A-modules* [2]*. The torsion free part P can be written as $P \simeq A^{n-1} \oplus I$ where n is the rank of M and I a rank one projective module which determines a unique class, called the* Steinitz class *of P over A, in the class group $\mathrm{Cl}(A)$. Furthermore, M_{tors} may be written uniquely in the form*

$$M_{\text{tors}} \simeq A/\mathfrak{a}_1 \oplus \cdots \oplus A/\mathfrak{a}_m,$$

[2] A being Dedekind, the rank one projective submodules are exactly the fractional A-ideals.

where $0 \neq \mathfrak{a}_1 \subseteq \cdots \subseteq \mathfrak{a}_m \neq A$ *is an ascending chain of ideals of* A.

Corollary 1.30. *A finitely generated module over a Dedekind domain is projective if and only if it is torsion free.*

Theorem 1.31. *Let* $\mathfrak{a}$ *be an integral ideal of the Dedekind domain* A *and* I *any fractional* A*-ideal. Then we have an isomorphism of* A*-modules*

$$A/\mathfrak{a} \simeq I/\mathfrak{a}I.$$

Proof. See [Rei03, Theorem 4.12]. □

Following [Cla15, section 8.2], we make the following definition

Definition 1.32. *An object* X *in a category* $\mathscr{C}$ *is called* Hopfian *if every surjective endomorphism of* X *is an isomorphism.*

As pointed out by Clark, this definition is not completely agreed upon since it does not reflect properly what would an Hopfian object be in more general categories other than the category of A-modules. However, it is sufficient for the purpose of this thesis since we only deal with A-modules.

Theorem 1.33. *Let* A *be a ring and* M *a finitely generated* A*-module. Then* M *is a Hopfian object in the category of* A*-modules.*

Proof. See [Cla15, Theorem 3.44]. □

Theorem 1.34. *Let* A *be a Dedekind domain with fraction field* F, K/F *be a quadratic extension,* $B = \mathscr{O}_K$ *the integral closure of* A *in* K *and assume that* B *is finitely generated as an* A*-module. Let* $\mathscr{O}$ *be an order in* K. *Let*

$$\mathfrak{f} := \mathrm{Ann}_A(B/\mathscr{O}).$$

Then $\mathfrak{f}$ *is a nonzero ideal of* A *and*

$$\mathscr{O} = \mathscr{O}_{\mathfrak{f}} := A + \mathfrak{f}B.$$

Proof. From Theorem 1.29, since K/F is quadratic, $B \simeq A \oplus I$ for some rank one projective A-module I, which we may assume contains A, so $B/A \simeq I$ is projective. Therefore the sequence

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] & B \arrow[r, "\pi"] & B/A \arrow[r] & 0 \end{tikzcd}$$

splits and there is a section $h : B/A \to B$ with $\pi \circ h = \mathrm{id}_{B/A}$. Now, let $g : I \xrightarrow{\sim} B/A$ be an isomorphism and put $\alpha := h \circ g(1)$, as an A-module we have

$$B = A \oplus I\alpha.$$

Now, since $\mathscr{O} \supseteq A$, $B/\mathscr{O}$ is a torsion quotient of I as an A-module. That is, there exists a non zero ideal $\mathfrak{f}$ of A such that $B/\mathscr{O} \simeq I/\mathfrak{f}I$ and by Theorem 1.31 we have

$$B/\mathscr{O} \simeq A/\mathfrak{f}. \tag{1.2.1}$$

On the other hand, the ring

$$A + \mathfrak{f}B = A \oplus \mathfrak{f}I\alpha$$

is an A-order in B, and from Theorem 1.31, as A-modules,

$$B/(A + \mathfrak{f}B) \simeq I\alpha/\mathfrak{f}I\alpha \simeq A/\mathfrak{f}.$$

From (1.2.1), we have $\mathfrak{f}B \subseteq \mathscr{O}$ so that $A + \mathfrak{f}B \subseteq \mathscr{O}$ and this gives a natural surjection of finitely generated A-modules which of each is isomorphic to $A/\mathfrak{f}$

$$q : B/(A + \mathfrak{f}B) \to B/\mathscr{O}.$$

Hence, by Theorem 1.33, q is an isomorphism and thus $\mathscr{O} = A + \mathfrak{f}B$. One can easily identify $\mathfrak{f}$ as $\mathrm{Ann}_A(B/\mathscr{O})$. □

1.2.2 Gorenstein orders

Let R be a commutative ring with unity and M an R-module. An *injective resolution* of M is an exact sequence of R-modules

$$0 \to M \to M_0 \to M_1 \to M_2 \to \cdots$$

such that the M_i's are injective R-modules for $i \geq 0$. The category of R-modules with module morphisms has enough injectives so M always has an injective resolution. Such a resolution is said to be finite of length $n \geq 0$ if M_n is non zero and $M_i = 0$ for all $i > n$. Otherwise it is said to be infinite.

Definition 1.35. *The* injective dimension *of M is, either infinite if M does not admit a finite injective resolution, or the minimal length amongst all injective resolutions of M.*

Definition 1.36. *A commutative Noetherian ring R is called a* Gorenstein ring *if for any maximal ideal $\mathfrak{m}$ of R, the localization $R_\mathfrak{m}$ has finite injective dimension as an $R_\mathfrak{m}$-module.*

Proposition 1.37. *A localization of a Gorenstein ring is Gorenstein.*

Proof. Let $S \subseteq R$ be a multiplicative subset of R and $S^{-1}R$ the corresponding localization. Let $\mathfrak{m}_S \in \operatorname{MaxSpec} S^{-1}R$, there exists $\mathfrak{m} \in \operatorname{MaxSpec} R$ such that $\mathfrak{m} \cap S = \emptyset$ and $\mathfrak{m}_S = \mathfrak{m}$. We have a canonical isomorphism $(S^{-1}R)_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$. Now, since R is Noetherian, any localization of R is Noetherian. Furthermore, localization of a module over a Noetherian ring preserves injectiveness. The proof is completed by noting that localization is an exact functor. □

We are interested in rings that are A-orders for some Dedekind domain A so we assume throughout the remainder of this section that R is commutative Noetherian of Krull dimension 1. More specifically, let's assume the following situation: A is a Dedekind domain with fraction field F, K/F is a finite separable extension, $B = \mathcal{O}_K$ is the integral closure of A in K, and R is an A-submodule of B with fraction field R. For fractional R-ideals I and J recall that

$$(I : J) := \{\alpha \in K | \alpha J \subseteq I\} = \operatorname{Hom}_R(J, I).$$

Proposition 1.38. *Assume moreover that A is a PID. Then:*

(i) The order R is Gorenstein if and only if every proper fractional R-ideal is invertible.

(ii) If R is monogenic over A, i.e. $R = A[\alpha]$ for some $\alpha \in R$, then R is Gorenstein.

Proof. (i) See [JT15, Characterization 4.2].

(ii) See [JT15, Theorem 4.3].

□

We now state some results that will be useful for the proof of the main result of the current section. Recall that a ring is called *semilocal* if it has only finitely many maximal ideals. This is a slight generalization of local rings.

Proposition 1.39. *If R is a semilocal ring and M a finitely generated projective R-module, then M is free if and only if M has constant rank.*

Proof. See [Cla15, Corollary 7.21]. □

Theorem 1.40. *For an A-module R the following are equivalent:*

(i) R is finitely generated and projective.

(ii) R is finitely presented and locally free.

Proof. See [Cla15, Theorem 7.29]. □

Theorem 1.41. *Let I be a nonzero fractional ideal for a domain R. Then I is invertible if and only if it is projective, in which case it is necessarily projective of rank one.*

Proof. See [Cla15, Theorem 19.11]. □

Proposition 1.42. *Let $f : R \to M$ be a homomorphism of A-modules. Then the following are equivalent:*

(i) f is surjective.

(ii) f is locally surjective, i.e. for all $\mathfrak{p} \in \operatorname{Spec} A$ the local homomorphisms $f_\mathfrak{p} : R_\mathfrak{p} \to M_\mathfrak{p}$ are surjective.

Proof. See [Cla15, Proposition 7.14]. □

Lemma 1.43. *For $\mathfrak{p} \in \operatorname{MaxSpec} A$ the ring $R_\mathfrak{p} := (A \setminus \mathfrak{p})^{-1}R$ is semilocal.*

Proof. The ring $A_\mathfrak{p}$ is a local subring of $R_\mathfrak{p}$ with maximal ideal $\mathfrak{p}A_\mathfrak{p}$. The maximal ideals of $R_\mathfrak{p}$ lie over $\mathfrak{p}A_\mathfrak{p}$ and are minimal over $\mathfrak{p}R_\mathfrak{p}$. Hence, $\operatorname{MaxSpec} R_\mathfrak{p}$ is finite since a Noetherian ring only has finitely many minimal prime ideals over any ideal. □

The main result of this section is the following.

Theorem 1.44. *(i) The A-order R is Gorenstein if and only if every proper fractional R-ideal is invertible.*

(ii) Every quadratic A-order is Gorenstein.

Proof. (i) We want to use Proposition 1.38 so we first reduce to that case by localising on A. That is, we will show the following statements: R is Gorenstein if and only if $R_\mathfrak{p}$ is Gorenstein for all $\mathfrak{p} \in \operatorname{MaxSpec} A$, the fractional R-ideal I is invertible (resp. proper) if and only if the fractional $R_\mathfrak{p}$-ideal $I_\mathfrak{p} := IR_\mathfrak{p}$ is invertible (resp. proper) for all $\mathfrak{p} \in \operatorname{MaxSpec} A$. The ring $A_\mathfrak{p}$ being a local Dedekind domain that is not a field, it is a DVR and hence a PID.

Let $\mathfrak{p} \in \operatorname{MaxSpec} A$, if R is Gorenstein then $R_\mathfrak{p}$ is Gorenstein by Proposition 1.37. Conversely, suppose that $R_\mathfrak{p}$ is Gorenstein for all $\mathfrak{p} \in \operatorname{MaxSpec} A$ and let $\mathscr{P} \in \operatorname{MaxSpec} R$. The ideal $\mathfrak{q} := \mathscr{P} \cap A$ is an element of $\operatorname{MaxSpec} A$ and $R_\mathscr{P} = (R \setminus \mathscr{P})^{-1}R = (R \setminus \mathscr{P})^{-1}R_\mathfrak{q}$. Hence

$R_{\mathscr{P}}$ is Gorenstein as a localization of the Gorenstein ring $R_{\mathfrak{q}}$. That is, R is Gorenstein.

Let I be an invertible fractional R-ideal. Then $IJ = R$ for some fractional R-ideal J. Localizing at $\mathfrak{p} \in \operatorname{MaxSpec} A$ gives $I_{\mathfrak{p}} J_{\mathfrak{p}} = R_{\mathfrak{p}}$ so $I_{\mathfrak{p}}$ is an invertible fractional $I_{\mathfrak{p}}$-ideal. Conversely, let I be a fractional R-ideal and suppose that $I_{\mathfrak{p}}$ is an invertible fractional $R_{\mathfrak{p}}$-ideal for all $\mathfrak{p} \in \operatorname{MaxSpec} A$. Theorem 1.41 implies that $I_{\mathfrak{p}}$ is projective of rank one. From Lemma 1.43, the ring $R_{\mathfrak{p}}$ is semilocal, and since $I_{\mathfrak{p}}$ is finitely generated and projective as an $R_{\mathfrak{p}}$-module, it is free according to Proposition 1.39. Therefore, as a rank one free $R_{\mathfrak{p}}$-module, $I_{\mathfrak{p}}$ is a principal fractional $R_{\mathfrak{p}}$-ideal. For $\mathscr{P} \in \operatorname{MaxSpec} R$, the ideal $\mathfrak{q} := \mathscr{P} \cap A$ is maximal in A and $I_{\mathscr{P}} = I_{\mathfrak{q}} R_{\mathscr{P}}$ is then principal. It follows that I is locally free and since I is finitely generated over the Noetherian ring R it is finitely presented [Sta19, Tag 00FM]. Theorem 1.40 implies that I is then projective so invertible by Theorem 1.41.

Let I be a proper fractional R-ideal, so $(I : I) = \operatorname{Hom}_R(I, I) = \operatorname{End}_R(I) = R$. Since I is finitely presented, using [Mat80, p. 7], for any multiplicative subset of R we have $(IS^{-1}R : IS^{-1}R) = (I : I)S^{-1}R = S^{-1}R$. Therefore for $\mathfrak{p} \in \operatorname{MaxSpec} A$, taking $S = A \setminus \mathfrak{p}$, the fractional $R_{\mathfrak{p}}$-ideal $I_{\mathfrak{p}}$ is proper. Conversely, suppose that $I_{\mathfrak{p}}$ is proper for all $\mathfrak{p} \in \operatorname{MaxSpec} R$. For $\mathscr{P} \in \operatorname{MaxSpec} R$, $\mathfrak{q} = \mathscr{P} \cap A$ is maximal in A and we have $(I_{\mathscr{P}} : I_{\mathscr{P}}) = (I_{\mathfrak{q}} R_{\mathscr{P}} : I_{\mathfrak{q}} R_{\mathscr{P}}) = (I_{\mathfrak{q}} : I_{\mathfrak{q}}) R_{\mathscr{P}} = R_{\mathfrak{q}} R_{\mathscr{P}} = R_{\mathscr{P}}$. Hence the fractional $R_{\mathscr{P}}$-ideal $I_{\mathscr{P}}$ is proper. The injection $R \hookrightarrow (I : I)$ is locally surjective, hence surjective by Proposition 1.42. That is I is proper.

Now it is enough to show the following: the $A_{\mathfrak{p}}$-order $R_{\mathfrak{p}}$ is Gorenstein if and only if every proper fractional $R_{\mathfrak{p}}$-ideal is invertible for all $\mathfrak{p} \in \operatorname{MaxSpec} A$. But that can be deduced from Proposition 1.38 since $A_{\mathfrak{p}}$ is a PID.

(ii) By Theorem 1.34, a quadratic A-order is of the form $R = A + \mathfrak{f}B = A \oplus \mathfrak{f}I\alpha$ for some ideals $\mathfrak{f}, I$ of A and $\alpha \in B$. Hence, if A is a PID then $\mathfrak{f} = (f), I = (i)$ and $R = A[fi\alpha]$ is monogenic so that R is Gorenstein by Proposition 1.38. As we have shown in part (i), we can reduce to that case by localizing on A. Let $\mathfrak{p} \in \operatorname{MaxSpec} A$, then $A_{\mathfrak{p}}$ is a local PID, $R_{\mathfrak{p}}$ being a quadratic $A_{\mathfrak{p}}$-order is monogenic as above, thus it is a Gorenstein $A_{\mathfrak{p}}$-order by Proposition 1.38 and we are done.

□

Chapter 2

Complex multiplication for Drinfeld modules

This chapter is expository and is mainly based on [Hay79], we will not give the proofs. We review the main theorem of complex multiplication for Drinfeld modules. This has been achieved by Drinfeld using methods from algebraic geometry, [Dri74, section 8]. Independently, Hayes obtained the same result without appealing to the machinery of algebraic geometry but rather developing methods along the line of Deuring's approach to elliptic curves with complex multiplication, [BCH$^+$66, Hay79] . On one hand, the theory of complex multiplication of elliptic curves provides an explicit class field theory for imaginary quadratic number fields and abelian varieties yield an explicit class field theory for number fields of CM type, i.e. imaginary quadratic extensions of totally real number fields. On the other hand, explicit class field theory for arbitrary global function fields can be obtained from a generalised version of rank one Drinfeld modules as developed by Hayes in [Hay79], he constructed all class fields of any global function fields of transcendence degree 1 over a finite field.

Let F be a global function field over $\mathbb{F}_q$, ∞ a fixed prime of degree d_∞ over $\mathbb{F}_q$ and A the ring of elements of F regular away from ∞. A *class field* of F is a finite abelian extension of F on which ∞ splits completely.

2.1 Orders and Picard groups

Recall that an *order* $\mathscr{O}$ in F is a subring of A containing 1 and has F as fraction field. The ring A is the *maximal order*. A *fractional ideal* of $\mathscr{O}$ or *fractional $\mathscr{O}$-ideal* is a non-zero noetherian[1] $\mathscr{O}$-submodule of F. Such submodule can be

[1] Recall that a module is noetherian if every submodule is finitely generated. In particular, such module is finitely generated.

written as $\mathcal{O}\alpha_1 + \cdots + \mathcal{O}\alpha_n$ for some $\alpha_1, \cdots, \alpha_n \in F$. Let I be a fractional $\mathcal{O}$-ideal, the *ring of multipliers* or *the endomorphism ring of* I is

$$(I : I) := \{x \in F | xI \subseteq I\}.$$

It is clear that $\mathcal{O} \subseteq (I : I)$ since I is an $\mathcal{O}$-module. Actually $(I : I)$ is also an order in F since its elements are integral over A and A is integrally closed, see [Ros87]. Indeed, if $I = \mathcal{O}\alpha_1 + \cdots + \mathcal{O}\alpha_n$ and $x \in (I : I)$ then $x\alpha_1, \cdots, x\alpha_n \in I$, so for each $0 \leq i \leq n$ we can write

$$x\alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j$$

for some $a_{ij} \in \mathcal{O}$. Now we can easily see that the $n \times n$ matrix

$$\mathrm{diag}(x - 2a_{ii})(a_{ij})_{i,j}$$

maps the vector $t_{(\alpha_1, \cdots, \alpha_n)}$ to the zero vector so that its determinant is zero, this gives a monic polynomial with coefficients in $\mathcal{O}$ for which x is a root. We say I is *proper* if $(I : I) = \mathcal{O}$.

In general the set of all fractional $\mathcal{O}$-ideals does not form a group but a monoid since $\mathcal{O}$ may not be a dedekind domain. Put

$$I^* = \{x \in F | xI \subseteq \mathcal{O}\}.$$

A fractional $\mathcal{O}$-ideal I is *invertible* if $II^* = \mathcal{O}$.

We denote by $I(\mathcal{O})$ the group of all the invertible fractional $\mathcal{O}$-ideals and by $P(\mathcal{O})$ the subgroup formed by the non-zero principal ideals.

Definition 2.1. *The* Picard group *of $\mathcal{O}$ is the quotient* $\mathbf{Pic}(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$.

2.2 Hayes theory of Drinfeld modules

In [Hay79], Hayes developed a more general theory of Drinfeld modules with A replaced by an order $\mathcal{O}$ in A. Most of the basic properties and invariants still make sense in this generalisation, such as the rank, the height, the characteristic. However, $\mathcal{O}$ is no longer integrally closed unless it is equal to A itself, so it is not a dedekind domain. For instance, we loose decomposition theorems of modules over dedekind domains. In particular, the analogue of Theorem 1.20 is no longer true in general.

Let L be a field of characteristic p and τ_p the p-th power Frobenius. Let $i : L \hookrightarrow L\{\tau_p\}$ be the canonical inclusion and $D : L\{\tau_p\} \to L$ the derivative map.

Definition 2.2. *Let $\mathcal{O}$ be an order in A. A Drinfeld $\mathcal{O}$-module over L is a ring homomorphism $\varphi : \mathcal{O} \to L\{\tau_p\}$ such that $\varphi \neq i \circ D \circ \varphi$.*

Proposition 2.3. *A Drinfeld $\mathcal{O}$-module is always injective.*

Proof. See [Hay79, Proposition 2.2.]. □

Remark 2.4. In Chapter 1 we defined a Drinfeld module as a certain homomorphism of $\mathbb{F}_q$-algebras and using the q-th power Frobenius τ instead of τ_p. We could have used τ_p instead since A and L are both naturally $\mathbb{F}_q$-algebras and by commutativity the image of A always land in $L\{\tau\}$. However, an order $\mathcal{O}$ which is not integrally closed is not naturally an $\mathbb{F}_q$-algebra ($\mathcal{O}$ may not contain $\mathbb{F}_q$) so a Drinfeld $\mathcal{O}$-module is only a homomorphism of rings (or $\mathbb{F}_p$-algebras). It is important to note that in our case, Chapter 3, the orders we consider are $\mathbb{F}_q$-algebras so that we can work with τ.

In view of the above remark we will always assume that $\varphi(\mathcal{O}) \subseteq L\{\tau\}$.

The notion of *rank* is well defined in the current context and its existence and properties are as defined in Chapter 1. The *characteristic* of φ is a unique maximal ideal of A, say $\mathfrak{p}_0$, such that $\mathfrak{p}_0 \cap \mathcal{O} = \mathrm{Ker}(D \circ \varphi)$. Just as in the case of Drinfeld A-modules, $\mathfrak{p}_0$ is determined by the valuation $a \mapsto -\deg \varphi_a$ for $a \in \mathcal{O}$. We keep the terminology "generic characteristic" and "special characteristic" according to whether $\mathrm{Ker}(D \circ \varphi) = 0$ or not[2]. The *height* is also defined as in Chapter 1 and it is an integer [Hay79, Proposition 3.3].

Let $\varphi : \mathcal{O} \to L\{\tau\}$ be a Drinfeld $\mathcal{O}$-module of rank r and height h. When $\mathcal{O}$ is not integrally closed we loose the nice structures of torsions.

Proposition 2.5. *Let $\mathfrak{p}$ be an invertible prime ideal of $\mathcal{O}$. Then*

$$\varphi_{\text{tors},\mathfrak{p}} := \bigcup_{n=1}^{\infty} \varphi[\mathfrak{p}^n] \simeq (F/\mathcal{O}_{\mathfrak{p}})^r \quad \text{if } \mathfrak{p} \neq \mathfrak{p}_0 \cap \mathcal{O}$$

and

$$\varphi_{\text{tors},\mathfrak{p}} \simeq (F/\mathcal{O}_{\mathfrak{p}})^{r-h} \quad \text{if } \mathfrak{p} = \mathfrak{p}_0 \cap \mathcal{O}.$$

where $\mathcal{O}_{\mathfrak{p}}$ is the localization at $\mathfrak{p}$.

Proof. See [Hay79, p. 181]. □

[2] Hayes uses the term "without characteristic" instead of "generic characteristic".

Isogenies and isomorphisms are defined in the same way as for Drinfeld A-modules.

From now on we fix an homomorphism of rings $\iota : \mathcal{O} \to L$ and we only consider Drinfeld $\mathcal{O}$-modules φ such that $D \circ \varphi = \iota$. We can think of ι as an $\mathcal{O}$-field[3].

We denote by $\mathrm{Drin}^r_{\mathcal{O}}(L)$ the category of rank r Drinfeld $\mathcal{O}$-modules over L and by $\mathscr{M}^r_{\mathcal{O}}(L)$ the set of isomorphism classes of rank r Drinfeld $\mathcal{O}$-modules over L.

In section 4 of [Hay79], Hayes develops an analytic theory of Drinfeld $\mathcal{O}$-modules which generalizes section 1.1.5 of Chapter 1. This analytic theory is very similar to that of the case $\mathcal{O} = A$. Hayes defines an $\mathcal{O}$-lattice[4] of rank r as a finitely generated discrete $\mathcal{O}$-submodule of $\mathbb{C}_\infty$ of rank r [Hay79, Definition 4.1. and Theorem 4.9.]. Two lattices Λ and Λ' are isomorphic if $\Lambda = w\Lambda'$ for some $w \in \mathbb{C}_\infty$.

We denote by $\mathscr{L}_r(\mathcal{O})$ the set of isomorphism classes of $\mathcal{O}$-lattices of rank r in $\mathbb{C}_\infty$. For an invertible $\mathcal{O}$-ideal $\mathfrak{a}$ and a rank r $\mathcal{O}$-lattice Λ of rank r, the $\mathcal{O}$-submodule $\mathfrak{a}^{-1}\Lambda$ is also an $\mathcal{O}$-lattice of rank r. Clearly, if $\mathfrak{b}$ is principal then $\Lambda \simeq \mathfrak{b}^{-1}\Lambda$ so that the association

$$\Lambda \mapsto \mathfrak{a}^{-1}\Lambda$$

induces an action of $\mathbf{Pic}(\mathcal{O})$ on $\mathscr{L}_r(\mathcal{O})$.

To an $\mathcal{O}$-lattice is associated an exponential function, denoted e_Λ [Hay79, (4.2)] , defined as in Definition 1.24 by

$$e_\Lambda(z) := z \prod_{\lambda \in \Lambda \setminus \{0\}} \left(1 - \frac{z}{\lambda}\right) \quad \forall\, z \in \mathbb{C}_\infty$$

with the same properties [Hay79, (4.9) and (4.10)]. We have an analytic isomorphism $\mathbb{C}_\infty/\Lambda \xrightarrow{\sim} \mathbb{C}_\infty$ via e_Λ [Hay79, Theorem 4.7. (1) and Proposition 4.10.]. The $\mathcal{O}$-module structure of $\mathbb{C}_\infty/\Lambda$ transported to $\mathbb{C}_\infty$ via the above isomorphism defines a Drinfeld $\mathcal{O}$-module structure φ^Λ [Hay79, (4.7)]. The analytic uniformization theorem, analogue of Theorem 1.28, also holds.

Theorem 2.6 (Analytic uniformization)**.** *Let φ be a Drinfeld $\mathcal{O}$-module over $\mathbb{C}_\infty$ with $\iota(a) = a$ for all $a \in \mathcal{O}$. Then there is an $\mathcal{O}$-lattice Λ in $\mathbb{C}_\infty$ such that $\varphi = \varphi^\Lambda$. Moreover, $\mathscr{M}^r_{\mathcal{O}}(\mathbb{C}_\infty)$ and $\mathscr{L}_r(\mathcal{O})$ are canonically isomorphic as representation*

[3] In analogy with the notion of an A-field in Chapter 1.

[4] Hayes does not use this terminology, he actually develops a more general theory of lattices with exponential functions associated to them and apply it to the case of discrete $\mathcal{O}$-submodules of $\mathbb{C}_\infty$.

spaces of $\mathbf{Pic}(\mathcal{O})$ *for every positive integer* r. *The isomorphism is induced by* $\Lambda \mapsto \varphi^{\Lambda}$.

Proof. [Hay79, Theorem 5.9. and Theorem 5.11.]. □

2.3 The action of $\mathbf{Pic}(\mathcal{O})$

An ideal of an order in an imaginary quadratic number field acts as an endomorphism of a CM elliptic curve. The same phenomenon occurs for Drinfeld modules. Let $\mathcal{O}$ be an order in F and $\mathfrak{a} \subseteq \mathcal{O}$ a non-zero ideal. Let L be an extension of F, φ be a Drinfeld $\mathcal{O}$-module over L of generic characteristic. As in Chapter 1 section 1.1.4, let $I_{\varphi,\mathfrak{a}}$ be the left ideal generated by $\{\varphi_a, a \in \mathcal{O}\}$. We know that $I_{\varphi,\mathfrak{a}} = L\{\tau\}\varphi_{\mathfrak{a}}$ for some unique monic twisted polynomial $\varphi_{\mathfrak{a}}$. Since $\mathfrak{a}$ is an ideal of $\mathcal{O}$ which is a commutative ring, $\mathfrak{a}$ is stable by multiplication from the right. Therefore $I_{\varphi,\mathfrak{a}}$ is stable by multiplication from the right by φ_a for $a \in \mathcal{O}$. Hence, for $a \in \mathcal{O}$ there exists $\varphi'_a \in L\{\tau\}$ such that $\varphi_{\mathfrak{a}}\varphi_a = \varphi'_a\varphi_{\mathfrak{a}}$. Since $L\{\tau\}$ is an integral domain, the map $\varphi' : \mathcal{O} \to L\{\tau\}$, $a \mapsto \varphi'_a$ defines a Drinfeld $\mathcal{O}$-module over L which is uniquely determined by $\varphi_{\mathfrak{a}}$. We will denote

$$\varphi' := \mathfrak{a} * \varphi.$$

In other words, this defines an operation $*$ of the ideals of $\mathcal{O}$ on the set of Drinfeld $\mathcal{O}$-modules over L characterized as follows: given an ideal $\mathfrak{a}$ and a Drinfeld $\mathcal{O}$-module φ, $\mathfrak{a} * \varphi$ is the unique Drinfeld $\mathcal{O}$-module over L such that $\varphi_{\mathfrak{a}}$ is an isogeny from φ to φ'. This tells us that when φ has generic characteristic then $\mathfrak{a} * \varphi = \varphi/\varphi[\mathfrak{a}]$. The operation $*$ satisfies the following properties.

Proposition 2.7. *Let* $\mathfrak{a} = a\mathcal{O}$ *be a principal ideal and let* w *be the leading coefficient of* φ_a. *Then* $\varphi_{\mathfrak{a}} = w^{-1}\varphi_a$, *and* $(\mathfrak{a} * \varphi)_b = w^{-1}\varphi_b w$ *for all* $b \in \mathcal{O}$.

Proof. See [Hay79, Lemma 3.5.]. □

Proposition 2.8. *Let* $\mathfrak{a}, \mathfrak{b}$ *be invertible ideals of* $\mathcal{O}$. *Then*

$$\varphi_{\mathfrak{a}\mathfrak{b}} = (\mathfrak{b} * \varphi)_{\mathfrak{a}}\varphi_{\mathfrak{b}}$$

and

$$\mathfrak{a} * (\mathfrak{b} * \varphi) = (\mathfrak{a}\mathfrak{b}) * \varphi.$$

Proof. See [Hay79, Proposition 3.7.]. □

The operation $*$ extends to $I(\mathscr{O})$. A fractional ideal I can be written as $a^{-1}\mathfrak{a}$ for some $a \in \mathscr{O}$ and an integral ideal $\mathfrak{a}$, we define

$$I * \varphi := u(\mathfrak{a} * \varphi)u^{-1}$$

where u is the leading coefficient of φ_a. Also, two isomorphic Drinfeld modules are sent to isomorphic Drinfeld modules by the action of a fractional ideal $\mathfrak{a}$ via $*$, see formula (2.3.1) in remark 2.9 below.

Isogenous Drinfeld modules have the same rank and height. Hence, by Proposition 2.8, $I(\mathscr{O})$ act on $\mathrm{Drin}^r_{\mathscr{O}}(L)$ via $*$, and by Proposition 2.7 the principal ideals act trivially on $\mathscr{M}^r_{\mathscr{O}}(L)$. Therefore, $*$ induces an action of $\mathbf{Pic}(\mathscr{O})$ on $\mathscr{M}^r_{\mathscr{O}}(L)$. The case $r = 1$ is of importance for applications to class field theory.

Remark 2.9. The canonical isomorphism $\mathscr{M}^r_{\mathscr{O}}(\mathbb{C}_\infty) \simeq \mathscr{L}_r(\mathscr{O})$ in Theorem 2.6 being an isomorphism as representation spaces of $\mathbf{Pic}(\mathscr{O})$ means that the assignment $\Lambda \mapsto \varphi^\Lambda$ commutes with the actions of $\mathbf{Pic}(\mathscr{O})$ on $\mathscr{L}_r(\mathscr{O})$ and $\mathscr{M}^r_{\mathscr{O}}(\mathbb{C}_\infty)$. Indeed, by [Hay79, (5.15)], for an invertible $\mathscr{O}$-ideal $\mathfrak{a}$

$$\varphi^{\mathfrak{a}^{-1}\Lambda} \simeq \mathfrak{a} * \varphi^\Lambda. \tag{2.3.1}$$

2.4 Field of invariants

From now on we assume that φ is a Drinfeld $\mathscr{O}$-module of generic characteristic with $D \circ \varphi(a) = a$ for all $a \in \mathscr{O}$.

Definition 2.10. *Let $\mathscr{O}$ be an order in A and $\varphi : \mathscr{O} \longrightarrow \mathbb{C}_\infty\{\tau\}$ a Drinfeld $\mathscr{O}$-module. We say that a subfield $k \subseteq \mathbb{C}_\infty$ is a* field of definition *for φ if there exists a Drinfeld $\mathscr{O}$-module φ' isomorphic to φ over $\mathbb{C}_\infty$ such that the coefficients of φ'_a are in k for all $a \in \mathscr{O}$. For a given Drinfeld $\mathscr{O}$-module φ, there exists a smallest field of definition for φ called its* field of invariants.

We will see later that the ring class field of the order $\mathscr{O}$, denoted by $H_{\mathscr{O}}$, coincides with the field of invariants of an appropriate Drinfeld $\mathscr{O}$-module associated to φ.

Let $\mathbf{X} = \{X_i\}_{i\geq 1}$ be a set of indeterminates and $F[\mathbf{X}]$ the corresponding polynomial ring over F, $F(\mathbf{X})$ its field of fractions. We define a graduation $F[\mathbf{X}]$ as follows:

$$\mathrm{grad}(aX_{i_1}^{\alpha_1}\cdots X_{i_k}^{\alpha_k}) := \sum_{j=1}^{k} \alpha_j m_{i_j} := \sum_{j=1}^{k} \alpha_j (q^{i_j} - 1)$$

for the monomial $aX_{i_1}^{\alpha_1}\cdots X_{i_k}^{\alpha_k} \in F[\mathbf{X}]$. We obtain a decomposition

$$F[\mathbf{X}] = \bigoplus_{i=0}^{\infty} R_i$$

where $R_0 = F$ and R_i is the subgroup of homogenous polynomials of grade i (including 0). We extend this to $F(\mathbf{X})$ by setting

$$\operatorname{grad}\left(\frac{f}{g}\right) := \operatorname{grad}(f) - \operatorname{grad}(g)$$

for homogenous $f, g \in F[\mathbf{X}]$ to get a uniquely determined doubly infinite graduation of $F(\mathbf{X})$, i.e. allowing negative indices.

Definition 2.11. *The field $F(\mathbf{X})_0$ of the homogenous elements of grade zero is called the* field of formal invariants.

Let $a \in \mathcal{O}$, we will define the *field of invariants* of φ at a. Write

$$\varphi_a = a + \sum_{i=1}^{\infty} c_i(\varphi, a)\tau^i,$$

it is clear that the $c_i(\varphi, a)$'s are almost all zeroes. Consider the substitution homomorphism

$$S_{a,\varphi} : F[\mathbf{X}] \to \mathbb{C}_\infty$$

that sends X_i to $c_i(\varphi, a)$ for $i \geq 1$. It is well defined. Now, let

$$V_{a,\varphi} := \left\{ \frac{f}{g} \in F(\mathbf{X})_0 | S_{a,\varphi}(g) \neq 0 \right\}.$$

One can easily see that $V_{a,\varphi}$ is a local ring with maximal ideal

$$\left\{ \frac{f}{g} \in F(\mathbf{X})_0 | S_{a,\varphi}(f) = 0 \right\}.$$

It is clear that $S_{a,\varphi}$ induces a homomorphism from $V_{a,\varphi}$ to $\mathbb{C}_\infty$ that we also call $V_{a,\varphi}$.

Definition 2.12. *For $a \in \mathcal{O}$, the subfield*

$$I_a(\varphi) := S_{a,\varphi}(V_{a,\varphi}) \subseteq \mathbb{C}_\infty$$

is called the field of invariants *of φ at a.*

The appellation "field of invariants" is appropriate since $I_a(\varphi)$ is an invariant of the isomorphism class of φ over $\mathbb{C}_\infty$. Indeed, if $\varphi \simeq \varphi'$, say $\varphi_b = w^{-1}\varphi'_b w$ for all $w \in \mathbb{C}_\infty$, then $c_i(\varphi, b) = w^{m_i} c_i(\varphi', b)$ by (1.1.1). Since the elements of $I_{a,\varphi}$ are ratios of homogenous polynomials of the same grade, $I_a(\varphi) = I_a(\varphi')$. This implies that $I_a(\varphi)$ is contained in every field of definition for φ. moreover, the following holds.

Theorem 2.13. *Let $a \in \mathcal{O}$. Then $I_a(\varphi)$ is a field of definition for φ.*

Proof. See [Hay79, Theorem 6.5.]. □

In particular, from the discussion above, $I_a(\varphi) \subseteq I_b(\varphi)$ for any non constants $a, b \in \mathcal{O}$. Thus, $I_a(\varphi)$ does not depend on a choice of a. Therefore, we can simply write

$$I_a(\varphi) = I(\varphi).$$

Theorem 2.14. *The subfield $I(\varphi)$ is the smallest field of definition for φ.*

Proof. This is immediate. □

Corollary 2.15 ([Hay79, Corollary 6.7.])**.** *Let $\mathfrak{a}$ be an integral ideal of $\mathcal{O}$ then*

$$I(\mathfrak{a} * \varphi) \subseteq I(\varphi).$$

If $\mathfrak{a}$ is invertible, then

$$I(\mathfrak{a} * \varphi) = I(\varphi).$$

2.5 The main theorem of complex multiplication

Let $\iota : \mathcal{O} \hookrightarrow \mathbb{C}_\infty$ be the inclusion homomorphism. In this section, we equip all Drinfeld $\mathcal{O}$-modules with the $\mathcal{O}$-field ι. For an invertible $\mathcal{O}$-ideal $\mathfrak{a}$, define

$$\varphi^{\mathfrak{a}} := \mathfrak{a}^{-1} * \varphi^{\mathcal{O}}.$$

From Theorem 2.6 and Corollary 2.15, $I(\varphi^{\mathfrak{a}}) = I(\varphi^{\mathfrak{b}})$ for any two invertible integral $\mathcal{O}$-ideals $\mathfrak{a}$ and $\mathfrak{b}$. We denote this common field of invariants by $H_{\mathcal{O}}$. We will identify $H_{\mathcal{O}}$ by class field theory as the ring class field associated to the order $\mathcal{O}$.

Let $G_\infty := \mathrm{Aut}(\mathbb{C}_\infty/F)$. G_∞ acts naturally on a Drinfeld $\mathcal{O}$-module φ by acting on the coefficients of φ_a for all $a \in \mathcal{O}$. For $\sigma \in G_\infty$, we denote this action by $\sigma(\varphi)$. Now, let $\mathfrak{a}$ be an integral $\mathcal{O}$-ideal and $\sigma \in G_\infty$. For all $a \in \mathcal{O}$,

$$\varphi_a \varphi_{\mathfrak{a}} = \varphi_{\mathfrak{a}} (\mathfrak{a} * \varphi)_a$$

so that

$$\sigma(\varphi_a\varphi_{\mathfrak{a}}) = \sigma(\varphi_a)\sigma(\varphi_{\mathfrak{a}}) = \sigma(\varphi_{\mathfrak{a}}(\mathfrak{a} * \varphi_a)_a) = \sigma(\varphi_{\mathfrak{a}})\sigma(\mathfrak{a} * \varphi_a)_a).$$

Hence, we have

$$\sigma(\mathfrak{a} * \varphi) = \mathfrak{a} * \sigma(\varphi)$$

Furthermore, if $\varphi \simeq \varphi'$ then $\sigma(\varphi) \simeq \sigma(\varphi')$. Thus we have the following.

Proposition 2.16. *The Galois group G_∞ acts on $\mathscr{M}^r_{\mathscr{O}}(\mathbb{C}_\infty)$ and the action commutes with that of* $\mathbf{Pic}(\mathscr{O})$*.*

We now focus on the case $r = 1$. Can we describe the action of G_∞ on $\mathscr{M}^1_{\mathscr{O}}(\mathbb{C}_\infty)$ internally? For instance using the Frobenius elements associated to ideals of $\mathscr{O}$. It turns out that it is possible for Drinfeld $\mathscr{O}$-modules of rank one that belongs to isomorphism classes containing Drinfeld modules $\varphi^{\mathfrak{a}}$ for some invertible ideal $\mathfrak{a}$. We denote by $\mathscr{M}^{1,*}_{\mathscr{O}}(\mathbb{C}_\infty) \subseteq \mathscr{M}^1_{\mathscr{O}}(\mathbb{C}_\infty)$ the subset of such isomorphism classes. The group action $*$ induces an action of $\mathbf{Pic}(\mathscr{O})$ on $\mathscr{M}^{1,*}_{\mathscr{O}}(\mathbb{C}_\infty)$: if $\mathfrak{a} \in \mathbf{Pic}(\mathscr{O})$ and $\varphi^{\mathfrak{b}} \in \mathscr{M}^{1,*}_{\mathscr{O}}(\mathbb{C}_\infty)$, then $\mathfrak{a} * \varphi^{\mathfrak{b}} \simeq \mathfrak{a}\mathfrak{b}^{-1} * \varphi^{\mathscr{O}} \in \mathscr{M}^{1,*}_{\mathscr{O}}(\mathbb{C}_\infty)$. Since every rank one $\mathscr{O}$-lattice is homothetic to a fractional $\mathscr{O}$-ideal and any fractional $\mathscr{O}$-ideal of rank one is an $\mathscr{O}$-lattice, with Theorem 2.6, the action of $\mathbf{Pic}(\mathscr{O})$ makes $\mathscr{M}^{1,*}_{\mathscr{O}}(\mathbb{C}_\infty)$ into a principal homogeneous space, i.e. the action is faithful and transitive. In particular $\#\mathscr{M}^{1,*}_{\mathscr{O}}(\mathbb{C}_\infty) = \#\,\mathbf{Pic}(\mathscr{O})$. We also have the following.

Proposition 2.17. *The subset $\mathscr{M}^{1,*}_{\mathscr{O}}(\mathbb{C}_\infty) \subseteq \mathscr{M}^1_{\mathscr{O}}(\mathbb{C}_\infty)$ is invariant under the action of G_∞.*

Proof. See [Hay79, Proposition 8.2. and Proposition 8.3.]. □

We now look at the field $H_{\mathscr{O}}$, it satisfies the following.

Proposition 2.18. *The extension $H_{\mathscr{O}}/F$ is finite and Galois. Further, ∞ splits completely in $H_{\mathscr{O}}/F$.*

Proof. See [Hay79, Proposition 8.4.]. □

Let $G_{\mathscr{O}} := \mathrm{Gal}(H_{\mathscr{O}}/F)$ be the Galois group of $H_{\mathscr{O}}$ over F. The Galois group $G_{\mathscr{O}}$ acts naturally on $\mathscr{M}^{1,*}_{\mathscr{O}}(\mathbb{C}_\infty)$. An equivalence class in $\mathscr{M}^{1,*}_{\mathscr{O}}(\mathbb{C}_\infty)$ will be denoted by $[.]$. Let $\sigma \in G_{\mathscr{O}}$ and $[\varphi^{\mathfrak{a}}] \in \mathscr{M}^{1,*}_{\mathscr{O}}(\mathbb{C}_\infty)$, we may assume that $\varphi^{\mathfrak{a}}_a \in H_{\mathscr{O}}\{\tau\}$ for all $a \in \mathscr{O}$ since $H_{\mathscr{O}}$ is a field of definition for $\varphi^{\mathfrak{a}}$ (we can pass to an isomorphic module), then $\sigma[\varphi^{\mathfrak{a}}] := [\sigma\varphi^{\mathfrak{a}}]$ where the action of σ is defined in the same way as G_∞ acts on $\mathscr{M}^{1,*}_{\mathscr{O}}(\mathbb{C}_\infty)$. Therefore, each element of $G_{\mathscr{O}}$ induces an automorphism of $\mathscr{M}^{1,*}_{\mathscr{O}}(\mathbb{C}_\infty)$ as principal homogeneous space over $\mathbf{Pic}(\mathscr{O})$, this gives us a natural injective homomorphism

$$\Psi : G_{\mathscr{O}} \hookrightarrow \mathbf{Pic}(\mathscr{O}). \tag{2.5.1}$$

In particular, we can deduce that $H_{\mathscr{O}}/F$ is an abelian extension.

The following theorem answers the question that followed Proposition 2.16.

Theorem 2.19. *Suppose $\mathfrak{p} \subseteq \mathscr{O}$ is a nonzero prime ideal which does not divide the conductor $\mathfrak{C}$ of $\mathscr{O}$ in A and which does not ramify in $H_{\mathscr{O}}/F$. Let $\sigma_{\mathfrak{p}} \in G_{\mathscr{O}}$ be the Frobenius automorphism associated to $\mathfrak{p}$. Let φ be a Drinfeld $\mathscr{O}$-module which has $H_{\mathscr{O}}$ as field of definition and which represents a class in $\mathscr{M}^{1,*}_{\mathscr{O}}(\mathbb{C}_\infty)$. Then*

$$\sigma_{\mathfrak{p}}(\varphi) \simeq \mathfrak{p} * \varphi.$$

Proof. See [Hay79, Theorem 8.5.]. □

It is a standard fact that a prime ideal in $\mathscr{O}$ is invertible if and only if it does not divide the conductor. Therefore, by Theorem 2.19, the map Ψ is surjective. Furthermore, a prime $\mathfrak{p}$ of A which does not divide the conductor $\mathfrak{C}$ splits completely in $H_{\mathscr{O}}/F$ if $\Psi(\sigma_{\mathfrak{p}}) = 1 = [\mathscr{O}]$, this is equivalent to $\mathscr{O} \cap \mathfrak{p}$ being principal in $\mathscr{O}$ by Theorem 2.19. More precisely

Theorem 2.20 ([Hay79, Theorem 8.8.])**.** *The map Ψ in (2.5.1) is a natural isomorphism. A prime ideal $\mathfrak{p}$ of A which does not divide the conductor $\mathfrak{C}$ of $\mathscr{O}$ splits completely in $H_{\mathscr{O}}/F$ if and only if $\mathfrak{p} \cap \mathscr{O}$ is principal in $\mathscr{O}$.*

We can now identify $H_{\mathscr{O}}$ as the ring class field associated to $\mathscr{O}$. We denote by $\mathscr{P}_{\mathscr{O}}(\mathfrak{C})$ the group of principal ideals of A generated by the ideals $a\mathscr{O}$ with $a \in \mathscr{O}$ and a prime to $\mathfrak{C}$. Let $\mathscr{P}_1(\mathfrak{C})$ be the subgroup consisting of the ideals xA with $x \in F$ and $x \equiv 1 (\mod \mathfrak{C})$.

Theorem 2.21 ([Hay79, Theorem 8.10.])**.** *The extension $H_{\mathscr{O}}/F$ is class field to the $\mathfrak{C}$-ideal group $\mathscr{P}_{\mathscr{O}}(\mathfrak{C})$, and $\mathbf{Pic}(\mathscr{O})$ is isomorphic to the $\mathfrak{C}$-ideal class group $\mathscr{I}(\mathfrak{C})/\mathscr{P}_{\mathscr{O}}(\mathfrak{C})$ where $\mathscr{I}(\mathfrak{C})$ is the group of ideals of A which are prime to $\mathfrak{C}$. Only primes dividing the conductor can ramify in $H_{\mathscr{O}}/F$. The field of constants of $H_{\mathscr{O}}$ has degree d_∞ over $\mathbb{F}_q$.*

We can now state the main theorem of complex multiplication for Drinfeld modules which follows from the above results.

Theorem 2.22 (Main Theorem of Complex Multiplication)**.** *Let φ be a Drinfeld A-module of rank r over $\mathbb{C}_\infty$ with complex multiplication. Let $\mathscr{O} = \mathrm{End}(\varphi)$ be the full endomorphism ring which is an order in the degree r purely imaginary extension $K = \mathscr{O} \otimes_A F$. Let $\mathfrak{C}$ be the conductor of $\mathscr{O}$ in K. Then the finite Galois extension $H_\mathscr{O}/K$ is the ring class field of K with respect to $\mathscr{O}$. In particular, $H_\mathscr{O}$ is unramified outside $\mathfrak{C}$, the prime ∞ splits completely in $H_\mathscr{O}/K$ and we have an isomorphism $\mathbf{Pic}(\mathscr{O}) \simeq \mathrm{Gal}(H_\mathscr{O}/K)$ via the Artin map. If $\mathfrak{a}$ is an invertible ideal in $\mathscr{O}$ and $\sigma_\mathfrak{a} = (\mathfrak{a}, H_\mathscr{O}/K)$ then*

$$\sigma_\mathfrak{a}(\varphi) = \mathfrak{a} * \varphi.$$

Proof. The Drinfeld module φ can be seen as a rank one Drinfeld $\mathscr{O}$-module and the result is spelled out in Theorems 2.19, 2.20 and 2.21. □

A generation of ray class fields is also treated in [Hay79, §9.], we will make use of the results therein in the next chapter.

Chapter 3

Torsion Bounds For CM Drinfeld Modules

Let $r \geq 1$ be an integer and $q = p^s$ a power of an odd prime p (to avoid technical complications that may arise in characteristic 2) where $s > 0$ is an integer. Let F be a global function field with full constant field $\mathbb{F}_q$, ∞ a prime of F and A the ring of elements of F regular away from ∞. F is a finite extension of $\mathbb{F}_q(T)$ and we denote by $d_F := [F : \mathbb{F}_q(T)]$ its degree over $\mathbb{F}_q(T)$. We denote by F_∞ the completion of F with respect to the normalized valuation v_∞ associated to ∞. As usual $\mathbb{C}_\infty$ will denote the completion of $\overline{F}_\infty$ with respect to the unique extension of v_∞ to $\overline{F}_\infty$.

If $a \in A$ and $v_\infty(a) \geq 0$ then a has no poles by definition of A. Therefore a is algebraic over $\mathbb{F}_q$ (see for example [Sti09] Corollary 1.1.20) and then $a \in \mathbb{F}_q$ since $\mathbb{F}_q$ is the full constant field. We then have $v_\infty(a) < 0$ for all $a \in A \setminus \mathbb{F}_q$. We define the following parameter:

$$D_A := \inf\{-v_\infty(a), a \in A \setminus \mathbb{F}_q \text{ and } v_\infty(a) < 0\}.$$

D_A is well defined and depends only on A.

In this chapter, we assume that all the Drinfeld modules we work with are of generic characteristic and equipped with the A-field $\iota : A \longrightarrow \mathbb{C}_\infty$ with $\iota(a) = a$ for all $a \in A$.

Our original goal was to prove the following conjecture:

Conjecture 5. *For a fixed A, there exists a constant $C_{A,r} > 0$ depending only on A (through D_A, d_F, d_∞ and q) and r such that for any field extension L of degree d over F and all Drinfeld A-module with complex multiplication (CM) $\varphi : A \longrightarrow L\{\tau\}$ defined over L and of rank r:*

$$\#\varphi(L)_{\text{tors}} \leq C_{A,r}\, d \log\log d.$$

However, we are only able to establish a weaker version and a particular case.

Although The constant C ultimately depends on D_A, d_F, d_∞, q and r, it is absolute in the sense that it depends neither on the field L nor on φ.

Let us start by fixing a degree d field extension L/F and a CM Drinfeld A-module $\varphi : A \longrightarrow L\{\tau\}$ of rank r defined over L. Recall that our aim is to prove Conjecture 5 with a positive constant C which eventually will be independent of φ and L. Our strategy consists roughly of reducing the problem to rank one Drinfeld module (in the sense of Hayes theory [Hay79]) with maximal endomorphism ring and using a version of Mertens' theorem for algebraic curves to prove a uniform lower bound on the analogue of Euler's totient function for function fields.

3.1 Reduction to rank one

In this section we will extend φ to an $\mathrm{End}(\varphi)$-Drinfeld module ψ of rank 1 and show that our problem can be reduced to that case. Although $\mathrm{End}(\varphi)$ is not a Drinfeld ring, a good theory of this generalization has been developed by Hayes [Hay79].

The endomorphism ring of φ over $\overline{F}$, $\mathcal{O} := \mathrm{End}(\varphi) = \{f \in \overline{F}\{\tau\}, f\varphi_a = \varphi_a f \ \forall a \in A\}$ is a commutative A-algebra of rank r and is by definition $\mathrm{Cent}_{\overline{F}\{\tau\}}(\varphi(A))$. Thus $\mathcal{O}$ is an order in a degree r extension of F (which is purely imaginary, look at Theorem 4.7.17 in [Gos98]), say $K \simeq \mathrm{End}(\varphi) \otimes_A F$, via the derivation map $D : \mathrm{End}(\varphi) \longrightarrow K$ that sends an element $f \in \mathrm{End}(\varphi)$ to the coefficient of τ^0 in f. The ring A being commutative, we have $\varphi(A) \subseteq \mathcal{O}$ and, as φ is an embedding, this allows us to extend φ to a Drinfeld $\mathcal{O}$-module (in the sense of Hayes) $\psi : \mathcal{O} \longrightarrow \overline{F}\{\tau\}$ such that $\psi_a = \varphi_a \ \forall a \in A$. As an $\mathcal{O}$-module ψ has rank $1 = \dfrac{r}{[K:F]}$.

Since our interest lies in bounding the size of the L-rational torsion submodule of φ, we need to compare $\#\varphi(L)_{\mathrm{tors}}$ and $\#\psi(L)_{\mathrm{tors}}$ to make sure that the reduction works. Actually, the L-rational torsion submodule is preserved.

Proposition 3.1. *If φ and ψ are as above then: $\varphi(L)_{\mathrm{tors}} = \psi(L)_{\mathrm{tors}}$.*

Proof. Since ψ is an extension of φ, it is clear that $\varphi(L)_{\mathrm{tors}} \subseteq \psi(L)_{\mathrm{tors}}$. Conversely, if $x \in \psi(L)_{\mathrm{tors}}$ then $x \in \mathrm{Ker}(f)$ for some $f \in \mathcal{O}$. If $\tilde{f}$ is a dual of f as an isogeny from φ to φ, then from Proposition 1.12, there exists $a \in A$ such that $\tilde{f}f = \varphi_a$. Taking into account Remark 1.4, we have $\varphi_a(x) = \tilde{f}f(x) =$

$\tilde{f}(f(x)) = \tilde{f}(0) = 0$, which means $x \in \operatorname{Ker} \varphi_a \subseteq \varphi_{\text{tors}}$. Hence, $x \in \varphi(L)_{\text{tors}}$ and the result follows. □

In view of our main goal, Proposition 3.1 allows us to reduce to proving Conjecture 5 for Drinfeld modules of rank one $\psi : \mathcal{O} \to \overline{F}\{\tau\}$ where $\mathcal{O}$ is an order in a degree r extension K/F. If a uniform bound occurs for such ψ then it also occurs for our original Drinfeld module.

The next step is to reduce to the case where $\mathcal{O} = \mathcal{O}_K$ is the maximal order of K. This allows more flexibility since $\mathcal{O}_K$ is a Dedekind domain. In particular we get a nice structure theorem for torsion submodules.

3.2 Field of definition

In this section we want to identify *fields of definition* of $\psi : \mathcal{O}_K \to \overline{F}\{\tau\}$, namely the smallest field extension that contains the coefficients of ψ_a for $a \in \mathcal{O}_K$ and the smallest field of definition of ψ.

Remark 3.2. To avoid confusions it is essential to make the following distinction between terminologies. When we say ϕ is defined over a subfield $k \subseteq \mathbb{C}_\infty$ we mean that ϕ_a has coefficients in k for all $a \in \mathcal{O}_K$, in particular k is a field of definition of ϕ. Being a field of definition is a much weaker condition, k can be a field of definition for ϕ even if it does not contain the coefficients of all the ϕ_a's. In [Hay79] these terminologies have the same meaning as in Definition 2.10 and $\phi : A \longrightarrow L\{\tau\}$ is said to be a Drinfeld module over L.

In the process of reducing $\varphi : A \longrightarrow L\{\tau\}$ to $\psi : \mathcal{O}_K \longrightarrow \overline{F}\{\tau\}$, the fact that φ is defined over L is not preserved because we extended by the whole endomorphism ring over $\overline{F}$. However, we have the following result:

Proposition 3.3. *The compositum LK is a field of definition of ψ and it contains the coefficients of ψ_a for all $a \in \mathcal{O}_K$.*

Proof. Let $f = \sum_{i=0}^{n} f_i \tau^i \in \operatorname{End}(\varphi)$ and choose $\varphi_a = \sum_{i=0}^{m} a_i \tau^i \in L\{\tau\}$ such that $a_0 \notin \mathbb{F}_q$ where $n, m > 0$. We have $\varphi_a f = f \varphi_a$ and after explicit computations we find:

$$\varphi_a f = \sum_{i=0}^{m} \left(\sum_{j=0}^{n} a_i f_j^{q^i} \tau^{i+j} \right) = \sum_{k=0}^{m+n} \left(\sum_{l=0}^{k} a_l f_{k-l}^{q^l} \right) \tau^k$$

and

$$f \varphi_a = \sum_{i=0}^{n} \left(\sum_{j=0}^{m} f_i a_j^{q^i} \tau^{i+j} \right) = \sum_{k=0}^{m+n} \left(\sum_{l=0}^{k} f_l a_{k-l}^{q^l} \right) \tau^k$$

with the convention $a_l = 0$ for $l > n$ and $f_l = 0$ for $l > m$. We deduce that for $1 \leq k \leq m$:

$$\sum_{l=0}^{k} a_l f_{k-l}^{q^l} = \sum_{l=0}^{k} f_l a_{k-l}^{q^l}$$

and then:

$$f_k(a_0 - a_0^{q^k}) = \sum_{l=0}^{k-1} f_l a_{k-l}^{q^l} - \sum_{l=1}^{k} a_l f_{k-l}^{q^l}.$$

Recall that we have a map $D : \sum_{i=0}^{n} c_i \tau^i \in \mathrm{End}(\varphi) \longmapsto c_0 \in K$ that injects $\mathrm{End}(\varphi)$ into K, thus $f_0 \in K$. Now, since φ has generic characteristic, $a_0 - a_0^{q^k} \neq 0$ so that f_k is a rational function of $f_0, \cdots, f_{k-1}, a_0, \cdots, a_k$ for all $k = 1, \cdots, m$. Therefore the a_i's $\in L$. We then have $f_k \in LK$ by induction. □

A field of definition of a Drinfeld module is clearly not unique and is defined up to isomorphism according to Definition 2.10. The following theorem asserts the existence of a smallest field of definition, i.e. one that is contained in any other field of definition.

Theorem 3.4 ([Hay79] section 8). *There exists a smallest field of definition $H_{\mathcal{O}_K}/K$ for $\psi : \mathcal{O}_K \longrightarrow LK\{\tau\}$ which is a finite Galois extension with Galois group* $\mathrm{Gal}(H_{\mathcal{O}_K}/K) \simeq \mathbf{Pic}(\mathcal{O}_K)$. *Furthermore $H_{\mathcal{O}_K}$ is the* Hilbert class field *associated to $\mathcal{O}_K$ by class field theory.*

Recall that $H_{\mathcal{O}_K}$ is the maximal unramified abelian extension of K over which ∞ splits completely. Essentially, the theorem says that each Drinfeld $\mathcal{O}_K$-module of rank one is isomorphic over $\mathbb{C}_\infty$ to one for which the coefficients of the images are in $H_{\mathcal{O}_K}$.

3.3 Ray class field containment

From now on we fix the following notations:

- If M is an R-module, the annihilator of an R-submodule $N \subseteq M$ is defined as:
$$\mathrm{Ann}(N) := \{s \in R : s.n = 0 \; \forall n \in N\}.$$
- For a field K and a non-zero ideal $\mathfrak{a} \subseteq \mathcal{O}_K$, $K^{(\mathfrak{a})}$ denotes the $\mathfrak{a}$-ray class field of K associated to $\mathfrak{a}$.
- $|\mathfrak{a}|_K := \#\mathcal{O}_K/\mathfrak{a}$ denotes the norm of $\mathfrak{a}$. If the context is clear and no confusion is likely to arise we drop the index and simply write $|\mathfrak{a}|$.

- The set of primes of K will be denoted $\mathbb{P}_K$.
- $\Phi_{\mathcal{O}_K}(\mathfrak{a}) := \#(\mathcal{O}_K/\mathfrak{a})^* = |\mathfrak{a}|\prod_{\substack{\mathfrak{p}|\mathfrak{a} \\ \mathfrak{p} \text{ prime}}}\left(1 - \frac{1}{|\mathfrak{p}|}\right)$ denotes the analogue of the Euler totient function for K.
- As usual if R is a Dedekind domain, h_R is its class number.

Let $[L : F] = d$, $\varphi : A \to L\{\tau\}$ be an $\mathcal{O}_K$-CM Drinfeld module of rank r defined over L/F and ψ the resulting rank one Drinfeld $\mathcal{O}_K$-module as in section 3.2. As pointed out previously, we are interested in the set of L-rational torsion points $\psi(L)_{\text{tors}}$. However, since ψ is defined over the larger field extension LK/L, $\psi(L)_{\text{tors}}$ is not an $\mathcal{O}_K$-submodule of $\overline{F}$. For this reason we need to look at the larger set of LK-rational torsion points $\psi(LK)_{\text{tors}}$. Essentially the LK-rational torsions come from a non-zero ideal $\mathfrak{a}_{LK} \subseteq \mathcal{O}_K$ since ψ is a rank one Drinfeld $\mathcal{O}_K$-module. The ray class field $K^{(\mathfrak{a}_{LK})}$ of K associated to $\mathfrak{a}_{LK}$ plays a crucial role, we want to prove a containment result about it which will allow us to deduce an inequality fundamental for the rest of this work.

Theorem 3.5. *Let φ be an $\mathcal{O}_K$-CM Drinfeld module of rank r defined over L and $\psi : \mathcal{O}_K \to LK\{\tau\}$ the corresponding rank one Drinfeld module. As an $\mathcal{O}_K$-module $\psi(LK)_{\text{tors}} = \psi[\mathfrak{a}_{LK}] \simeq \mathcal{O}_K/\mathfrak{a}_{LK}$ for some non-zero ideal $\mathfrak{a}_{LK} \subseteq \mathcal{O}_K$.*

Proof. Since the ring $\mathcal{O}_K$ is Dedekind and $\psi(LK)_{\text{tors}}$ is a torsion $\mathcal{O}_K$-module, Theorem 1.29 implies that $\psi(LK)_{\text{tors}}$ can be written uniquely as

$$\psi(LK)_{\text{tors}} \simeq \mathcal{O}_K/\mathfrak{a}_1 \oplus \cdots \oplus \mathcal{O}_K/\mathfrak{a}_m,$$

where $\mathfrak{a}_1 \subseteq \cdots \subseteq \mathfrak{a}_m$ is a chain of non zero proper ideals of $\mathcal{O}_K$. Therefore, as ψ has rank one and $\psi[\mathfrak{a}_m] \subseteq \cdots \subseteq \psi[\mathfrak{a}_1] \subseteq \psi(LK)_{\text{tors}}$, we have $m = 1$ so that $\psi(LK)_{\text{tors}} \simeq \mathcal{O}_K/\mathfrak{a}_1$. It suffices to take $\mathfrak{a}_{LK} = \mathfrak{a}_1$. □

Our next goal is to bound the degree $d = [L : F]$ from below by a constant (depending only on q and r) multiple of $h_{\mathcal{O}_K}\Phi_{\mathcal{O}_K}(\mathfrak{a}_{LK})$. To do so we compute the degree $[K^{(\mathfrak{a}_{LK})} : K]$, which is equal to $\dfrac{h_{\mathcal{O}_K}\Phi_{\mathcal{O}_K}(\mathfrak{a}_{LK})}{(q-1)}$, and show that $K^{(\mathfrak{a}_{LK})}$ is contained in an extension of LK that is not too big. This can be done by using a Drinfeld $\mathcal{O}_K$-module of rank one defined over $H_{\mathcal{O}_K}$. However, our Drinfeld module $\psi : \mathcal{O}_K \to LK\{\tau\}$ is not defined over $H_{\mathcal{O}_K}$ in general but it is isomorphic to one such Drinfeld module by Theorem 3.4. We will see that we can pass to an isomorphic module.

The following ray class field containment result is essentially the main part of our argument.

Theorem 3.6. *Let $\varphi : \mathscr{O}_K \to H_{\mathscr{O}_K}\{\tau\}$ be a rank one Drinfeld module defined over $H_{\mathscr{O}_K}$ and $\mathfrak{a} \subseteq \mathscr{O}_K$ be a non-zero ideal. Then $K^{(\mathfrak{a})} \subseteq H_{\mathscr{O}_K}(\varphi[\mathfrak{a}])$.*

Proof. We give a sketch of the proof, for all the details we refer to [Hay79]. Since φ is of generic characteristic, $\varphi_{\mathfrak{a}}(x)$ is separable and then $H_{\mathscr{O}_K}(\varphi[\mathfrak{a}])/H_{\mathscr{O}_K}$ is a Galois extension. Denote by $G_{\mathfrak{a}}$ the Galois group $\mathrm{Gal}(H_{\mathscr{O}_K}(\varphi[\mathfrak{a}])/H_{\mathscr{O}_K})$. Now, since φ is defined over $H_{\mathscr{O}_K}$ we have a Galois action

$$\Psi_{\mathfrak{a}} : G_{\mathfrak{a}} \to \mathrm{Aut}_{\mathscr{O}_K}(\varphi[\mathfrak{a}]) \tag{3.3.1}$$

with $\mathrm{Aut}_{\mathscr{O}_K}(\varphi[\mathfrak{a}]) = \mathrm{Aut}_{\mathscr{O}_K}(\varphi_{\mathfrak{a}}) \simeq (\mathscr{O}_K/\mathfrak{a})^*$ which is easily seen to be injective (the Galois action permutes the roots of $\varphi_{\mathfrak{a}}$). The map Ψ is actually an isomorphism (Theorem 9.2 of [Hay79]) and the $\mathfrak{a}$-ray class field $K^{(\mathfrak{a})}$ is the fixed field of the inverse image of $\mathbb{F}_q^*$ by the above action (Theorem 9.7 of [Hay79]). □

An analogue of Theorem 3.6 holds for elliptic curves with complex multiplication by the maximal order of an imaginary quadratic number field. See for instance [Sil94] Theorem 5.6.

Lemma 3.7. *Let K be a function field over $\mathbb{F}_q$. Then $[H_{\mathscr{O}_K} : K] = h_{\mathscr{O}_K}$.*

Proof. This is a standard result. See for instance [Ros87] Theorem 1.3. □

Lemma 3.8. *Let K/F be a purely imaginary extension with ring of integers $\mathscr{O}_K$ and $\mathfrak{a} \subseteq \mathscr{O}_K$ a non-zero ideal. Then $[K^{(\mathfrak{a})} : K] = \dfrac{h_{\mathscr{O}_K}\Phi_{\mathscr{O}_K}(\mathfrak{a})}{q-1}$.*

Proof. Let $\varphi : \mathscr{O}_K \to H_{\mathscr{O}_K}\{\tau\}$ be a rank one Drinfeld $\mathscr{O}_K$-module defined over $H_{\mathscr{O}_K}$. By Theorem 3.6, $K^{(\mathfrak{a})} \subseteq H_{\mathscr{O}_K}(\varphi(\mathfrak{a}))$ so that

$$[K^{(\mathfrak{a})} : K] = \frac{[H_{\mathscr{O}_K}(\varphi[\mathfrak{a}]) : K]}{[H_{\mathscr{O}_K}(\varphi[\mathfrak{a}]) : K^{(\mathfrak{a})}]}.$$

We have $[H_{\mathscr{O}_K}(\varphi[\mathfrak{a}]) : K] = [H_{\mathscr{O}_K}(\varphi[\mathfrak{a}]) : H_{\mathscr{O}_K}][H_{\mathscr{O}_K} : K]$. Since the Galois action $\Psi_{\mathfrak{a}}$ (3.3.1) is an isomorphism

$$[H_{\mathscr{O}_K}(\varphi[\mathfrak{a}]) : H_{\mathscr{O}_K}] = \#(\mathscr{O}_K/\mathfrak{a})^* = \Phi_{\mathscr{O}_K}(\mathfrak{a}).$$

With Lemma 3.7 this gives us $[H_{\mathscr{O}_K}(\varphi[\mathfrak{a}]) : K] = h_{\mathscr{O}_K}\Phi_{\mathscr{O}_K}(\mathfrak{a})$. Now Theorem 9.7 of [Hay79] says that $K^{(\mathfrak{a})}$ is the fixed field of $\Psi_{\mathfrak{a}}^{-1}(\mathbb{F}_q^*)$, which implies $\mathrm{Gal}(H_{\mathscr{O}_K}(\varphi[\mathfrak{a}])/K^{(\mathfrak{a})}) \simeq \mathbb{F}_q^*$ and therefore $[H_{\mathscr{O}_K}(\varphi[\mathfrak{a}]) : K^{(\mathfrak{a})}] = q-1$. □

Lemma 3.9. *Let L/F be a degree d extension, $\varphi : A \to L\{\tau\}$ be a rank r $\mathcal{O}_K$-CM Drinfeld A-module and $\psi : \mathcal{O}_K \to LK\{\tau\}$ the rank one Drinfeld $\mathcal{O}_K$-module obtained from φ as in section 3.1. Then there exists a Drinfeld $\mathcal{O}_K$ module ψ' defined over $H_{\mathcal{O}_K}$ and an isomorphism $c : \psi \to \psi' \in \overline{F}$ such that $[LK(c) : LK] \leq q^{rD_A d_\infty} - 1$.*

Proof. From Theorem 3.4, there exists a Drinfeld $\mathcal{O}_K$-module ψ' defined over $H_{\mathcal{O}_K}$ such that $\psi \simeq \psi'$ over $\mathbb{C}_\infty$ (actually over $\overline{F}$ since ψ and ψ' are both defined over $LK \supseteq H_{\mathcal{O}_K}$). Therefore, there exists $c \neq 0 \in \overline{F}$ such that $c\psi_a = \psi'_a c$ for all $a \in \mathcal{O}_K$. Consider an element $b \in A$ such that $-v_\infty(b) = D_A$, that is to say $\deg(b) = d_\infty D_A$.Then the twisted polynomials ψ_b and ψ'_b are of degree $rd_\infty D_A$ in τ since ψ is an extension of φ which has rank r. Therefore $\psi_b(x)$ and $\psi'_b(x) \in LK[x]$ are $\mathbb{F}_q$-linear polynomials of degree $q^{rd_\infty D_A}$. Set $t = rd_\infty D_A$. Now let $\psi_b(x) = \alpha_0 x + \alpha_1 x^q + \cdots + \alpha_t x^{q^t}$ and $\psi'_b(x) = \beta_0 x + \beta_1 x^q + \cdots + \beta_t x^{q^t}$ where $\alpha_i, \beta_i \in LK$ with $\alpha_t, \beta_t \neq 0$. From the equality $c\psi_b = \psi'_b c$ we deduce that $c\alpha_0 x + c\alpha_1 x^q + \cdots + c\alpha_t x^{q^t} = c\beta_0 x + c^q\beta_1 x^q + \cdots + c^{q^t}\beta_t x^{q^t}$ which implies $c\alpha_t = c^{q^t}\beta_t$. As $c \neq 0$, it satisfies the polynomial equation $\alpha_t - \beta_t x^{q^t - 1} = 0$. Therefore $[LK(c) : LK] \leq q^t - 1$. □

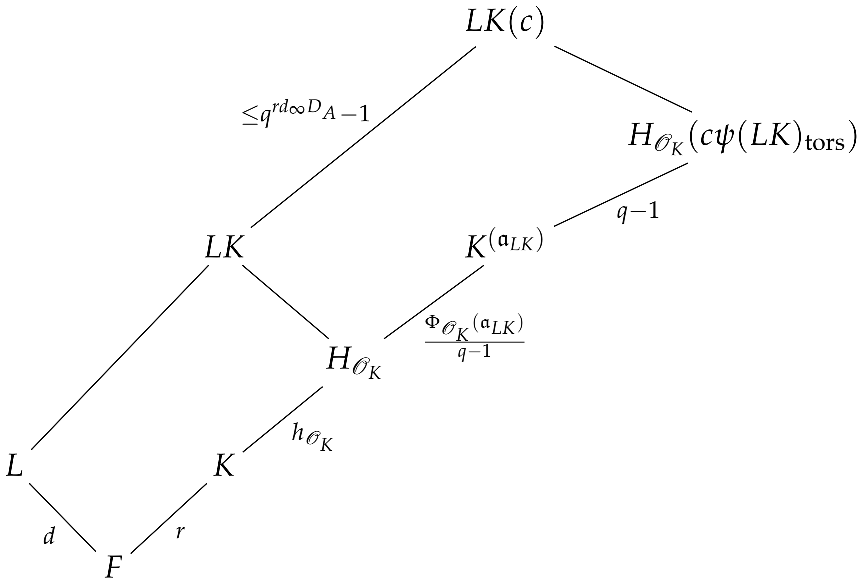
Lemma 3.10. *Let φ and $\psi : A \to L\{\tau\}$ be two isomorphic Drinfeld modules defined over L and $c : \varphi \to \psi$ an isomorphism. Then $\varphi(L)_{\text{tors}} = c^{-1}\psi(L)_{\text{tors}}$.*

Proof. By definition, $c\varphi_a = \psi_a c$ for all $a \in A$. Let $x \in \varphi(L)_{\text{tors}}$, for some $a \in A$ we have $\varphi_a(x) = 0$ so that $\psi_a(cx) = 0$. Therefore $cx \in \psi(L)_{\text{tors}}$ and $\varphi(L)_{\text{tors}} \subseteq c^{-1}\psi(L)_{\text{tors}}$. Conversely, if $y \in \psi(L)_{\text{tors}}$ then $(c\varphi_a c^{-1})(y) = \psi_a(y) = 0$ for some $a \in A$. Hence, $c\varphi_a(c^{-1}y) = 0$ and then $c^{-1}y \in \varphi(L)_{\text{tors}}$. Therefore $y \in c\varphi(L)_{\text{tors}}$ and then $\psi(L)_{\text{tors}} \subseteq c\varphi(L)_{\text{tors}}$, which implies that $c^{-1}\psi(L)_{\text{tors}} \subseteq \varphi(L)_{\text{tors}}$. □

Theorem 3.11. *Let L/F be a degree d extension, $\varphi : A \to L\{\tau\}$ a rank r $\mathcal{O}_K$-CM Drinfeld module, $\psi : \mathcal{O}_K \to LK\{\tau\}$ its extension to a rank one Drinfeld $\mathcal{O}_K$-module and $\psi(LK)_{\text{tors}} = \psi[\mathfrak{a}_{LK}] \simeq \mathcal{O}_K/\mathfrak{a}_{LK}$. Then*

$$d \geq \frac{h_{\mathcal{O}_K}\Phi_{\mathcal{O}_K}(\mathfrak{a})}{r(q-1)(q^{rd_\infty D_A} - 1)}.$$

Proof. We deduce from Lemma 3.9and Lemma 3.10 that there exists a Drinfeld $\mathcal{O}_K$-module ψ' defined over $H_{\mathcal{O}_K}$ and an isomorphism $c : \psi \to \psi'$ such that $[LK(c) : LK] \leq q^{rd_\infty D_A} - 1$ and $\psi'(LK)_{\text{tors}} = c\psi(LK)_{\text{tors}}$. Theorem 3.6 implies that $K^{(\mathfrak{a}_{LK})} \subseteq H_{\mathcal{O}_K}(\psi'(LK)_{\text{tors}}) = H_{\mathcal{O}_K}(c\psi(LK)_{\text{tors}})$. Now, since $H_{\mathcal{O}_K} \subseteq LK$ (LK is a field of definition and $H_{\mathcal{O}_K}$ is the smallest field of definition) and $\psi(LK)_{\text{tors}} \subseteq LK$, we have $H_{\mathcal{O}_K}(\psi'(LK)_{\text{tors}}) \subseteq LK(c)$. We then have the following towers of fields with the corresponding degrees:


$LK(c)$
$\leq q^{rd_\infty D_A}-1$
$H_{\mathscr{O}_K}(c\psi(LK)_{\text{tors}})$
$q-1$
LK
$K^{(\mathfrak{a}_{LK})}$
$\frac{\Phi_{\mathscr{O}_K}(\mathfrak{a}_{LK})}{q-1}$
$H_{\mathscr{O}_K}$
$h_{\mathscr{O}_K}$
L
K
d
r
F

Consequently, with Lemma 3.8 we get:

$$dr(q^{rd_\infty D_A}-1) \geq [LK(c):F] \geq [K^{(\mathfrak{a}_{LK})}:K] = \frac{h_{\mathscr{O}_K}\Phi_{\mathscr{O}_K(\mathfrak{a}_{LK})}}{q-1}$$

Therefore

$$d \geq \frac{h_{\mathscr{O}_K}\Phi_{\mathscr{O}_K}(\mathfrak{a})}{r(q-1)(q^{rd_\infty D_A}-1)}.$$

□

3.4 Uniform lower bound for the Euler function

We first introduce a version of Mertens theorem for algebraic curves, this will allow us to give a uniform lower bound for $\Phi_{\mathscr{O}_K}(\mathfrak{a})$.

3.4.1 Generalized Mertens theorem

Phillipe Lebacque proved a generalised version of the celebrated Mertens theorem for smooth absolutely irreducible projective algebraic varieties defined over $\mathbb{F}_q$, [Leb07, Theorem 7.]. We are only interested in the particular case of smooth geometrically irreducible projective algebraic curves. Let $\mathscr{C}$ be such a curve of genus g and let $|\mathscr{C}|$ be the set of its closed points (which is in a one-to-one correspondence with the set of primes of the function field $\mathbb{F}_q(\mathscr{C})$ of $\mathscr{C}$. For $n \geq 1$ an integer, define the following quantity:

$$\Phi_{q^n} := \{\mathfrak{p} \in |\mathscr{C}| / \deg(\mathfrak{p}) = n\}.$$

We also consider the arithmetic zeta function of $\mathscr{C}$ defined as

$$\zeta_{\mathscr{C}}(s) = \prod_{\mathfrak{p} \in |\mathscr{C}|} \left(\frac{1}{1 - |\mathfrak{p}|^{-s}} \right),$$

where $|\mathfrak{p}| = q^{\deg(\mathfrak{p})}$ is the degree of the residue field at $\mathfrak{p}$ over $\mathbb{F}_q$.

Theorem 3.12 (Mertens theorem for curves, [Leb07, Theorem 7.]). *For any smooth geometrically irreducible projective algebraic curve $\mathscr{C}|_{\mathbb{F}_q}$, one has, as $N \to +\infty$:*

$$\sum_{n=1}^{N} \Phi_{q_n} \log \left(\frac{q^n}{q^n - 1} \right) = \log N + \gamma + \log \left(\chi_{\mathscr{C}} \log q \right) + \mathscr{O}\left(\frac{1}{N} \right) + b\mathscr{O}\left(\frac{q^{-\frac{N}{2}}}{N} \right)$$

where $\gamma \simeq 0.5772156649$ is the Euler-Mascheroni constant, $b = \max(1, g)$ and $\chi_{\mathscr{C}} = \operatorname{Res}_{s=1} \zeta_{\mathscr{C}}(s)$. Furthermore, the constants in the $\mathscr{O}$ are effective and do not depend on the curve $\mathscr{C}$.

For later use we want to compute the quantity $\chi_{\mathscr{C}}$ using the zeta function. The following theorem establishes the rationality of the zeta function of an algebraic curve over a finite field and the functional equation that it satisfies.

Theorem 3.13. *Let $\mathscr{C}$ be a smooth geometrically irreducible projective algebraic curve over $\mathbb{F}_q$ of genus g. Let $t = q^{-s}$ and write $\zeta_{\mathscr{C}}(s) = Z(\mathscr{C}, t)$. Then there is a polynomial $P_{\mathscr{C}}(t) \in \mathbb{Z}[t]$ of degree $2g$ such that*

$$Z(\mathscr{C}, t) = \frac{P_{\mathscr{C}}(t)}{(1-t)(1-qt)}$$

for all $s \in \mathfrak{R}(s) > 1$, the rational function provides an analytic continuation to the whole complex plane. $Z(\mathscr{C}, t)$ has simple poles at $s = 0$ and $s = 1$. One has $P_{\mathscr{C}}(0) = 1$ and $P_{\mathscr{C}}(1) = h_{\mathbb{F}_q(\mathscr{C})}$. Furthermore, $P_{\mathscr{C}}(t)$ satisfies the functional equation $P_{\mathscr{C}}(t) = q^g t^{2g} P_{\mathscr{C}}(\frac{1}{qt})$ for all s.

Proof. One can consult [Ros02] Theorem 5.9 for a proof. The way the theorem is stated in [Ros02] does not refer to algebraic curves but rather the associated function fields. □

With the Riemann hypothesis, Theorem 3.13 is a particular case for curves of the celebrated Weil conjectures. As a corollary we can now easily compute $\chi_{\mathscr{C}}$.

Corollary 3.14. *Let $h_{\mathbb{F}_q(\mathscr{C})}$ be the class number of the function field of $\mathscr{C}$, then*

$$\chi_{\mathscr{C}} = \frac{h_{\mathbb{F}_q(\mathscr{C})}}{q^g(1-q^{-1})\log q}.$$

Proof. Since $Z(\mathscr{C},t) = Z(\mathscr{C},q^{-s})$ has a simple pole at $s=1$ we can compute the corresponding residue as follows:

$$\begin{aligned}
\chi_{\mathscr{C}} &= \operatorname{Res}_{s=1} Z(\mathscr{C},q^{-s}) \\
&= \lim_{s\to 1}(s-1)Z(\mathscr{C},q^{-s}) \\
&= \lim_{s\to 1}(s-1)\frac{P_{\mathscr{C}}(q^{-s})}{(1-q^{-s})(1-q^{-s})} \\
&= \lim_{s\to 1}(s-1)\frac{P_{\mathscr{C}}\left(\frac{1}{q^{1-s}}\right)q^g q^{-2gs}}{(1-q^{-s})(1-q^{-s})} \quad \text{using the functional equation of Theorem 3.13} \\
&= \frac{h_{\mathbb{F}_q(\mathscr{C})}}{q^g(1-q^{-1})}\lim_{s\to 1}\frac{s-1}{1-q^{1-s}}
\end{aligned}$$

Now, since $\frac{1}{1-q^{1-s}}$ has a simple pole at $s=1$,

$$\begin{aligned}
\lim_{s\to 1}\frac{s-1}{1-q^{1-s}} &= \operatorname{Res}_{s=1}\frac{1}{1-q^{1-s}} \\
&= \frac{1}{\frac{\mathrm{d}}{\mathrm{d}s}(1-q^{1-s})|_{s=1}} \\
&= \frac{1}{\log q}.
\end{aligned}$$

The second equality above holds because $1-q^{1-s}$ is holomorphic. □

Next, we need to compute an upper bound of the product $\prod_{|\mathfrak{p}|\leq q^N}\left(1-\frac{1}{|\mathfrak{p}|}\right)^{-1}$ in terms of $Nh_{\mathbb{F}_q(\mathscr{C})}$ up to an absolute constant multiple (which eventually depends on q) when N is large enough. This can be deduced from Theorem 3.12.

To proceed we introduce some auxilliary series, see section 4.2 of [Leb07].

For any sequence $(v_n)_{n\in\mathbb{N}}$ such that the series $\sum_{n\in\mathbb{N}} v_n t^n$ has strictly positive radius of convergence ρ, put:

$$\psi_{m,v}(t) = \sum_{n=1}^{+\infty} v_{mn}t^{mn}.$$

We have an explicit formula :

Theorem 3.15. *For $t < q^{-1}\rho$ we have:*

$$\sum_{n=1}^{\infty} n\Phi_{q^n}\psi_{n,v}(t) = \psi_{1,v}(t) + \psi_{1,v}(qt) - \sum_{i=1}^{g} \psi_{1,v}(q^{\frac{1}{2}}\omega_i t) \tag{3.4.1}$$

where the ω_i's are algebraic numbers of modulus 1.

Proof. See [LT97]. □

For a fixed $N \in \mathbb{N}$ consider the following sequence:

$$v_n(N) = \begin{cases} \frac{1}{n} \text{ if } n \leq N \\ 0 \text{ otherwise.} \end{cases}$$

Appying the explicit formula 3.4.1 with $t = q^{-1}$, we obtain

$$S_0(N) = S_1(N) + S_2(N) + S_3(N)$$

where, with a little computation:

$$S_0(N) = \sum_{n=1}^{N} \left(\frac{1}{nq^n} \sum_{m|n} m\Phi_{q^m} \right)$$

$$S_1(N) = \sum_{n=1}^{N} \frac{1}{n}$$

$$S_2(N) = \sum_{n=1}^{N} \frac{1}{nq^n}$$

$$S_3(N) = -\sum_{i=1}^{g}\sum_{n=1}^{N} \frac{1}{n}(q^{-\frac{1}{2}}\omega_i)^n.$$

The following four lemmas relate the quantities $S_0(N), S_1(N), S_2(N)$ and $S_3(N)$ to Theorem 3.12. These are actually the main ingredients of its proof for which we refer to [Leb07] section 4.2. We state the lemmas only for dimension 1 (i.e. for curves).

Lemma 3.16.

$$0 \leq \sum_{n=1}^{N} \Phi_{q^n} \log\left(\frac{q^n}{q^n - 1}\right) - S_0(N) \leq \frac{8}{Nq^{\frac{N}{2}}} + \frac{12g}{Nq^{\frac{3N}{4}}}$$

Lemma 3.17.

$$0 \leq \log\left(\frac{q}{q-1}\right) - S_2(N) = \sum_{n=N+1}^{+\infty} \frac{1}{nq^n} \leq \frac{1}{q^N(N+1)(q-1)}$$

Lemma 3.18.

$$\frac{1}{N(N+1)} \leq S_1(N) - \log N - \gamma \leq \frac{1}{N}$$

Lemma 3.19.

$$\left|S_3(N) - \log\left(\chi_{\mathscr{C}} \log q\right) + \log\left(\frac{q}{q-1}\right)\right| \leq \frac{b}{(q^{\frac{1}{2}}-1)(N+1)(q^{\frac{N}{2}}-1)}$$

We are now ready to prove the following theorem:

Theorem 3.20. *Let $\mathscr{C}$ be a smooth geometrically irreducible projective algebraic curve over $\mathbb{F}_q$. Then for $N \geq 6$ we have the following inequality:*

$$\prod_{|\mathfrak{p}| \leq q^N} \left(1 - \frac{1}{|\mathfrak{p}|}\right)^{-1} \leq e^4 N\, h_{\mathbb{F}_q(\mathscr{C})}$$

where the product runs over the primes of $\mathbb{F}_q(\mathscr{C})$.

Proof. Recall that Φ_{q^n} is the number of primes of degree n in $\mathbb{F}_q$ and that $|\mathfrak{p}| \leq q^N$ is equivalent to $\deg(\mathfrak{p}) \leq n$. Then we have:

$$\begin{aligned}\prod_{|\mathfrak{p}| \leq q^N} \left(1 - \frac{1}{|\mathfrak{p}|}\right)^{-1} &= \prod_{n=1}^{N} \left(1 - \frac{1}{q^n}\right)^{-\Phi_{q^n}} \\ &= \prod_{n=1}^{N} \left(\frac{q^n}{q^n-1}\right)^{\Phi_{q^n}}.\end{aligned}$$

Taking logarithms of both sides gives us

$$\log\left(\prod_{|\mathfrak{p}| \leq q^N} \left(1 - \frac{1}{|\mathfrak{p}|}\right)^{-1}\right) = \sum_{n=1}^{N} \Phi_{q^n} \log\left(\frac{q^n}{q^n-1}\right).$$

It suffices now to bound the right hand side of the above equality which we recognize as the left hand side of the equality in Theorem 3.12.

Lemma 3.16, Lemma 3.18 and Lemma 3.19 together yield:

$$\begin{aligned}\sum_{n=1}^{N} \Phi_{q^n} \log\left(\frac{q^n}{q^n-1}\right) - S_0(N) + S_1(N) + S_3(N) + \log\left(\frac{q}{q-1}\right)& \\ \leq \frac{8}{Nq^{\frac{N}{2}}} + \frac{12g}{Nq^{\frac{3N}{4}}} + \frac{1}{N} + \log N + \gamma + \log\left(\chi_{\mathscr{C}} \log q\right)& \\ + \frac{b}{(q^{\frac{1}{2}}-1)(N+1)(q^{\frac{N}{2}}-1)}.& \end{aligned} \tag{3.4.2}$$

Now Lemma 3.17 tells us that $S_2(N) - \log\left(\frac{q}{q-1}\right) \leq 0$ and adding this quantity to the left hand side of the inequality (3.4.2), taking into account the fact that $-S_0(N) + S_1(N) + S_2(N) + S_3(N) = 0$, we establish that:

$$\begin{aligned}\sum_{n=1}^{N} \Phi_{q^n} \log\left(\frac{q^n}{q^n-1}\right) \leq \frac{8}{Nq^{\frac{N}{2}}} + \frac{12g}{Nq^{\frac{3N}{4}}} + \frac{1}{N} + \log N + \gamma + \log\left(\chi_{\mathscr{C}} \log q\right)& \\ + \frac{b}{(q^{\frac{1}{2}}-1)(N+1)(q^{\frac{N}{2}}-1)}.& \end{aligned} \tag{3.4.3}$$

From Lemma 3.14,

$$\log\left(\chi_{\mathscr{C}} \log q\right) = \log\left(\frac{h_{\mathbb{F}_q(\mathscr{C})}}{q^g(1-\frac{1}{q})}\right)$$

and then the inequality (3.4.3) becomes, after rearranging:

$$\begin{aligned}\sum_{n=1}^{N} \Phi_{q^n} \log\left(\frac{q^n}{q^n-1}\right) \leq \log(Nh_{\mathbb{F}_q(\mathscr{C})}) + \gamma - \log\left(1-\frac{1}{q}\right)& \\ + \frac{1}{N} + \frac{8}{Nq^{\frac{N}{2}}} + \frac{12g}{Nq^{\frac{3N}{4}}}& \\ + \frac{b}{(q^{\frac{1}{2}}-1)(N+1)(q^{\frac{N}{2}}-1)} - g\log q.& \end{aligned} \tag{3.4.4}$$

Since $\frac{1}{N} \leq 1, q^{\frac{1}{2}} - 1 \geq 0.414 \geq \frac{4}{10}, q^{\frac{N}{2}} \leq q^{\frac{3N}{4}}$ and $-\log\left(1-\frac{1}{q}\right) \leq \log 2$ for $q \geq 2$, we have

$$\begin{aligned}\sum_{n=1}^{N}\Phi_{q^n}\log\left(\frac{q^n}{q^n-1}\right) &\leq \log(Nh_{\mathbb{F}_q(\mathscr{C})})+\gamma+\log 2+1\\ &+\frac{(8+12g)}{Nq^{\frac{N}{2}}}+\frac{10b}{4(N+1)(q^{\frac{N}{2}}-1)}\\ &-g\log q. \qquad (3.4.5)\end{aligned}$$

If the genus $g=0$ then $b=1$ and then for $N\geq 1$,

$$\begin{aligned}\sum_{n=1}^{N}\Phi_{q^n}\log\left(\frac{q^n}{q^n-1}\right) &\leq \log(Nh_{\mathbb{F}_q(\mathscr{C})})+\gamma+\log 2+1\\ &+\frac{8}{Nq^{\frac{N}{2}}}+\frac{10}{4(N+1)(q^{\frac{N}{2}}-1)}\\ &\leq \log(Nh_{\mathbb{F}_q(\mathscr{C})})+\gamma+\log 2+2\\ &\leq \log(Nh_{\mathbb{F}_q(\mathscr{C})})+4 \qquad (3.4.6)\end{aligned}$$

keeping in mind that $\log 2\leq 0.7$.

Assume now that the genus $g\geq 1$, then $b=g$. In view of the inequality (3.4.5) it is sufficient to find a value $N_{q,g}$ such that for $N\geq N_{q,g}$,

$$\frac{(8+12g)}{Nq^{\frac{N}{2}}}+\frac{10g}{4(N+1)(q^{\frac{N}{2}}-1)}-g\log q\leq 0$$

and since $g\geq 0, 8+12g\leq 20g$ it suffices to find $N_{q,g}$ sucht that for $N\geq N_{q,g}$,

$$\frac{20}{Nq^{\frac{N}{2}}}+\frac{10}{4(N+1)(q^{\frac{N}{2}}-1)}-\log q\leq 0.$$

At this stage one can see that we may choose an integer $N_{q,g}$ that doesn't actually depend on g.

For $N\geq 6$ and $q\geq 2$ we have $Nq^{\frac{N}{2}}\leq (N+1)(q^{\frac{N}{2}}-1)$, which implies

$$\frac{20}{Nq^{\frac{N}{2}}}+\frac{10}{4(N+1)(q^{\frac{N}{2}}-1)}\leq\frac{20}{Nq^{\frac{N}{2}}}+\frac{10}{4Nq^{\frac{N}{2}}}=\frac{\frac{90}{4}}{Nq^{\frac{N}{2}}}.$$

It now remains to find an $N_{q,g}$ such that for $N\geq N_{q,g}$

$$\frac{\frac{90}{4}}{Nq^{\frac{N}{2}}}-\log q\leq 0 \qquad (3.4.7)$$

and this is equivalent to

$$Nq^{\frac{N}{2}} \log q - 22.5 \geq 0.$$

Lastly since $q \geq 2$, we can reduce the problem to finding $N_{q,g}$ such that for $N \geq N_{q,g}$,

$$N2^{\frac{N}{2}} \log 2 - 22.5 \geq 0.$$

It is clear that $N_{q,g}$ can be chosen to be independent from q as well.

One can easily check that it suffices to take $N_{q,g} = 6$.

Therefore, for $N \geq 6$, inequality (3.4.5) implies:

$$\begin{aligned}\sum_{n=1}^{N} \Phi_{q^n} \log\left(\frac{q^n}{q^n - 1}\right) &\leq \log(Nh_{\mathbb{F}_q(\mathscr{C})}) + \gamma + \log 2 + 1 \\ &\leq \log(Nh_{\mathbb{F}_q(\mathscr{C})}) + 3. \qquad (3.4.8)\end{aligned}$$

Combined with the inequality (3.4.6), this gives the result. □

3.4.2 Prime number theorem for polynomials

In this subsection we make a brief digression to $\mathbb{F}_q[T]$. It is necessary to do so since we want a lower bound on the Euler function with a constant multiple that does not depend on the CM-field of φ. This is explained in Remark 3.25 at the end of this subsection.

Let $\pi(x)$ be the number of primes less than or equal to x for any real number x. The prime number theorem gives an asymptotic formula for $\pi(x)$, namely $\pi(x) \backsim \dfrac{x}{\log x}$. Consequently, if p_n is the n-th prime number then $p_n \backsim \dfrac{n}{\log n}$ as $n \to \infty$. The analogue of the prime number theorem for $\mathbb{F}_q[T]$ gives an asymptotic formula for the number of primes of degree n. Recall that the the finite primes of $\mathbb{F}_q[T]$ are in one-to-one correspondence with the monic irreducible polynomials, the notion of degree then coincides with the usual degree of a polynomial.

Theorem 3.21 (Prime number theorem for polynomials)**.** *Let $a_n := \#\{P \in \mathbb{F}_q[T]/P \text{ is prime and } \deg(P) = n\}$ for $n \in \mathbb{N}$. Then we have:*

$$a_n = \frac{q^n}{n} + \mathscr{O}(\frac{q^{\frac{n}{2}}}{n}).$$

The proof of Theorem 3.21 is simple compared to that of its classical counterpart. We give a complete proof for the sake of completeness. Most of the material in this subsection can be found in chapter 2 of [Ros02].

The zeta function associated to $\mathbb{F}_q[T]$ is:

$$\zeta_{\mathbb{F}_q[T]}(s) := \sum_{\substack{f \in \mathbb{F}_q[T] \\ f \text{ monic}}} \frac{1}{|f|^s}$$

where $|f| = \#(\mathbb{F}_q[T]/f\mathbb{F}_q[T]) = q^{\deg(f)}$ and s a complex number with $\Re(s) > 1$ (we will see shortly that the zeta function is well defined for these values of s). In the polynomial case the zeta function has a particularly simple form. We easily see that there are exactly q^d monic polymomials of degree d in $\mathbb{F}_q[T]$, so by taking the limit when $d \to \infty$ of the partial summation

$$\sum_{\substack{\deg(f) \leq d \\ f \text{ monic}}} \frac{1}{|f|^s} = 1 + q^{1-s} + (q^{1-s})^2 + \cdots + (q^{1-s})^d$$

which converges for $\Re(s) > 1$, we get:

$$\zeta_{\mathbb{F}_q[T]}(s) = \frac{1}{1 - q^{1-s}}. \tag{3.4.9}$$

This rational fraction extends $\zeta_{\mathbb{F}_q[T]}(s)$ meromorphically to the whole complex plane with a unique pole at $s = 1$ which is simple. Now, since each polynomial in $\mathbb{F}_q[T]$ decomposes uniquely into a product of irreducibles, we can write $\zeta_{\mathbb{F}_q[T]}(s)$ as an Euler product for $\Re(s) > 1$,

$$\zeta_{\mathbb{F}_q[T]}(s) = \prod_{\substack{P \text{ irreducible} \\ P \text{ monic}}} \left(1 - \frac{1}{|P|^s}\right)^{-1}. \tag{3.4.10}$$

We next recall the Möbius function defined for $n \in \mathbb{N}$ as:

$$\mu(n) := \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \text{ is not square} - \text{free} \\ (-1)^t & \text{if } n \text{ is a product of } t \text{ distinct primes.} \end{cases}$$

It is well known that μ is a multiplicative function and most importantly we have the following inversion formula.

Proposition 3.22 (Möbius inversion formula). *Let f and g be two arithmetical functions satisfying*

$$\sum_{d|n} f(d) = g(n),$$

then

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d).$$

We can now proceed to prove the prime number theorem.

Proof of Theorem 3.21. Since there are exactly a_d monic irreducibles of degree d, equations (3.4.9) and (3.4.10) gives

$$\frac{1}{1-qu} = \prod_{d=1}^{\infty}\left(1 - \frac{1}{u^d}\right)^{-a_d}$$

for $\Re(s) > 1$ and $u = q^{-s}$. Now we take the logarithmic derivatives with respect to u to get

$$\frac{q}{1-qu} = \sum_{d=1}^{\infty} \frac{da_d u^{d-1}}{1-u^d}.$$

Multiplying by u on both sides and expanding into power series (which can be done since $|qu|, |u| < 1$ whenever $\Re(s) > 1$) gives

$$\sum_{n=1}^{\infty}(qu)^n = \sum_{d=1}^{\infty} da_d \left(\sum_{n=1}^{\infty} u^{dn}\right) = \sum_{n=1}^{\infty}\left(\sum_{d|n} da_d\right) u^n.$$

Hence $q^n = \sum_{d|n} da_d$ for all $n \geq 1$. Therefore, by Proposition 3.22 we get a formula for a_n:

$$a_n = \frac{1}{n}\sum_{d|n}\mu(d) q^{\frac{n}{d}}.$$

We are now going to bound $\left|a_n - \frac{q^n}{n}\right|$ using the above formula. Write $n = \prod_{i=1}^{t} p_i^{\alpha_i}$ where the p_i's are t distinct primes and let $m = \max\{\frac{n}{d}, d \geq 2, d|n\}$. We have

$$\left|a_n - \frac{q^n}{n}\right| = \left|\frac{1}{n}\sum_{d|n, d>1} \mu(d) q^{\frac{n}{d}}\right|$$

$$\begin{aligned}
&\leq \frac{1}{n} \sum_{d|n, d>1} |\mu(d)| q^{\frac{n}{d}} \\
&\leq \frac{q^m}{n} + \frac{1}{n} \sum_{d|n, d>\frac{n}{m}} |\mu(d)| q^{\frac{n}{d}} \\
&\leq \frac{q^{\frac{n}{2}}}{n} + \frac{1}{n} \sum_{d|n, d>\frac{n}{m}} |\mu(d)| q^{\frac{n}{d}}.
\end{aligned}$$

Each term in the summation $\frac{1}{n} \sum_{d|n, d>\frac{n}{m}} |\mu(d)| q^{\frac{n}{d}}$ is less than or equal to $\frac{q^{\frac{n}{3}}}{n}$ and there are exactly $2^t - 2$ non-zero summands by definition of μ. Since $2^t - 2 \leq n$, we get $\frac{1}{n} \sum_{d|n, d>\frac{n}{m}} |\mu(d)| q^{\frac{n}{d}} \leq q^{\frac{n}{3}}$. Therefore

$$\begin{aligned}
\left| a_n - \frac{q^n}{n} \right| &\leq \frac{q^{\frac{n}{2}}}{n} + q^{\frac{n}{3}} \\
&= \frac{q^{\frac{n}{2}}}{n} \left(1 + \frac{n}{q^{\frac{n}{6}}} \right) \\
&\leq \frac{q^{\frac{n}{2}}}{n} \left(1 + \frac{n}{3^{\frac{n}{6}}} \right)
\end{aligned}$$

which completes our proof since $1 + \frac{n}{3^{\frac{n}{6}}}$ is clearly bounded above. □

The last inequality in the proof of Theorem 3.21 gives the following lower bound on a_n

Proposition 3.23. *Let $q \geq 3$ and $n \geq 4$, then we have the inequality:*

$$a_n \geq \frac{q^n}{9n}.$$

Proof. From the inequality $\left| a_n - \frac{q^n}{n} \right| \leq \frac{q^{\frac{n}{2}}}{n} + q^{\frac{n}{3}} = q^{\frac{n}{2}} \left(\frac{1}{n} + \frac{1}{q^{\frac{n}{6}}} \right)$, we can easily see that $\left| a_n - \frac{q^n}{n} \right| \leq 2q^{\frac{n}{2}}$. Therefore, since $q \geq 3$

$$a_n \geq \frac{q^n}{n} - 2q^{\frac{n}{2}} = \frac{q^n}{n} \left(1 - \frac{2n}{q^{\frac{n}{2}}} \right) \geq \frac{q^n}{n} \left(1 - \frac{2n}{3^{\frac{n}{2}}} \right).$$

Now, for $n \geq 4$ the term $\left(1 - \frac{2n}{3^{\frac{n}{2}}} \right)$ is positive and increasing in n. This implies that it is bounded below by $\frac{1}{9}$ which completes the proof. □

The main purpose of this subsection is to establish the following inequality which we will use subsequently when bounding the Euler totient function in the next subsection.

Corollary 3.24. *Let $q \geq 3$ and $N \geq 4$. Then there exists a constant $C > 0$ depending only on q, namely $C = q^8$, such that:*

$$\prod_{|P| \leq C \log N} |P| \geq N$$

where the product runs through the finite primes of $\mathbb{F}_q[T]$.

Proof. Let $C > 0$ be an arbitrary positive constant for now. Later on we will choose an appropriate value of C. Recall that $|P| = q^{\deg P}$. Taking the base q logarithm of $\prod_{|P| \leq C \log N} |P|$ gives

$$\begin{aligned}
\log_q \left(\prod_{|P| \leq C \log N} |P| \right) &= \sum_{|P| \leq C \log N} \log_q(|P|) \\
&= \sum_{|P| \leq C \log N} \deg P \\
&= \sum_{\deg P \leq \log_q(C \log N)} \deg P \\
&\geq \sum_{\frac{1}{2} \log_q(C \log N) \leq \deg P \leq \log_q(C \log N)} \deg P \\
&= \sum_{m \leq \deg P \leq M} \deg(P) \\
&\geq m \left(\sum_{m \leq \deg P \leq M} 1 \right) \qquad (3.4.11)
\end{aligned}$$

where $m = \left\lceil \frac{1}{2} \log_q(C \log N) \right\rceil = \frac{1}{2} \log_q(C \log N) + c_m$ and $M = \left\lfloor \log_q(C \log N) \right\rfloor = \log_q(C \log N) + c_M$ for some constants $0 \leq c_m < 1$ and $-1 < c_M \leq 0$. We now bound the sum $\left(\sum_{m \leq \deg P \leq M} 1 \right)$ from below using Proposition 3.23. However, for us to be able to use Proposition 3.23 we need to make sure that $m \geq 4$ by choosing C large enough. This amounts to choosing C in such a way that $N \geq e^{\frac{q^8}{C}}$. Since $N \geq 4$, it is enough to take $C = q^8$. Therefore, the following holds

$$\sum_{m \leq \deg P \leq M} 1 = \sum_{k=m}^{M} a_k = \sum_{j=0}^{M-m} a_{j+m} \geq \frac{1}{9} \sum_{j=0}^{M-m} \frac{q^{j+m}}{j+m} = \frac{q^m}{9m} \left(\sum_{j=0}^{M-m} \frac{q^j}{1 + \frac{j}{m}} \right).$$

As $1 \leq 1 + \frac{j}{m} \leq 1 + \frac{M-m}{m} = \frac{M}{m} \leq 2$ we deduce that

$$\sum_{m \leq \deg P \leq M} 1 \geq \frac{q^m}{18m} \left(\sum_{j=0}^{M-m} q^j \right) = \frac{q^m}{18m} \left(\frac{q^{M-m+1}-1}{q-1} \right).$$

Therefore, together with (3.4.11), we have the following inequalities

$$\begin{aligned}
\log_q \left(\prod_{|P| \leq C \log N} |P| \right) \geq & \frac{q^m}{18} \left(\frac{q^{M-m+1}-1}{q-1} \right) \\
\geq & \frac{q^m}{18q} \left(q^{M-m+1} - 1 \right) \\
\geq & \frac{q^m}{18q} \left(q^{M-m+1} - 1 \right) \\
\geq & \frac{q^m}{18q} \left(q^{M-m} \right) \\
= & \frac{q^M}{18q} \\
= & \frac{1}{18q} (C \log N) q^{C_M} \\
\geq & \frac{1}{18q^2} (C \log N) \quad \text{since } \frac{1}{q} < q^{c_M} \leq 1 \\
= & \frac{q^8 \log q}{18q^2} \log_q N \quad \text{since } C = q^8 \\
\geq & \log_q N.
\end{aligned}$$

Hence, it suffices to take the q^{th} power of both sides. □

Remark 3.25. The prime number theorem can be generalized to arbitrary function fields, not just the rational function field $\mathbb{F}_q(T)$, and Corollary 3.24 still holds. However, we need to descend to $\mathbb{F}_q(T)$ otherwise the eventual constant C of Conjecture 5 will depend on the genus of the CM-field of our fixed Drinfeld module φ which weakens the uniformity of our result.

3.4.3 Uniform bound for $\Phi_{\mathcal{O}_K}(\mathfrak{a})$

To prove our main theorem we need a uniform lower bound for $\Phi_{\mathcal{O}_K}(\mathfrak{a})$ as a function of $|\mathfrak{a}|$, $\log\log|\mathfrak{a}|$ and h_K.

Lemma 3.26. *Let K/F be a finite extension with ring of integers $\mathcal{O}_K$ and $N \geq 1$ an integer. If $\mathfrak{a}$ is an integral ideal of $\mathcal{O}_K$ such that $\prod\limits_{|\mathfrak{p}|\leq N} |\mathfrak{p}| \geq |\mathfrak{a}|$ then $\dfrac{\Phi_{\mathcal{O}_K}(\mathfrak{a})}{|\mathfrak{a}|} \geq \prod\limits_{|\mathfrak{p}|\leq N} \left(1 - \dfrac{1}{|\mathfrak{p}|}\right)$ where the products run through the primes of K.*

Proof. Let $P_{\mathfrak{a}} = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_n\}$ be the set of distinct primes dividing $\mathfrak{a}$ and $P_N = \{\mathfrak{q}_1, \cdots, \mathfrak{q}_m\}$ be the set of distinct primes $\mathfrak{p}$ such that $|\mathfrak{p}| \leq N$. There are less distinct primes dividing $\mathfrak{a}$ than distinct primes of norm less than N, i.e. $n \leq m$, because $|\mathfrak{p}_1 \cdots \mathfrak{p}_n| = |\mathfrak{p}_1| \cdots |\mathfrak{p}_n| \leq |\mathfrak{a}| \leq \prod\limits_{|\mathfrak{p}|\leq N} |\mathfrak{p}|$. Indeed, if that is not the case, the product on the left would exceed $\prod\limits_{|\mathfrak{p}|\leq N} |\mathfrak{p}|$. For $x \geq 1$, $0 \leq 1 - \dfrac{1}{x} \leq 1$ and its an increasing function of x. Therefore,

$$\prod_{\mathfrak{p}\in P_{\mathfrak{a}}\setminus P_N} \left(1 - \frac{1}{|\mathfrak{p}|}\right) \geq \prod_{\mathfrak{p}\in P_N\setminus P_{\mathfrak{a}}} \left(1 - \frac{1}{|\mathfrak{p}|}\right)$$

because the product on the left hand side has less terms and each of its term is larger than any of the terms of the product on the right hand side. We conclude as follows

$$\begin{aligned}
\frac{\Phi_{\mathcal{O}_K}(\mathfrak{a})}{|\mathfrak{a}|} &= \prod_{\mathfrak{p}|\mathfrak{a}} \left(1 - \frac{1}{|\mathfrak{p}|}\right) = \prod_{\mathfrak{p}\in P_{\mathfrak{a}}} \left(1 - \frac{1}{|\mathfrak{p}|}\right) \\
&= \prod_{\mathfrak{p}\in P_{\mathfrak{a}}\cap P_N} \left(1 - \frac{1}{|\mathfrak{p}|}\right) \prod_{\mathfrak{p}\in P_{\mathfrak{a}}\setminus P_N} \left(1 - \frac{1}{|\mathfrak{p}|}\right) \\
&\geq \prod_{\mathfrak{p}\in P_{\mathfrak{a}}\cap P_N} \left(1 - \frac{1}{|\mathfrak{p}|}\right) \prod_{\mathfrak{p}\in P_N\setminus P_{\mathfrak{a}}} \left(1 - \frac{1}{|\mathfrak{p}|}\right) \\
&= \prod_{\mathfrak{p}\in P_N} \left(1 - \frac{1}{|\mathfrak{p}|}\right) \\
&= \prod_{|\mathfrak{p}|\leq N} \left(1 - \frac{1}{|\mathfrak{p}|}\right).
\end{aligned}$$

□

Lemma 3.27. *Let $N > 0$ be a positive integer and K/F a degree r extension. We have:*

$$\prod_{|\mathfrak{p}|_K\leq N} |\mathfrak{p}|_K \geq \prod_{|P|_F\leq N^{\frac{1}{r}}} |P|_F$$

where the product on the left hand side runs through the primes of K and the one on the right hand side through the primes of F.

Proof. Recall that if $\mathfrak{p}$ is a prime of K lying above the prime P of F then $|\mathfrak{p}|_K = |P|_F^{f_\mathfrak{p}}$ where $1 \leq f_\mathfrak{p} \leq r$ is the inertial degree of $\mathfrak{p}$ so that $|P|_F \leq |\mathfrak{p}|_K \leq |P|_F^r$. Therefore, if $|P|_F \leq N^{\frac{1}{r}}$ then $|\mathfrak{p}|_K \leq N$. To conclude, its enough to notice that if P and Q are two distinct primes of F and if $\mathfrak{p}$ (resp. $\mathfrak{q}$) lies above P (resp. Q) then $\mathfrak{p} \neq \mathfrak{q}$. □

We can now bound $\Phi_{\mathcal{O}_K}(\mathfrak{a})$ from below as follows.

Theorem 3.28. *Let $r \geq 1$, $q \geq 3$ where q is a power of a prime. Let F be a global function field over $\mathbb{F}_q$ of degree $d_F = [F : \mathbb{F}_q(T)]$. Then for any extension K/F of degree r and all non-zero ideals $\mathfrak{a} \subseteq \mathcal{O}_K$ such that $|\mathfrak{a}|_K \geq 4$, we have:*

$$\Phi_{\mathcal{O}_K}(\mathfrak{a}) \geq \frac{1}{18e^4 r d_F} \frac{|\mathfrak{a}|_K}{h_K \log\log|\mathfrak{a}|_K}.$$

Proof. Let K/F be a degree r extension of F and $\mathfrak{a} \subseteq \mathcal{O}_K$ a non-zero ideal. Now, for $|\mathfrak{a}|_K \geq 4$, Corollary 3.24 tells us that

$$\prod_{|P|_{\mathbb{F}_q[T]} \leq C \log|\mathfrak{a}|_K} |P|_{\mathbb{F}_q[T]} \geq |\mathfrak{a}|_K$$

where the product runs through the primes of $\mathbb{F}_q[T]$ and $C = q^8$.

On the other hand Lemma 3.27 implies

$$\prod_{|\mathfrak{p}|_K \leq (C \log|\mathfrak{a}|_K)^{rd_F}} |\mathfrak{p}|_K \geq \prod_{|P|_{\mathbb{F}_q[T]} \leq C \log|\mathfrak{a}|_K} |P|_{\mathbb{F}_q[T]} \geq |\mathfrak{a}|_K.$$

Therefore, by Lemma 3.26 we have:

$$\frac{\Phi_{\mathcal{O}_K}(\mathfrak{a})}{|\mathfrak{a}|_K} \geq \prod_{|\mathfrak{p}|_K \leq (C \log|\mathfrak{a}|_K)^{rd_F}} \left(1 - \frac{1}{|\mathfrak{p}|_K}\right).$$

From Theorem 3.20 we get

$$\begin{aligned}\prod_{|\mathfrak{p}|_K \leq (C \log|\mathfrak{a}|_K)^{rd_F}} \left(1 - \frac{1}{|\mathfrak{p}|_K}\right) &\geq \frac{1}{e^4 h_K \log_q (C\log|\mathfrak{a}|_K)^{rd_F}} \\ &= \frac{\log q}{e^4 r d_F} \frac{1}{h_K \log(C\log|\mathfrak{a}|_K)}. \end{aligned} \tag{3.4.12}$$

Now, for $|\mathfrak{a}|_K \geq 3$ and $C = q^8$ we have

$$\log(C\log|\mathfrak{a}|_K) = \left(1 + \frac{8\log q}{\log\log|\mathfrak{a}_K|}\right) \log\log|\mathfrak{a}_K|$$

$$\begin{aligned} &\leq \left(1 + \frac{8\log q}{\log\log 3}\right) \log\log |\mathfrak{a}_K| \\ &\leq 18 \log q. \end{aligned}$$

Therefore, for $|\mathfrak{a}|_K \geq 3$ and equation (3.4.12)

$$\frac{\Phi_{\mathscr{O}_K}(\mathfrak{a})}{|\mathfrak{a}|_K} \geq \frac{1}{18e^4 r d_F} \frac{1}{h_K \log\log |\mathfrak{a}|_K}$$

and the result follows. □

3.5 Proof of the main result and the case r=1

In this last section we deduce a weaker version of Conjecture 5. Recall that F is a global function field over $\mathbb{F}_q$ such that $[F : \mathbb{F}_q(T)] = d_F$ and that we fixed a prime at infinity ∞ of degree d_∞. The following lemma is a particular case of [Bre10] Lemma 2.5, we compute explicitly the constants here.

Lemma 3.29. *Suppose $d, h \geq 3$ are integers. If $d \geq C\dfrac{h}{\log\log h}$ for some constant $C > 0$ then there exists $C' > 0$ depending on C such that $h \leq C' \, d \log\log d$.*

Proof. For $h \geq 3$ one can easily check that $h^{\frac{1}{2}} \geq \log\log h$. Therefore $d \geq C\dfrac{h}{h^{\frac{1}{2}}} = Ch^{\frac{1}{2}}$. We consider the following cases:

<u>Case 1</u>: $C \geq 1$.
If $C \geq 1$ then $d \geq h^{\frac{1}{2}}$ and we get:

$$\begin{aligned} \log\log h &\leq \log\log d + \log 2 \\ &= \left(1 + \frac{\log 2}{\log\log d}\right) \log\log d \\ &\leq \left(1 + \frac{\log 2}{\log\log 3}\right) \log\log d \quad \text{since } d \geq 3 \\ &\leq 9 \log\log d. \end{aligned}$$

Hence, if $d \geq C\dfrac{h}{\log\log h}$ then $h \leq \dfrac{9}{C} d \log\log d$.

<u>Case 2</u>: $C < 1$.
If $C < 1$ then $\dfrac{1}{C} > 1$ so that $\log\dfrac{d}{C} \leq \dfrac{1}{C}\log d$ for all $d \geq 3$. Furthermore, since $d \geq Ch^{\frac{1}{2}}$ we have:

$$\log\log h \leq \log\log\frac{d}{C} + \log 2$$

$$
\begin{aligned}
&\leq \log\left(\frac{1}{C}\log d\right) + \log 2 \\
&= \log\log d + \log\frac{2}{C} \\
&= \left(1 + \frac{\log\frac{2}{C}}{\log\log d}\right)\log\log d \\
&\leq \left(1 + \frac{\log\frac{2}{C}}{\log\log 3}\right)\log\log d.
\end{aligned}
$$

Therefore, $d \geq C\dfrac{h}{\log\log h}$ implies $h \leq \left(\dfrac{\log\log 3 + \log\frac{2}{C}}{C\log\log 3}\right) d\log\log d$.

Now it suffices to take

$$
C' = \begin{cases} \dfrac{9}{C} & \text{if } C \geq 1 \\ \left(\dfrac{\log\log 3 + \log\frac{2}{C}}{C\log\log 3}\right) & \text{if } C < 1. \end{cases}
$$

□

Lemma 3.30. *Let K be a global function field over $\mathbb{F}_q$, ∞' a fixed prime of K and A the ring of elements of K regular away from ∞'. Then $h_A = h_K \deg\infty'$ where $d_{\infty'}$ is the degree of ∞' over $\mathbb{F}_q$.*

Proof. This is Corollary 4.1.3. in [Gos98]. Essentially, one can show that the following sequence is exact

$$0 \to \mathscr{D}_K^0/\mathscr{P}_K \xrightarrow{\pi} \mathbf{Pic}(A) \xrightarrow{\deg} \mathbb{Z}/d_{\infty'}\mathbb{Z} \to 0$$

where $\mathscr{D}_K^0$ is the group of divisors of K of degree 0, $\mathscr{P}_K$ the group of principal divisors of K and $\mathbf{Pic}(A)$ the Picard group of A as a Dedekind domain. The map π sends an element D to the fractional ideal associated to the non-infinite (i.e excluding the term with ∞') part of D. One can directly conclude since $|\mathscr{D}_K^0/\mathscr{P}_K| =: h_K$ and $|\mathbf{Pic}(A)| =: h_A$. □

We can now prove our main theorem.

Theorem 3.31. *Let $r \geq 1$ and $q \geq 3$ be integers where q is a power of a prime. There exists an absolute constant $C > 0$ (depending only on r, D_A, d_F, d_∞ and q) such that, for any extension L/F of degree $d \geq 3$ and any Drinfeld A-module $\varphi : A \to L\{\tau\}$ defined over L of rank r with complex multiplication by a degree r purely imaginary extension K/F satisfying* $\mathrm{End}(\varphi) = \mathcal{O}_K$*:*

$$\#\varphi(L)_{\mathrm{tors}} \leq Cd \log\log d.$$

Proof. Let $[L : F] = d$ and $\varphi : A \to L\{\tau\}$ be an $\mathcal{O}_K$-CM Drinfeld A-module of rank r. Let $\psi : \mathcal{O}_K \to LK\{\tau\}$ be its rank one extension to $\mathcal{O}_K$. By Proposition 3.1 it is enough to bound $\#\psi(L)_{\mathrm{tors}}$. We proceed by first bounding $\#\psi(LK)_{\mathrm{tors}}$, this is enough in view of Lemma 3.29 and the fact that $[LK : K]$ is uniformly bounded in terms of A and r. According to Theorem 3.5, there exists a non-zero ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ such that $\psi(LK)_{\mathrm{tors}} \simeq \mathcal{O}_K/\mathfrak{a}$, i.e. $\#\psi(LK)_{\mathrm{tors}} = |\mathfrak{a}|$. From Theorem 3.11 we have

$$d \geq \frac{h_{\mathcal{O}_K}\Phi_{\mathcal{O}_K}(\mathfrak{a})}{r(q-1)(q^{rd_\infty D_A}-1)}$$

which implies

$$|\mathfrak{a}| \leq \frac{r(q-1)(q^{rd_\infty D_A}-1)d}{h_{\mathcal{O}_K}} \frac{|\mathfrak{a}|}{\Phi_{\mathcal{O}_K}(\mathfrak{a})}.$$

If $\#\psi(LK)_{\mathrm{tors}} = |\mathfrak{a}| < 4$ then $\#\varphi(L)_{\mathrm{tors}} < 4$ and the theorem is true for $d \geq 3$.

Otherwise, if $|\mathfrak{a}| \geq 4$, we can use Theorem 3.28 to get

$$|\mathfrak{a}| \leq 18e^4 d_F r^2 (q-1)(q^{rd_\infty D_A}-1)\frac{h_K}{h_{\mathcal{O}_K}} d \log\log|\mathfrak{a}|.$$

Since K is a purely imaginary extension of F there is exactly one prime ∞' of K, of degree ∞', above ∞. Furthermore, from Lemma 3.30 we have $\dfrac{h_K}{h_{\mathcal{O}_K}} = d_{\infty'} \leq rd_\infty$. Hence,

$$|\mathfrak{a}| \leq C_0 d \log\log|\mathfrak{a}|,$$

where $C_0 = 18e^4 d_F d_\infty r^3 (q-1)(q^{rd_\infty D_A}-1)$.

Now, since $d \geq \dfrac{1}{C_0}\dfrac{|\mathfrak{a}|}{\log\log|\mathfrak{a}|}$ and clearly $\dfrac{1}{C_0} < 1$ we can deduce from Lemma 3.29:

$$\#\varphi(L)_{\mathrm{tors}} = \#\psi(L)_{\mathrm{tors}} \leq \#\psi(LK)_{\mathrm{tors}} = |\mathfrak{a}| \leq Cd\log\log d$$

with $C = C_0\left(1 + \dfrac{\log(2C_0)}{\log\log 3}\right)$. □

Remark 3.32.

1. The constant C is not optimal and can be slightly improved at the cost of having a more complicated looking constant.
2. The parameter D_A can actually be replaced by $g_F + 1$ where g_F is the genus of F because $D_A \leq g_F + 1$.

Let us look closely at Remark 3.32 part(2). We first recall the *Rieman-Roch Theorem*, the notion of *gap number* of a prime and the *Weierstrass Gap Theorem*. A good reference is [Sti09] chapter 1. Let $A \in \mathscr{D}_F$ be a divisor of F, the Riemann-Roch space associated to A is the $\mathbb{F}_q$-vector space

$$\mathscr{L}(A) := \{x \in F | (x) \geq -A\} \cup \{0\}$$

where $(x) := \sum_{P \in \mathbb{P}_F} v_P(x)P$ is the principal divisor associated to $x \in F$. The dimension of $\mathscr{L}(A)$ is denoted $\ell(A)$.

Theorem 3.33 (Riemann-Roch Theorem, [Sti09] Theorem1.5.15)**.** *Let W be a canonical divisor of F. Then for each divisor A of F,*

$$\ell(A) = \deg A + 1 - g_F + \ell(W - A).$$

We do not need to know what a canonical divisor is but just the fact that $\ell(W - A) \geq 0$.

For $x \in F$, $(x)_\infty$ is the pole divisor of x.

Definition 3.34. *Let $P \in \mathbb{P}_F$. An integer $n \geq 0$ is called a* pole number *of P if there exists $x \in F$ such that $(x)_\infty = nP$. Otherwise n is called a* gap number *of P.*

The number n is a pole number if there is an element $x \in F$ which has exactly one pole, this pole being of order n at P.

Theorem 3.35 (Weierstrass Gap Theorem, [Sti09] Theorem 1.6.8)**.** *Suppose that F has genus g_F and that P is a prime of degree one. Then there are exactly g_F gap numbers $i_1 < \cdots < i_{g_F}$ where $i_1 = 1$ and $i_{g_F} \leq 2g_F - 1$.*

We prove the claim in Remark 3.32 part(2).

Proposition 3.36. *Let F be a function field with full constant field $\mathbb{F}_q$. Let ∞ be a prime of F of degree d_∞ and A the ring of elements of F regular away from ∞. Then*

$$D_A = \inf\{-v_\infty(a), a \in A \setminus \mathbb{F}_q \text{ and } v_\infty(a) < 0\} \leq g_F + 1.$$

Proof. Notice that if $n \geq 0$ is a pole number of ∞ then there exists $x \in F$ with $(x)_\infty = n\infty$, which means that x is regular away from ∞ so that $x \in A$. Therefore D_A is the smallest pole number of ∞. If $d_\infty = 1$ then, by the Weierstrass Gap Theorem (Theorem 3.35), there are exactly g_F gap numbers between 1 and $2g_F - 1$. Hence the smallest pole number is less than $g_F + 1$, i.e. $D_A \leq g_F + 1$. If $d_\infty > 1$, then by the Riemann-Roch (Theorem 3.33) we have $\ell(g_F\infty) \geq g_F d_\infty + 1 - g_F > 1$. This tells us that there exists an element $a \in A \setminus \mathbb{F}_q$ such that $(a)_\infty \geq -g_F\infty$, that is $D_A \leq g_F$. □

We now turn to the special case $r = 1$. Our method yields a uniform boundedness for Drinfeld A-modules of rank one and we recover Theorem 8 of [Poo97] with an explicit constant. Let L/F be a degree $d \geq 3$ extension and $\varphi : A \to L\{\tau\}$ a Drinfeld A-module of rank one and of generic characteristic. The notion of complex multiplication becomes trivial in this case and any such module has CM with $\mathrm{End}(\varphi) = A$. Indeed, $\mathrm{End}(\varphi)$ is an order in F and it contains the maximal order A.

Theorem 3.37 ([Poo97] Theorem 8.). *Let F be a global function field over $\mathbb{F}_q$ of genus g_F and A the ring of elements of F regular away from a fixed prime ∞ of degree d_∞. There exists a constant $C > 0$ depending only on q, d_F, g_F and d_∞ such that for any extension L/F of degree d and any Drinfeld A-module φ of rank one defined over L:*

$$\#\varphi(L)_{\mathrm{tors}} \leq Cd \log\log d.$$

Proof. We essentially follow through the proof of Theorem 3.31 and adjust with all the simplifications. Let $[L : F] = d$ and $\varphi : A \to L\{\tau\}$ be a rank one Drinfeld A-module. There exists a non-zero ideal $\mathfrak{a} \subseteq A$ such that $\varphi(L)_{\mathrm{tors}} \simeq A/\mathfrak{a}$. Since $r = 1$, Theorem 3.11 implies

$$d \geq \frac{h_A \Phi_A(\mathfrak{a})}{(q-1)(q^{d_\infty D_A} - 1)}$$

so that

$$|\mathfrak{a}| \leq (q-1)(q^{d_\infty D_A} - 1)d\frac{|\mathfrak{a}|}{h_A \Phi_A(\mathfrak{a})}.$$

If $\#\varphi(L)_{\mathrm{tors}} = |\mathfrak{a}| < 4$ then the theorem is true for $d \geq 3$. Now for $|\mathfrak{a}| \geq 4$, we have by Theorem 3.28

$$|\mathfrak{a}| \leq 18e^4 d_F (q-1)(q^{d_\infty D_A} - 1)\frac{h_F}{h_A} d \log\log|\mathfrak{a}|,$$

and since $\dfrac{h_F}{h_A} \leq d_\infty$ we get

$$|\mathfrak{a}| \leq 18e^4 d_F d_\infty (q-1)(q^{d_\infty D_A} - 1)d \log\log|\mathfrak{a}|.$$

Finally Lemma 3.29 allows to conclude

$$\#\varphi(L)_{\mathrm{tors}} \leq Cd \log\log d.$$

From Proposition 3.36 we can choose $C = C'\left(1 + \dfrac{\log(2C')}{\log\log 3}\right)$ with $C' = 18e^4 d_F d_\infty (q-1)(q^{d_\infty(g_F+1)} - 1)$. □

Remark 3.38. In the rank one case, since the CM-field is F itself, we do not need to descend to $\mathbb{F}_q(T)$ as in section 3.4.2 since we can allow our constant to depend on F. We can directly use the prime number theorem for general function fields to make the necessary estimations.

We can easily deduce the following corollary with an integer constant.

Corollary 3.39. *Let F be the rational function field $\mathbb{F}_q[T]$ and ∞ be the prime associated to the $\frac{1}{T}$-adic absolute value. Then, for any extension L/F of degree d and any Drinfeld $\mathbb{F}_q[T]$-module φ of rank one defined over L:*

$$\#\varphi(L)_{\mathrm{tors}} \leq 23330916(q-1)^3 d \log\log d.$$

Proof. We have $d_\infty = d_F = 1$ and $g_F = 0$. We get the constant by bounding $C'\left(1 + \dfrac{\log(2C')}{\log\log 3}\right)$ from above where $C' = 18e^4(q-1)^2$. □

3.6 Uniform torsion bound for CM Drinfeld $\mathbb{F}_q[T]$-modules of rank 2

Throughout this section, unless explicitely stated, we restrict to the case $r = 2$, $F = \mathbb{F}_q(T)$ and $A = \mathbb{F}_q[T]$. The place at infinity corresponds to the $\frac{1}{T}$-adic absolute value and we denote by F_∞ the completion of $\mathbb{F}_q(T)$ at this place. We fix an algebraic closure $\overline{\mathbb{F}_q[T]} \subseteq \mathbb{C}_\infty$. We prove Conjecture 5 for rank 2 Drinfeld $\mathbb{F}_q[T]$-modules with complex multiplication. The main idea is to prove an analogue of the Isogeny Torsion Theorem for CM-elliptic curves to reduce to the case of maximal order and combine with Theorem 3.31.

Let E be an $\mathcal{O}$-CM elliptic curve defined over a number field L, where $\mathcal{O}$ is the order of conductor $\mathfrak{f}$ in an imaginary quadratic field K, and $\mathfrak{f}'$ be a positive integer dividing $\mathfrak{f}$. Then, according to [BP16, Proposition 2.2], there exists an $\mathcal{O}'$-CM elliptic curve $E_{\mathfrak{f}'}$, where $\mathcal{O}'$ is the order of conductor $\mathfrak{f}'$ in K, and an L-rational cyclic isogeny $\iota_{\mathfrak{f}'} : E \to E_{\mathfrak{f}'}$ of degree $\frac{\mathfrak{f}}{\mathfrak{f}'}$.

Theorem 3.40 (Isogeny Torsion Theorem, [BC18] Theorem 1.7)**.** *Let $\mathcal{O}$ be an order in an imaginary quadratic number field K, of conductor $\mathfrak{f}$ and let $\mathfrak{f}'$ be a positive integer dividing $\mathfrak{f}$. Let $L \supset K$ be a number field, and let $E_{|L}$ be an $\mathcal{O}$-CM elliptic curve. Let $\iota_{\mathfrak{f}'} : E \to E_{\mathfrak{f}'}$ be the L-rational isogeny to an elliptic curve $E_{\mathfrak{f}'}$ with CM by the order in K of conductor $\mathfrak{f}'$. Then we have*

$$\#E(L)_{\text{tors}} | \#E_{\mathfrak{f}'}(L)_{\text{tors}}.$$

We can see in particular that $\#E(L)_{\text{tors}} \leq \#E_{\mathfrak{f}'}(L)_{\text{tors}}$. The analogous result for CM Drinfeld $\mathbb{F}_q[T]$-modules of rank 2 yields a uniform torsion bound and together with Theorem 3.31, by choosing $\mathfrak{f}' = 1$, is enough to prove the corresponding case of Conjecture 5.

3.6.1 Orders and endomorphism rings

Most of the materials in this subsection can be found in [Bre02]. One can also consult [Sti09], [Ros02] or [Sal06] for basic properties of global function fields.

As the endomorphism ring of a rank 2 CM Drinfeld $\mathbb{F}_q[T]$-module, say φ, is an order in a purely imaginary quadratic function field (the CM-field of φ), we recall some basic facts about those kind of orders. Let $K/\mathbb{F}_q(T)$ be a purely imaginary quadratic function field. Since we assumed that q is odd, $1 \neq -1$ in $\mathbb{F}_q(T)$ and K contains two distinct 2nd roots of unity. Then it is a Kummer extension and can be written as $K = \mathbb{F}_q(T)(\sqrt{d})$ for some non square $d \in F$. In this case, the integral closure of $\mathbb{F}_q[T]$ in K is $\mathcal{O}_K := \mathbb{F}_q[T][\sqrt{d'}]$, where d' is the square-free part of d, and it coincides with the ring of integers of K, see for instance [Ros87]. For $f \in \mathbb{F}_q[T]$ the subrings of $\mathcal{O}_K$ of the form $\mathbb{F}_q[T] + f\mathcal{O}_K$ are orders of K but they are not the only subgroups of finite index, for instance the rings of the form $\mathbb{F}_{p^m} + f\mathcal{O}_K$, $1 \leq m \leq s$, are of finite index[1]. However, we will see that these are the only ones that arise as endomorphism rings of Drinfeld $\mathbb{F}_q[T]$-modules of rank 2 over $\mathbb{C}_\infty$. The conductor of $\mathcal{O} = \mathbb{F}_q[T] + f\mathcal{O}_K$ in $\mathcal{O}_K$ is the ideal $f\mathcal{O}_K \subseteq \mathcal{O}$ by definition but we will make an abuse of language and call f also the *conductor* of the order $\mathcal{O}$ in $\mathcal{O}_K$.

Let φ be a CM Drinfeld $\mathbb{F}_q[T]$-module of rank 2 over $\mathbb{C}_\infty$. By the analytic uniformization theorem, there exists a rank 2 $\mathbb{F}_q[T]$-lattice Λ such that $\varphi \simeq \mathbb{C}_\infty/\Lambda := \varphi^\Lambda$. In this case

$$\mathcal{O} := \text{End}(\varphi) \simeq \text{End}(\Lambda) = \{x \in \mathbb{C}_\infty / x\Lambda \subseteq \Lambda\}.$$

[1] This is in contrast with the imaginary quadratic number fields case. The only subrings of finite index of an imaginary quadratic number field K are the subrings of the form $\mathbb{Z} + f\mathcal{O}_K, f \in \mathbb{Z}$.

Since $\mathbb{F}_q[T]$ is a PID, we can write $\Lambda = z_1\mathbb{F}_q[T] + z_2\mathbb{F}_q[T] =< z_1, z_2 >$ where $\{z_1, z_2\}$ is a basis of Λ as an F_∞-subspace of $\mathbb{C}_\infty$. We may scale Λ by a non-zero factor to get $\Lambda \simeq \Lambda_z =< z, 1 >$ where $z \notin F_\infty$. This determines z uniquely. Because φ has CM we have $\mathbb{F}_q[T] \subsetneq \mathrm{End}(\varphi)$. Let $x \in \mathrm{End}(\varphi) \setminus \mathbb{F}_q[T]$ ($x \notin F_\infty$ automatically), then $x = az + b$ and $xz = cz + e$ for some $a \neq 0, b, c, e \in \mathbb{F}_q[T]$. Therefore z satisfies a quadratic equation $az^2 + b'z + c' = 0$ with $b', c' \in \mathbb{F}_q[T]$. Denote by $D_z = b'^2 - 4ac'$ the *discriminant* of z, it is also uniquely determined. Since $z \notin F_\infty$, we get $\sqrt{D_z} \notin F_\infty$. As in the number field case, the field $K = \mathbb{F}_q(T)(z) = \mathbb{F}_q(T)(\sqrt{D_z})$ is an imaginary quadratic extension of $\mathbb{F}_q(T)$, it is the CM field of φ. In this case $D := D_z$ is called the *discriminant of* $\mathcal{O}$. The *discriminant of* K is simply the discriminant of $\mathcal{O}_K$. Furthermore,

$$\mathcal{O} = \mathrm{End}(\Lambda) = \mathbb{F}_q[T][\sqrt{D}]$$

is an order in K and we see that the endomorphism rings of rank 2 CM Drinfeld $\mathbb{F}_q[T]$-modules are of the form $\mathbb{F}_q[T] + f\mathcal{O}_K, f \in \mathbb{F}_q[T]$, where f^2 is the square part of D.

3.6.2 A canonical isogeny

The content and results in the current subsection, except for Lemma 3.41 and Lemma 3.46, have been communicated privately to the author by Pete Clark as part of a joint work of his with Paul Pollack. These constitute an important part of the arguments in the subsequent proof of the Isogeny Torsion Theorem.

It is now understood that in order to prove a uniform bound we need to reduce to the case of maximal endomorphism ring. This can be achieved by means of a canonical isogeny to an appropriate Drinfeld module having its endomorphism ring being the maximal order in its CM field. Our first attempt towards that goal, which will subsequently be substituted by a much better result, is the following

Lemma 3.41. *Let $\varphi_{|L}$ be an $\mathcal{O}$-CM Drinfeld A-module defined over L with CM-field K such that $K \subseteq L$. Then there exists an $\mathcal{O}_K$-CM Drinfeld A-module φ' defined over L and a canonical L-rational isogeny $\iota' : \varphi \to \varphi'$.*

Proof. Let $\mathfrak{C}$ be the conductor of $\mathcal{O}$ in $\mathcal{O}_K$. We know that φ can be seen as an $\mathcal{O}$-module, say $\tilde{\varphi} : \mathcal{O} \to LK\{\tau\} = L\{\tau\}$, defined over LK and hence over L since we assume that $K \subseteq L$. Now, choose $\varphi' = (\mathfrak{C} * \tilde{\varphi})|_A$ and $\iota' = \tilde{\varphi}_{\mathfrak{C}}$. By the definition of the operation $*$ it is clear that φ' is defined over L and ι' is an L-rational isogeny from φ to φ'. It remains to show that $\mathrm{End}(\varphi') \simeq \mathcal{O}_K$. Let $\alpha \in \mathcal{O}_K$ and $0 \neq c \in \mathfrak{C}$. Recall that $\mathfrak{C} = \{x \in \mathcal{O} | x\mathcal{O}_K \subseteq \mathcal{O}\}$. Thus $c\alpha \in \mathcal{O}$ and gives rise to an endomorphism of φ that we still denote by $c\alpha$. We have an inclusion of $\mathbb{F}_q$-vector spaces $\mathrm{Ker}(\tilde{\varphi}_{\mathfrak{C}}c) = \varphi[c\mathfrak{C}] \subseteq \mathrm{Ker}(\tilde{\varphi}_{\mathfrak{C}}c\alpha) = \varphi[c\alpha\mathfrak{C}]$. We can complete the one to get the other. Thus, there exists a morphism $\tilde{\alpha} : \varphi' \to \varphi'$ such that $\tilde{\varphi}_{\mathfrak{C}}c\alpha = \tilde{\alpha}\tilde{\varphi}_{\mathfrak{C}}c$, i.e. the following diagram is commutative

$$\begin{tikzcd}
\varphi \arrow[r, "c\alpha"] \arrow[d, "c"'] & \varphi \arrow[dd, "\tilde{\varphi}_{\mathfrak{C}}"] \\
\varphi \arrow[d, "\tilde{\varphi}_{\mathfrak{C}}"'] & \\
\varphi' \arrow[r, "\tilde{\alpha}"'] & \varphi'
\end{tikzcd} .$$

This shows that each element α of $\mathscr{O}_K$ corresponds to a morphism $\tilde{\alpha} \in \mathrm{End}(\varphi')$ and it is clear that this correspondence is one-to-one. Hence $\mathrm{End}(\varphi') \simeq \mathscr{O}_K$. □

This proof of Lemma 3.41 is essentially the same as the proof of [Gos98, Proposition 4.7.19.] using the $*$ operation as suggested in the remark thereafter.

The next step is to extend the isogeny $\iota' : \varphi \to \varphi'$ to $\mathbb{C}_\infty$ by analytic uniformization and with an appropriate embedding of L into $\mathbb{C}_\infty$ so that it becomes the quotient map $\mathbb{C}_\infty/\mathscr{O} \to \mathbb{C}_\infty/\mathscr{O}_K$.

Let L/F be a finite extension. In the remainder of this subsection we will provide a much better version of Lemma 3.41, courtesy of Pete Clark and Paul Pollack, which not only is true for general orders $\mathscr{O}' \supseteq \mathscr{O}$ (not necessarily $\mathscr{O}_K$) but also gives, in some sense, the best possible φ'.

Let $\mathscr{O}$ be an order in K, $\mathscr{O}_K$ the maximal order and $\mathfrak{C}(\mathscr{O})$ the conductor of $\mathscr{O}$. We denote by $H_{\mathscr{O}}$ the *ring class field*[2] of $\mathscr{O}$ associated to the order $\mathscr{O}$ by class field theory. The following theorem summarizes the main properties of $H_{\mathscr{O}}$.

Theorem 3.42. *The extension $H_{\mathscr{O}}/K$ is a finite abelian extension in which ∞ splits completely and each finite prime $\mathfrak{p}$ of K dividing $\mathfrak{C}(\mathscr{O})$ ramifies. Furthermore, there is a canonical isomorphism* $\mathrm{Gal}(H_{\mathscr{O}}/K) \simeq \mathbf{Pic}(\mathscr{O})$.

Proof. See [Hay79, §8] Proposition 8.4, Theorems 8.8 and 8.10. □

For a rank 1 Drinfeld $\mathscr{O}$-module φ we will always assume, in this subsection, that $\mathrm{End}(\varphi) = \mathscr{O}$. This assumption is satisfied when we reduce

[2] In [Hay79], Hayes calls it the "Hilbert class field" which is usually understood to be the ring class field of the maximal order.

to rank one as is section 3.1 so there is no loss in making it. In this case $\varphi \simeq_{\mathbb{C}_\infty} \mathbb{C}_\infty/\Lambda$ for some lattice Λ which is proper as a fractional $\mathcal{O}$-ideal, i.e.

$$\mathrm{End}(\varphi) = (\Lambda : \Lambda) = \{x \in K | x\Lambda \subseteq \Lambda\} = \mathcal{O}$$

For an invertible integral ideal $\mathfrak{a}$ in $\mathcal{O}$ we have

$$\varphi[\mathfrak{a}] = (\mathbb{C}_\infty/\Lambda)[\mathfrak{a}] = \mathfrak{a}^{-1}\Lambda/\Lambda = \mathrm{Ker}(\mathbb{C}_\infty/\Lambda \to \mathbb{C}_\infty/\mathfrak{a}^{-1}\Lambda).$$

This tells us that under analytic uniformization the isogeny $\varphi \to \varphi/\varphi[\mathfrak{a}] = \mathfrak{a} * \varphi$ becomes $\mathbb{C}_\infty/\Lambda \to \mathbb{C}_\infty/\mathfrak{a}^{-1}\Lambda$.

Definition 3.43. *A Drinfeld $\mathcal{O}$-module φ is said to be* invertible *if it has rank one and is isomorphic over $\mathbb{C}_\infty$ to a Drinfeld $\mathcal{O}$-module uniformized by a lattice which is an invertible fractional $\mathcal{O}$-ideal.*

Theorem 3.44. *Let $\mathcal{O}$ be an order in $\mathcal{O}_K$ and let φ_L be an invertible Drinfeld $\mathcal{O}$-module.*

(i) If $\varphi_{|L}$ is a rank 1 Drinfeld $\mathcal{O}$-module, then $L \supseteq H_{\mathcal{O}}$. Furthermore, $H_{\mathcal{O}}$ is the smallest field of definition for φ.

(ii) Let $\mathfrak{a} \subseteq \mathcal{O}$ be an ideal that is prime to $\mathfrak{C}(\mathcal{O})$. Then $\mathfrak{a}\mathcal{O}_K$ is a product of prime ideals that are unramified in the abelian extension $H_{\mathcal{O}}/K$, so the Artin map gives an element $\sigma_{\mathfrak{a}\mathcal{O}_K} \in \mathrm{Gal}(H_{\mathcal{O}}/K)$. Then we have

$$\sigma_{\mathfrak{a}\mathcal{O}_K}(\varphi) = \mathfrak{a} * \varphi = \varphi/\varphi[\mathfrak{a}].$$

Proof. See [Hay79, §8]. In particular, Theorem 8.5 treats the case (ii) for prime ideals but this can be extended by class field theory to $\mathfrak{a}$. □

Corollary 3.45. *Let $\mathcal{O}$ be an order in $\mathcal{O}_K$. If $\varphi_{|L}$ is an invertible Drinfeld $\mathcal{O}$-module then there is an embedding $i : L \hookrightarrow \mathbb{C}_\infty$ such that*

$$i(\varphi) \simeq_{\mathbb{C}_\infty} \mathbb{C}_\infty/\mathcal{O}.$$

Proof. Every invertible fractional $\mathcal{O}$-ideal is isomorphic to an integral $\mathcal{O}$-ideal $\mathfrak{a}$ in $\mathbf{Pic}(\mathcal{O})$ that is prime to $\mathfrak{C}(\mathcal{O})$. Therefore, $\varphi \simeq_{\mathbb{C}_\infty} \mathbb{C}_\infty/\mathfrak{a}$, so $\sigma_{\mathfrak{a}\mathcal{O}_K}(\varphi) = \varphi/\varphi[\mathfrak{a}] \simeq \mathbb{C}_\infty/\mathfrak{a}\mathfrak{a}^{-1} = \mathbb{C}_\infty/\mathcal{O}$. □

Lemma 3.46. *An isogeny between two Drinfeld modules of generic characteristic is separable.*

Proof. See [Pin12, Proposition 6.41 (c)]. □

Theorem 3.47. *Let $\mathscr{O} \subseteq \mathscr{O}' \subseteq \mathscr{O}_K$ be orders in K, let L/K be a finite field extension, and let $\varphi_{|L}$ be an invertible Drinfeld $\mathscr{O}$-module. Then there is an invertible Drinfeld $\mathscr{O}'$-module $\varphi'_{|L}$ and an L-rational isogeny of Drinfeld $\mathscr{O}$-modules $f : \varphi \to \varphi'$ that is universal for isogenies from φ to an invertible Drinfeld $\mathscr{O}'$-module: if $\psi_{|\mathbb{C}_\infty}$ is an invertible Drinfeld $\mathscr{O}'$-module and $f_\psi : \varphi \to \psi$ is an isogeny of Drinfeld $\mathscr{O}$-modules, then there is a unique isogeny $g : \varphi' \to \psi$ of Drinfeld $\mathscr{O}$-modules such that $f_\psi = g \circ f$.*

Proof. Since φ is invertible, there is an invertible $\mathscr{O}$-ideal Λ such that $\varphi \simeq \mathbb{C}_\infty/\Lambda$ over $\mathbb{C}_\infty$. Let ψ be an invertible Drinfeld $\mathscr{O}'$-module and $f_\psi : \varphi \to \psi$ an isogeny of Drinfeld $\mathscr{O}$-modules. There exists an invertible $\mathscr{O}'$-ideal $\mathfrak{a}$ such that over $\mathbb{C}_\infty$ we have $\psi \simeq \mathbb{C}_\infty/\mathfrak{a}$. Me may assume that $\Lambda \subseteq \mathfrak{a}$ because over $\mathbb{C}_\infty$ the isogeny f_ψ corresponds to multiplication by some $c \in \mathbb{C}_\infty \setminus \{0\}$ such that $c\Lambda \subseteq \mathfrak{a}$ by analytic uniformization, thus $\Lambda \subseteq c^{-1}\mathfrak{a}$ and we may replace ψ by the isomorphic module $\mathbb{C}_\infty/c^{-1}\mathfrak{a}$. It follows that $\mathfrak{a} \supseteq \Lambda\mathscr{O}'$. Put $\varphi' := \mathbb{C}_\infty/\Lambda\mathscr{O}'$ and $f : \varphi \to \varphi'$ defined over $\mathbb{C}_\infty$ by the canonical surjection $\mathbb{C}_\infty/\Lambda \to \mathbb{C}_\infty/\Lambda\mathscr{O}'$. The Drinfeld $\mathscr{O}'$-module φ' is defined over L since $L \supseteq K$. Now, $\Lambda\mathscr{O}'$ is the image of Λ by the canonical map $\mathbf{Pic}(\mathscr{O}) \to \mathbf{Pic}(\mathscr{O}')$ so it is an invertible $\mathscr{O}'$-ideal. Hence, $\Lambda\mathscr{O}'$ is proper and $\operatorname{End}(\varphi') = \mathscr{O}'$ so that φ' is an invertible Drinfeld $\mathscr{O}'$-module. The isogeny f_ψ factors through f as in the following commutative diagram

$$\begin{tikzcd}
\mathbb{C}_\infty/\Lambda \simeq \varphi \arrow[rr, "f"] \arrow[dr, "f_\psi"'] & & \varphi' \simeq \mathbb{C}_\infty/\Lambda\mathscr{O}' \arrow[dl, dashed, "\exists\,!\,g"] \\
& \psi \simeq \mathbb{C}_\infty/\mathfrak{a} &
\end{tikzcd}$$

i.e. $f_\psi = g \circ f$ for a unique isogeny $g : \varphi' \to \psi$, where over $\mathbb{C}_\infty$, $f_\psi : \mathbb{C}_\infty/\Lambda \to \mathbb{C}_\infty/\mathfrak{a}$ and $g : \mathbb{C}_\infty/\Lambda\mathscr{O}' \to \mathbb{C}_\infty/\mathfrak{a}$ correspond to multiplication by some $c_\psi \in \mathbb{C}_\infty \setminus \{0\}$ ($c_\psi\Lambda\mathscr{O}' \subseteq \mathfrak{a}$ since $c_\psi\Lambda \subseteq \mathfrak{a}$). This constructs φ' and f over $\mathbb{C}_\infty$ and verifies the universal property. It remains to show that f is L-rational. By Lemma 3.46, since $\varphi_{|L}$ and $\varphi'_{|L}$ have generic characteristic, $f \in L^{\text{sep}}\{\tau\}$. Let $H_f := \operatorname{Ker} f$ be the geometric kernel of f, it is a subgroup scheme of $\mathbb{G}_a$ defined over L^{sep}. Let $\sigma \in \operatorname{Gal}(L^{\text{sep}}/L)$ and define $f_\sigma := \sum\limits_{i=0}^{n} \sigma(f_i)\tau^i$ if $f = \sum_{i=0}^{n} f_i\tau^i$. Since φ and φ' are L-rational, $f_\sigma : \varphi \to \varphi'$ defines an isogeny. By the universal property we have the following commutative diagram

$$\begin{tikzcd}
\varphi \arrow[rr, "f"] \arrow[dr, "f_\sigma"'] & & \varphi' \arrow[dl, dashed, "\exists\,!\,g"] \\
& \varphi' &
\end{tikzcd}$$

i.e. $f_\sigma = g \circ f$ for some isogeny g. By comparing degrees we have that $g \in L^{\mathrm{sep}} \setminus \{0\}$. Thus, $\sigma(H_f) = H_f$ i.e. H_f is $\mathrm{Gal}(L^{\mathrm{sep}}/L)$-invariant. This implies that H_f is defined over L, i.e. f is L-rational. □

Remark 3.48. Theorem 3.47 is an analogue of [BC19, §2.6], the proof of which is modelled from materials therein, on CM elliptic curves which proves that if $E_{|L}$ is a CM elliptic curve defined over a number field L such that $\mathrm{End}\, E = \mathscr{O}$ is an order in a quadratic imaginary field K, then for any order $\mathscr{O}'$ with $\mathscr{O} \subseteq \mathscr{O}' \subseteq K$ there is an L-rational isogeny $f : E \to E'$ with $\mathrm{End}\, E' = \mathscr{O}'$ that is universal for isogenies from an $\mathscr{O}$-CM elliptic curve to an $\mathscr{O}'$-CM elliptic curve. However, Theorem 3.47 is slightly weaker for higher rank (> 2). First of all, it only works for Drinfeld A-modules φ which are invertible when considered as rank one Drinfeld $\mathrm{End}\,\varphi$-modules. Second, the complex multiplication of φ is assumed to be L-rational, i.e. $\mathrm{End}\,\varphi = \mathrm{End}_L\,\varphi$.

Assuming that the complex multiplication is L-rational is enough for our purpose.

3.6.3 Isogeny Torsion Theorem for Drinfeld modules

We want to formulate and prove an analogue of Theorem 3.40 for CM Drinfeld $\mathbb{F}_q[T]$-modules of rank 2. In view of our main goal, this will allow us to reduce to the case of a Drinfeld module with endomorphism ring being the maximal order of its CM field so that we can get rid of the hypothesis $\mathrm{End}(\varphi) = \mathscr{O}_K$ in Theorem 3.31. Uniform bound will follow from this as in Conjecture 5.

Let $L/\mathbb{F}_q(T)$ be a finite extension and $\varphi_{|L} : \mathbb{F}_q[T] \to L\{\tau\}$ be a Drinfeld $\mathbb{F}_q[T]$-module of rank 2 defined over L with CM by an order $\mathscr{O}$ in the quadratic function field $K \supseteq \mathbb{F}_q(T)$. We furthermore assume that $L \supseteq K$, this assumption will allow us to make explicit computations with the Galois representations associated to φ which works for the rank 2 Drinfeld $\mathbb{F}_q[T]$-module case. In general, in higher rank the computations become more complicated and it hints for the need of a more conceptual (non-explicit) proof. For a non zero element $g \in \mathbb{F}_q[T]$, we consider the *mod g Galois representation* associated to φ

$$\rho_g : \mathfrak{g}_L \longrightarrow \mathrm{Aut}(\varphi[g]) \simeq \mathrm{GL}_2(\mathbb{F}_q[T]/g\mathbb{F}_q[T])$$

where $\mathfrak{g}_L := \mathrm{Gal}(L^{\mathrm{sep}}/L)$ acts naturally on $\varphi[g]$ and the isomorphism on the right hand side depends on the choice of a basis of $\varphi[g] \simeq (\mathbb{F}_q[T]/g\mathbb{F}_q[T])^2$ as an $\mathbb{F}_q[T]$-module, but our results do not depend on such a choice. Now, since $\mathscr{O}$ is a quadratic order, it is Gorenstein by Theorem 1.44 (ii) so that $\varphi[g] \simeq \mathscr{O}/g\mathscr{O}$ as an $\mathscr{O}$-module; one can see this by reducing φ at a well chosen prime of L for which the endomorphism ring and the g-torsions don't change and use [GP20, Theorem 4.9 and discussion after the proof of Theorem 4.6]. Since φ has $\mathscr{O}$-CM and $L \supseteq K$, the action of $\mathscr{O}$ on $\varphi[g]$ commutes with that of $\mathfrak{g}_L$ and the Galois representation takes values in $(\mathscr{O}/g\mathscr{O})^*$

$$\rho_g : \mathfrak{g}_L \longrightarrow \mathrm{Aut}_{\mathscr{O}}(\varphi[g]) \simeq \mathrm{GL}_1(\mathscr{O}/g\mathscr{O}) \simeq (\mathscr{O}/g\mathscr{O})^*.$$

Now, we will embedd $\mathscr{O}$ in the matrix group $M_2(\mathbb{F}_q[T])$ of 2×2 matrices with coefficients in $\mathbb{F}_q[T]$ to make explicit computations. We have a natural embedding $K \hookrightarrow \mathrm{End}_F(K)$ by sending an element α to the multiplication by α map. Choosing a basis of K over F we have $\mathrm{End}_F(K) \simeq M_2(F)$ and an integral element of K over F lands in $M_2(\mathbb{F}_q[T])$. Let D_K be the discriminant of K and f the conductor of $\mathscr{O}$ as in section 3.6.1, i.e. $\mathscr{O} = \mathbb{F}_q[T][f\sqrt{D_K}]$. Then $\{1, f\sqrt{D_K}\}$ is an $\mathbb{F}_q[T]$-basis of $\mathscr{O}$ and an element $a + bf\sqrt{D_K} \in \mathscr{O}$, $a, b \in \mathbb{F}_q[T]$, corresponds to the matrix

$$\begin{bmatrix} a & bf^2D_K \\ b & a \end{bmatrix}.$$

Before proving the Isogeny Torsion Theorem we recall some structure theorems about finitely generated $\mathbb{F}_q[T]$-modules. Since $\mathbb{F}_q[T]$ is a PID, these theorems look very much like the ones for finitely generated abelian groups (or $\mathbb{Z}$-modules). We only state them for $\mathbb{F}_q[T]$ even if they can be formulated for more general types of modules (at least modules over Dedekind domains). Every finitely generated $\mathbb{F}_q[T]$-module M is a direct sum $M = M_{\mathrm{tor}} \oplus M'$ where M_{tor} is its torsion submodule which is finite and M' a finitely generated free $\mathbb{F}_q[T]$-module. The rank of M is in this case the rank of M' as a free module. We are interested in the structure of M_{tor}. Let P be a monic irreducible element of $\mathbb{F}_q[T]$ i.e. a finite prime, the submodule $M[P^\infty] := \{m \in M, P^n m = 0 \text{ for some n} \geq 1\}$ is called the *P-primary component* of M.

Theorem 3.49 (Primary decomposition)**.** *Let M be a finitely generated torsion $\mathbb{F}_q[T]$-module, i.e. $M = M_{\mathrm{tor}}$. Then $M[P^\infty] = \{0\}$ for almost all prime P and*

$$M \simeq \oplus_P M[P^\infty].$$

The P-primary component of M decomposes as follows.

Theorem 3.50. *Let M be a finitely generated $\mathbb{F}_q[T]$-module and P a prime of $\mathbb{F}_q[T]$. Then*

$$M[P^\infty] \simeq \oplus_{i=1}^k \mathbb{F}_q[T]/(P)^{n_i}$$

where $n_1 \leq \cdots \leq n_k$ are positive integers. Furthermore, the sequence $n_1 \leq \cdots \leq n_k$ is uniquely determined by M.

For all primes P of $\mathbb{F}_q[T]$, the prime powers $(P)^{n_i}$ in the decomposition of M as in Theorem 3.50 are called the *elementary divisors* of M.

If M is a finitely generated torsion $\mathbb{F}_q[T]$-module and $x \neq 0 \in M$, then $\operatorname{Ann}(x) = (g)$ for some monic polynomial $g \in \mathbb{F}_q[T]$ which is unique up to multiplication by a unit, g is called the *order* of x. Similarly, $\operatorname{Ann}(M) = (g')$ for some monic polynomial g' unique up to multiplication by a unit, g' is called the *exponent* of M. In the case of abelian groups, i.e. $\mathbb{Z}$-modules, these notions coincide with the order of an element and the exponent of an abelian group respectively.

Lemma 3.51. *Let A and F be as in our general setting, let K/F be a quadratic field extension and let $\mathcal{O}$ be a quadratic A-order in K. Then every rank one Drinfeld $\mathcal{O}$-module φ such that* $\operatorname{End}\varphi = \mathcal{O}$ *is invertible.*

Proof. This is a consequence of Theorem 1.44. Such Drinfeld module is uniformized by a proper ideal Λ, and since the order is quadratic it is Gorenstein. It follows that Λ is invertible. □

Theorem 3.52 (Isogeny Torsion Theorem)**.** *Let $\mathcal{O} := \mathbb{F}_q[T] + f\mathcal{O}_K$ be an order in an imaginary quadratic function field $K/\mathbb{F}_q(T)$, where $f \in \mathbb{F}_q[T]$, $L \supseteq K$ be a global function field, $\varphi_{|L}$ be an $\mathcal{O}$-CM Drinfeld $\mathbb{F}_q[T]$-module of rank 2. Then there exists an $\mathcal{O}_K$-CM Drinfeld $\mathbb{F}_q[T]$-module φ'_L defined over L such that*

$$\#\varphi(L)_{\text{tors}} | \#\varphi'(L)_{\text{tors}}$$

or equivalently

$$\#\varphi(L)_{\text{tors}} \leq \#\varphi'(L)_{\text{tors}}$$

since both cardinalities are powers of q.

Proof. By Lemma 3.51, φ is invertible as an $\mathcal{O}$-module, and by Corollary 3.45 we can choose an embedding $L \hookrightarrow \mathbb{C}_\infty$ such that over $\mathbb{C}_\infty$ we have $\varphi \simeq \mathbb{C}_\infty/\mathcal{O}$. Moreover, since we are assuming that $L \supseteq K$, by Theorem 3.47 the narural map $\mathbb{C}_\infty/\mathcal{O} \to \mathbb{C}_\infty/\mathcal{O}_K$ is the extension to $\mathbb{C}_\infty$ of an L-rational isogeny $\iota' : \varphi \to \varphi'$ where φ' is a Drinfeld $\mathbb{F}_q[T]$- module of rank 2 defined over L with $\operatorname{End}(\varphi') = \mathcal{O}_K$. The kernel of $\iota'_{\mathbb{C}_\infty}$ is $\mathcal{O}_K/\mathcal{O}$ which is a cyclic $\mathbb{F}_q[T]$-module isomorphic to $\mathbb{F}_q[T]/f\mathbb{F}_q[T]$ and of order f. Let D_K (respectively D) be the discriminant of K (respectively $\mathcal{O}$), i.e. $D = f^2 D_K$ as one can see from the discussion in subsection 3.6.1, where f is the conductor of $\mathcal{O}$. Let $\tau_K := \sqrt{D_K}$ so that $\mathcal{O}_K = \mathbb{F}_q[T][\tau_K]$ and $\mathcal{O} = \mathbb{F}_q[T][f\tau_K]$. Identifying φ_{tors} with $\mathbb{C}_\infty/\mathcal{O}[\text{tors}]$, for a monic polynomial $g \in \mathbb{F}_q[T]$, we get an $\mathbb{F}_q[T]/g\mathbb{F}_q[T]$-basis of $\varphi[g]$: $\{e_1 := \dfrac{1}{g} + \mathcal{O},\ e_2 := \dfrac{f\tau_K}{g} + \mathcal{O}\}$. In a similar way we have an $\mathbb{F}_q[T]/g\mathbb{F}_q[T]$-basis of $\varphi'[g]$: $\{e_1' := \dfrac{1}{g} + \mathcal{O}_K,\ e_2 := \dfrac{\tau_K}{g} + \mathcal{O}_K\}$. Following the discussion at the beginning of this subsection, with respect to the above basis, the image of the *mod* g Galois representation of φ consists of matrices of the form

$$\begin{bmatrix} a & bf^2D_K \\ b & a \end{bmatrix} |a, b \in \mathbb{F}_q[T]/g\mathbb{F}_q[T].$$

Now, according to Theorem 3.49, since $\varphi(L)_{\text{tors}}$ and $\varphi'(L)_{\text{tors}}$ are finite torsion $\mathbb{F}_q[T]$-modules (by the analogue of the Mordell-Weil theorem) it is enough to show that $\varphi(L)_{\text{tors}}[P^\infty]$ divides $\varphi'(L)_{\text{tors}}[P^\infty]$ for all primes $P \in \mathbb{F}_q[T]$. So we fix a prime $P \in \mathbb{F}_q[T]$. If $P \nmid f$ then $\iota'|_{\varphi(L)_{\text{tors}}[P^\infty]}(Q) = 0$ if and only if $Q = 0$, and if $Q \in \varphi(L)_{\text{tors}}[P^\infty]$ one can easily check that $\iota'(Q) \in \varphi'(L)_{\text{tors}}[P^\infty]$ since ι' is L-rational. Hence $\iota'_{\mathbb{C}_\infty}$ induces an injection

$$\varphi(L)_{\text{tors}}[P^\infty] \hookrightarrow \varphi'(L)_{\text{tors}}[P^\infty]$$

and we are done. So we may assume that $P|f$ i.e. $\operatorname{ord}_P f \geq 1$ where $f = P^{\operatorname{ord}_P f} f'$ and $\gcd(P, f') = 1$. By Theorem 3.50, we have

$$\varphi(L)_{\text{tors}}[P^\infty] \simeq \oplus_{i=1}^{l} \mathbb{F}_q[T]/(P)^{n_i} \text{ for some } 1 \geq 1$$

with $1 \leq n_1 \leq \cdots \leq n_l$ uniquely determined. Put $\mathfrak{a}_{L,P} = \operatorname{Ann}(\varphi(L)_{\text{tors}}[P^\infty])$ a non-zero ideal of $\mathbb{F}_q[T]$. We have $\varphi(L)_{\text{tors}}[P^\infty] \subseteq \varphi[\mathfrak{a}_{L,P}] \simeq (\mathbb{F}_q[T]/\mathfrak{a}_{L,P}\mathbb{F}_q[T])^2$ so that

$$\varphi(L)_{\text{tors}}[P^\infty] \simeq \mathbb{F}_q[T]/(P)^m \oplus \mathbb{F}_q[T]/(P)^n$$

for some $0 \leq m \leq n$. We may assume $n \geq 1$. We then have $\varphi(L)_{\text{tors}}[P^\infty] \subseteq \varphi[P^n]$ and let $\{e_1, e_2\}$ be the basis for $\varphi[P^n]$ and $\{e_1', e_2'\}$ be the basis for $\varphi'[P^n]$ as above.

Put $k = \min(\operatorname{ord}_P f, n)$. Since $\varphi(L)_{\text{tors}}[P^\infty] \simeq \mathbb{F}_q[T]/(P)^m \oplus \mathbb{F}_q[T]/(P)^n$, there exists an element $x \in \varphi(L)$ of order P^n, one can choose x to be a generator of the cyclic submodule isomorphic to $\mathbb{F}_q[T]/(P)^n$ of order P^n. Then $\varphi_{P^n}(x) = 0$ so that $\iota'(\varphi_{P^n}(x)) = 0 = \varphi'_{P^n}(\iota'(x))$. Hence $x' = \iota'(x)$, which is still an element of $\varphi'(L)$ since ι' is L-rational, has order P^d for some d with $n - k \leq d \leq n$ (recall that the kernel of ι' is cyclic of order f). The idea is to show that $\varphi'(L)_{\text{tors}}[P^\infty]$ has full P^γ-torsion for some γ such that $\gamma + d \geq m + n$. In this case $\varphi'(L)_{\text{tors}}[P^\infty]$ would have size at least $|P|^{\gamma+d}$ which is larger than $|P|^{m+n} = \#\varphi(L)_{\text{tors}}[P^\infty]$.

If $d = n$ then clearly $\varphi'(L)_{\text{tors}}[P^n]$ has exponent P^n. In addition $\varphi'(L)_{\text{tors}}[P^n]$ has full P^m-torsion because $\iota'(P^{n-m}e_1) = P^{n-m}(\iota'(e_1)) = P^{n-m}e_1' = \dfrac{1}{P^m} + \mathcal{O}_K \in \varphi'(L)$ generates $\varphi'(L)_{\text{tors}}[P^m]$ as an $\mathcal{O}_K$-module. Therefore $\varphi'(L)_{\text{tors}}[P^m]$ has size at least $|P|^{m+n} = q^{(m+n)\deg P} = \#\varphi(L)_{\text{tors}}[P^\infty]$ and we are done.

So we may assume that $d < n$. Using the Galois representations described above, we are going to show that if $d > m$ then $\varphi'(F)_{\text{tors}}[P^\infty]$ has full P^n-torsion and if $d \leq m$ then $\varphi'(F)_{\text{tors}}[P^\infty]$ has full P^{m+n-d}-torsion which gives the result since we know that $\varphi'(F)_{\text{tors}}[P^\infty]$ has a point of order P^d namely x'. We treat the two cases at once by considering $\delta := \min(m+n-d, n)$.

Write $x = \alpha e_1 + \beta e_2$ where $\alpha, \beta \in \mathbb{F}_q[T]/(P^n)$ so we have

$$\begin{aligned} 0 &= P^d \iota'(x) \\ &= \iota'(P^d x) \\ &= \iota'(P^d \alpha e_1 + P^d \beta e_2) \\ &= \iota'(P^d \alpha e_1 + P^d \beta e_2) \\ &= \iota'(P^d \alpha e_1) + \iota'(P^d \beta e_2) \\ &= P^d \alpha e_1' + P^d f \beta e_2' \\ &= P^d \alpha e_1' \end{aligned}$$

where the last equality holds since $P^k | f$ and $d + k \geq n$ so that $P^d f \beta e_2' = P^{d+k} \beta' e_2' = 0 \mod P^n$. This implies $P^{n-d} | \alpha$ since $P^d \alpha = 0 \mod P^n$, so we can write $\alpha = P^{n-d}\alpha'$ for some α'. In addition, $P \nmid \beta$ since $P^d x = P^d \beta e_2$ has order P^{n-d} (otherwise it would have order strictly less than P^{n-d}).

We now consider the $\mod P^\delta$ Galois representation associated to φ_L. We know that the image of ρ_{P^δ} consists of matrices in $\mathrm{GL}_2(\mathbb{F}_q[T]/P^\delta \mathbb{F}_q[T])$ of the form $\begin{bmatrix} a & bf^2 D_K \\ b & a \end{bmatrix}$, $a, b \in \mathbb{F}_q[T]/P^\delta \mathbb{F}_q[T]$. Since $\varphi(L)_{\text{tors}}[P^\infty]$ has full P^m-torsion, the Galois group $\mathfrak{g}_L$ leaves the elements of $\varphi[P^m]$ fixed. Hence $a = 1 \mod P^m$ and $b = bf^2 D_K \mod P^m$ so that $a = 1 + P^m \mathbb{F}_q[T]$, $b = P^m B$ for some $\mathbb{F}_q[T], B \in \mathbb{F}_q[T]/P^\delta \mathbb{F}_q[T]$. Also, since $\delta \leq m + n - d \leq m + k$ and $\mathrm{ord}_P(bf^2 D_K) \geq m + 2k \geq \delta$, we have $bf^2 D_K = 0 \mod P^\delta$. Thus the $\mod P^\delta$ Galois representation associated to φ_L has a restricted form

$$\rho_{P^\delta}(\mathfrak{g}_L) \subseteq \left\{ \begin{bmatrix} 1 + P^m a & 0 \\ P^m b & 1 + P^m a \end{bmatrix} | a, b \in \mathbb{F}_q[T]/P^\delta \mathbb{F}_q[T] \right\}.$$

Since the set $\{h_1 = P^{n-\delta} e_1, h_2 = P^{n-\delta} e_2\}$ forms a $\mathbb{F}_q[T]/P^\delta \mathbb{F}_q[T]$-basis of $\varphi[P^\delta]$ and $P^{n-\delta} x = \alpha h_1 + \beta h_2 = P^{n-d}\alpha' h_1 + \beta h_2$ is L-rational (therefore fixed by the action of $\mathfrak{g}_L$), the matrices in $\rho_{P^\delta}(\mathfrak{g}_L)$ satisfy

$$\begin{bmatrix} 1 + P^m a & 0 \\ P^m b & 1 + P^m a \end{bmatrix} \begin{bmatrix} P^{n-d}\alpha' \\ \beta \end{bmatrix} = \begin{bmatrix} P^{n-d}\alpha' \\ \beta \end{bmatrix}$$

which gives the congruence

$$P^{m+n-d}\alpha' b + \beta P^m a = 0 \mod P^\delta.$$

Since $\delta \leq m+n-d$ and $P \nmid \beta$, we deduce that $P^{\delta-m}|a$. Therefore the image of the $\mod P^{\delta}$ Galois representation consists of matrices of the form

$$\begin{bmatrix} 1 & 0 \\ P^m b & 1 \end{bmatrix}.$$

Let $\sigma \in \mathfrak{g}_L$, we compute $\sigma(\iota'(P^{n-\delta}e_1))$

$$\begin{aligned} \sigma(\iota'(P^{n-\delta}e_1)) &= \iota'(\sigma(P^{n-\delta}e_1)) \text{ since } \iota' \text{ is } L\text{−rational} \\ &= \iota'\left(\begin{bmatrix} 1 & 0 \\ P^m b & 1 \end{bmatrix}\begin{bmatrix} P^{n-\delta} \\ 0 \end{bmatrix}\right) \text{ for some } b \in \mathbb{F}_q[T]/P^{\delta}\mathbb{F}_q[T] \\ &= \iota'(P^{n-\delta}e_1 + bP^{m+n-\delta}e_2) \\ &= \iota'(P^{n-\delta}e_1) + bP^{m+n-\delta}fe_2' \\ &= \iota'(P^{n-\delta}e_1) \end{aligned}$$

where the last equality holds because $P^k|f$ so that $\mathrm{ord}_P(BP^{m+n-\delta}f) \geq m+n+k-\delta \geq n \geq \delta$. Therefore $\iota'(P^{n-\delta}e_1) \in \varphi'(L)_{\text{tors}}[P^{\delta}]$ is fixed by $\mathfrak{g}_L$ which means that its L-rational. In addition, $\iota'(P^{n-\delta}e_1)$ is of order P^{δ} and generates $\varphi'[P^{\delta}]$ as an $\mathscr{O}_K$-module.

Therefore, if $d < m$ i.e. $\delta = n$, then we have

$$\#\varphi(L)_{\text{tors}}[P^{\infty}] = |P|^{m+n} \leq |P|^{2n} = \#\varphi'(L)_{\text{tors}}[P^n] \leq \#\varphi'(L)_{\text{tors}}[P^{\infty}]$$

and we are done. On the other hand if $d \geq m$ i.e. $\delta = m+n-d$, as we have just seen above $\varphi'(L)_{\text{tors}}[P^{\infty}]$ has full P^{δ}-torsion and a point of order P^d namely $x' = \iota'(x)$. Thus $\varphi'(L)_{\text{tors}}[P^{\infty}]$ has size at least $|P|^{\delta+d} = |P|^{m+n} = \#\varphi(L)_{\text{tors}}[P^{\infty}]$ and we are done. We conclude that

$$\#\varphi(L)_{\text{tors}} | \#\varphi'(L)_{\text{tors}}.$$

□

The above proof of Theorem 3.52 is an analogue of Clark and Bourdon's proof of Theorem 3.40 for the case $\mathfrak{f}' = 1$.

3.6.4 Uniform torsion bound for CM Drinfeld modules

As a consequence of combining the Isogeny Torsion Theorem 3.52 and Theorem 3.31 we deduce that Conjecture 5 is true for $A = \mathbb{F}_q[T]$ and $r = 2$.

Theorem 3.53. *Let $q \geq 3$ be a power of an odd prime. There exists an absolute and effective constant $C_q > 0$ such that for any extension $L/\mathbb{F}_q(T)$ of degree $d \geq 3$ and any rank 2 Drinfeld $\mathbb{F}_q[T]$-module with complex multiplication φ defined over L*

$$\#\varphi(L)_{\text{tors}} \leq C_q d \log\log d.$$

Proof. Let $\mathscr{O} := \operatorname{End}(\varphi)$ and K be the CM field of φ. The Isogeny Torsion Theorem guarantees the existence of a Drinfeld $\mathbb{F}_q[T]$-module φ' defined over L such that $\operatorname{End}(\varphi') = \mathscr{O}_K$ and $\#\varphi(L)_{\text{tors}} \leq \#\varphi'(L)_{\text{tors}}$. Now, it is enough to bound $\#\varphi'(LK)_{\text{tors}}$ and proceed as in Theorem 3.31 and we are done. One can choose

$$C_q = 144e^4(q+1)(q-1)^2\left(1 + \frac{\log(288e^4(q+1)(q-1)^2)}{\log\log 3}\right)$$

as in Theorem 3.31. □

List of References

[Abr95] Dan Abramovich. Formal finiteness and the torsion on elliptic curves. *Astérisque*, 228, 1995.

[Arm12] Cécile Armana. Torsion des modules de drinfeld de rang 2 et formes modulaires de drinfeld. *Algebra Number Theory*, 6(6):1239–1288, 2012.

[BC18] Abbey Bourdon and Pete Clark. Torsion points and Galois representations on CM elliptic curves. *arXiv:1612.03229v3 [math.NT]*, 2018.

[BC19] A. Bourdon and P.L. Clark. Torsion points and isogenies on CM elliptic curves. http://alpha.math.uga.edu/~pete/BCII.pdf, 2019.

[BCH+66] A. Borel, S. Chowla, C. S. Herz, K. Iwasawa, and J. P. Serre. *Seminar on complex multiplications*, volume 21 of *Lecture Notes in Mathematics*. Springer-Verlag Berlin Heidelberg, 1966.

[BP16] Abbey Bourdon and Paul Pollack. Torsion subgroups of CM elliptic curves over odd degree number fields. *Int. Math. Res. Not. IMRN*, 2017:4923–4961, 2016.

[Bre02] F. Breuer. *On the André-Oort conjecture and Drinfeld modular curves*. PhD thesis, Université Paris 7 - Denis Diderot, 2002.

[Bre10] Florian Breuer. Torsion bounds for elliptic curves and Drinfeld modules. *Journal of Number Theory*, 130(5):1241 – 1250, 2010.

[Cla15] P.L. Clark. Commutative algebra. http://math.uga.edu/~pete/integral2015.pdf, 2015.

[CP15] Pete L. Clark and Paul Pollack. The truth about torsion in the CM case. *Comptes Rendus Mathematique*, 353(8):683 – 688, 2015.

[CP17] Pete L. Clark and Paul Pollack. The truth about torsion in the CM case, II. *The Quarterly Journal of Mathematics*, 2017.

[Dri74] Vladimir G. Drinfel'd. Elliptic modules. *Mathematics of the USSR-Sbornik*, 23(4):561, 1974.

[Gos98] David Goss. *Basic Structures of Function Field Arithmetic*. Springer-Verlag Berlin Heidelberg, 1998.

[GP20] S. Garai and M. Papikian. Computing endomorphism rings and frobenius matrices of drinfeld modules. *J. Number Theory*, 2020.

[Hay79] 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.

[HS99] Marc Hindry and Joseph Silverman. Sur le nombre de points de torsion rationnels sur une courbe elliptique. *C. R. Acad. Sci. Paris, Ser. I*, 329 (2):97–100, 1999.

[JT15] C.U. Jensen and A. Thorup. Gorenstein orders. *J. Pure Appl. Algebra*, 219:551–562, 2015.

[Kam92] Sheldon Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Invent. Math.*, 109:221–229, 1992.

[Leb07] Phillipe Lebacque. Generalised Mertens and Brauer-Siegel theorems. *Acta Arithmetica*, 130:333–350, 2007.

[LT97] G. Lachaud and M.A. Tsfasman. Formules explicites pour le nombre de points des varietes sur un corps fini. *J. Reine Angew. Math.*, 493:1–60, 1997.

[Mat80] H. Matsumura. *Commutative Algebra*. Math Lecture Notes Series. Benjamin/Cummings Publishing Company, 1980.

[Maz78] Barry Mazur. Modular curves and the Eisenstein ideals. *Publ. Math. IHES*, 47:33–186, 1978.

[Mer96] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Inventiones mathematicae*, 124(1):437–449, Feb 1996.

[Pal10] Ambrus Pal. On the torsion of drinfeld modules of rank two. *Journal fur die reine und angewandte Mathematik*, (640):1–45, 2010.

[Par99] Pierre Parent. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *Journal fur die reine und angewandte Mathematik (Crelles Journal)*, pages 85–116, 1999.

[Pin12] R. Pink. Lectures on Drinfeld modules. `https://typo.iwr.uni-heidelberg.de/fileadmin/groups/arithgeo/templates/data/Yujia_Qiu/dm/Pink-Drinfeld_modules_2012_08_24.pdf`, 2012.

[Poo95] Bjorn Poonen. Local height functions and the mordell-weil theorem for Drinfeld modules. *Compositio Mathematica*, (97):349–368, 1995.

[Poo97] Bjorn Poonen. Torsion in rank 1 Drinfeld modules and the uniform boundedness conjecture. *Mathematische Annalen*, (308):571–586, 1997.

[Poo17] B. Poonen. Introduction to Drinfeld modules. `http://www-math.mit.edu/~poonen/papers/drinfeld.pdf`, 2017.

[Rei03] I. Reiner. *Maximal Orders*. London Mathematical Society monographs series: London Mathematical Society. Clarendon Press, 2003.

[Ros87] Michael Rosen. The Hilbert class field in function fields. *Exposition. Math.*, (5):365–378, 1987.

[Ros02] Michael Rosen. *Number Theory in Function Fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 2002.

[Sal06] Gabriel Salvador. *Topics in the theory of algebraic function fields*. Birkhäuser, Boston Berlin, 2006.

[Sch03] Andreas Schweizer. On the uniform boundedness conjecture for drinfeld modules. *Mathematische Zeitschrift*, 244(3):601–614, Jul 2003.

[Sil94] Joseph Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate texts in mathematics. Springer-Verlag, 1994.

[Sta19] The Stacks project authors. The stacks project. `https://stacks.math.columbia.edu`, 2019.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*. Springer, Berlin, 2009.