T2R2 東京工業大学リサーチリポジトリ
Tokyo Tech Research Repository

論文 / 著書情報
Article / Book Information

題目(和文)	Rasmussen-Tamagawa予想のDrinfeld加群類似
Title(English)	A Drinfeld module analogue of the Rasmussen-Tamagawa conjecture
著者(和文)	奥村喜晶
Author(English)	Yoshiaki Okumura
出典(和文)	学位:博士(理学), 学位授与機関:東京工業大学, 報告番号:甲第11035号, 授与年月日:2019年3月26日, 学位の種別:課程博士, 審査員:田口 雄一郎,加藤 文元,内藤 聡,鈴木 正俊,馬 昭平
Citation(English)	Degree:Doctor (Science), Conferring organization: Tokyo Institute of Technology, Report number:甲第11035号, Conferred date:2019/3/26, Degree Type:Course doctor, Examiner:,,,,
学位種別(和文)	博士論文
Type(English)	Doctoral Thesis

Powered by T2R2 (Tokyo Institute Research Repository)

A Drinfeld module analogue of the Rasmussen-Tamagawa conjecture

(Rasmussen-Tamagawa 予想の Drinfeld 加群類似)

Yoshiaki Okumura

(奥村 喜晶)

Tokyo Institute of Technology

A thesis submitted for the degree of
Doctor of Science

February 26, 2019

This thesis is dedicated to my parents
Hiroki Okumura and Mieko Okumura.

Abstract

In the arithmetic of function fields, Drinfeld modules play the role that elliptic curves do in the arithmetic of number fields. The aim of this thesis is to study a non-existence problem of Drinfeld modules with constrained torsion points at places with large degree, which is motivated by a conjecture of Christopher Rasmussen and Akio Tamagawa related with abelian varieties over number fields with some arithmetic constraints. We prove the non-existence of Drinfeld modules in the case where the inseparable degree of base fields is not divisible by the rank of Drinfeld modules. In other cases, we conversely give an example of Drinfeld modules satisfying Rasmussen-Tamagawa-type conditions.

This thesis is submitted to Tokyo Institute of Technology for the degree of Doctor of Science. Several results in the thesis are contained in the author's previous paper [Oku], which will be published in Kyushu Journal of Mathematics, published by Faculty of Mathematics Kyushu University.

Acknowledgments

The author's first and greatest thanks goes to his supervisor Yuichiro Taguchi. The author would like to thank him for providing the interesting topic and for his guidance in preparing this thesis. His teaching has been most important during these few years.

The author is greatly indebted to Akio Tamagawa for providing his idea to construct examples in Propositions 6.1.4 and 6.2.4. The author also would like to thank Yoshiyasu Ozeki for his helpful comments on Proposition 3.3.6.

Finally the author would like to acknowledge everyone who directly or indirectly influence this thesis.

Contents

Chapter 1

Introduction

The aim of this thesis is to formulate a function field[1] analogue of a conjecture of Rasmussen and Tamagawa [RT08] on certain abelian varieties over number fields and to give some results on it. It is known that there are beautiful analogies between the arithmetic of number fields and the arithmetic of function fields. In 1974, Drinfeld [Dri74] invented the analog of elliptic curves under the name "elliptic modules". These are today called *Drinfeld modules*, see Chapter 2. In this thesis, following the philosophy about analogies between number fields and function fields, we consider a non-existence problem on Drinfeld modules of "Rasmussen-Tamagawa type".

In the arithmetic of number fields, problems of finiteness or non-existence of isomorphism classes of various number theoretic objects have been studied by many people. For example, the Hermite-Minkowski theorem, which is a famous arithmetic result, says that there exist only finitely many isomorphism classes of number fields with given degree and ramification set of places. As a generalization of the Hermite-Minkowski theorem, Faltings [Fal83] proved the Shafarevich conjecture, which is as follows: there exist only finitely many isomorphism classes of abelian varieties over a number field with a give dimension, polarization of a give degree, and good reduction outside a give set of places. Furthermore, Zarhin improved Faltings' result by omitting the assumption on polarization in [Zar85].

A conjecture of Rasmussen and Tamagawa is in the spirit of the Shafarevich conjecture. Inspired by the study of a question of Ihara [Iha86] related with the kernel of the canonical outer Galois representation of the pro-ℓ fundamental group of $\mathbb{P}^1\backslash\{0,1,\infty\}$, Rasmussen and Tamagawa define a

[1] In this thesis, a "function field" always means a finitely generated field of transcendental degree one over a finite field.

set $\mathscr{A}(k,g,\ell)$ of k-isomorphism classes of g-dimensional abelian varieties over a number field k with constrained ℓ-power torsion points for a prime number ℓ. We can easily see that the set $\mathscr{A}(k,g,\ell)$ is finite by the Shafarevich conjecture. Rasmussen and Tamagawa conjectured that such a finiteness also should hold for the union $\mathscr{A}(k,g) := \cup_\ell \mathscr{A}(k,g,\ell)$ of these sets, where ℓ runs through all prime numbers. In other word, the Rasmussen-Tamagawa conjecture says that there is a positive constant $C = C(k,g) > 0$ depending only on k and g such that $\mathscr{A}(k,g,\ell)$ is empty for all $\ell > C$.

There are some results on the conjecture, see §§3.2.2. For example, Rasmussen and Tamagawa [RT08] prove that the conjecture is true for elliptic curves over $\mathbb{Q}$. However, it remains open in general. We notice that, under the assumption of the Generalized Riemann Hypothesis (GRH) for Dedekind zeta functions of number fields, the conjecture is true in general [RT17, Theorem 5.1]. The key tool of this proof is the effective version of the Chebotarev density theorem for number fields, which holds under GRH. Rasmussen and Tamagawa also state the "uniform version" of the conjecture [RT17, Conjecture 2], which says that one can take a lower bound of ℓ satisfying $\mathscr{A}(k,g,\ell) = \varnothing$ depending only on the degree $[k : \mathbb{Q}]$ and g. For instance, the uniform version of the conjecture for CM abelian varieties is proved by Bourdon [Bou15, Corollary 1] and Lombardo [Lom, Theorem 1.3]. Under GRH, the uniform version of the conjecture is true if $[k : \mathbb{Q}]$ is odd [RT17, Theorem 5.2].

Now let us state main results in this thesis. We first introduce some notations. Let p be a prime number and fix some p-power $q = p^\nu$. Write $A := \mathbb{F}_q[t]$ for the polynomial ring in one variable t over $\mathbb{F}_q$ and set $F := \mathbb{F}_q(t)$. In the arithmetic of function fields, the ring A and the field F are analogues of $\mathbb{Z}$ and $\mathbb{Q}$, respectively. Let K be a finite extension of F. In this thesis, we often identify every monic irreducible element $\pi \in A$ with the corresponding finite place of F. Write $\mathbb{F}_\pi = A/\pi A$ for the residue field at π and set $q_\pi := \#\mathbb{F}_\pi = q^{\deg(\pi)}$.

The arithmetic properties of Drinfeld modules over function fields are similar to those of elliptic curves over number fields. For instance, there are reduction theory and Galois representations attached to torsion points of Drinfeld modules, see Chapter 2 for details. Under this analogy, we can define the analogue of $\mathscr{A}(k,g,\ell)$. Let r be a positive integer and $\pi \in A$ a monic irreducible element. Define $\mathscr{D}(K,r,\pi)$ to be the set of K-isomorphism classes $[\phi]$ of Drinfeld modules ϕ of rank r over K which satisfy the following two conditions:

(D1) ϕ has good reduction at any finite place of K not lying above π,

(D2) the mod π representation $\bar{\rho}_{\phi,\pi} : G_K \to \mathrm{GL}_r(\mathbb{F}_\pi)$ attached to ϕ is of the form

$$\bar{\rho}_{\phi,\pi} \simeq \begin{pmatrix} \chi_\pi^{i_1} & * & \cdots & * \\ & \chi_\pi^{i_2} & \ddots & \vdots \\ & & \ddots & * \\ & & & \chi_\pi^{i_r} \end{pmatrix},$$

where χ_π is the *mod π Carlitz character* (Definition 2.5.4) and $0 \leq i_1, \ldots, i_r < q_\pi - 1$ are integers.

Proposition 3.3.6 in Chapter 3 means that the condition (D1)+(D2) is a Drinfeld module analogue of the defining condition of the set $\mathscr{A}(k, g, \ell)$. See also Proposition 3.2.1. The purpose of this thesis is to give a complete answer to the following question:

Question 1.0.1. *Does there exist a positive constant $C > 0$ depending only on K q, and r which satisfies the following: if $\deg(\pi) > C$, then the set $\mathscr{D}(K, r, \pi)$ is empty?*

We show that the answer to the question is YES if r does not divide the inseparable degree $[K : F]_{\mathrm{i}}$ of K/F:

Theorem 1.0.2 (Theorem 4.3.9 (2) and Theorem 5.4.4)**.** *Suppose that r does not divide $[K : F]_{\mathrm{i}}$. Then the set $\mathscr{D}(K, r, \pi)$ is empty for any monic irreducible element $\pi \in A$ whose degree is large enough.*

The proof of Theorem 1.0.2 consists of the two cases: (i) $r = p^\nu$, and (ii) $r = r_0 p^\nu$ for some $r_0 > 1$ which is prime to p. The proof in the case (i) is provided by observations about the *tame inertia weights* (Definition 4.1.4) of $\bar{\rho}_{\phi,\pi}$ for any $[\phi] \in \mathscr{D}(K, r, \pi)$. This technique is used in [Oze11] and [RT17]. In the case (ii), we employ the strategy in [RT17] and use the effective version of the Chebotarev density theorem for function fields proved by Kumer and Scherk [KS94]. We notice that the same argument dose not work well in the case (i).

In addition, as an analogue of [RT17, Theorem 5.2], we obtain a uniform result as follows:

Theorem 1.0.3 (Corollary 4.3.5 and Theorem 5.4.5)**.** *Let r and π be as above. Let n be a positive integer not divisible by r. Then there exists a positive constant $C > 0$ determined by r, q, and n such that for all finite extensions K/F of degree n, the set $\mathscr{D}(K, r, \pi)$ is empty if $\deg(\pi) > C$.*

On the other hand, there are differences between the number field setting and the function field setting. Indeed, if r divides $[K : F]_{\mathrm{i}}$ (for which there is no number field setting), then we construct a Drinfeld module Φ of rank r over K satisfying (D1) and (D2) for all monic irreducible elements $\pi \in A$. Namely the following holds:

Theorem 1.0.4 (Theorem 6.1.1)**.** *If r divides $[K : F]_{\mathrm{i}}$, then the set $\mathscr{D}(K, r, \pi)$ is never empty for any π.*

Consequently we obtain a complete answer to Question 1.0.1 by Theorem 1.0.2 and Theorem 1.0.4.

The organization of the thesis is as follows. In Chapter 2, after reviewing several basic facts on function fields, we introduce well-known facts on Drinfeld modules. In Chapter 3, we explain a motivation of the Rasmussen-Tamagawa conjecture and the precise statement of it. After that, we define the set $\mathscr{D}(K, r, \pi)$. In Chapter 4, for any $[\phi] \in \mathscr{D}(K, r, \pi)$, an important integer $e_{\pi}(\phi)$ is introduced and we prove some non-trivial properties of it. Using it, we give some non-existence results on certain Drinfeld modules and prove Theorem 1.0.2 in the case (i). The aim of Chapter 5 is to give the proof of Theorem 1.0.2 in the case (ii). Finally, in Chapter 6, we construct a Drinfeld module satisfying both (D1) and (D2) for any π in the case where r divides $[K : F]_{\mathrm{i}}$. We also show that the set $\mathscr{D}(K, r, \pi)$ is infinite if $\pi = t$ and $r \geq 2$.

Notation

For an arbitrary field $\mathcal{F}$, write $G_{\mathcal{F}} = \mathrm{Gal}(\mathcal{F}^{\mathrm{sep}}/\mathcal{F})$ for the absolute Galois group of $\mathcal{F}$. Throughout this thesis, we denote by

$\mathbb{F}_q$	the finite field of q elements of characteristic p,
A	$:= \mathbb{F}_q[t]$,
F	$:= \mathbb{F}_q(t)$,
$\mathbb{F}_\pi$	$:= A/\pi A$; the residue field at a monic irreducible element $\pi \in A$,
q_π	$:= \#\mathbb{F}_\pi = q^{\deg(\pi)}$.

For a finite extension K of F and a place u of K, we denote by

K_{s}	the separable closure of F in K,
K_u	the completion of K at u,
$\mathcal{O}_{K_u}$	the valuation ring of K_u with the maximal ideal $\mathfrak{p}_u$,
$\mathbb{F}_u$	the residue field of K_u,
q_u	$:= \#\mathbb{F}_u$.

We use the same symbol u for the normalized valuation of K_u. Identify G_{K_u} with the decomposition group of G_K at u and regard it as a subgroup of G_K. Denote by I_{K_u} the inertia subgroup of G_{K_u} at u and choose a lift $\mathrm{Frob}_u \in G_{K_u}$ of the Frobenius element of G_{K_u}/I_{K_u}. If π is the place of F below u, then we denote by $e_{u|\pi}$ (or $e(K_u/F_\pi)$) the ramification index and set $f_{u|\pi} := [\mathbb{F}_u : \mathbb{F}_\pi]$.

Let $F_\infty := \mathbb{F}_q((1/t))$ be the completion of F at the place ∞ of F corresponding to the $(1/t)$-adic valuation of F. Write $\mathbb{C}_\infty$ for the completion of a fixed algebraic closure of F_∞. Every algebraic extension of F is always regarded as a subfield of $\mathbb{C}_\infty$. Let $|\cdot|$ be the absolute value of F_∞ attached to the normalized valuation of F_∞. We also denote by $|\cdot|$ the unique extension of it to $\mathbb{C}_\infty$ and its restriction to each algebraic extension of F. For any non-zero $a \in A$, we see that $|a| = \#(A/aA) = q^{\deg(a)}$.

The notation $C = C(x, y, \dots, z)$ indicates a constant C depending only on $x, y, \dots,$ and z. We use the notation ρ^{ss} for the semisimplification of a linear representation of a group ρ.

Chapter 2

Preliminaries

Drinfeld modules are introduced by V. G. Drinfeld [Dri74] to prove the Langlands conjecture for $\mathrm{GL}(2)$ over function fields. In this chapter, we review several well-known results on Drinfeld modules and see that there are various analogies between the arithmetic properties of Drinfeld modules and that of elliptic curves. Our exposition of the theory of function fields and Drinfeld modules follows [Dri74], [Hay74],[Gos96], and [Ros02].

After recalling basic facts in the arithmetic of function fields in §2.1, we introduce the definition of Drinfeld modules and study torsion points of them in §2.2. In §2.3, we first introduce the notion of good and stable reduction of Drinfeld modules. For a monic irreducible element $\pi \in A$, we also define Galois representations attached to π-adic Tate modules and π-torsion points of Drinfeld modules. The purpose of §2.4 is to explain Drinfeld's theorem on Tate uniformization, which gives an analytic description of Drinfeld modules with stable reduction. In the final section §2.5, we define the Carlitz module and recall the properties of cyclotomic function fields.

2.1 Function field arithmetic

We summarize some basic arithmetic facts on function fields and introduce further notations and conventions used in this thesis.

The rational function field $F = \mathbb{F}_q(t)$ has two kinds of places — places corresponding to monic irreducible elements of A and ∞. In this thesis, we often identify every monic irreducible element $\pi \in A$ with the corresponding place of F and use the same symbol "π".

Definition 2.1.1. Let K/F be a finite extension and v a place of K. We say that v is a *finite place* if it lies above some monic irreducible element $\pi \in A$, and that v is an *infinite place* if it lies above ∞.

Definition 2.1.2. Let $L/K/F$ be algebraic extensions.

(1) The algebraic closure of $\mathbb{F}_q$ in K is called the *constant field* of K and we denote it by $\mathbb{F}_K$.

(2) We say that L/K is a *constant field extension* if $L = \mathbb{F}_L K$, and that L/K is a *geometric extension* if $\mathbb{F}_L = \mathbb{F}_K$.

In general, the composite field $\mathbb{F}_L K$ is the maximal constant extension of K in L and clearly L is a geometric extension of $\mathbb{F}_L K$. If L/K is finite, then we define the *geometric extension degree* of L/K by $[L : K]_{\mathrm{g}} := [L : \mathbb{F}_L K]$.

Example 2.1.3. Let $\mathfrak{n} \in A$ be a non-zero element. Then the "cyclotomic function field" $F(\zeta_{\mathfrak{n}})$ defined in §1.4 is geometric over F (see Corollary 2.5.8).

Fix a finite extension K of F.

Proposition 2.1.4. *Let L/K be a finite extension.*

(1) *If L/K is a constant field extension, then it is unramified at all places.*

(2) *If L/K is a purely inseparable extension, then it is totally ramified at all places.*

Proof. See [Ros02, Proposition 7.5] and [Ros02, Proposition 8.5]. □

Remark 2.1.5. Proposition 2.1.4 implies that every purely inseparable extension L/K is geometric.

Proposition 2.1.6. *Let L/K be a finite extension. Suppose that v is a place of K and $\{w_1, \ldots, w_r\}$ the set of places of L above v. Then the equation*

$$[L : K] = \sum_{s=1}^{r} e_{w_s|v} f_{w_s|v}$$

holds.

Proof. See [Ros02, Theorem 7.6]. □

2.2 Drinfeld modules

Let K be an $\mathbb{F}_q$-algebra and let $\mathbb{G}_{a,K}$ be the additive group scheme defined over K. Write τ for the q-power Frobenius map of $\mathbb{G}_{a,K}$. Then the ring $\mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,K})$ of $\mathbb{F}_q$-linear endomorphisms of $\mathbb{G}_{a,K}$ is the non-commutative polynomial ring

$$K\{\tau\} := \left\{ \mu = \sum_{s=0}^{r} c_s \tau^s \ ; \ r \in \mathbb{Z}_{\geq 0} \text{ and } c_s \in K \right\}$$

in one variable τ satisfying $\tau c = c^q \tau$ for any $c \in K$. Denote by

$$K\langle T\rangle := \left\{ f(T) \in K[T]; f(T) = \sum_{s=0}^{r} c_s T^{q^s} \right\}$$

the set of $\mathbb{F}_q$-linear additive polynomials. Define its multiplication by composition

$$f(T) \circ g(T) = f(g(T))$$

of polynomials. Then $K\langle T\rangle$ is a non-commutative ring and $K\{\tau\} \cong K\langle T\rangle$ by the correspondence $\tau^s \mapsto T^{q^s}$.

Definition 2.2.1. An *A-field* is a field K equipped with an $\mathbb{F}_q$-algebra homomorphism $\iota : A \to K$. The kernel $\mathfrak{p} = \ker \iota$ is called the *A-characteristic* of K.

Remark 2.2.2. In this thesis, we only consider A-fields with A-characteristic $\mathfrak{p} = (0)$.

Drinfeld modules are given as group schemes endowed with some A-module structures.

Definition 2.2.3. Let (K, ι) be an A-field and r a positive integer. A *Drinfeld module* ϕ of rank r defined over K is an $\mathbb{F}_q$-algebra homomorphism

$$\begin{array}{rccc} \phi : & A & \to & K\{\tau\} \\ & a & \mapsto & \phi_a \end{array}$$

such that $\phi_t = \iota(t) + c_1\tau + \cdots + c_r\tau^r \in K\{\tau\}$ with $c_r \neq 0$.

Let $\mathfrak{p}$ be the A-characteristic of K. If $\mathfrak{p} = (0)$ (resp. $\mathfrak{p} \neq (0)$), then ϕ is said to be of *generic characteristic* (resp. *special characteristic*).

Remark 2.2.4. Since $\phi : A \to K\{\tau\}$ is an $\mathbb{F}_q$-algebra homomorphism, it is completely determined by $\phi_t \in K\{\tau\}$.

Throughout this thesis, we always assume that Drinfeld modules are of generic characteristic, that is, assume that any A-field structure $\iota : A \to K$ is injective.

Remark 2.2.5. (1) More generally, let R be an A-algebra and let $\iota : A \to R$ be its A-algebra structure. Then a Drinfeld module over R is defined to be an $\mathbb{F}_q$-algebra homomorphism $\phi : A \to R\{\tau\}$ such that

$$\phi_t = \iota(t) + c_1\tau + \cdots + c_r\tau^r \in R\{\tau\} \text{ with } c_r \in R^\times.$$

(2) Drinfeld modules are defined in a more general setting: let X be a smooth projective, geometrically irreducible curve over $\mathbb{F}_q$. Let $\infty \in X$ be a fixed closed point and let $\mathcal{A} := \Gamma(X \backslash \{\infty\}, \mathcal{O}_X)$ be the $\mathbb{F}_q$-algebra of rational functions on X which are regular outside ∞. Then a Drinfeld $\mathcal{A}$-module defined over an $\mathcal{A}$-field $(K, \iota : \mathcal{A} \to K)$ is an $\mathbb{F}_q$-algebra homomorphism $\phi : \mathcal{A} \to K\{\tau\}$ satisfying $\phi_a = \iota(a) + \sum_{s=1}^{n} c_s\tau^s$ for any $a \in \mathcal{A}$ and $\phi_a \neq \iota(a)$ for some $a \in \mathcal{A}$.

Let K be an A-field.

Definition 2.2.6. A *homomorphism* $\mu : \phi \to \psi$ between two Drinfeld modules over K is an element $\mu \in K\{\tau\}$ such that

$$\mu\phi_a = \psi_a\mu$$

for any $a \in A$. Namely μ makes the following diagram commutative

$$\begin{array}{ccc} \mathbb{G}_{a,K} & \xrightarrow{\mu} & \mathbb{G}_{a,K} \\ \downarrow{\scriptstyle \phi_a} & & \downarrow{\scriptstyle \psi_a} \\ \mathbb{G}_{a,K} & \xrightarrow[\mu]{} & \mathbb{G}_{a,K} \end{array}$$

for any $a \in A$.

A non-zero homomorphism $\mu : \phi \to \psi$ is called an *isogeny* and then ϕ and ψ are said to be *isogenous*. We say that μ is an *isomorphism* if it is an isomorphism of group schemes. It is easily seen that μ is an isomorphism if and only if $\mu \in K^\times$. Hence every Drinfeld module ψ which is isomorphic to ϕ is given by $\psi_t = c^{-1}\phi_t c$ for some $c \in K^\times$.

For a Drinfeld module $\phi : A \to K\{\tau\}$, denote by

$$\mathrm{End}_K(\phi) = \{\mu \in K\{\tau\}; \mu\phi_a = \phi_a\mu \text{ for any } a \in A\}$$

the ring of endomorphisms of ϕ over K. Clearly $\phi_a \in \mathrm{End}_K(\phi)$ for any $a \in A$ and thus we have an embedding $A \hookrightarrow \mathrm{End}_K(\phi)$. Suppose that ϕ is of rank r. Since we now assume that ϕ is of generic characteristic, it follows that $\mathrm{End}_K(\phi)$ is a commutative A-algebra and free of finite rank $\leq r$ as an A-module by [Dri74, Corollary of Proposition 2.4].

Definition 2.2.7. We say that a Drinfeld module $\phi : A \to K\{\tau\}$ of rank r has *complex multiplication* if $\mathrm{End}_K(\phi)$ is isomorphic, as an A-algebra, to an A-order $\mathcal{O}$ of a finite extension E of F with $[E : F] = r$.

Example 2.2.8. For a rank-two Drinfeld module $\phi : A \to K\{\tau\}$ determined by $\phi_t = \iota(t) + \lambda\tau + \Delta\tau^2$, the *j-invariant* of ϕ is defined by

$$j(\phi) := \frac{\lambda^{q+1}}{\Delta}.$$

It is known that rank-two Drinfeld modules ϕ and ψ over K are isomorphic over $\bar{K}$ if and only if $j(\phi) = j(\psi)$.

Let $\sqrt{t} \in \bar{F}$ be a square root of $t \in F$. Regard $\bar{F}$ as an A-field by the canonical inclusion $A \hookrightarrow F \subset \bar{F}$. Let $\phi : A \to \bar{F}\{\tau\}$ be the Drinfeld module of rank two determined by

$$\phi_t = (\sqrt{t} + \tau)(\sqrt{t} + \tau) = t + (\sqrt{t} + \sqrt{t}^q)\tau + \tau^2.$$

Clearly $\mu := \sqrt{t} + \tau \in \mathrm{End}_{\bar{F}}(\phi)$ and $\mu^2 = \phi_t$, so that the ring $A[\sqrt{t}]$ injects into $\mathrm{End}_{\bar{F}}(\phi)$. Since $A[\sqrt{t}]$ is a maximal A-order of the quadratic extension $E = F(\sqrt{t}) = \mathbb{F}_q(\sqrt{t})$ of F, we see that $A[\sqrt{t}] \cong \mathrm{End}_{\bar{F}}(\phi)$ and so ϕ has complex multiplication. Suppose that q is odd. Then the j-invariant of ϕ is

$$j := j(\phi) = t^{\frac{q+1}{2}}(1 + t^{\frac{q-1}{2}})^{q-1} \in F.$$

The Drinfeld module ψ determined by

$$\psi_t = t + j\tau + j^q\tau^2$$

is defined over F and its j-invariant is $j(\psi) = j$. Hence $\phi \cong \psi$ over $\bar{F}$. Namely ϕ has a model defined over F. This is the analogue of the fact that an elliptic curve with complex multiplication by the ring of integer of an imaginary quadratic field with class number one can be defined over $\mathbb{Q}$.

Let $\phi : A \to K\{\tau\}$ be a Drinfeld module. For any K-algebra Ω, by definition ϕ endows the additive group $\mathbb{G}_{a,K}(\Omega) = \Omega$ with a new A-module structure defined by $a \cdot \lambda := \phi_a(\lambda)$ for any $\lambda \in \Omega$ and $a \in A$. Denote by

${}_{\phi}\Omega$ this A-module. Clearly any homomorphism $\mu : \phi \to \psi$ between two Drinfeld modules ϕ and ψ over K induces an A-module homomorphism $\mu : {}_{\phi}\Omega \to {}_{\psi}\Omega$.

In the case where $\Omega = \bar{K}$, for any non-zero element $a \in A$, we define the set of *a-torsion points* of ϕ by

$$\phi[a] = \{\lambda \in {}_{\phi}\bar{K}; \phi_a(\lambda) = 0\},$$

which is a finite torsion A-submodule of ${}_{\phi}\bar{K}$. Since ϕ is now of generic characteristic, it follows that ϕ_a is separable as an additive polynomial in $K\langle T\rangle$. Hence $\phi[a]$ is in fact a finite torsion A-submodule of ${}_{\phi}K^{\mathrm{sep}}$ and hence the absolute Galois group G_K of K canonically acts on it. Clearly the field $K(\phi[a])$ generated by all a-torsion points of ϕ is a finite Galois extension of K. If ϕ is of rank r, then

$$\phi[a] \cong (A/aA)^{\oplus r}$$

as an A-module by [Ros02, Proposition 12.4]. Thus the G_K-action on $\phi[a]$ induces an injective homomorphism

$$\mathrm{Gal}(K(\phi[a])/K) \hookrightarrow \mathrm{Aut}_{A/aA}(\phi[a]) \cong \mathrm{GL}_r(A/aA).$$

In particular, if ϕ is of rank one, then $K(\phi[a])/K$ is an abelian extension.

2.3 Reduction theory and Galois representations

From now on, unless otherwise stated, we always regard any extension field $\mathcal{F}$ of F as an A-field via the inclusion $A \hookrightarrow F \subset \mathcal{F}$. We often consider the case where $\mathcal{F}$ is a finite extension of F or its completion.

In this section, denote by K a finite extension of F.

Definition 2.3.1. Let v be a finite place of K.

(1) We say that a Drinfeld module $\phi : A \to K_v\{\tau\}$ of rank r over K_v has *stable reduction* if ϕ is K_v-isomorphic to a Drinfeld module $\psi : A \to K_v\{\tau\}$ satisfying

$$\psi_t = t + c'_1\tau + \cdots + c'_r\tau^r \in \mathcal{O}_{K_v}\{\tau\} \text{ and } c'_{r'} \in \mathcal{O}_{K_v}^{\times}$$

for some $1 \leq r' \leq r$. In particular if $c'_r \in \mathcal{O}_{K_v}^{\times}$, then we say that ϕ has *good reduction*.

(2) We say that a Drinfeld module $\phi : A \to K\{\tau\}$ over K has *stable reduction* (resp. *good reduction*) at v if $\phi : A \to K\{\tau\} \subset K_v\{\tau\}$, considered as a Drinfeld module over K_v, has stable reduction (resp. good reduction) in the above sense.

Suppose that $\phi : A \to K\{\tau\}$ has stable reduction at v. As in the notations in Definition 2.3.1, the integer $\max\{s; c'_s \in \mathcal{O}_{K_v}^{\times}\}$ is called the *stable rank* of ϕ. By definition ϕ has good reduction if and only if its stable rank is equal to the rank of ϕ.

Remark 2.3.2. By Remark 2.2.5 (1), any Drinfeld module defined over $\mathcal{O}_{K_v}$ has good reduction since its rank and stable rank are equal.

Remark 2.3.3. On the other hand, let v_∞ be an infinite place of K, that is, a place above ∞. Then for any Drinfeld module $\phi : A \to K_{v_\infty}\{\tau\}$, the constant term of ϕ_t is t by definition and $v_\infty(t) < 0$. Hence there is no Drinfeld module ϕ with $\phi_t \in \mathcal{O}_{K_{v_\infty}}\{\tau\}$.

It is known that every Drinfeld module has potentially stable reduction.

Proposition 2.3.4. *Let v be a finite place of K and let $\phi : A \to K_v\{\tau\}$ be a Drinfeld module of rank r. Then there is a finite extension L/K_v such that $\phi : A \to K_v\{\tau\} \subset L\{\tau\}$ has stable reduction. Moreover we can choose such an L which is a finite separable extension with $e(L/K_v) \mid (q^s - 1)$ for some $1 \le s \le r$.*

Remark 2.3.5. It follows by Proposition 2.3.4 that every Drinfeld module $\phi : A \to K_v\{\tau\}$ over K_v of rank r has stable reduction over a finite separable extension L/K_v whose ramification index is a divisor of the integer $\prod_{s=1}^{r}(q^s - 1)$ depending only on r and q.

Proof of Proposition 2.3.4. Write $\phi_t = t + c_1\tau + \cdots + c_r\tau^r \in K_v\{\tau\}$ and choose an integer $1 \le r' \le r$ such that

$$\frac{v(c_{r'})}{q^{r'} - 1} \le \frac{v(c_s)}{q^s - 1} \tag{2.3.1}$$

for all $1 \le s \le r$.

Take [1]a finite separable extension L of K_v with $e(L/K_v) = q^{r'} - 1$. Let w be the normalized valuation of L. Take an element $\theta \in L$ with $w(\theta) = -v(c_{r'})$ and consider the Drinfeld module $\psi : A \to L\{\tau\}$ determined by

$$\psi_t = \theta^{-1}\phi_t\theta = t + \theta^{q-1}c_1\tau + \theta^{q^2-1}c_2\tau^2 + \cdots + \theta^{q^r-1}c_r\tau^r.$$

[1]For example, for a uniformizer $\varpi \in K_v$, since $T^{q^{r'}-1} - \varpi \in K_v[T]$ is an Eisenstein polynomial and $q^{r'} - 1$ is not divisible by p, the extension $L = K_v(\varpi^{1/q^{r'}-1})$ is separable and totally tamely ramified with ramification index $q^{r'} - 1$ over K_v.

It is isomorphic to ϕ over L. For any $1 \leq s \leq r$, the inequality (2.3.1) implies

$$\begin{aligned} w(\theta^{q^s-1}c_s) &= (q^s-1)w(\theta)+w(c_s) \\ &= -(q^s-1)v(c_{r'})+e_{w|v}v(c_s) \\ &= (q^s-1)\left(-v(c_{r'})+(q^{r'}-1)\frac{v(c_s)}{q^s-1}\right) \\ &\geq (q^s-1)\left(-v(c_{r'})+(q^{r'}-1)\frac{v(c_{r'})}{q^{r'}-1}\right)=0. \end{aligned}$$

Thus we see that $\psi_t \in O_L\{\tau\}$ and $w(\theta^{q^{r'}-1}c_{r'}) = 0$. Hence ϕ has stable reduction over L. □

Remark 2.3.6. In particular, every rank-one Drinfeld module has potentially good reduction at all finite places.

Let $\phi : A \to K\{\tau\}$ be of rank r. For any monic irreducible element $\pi \in A$, the set of π-torsion points $\phi[\pi]$ is a G_K-stable r-dimensional $\mathbb{F}_\pi$-vector space. Thus it carries an $\mathbb{F}_\pi$-linear representation

$$\bar{\rho}_{\phi,\pi} : G_K \to \mathrm{Aut}_{\mathbb{F}_\pi}(\phi[\pi]) \simeq \mathrm{GL}_r(\mathbb{F}_\pi)$$

describing the G_K-action on $\phi[\pi]$. It is called the *mod π-representation* attached to ϕ.

Theorem 2.3.7 (Pink and Rütsche)**.** *Let $\phi : A \to K\{\tau\}$ be a Drinfeld module with $\mathrm{End}_K(\phi) = A$. Then the mod π representation $\bar{\rho}_{\phi,\pi}$ is absolutely irreducible*[2] *for almost all monic irreducible elements $\pi \in A$.*

Proof. It follows from [PR09a, Theorem 4.1]. □

Remark 2.3.8. By contrast, for any Drinfeld module ϕ with $\mathrm{End}_K(\phi) \neq A$ and any monic irreducible element $\pi \in A$, the mod π representation $\bar{\rho}_{\phi,\pi}$ is never absolutely irreducible.

For any positive integer n, the map $\phi[\pi^{n+1}] \to \phi[\pi^n]; \lambda \mapsto \phi_\pi(\lambda)$ is G_K-equivariant and $\{\phi[\pi^n]\}_{n\geq 1}$ becomes an inverse system. Write

$$A_\pi := \varprojlim_n A/\pi^n A$$

for the π-adic completion of A.

[2] We say that $\bar{\rho}_{\phi,\pi}$ is *absolutely irreducible if* $\bar{\rho}_{\phi,\pi} \otimes_{\mathbb{F}_\pi} \bar{\mathbb{F}}_\pi$ is irreducible.

Definition 2.3.9. The inverse limit

$$T_\pi(\phi) := \varprojlim_n \phi[\pi^n]$$

is called the *π-adic Tate module* of ϕ.

By construction, if ϕ is of rank r, then the π-adic Tate module $T_\pi(\phi)$ is a free A_π-module of rank r on which G_K acts continuously. Hence it carries a continuous Galois representation

$$\rho_{\phi,\pi} : G_K \to \mathrm{Aut}_{A_\pi}(T_\pi(\phi)) \cong \mathrm{GL}_r(A_\pi).$$

The next proposition is an analogue of the Néron-Ogg-Shafarevich criterion for good reduction of abelian varieties (cf. [ST68, Theorem 1]).

Proposition 2.3.10 (Takahashi [Tak82, Theorem 1])**.** *Let $\phi : A \to K\{\tau\}$ be a Drinfeld module and $\pi \in A$ a monic irreducible element. Let v be a finite place of K not lying above π. Then ϕ has good reduction at v if and only if $T_\pi(\phi)$ is unramified at v, that is, $\rho_{\phi,\pi}(I_{K_v}) = \{1\}$.*

Let $\pi \in A$ be a monic irreducible element and let v be a finite place of K not lying above π. Let $\phi : A \to K\{\tau\}$ be a Drinfeld module of rank r and assume that ϕ has good reduction at v. Since $\rho_{\phi,\pi}$ is unramified at v by Proposition 2.3.10, it follows that $\rho_{\phi,\pi}(\mathrm{Frob}_v) \in \mathrm{GL}_r(A_\pi)$ is independent of the choice of a lift Frob_v. Denote by

$$P_v(T) := \det(T - \rho_{\phi,\pi}(\mathrm{Frob}_v)|T_\pi(\phi)) \in A_\pi[T]$$

the characteristic polynomial of Frob_v. Then we have the following fact:

Proposition 2.3.11 (Takahashi [Tak82, Proposition 3 (ii)])**.** *Let ϕ, v and π be as above. Then the polynomial $P_v(T)$ has coefficients in A and is independent of π. Any root α of $P_v(T)$ satisfies $|\alpha| = q_v^{1/r}$.*

For a Drinfeld module $\phi : A \to K\{\tau\}$, denote by

$$\mathrm{End}_{\bar{K}}(\phi) := \{\mu \in \bar{K}\{\tau\};\ \mu\phi_a = \phi_a\mu \text{ for any } a \in A\}$$

the endomorphism ring of ϕ over $\bar{K}$. We have the following.

Theorem 2.3.12 (Pink and Rütsche)**.** *Let $\phi : A \to K\{\tau\}$ be a Drinfeld module with $\mathrm{End}_{\bar{K}}(\phi) = A$. Then for almost all monic irreducible elements $\pi \in A$, the representation $\rho_{\phi,\pi}$ is surjective.*

Proof. This is the special case of [PR09b, Theorem 0.1]. □

Remark 2.3.13. We see that the "reduction" of $\rho_{\phi,\pi}$ coincides with $\bar{\rho}_{\phi,\pi}$, that is, the projection $\mathrm{Aut}_{A_\pi}(T_\pi(\phi)) \twoheadrightarrow \mathrm{Aut}_{\mathbb{F}_\pi}(\phi[\pi])$ induced by the reduction map $A_\pi \twoheadrightarrow \mathbb{F}_\pi$ makes the following diagram commutative.

$$\begin{array}{ccc} G_K & \xrightarrow{\rho_{\phi,\pi}} & \mathrm{Aut}_{A_\pi}(T_\pi(\phi)) \\ & \searrow^{\bar{\rho}_{\phi,\pi}} & \downarrow \\ & & \mathrm{Aut}_{\mathbb{F}_\pi}(\phi[\pi]) \end{array}$$

Hence Theorem 2.3.12 implies that the mod π representation $\bar{\rho}_{\phi,\pi}$ is also surjective for all but finitely many π if $\mathrm{End}_{\bar{K}}(\phi) = A$. This is an analogue of Serre's classical result [Ser72] on the surjectivity of mod ℓ Galois representations attached to non-CM elliptic curves over number fields.

2.4 Tate uniformization

In this section, we see that every Drinfeld module over K_v with stable reduction can be constructed from a Drinfeld module with good reduction by dividing out a "lattice". We follows the expositions in [Dri74, §7] and [Leh09, Chapter 4 §3].

Let v be a finite place of a finite extension K of F. For a Drinfeld module $\psi : A \to K_v\{\tau\}$, consider the A-module ${}_\psi K_v^{\mathrm{sep}}$ and the metric on it determined by the normalized valuation of K_v^{sep}. A subset $\Lambda \subset {}_\psi K_v^{\mathrm{sep}}$ is said to be *discrete* if any ball of finite radius in ${}_\psi K_v^{\mathrm{sep}}$ contains only finitely many elements of Λ.

Let $\psi : A \to \mathcal{O}_{K_v}\{\tau\}$ be a Drinfeld module defined over $\mathcal{O}_{K_v}$. We notice that ψ has good reduction (see Remark 2.2.5 and Remark 2.3.2).

Definition 2.4.1. Let $\psi : A \to \mathcal{O}_{K_v}\{\tau\}$ be as above. A *ψ-lattice* is a finitely generated projective A-submodule $\Lambda \subset {}_\psi K_v^{\mathrm{sep}}$ such that

(1) Λ is discrete,

(2) Λ is stable under the G_{K_v}-action.

The *rank* of Λ is its rank as a projective A-module.

Remark 2.4.2. A ψ-lattice Λ is actually free of finite rank over A since A is a PID. Since Λ is finitely generated over A, it is contained in a finite separable extension of K_v. Hence the G_{K_v}-action on Λ factors through some finite quotient of G_{K_v}.

Definition 2.4.3. A *Tate datum* of rank (r_1, r_2) over $\mathcal{O}_{K_v}$ is a pair (ψ, Λ), where $\psi : A \to \mathcal{O}_{K_v}\{\tau\}$ is a Drinfeld module of rank r_1 and Λ is a ψ-lattice of rank r_2. The sum $r = r_1 + r_2$ is called the *total rank* of (ψ, Λ).

Let (ψ, Λ) and (ψ', Λ') be Tate data over $\mathcal{O}_{K_v}$. A *morphism* of Tate data $\mu : (\psi, \Lambda) \to (\psi', \Lambda')$ is a homomorphism $\mu : \psi \to \psi'$ of Drinfeld modules such that the induced A-module homomorphism

$$\mu : {}_{\psi}K_v^{\mathrm{sep}} \to {}_{\psi'}K_v^{\mathrm{sep}}$$

satisfies $\mu(\Lambda) \subset \Lambda'$. It is called an *isomorphism* if μ is an isomorphism of Drinfeld modules satisfying $\mu(\Lambda) = \Lambda'$.

Then we obtain the following "analytic" description of stable Drinfeld modules, so called *Tate uniformization*.

Proposition 2.4.4 (cf. [Dri74, Proposition 7.2] and [Leh09, Proposition 3.5])**.** *Let r_1 and r_2 be positive integers and set $r = r_1 + r_2$. Then the category of Tate data of total rank r over $\mathcal{O}_{K_v}$ is equivalent to the full subcategory of all Drinfeld modules of rank r over K_v consisting of those having stable reduction. Moreover there is a bijection between the following:*

(1) *The set of K_v-isomorphism classes of Drinfeld modules $\phi : A \to K_v\{\tau\}$ of rank r with stable reduction of stable rank r_1.*

(2) *The set of isomorphism classes of Tate data (ψ, Λ) of rank (r_1, r_2) over $\mathcal{O}_{K_v}$.*

Sketch of the proof of Proposition 2.4.4. We roughly explain the above correspondence. See [Dri74, §7] and [Leh09, Chapter 4] for details. Notice that the discreteness of ψ-lattices is needed to use some analytic arguments.

Let (ψ, Λ) be a Tate datum over $\mathcal{O}_{K_v}$ of rank (r_1, r_2) and consider the power series

$$e_\Lambda(T) = T \prod_{\lambda \in \Lambda \setminus \{0\}} \left(1 - \frac{T}{\lambda}\right).$$

It is an additive, $\mathbb{F}_q$-linear formal power series with $e_\Lambda \in K_v[[T]]$ and converges for all $\lambda \in K_v^{\mathrm{sep}}$ by [Gos96, Propositions 4.2.4 and 4.2.5]. Thus it can be regarded as an element of the non-commutative ring $K_v\{\{\tau\}\}$ of formal power series in τ over K_v. Then, for any $a \in A$, there is a unique $\phi_a \in K_v\{\tau\}$ satisfying

$$e_\Lambda \psi_a = \phi_a e_\Lambda.$$

These elements actually define a Drinfeld module $\phi : A \to K_v\{\tau\}$ of rank $r = r_1 + r_2$ with stable reduction of stable rank r_1.

Conversely, let $\phi : A \to K_v\{\tau\}$ be a Drinfeld module of rank $r = r_1 + r_2$ with stable reduction of stable rank r_1. After possibly replacing ϕ with a K_v-isomorphic Drinfeld module, we may assume that $\phi_a \in \mathcal{O}_{K_v}\{\tau\}$ for any $a \in A$. Then we see that there exist a unique Drinfeld module ψ defined over $\mathcal{O}_{K_v}$ of rank r_1 and a unique power series

$$\mu = 1 + \sum_{s=1}^{\infty} c_s \tau^s \in \mathcal{O}_{K_v}\{\{\tau\}\}$$

with $c_s \in \mathfrak{p}_v$ and $c_s \to 0$ (as $s \to \infty$) such that

$$\mu\psi_a = \phi_a \mu$$

for any $a \in A$. Then μ induces a surjective A-module homomorphism

$$\mu : {}_{\psi}K_v^{\mathrm{sep}} \twoheadrightarrow {}_{\phi}K_v^{\mathrm{sep}}$$

whose kernel $\Lambda := \ker \mu$ is a ψ-lattice of rank $r - r_1 = r_2$. □

Let (ψ, Λ) be a Tate datum corresponding to a stable Drinfeld module $\phi : A \to K_v\{\tau\}$ and let $\mu \in \mathcal{O}_{K_v}\{\{\tau\}\}$ be the power series as above. Let $a \in A$ has positive degree. Then ψ_a induces a surjective G_{K_v}-equivariant A-module homomorphism

$$\psi_a^{-1}(\Lambda)/\Lambda \to \Lambda/a\Lambda$$

whose kernel is $\psi_a^{-1}(0) = \psi[a]$. Since $\Lambda = \ker \mu$, we see that $\mu(\lambda) \in \phi[a]$ for any $a \in \psi_a^{-1}(\Lambda)$, so that $\psi_a^{-1}(\Lambda)/\Lambda \cong \phi[a]$. Therefore we get a G_{K_v}-equivariant short exact sequence

$$0 \to \psi[a] \to \phi[a] \to \Lambda/a\Lambda \to 0$$

of A-modules. Let $\pi \in A$ be a monic irreducible element. Then we also obtain a G_{K_v}-equivariant exact sequence

$$0 \to T_\pi(\psi) \to T_\pi(\phi) \to \Lambda \otimes_A A_\pi \to 0 \tag{2.4.1}$$

of A_π-modules.

We immediately obtain the following.

Proposition 2.4.5. *Let $\phi : A \to K\{\tau\}$ be a Drinfeld module over a finite extension K of F. Let $\pi \in A$ be a monic irreducible element and v a finite place of K. If v does not lie above π, then the I_{K_v}-action on $T_\pi(\phi)$ is potentially unipotent* [3].

[3] Namely there exists a finite extension L/K_v such that $\rho_{\phi,\pi}(\sigma) \in \mathrm{GL}_r(A_\pi)$ is a unipotent matrix for any $\sigma \in I_L$. See also §§ 3.3.1.

Proof. By Proposition 2.3.4, we may assume that $\phi : A \to K_v\{\tau\}$ has stable reduction. Then we have the exact sequence

$$0 \to T_\pi(\psi) \to T_\pi(\phi) \to \Lambda \otimes_A A_\pi \to 0$$

determined by the Tate datum (ψ, Λ) corresponding to ϕ. Since ψ has good reduction, its π-adic Tate module $T_\pi(\psi)$ is unramified at v by Proposition 2.3.10. We already see that the action of G_{K_v} on $\Lambda \otimes_A A_\pi$ is potentially unramified. Hence we get the conclusion by the above exact sequence and Lemma 3.3.2 in §§ 3.3.1. $\square$

Remark 2.4.6. By the theory of "analytic τ-sheaves"(see [Gar01], [Gar02] and [Gar03a]), the sequence (2.4.1) can be reinterpreted as follows. For any Drinfeld module ϕ over K_v, one can construct an analytic τ-sheaf $\tilde{M}(\phi)$ associated with ϕ. It is a locally free $\mathcal{O}_{\tilde{\mathbb{A}}^1_{K_v}}$-module of finite rank on $\tilde{\mathbb{A}}^1_{K_v}$ with some additional structures, where $\tilde{\mathbb{A}}^1_{K_v}$ is the rigid analytic space associated with the affine line $\mathbb{A}^1_{K_v} = \mathrm{Spec} A \times_{\mathrm{Spec} \mathbb{F}_q} \mathrm{Spec} K_v$. Then the π-adic Tate module $T_\pi(\tilde{M}(\phi))$ of $\tilde{M}(\phi)$ can be defined and it is canonically isomorphic to $T_\pi(\phi)$. The Tate uniformization implies that there exist an analytic τ-sheaf $\tilde{N}$ which is potentially trivial and an exact sequence

$$0 \to \tilde{N} \to \tilde{M}(\phi) \to \tilde{M}(\psi) \to 0$$

of analytic τ-sheaves. Since $\tilde{M} \mapsto T_\pi(\tilde{M})$ is a contravariant exact functor, we obtain

$$0 \to T_\pi(\tilde{M}(\psi)) \to T_\pi(\tilde{M}(\phi)) \to T_\pi(\tilde{N}) \to 0,$$

which coincides with the sequence (2.4.1) (for example, see [Gar03b, Example 7.1]).

2.5 Cyclotomic function fields

We recall some properties of a function field analogue of cyclotomic extensions of the rational number field $\mathbb{Q}$ (cf. [Hay74] and [Ros02, Chapter 12]). In this section, we will use the letters "a" and "$\mathfrak{n}$" as our typical non-zero elements of A.

Definition 2.5.1. The Drinfeld module

$$\mathcal{C} : A \to F\{\tau\}$$

determined by $\mathcal{C}_t = t + \tau$ is called the *Carlitz module*.

The Carlitz module $\mathcal{C}$ is of rank one and has good reduction at all finite places. For any non-zero $\mathfrak{n} \in A$, we know that $\mathcal{C}[\mathfrak{n}] \cong A/\mathfrak{n}A$ as an A-module. Let $\zeta_{\mathfrak{n}}$ be a generator of $\mathcal{C}[\mathfrak{n}]$. Then it is easy to see that $\mathcal{C}_a(\zeta_{\mathfrak{n}})$ is also a generator of $\mathcal{C}[\mathfrak{n}]$ if and only if $(a, \mathfrak{n}) = 1$. Thus, it follows that $F(\zeta_{\mathfrak{n}}) = F(\mathcal{C}[\mathfrak{n}])$. We see that the action of $\mathrm{Gal}(F(\zeta_{\mathfrak{n}})/F)$ on $\mathcal{C}[\mathfrak{n}]$ is faithful and so we have an injection

$$\mathrm{Gal}(F(\zeta_{\mathfrak{n}})/F) \hookrightarrow (A/\mathfrak{n}A)^{\times}. \tag{2.5.1}$$

Hence $F(\zeta_{\mathfrak{n}})/F$ is an abelian extension. Its arithmetic behavior is similar to that of cyclotomic number fields:

Proposition 2.5.2. *Let $\pi \in A$ be a monic irreducible element.*

(1) *For every $e \in \mathbb{Z}_{>0}$, $F(\zeta_{\pi^e})$ is unramified at every place of F distinct from π and ∞. The place π is totally ramified with ramification index $\#(A/\pi^e A)^{\times} = q_{\pi}^{e-1}(q-1)$.*

(2) *Let $\mathfrak{n} \in A$ be an element of positive degree. Then π is ramified in $F(\zeta_{\mathfrak{n}})$ if and only if $(\mathfrak{n}, \pi) = 1$. We have $[F(\zeta_{\mathfrak{n}}) : F] = \#(A/\mathfrak{n}A)^{\times}$.*

Proof. See [Hay74, Proposition 2.2] and [Ros02, Theorem 12.8]. □

Proposition 2.5.2 (2) implies that the map (2.5.1) is an isomorphism $\mathrm{Gal}(F(\zeta_{\mathfrak{n}})/F) \cong (A/\mathfrak{n}A)^{\times}$. We look at this isomorphism more closely. Notice that $\zeta_{\mathfrak{n}}$ is a generator of $\mathcal{C}[\mathfrak{n}]$. If $\sigma \in \mathrm{Gal}(F(\zeta_{\mathfrak{n}})/F)$, then clearly $\sigma(\zeta_{\mathfrak{n}})$ is also a generator of $\mathcal{C}[\mathfrak{n}]$. Thus there is an element $a \in A$ with $(a, \mathfrak{n}) = 1$ such that $\sigma(\zeta_{\mathfrak{n}}) = \mathcal{C}_a(\zeta_{\mathfrak{n}})$. The σ is completely determined by this relation. Then it follows that the map $\sigma \mapsto a$ coincides with the isomorphism $\mathrm{Gal}(F(\zeta_{\mathfrak{n}})/F) \cong (A/\mathfrak{n}A)^{\times}$.

For any $a \in A$ with $(a, \mathfrak{n}) = 1$, write $\sigma_a \in \mathrm{Gal}(F(\zeta_{\mathfrak{n}})/F)$ for the unique element satisfying $\sigma_a(\zeta_{\mathfrak{n}}) = \mathcal{C}_a(\zeta_{\mathfrak{n}})$. Then we have the following important fact.

Proposition 2.5.3 (Hayes [Hay74, Corollary 2.5])**.** *Let $\pi \in A$ be a monic irreducible element not dividing $\mathfrak{n}$. Then the element $\sigma_{\pi} \in \mathrm{Gal}(F(\zeta_{\mathfrak{n}})/F)$ coincides with the Artin automorphism [4] $(\pi, F(\zeta_{\mathfrak{n}})/F)$ for π.*

We introduce an important Galois character as follows.

[4] see § 5.2.

Definition 2.5.4. Let $\pi \in A$ be a monic irreducible element. The character

$$\chi_\pi (:= \bar{\rho}_{\mathcal{C},\pi}) : G_F \to \mathbb{F}_\pi^\times$$

describing the G_F-action on $\mathcal{C}[\pi]$ is called the *mod π Carlitz character*.

By definition, it factors as $\chi_\pi : G_F \twoheadrightarrow \mathrm{Gal}(F(\zeta_\pi)/F) \cong \mathbb{F}_\pi^\times$ and satisfies the following.

Proposition 2.5.5. *Let $\pi_0 \in A$ be a monic irreducible element with $\pi_0 \neq \pi$. Then χ_π is unramified at π_0 and we have*

$$\chi_\pi(\mathrm{Frob}_{\pi_0}) \equiv \pi_0 \pmod{\pi}.$$

Proof. By Proposition 2.3.10 or Proposition 2.5.2 (2), it follows that χ_π is unramified at π_0. Since $\mathrm{Frob}_{\pi_0}|_{F(\zeta_\pi)} = (\pi_0, F(\zeta_\pi)/F)$ holds, the above congruence follows from Proposition 2.5.3. □

Remark 2.5.6. In general, let K be a finite extension of F and let v be a place of K above π_0. If $\pi \neq \pi_0$, then we have $\chi_\pi(\mathrm{Frob}_v) = \chi_\pi(\mathrm{Frob}_{\pi_0}^{f_{v|\pi_0}})$. Thus

$$\chi_\pi(\mathrm{Frob}_v) \equiv \pi_0^{f_{v|\pi_0}} \pmod{\pi}$$

holds.

The last task in this section is to study the ramification of the infinite place ∞. Let $\mathfrak{n} \in A$ have positive degree. Define

$$J = \{\sigma_x \in \mathrm{Gal}(F(\zeta_\mathfrak{n})/F); x \in \mathbb{F}_q^\times\}$$

and consider the fixed subfield $F(\zeta_\mathfrak{n})^+ \subset F(\zeta_\mathfrak{n})$ by J. We notice that $J \cong \mathbb{F}_q^\times$ and $[F(\zeta_\mathfrak{n}) : F(\zeta_\mathfrak{n})^+] = q - 1$. Then we have:

Proposition 2.5.7. *The infinite place ∞ of F splits completely in $F(\zeta_\mathfrak{n})^+$ and every place of $F(\zeta_\mathfrak{n})^+$ above ∞ is totally and tamely ramified with ramification index $q - 1$.*

Proof. See [Ros02, Theorem 12.14]. □

Corollary 2.5.8. *For any $\mathfrak{n} \in A$ with $\mathfrak{n} \neq 0$, the constant field of $F(\zeta_\mathfrak{n})$ is $\mathbb{F}_q$, that is, $F(\zeta_\mathfrak{n})/F$ is a geometric extension.*

Proof. It is trivial when $\mathfrak{n} \in \mathbb{F}_q^\times$. Suppose that $\mathfrak{n}$ has positive degree. Let $w_\infty | v_\infty$ be places of $F(\zeta_\mathfrak{n})/F(\zeta_\mathfrak{n})^+$ above ∞. Then Proposition 2.5.7 means that $f_{w_\infty|v_\infty} = f_{v_\infty|\infty} = 1$, so that the residue field at w_∞ is $\mathbb{F}_q$. Since the constant field of $F(\zeta_\mathfrak{n})$ injects into the residue field at w_∞, the result follows. □

Chapter 3

Rasmussen-Tamagawa type conditions

In this chapter, we explain a motivation of the Rasmussen-Tamagawa conjecture and the precise statement of it. After that, following the analogy between number fields and function fields, we define the set $\mathscr{D}(K, r, \pi)$ of K-isomorphism classes of Drinfeld modules with Rasmussen-Tamagawa type conditions.

3.1 Ihara's question

The absolute Galois group G_k of a global field k is a fundamental object in number theory. However its structure is very complicated and still mysterious. To describe this, it is important to study various arithmetic objects on which G_k acts. Typical examples of such objects are Galois representations defined by the ℓ-adic Tate modules of abelian varieties over k and the ℓ-adic étale cohomology groups of schemes over k, where ℓ is a prime number. In the case where k is a function field, Drinfeld modules also provide Galois representations.

Using the étale fundamental groups, one can construct other such objects so-called outer Galois representations. For a connected scheme X over k, one can define the étale fundamental group $\pi_1(X)$, which is an scheme-theoretic analogue of a topological fundamental group. Indeed if X is of finite type over the field of complex numbers $\mathbb{C}$, then its étale fundamental group is isomorphic to the profinite completion of the topological fundamental group of $X(\mathbb{C})$, the complex analytic space attached to X. It is well-known that the étale fundamental group of Spec k is precisely the absolute Galois group $\pi_1(\mathrm{Spec}\, k) \cong G_k$.

Suppose that X is a quasi-compact and geometrically irreducible scheme over k and set $\bar{X} := X \times_{\mathrm{Spec}\, k} \mathrm{Spec}\, k^{\mathrm{sep}}$. Then it follows that the étale fundamental group $\pi_1(X)$ is an extension of G_k by $\pi_1(\bar{X})$. Namely there is a short exact sequence

$$1 \to \pi_1(\bar{X}) \to \pi_1(X) \to G_k \to 1, \tag{3.1.1}$$

which is called the *homotopy exact sequence*. Denote by $\mathrm{Inn}(\pi_1(\bar{X}))$ the subgroup of $\mathrm{Aut}(\pi_1(\bar{X}))$ consisting of all inner automorphisms of $\pi_1(\bar{X})$. It is a normal subgroup of $\mathrm{Aut}(\pi_1(\bar{X}))$ and so we have the group

$$\mathrm{Out}(\pi_1(\bar{X})) := \mathrm{Aut}(\pi_1(\bar{X}))/\mathrm{Inn}(\pi_1(\bar{X}))$$

of *outer automorphisms* of $\pi_1(\bar{X})$. For any $\sigma \in G_k$ and $y \in \pi_1(\bar{X})$, consider a conjugation $x_\sigma^{-1} y x_\sigma$ by a lift $x_\sigma \in \pi_1(X)$ of σ, which is also an element of $\pi_1(\bar{X})$ by the exact sequence (3.1.1). Thus we have an automorphism $y \mapsto x_\sigma^{-1} y x_\sigma$ of $\pi_1(\bar{X})$. It follows that this automorphism is uniquely determined by σ up to inner automorphisms. Thus we obtain a group homomorphism

$$\Phi : G_k \to \mathrm{Out}(\pi_1(\bar{X}))$$

so-called the *outer Galois representation*.

It is believed that such outer representations have ample information about Galois groups. Let us consider the case where $k = \mathbb{Q}$ and $\bar{X} = \mathbb{P}^1_{0,1,\infty} := \mathbb{P}^1_{\bar{\mathbb{Q}}} \setminus \{0, 1, \infty\}$. Then Belyĭ's result in [Bel80] shows that the outer Galois representation

$$\Phi_{\mathbb{Q}} : G_{\mathbb{Q}} \to \mathrm{Out}(\pi_1(\mathbb{P}^1_{0,1,\infty}))$$

is injective. Therefore studying the group $\mathrm{Out}(\pi_1(\mathbb{P}^1_{0,1,\infty}))$ is helpful to understand the structure of $G_{\mathbb{Q}}$.

Ihara studied the structure of $\Phi_{\mathbb{Q}}$ and $\mathrm{Out}(\pi_1(\mathbb{P}^1_{0,1,\infty}))$ as follows. For a fixed prime number ℓ, denote by $\pi_1^\ell(\mathbb{P}^1_{0,1,\infty})$ the maximal pro-ℓ quotient of $\pi_1(\mathbb{P}^1_{0,1,\infty})$. It is a characteristic quotient of $\pi_1(\mathbb{P}^1_{0,1,\infty})$ and so there is a canonical surjection $\mathrm{Out}(\pi_1(\mathbb{P}^1_{0,1,\infty})) \twoheadrightarrow \mathrm{Out}(\pi_1^\ell(\mathbb{P}^1_{0,1,\infty}))$. Then the *pro-$\ell$ outer representation*

$$\Phi_{\mathbb{Q},\ell} : G_{\mathbb{Q}} \to \mathrm{Out}(\pi_1^\ell(\mathbb{P}^1_{0,1,\infty}))$$

is defined by the following diagram:

$$\begin{array}{ccc} G_{\mathbb{Q}} & \xrightarrow{\Phi_{\mathbb{Q}}} & \mathrm{Out}(\pi_1(\mathbb{P}^1_{0,1,\infty})) \\ & {\scriptstyle \Phi_{\mathbb{Q},\ell}} \searrow & \downarrow\!\!\downarrow \\ & & \mathrm{Out}(\pi_1^\ell(\mathbb{P}^1_{0,1,\infty})). \end{array}$$

Denote by $\mu_{\ell^\infty} = \mu_{\ell^\infty}(\bar{\mathbb{Q}})$ the set of all ℓ-power roots of unity in $\bar{\mathbb{Q}}$. Ihara's result in [Iha86] shows that the fixed subfield

$$\Omega_{\mathbb{Q},\ell} := \bar{\mathbb{Q}}^{\ker \Phi_{\mathbb{Q},\ell}}$$

of $\bar{\mathbb{Q}}$ is an infinite non-abelian pro-ℓ extension of $\mathbb{Q}(\mu_{\ell^\infty})$ unramified outside ℓ, that is, unramified at all places not lying above ℓ. Therefore if we write $\Lambda_{\mathbb{Q},\ell}$ for the maximal pro-ℓ extension of $\mathbb{Q}(\mu_{\ell^\infty})$ unramified outside ℓ, then

$$\Omega_{\mathbb{Q},\ell} \subseteq \Lambda_{\mathbb{Q},\ell}$$

holds. Ihara asked the following:

Question 3.1.1 (Ihara [Iha86])**.** *For any prime number ℓ, does $\Omega_{\mathbb{Q},\ell} = \Lambda_{\mathbb{Q},\ell}$ hold?*

Remark 3.1.2. If ℓ is odd and regular, then Scharifi's work [Sha02, Theorem 1.1] shows that the question is equivalent to a conjecture of Deligne and Ihara on the nature of a certain graded Lie algebra constructed from the lower central series of $\pi_1^\ell(\mathbb{P}^1_{0,1,\infty})$. This conjecture is recently proved by Brown in [Bro12]. Hence the answer to Ihara's question is given in the odd regular prime case. However it is still open in general.

3.2 The Rasmussen-Tamagawa conjecture

3.2.1 Motivations Let k be a finite extension of $\mathbb{Q}$ and let ℓ be a prime number. Denote by $\Omega_{k,\ell}$ the fixed subfield of k^{sep} by $\ker \Phi_{\mathbb{Q},\ell}|_{G_k}$ and by $\Lambda_{k,\ell}$ the maximal pro-ℓ extension of $k(\mu_{\ell^\infty})$ unramified outside ℓ. As in §3.1, we see that $\Omega_{k,\ell} \subseteq \Lambda_{k,\ell}$. In this situation, does the equality $\Omega_{k,\ell} = \Lambda_{k,\ell}$ hold? To consider this open question, it is worth studying subfields of $\Omega_{k,\ell}$ arising from ℓ-power torsion points of abelian varieties in the following reason.

Let X be an abelian variety over k. Let $X^\vee$ be the dual abelian variety to X and let $\theta : X \to X^\vee$ be a polarization. Then it is known that the polarization θ induces a non-degenerate pairing

$$e^\theta : V_\ell(X) \times V_\ell(X) \to \mathbb{Q}_\ell(1)$$

of rational ℓ-adic Tate module $V_\ell(X) := T_\ell(X) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ of X, where $\mathbb{Q}_\ell(1)$ is the one-dimensional $\mathbb{Q}_\ell$-vector space on which G_k acts via the ℓ-adic cyclotomic character. By the paring, we see that

$$k(\mu_{\ell^\infty}) \subset k(X[\ell^\infty]),$$

where $k(X[\ell^\infty]) = k(\cup_{n\geq 1} X[\ell^n])$ is the field generated by all ℓ-power torsion points of X. See [Mum70, §20] for details.

If X has good reduction at any finite place of k not lying above ℓ, then by the Néron-Ogg-Shafarevich criterion in [ST68] the extension $k(X[\ell^\infty])/k(X[\ell])$ is pro-ℓ and unramified outside ℓ. Hence if $k(X[\ell]) \subset \Lambda_{k,\ell}$, then also $k(X[\ell^\infty]) \subset \Lambda_{k,\ell}$. In this case, to consider the question of Ihara, it is worth studying whether or not $k(X[\ell^\infty]) \subset \Omega_{k,\ell}$.

For example, if X is the Jacobian variety of one of the following curves over k, then it is known that $k(X[\ell^\infty]) \subset \Omega_{k,\ell}$ holds:

- Fermat curves or Heisenberg curves for any ℓ [AI98, §0.6],
- Principal modular curves $X(2^n)$, $\ell = 2$ [AI98, §0.6],
- Elliptic curves $E/\mathbb{Q}$ with good outside $\ell = 2$ [Ras08, Theorem 1.1],
- Elliptic curves $E/\mathbb{Q}$ with good outside $\ell = 3$ [PaR07, Corollary 4],
- Modular curves $X(\ell^n)$, $X_0(\ell^n)$ and $X_1(\ell^n)$, $\ell = 2, 3$ [PaR07, Theorem 1 and §3.2].

3.2.2 Statements of conjectures and known results By the above reason, we are interested in the existence of abelian varieties X over k satisfying $k(X[\ell^\infty]) \subset \Lambda_{k,\ell}$ for some prime number ℓ. Notice that such X has good reduction at any finite places of k not lying above ℓ by the Néron-Ogg-Shafarevich criterion in [ST68].

Despite the existence of these examples for some small ℓ as in the above subsection, the constraints on such abelian varieties are strong and so such abelian varieties are quite rare. For an abelian variety X over k, denote by $[X]$ its k-isomorphism class. For a positive integer $g > 0$ and a prime number ℓ, define

$$\mathscr{A}(k, g, \ell) := \{[X];\ \dim X = g \text{ and } k(X[\ell^\infty]) \subset \Lambda_{k,\ell}\}.$$

For a finite set S of finite places of k, we also define $\mathscr{G}(k, g, S)$ to be the set of k-isomorphism classes of g-dimensional abelian varieties over k which have good reduction outside S. If S contains all places above ℓ, then $\mathscr{A}(k, g, \ell) \subset \mathscr{G}(k, g, S)$. Faltings proved in [Fal83] the conjecture of Shafarevich: for fixed positive integer d and fixed k,g, and S, the subset of $\mathscr{G}(k, g, S)$ consisting of those abelian varieties which admit a polarization of degree d is finite. In [Zar85, Theorem 1], Zarhin later improved Faltings' result to give the finiteness of $\mathscr{G}(k, g, S)$ for any k, g and S. Consequently the set $\mathscr{A}(k, g, \ell)$ is also finite. By the structure lemma (Lemma 3.3.1), we have the following equivalence. See also the proof of Proposition 3.3.6.

Proposition 3.2.1. *For an abelian variety X over k and a prime number ℓ, the following conditions are equivalent:*

(RT-1) $k(X[\ell^\infty]) \subseteq \Lambda_{k,\ell}$,

(RT-2) *X has good reduction at any finite place of k not lying above ℓ and $k(X[\ell])/k(\mu_\ell)$ is an ℓ-extension,*

(RT-3) *X has good reduction at any finite place of k not lying above ℓ and the mod ℓ representation $\bar{\rho}_{X,\ell} : G_k \to \mathrm{Aut}_{\mathbb{F}_\ell}(X[\ell]) \simeq \mathrm{GL}_{2g}(\mathbb{F}_\ell)$ is of the form*

$$\bar{\rho}_{X,\ell} \simeq \begin{pmatrix} \chi_\ell^{i_1} & * & \cdots & * \\ & \chi_\ell^{i_2} & \ddots & \vdots \\ & & \ddots & * \\ & & & \chi_\ell^{i_{2g}} \end{pmatrix},$$

where χ_ℓ is the mod ℓ cyclotomic character and $\dim X = g$.

In 2008, Rasmussen and Tamagawa stated the following conjecture (the Rasmussen-Tamagawa conjecture):

Conjecture 3.2.2 (Rasmussen and Tamagawa [RT08, Conjecture 1])**.** *Let $k/\mathbb{Q}$ be a finite extension and $g \geq 0$. Then for any sufficiently large prime ℓ, the set $\mathscr{A}(k,g,\ell)$ is empty.*

This conjecture says that there exists a positive constant $C = C(k,g) > 0$ depending only on k and g such that $\mathscr{A}(k,g,\ell) = \varnothing$ for any prime $\ell > C$. Since $\mathscr{A}(k,g,\ell)$ is finite for all ℓ, the conjecture is equivalent to saying that the disjoint union

$$\mathscr{A}(k,g) := \bigcup_{\ell} \mathscr{A}(k,g,\ell)$$

is finite. Under the assumption on the Generalized Riemann Hypothesis (GRH, for short) for Dedekind zeta functions of number fields, Rasmussen and Tamagawa proved the conjecture is true in [RT17, Theorem 5.1]. Therefore it is believed that the conjecture is true in general. Without the assumption of GRH, the conjecture is true in the following cases:

- $k = \mathbb{Q}$ and $g = 1$ [RT08, Theorem 2],
- $k = \mathbb{Q}$ and $g = 2, 3$ [RT17, Proposition 7.1 and Proposition 7.2],
- $k/\mathbb{Q}$ be a quadratic extension and $g = 1$ [RT17, Proposition 7.4],

- $k/\mathbb{Q}$ is a Galois extension whose Galois group $\mathrm{Gal}(k/\mathbb{Q})$ has exponent 3 and $g = 1$ [RT17, Proposition 7.7].

Sometimes one can prove non-existence of subsets of $\mathscr{A}(k, g, \ell)$ (cf. Remark 3.2.7). For example,

- for abelian varieties with everywhere semistable reduction [Oze11, Corollary 4.5] and [RT17, Theorem 3.6],
- for abelian varieties with abelian Galois representations [Oze13, Corollary 1.3],
- for QM abelian surfaces over certain imaginary quadratic number fields [Ara14, Theorem 9.3].

For an arbitrary field $\mathcal{F}$ and a positive integer $n > 0$, define

$$\mathscr{F}_n(\mathcal{F}) := \{K; [K : \mathcal{F}] = n\}$$

to be the set of finite extensions of $\mathcal{F}$ of degree n. Rasmussen and Tamagawa also stated a uniform version of conjecture 3.2.2:

Conjecture 3.2.3 (Rasmussen and Tamagawa [RT17, Conjecture 2])**.** *Let $g > 0$ and $n > 0$ be positive integers. Then there exists a positive constant $C = C(g, n) > 0$ such that $\mathscr{A}(k, g, \ell) = \varnothing$ for any $k \in \mathscr{F}_n(\mathbb{Q})$ and any prime $\ell > C$.*

Under the assumption of GRH, one can prove the conjecture in the odd degree case:

Theorem 3.2.4 (Rasmussen and Tamagawa [RT17, Theorem 5.2])**.** *Assume that the Generalized Riemann Hypothesis. Then Conjecture 3.2.3 is true for any $g > 0$ and any odd n.*

Rasmussen and Tamagawa also prove the next stronger result:

Theorem 3.2.5 (Rasmussen and Tamagawa [RT17, Theorem 5.3])**.** *Let k_0 be a finite extension of $\mathbb{Q}$ and assume the Generalized Riemann Hypothesis. For any $g > 0$ and any odd $n > 0$, there exists a positive constant $C = C(g, n) > 0$ such that $\mathscr{A}(k, g, \ell) = \varnothing$ for any $k \in \mathscr{F}_n(k_0)$ and $\ell > C$.*

Although the uniform version of the conjecture is not proved without the assumption of the GRH, several partial results are known. For example, the result of Rasmussen and Tamagawa [RT17, Corollary 3.8] shows that for any $g > 0$ and any $n > 0$ not divisible by 4, there exists a positive constant $C = C(g, n) > 0$ such that $\mathscr{A}^{\mathrm{ss}}(k, g, \ell) = \varnothing$ for any $k \in \mathscr{F}_n(\mathbb{Q})$ and any

$\ell > C$, where $\mathscr{A}^{\mathrm{ss}}(k,g,\ell)$ is the subset of $\mathscr{A}(k,g,\ell)$ consisting of those k-isomorphism classes of abelian varieties which have semistable reduction at every finite places of k. In the CM elliptic curve case, Bourdon proves the following finiteness result:

Theorem 3.2.6 (Bourdon [Bou15, Theorem 1])**.** *Let k be a finite extension of $\mathbb{Q}$ of degree n. Then there exists a positive constant $C = C(n) > 0$ with the following property: If there exists an elliptic curve E over k such that $E_{\bar{\mathbb{Q}}}$ has complex multiplication and $k(E[\ell^\infty])$ is a pro-ℓ extension of $k(\mu_\ell)$, then $\ell \leq C$.*

Remark 3.2.7. Define

$$\mathscr{A}^{\mathrm{CM}}(k,g,\ell) := \{[X] \in \mathscr{A}(k,g,\ell);\ X_{\bar{\mathbb{Q}}} \text{ has complex multiplication}\}.$$

Then the above result of Bourdon implies that Conjecture 3.2.3 for the set $\mathscr{A}^{\mathrm{CM}}(k,1,\ell)$ is true. For any $g > 0$ and $n > 0$, the recent work of Lombardo [Lom, Theorem 1.3] shows that there exists a positive constant $C = C(g,n) > 0$ such that $\mathscr{A}^{\mathrm{CM}}(k,g,\ell) = \varnothing$ for any $k \in \mathscr{F}_n(\mathbb{Q})$ and $\ell > C$.

3.3 Definition of the set $\mathscr{D}(K,r,\pi)$

The main task of this section is to formulate a Drinfeld module analogue of the Rasmussen-Tamagawa conjecture. As usual, we denote by K a finite extension of F and by r a positive integer. Let $\pi \in A$ be a monic irreducible element. As an analogue of $\mathscr{A}(k,g,\ell)$, let us define the set $\mathscr{D}(K,r,\pi)$ of K-isomorphism classes of Drinfeld modules with Rasmussen-Tamagawa type conditions.

3.3.1 Group theoretic lemmas In the number field case, $\mathscr{A}(k,g,\ell)$ is determined by the equivalent conditions (RT-1), (RT-2), and (RT-3) in Proposition 3.2.1. The equivalence of them follows from the criterion of Néron-Ogg-Shafarevich and the next group theoretic lemma:

Lemma 3.3.1 (cf. Rasmussen and Tamagawa [RT17, Lemma 3.4])**.** *Let $\mathbb{F}$ be a finite field of characteristic ℓ. Suppose G is a profinite group, $N \subset G$ is a pro-ℓ open normal subgroup, and $C = G/N$ is a finite cyclic subgroup with $\#C | \#\mathbb{F}^\times$. Let V be an $\mathbb{F}$-vector space of dimension r on which G acts continuously. Fix a group homomorphism $\chi_0 : G \to \mathbb{F}^\times$ with $\ker \chi_0 = N$. Then there exists a filtration*

$$0 = V_0 \subset V_1 \subset \cdots \subset V_r = V$$

of $\mathbb{F}$-vector spaces such that for each $0 \leq s \leq r$,

- *V_s is G-stable,*
- $\dim_{\mathbb{F}} V_s = s$*,*
- *the G-action on V_s/V_{s-1} is given by $\chi_0^{i_s}$ for some integer i_s satisfying $0 \le i_s < \#C$.*

Proof. It is proved by induction on r. The $r = 1$ case is trivial since G must act on V via a power of χ_0. Suppose that the result holds for spaces of dimension $r-1$. Let V be an $\mathbb{F}$-vector space of dimension r with G-action. Consider the action of N on V. Then we see that it factors through some finite ℓ-group. Hence every N-orbit of V has an ℓ-power order and so the subspace V^N of fixed points is non-trivial. Indeed if $V^N = \{0\}$, then it follows that $\#V - 1$ is divisible by ℓ, which is impossible. Since N is a normal subgroup of G, we see that V^N is G-stable and there exists a well-defined action of C on V^N. Let $\gamma \in C$ be a generator of C, so that $C = \langle \gamma \rangle$. Set $c := \#C$.

Choose an ordered basis for V^N and denote the associated representation by $\rho : C \to \mathrm{Aut}_{\mathbb{F}}(V^N) \cong \mathrm{GL}_d(\mathbb{F})$, where $d = \dim_{\mathbb{F}} V^N$. Since $\rho(\gamma)^c$ is the identity matrix, the minimal polynomial of $\rho(\gamma)$ splits completely over $\mathbb{F}$. Thus there is an eigenvector $w \in V^N$ of $\rho(\gamma)$ with eigenvalue $\xi \in \mathbb{F}^\times$ satisfying $\xi^c = 1$. The homomorphism $\chi_0 : G \to \mathbb{F}^\times$ induces an isomorphism $\bar{\chi}_0$ between C and the cyclic subgroup of $\mathbb{F}^\times$ of order c. Since $\ker \chi_0 = N$, it follows that $\bar{\chi}_0(\gamma)$ has exact order c and so $\xi = \bar{\chi}_0(\gamma)^j$ for some integer j satisfying $0 \le j < c$.

Let $V_1 \subset V^N$ be the subspace generated by w. Clearly V_1 is G-stable and the G-action on V_1 is given by χ_0^j. Consider the induced action of G on the quotient $V' := V/V_1$. Since this quotient is of dimension $r-1$, by the assumption of induction there exists a filtration

$$\{0\} = V'_0 \subset \cdots \subset V'_{r-1} = V'$$

of G-stable subspaces of V' such that for all $0 \le s \le r-1$, $\dim_{\mathbb{F}} V'_s = s$ and G acts on V'_s/V'_{s-1} via $\chi_0^{i'_s}$ with $0 \le i'_s < c$. Let $\Pi : V \twoheadrightarrow V' (= V/V_1)$ be the natural projection. Set $V_0 := \{0\}$ and $V_s := \Pi^{-1}(V'_{s-1})$ for $1 \le s \le r$. Then the restriction of Π to V_s is a G-equivariant surjection $V_s \twoheadrightarrow V'_{s-1}$ and hence the induce isomorphism $V_s/V_{s-1} \cong V'_{s-1}/V'_{s-2}$ is also G-equivariant for each $1 < s \le r$. If we set $i_s = i'_{s-1}$ for each $1 < s \le r$, then the filtration $\{V_s\}_{s=0}^r$ has the required properties. □

We shall prepare two fundamental lemmas which are needed in the next subsection. Let $\mathcal{F}$ be a field of positive characteristic p and $\mathcal{U} \in$

$\mathrm{GL}_n(\mathcal{F})$ for a positive integer n. We say that $\mathcal{U}$ is *unipotent* if $U - I_n$ is nilpotent, where $I_n \in \mathrm{GL}_n(\mathcal{F})$ is the identity matrix. Denote by

$$\mathrm{DT}_n(\mathcal{F}) := \left\{ \begin{pmatrix} 1 & * & \cdots & * \\ & 1 & \ddots & \vdots \\ & & \ddots & * \\ & & & 1 \end{pmatrix} \in \mathrm{GL}_n(\mathcal{F}) \right\}$$

the subgroup of $\mathrm{GL}_n(\mathcal{F})$ consisting of those triangular matrices with diagonal elements equal to 1.

Lemma 3.3.2. *Let $\mathcal{F}$ and n be as above.*

(1) *$U \in \mathrm{GL}_n(\mathcal{F})$ is unipotent if and only if it is of p-power order.*

(2) *The subgroup $\mathrm{DT}_n(\mathcal{F})$ is a maximal unipotent subgroup of $\mathrm{GL}_n(\mathcal{F})$. All maximal unipotent subgroups of $\mathrm{GL}_n(\mathcal{F})$ are conjugate to $\mathrm{DT}_n(\mathcal{F})$ under $\mathrm{GL}_n(\mathcal{F})$.*

Proof. See [Zas69, Theorem 1 and Theorem 2]. □

Next, for any positive integer n and any local ring R with residue field $\mathbb{F}$, denote by

$$\Gamma_n(R) := \ker\left(\mathrm{GL}_n(R) \to \mathrm{GL}_n(\mathbb{F})\right)$$

the kernel of the canonical surjection induced by the reduction map $R \twoheadrightarrow \mathbb{F}$.

Lemma 3.3.3 (cf. [Gou01, Lemma 5.1 and Problem 5.1])**.** *Let n be a positive integer. Let R be a complete noetherian local ring with finite residue field $\mathbb{F}$ of positive characteristic p. Then $\Gamma_n(R)$ is a pro-p group.*

Proof. Let $\mathfrak{m} \subset R$ be the maximal ideal of R. Then by definition R is isomorphic to $\varprojlim_k R/\mathfrak{m}^k$. For every positive integer k, denote by

$$f_k : \Gamma_n(R/\mathfrak{m}^{k+1}) \to \Gamma_n(R/\mathfrak{m}^k)$$

the homomorphism induced by the canonical map $R/\mathfrak{m}^{k+1} \to R/\mathfrak{m}^k$. Then the groups $\Gamma_n(R/\mathfrak{m}^k)$ form an inverse system by f_k and we see that

$$\Gamma_n(R) \cong \varprojlim_k \Gamma_n(R/\mathfrak{m}^k).$$

Therefore it suffices to show that $\Gamma_n(R/\mathfrak{m}^k)$ is a p-group for every k. To prove this, we check that both $\ker f_k$ and $\operatorname{Im} f_k$ are p-groups.

We see that $\ker f_k$ consists of those matrices whose off-diagonal entries are in the ideal $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ and whose diagonal entries are in $1+\mathfrak{m}^k/\mathfrak{m}^{k+1}$. Namely we have

$$\ker f_k = 1 + \mathrm{M}_n(\mathfrak{m}^k/\mathfrak{m}^{k+1}).$$

Here it is isomorphic to the additive group $\mathrm{M}_n(\mathfrak{m}^k/\mathfrak{m}^{k+1})$. Indeed any two matrices X and Y in $\mathrm{M}_n(\mathfrak{m}^k/\mathfrak{m}^{k+1})$ satisfy $XY = 0$ and so the map

$$\begin{array}{ccc} 1+\mathrm{M}_n(\mathfrak{m}^k/\mathfrak{m}^{k+1}) & \to & \mathrm{M}_n(\mathfrak{m}^k/\mathfrak{m}^{k+1}) \\ 1+X & \mapsto & X \end{array}$$

is a group isomorphism. Since $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ is a one-dimensional $\mathbb{F}$-vector space, the group $\mathrm{M}_n(\mathfrak{m}^k/\mathfrak{m}^{k+1})$ is a p-group and hence $\ker f_k$ is also a p-group.

We next prove that $\mathrm{Im}\ f_k$ is a p-group by induction on k. Notice that $\Gamma_n(R/\mathfrak{m}) = \Gamma_n(\mathbb{F}) = \{1\}$ and so $\mathrm{Im}\ f_1 = \{1\}$ is a p-group. Suppose that $\mathrm{Im}\ f_{k-1}$ is a p-group for an integer $k \geq 2$. Then

$$1 \to \ker f_{k-1} \cap \mathrm{Im}\ f_k \to \mathrm{Im}\ f_k \xrightarrow{f_{k-1}} \mathrm{Im}\ f_{k-1}$$

is exact and both $\ker f_{k-1} \cap \mathrm{Im}\ f_k$ and $\mathrm{Im}\ f_{k-1}$ are p-groups, and so is $\mathrm{Im}\ f_k$. □

3.3.2 Equivalent conditions Let $\phi : A \to K\{\tau\}$ be a Drinfeld module of rank r and let $\pi \in A$ be a monic irreducible element. We give some conditions which are equivalent to the condition (D1)+(D2) in Chapter 1.

Recall that the mod π Carlitz character $\chi_\pi : G_K \to \mathrm{Aut}_{\mathbb{F}_\pi}(\mathcal{C}[\pi]) \cong \mathbb{F}_\pi^\times$ is an analogue of the mod ℓ cyclotomic character. Let $\zeta_\pi \in \mathcal{C}[\pi]$ be a generator of $\mathcal{C}[\pi]$ as an A-module. Then we have $K(\mathcal{C}[\pi]) = K(\zeta_\pi)$. Consider the subfield

$$L := K(\phi[\pi]) \cap K(\zeta_\pi)$$

of $K(\phi[\pi])$. Then we have the following equivalent conditions.

Lemma 3.3.4. *Let ϕ, π and L be as above. Then the following conditions are equivalent.*

(a) *$K(\phi[\pi])/L$ is a p-extension,*

(b) *The mod π representation $\bar{\rho}_{\phi,\pi}|_{G_L}$ restricted to G_L is of the form*

$$\bar{\rho}_{\phi,\pi}|_{G_L} \simeq \begin{pmatrix} 1 & * & \cdots & * \\ & 1 & \ddots & \vdots \\ & & \ddots & * \\ & & & 1 \end{pmatrix},$$

(c) ϕ *satisfies* (D2), *that is, the mod* π *representation* $\bar{\rho}_{\phi,\pi}$ *is of the form*

$$\bar{\rho}_{\phi,\pi} \simeq \begin{pmatrix} \chi_\pi^{i_1} & * & \cdots & * \\ & \chi_\pi^{i_2} & \ddots & \vdots \\ & & \ddots & * \\ & & & \chi_\pi^{i_r} \end{pmatrix}$$

for some integers $0 \leq i_s < q_\pi - 1$.

Proof. Since $K(\phi[\pi])$ is the fixed subfield of K^{sep} by $\ker \bar{\rho}_{\phi,\pi}$, the representation $\bar{\rho}_{\phi,\pi}$ factors through an injection

$$\bar{\rho} : \mathrm{Gal}(K(\phi[\pi])/K) \hookrightarrow \mathrm{GL}_r(\mathbb{F}_\pi).$$

Then it follows that $\bar{\rho}_{\phi,\pi}(G_L) = \bar{\rho}(\mathrm{Gal}(K(\phi[\pi])/L)) \subset \mathrm{GL}_r(\mathbb{F}_\pi)$. By Lemma 3.3.2 we see that $\mathrm{Gal}(K(\phi[\pi])/L)$ is a p-group if and only if $\bar{\rho}_{\phi,\pi}(G_L)$ is a unipotent subgroup of $\mathrm{GL}_r(\mathbb{F}_\pi)$. In this case, up to conjugation $\bar{\rho}_{\phi,\pi}(G_L)$ is a subgroup of $\mathrm{DT}_r(\mathbb{F}_\pi)$. Hence (a) and (b) are equivalent.

Suppose that (c) holds. By definition, it follows that $\chi_\pi(\sigma) = 1$ for any element $\sigma \in G_{K(\zeta_\pi)}$. Now $\bar{\rho}_{\phi,\pi}$ factors through $\mathrm{Gal}(K(\phi[\pi])/K)$, so that $\bar{\rho}_{\phi,\pi}(G_{K(\zeta_\pi)}) = \bar{\rho}_{\phi,\pi}(G_L)$. Hence (c) implies (b).

Finally suppose that (a) holds. Consider the composite field $M := K(\phi[\pi], \zeta_\pi)$ of $K(\phi[\pi])$ and $K(\zeta_\pi)$.

$$\begin{array}{ccc} & M := K(\phi[\pi], \zeta_\pi) & \\ K(\phi[\pi]) & & K(\zeta_\pi) \\ & L & \end{array}$$

Since $L = K(\phi[\pi]) \cap K(\zeta_\pi)$, we see that $[M : K(\zeta_\pi)] = [K(\phi[\pi]) : L]$ and therefore $M/K(\zeta_\pi)$ is also a p-extension. By construction, both $\bar{\rho}_{\phi,\pi} : G_K \to \mathrm{GL}_r(\mathbb{F}_\pi)$ and $\chi_\pi : G_K \to \mathbb{F}_\pi^\times$ factor through the Galois group $G := \mathrm{Gal}(M/K)$. Denote by $\chi_0 : G \to \mathbb{F}_\pi^\times$ the character given by the decomposition

$$\chi_\pi : G_K \twoheadrightarrow G \xrightarrow{\chi_0} \mathbb{F}_\pi^\times.$$

Then we have $N := \ker \chi_0 = \mathrm{Gal}(M/K(\zeta_\pi))$, which is a normal p-subgroup of G. Hence applying Lemma 3.3.1 to $V = \phi[\pi]$, G, χ_0, and N as above, we see that the semisimplification $\bar{\rho}^{\mathrm{ss}}_{\phi,\pi}$ is isomorphic to $\chi_\pi^{i_1} \oplus \cdots \oplus \chi_\pi^{i_r}$ for some integers i_s with $0 \le i_s < \#G/N = \#\mathrm{Gal}(K(\zeta_\pi)/K) \le q_\pi - 1$. Hence (c) holds. □

Remark 3.3.5. Unlike the abelian variety case, the field $K(\phi[\pi])$ may not contain $K(\zeta_\pi)$. For example, for $x \in \mathbb{F}_q^\times \backslash \{1\}$, consider the rank-one Drinfeld module ϕ over F determined by $\phi_t = t + x\tau$ and suppose $q \neq 2$. Then the fields $F(\phi[t])$ and $F(\zeta_t)$ are generated by the roots of $t + xT^{q-1}$ and $t + T^{q-1}$, respectively. By Kummer theory, we see that $F(\phi[t]) \neq F(\zeta_t)$, so that $F(\phi[t]) \not\supset F(\zeta_t)$.

Using the above lemma, we can formulate the Rasmussen-Tamagawa type conditions for Drinfeld modules as follows. Consider the field

$$K(\phi[\pi^\infty]) := K(\textstyle\bigcup_{n\ge1}\phi[\pi^n])$$

generated by all π-power torsion points of ϕ. Notice that it is the fixed subfield of K^{sep} by the kernel of the π-adic representation $\rho_{\phi,\pi} : G_K \to \mathrm{GL}_r(A_\pi)$.

Proposition 3.3.6. *Let the notations be as above. Then the following conditions are equivalent.*

- (DR-1) *$K(\phi[\pi^\infty])/L$ is a pro-p extension which is unramified at any finite place of L not lying above π,*
- (DR-2) *ϕ has good reduction at any finite place of K not lying above π and $K(\phi[\pi])/L$ is a p-extension,*
- (DR-3) *ϕ satisfies* (D1) *and* (D2).

Proof. The proof is parallel to that in the abelian variety case. Clearly both $\rho_{\phi,\pi}$ and $\bar{\rho}_{\phi,\pi}$ factor through $\mathrm{Gal}(K(\phi[\pi^\infty])/K)$ and so we can regard them as representations of $\mathrm{Gal}(K(\phi[\pi^\infty])/K)$. By Remark 2.3.13, we have the following diagram

$$\begin{array}{ccc} \mathrm{Gal}(K(\phi[\pi^\infty])/K) & \xrightarrow{\rho_{\phi,\pi}} & \mathrm{GL}_r(A_\pi) \\ & \searrow^{\bar{\rho}_{\phi,\pi}} & \downarrow \\ & & \mathrm{GL}_r(\mathbb{F}_\pi). \end{array}$$

It implies that

$$\ker \bar{\rho}_{\phi,\pi} = \mathrm{Gal}(K(\phi[\pi^\infty])/K(\phi[\pi])).$$

Here $\rho_{\phi,\pi} : \mathrm{Gal}(K(\phi[\pi^\infty])/K) \to \mathrm{GL}_r(A_\pi)$ is injective and so $\ker \bar{\rho}_{\phi,\pi}$ is embedded into the kernel $\Gamma_r(A_\pi)$ of $\mathrm{GL}_r(A_\pi) \to \mathrm{GL}_r(\mathbb{F}_\pi)$. Since $\Gamma_r(A_\pi)$ is a pro-p group by Lemma 3.3.3, the extension $K(\phi[\pi^\infty])/K(\phi[\pi])$ is always pro-p. Consequently $K(\phi[\pi^\infty])/L$ is pro-p if and only if $K(\phi[\pi])/L$ is a p-extension. By Proposition 2.3.10, we know that ϕ has good reduction at any finite place v of K not lying above π if and only if v is unramified in $K(\phi[\pi^\infty])$. Hence the result follows from Lemma 3.3.4. □

Now we can define a Drinfeld module analogue of the set $\mathscr{A}(k, g, \ell)$.

Definition 3.3.7. Let K, r and π be as above. We define $\mathscr{D}(K, r, \pi)$ to be the set of K-isomorphism classes $[\phi]$ of Drinfeld modules $\phi : A \to K\{\tau\}$ of rank r satisfying the equivalent conditions in Proposition 3.3.6.

Remark 3.3.8. In the abelian variety case, the set $\mathscr{A}(k, g, \ell)$ is always finite by the Shafarevich conjecture (cf. §§ 3.2.2). However the Drinfeld module analogue of this conjecture does not hold, see Example 6.2.1. Therefore it is not known whether or not $\mathscr{D}(K, r, \pi)$ is finite. If $r \geq 2$ and $\pi = t$, then we prove that $\mathscr{D}(K, r, t)$ is infinite in Chapter 6.

Remark 3.3.9. The original conjecture of Rasmussen and Tamagawa is formulated for abelian varieties of arbitrary dimension, and so we would like to formulate its function field analogue for some higher dimensional objects (recall that Drinfeld modules are analogues of elliptic curves).

In [And86], Anderson introduced objects called *t-motives* as analogues of abelian varieties of higher dimensions, which are also generalizations of Drinfeld modules. In fact the category of Drinfeld modules is anti-equivalent to that of t-motives of dimension one. It is known that t-motives have the notions of good reduction and Galois representations attached to their π-torsion points (see, for example [Gar01]), so that we can consider the conditions (D1) and (D2) for t-motives. Moreover, Proposition 3.3.6 is also generalized to t-motives since the Galois criterion of good reduction for t-motives holds.

Therefore the set $\mathscr{M}(K, d, r, \pi)$ of isomorphism classes of d-dimensional t-motives over K of rank r satisfying the Rasmussen-Tamagawa type conditions can be defined and the following question makes sense: Is the set $\mathscr{M}(K, d, r, \pi)$ empty for any π with sufficiently large degree?

Chapter 4

Inertia action on torsion points

Throughout this chapter, let $\pi \in A$ be a monic irreducible element and K a finite extension of F. In this chapter, studying the ramification of mod π representations attached to Drinfeld modules, we show some non-existence results on certain Drinfeld modules. As a corollary of them, we have a part of Theorem 1.0.2 (= Theorem 4.3.9).

In §4.1, we introduce the notion of *tame inertia weight*, which is a key tool to prove the non-existence theorems. In §4.2, considering the tame inertia weights of the mod π Galois representation attached to a Drinfeld module $\phi : A \to K\{\tau\}$, we define an invariant $e_\pi(\phi)$ (Definition 4.2.5) and prove some important properties on it. In §4.3, we define a set $\mathcal{D}(K, r, \pi, d)$ of K-isomorphism classes of certain Drinfeld modules satisfying $\mathscr{D}(K, r, \pi) \subset \mathcal{D}(K, r, \pi, d)$. Using some facts on $e_\pi(\phi)$, we prove the emptiness of the set when π has large degree, which implies Theorem 4.3.9.

4.1 Tame inertia weights

Let u be a finite place of K above π. For a fixed separable closure K_u^{sep} of K_u with residue field $\bar{\mathbb{F}}_u$, denote by K_u^{ur} (resp. K_u^{t}) the maximal unramified (resp. maximal tamely ramified) extension of K_u in K_u^{sep}. Notice that I_{K_u} is isomorphic to $\mathrm{Gal}(K_u^{\mathrm{sep}}/K_u^{\mathrm{ur}})$. Denote by $I_{K_u}^{\mathrm{w}} := \mathrm{Gal}(K_u^{\mathrm{sep}}/K_u^{\mathrm{t}})$ the *wild inertia subgroup* of I_{K_u}. It is a normal subgroup of I_{K_u} and then we define $I_{K_u}^{\mathrm{t}} := I_{K_u}/I_{K_u}^{\mathrm{w}} \cong \mathrm{Gal}(K_u^{\mathrm{t}}/K_u^{\mathrm{ur}})$, which is called the *tame inertia group* of K_u.

4.1.1 Fundamental characters Let d be a positive integer and $\mathbb{F}$ the finite field with q_π^d elements in $\bar{\mathbb{F}}_u$. Then $\mathbb{F}$ is the finite extension of $\mathbb{F}_\pi$ of degree d. Write $\mu_{q_\pi^d-1}(K_u^{\mathrm{sep}})$ for the set of $(q_\pi^d - 1)$-st roots of unity in K_u^{sep} and fix the isomorphism $\mu_{q_\pi^d-1}(K_u^{\mathrm{sep}}) \xrightarrow{\sim} \mathbb{F}^\times$ coming from the reduction map

$\mathcal{O}_{K_u^{\mathrm{sep}}} \twoheadrightarrow \bar{\mathbb{F}}_u$. For a uniformizer ϖ of K_u, choose a solution $\eta \in K_u^{\mathrm{sep}}$ to the equation $X^{q_\pi^d - 1} - \varpi = 0$ and define

$$\begin{array}{cccccc} \omega_{d,K_u}: & I_{K_u} & \to & \mu_{q_\pi^d - 1}(K_u^{\mathrm{sep}}) & \xrightarrow{\sim} \mathbb{F}^\times. \\ & \sigma & \mapsto & \frac{\sigma(\eta)}{\eta} & \end{array}$$

It is independent of the choices of ϖ and η and factors through $I_{K_u}^{\mathrm{t}}$ (cf. [Ser72]).

Definition 4.1.1. The $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_\pi)$-conjugates of ω_{d,K_u}

$$(\omega_{d,K_u})^{q_\pi^i} : I_{K_u}^{\mathrm{t}} \to \mathbb{F}^\times \ \ (0 \le i \le d-1)$$

are called the *fundamental characters* of level d.

It is easy to check that

$$(\omega_{d,K_u})^{1+q_\pi+\cdots+q_\pi^{d-1}} = \omega_{1,K_u}$$

and $(\omega_{d,K_u})^{q_\pi^d - 1} = 1$. For any finite extension L of K_u, we see that $(\omega_{d,K_u})|_{I_L} = (\omega_{d,L})^{e(L/K_u)}$ by definition.

As an analogue of Serre's classical result on the mod ℓ cyclotomic character [Ser72, Proposition 8], the following fact is known.

Proposition 4.1.2 (Kim [Kim09, Proposition 9.4.3. (2)])**.** *The character $(\omega_{1,K_u})^{e_{u|\pi}}$ coincides with the mod π Lubin-Tate character restricted to I_{K_u}.*

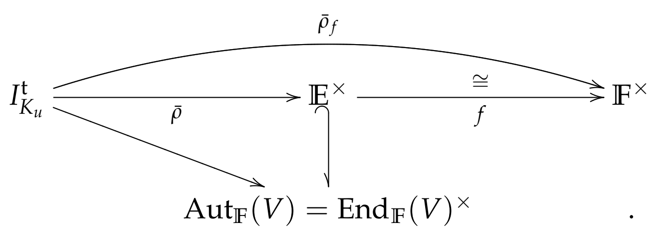
Remark 4.1.3. The *mod π Lubin-Tate character* is the character describing the G_{K_u} action on the π-torsion points of Lubin-Tate formal group over $\mathcal{O}_{K_u}$ associated with π. It is also known that it coincides with the mod π Carlitz character χ_π restricted to I_{K_u}, so that $\chi_\pi = (\omega_{1,K_u})^{e_{u|\pi}}$ on I_{K_u}.

4.1.2 The definition of tame inertia weights Let V be a d-dimensional irreducible $\mathbb{F}_\pi$-representation of I_{K_u}. Then we see that the action of I_{K_u} on V factors through $I_{K_u}^{\mathrm{t}}$ as follows. Since $I_{K_u}^{\mathrm{w}}$ is a normal subgroup of I_{K_u}, the fixed subspace $V^{I_{K_u}^{\mathrm{w}}}$ of V is stable under the action of I_{K_u}. The irreducibility of V implies that $V^{I_{K_u}^{\mathrm{w}}} = V$ or 0. Since $I_{K_u}^{\mathrm{w}}$ is a pro-p group, there is a non-zero element of V fixed by $I_{K_u}^{\mathrm{w}}$ and hence $V^{I_{K_u}^{\mathrm{w}}} = V$. Consequently the wild inertia subgroup $I_{K_u}^{\mathrm{w}}$ acts on V trivially. Thus V can be regarded as a representation of $I_{K_u}^{\mathrm{t}}$.

Using Schur's lemma, we see that $\mathbb{E} := \mathrm{End}_{I^{\mathrm{t}}_{K_u}}(V)$ is a finite field of order q_π^d. Therefore we can regard V as a one-dimensional $\mathbb{E}$-representation of $I^{\mathrm{t}}_{K_u}$. Denote by $\bar{\rho} : I^t_{K_u} \to \mathbb{E}^\times$ the character describing the $I^{\mathrm{t}}_{K_u}$-action on V. Fix an isomorphism $f : \mathbb{E} \xrightarrow{\cong} \mathbb{F}$ and consider the composition

$$\bar{\rho}_f : I^{\mathrm{t}}_{K_u} \xrightarrow{\bar{\rho}} \mathrm{End}_{I^{\mathrm{t}}}(V)^\times \xrightarrow{\sim} \mathbb{F}^\times.$$

Then we have the following commutative diagram:



Since $I^{\mathrm{t}}_{K_u}$ is pro-cyclic and ω_{d,K_u} is surjective, there exists an integer $0 \leq n \leq q_\pi^d - 2$ such that $\bar{\rho}_f = (\omega_{d,K_u})^n$. If we decompose

$$n = j_0 + j_1 q_\pi + \cdots + j_{d-1} q_\pi^{d-1}$$

with integers $0 \leq j_s \leq q_\pi - 1$, then the set $\{j_0, j_1, \ldots, j_{d-1}\}$ is independent of the choice of f.

Definition 4.1.4. For a d-dimensional irreducible $\mathbb{F}_\pi$-representation V of I_{K_u}, the integers $j_0, j_1, \ldots, j_{d-1}$ as above are called the *tame inertia weights* of V. For any $\mathbb{F}_\pi$-representation $\bar{\rho} : G_{K_u} \to \mathrm{Aut}_{\mathbb{F}_\pi}(V)$, the tame inertia weights of $\bar{\rho}$ are the tame inertia weights of all the Jordan-Hölder quotients of $V|_{I_{K_u}}$. Denote by $\mathrm{TI}_{K_u}(\bar{\rho})$ the set of tame inertia weights of $\bar{\rho}$.

Lemma 4.1.5. *Let $\bar{\rho} : G_{K_u} \to \mathrm{Aut}_{\mathbb{F}_\pi}(V)$ be an $\mathbb{F}_\pi$-representation and assume that I_{K_u} acts on V unipotently. Then $\mathrm{TI}_{K_u}(\bar{\rho}) = \{0\}$.*

Proof. By Lemma 3.3.2, the semisimplification $\bar{\rho}^{\mathrm{ss}}$ of $\bar{\rho}$ is isomorphic to a direct sum of the trivial character. Hence $\mathrm{TI}_{K_u}(\bar{\rho}) = \{0\}$ by definition. □

Let us now consider the tame inertia weights of more π representations attached to Drinfeld modules with good reduction. By [Gar01, Theorem 2.14], the following holds.

Proposition 4.1.6. *Let $\phi : A \to K_u\{\tau\}$ be a Drinfeld module. If ϕ has good reduction, then every tame inertia weight j of $\bar{\rho}_{\phi,\pi}$ satisfies $0 \leq j \leq e_{u|\pi}$.*

4.2 Tame inertia weights of stable Drinfeld modules

Fix a monic irreducible element $\pi \in A$. Let u be a finite place of K above π and let $\phi : A \to K_u\{\tau\}$ be a Drinfeld module of rank r. By using Tate uniformization (Proposition 2.4.4), if ϕ has stable reduction, then there exists a unique (up to isomorphism) Tate datum (ψ, Λ) of rank (r_1, r_2) with $r = r_1 + r_2$ corresponding to ϕ. Then $\Lambda/\pi\Lambda \cong \Lambda \otimes_A \mathbb{F}_\pi$ and we have a G_{K_u}-equivariant short exact sequence

$$0 \to \psi[\pi] \to \phi[\pi] \to \Lambda \otimes_A \mathbb{F}_\pi \to 0 \tag{4.2.1}$$

of $\mathbb{F}_\pi$-vector spaces. We consider the following condition (SU) for Drinfeld modules over K_u.

(SU) $\phi : A \to K_u\{\tau\}$ has stable reduction and I_{K_u} acts on $\Lambda \otimes_A \mathbb{F}_\pi$ unipotently.

Then as an extension of Proposition 4.1.6, we obtain the following estimate of tame inertia wights.

Proposition 4.2.1. *Let u be a finite place of K above π. If a Drinfeld module $\phi : A \to K_u\{\tau\}$ satisfies the condition* (SU)*, then every tame inertia weight j of $\bar{\rho}_{\phi,\pi}$ satisfies $0 \leq j \leq e_{u|\pi}$.*

Proof. Let (ψ, Λ) be the Tate datum corresponding to ϕ. Suppose that (ψ, Λ) is of rank (r_1, r_2). Since ψ has good reduction, Proposition 4.1.6 implies that $\mathrm{TI}_{K_u}(\bar{\rho}_{\psi,\pi}) \subset [0, e_{u|\pi}]$. Denote by

$$\bar{\rho}_{\Lambda,\pi} : G_{K_u} \to \mathrm{Aut}_{\mathbb{F}_\pi}(\Lambda \otimes \mathbb{F}_\pi) \cong \mathrm{GL}_{r_2}(\mathbb{F}_\pi)$$

the representation describing the Galois action on $\Lambda \otimes_A \mathbb{F}_\pi$. Since I_{K_u} acts on $\Lambda \otimes_A \mathbb{F}_\pi$ unipotently, Lemma 4.1.5 implies $\mathrm{TI}_{K_u}(\bar{\rho}_{\Lambda,\pi}) = \{0\}$. Since the semisimplification of $\bar{\rho}_{\phi,\pi}$ satisfies $\bar{\rho}^{\mathrm{ss}}_{\phi,\pi} \simeq \bar{\rho}^{\mathrm{ss}}_{\psi,\pi} \oplus \bar{\rho}^{\mathrm{ss}}_{\Lambda,\pi}$ by the above exact sequence (4.2.1), we see that

$$\mathrm{TI}_{K_u}(\bar{\rho}_{\phi,\pi}) = \mathrm{TI}_{K_u}(\bar{\rho}_{\psi,\pi}) \cup \mathrm{TI}_{K_u}(\bar{\rho}_{\Lambda,\pi}),$$

which implies the conclusion. □

We know that every Drinfeld module $\phi : A \to K_u\{\tau\}$ has potentially stable reduction and the Galois action on a ψ-lattice Λ factors through some finite quotient. Hence it follows that there exists a finite extension L/K_u such that $\phi : A \to L\{\tau\}$ satisfies the condition (SU).

We want to take such an L with small ramification index. To do this, we study the ramification of the representation

$$\rho_\Lambda : G_{K_u} \to \mathrm{Aut}_A(\Lambda) \cong \mathrm{GL}_{r_2}(A)$$

since it determines the G_{K_u}-action on $\Lambda \otimes_A \mathbb{F}_\pi$.

Lemma 4.2.2. *Let n be a positive integer and let G be a finite subgroup of $\mathrm{GL}_n(A)$. Then the maximal prime-to-p divisor of $\#G$ is a factor of $\prod_{s=1}^n (q^s - 1)$.*

Proof. Consider the t-adic completion $A_t (\cong \mathbb{F}_q[[t]])$ of A and regard G as a finite subgroup of $\mathrm{GL}_n(A_t)$. Recall that $\Gamma_n(A_t)$ is the kernel of the map $\mathrm{GL}_n(A_t) \twoheadrightarrow \mathrm{GL}_n(\mathbb{F}_q)$ induced by the reduction map $A_t \twoheadrightarrow \mathbb{F}_q$. Since A_t is a complete noetherian local ring whose residue field is finite of characteristic p, Lemma 3.3.3 implies that $\Gamma_n(A_t)$ is a pro-p group. Hence the short exact sequence

$$1 \to \Gamma_n(A_t) \to \mathrm{GL}_n(A_t) \to \mathrm{GL}_n(\mathbb{F}_q) \to 1$$

shows that the maximal prime-to-p divisor of $\#G$ is a factor of $\#\mathrm{GL}_n(\mathbb{F}_q) = q^{n(n-1)/2} \prod_{s=1}^n (q^s - 1)$. Hence it in particular divides $\prod_{s=1}^n (q^s - 1)$. □

Proposition 4.2.3. *Let u be a finite place of K above π and let $\phi : A \to K_u\{\tau\}$ be a Drinfeld module of rank r. Then there is a finite separable tamely ramified extension L/K_u such that*

- *$\phi : A \to K_u\{\tau\} \subset L\{\tau\}$ satisfies the condition* (SU)*,*
- *the ramification index $e(L/K_u)$ divides $(q^r - 1) \prod_{s=1}^{r-1} (q^s - 1)^2$.*

Proof. By Proposition 2.3.4, we can take a finite separable extension L_0/K_u such that ϕ has stable reduction over L_0 and $e(L_0/K_u)$ divides $\prod_{s=1}^r (q^s - 1)$.

Let (ψ, Λ) be the Tate datum over $\mathcal{O}_{L_0}$ corresponding to $\phi : A \to L_0\{\tau\}$. Suppose that Λ is of rank r' $(\leq r-1)$. Consider the representation

$$\rho_\Lambda : G_{L_0} \to \mathrm{Aut}_A(\Lambda) \cong \mathrm{GL}_{r'}(A)$$

and denote by $E \subset K_u^{\mathrm{sep}}$ the fixed subfield by $\ker \rho_\Lambda$. Then the representation is the composition

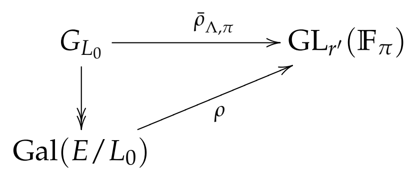
$$\rho_\Lambda : G_{L_0} \twoheadrightarrow \mathrm{Gal}(E/L_0) \hookrightarrow \mathrm{GL}_{r'}(A)$$

of the canonical restriction map and an injection $\mathrm{Gal}(E/L_0) \hookrightarrow \mathrm{GL}_{r'}(A)$. Let L be the maximal tamely ramified extension of L_0 in E. Since $\mathrm{Gal}(E/L_0)$

is isomorphic to a finite subgroup of $\mathrm{GL}_{r'}(A)$, it follows that $e(L/L_0)$ divides $\prod_{s'=1}^{r'}(q^{s'}-1)$ by Lemma 4.2.2. Hence by the assumption on L_0 and $r' \leq r-1$, we see that

$$e(L/K_u) = e(L/L_0)e(L_0/K_u) \mid (q^r - 1)\prod_{s=1}^{r-1}(q^s-1)^2.$$

We prove that the inertia subgroup I_L of L acts on $\Lambda \otimes_A \mathbb{F}_\pi$ unipotently. Since the action of G_E on $\Lambda \otimes_A \mathbb{F}_\pi$ is trivial, we see that the representation $\bar{\rho}_{\Lambda,\pi} : G_{L_0} \to \mathrm{Aut}_{\mathbb{F}_\pi}(\Lambda \otimes_A \mathbb{F}_\pi) \cong \mathrm{GL}_{r'}(\mathbb{F}_\pi)$ factors though a group homomorphism $\rho : \mathrm{Gal}(E/L_0) \to \mathrm{GL}_{r'}(\mathbb{F}_\pi)$.



The image of I_L by $G_{L_0} \twoheadrightarrow \mathrm{Gal}(E/L_0)$ is $\mathrm{Gal}(E/L)$, which is a p-group. We see that $\bar{\rho}_{\Lambda,\pi}(I_L) = \rho(\mathrm{Gal}(E/L))$ is also a p-subgroup of $\mathrm{GL}_{r'}(\mathbb{F}_\pi)$. Hence the I_L-action on $\Lambda \otimes_A \mathbb{F}_\pi$ is unipotent by Lemma 3.3.2 and so ϕ satisfies the condition (SU) over L. □

Remark 4.2.4. A Drinfeld module $\phi : A \to L\{\tau\}$ satisfying (SU) can be regarded as an analogue of a semistable elliptic curves. By the definition of L, for any monic irreducible element $\pi_0 \in A$ with $\pi_0 \neq \pi$, we see that the inertia subgroup I_L acts on $T_{\pi_0}(\psi)$ trivially and on $\Lambda \otimes_A A_{\pi_0}$ unipotently, so that its action on $T_{\pi_0}(\phi)$ is unipotent. Then the analytic τ-sheaf $\tilde{M}(\phi)$ attached to ϕ is *strongly semistable* over L in the sense of [Gar03a, Definition 4.6].

Definition 4.2.5. Let $\phi : A \to K\{\tau\}$ be a Drinfeld module over K. For any finite place u of K above π, we denote by

$$e_u(\phi) := \min\{e(L/F_\pi)\}$$

the minimum of ramification indeces of all finite extensions $L/K_u/F_\pi$ such that $\phi : A \to L\{\tau\}$ satisfies (SU). We also set

$$e_\pi(\phi) := \gcd\{e_u(\phi); u|\pi\},$$

where u runs through all finite places of K above π.

Set

$$C_1 = C_1(q,r) := (q^r - 1)\prod_{s=1}^{r-1}(q^s - 1)^2.$$

Then we have the following.

Lemma 4.2.6. *Suppose that $\phi : A \to K\{\tau\}$ is of rank r and $[K : F] = n$.*

(1) *For any finite place $u|\pi$ of K, the index $e_u(\phi)$ divides $e_{u|\pi}C_1(q,r)$.*

(2) *$e_\pi(\phi)$ divides $nC_1(q,r)$.*

(3) *If π is unramified in K_{s}, then $e_\pi(\phi)$ divides $[K : F]_{\mathrm{i}}C_1(q,r)$.*

Proof. Let u be a finite place of K above π. Then by Proposition 4.2.3 we see that there is a finite extension L/K_u such that ϕ satisfies (SU) over L and $e(L/K_u) \mid C_1(q,r)$. Hence (1) holds. Since $n = \sum_{u|\pi} e_{u|\pi}f_{u|\pi}$ holds, we see that n is divisible by $\gcd\{e_{u|\pi}\}$. Hence $nC_1(q,r)$ is divisible by $e_\pi(\phi)$, so that (2) holds. Finally if π is unramified in K_{s}, then $e_{u|\pi} = [K : F]_{\mathrm{i}}$ holds. Therefore (1) implies (3). □

4.3 Ramification of constrained torsion points

In this section, by showing some non-trivial properties of the index $e_\pi(\phi)$ defined in the previous section, we prove some non-existence theorems on certain Drinfeld modules. As a corollary of them, we obtain a part of Theorem 1.0.2.

Let K be a finite extension of F and let $\pi \in A$ be a monic irreducible element. Denote by $n := [K : F]$ the degree of K/F. Also let r be a positive integer. For any positive integer d, we define a set $\mathcal{D}(K,r,\pi,d)$ satisfying $\mathscr{D}(K,r,\pi) \subset \mathcal{D}(K,r,\pi,d)$ as follows. Recall that $\mathscr{D}(K,r,\pi)$ consists of all K-isomorphism classes $[\phi]$ of Drinfeld modules $\phi : A \to K\{\tau\}$ of rank r over K satisfying the conditions (D1) and (D2); see Chapter 1. We now replace (D1) with the following general condition:

(D1)′ There exists a monic irreducible element $\pi_0 \in A$ with $\deg(\pi_0) \le d$ such that ϕ has good reduction at a finite place v of K above π_0.

Definition 4.3.1. Define $\mathcal{D}(K,r,\pi,d)$ to be the set of K-isomorphism classes of Drinfeld modules $\phi : A \to K\{\tau\}$ of rank r satisfying (D1)′ and (D2).

Let ϕ be a Drinfeld module with $[\phi] \in \mathcal{D}(K,r,\pi,d)$. By the condition (D2), it follows that the semisimplification $\bar{\rho}^{\mathrm{ss}}_{\phi,\pi}$ is of the form

$$\bar{\rho}^{\mathrm{ss}}_{\phi,\pi} \cong \chi_\pi^{i_1} \oplus \cdots \oplus \chi_\pi^{i_r}$$

for integers $0 \le i_1,\ldots,i_r < q_\pi - 1$.

Lemma 4.3.2. *Let $[\phi] \in \mathcal{D}(K, r, \pi, d)$ be as above and let u be a finite place of K above π. Then for each $1 \leq s \leq r$, there exists an integer j_s with $0 \leq j_s \leq e_u(\phi)$ such that*

$$i_s e_u(\phi) \equiv j_s \pmod{q_\pi - 1}$$

holds.

Proof. By Proposition 4.2.3, there is a finite extension L/K_u with $e(L/F_\pi) = e_u(\phi)$ such that ϕ satisfies the condition (SU) over L. Then it follows that $\mathrm{TI}_L(\bar{\rho}_{\phi,\pi}|_{G_L}) \subset [0, e_u(\phi)]$ by Proposition 4.2.1. For any irreducible factor $\chi_\pi^{i_s}$ of $\bar{\rho}_{\phi,\pi}^{\mathrm{ss}}$, we have

$$\chi_\pi^{i_s}|_{I_L} = (\omega_{L,1})^{j_s}$$

for some $j_s \in \mathrm{TI}_L(\bar{\rho}_{\phi,\pi}|_{G_L})$. Since $\chi_\pi|_{I_L} = (\omega_{1,L})^{e_u(\phi)}$ by Remark 4.1.3, we have

$$(\omega_{1,L})^{i_s e_u(\phi)} = (\omega_{1,L})^{j_s},$$

which implies the result. □

Recall that $C_1(q,r) = (q^r - 1)\prod_{s=1}^{r-1}(q^s - 1)^2$. Define a positive constant C_2' by

$$C_2' = C_2'(n, q, r, d) := drn^2 C_1(q, r).$$

Then we obtain the following important proposition.

Proposition 4.3.3. *Let $[\phi] \in \mathcal{D}(K, r, \pi, d)$ be as in Lemma 4.3.2 and let u be a finite place of K above π. Suppose that* $\deg(\pi) > C_2'$. *Then $e_u(\phi)$ is divisible by r and the congruence*

$$i_s e_u(\phi) \equiv \frac{e_u(\phi)}{r} \pmod{q_\pi - 1}$$

holds for any $1 \leq s \leq r$.

Proof. Set $e_u = e_u(\phi)$ for short. By the condition (D1)′, we can take a monic irreducible element $\pi_0 \in A$ with $\deg(\pi_0) \leq d$ and a finite place v of K above π_0 at which ϕ has good reduction. Notice that the π_0 is distinct from π since $\deg(\pi) > C_2' > \deg(\pi_0)$. Then we can consider the characteristic polynomial

$$P_{v,e_u}(T) = \det(T - \rho_{\phi,\pi}(\mathrm{Frob}_v^{e_u})|T_\pi(\phi)) \in A[T]$$

of $\mathrm{Frob}_v^{e_u}$. Denote by $\{\alpha_s\}_{s=1}^r$ the roots of the characteristic polynomial $P_v(T)$ of Frob_v. Then the roots of $P_{v,e_u}(T)$ are given by $\{\alpha_s^{e_u}\}_{s=1}^r$. On the other hand, the condition (D2) implies that the roots of the polynomial

$$\bar{P}_{v,e_u}(T) := P_{v,e_u}(T) \pmod{\pi} \in \mathbb{F}_\pi[T]$$

are given by $\{\chi_\pi(\mathrm{Frob}_v)^{i_s e_u}\}_{s=1}^r$. Set $\pi_v := \pi_0^{f_{v|\pi_0}}$. Then we have

$$|\pi_v| = q_v = q^{f_{v|\pi_0}\deg(\pi_0)}.$$

For any $1 \leq s \leq r$, Lemma 4.3.2 implies that $\chi_\pi(\mathrm{Frob}_v)^{i_s e_u} = \chi_\pi(\mathrm{Frob}_v)^{j_s}$ for some integer $0 \leq j_s \leq e_u$. Since $\chi_\pi(\mathrm{Frob}_v)^{j_s} \equiv \pi_v^{j_s} \pmod{\pi}$ holds by Remark 2.5.6, we obtain

$$\bar{P}_{v,e_u}(T) = \prod_{s=1}^{r}(T - \chi_\pi(\mathrm{Frob}_v)^{j_s}) \equiv \prod_{s=1}^{r}(T - \pi_v^{j_s}) \pmod{\pi}. \tag{4.3.1}$$

For each integer $0 \leq k \leq r$, denote by

$$S_k(x_1, \ldots, x_r) = \sum_{1\leq s_1 < \cdots < s_k \leq r} x_{s_1}x_{s_2}\cdots x_{s_k}$$

the fundamental symmetric polynomial of degree k with r variables $x_1, \ldots, x_r$. Then we have

$$\prod_{s=1}^{r}(T - x_s) = \sum_{k=0}^{r}(-1)^k S_k(x_1, \ldots, x_r)T^{r-k}.$$

Notice that $|\alpha_s^{e_u}| = q_v^{e_u/r}$ holds for any $1 \leq s \leq r$ by Proposition 2.3.11. Since $0 \leq j_s \leq e_u$ for each s, we have

$$\begin{aligned}\left|S_k(\alpha_1^{e_u}, \ldots, \alpha_r^{e_u}) - S_k(\pi_v^{j_1}, \ldots, \pi_v^{j_r})\right| &\leq \max_{1\leq s_1<\cdots<s_k\leq r}\left\{q_v^{\frac{ke_u}{r}}, q_v^{j_{s_1}+\cdots+j_{s_k}}\right\} \\ &\leq q_v^{ke_u} \\ &\leq q_v^{re_u} = q^{re_u f_{v|\pi_0}\deg(\pi_0)}\end{aligned}$$

for any $0 \leq k \leq r$. We know that e_u divides $e_{u|\pi}C_1(q,r)$ by Lemma 4.2.6. Clearly both $e_{u|\pi}$ and $f_{v|\pi_0}$ are less than or equal to $n = [K : F]$. We now suppose that $\deg(\pi) > C_2' = drn^2C_1(q,r)$ and hence we have

$$q^{re_u f_{v|\pi_0}\deg(\pi_0)} \leq q^{C_2'} < q^{\deg(\pi)} = |\pi|.$$

It means that all absolute values of coefficients of $P_{v,e_u}(T) - \prod_{s=1}^r(T - \pi_v^{j_s})$ are smaller than $|\pi|$. Hence the congruence (4.3.1) implies

$$P_{v,e_u}(T) = \prod_{s=1}^{r}(T - \pi_v^{j_s}).$$

Comparing the absolute values of the roots of $P_{v,e_u}(T)$ and $\prod_{s=1}^r(T - \pi_v^{j_s})$, we see that $e_u/r = j_s$ for any $1 \leq s \leq r$. Hence e_u/r is an integer and Lemma 4.3.2 implies the conclusion. □

Recall that $\mathscr{F}_n(F)$ is the set of finite extensions K of F with $n = [K : F]$. We denote by v_p the normalized p-adic valuation of $\mathbb{Q}$. Then any positive integer r is written as $r = r_0 p^{v_p(r)}$ for some integer r_0 not divisible by p. We have the following uniform non-existence result.

Theorem 4.3.4. *Let r, d, and n be positive integers and let $\pi \in A$ be a monic irreducible element. Suppose that n is not divisible by $p^{v_p(r)}$. If $\deg(\pi) > C'_2(n, q, r, d)$, then the set $\mathcal{D}(K, r, \pi, d)$ is empty for all $K \in \mathscr{F}_n(F)$.*

Proof. Let K/F be a finite extension of degree n. Assume that $\mathcal{D}(K, r, \pi, d)$ is not empty. Then for any $[\phi] \in \mathcal{D}(K, r, \pi, d)$ and any finite place u of K above π, Proposition 4.3.3 implies that $e_u(\phi)$ is divisible by r. Hence by Lemma 4.2.6 (2), we have

$$r \mid e_\pi(\phi) = \gcd\{e_u(\phi)\} \mid nC_1(q, r).$$

Since $C_1(q, r)$ is not divisible by p, it implies $p^{v_p(r)} | n$, which contradict to the assumption. □

In the case where $d = 1$, define

$$C_2 = C_2(n, q, r) := C'_2(n, q, r, 1).$$

Then we have the following uniform result.

Corollary 4.3.5. *Let the notations and hypothesis be as in Theorem 4.3.4. If $\deg(\pi) > C_2(n, q, r)$, then the set $\mathscr{D}(K, r, \pi)$ is empty for all $K \in \mathscr{F}_n(F)$.*

Proof. Since $\mathscr{D}(K, r, \pi) \subset \mathcal{D}(K, r, \pi, 1)$ holds, the result immediately follows from Theorem 4.3.4. □

Definition 4.3.6. Define $\mathcal{D}(K, r, \pi, d)_{\mathrm{SU}}$ to be the subset of $\mathcal{D}(K, r, \pi, d)$ which consists of all elements $[\phi] \in \mathcal{D}(K, r, \pi, d)$ such that $\phi : A \to K_u\{\tau\}$ satisfies (SU) for any finite place u of K above π. Also define $\mathscr{D}(K, r, \pi)_{\mathrm{SU}}$ in the same way, so that

$$\mathscr{D}(K, r, \pi)_{\mathrm{SU}} = \mathscr{D}(K, r, \pi) \cap \mathcal{D}(K, r, \pi, d)_{\mathrm{SU}}$$

holds for any positive integer d.

Theorem 4.3.7. *Let r, d, and n be positive integers and let $\pi \in A$ be a monic irreducible element. Suppose that $\deg(\pi) > C'_2(n, q, r, d)$ and n is not divisible by r. Then the set $\mathcal{D}(K, r, \pi, d)_{\mathrm{SU}}$ is empty for all $K \in \mathscr{F}_n(F)$.*

Proof. Let K/F be a finite extension of degree n. Assume that $\mathcal{D}(K,r,\pi,d)_{\mathrm{SU}}$ is not empty. Then we can take $[\phi] \in \mathcal{D}(K,r,\pi,d)_{\mathrm{SU}}$. For any finite place u of K above π, it follows that $e_u(\phi) = e_{u|\pi}$ by the definition of $e_u(\phi)$. By Proposition 4.3.3, we see that $e_u(\phi)$ is divisible by r. Thus we obtain

$$r \mid e_\pi(\phi) = \gcd\{e_{u|\pi}\} \mid \sum e_{u|\pi} f_{u|\pi} = n,$$

which contradicts to the assumption on n. □

The following is an analogue of [RT17, Corollary 3.8]:

Corollary 4.3.8. *Let the notations be as in Theorem 4.3.7. Suppose that* $\deg(\pi) > C_2(n,q,r)$ *and n is not divisible by r. Then the set $\mathscr{D}(K,r,\pi)_{\mathrm{SU}}$ is empty for all $K \in \mathscr{F}_n(F)$.*

Proof. Since $\mathscr{D}(K,r,\pi)_{\mathrm{SU}} \subset \mathcal{D}(K,r,\pi,1)_{\mathrm{SU}}$ holds, the result immediately follows from Theorem 4.3.7. □

For any finite separable extension L/F, let $\{\pi_1,\ldots,\pi_k\}$ be the set of finite places of F which are ramified in L and define

$$C_3 = C_3(L) := \max\{\deg(\pi_1),\ldots,\deg(\pi_k)\}.$$

Recall that we denote by K_{s} the separable closure of F in K. Consider the two positive constants

$$C_4' = C_4'(n,q,r,K_{\mathrm{s}},d) := \max\{C_2'(n,q,r,d), C_3(K_{\mathrm{s}})\}$$

and

$$C_4 = C_4(n,q,r,K_{\mathrm{s}}) := C_4'(n,q,r,K_{\mathrm{s}},1).$$

Then we obtain a part of Theorem 1.0.2.

Theorem 4.3.9. *Let d be a positive integer. Let K/F be a finite extension of degree n and let $\pi \in A$ be a monic irreducible element. Suppose that $[K:F]_{\mathrm{i}} C_1(q,r)$ is not divisible by r.*

(1) *If $\deg(\pi) > C_4'(n,q,r,K_{\mathrm{s}},d)$, then the set $\mathcal{D}(K,r,\pi,d)$ is empty.*

(2) *If $\deg(\pi) > C_4(n,q,r,K_{\mathrm{s}})$, then the set $\mathscr{D}(K,r,\pi)$ is empty.*

Proof. It suffices to prove (1). Assume that $\deg(\pi) > C_4'(n,q,r,K_{\mathrm{s}},d)$ and $\mathcal{D}(K,r,\pi,d)$ is not empty. Take $[\phi] \in \mathcal{D}(K,r,\pi,d)$. Then π is unramified in K_{s} since $\deg(\pi) > C_3(K_{\mathrm{s}})$. Hence we have

$$r \mid e_\pi(\phi) \mid [K:F]_{\mathrm{i}} C_1(q,r)$$

by Proposition 4.3.3 and Lemma 4.2.6 (3). It contradicts the assumption. Hence $\mathcal{D}(K,r,\pi,d)$ is empty □

Remark 4.3.10. In particular the above non-existence theorem holds when $r = p^{\nu} > 1$ does not divide $[K : F]_{\mathrm{i}}$. Indeed the relation in the proof of Theorem 4.3.9 implies

$$r \mid [K : F]_{\mathrm{i}}$$

since $C_1(q, r)$ is not divisible by p.

Chapter 5

Observations at places with small degree

As usual, let K/F be a finite extension and let r be a positive integer. Let $\pi \in A$ be a monic irreducible element. The aim of Chapter 5 is to give the proof of Theorem 1.0.2 in the case where r is not a p-power.

After recalling basic facts on divisors of function fields in §5.1 and introducing the statement of the effective version of the Chebotarev density theorem in §5.2, we consider an existence problem of an *m-th power residue modulo* π (Definition 5.3.1) for a positive integer $m | q_\pi - 1$ in §5.3. By using the effective version of the Chebotarev density theorem, we see that there exists an m-th power residue modulo π whose degree is smaller than $\deg(\pi)$ if $\deg(\pi)$ is sufficiently large (Propositions 5.3.4). On the other hand, for any $[\phi] \in \mathscr{D}(K, r, \pi)$, we define in §5.4 an integer m_ϕ and a character $\chi(m_\phi)$. We show the property that $\chi(m_\phi)$ never vanishes on the Frobenius elements of places with some conditions (Proposition 5.4.3). It contradicts the consequence of §5.3 if $\deg(\pi)$ is sufficiently large and therefore we have the non-existence result.

5.1 Divisors of function fields

We introduce some notations and properties of divisors of function fields in this section. Denote by $\mathrm{Div}(K)$ the divisor group of K, that is, the free abelian group generated by all places of K. We write divisors additively, so that a typical divisor is of the form $D = \sum_v n_v v$ for some integers $n_v \in \mathbb{Z}$ such that $n_v = 0$ for almost all v. For any place v of K, the notation $v \notin D$ means that $n_v = 0$.

Recall that we write $\mathbb{F}_K$ for the constant field of K. The *degree* of a place v of K is defined by $\deg_K v := [\mathbb{F}_v : \mathbb{F}_K]$ and it is extended to any divisor $D = \sum_v n_v v$ by $\deg_K D = \sum_v n_v \deg_K v$. Notice that the degree $\deg_F \pi$ of a finite place π of F is exactly the degree $\deg(\pi)$ as a polynomial.

For any $\lambda \in K^\times$, the value $v(\lambda)$ is zero for all but finitely many places v of K. A divisor of the form $(\lambda) = \sum_v v(\lambda)v$ is called a *principal divisor*. Denote by $\mathrm{P}(K)$ the subgroup of $\mathrm{Div}(K)$ consisting of all principal divisors. The quotient $\mathrm{Cl}_K := \mathrm{Div}(K)/\mathrm{P}(K)$ is called the *divisor class group* of K.

A divisor $D = \sum_v n_v v$ is said to be *effective* if $n_v \geq 0$ for all v, and then we write $D \geq 0$. Set

$$\mathcal{L}(D) := \{\lambda \in K^\times ; (\lambda) + D \geq 0\} \cup \{0\},$$

which is a finite dimensional $\mathbb{F}_K$-vector space. Set $\ell(D) := \dim_{\mathbb{F}_K} \mathcal{L}(D)$.

Theorem 5.1.1 (the Riemann-Roch theorem)**.** *There exist an integer $g \geq 0$ and a divisor class $\mathscr{C} \in \mathrm{Cl}_K$ such that for any $C \in \mathscr{C}$ and $D \in \mathrm{Div}(K)$, we have*

$$\ell(D) = \deg D - g + 1 + \ell(C - D).$$

The integer g is uniquely determined by K.

Proof. See [Ros02, Chapter 6] for example. □

The unique non-negative integer as in Theorem 5.1.1 is called the *genus* of K and denoted by g_K.

Remark 5.1.2. Since K is a finitely generated field of transcendental degree one over the finite field $\mathbb{F}_K$, it coincides with the field of rational functions on a smooth projective curve X defined over $\mathbb{F}_K$ by [Liu02, Chapter 7.3 Proposition 3.13]. Then g_K is the genus of the projective curve X.

Suppose that L is a finite separable extension of K. Then the *conorm map* $i_{L/K} : \mathrm{Div}(K) \to \mathrm{Div}(L)$ is defined to be the linear extension of

$$i_{L/K} v = \sum_{w|v} e_{w|v} w,$$

where v is a place of K and w runs through all places of L above v. Recall that $[L : K]_{\mathrm{g}}$ is the geometric extension degree of L/K (see § 2.1).

Lemma 5.1.3. *Let w be a place of L above a place v of K and $D \in \mathrm{Div}(K)$. Then*

$$\deg_L i_{L/K} D = [L : K]_{\mathrm{g}} \deg_K D \text{ and } \deg_L w = \frac{f_{w|v}}{[\mathbb{F}_L : \mathbb{F}_K]} \deg_K v.$$

Proof. See [Ros02, Proposition 7.7] for example. □

Let w be a place of L above a place v of K. Recall that we denote by $\mathfrak{p}_w$ the maximal ideal of $\mathcal{O}_{L_w}$. Define δ_w to be the exact power of $\mathfrak{p}_w$ dividing the different of $\mathcal{O}_{L_w}$ over $\mathcal{O}_{K_v}$. Then it follows that $\delta_w \geq e_{w|v} - 1$ with equality holding if and only if $e_{w|v}$ is not divisible by p (see [Ros02, Corollary 2 of Lemma 7.10]). Define the *ramification divisor* of L/K by $\mathcal{D}_{L/K} = \sum_w \delta_w w$.

Lemma 5.1.4. *For any intermediate field K' of L/K, we have*

$$\mathcal{D}_{L/K} = \mathcal{D}_{L/K'} + i_{L/K'}\mathcal{D}_{K'/K}.$$

Proof. See [Ser79, Chapter III 4] for example. □

Hence $\mathcal{D}_{L/K'} \leq \mathcal{D}_{L/K}$ holds. In addition, the following holds (cf. [CL13, Lemma 2.6]).

Lemma 5.1.5. *Let L/K and L'/K be finite separable extensions. Then*

$$\mathcal{D}_{LL'/K} \leq i_{LL'/L}\mathcal{D}_{L/K} + i_{LL'/L'}\mathcal{D}_{L'/K}.$$

5.2 The Effective Chebotarev density theorem

Let E be a finite Galois extension of K and set $G := \mathrm{Gal}(E/K)$. Let v be a place of K and suppose that it is unramified in E. Then for every place w of E above v, the Frobenius element $\mathrm{Fr}_{w|v} \in G$ is well-defined. It follows that the subset

$$\left[\frac{E/K}{v}\right] := \{\mathrm{Fr}_{w|v}; w|v\ \} \subset G$$

is a conjugacy class in G, which is called the *Frobenius conjugacy class* at v. If E/K is an abelian extension, then the conjugacy class determines an element $(v, E/K) \in G$, which is called the *Artin automorphism* for v.

Define $\Sigma_{E/K}$ to be the divisor of K that is the sum of all ramified places of K in E. Let $\mathscr{C} \subset G$ be a conjugacy class. For a positive integer $N > 0$, denote by $\pi_{\mathscr{C}}(N)$ the number of places v of K with $v \notin \Sigma_{E/K}$ such that $\deg_K v = N$ and $\left[\frac{E/K}{v}\right] = \mathscr{C}$. Also denote by $\pi(N)$ the number of places $v \notin \Sigma_{E/K}$ of K such that $\deg_K v = N$. Set $q_K = \#\mathbb{F}_K$ and write $\varphi \in G_{\mathbb{F}_K}$ for the Frobenius element, so that $\varphi(x) = x^{q_K}$ for $x \in \bar{\mathbb{F}}_K$. Kumar and Scherk proved the following effective version of the Chebotarev density theorem:

Theorem 5.2.1 (Kumar and Scherk [KS94, Theorem 1])**.** *Let E/K be a finite Galois extension with Galois group G. Set $d := [\mathbb{F}_E : \mathbb{F}_K]$. Suppose that $\mathscr{C} \subset G$*

is a conjugacy class whose restriction to $\mathbb{F}_E$ is $\varphi^N|_{\mathbb{F}_E}$ for some integer N. Then

$$\left|\pi_{\mathscr{C}}(N) - d\frac{\#\mathscr{C}}{\#G}\pi(N)\right| \leq 2g_E\frac{\#\mathscr{C}}{\#G}\frac{q_K^{N/2}}{N} + 2(2g_K+1)\#\mathscr{C}\frac{q_K^{N/2}}{N} + (1+\frac{\#\mathscr{C}}{N})\deg_K \Sigma_{E/K}$$

holds.

As a consequence of this theorem, Chen and Lee prove the following estimate.

Proposition 5.2.2 (Chen and Lee [CL13, Corollary 3.4])**.** *Let E/K be a finite Galois extension and Σ a divisor of K such that $\Sigma \geq \Sigma_{E/K}$. Set $d_0 := [\mathbb{F}_K : \mathbb{F}_q]$ and $d := [\mathbb{F}_E : \mathbb{F}_K]$. Define the constant $B = B(E/K, \Sigma)$ by*

$$B = \max\{\deg_K \Sigma, \deg_E \mathcal{D}_{E/\mathbb{F}_E K}, 2[E : \mathbb{F}_E K] - 2, 1\}.$$

Then for any nonempty conjugacy class $\mathscr{C}$ in $\mathrm{Gal}(E/K)$, there exists a place v of K with $v \notin \Sigma$ such that

- $\mathscr{C} = \left[\frac{E/K}{v}\right]$,
- $\deg_K v \leq \frac{4}{d_0}\log_q \frac{4}{3}(B + 3g_K + 3) + d.$

5.3 Existence of m-th power residues modulo π

Let $\pi \in A$ be a monic irreducible element. Let K be a finite extension of F and suppose that $[K : F] = n$. In this section, we fix an integer $m \geq 1$ with $m \mid \#\mathbb{F}_\pi^\times = q_\pi - 1$.

Definition 5.3.1. A non-zero element $\mathfrak{n} \in A$ satisfying $(\mathfrak{n}, \pi) = 1$ is called an *m-th power residue modulo π* if $\mathfrak{n} \equiv a^m \pmod{\pi}$ for some $a \in A$.

As an application of Proposition 5.2.2, we will show that one can find an m-th power residue modulo π whose degree is smaller than $\deg(\pi)$ if $\deg(\pi)$ is sufficiently large. Take a generator ζ_π of $\mathcal{C}[\pi]$. Denote by F_m the unique subfield of $F(\zeta_\pi)$ with $[F_m : F] = m$ and consider the character $\chi(m) : G_F \xrightarrow{\chi_\pi} \mathbb{F}_\pi^\times \twoheadrightarrow \mathbb{F}_\pi^\times/(\mathbb{F}_\pi^\times)^m$.

Lemma 5.3.2. *For a monic irreducible element $\pi_0 \in A$, the following are equivalent.*

- *π_0 is an m-th power residue modulo π,*

- $\chi(m)(\mathrm{Frob}_{\pi_0}) = 1$,
- $\mathrm{Frob}_{\pi_0}|_{F_m} = \mathrm{id}$.

Proof. It is trivial when $m = 1$. If not, then this lemma immediately follows from that $\chi_\pi(\mathrm{Frob}_{\pi_0}) \equiv \pi_0 \pmod{\pi}$ and F_m is the fixed subfield of F^{sep} by $\ker \chi(m)$. □

Denote by $\tilde{K}$ the Galois closure of K_{s} over F. Set $E := \tilde{K}F_m$, which is also a Galois extension of F. Consider the divisor

$$\Sigma := \Sigma_{E/F} + \pi + \infty \in \mathrm{Div}(F)$$

and the constant

$$B = B(E/F, \Sigma) = \max\{\deg_F \Sigma, \deg_E \mathcal{D}_{E/\mathbb{F}_E F}, 2[E : \mathbb{F}_E F] - 2, 1\}.$$

Let us compute a bound of B. Since the degree $[\tilde{K} : F]$ is less than or equal to $n!$, we see that $[\mathbb{F}_{\tilde{K}} : \mathbb{F}_q] \leq n!$ and so $[E : \mathbb{F}_E F] \leq m \cdot n!$. Then we obtain the following important lemma.

Lemma 5.3.3. *If* $\deg(\pi) > C_3(K_{\mathrm{s}})$, *then there exist two positive constants* B_1 *and* B_2 *depending only on* $K_{\mathrm{s}}, n, q,$ *and* m *such that*

$$B \leq B_1 \deg(\pi) + B_2.$$

In particular for any positive $N > 0$, *one can take a positive constant* $C_5 = C_5(K_{\mathrm{s}}, n, q, m, N) > 0$ *such that if* $\deg(\pi) > C_5$, *then*

$$4 \log_q \frac{4}{3}(B + 3) + [\mathbb{F}_{\tilde{K}} : \mathbb{F}_q] < \frac{1}{N} \deg(\pi)$$

holds.

Proof. Notice that $\deg(\pi) > C_3(K_{\mathrm{s}})$ implies that π is unramified in K_{s}. By Proposition 2.5.7, the infinite place ∞ of F splits into at most m places in F_m whose ramification indices divide $q - 1$ and π is totally ramified in F_m. Thus we see that

$$\deg_F \Sigma \leq \deg_F(\Sigma_{F_m/F} + \Sigma_{\tilde{K}/F} + \pi + \infty) \leq 2\deg(\pi) + 2 + \deg_F \Sigma_{\tilde{K}/F}.$$

Now $\mathcal{D}_{E/\mathbb{F}_E F} = \mathcal{D}_{E/F}$ holds. Lemmas 5.1.3 and 5.1.5 imply

$$\begin{aligned} \deg_E \mathcal{D}_{E/F} &\leq \deg_E i_{E/\tilde{K}} \mathcal{D}_{\tilde{K}/F} + \deg_E i_{E/F_m} \mathcal{D}_{F_m/F} \\ &\leq m \deg_{\tilde{K}} \mathcal{D}_{\tilde{K}/F} + [E : F_m]_{\mathrm{g}} \deg_{F_m}(\sum_{v|\infty} (q-2)v + m\pi) \\ &\leq m \deg_{\tilde{K}} \mathcal{D}_{\tilde{K}/F} + m \cdot n!(q - 2 + \deg(\pi)). \end{aligned}$$

Hence there exist positive constants B_1 and B_2 depending only on K_{s}, n, q, and m such that $B \leq B_1 \deg(\pi) + B_2$ holds. Therefore if $\deg(\pi)$ is sufficiently large with respect to K_{s}, n, q, m, and N, then $4 \log_q \frac{4}{3}(B+3) + [\mathbb{F}_{\tilde{K}} : \mathbb{F}_q] < \frac{1}{N} \deg(\pi)$ holds. □

Proposition 5.2.2 and Lemma 5.3.3 imply the following:

Proposition 5.3.4. *Let N be a positive integer. If $\deg(\pi) > C_5$, then there exist a monic irreducible element $\pi_0 \in A$ and a place v of K above π_0 such that*

- *π_0 is an m-th power residue modulo π,*
- *$\deg(\pi_0) < \frac{1}{N} \deg(\pi)$,*
- *$f_{v|\pi_0} = 1$.*

Proof. We may assume that $K = K_{\mathrm{s}}$ since the extension K/K_{s} is totally ramified at any place. Let $\tilde{K}$ and $E = \tilde{K}F_m$ be as above and fix an element $\sigma \in \mathrm{Gal}(E/F)$ such that $\sigma|_{KF_m} = \mathrm{id}$. For the conjugacy class

$$\mathscr{C} = \{g\sigma g^{-1}; g \in \mathrm{Gal}(E/F)\}$$

of σ in $\mathrm{Gal}(E/F)$, by Proposition 5.2.2 and Lemma 5.3.3 there exists a place π_0 of F with $\pi_0 \notin \Sigma$ (hence it is a finite place) such that

- $\left[\frac{E/F}{\pi_0}\right] = \mathscr{C}$,
- $\deg(\pi_0) < \frac{1}{N} \deg(\pi)$,

so that $\sigma = \mathrm{Fr}_{w|\pi_0}$ for some place w of E. Then the decomposition group Z_w of w over π_0 is generated by σ and it is a subgroup of $\mathrm{Gal}(E/KF_m)$. Denote by K' the fixed subfield of E by Z_w. Then we see that the place v' of K' below w satisfies $e_{v'|\pi_0} = 1$ and $f_{v'|\pi_0} = 1$. Hence $f_{v|\pi_0} = 1$, where v is the place of K below v'. By construction, we see that $\mathrm{Frob}_v|_{F_m} = \mathrm{id}$. Lemma 5.3.2 means that π_0 is an m-th power residue modulo π. □

5.4 Non-p-power rank case

Fix a Drinfeld module $\phi : A \to K\{\tau\}$ of rank r satisfying $[\phi] \in \mathscr{D}(K, r, \pi)$. Suppose that $[K : F] = n$. In this section, we always assume that

$$r = r_0 p^{\nu}$$

for some $r_0 > 1$ not divisible by p.

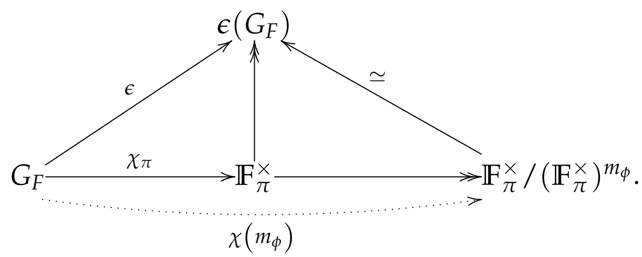
Now let $i_1, \dots, i_r$ be the positive integers satisfying $\bar{\rho}^{\mathrm{ss}}_{\phi,\pi} \simeq \chi_\pi^{i_1} \oplus \cdots \oplus \chi_\pi^{i_r}$ by (D2). Set

$$\mathbb{S}_r := \{\mathbf{s} = (s_1, \dots, s_r) \in \mathbb{Z}^r ; 1 \le s_k \le r\}.$$

For any $\mathbf{s} = (s_1, \dots, s_r) \in \mathbb{S}_r$, set $\varepsilon_{\mathbf{s}} := {\chi_\pi}^{i_{s_1} + \cdots + i_{s_r} - 1}$ and define

$$\epsilon := (\varepsilon_{\mathbf{s}})_{\mathbf{s} \in \mathbb{S}_r} : G_F \to (\mathbb{F}_\pi^\times)^{\oplus r^r}.$$

Set $m_\phi := \#\epsilon(G_F)$, which is the least common multiple of the orders of $\varepsilon_{\mathbf{s}}$. Since ϵ factors through $\chi_\pi : G_F \to \mathbb{F}_\pi^\times$, the image $\epsilon(G_F)$ is cyclic and $m_\phi | (q_\pi - 1)$. Then we obtain the following commutative diagram



Hence a monic irreducible element $\pi_0 \in A$ is an m_ϕ-th power residue modulo π if and only if $\varepsilon_{\mathbf{s}}(\mathrm{Frob}_{\pi_0}) = 1$ for any $\mathbf{s} \in \mathbb{S}_r$.

Lemma 5.4.1. *Suppose that* $\deg(\pi) > C_2$. *For any* $(s_1, \dots, s_r) \in \mathbb{S}_r$, *the relation* $e_\pi(\phi)(i_{s_1} + \cdots + i_{s_r} - 1) \equiv 0 \pmod{q_\pi - 1}$ *holds.*

Proof. By Proposition 4.3.3, we see that $i_s e_\pi(\phi) \equiv \frac{e_\pi(\phi)}{r} \pmod{q_\pi - 1}$. Adding these congruences for $s_1, \dots, s_r$ gives

$$e_\pi(\phi)(i_{s_1} + \cdots + i_{s_r}) \equiv e_\pi(\phi) \pmod{q_\pi - 1}.$$

□

Lemma 5.4.2. *If* $\deg(\pi) > C_2(n, q, r)$, *then* m_ϕ *divides the greatest common divisor* $(e_\pi(\phi), q_\pi - 1)$. *In particular, it divides* $nC_1(q, r)$.

Proof. By Lemma 5.4.1, we see that $\varepsilon_{\mathbf{s}}^{e_\pi(\phi)} = 1$ for all $\mathbf{s} \in \mathbb{S}_r$. Hence we have $m_\phi \mid e_\pi(\phi)$ and so m_ϕ divides $(e_\pi(\phi), q_\pi - 1)$. □

Proposition 5.4.3. *If there exist a monic irreducible element* $\pi_0 \in A$ *and a finite place* v *of* K *above* π_0 *such that* $\deg(\pi) > f_{v|\pi_0} \deg(\pi_0)$ *and* $f_{v|\pi_0}$ *is not divisible by* r_0, *then both* $m_\phi > 1$ *and* $\chi(m_\phi)(\mathrm{Frob}_v) \neq 1$ *hold.*

Proof. Assume that either $m_\phi = 1$ or $\chi(m_\phi)(\mathrm{Frob}_v) = 1$ holds. Then it follows that $\varepsilon_{\mathbf{s}}(\mathrm{Frob}_v) = 1$ for any $\mathbf{s} \in \mathbb{S}_r$. Denote by $a_{v,p^\nu} \in A$ the coefficient of T^{r-p^ν} in the characteristic polynomial $P_v(T)$ of Frob_v on $T_\pi(\phi)$. It is given by

$$a_{v,p^\nu} = (-1)^{p^\nu} S_{p^\nu}(\alpha_1, \ldots, \alpha_r),$$

where $\alpha_1, \ldots, \alpha_r$ are the roots of $P_v(T)$ and $S_{p^\nu}(x_1, \ldots, x_r)$ is the fundamental symmetric polynomial of degree p^ν with r variables. Set

$$\mathbb{S}_{r,p^\nu} := \{(s_1, \ldots, s_{p^\nu}); 1 \le s_1 < \cdots < s_{p^\nu} \le r\} \subset \mathbb{Z}^{p^\nu}.$$

Then we have

$$S_{p^\nu}(x_1, \ldots, x_r) = \sum_{(s_1,\ldots,s_{p^\nu}) \in \mathbb{S}_{r,p^\nu}} x_{s_1} x_{s_2} \cdots x_{s_{p^\nu}},$$

which is the sum of $\binom{r}{p^\nu}$ monomials of degree p^ν.

Consider the product $\mathbb{S}_{p^\nu}^{r_0}$ of $\mathbb{S}_{p^\nu}$ and regard it as a subset of $\mathbb{S}_r$. Then we obtain that

$$\begin{aligned}
(a_{v,p^\nu})^{r_0} &= (-1)^r S_{p^\nu}(\alpha_1, \ldots, \alpha_r)^{r_0} \\
&\equiv (-1)^r \left(\sum_{(s_1,\ldots,s_{p^\nu}) \in \mathbb{S}_{r,p^\nu}} \chi_\pi^{i_{s_1} + \cdots + i_{s_{p^\nu}}}(\mathrm{Frob}_v) \right)^{r_0} \\
&\equiv (-1)^r \sum_{\mathbf{s} \in \mathbb{S}_{p^\nu}^{r_0}} \varepsilon_{\mathbf{s}}(\mathrm{Frob}_v) \chi_\pi(\mathrm{Frob}_v) \\
&\equiv (-1)^r \sum_{\mathbf{s} \in \mathbb{S}_{p^\nu}^{r_0}} \chi_\pi(\mathrm{Frob}_v) \\
&\equiv (-1)^r \binom{r}{p^\nu}^{r_0} \pi_0^{f_{v|\pi_0}} \pmod{\pi}. \qquad (5.4.1)
\end{aligned}$$

Since $\binom{r}{p^\nu}$ is not divisible by p, we see that $(-1)^r \binom{r}{p^\nu}^{r_0} \pi_0^{f_{v|\pi_0}} \neq 0$. Here it follows that

$$|(a_{v,p^\nu})^{r_0}| \le q_v = q^{f_{v|\pi_0} \deg(\pi_0)} < |\pi|$$

and

$$\left| (-1)^r \binom{r}{p^\nu}^{r_0} \pi_0^{f_{v|\pi_0}} \right| = |\pi_0^{f_{v|\pi_0}}| = q_v < |\pi|.$$

Hence the above congruence (5.4.1) implies $(a_{v,p^\nu})^{r_0} = (-1)^r \binom{r}{p^\nu}^{r_0} \pi_0^{f_{v|\pi_0}}$. Comparing the π_0-adic valuations of both sides, we obtain $r_0 | f_{v|\pi_0}$, which is a contradiction. □

Recall that $n = [K : F]$ and m_ϕ divides $nC_1(q,r)$ by Lemma 5.4.2. Set

$$C_6 = C_6(K_s, n, q, r) := \max\{C_5(K_s, n, q, m, 1);\ m|nC_1(q,r)\}$$

and

$$C_7 = C_7(K_s, n, q, r) := \max\{C_2(n, q, r), C_6(K_s, n, q, r)\}.$$

Then we have the following theorem.

Theorem 5.4.4. *Suppose that $r = r_0 p^\nu$ and $r_0 > 1$ is not divisible by p. If $\deg(\pi) > C_7$, then the set $\mathscr{D}(K, r, \pi)$ is empty.*

Proof. Assume that $\mathscr{D}(K, r, \pi)$ is not empty and $[\phi] \in \mathscr{D}(K, r, \pi)$. By Proposition 5.3.4, there exist a monic irreducible element $\pi_0 \in A$ and a place v of K above π_0 such that

$$\chi(m_\phi)(\mathrm{Frob}_{\pi_0}) = 1,$$
$$\deg(\pi_0) < \deg(\pi),$$

and

$$f_{v|\pi_0} = 1.$$

However, since π_0 and v satisfy the assumption of Proposition 5.4.3, we see that $\chi(m_\phi)(\mathrm{Frob}_v) = \chi(m_\phi)(\mathrm{Frob}_{\pi_0}) \neq 1$. It is a contradiction. □

By the same argument, we can also prove a uniform non-existence theorem as follows. For a fixed finite separable extension K_0 of F with degree $n_0 := [K_0 : F]$ and a positive integer n, set

$$C_8 = C_8(K_0, q, r, n) := \max\{C_2(nn_0, q, r), \max\{C_5(K_0, n_0, q, m, n);\ m|n_0C_1(q,r)\}\}.$$

Theorem 5.4.5. *Let $r = r_0 p^\nu$, K_0, and $n_0 = [K_0 : F]$ be as above. Let n be a positive integer. If n is not divisible by r_0 and $\deg(\pi) > C_8$, then the set $\mathscr{D}(K, r, \pi)$ is empty for all $K \in \mathscr{F}_n(K_0)$.*

Proof. Let K be a finite extension of K_0 with $[K : K_0] = n$ and assume that $[\phi] \in \mathscr{D}(K, r, \pi)$. Applying Proposition 5.3.4 to K_0, we can find a monic irreducible element $\pi_0 \in A$ and a finite place v_0 of K_0 above π_0 such that

$$\chi(m_\phi)(\mathrm{Frob}_{\pi_0}) = 1,$$

$$\deg(\pi_0) < \frac{1}{n}\deg(\pi),$$

and

$$f_{v_0|\pi_0} = 1.$$

Now we can take a place v of K above v_0 such that $f_{v|v_0}(= f_{v|\pi_0})$ is not divisible by r_0. Indeed, if not, then r_0 must divide $n = \sum_{v|v_0} e_{v|v_0} f_{v|v_0}$. Since $f_{v|\pi_0} \deg(\pi_0) < n \deg(\pi_0) < \deg(\pi)$, by Proposition 5.4.3 we see that $\chi(m_\phi)(\mathrm{Frob}_v) = \chi(m_\phi)(\mathrm{Frob}_{\pi_0})^{f_{v|\pi_0}} \neq 1$. It is a contradiction. □

Remark 5.4.6. In particular by Corollary 4.3.5 and Theorem 5.4.5 for $K_0 = F$, we have the following: if a positive integer n is not divisible by r, then $\mathscr{D}(K, r, \pi) = \varnothing$ for all $K \in \mathscr{F}_n(F)$ and π with $\deg(\pi) > C_8$.

Chapter 6

Comparison with number field case

We denote by K a finite extension of F and by r a positive integer as usual. In this final chapter, we focus on differences between the Rasmussen-Tamagawa conjecture and its Drinfeld module analogue.

In §6.1, under the assumption that r divides $[K:F]_{\mathrm{i}}$, we construct an example of a Drinfeld module $\Phi : A \to K\{\tau\}$ satisfying $[\Phi] \in \mathscr{D}(K,r,\pi)$ for all monic irreducible elements $\pi \in A$. In §6.2, we prove the infiniteness of $\mathscr{D}(K,r,\pi)$ for $r \geq 2$ and $\pi = t$ (Proposition 6.2.5). These constructions are based on the suggestion by Akio Tamagawa.

6.1 Non-emptiness of $\mathscr{D}(K,r,\pi)$

In this section, by constructing a concrete example, we prove the following theorem:

Theorem 6.1.1. *If r divides $[K:F]_{\mathrm{i}}$, then the set $\mathscr{D}(K,r,\pi)$ is never empty for any π.*

If $r = 1$, then Theorem 6.1.1 is trivial since the Carlitz module $\mathcal{C}$ satisfies both (D1) and (D2). Assume that $r \geq 2$ and $[K:F]_{\mathrm{i}}$ is divisible by r. Then r is a p-power and so the r-power map $A \to A; a \mapsto a^r$ is an injective ring homomorphism.

For any $a = \sum x_n t^n \in A$ with $x_n \in \mathbb{F}_q$, set $\hat{a} := \sum x_n^{1/r} t^n$. Then we see that $a \mapsto \hat{a}$ is a ring automorphism of A and the map $A \to A; a \mapsto \hat{a}^r$ is an injective $\mathbb{F}_q$-algebra homomorphism.

Lemma 6.1.2. *Set $[K:F]_{\mathrm{i}} = p^\nu$. Then $K_{\mathrm{s}} = K^{p^\nu}$.*

Proof. Since K is a purely inseparable extension of K_{s} of degree p^ν, the field K^{p^ν} is contained in K_{s}. Consider the sequence of fields $K \supset K^p \supset \cdots \supset$

K^{p^ν}. Proposition 7.4 of [Ros02] implies that each extension $K^{p^n}/K^{p^{n+1}}$ is of degree p. Hence $[K : K^{p^\nu}] = p^\nu = [K : K_{\mathrm{s}}]$, which means that $K_{\mathrm{s}} = K^{p^\nu}$. □

Since r divides $[K : F]_{\mathrm{i}}$, Lemma 6.1.2 implies that K contains the field $F^{1/r}$. In particular the r-th root $t^{1/r}$ of t is contained in K. Then we have a new injective A-field structure $\iota : A \to K$ defined by $\iota(t) = t^{1/r}$. Define the rank-one Drinfeld module

$$\mathcal{C}' : A \to K\{\tau\}$$

over the A-field (K, ι) by $\mathcal{C}'_t = t^{1/r} + \tau$.

Set ${}^{(r)}\mu := \sum c_i^r \tau^i$ for any $\mu = \sum c_i \tau^i \in K\{\tau\}$. Then

$$\begin{array}{ccc} K\{\tau\} & \to & K\{\tau\} \\ \mu & \mapsto & {}^{(r)}\mu \end{array}$$

is a ring endomorphism. We can relate $\mathcal{C}'$ with the Carlitz module $\mathcal{C}$ as follows:

Lemma 6.1.3. *Let $a \in A$.*

(1) ${}^{(r)}\mathcal{C}'_{\hat{a}} = \mathcal{C}_a$.

(2) *For any $\lambda \in \mathcal{C}'[\hat{a}]$, there exists a unique $\delta \in \mathcal{C}[a]$ such that $\lambda = \delta^{1/r}$.*

Proof. Clearly ${}^{(r)}\mathcal{C}'_{\hat{x}} = x = \mathcal{C}_x$ for any $x \in \mathbb{F}_q$ and ${}^{(r)}\mathcal{C}'_{\hat{t}} = {}^{(r)}\mathcal{C}'_t = \mathcal{C}_t$. Hence for any $a = \sum x_n t^n \in A$,

$${}^{(r)}\mathcal{C}'_{\hat{a}} = {}^{(r)}\left(\sum x_n^{1/r} (\mathcal{C}'_t)^n\right) = \sum x_n (\mathcal{C}_t)^n = \mathcal{C}_a.$$

For any $\lambda \in \mathcal{C}'[\hat{a}]$, we see that

$$0 = \left(\mathcal{C}'_{\hat{a}}(\lambda)\right)^r = {}^{(r)}\mathcal{C}'_{\hat{a}}(\lambda^r) = \mathcal{C}_a(\lambda^r).$$

Hence $\lambda^r \in \mathcal{C}[a]$ and we have the injective homomorphism $\mathcal{C}'[\hat{a}] \to \mathcal{C}[a]; \lambda \mapsto \lambda^r$ of finite groups. Since $\#\mathcal{C}'[\hat{a}]$ is equal to $\#\mathcal{C}[a]$ by $\deg(\hat{a}) = \deg(a)$, it is a bijection. □

Define $\Phi_a := \mathcal{C}'_{\hat{a}^r} = (\mathcal{C}'_{\hat{a}})^r \in K\{\tau\}$ for any $a \in A$. Then by construction it gives an $\mathbb{F}_q$-algebra homomorphism

$$\Phi : A \to K\{\tau\},$$

which is determined by $\Phi_t = (t^{1/r} + \tau)^r$. Since $\iota(\hat{a}^r) = a$ holds, Φ is a rank-r Drinfeld module over K. Moreover it has good reduction at every finite place v of K since $v(t^{1/r}) \geq 0$.

By the following proposition, we see that $[\Phi] \in \mathscr{D}(K, r, \pi)$, which implies Theorem 6.1.1.

Proposition 6.1.4. *Let i be the positive integer satisfying $ir \equiv 1 \pmod{q_\pi - 1}$ and $i < q_\pi - 1$. Then the mod π representation attached to Φ is of the form*

$$\bar{\rho}_{\Phi,\pi} \simeq \begin{pmatrix} \chi_\pi^i & * & \cdots & * \\ & \chi_\pi^i & \ddots & \vdots \\ & & \ddots & * \\ & & & \chi_\pi^i \end{pmatrix}.$$

Proof. It suffices to prove that $\bar{\rho}^{\mathrm{ss}}_{\Phi,\pi} = (\chi_\pi^i)^{\oplus r}$. For each $1 \leq s \leq r$, set

$$V_s := \{\lambda \in {}_\Phi K^{\mathrm{sep}}; \mathcal{C}'_{\hat{\pi}^s}(\lambda) = 0\}.$$

For any $a \in A$ and $\lambda \in V_s$, we see that $\Phi_a(\lambda) \in V_s$ since $\mathcal{C}'_{\hat{\pi}^s}(\Phi_a(\lambda)) = \mathcal{C}'_{\hat{\pi}^s}(\mathcal{C}'_{\hat{a}^r}(\lambda)) = \mathcal{C}'_{\hat{a}^r}(\mathcal{C}'_{\hat{\pi}^s}(\lambda)) = 0$. Hence V_s is an A-submodule of ${}_\Phi K^{\mathrm{sep}}$ with the natural G_K-action. Moreover $\Phi_\pi(\lambda) = 0$ for any $\lambda \in V_s$, so that V_s is an $\mathbb{F}_\pi(= A/\pi A)$-vector space. Here $\Phi[\pi] = V_r$ by the definition of Φ. Then we obtain the filtration

$$0 = V_0 \subset V_1 \subset V_2 \subset \cdots \subset V_r = \Phi[\pi]$$

of G_K-stable $\mathbb{F}_\pi$-subspaces of $\Phi[\pi]$. The map $V_s \to V_1; \lambda \mapsto \mathcal{C}'_{\hat{\pi}^{s-1}}(\lambda)$ induces a G_K-equivariant isomorphism $V_s/V_{s-1} \cong V_1$. Since $V_1 = \mathcal{C}'[\hat{\pi}]$ (as a set) and $\deg(\pi) = \deg(\hat{\pi})$, we have $\# V_1 = q_{\hat{\pi}} = q_\pi (= \#\mathbb{F}_\pi)$. Hence $\dim_{\mathbb{F}_\pi} V_1 = 1$ and the semisimplification of $\Phi[\pi]$ (as an $\mathbb{F}_\pi[G_K]$-module) is $\Phi[\pi]^{\mathrm{ss}} = \oplus_{s=1}^r V_s/V_{s-1} \cong V_1^{\oplus r}$. For any $\sigma \in G_K$ and $\lambda \in V_1$, we prove $\sigma(\lambda) = \chi_\pi(\sigma)^i \cdot \lambda$ as follows. Take an element $a_\sigma \in A$ satisfying $a_\sigma \equiv \chi_\pi(\sigma) \pmod{\pi}$. By Lemma 6.1.3 (2), $\lambda = \delta^{1/r}$ for some $\delta \in \mathcal{C}[\pi]$. Then

$$\sigma(\lambda)^r = \sigma(\delta) = \chi_\pi(\sigma) \cdot \delta = \mathcal{C}_{a_\sigma}(\delta).$$

The $\mathbb{F}_\pi$-vector space structure of V_1 is determined by Φ and so $\chi_\pi(\sigma)^i \cdot \lambda = \Phi_{a_\sigma^i}(\lambda) = \mathcal{C}'_{\hat{a}_\sigma^{ir}}(\lambda)$. Since $ir \equiv 1 \pmod{q_{\hat{\pi}} - 1}$ holds, we have $\hat{a}_\sigma^{ir} \equiv \hat{a}_\sigma \pmod{\hat{\pi}}$. This implies $\mathcal{C}'_{\hat{a}_\sigma^{ir}}(\lambda) = \mathcal{C}'_{\hat{a}_\sigma}(\lambda)$. By Lemma 6.1.3 (1), we obtain

$$\left(\chi_\pi(\sigma)^i \cdot \lambda\right)^r = \left(\mathcal{C}'_{\hat{a}_\sigma}(\lambda)\right)^r = {}^{(r)}\mathcal{C}'_{\hat{a}_\sigma}(\lambda^r) = \mathcal{C}_{a_\sigma}(\delta) = \sigma(\lambda)^r.$$

Since the r-power map is injective, we have $\sigma(\lambda) = \chi_\pi(\sigma)^i \cdot \lambda$. Hence the G_K-action on V_1 is given by χ_π^i. □

Remark 6.1.5. Proposition 6.1.4 means that the mod π representation $\bar{\rho}_{\Phi,\pi}$ is reducible for all π. Hence $\mathrm{End}_K(\Phi) \neq A$ must hold by Theorem 2.3.7.

In fact $\mathcal{C}'_t = t^{1/r} + \tau \in K\{\tau\}$ is an endomorphism of Φ and the correspondence $t^{1/r} \mapsto \mathcal{C}'_t$ induces an isomorphism $A[t^{1/r}] \cong \mathrm{End}_K(\Phi)$, so that Φ has complex multiplication.

Remark 6.1.6. Let u be a finite place of K above π. Now r divides $e_{u|\pi}$ by assumption. Set $e = e_{u|\pi}/r$. Since $ir \equiv 1 \pmod{q_\pi - 1}$, we see that

$$\chi_\pi^i|_{I_{K_u}} = (\omega_{1,K_u})^{i\cdot e_{u|\pi}} = (\omega_{1,K_u})^{i\cdot r\cdot e} = (\omega_{1,K_u})^e.$$

Hence the set of tame inertia weights of $\bar{\rho}_{\Phi,\pi}|_{I_{K_u}}$ is $\mathrm{TI}_{K_u}(\bar{\rho}_{\Phi,\pi}) = \{e\}$.

6.2 Infiniteness of $\mathscr{D}(K, r, t)$

Finally, for $\pi = t$ and $r \geq 2$, we construct an infinite subset of $\mathscr{D}(K, r, t)$. In the number field case, the set $\mathscr{A}(k, g, \ell)$ is always finite because of the Shafarevich conjecture proved by Faltings [Fal83]. However, the Drinfeld module analogue of it does not hold as follows:

Example 6.2.1. For any $a \in A$, consider the rank-two Drinfeld module $\phi^{(a)} : A \to F\{\tau\}$ given by $\phi_t^{(a)} = t + a\tau + \tau^2$. It is easily seen that $\phi^{(a)}$ has good reduction at any finite place of F.

If $\phi^{(a)}$ is F-isomorphic to $\phi^{(a')}$ for some $a' \in A$, then there exists an element $c \in F$ such that $c\phi_t^{(a')} = \phi_t^{(a)}c$. Hence

$$\phi_t^{(a')} = t + a'\tau + \tau^2 = t + c^{q-1}a\tau + c^{q^2-1}\tau^2.$$

This means that $c \in \mathbb{F}_q^\times$ and hence $a' = c^{q-1}a = a$. Therefore the set of F-isomorphism classes $\{[\phi^{(a)}]; a \in A\}$ is infinite.

Let W be a G_K-stable one-dimensional $\mathbb{F}_q$-vector space contained in K^{sep} and write $\kappa_W : G_K \to \mathbb{F}_q^\times$ for the character attached to W. Set $P_W(T) := \prod_{\lambda \in W}(T - \lambda)$, which is an $\mathbb{F}_q$-linear polynomial of the form

$$P_W(T) = T^q + c_W T, \quad c_W := \prod\nolimits_{\lambda \in W\setminus\{0\}} \left(-\lambda\right) \in K^\times$$

by [Gos96, Corollary 1.2.2]. For any $c \in K^\times$, denote by $\bar{c} \in K^\times/(K^\times)^{q-1}$ the class of c and by $\kappa_{(c)} : G_K \to \mathbb{F}_q^\times$ the character corresponding to $\bar{c}$ by the map $K^\times/(K^\times)^{q-1} \xrightarrow{\sim} \mathrm{Hom}(G_K, \mathbb{F}_q^\times)$ of Kummer theory.

Lemma 6.2.2. *For the above element $c_W \in K^\times$, the character $\kappa_{(-c_W)}$ coincides with κ_W.*

Proof. Since $\lambda^{q-1} = -c_W$ for any $\lambda \in W \setminus \{0\}$, the character $\kappa_{(-c_W)}$ is given by $\kappa_{(-c_W)}(\sigma) = \sigma(\lambda)/\lambda = \kappa_W(\sigma)$ for any $\sigma \in G_K$. □

Identify $\mathbb{F}_t = A/tA = \mathbb{F}_q$. Then $\mathcal{C}[t]$ is a one-dimensional $\mathbb{F}_q$-subspace of K^{sep} and $P_{\mathcal{C}[t]}(T) = T^q + tT$ by the definition of $\mathcal{C}$. By Lemma 6.2.2, we see that $\chi_t = \kappa_{(-t)}$. Note that $\chi_t^i = \kappa_{((-t)^i)}$ for any integer i.

Take r elements $c_1, \ldots, c_r \in K^\times$. For any $1 \le s \le r$, define $f_s(\tau) := (\tau + c_s)(\tau + c_{s-1}) \cdots (\tau + c_1) \in K\{\tau\}$. Set $W_s := \ker f_s : K^{\mathrm{sep}} \to K^{\mathrm{sep}}$, which is a G_K-stable s-dimensional $\mathbb{F}_q$-subspace of K^{sep}. Thus we obtain the filtration

$$0 = W_0 \subset W_1 \subset \cdots \subset W_r$$

of $\mathbb{F}_q[G_K]$-modules.

Lemma 6.2.3. *The $\mathbb{F}_q$-linear representation $\bar{\rho} : G_K \to \mathrm{Aut}_{\mathbb{F}_q}(W_r) \cong \mathrm{GL}_r(\mathbb{F}_q)$ is of the form*

$$\bar{\rho} \simeq \begin{pmatrix} \kappa_{(-c_1)} & * & \cdots & * \\ & \kappa_{(-c_2)} & \ddots & \vdots \\ & & \ddots & * \\ & & & \kappa_{(-c_r)} \end{pmatrix}.$$

Proof. For any $1 \le s \le r$, the quotient W_s/W_{s-1} is isomorphic to $\mathrm{Ker}(\tau + c_s : K^{\mathrm{sep}} \to K^{\mathrm{sep}})$ as an $\mathbb{F}_q[G_K]$-module. Hence each W_s/W_{s-1} is embedded into K^{sep}. By Lemma 6.2.2, the action of G_K on W_s/W_{s-1} is given by $\kappa_{(-c_s)}$. □

Fix r integers $i_1, \ldots, i_r$ satisfying $\sum_{s=1}^r i_s = 1$. For any $\mathbf{m} = (m_1, \ldots, m_r) \in \mathbb{Z}^r$ satisfying $\sum_{s=1}^r m_s = 0$, consider the $\mathbb{F}_q$-algebra homomorphism $\phi^{\mathbf{m}} : A \to K\{\tau\}$ given by

$$\phi_t^{\mathbf{m}} = (-1)^{r-1} \prod_{s=1}^r (\tau - (-t)^{k_s}),$$

where $k_s = i_s + m_s(q-1)$ for any $1 \le s \le r$. Now $\sum_{s=1}^r k_s = 1$, so that the constant term of $\phi_t^{\mathbf{m}}$ is $(-1)^{r-1} \prod_{s=1}^r (-(-t)^{k_s}) = (-1)^{2r} t = t$. Hence $\phi^{\mathbf{m}}$ is a rank-r Drinfeld module over K.

Proposition 6.2.4. *The K-isomorphism class $[\phi^{\mathbf{m}}]$ is contained in $\mathscr{D}(K,r,t)$. Moreover, the mod t representation attached to $\phi^{\mathbf{m}}$ is of the form*

$$\bar{\rho}_{\phi^{\mathbf{m}},t} \simeq \begin{pmatrix} \chi_t^{i_1} & * & \cdots & * \\ & \chi_t^{i_2} & \ddots & \vdots \\ & & \ddots & * \\ & & & \chi_t^{i_r} \end{pmatrix},$$

where $i_1, \ldots, i_r$ are the integers fixed as above.

Proof. For any finite place v of K not lying above t, since $-t \in \mathcal{O}_{K_v}$ and the leading coefficient of $\phi^{\mathbf{m}}_t$ is $(-1)^{r-1}$, we see that $\phi^{\mathbf{m}}$ has good reduction at v. Now $\phi^{\mathbf{m}}[t]$ coincides with the kernel of $\prod_{s=1}^{r}(\tau - (-t)^{k_s})$. Applying Lemma 6.2.3 to $f_s = (\tau - (-t)^{k_s}) \cdots (\tau - (-t)^{k_1})$, we see that $\bar{\rho}_{\phi^{\mathbf{m}},t}$ is given as above since $\kappa_{((-t)^{k_s})} = \chi_t^{k_s} = \chi_t^{i_s}$ for any $1 \leq s \leq r$. □

Proposition 6.2.5. *If $r \geq 2$, then the set $\mathscr{D}(K,r,t)$ is infinite.*

Proof. We construct an infinite subset of $\mathscr{D}(K,r,t)$ as follows. Fix r integers $i_1, \ldots, i_r$ satisfying $\sum_{s=1}^{r} i_s = 1$. For any positive integer m, consider $(-m, 0, \ldots, 0, m) \in \mathbb{Z}^r$ and define $\phi^m := \phi^{(-m,0,\ldots,0,m)}$, which is a Drinfeld module satisfying $[\phi^m] \in \mathscr{D}(K,r,t)$ by Proposition 6.2.4. Write $\phi^m_t = t + c_1\tau + \cdots + c_{r-1}\tau^{r-1} + (-1)^{r-1}\tau^r \in K\{\tau\}$. Then by construction the coefficient c_{r-1} is given by

$$c_{r-1} = (-t)^{i_1 - m(q-1)} + (-t)^{i_r + m(q-1)} + \sum_{s=2}^{r-1}(-t)^{i_s}.$$

For any finite place u of K above t, if m is sufficiently large, then

$$u(c_{r-1}) = (i_1 - m(q-1))u(-t) < 0.$$

Hence we see that $u(c_{r-1}) \to -\infty$ as $m \to \infty$. On the other hand, for two positive integers m and m', if $\phi^{m'}$ is isomorphic to ϕ^m, then $\phi^{m'}_t = x^{-1}\phi^m_t x$ for some $x \in \mathbb{F}_K^\times$ by the same argument of Example 6.2.1. These facts imply that if m' is sufficiently large, then ϕ^m and $\phi^{m'}$ are not isomorphic. Therefore the subset $\{[\phi^m]; m \in \mathbb{Z}_{>0}\}$ of $\mathscr{D}(K,r,t)$ is infinite. □

Bibliography

[And86] Greg W. Anderson, *t-motives*, Duke Math. J. **53**, 457–502 (1986)

[AI98] Greg W. Anderson and Yasutaka Ihara, *Pro-ℓ branched covering of $\mathbb{P}^1$ and higher circular ℓ units*, Ann. of Math. (2) **128**, no. 2, (1998), 271–293

[Ara14] Keisuke Arai, *Algebraic points on Shimura curves of $\Gamma_0(p)$-type*, J. reine angew. Math. **690** (2014), 179–202

[Bel80] G. V. Belyi, *On galois extensions of a maximal cyclotomic field*, Math. USSR-Izw. **14**, no. 2, (1980), 247–256

[Bou15] Abbey M. Bourdon, *A uniform version of a finiteness conjecture for CM elliptic curves*, Math. Res. Lett. **22**, (2015), 403–416

[Bro12] Francis Brown, *Mixed Tate motives over $\mathbb{Z}$*, Ann. of Math. (2) **175**, no.2, (2012), 949–976

[CL13] Imin Chen and Yoonjin Lee, *Explicit isogeny theorem for Drinfeld modules*, Pacific J. Math. **263**, no.1 (2013), 87–116

[Dri74] Vladimir G. Drinfeld, *Elliptic modules*, Math. USSR Sub. **23** (1974), 561–592

[Fal83] Gerd Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpen* (German), Invent. Math. **73**, no. 3 (1983), 349–366. (Engl. transl. in: "Arithmetic Geometry", G. Cornell, J. H. Silverman(eds.), Springer-Verlag (1986), 9–27)

[Gar01] F. Gardeyn, *t-motives and Galois representations*, Ph.D.thesis, Universiteit Gent (2001)

[Gar02] Francis Gardeyn, *A Galois criterion for good reduction of τ-sheaves*, J. Number Theory **97** (2002), 447–471

[Gar03a] Francis Gardeyn, *The structure of analytic τ-sheaves*, J. Number Theory **100** (2003), 332–362

[Gar03b] Francis Gardeyn, *Analytic morphisms of t-motives*, Math. Ann. **325** (2003), 795–828

[Gos96] David Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete Volume 35, Springer-Verlag, Berlin (1996)

[Gou01] Fernando Q. Gouvêa, *Deformations of Galois Representations*, in: "Arithmetic algebraic geometry" (Park City, UT, 1991), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI (2001), 233–406. Appendix 1 by Mark Dickinson, Appendix 2 by Tom Weston and Appendix 3 by Matthew Emerton

[Hay74] David R. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. **189** (1974), 77–91

[Iha86] Yasutaka Ihara, *Profinite braid groups, Galois representations and complex multiplications*, Ann. of Math. **123** (1986), 43–106

[Kim09] Wansu Kim, *Galois deformation theory for norm fields and its arithmetic applications*, Thesis, The University of Michigan (2009)

[KS94] Vijaya Kumer Murty and John Scherk, *Effective versions of the Chebotarev density theorem for function fields*, C. R. Acad. Paris Sér. I Math. **319**, no.6 (1994), 523–528

[Liu02] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press (2002)

[Leh09] Thomas Lehmkuhl, *Compactification of the Drinfeld modular surfaces*, Mem. Amer. Math. Soc. **197** no. 921, (2009)

[Lom] Davide Lombardo, *On the uniform Rasmussen-Tamagawa conjecture in the CM case*, arXiv:1511.09019 `https://arxiv.org/abs/1511.09019`

[Mum70] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No.5, Oxford University Press (1970)

[Oku] Yoshiaki Okumura, *A function field analogue of the Rasmussen-Tamagawa conjecture: The Drinfeld module case*, to appear in Kyushu J. Math.

[Oze11] Yoshiyasu Ozeki, *Non-existence of certain Galois representations with a uniform tame inertia weight*, Int. Math. Res. Not. (2011), 2377–2395

[Oze13] Yoshiyasu Ozeki, *Non-existence of certain CM abelian varieties with prime power torsion*, Tohoku Math. J. **65** (2013), 357–371

[PR09a] Richard Pink and Egon Rütsche, *Image of the group ring of the Galois representation associated to Drinfeld modules*, J. Number Theory **129** (2009), 866–881

[PR09b] Richard Pink and Egon Rütsche, *Adelic openness for Drinfeld modules in generic characteristic*, J. Number Theory **129** (2009), 882–907

[PaR07] Matthew Papanikolas and Christopher Rasmussen, *On the torsion of the Jacobians of principal modular curves of level* 3^n, Arch. Math. (Basel) **88** (2007), no. 1, 19–28

[Ras08] Christopher Rasmussen, *On the field of the* 2*-power torsions of certain elliptic curves*, Math. Res. Lett. **15** (2008), 1223–1231

[Ros02] Michael Rosen, *Number Theory in Function Fields*, Graduate Texts in Mathematics **210**, Springer-Verlag, New York (2002)

[RT08] Christopher Rasmussen and Akio Tamagawa, *A finiteness conjecture on abelian varieties with constrained prime power torsion*, Math. Res. Lett. **11** (2008),no. 4, 529–538

[RT17] Christopher Rasmussen and Akio Tamagawa, *Arithmetic of abelian varieties with constrained torsion*, Trans. Amer. Math. Soc. **369** (2017), 2395–2424

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'order fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331

[Ser79] Jean-Pierre Serre, *Local Fields*, Graduate Texts in Mathematics **67**, Springer, New York (1979)

[ST68] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. **88** (1968), 492–517

[Sha02] Romyar T. Sharifi, *Relationships between conjectures on the structure of pro-p Galois groups unramified outside p*, in:"Arithmetic fundamental groups and noncommutative algebra", Proc. Sympos. Pure Math. vol. 70, Amer. Math. Soc., (2002), 275–284

[Tak82] Toyofumi Takahashi, *Good reduction of elliptic modules*, J. Math. Soc. Japan **34**, no.3 (1982), 475–487

[Zar85] Yuri G. Zarhin, *A finiteness theorem for unpolarized Abelian varieties over number fields with prescribed places of bad reduction*, Invent. math. **79**, (1985), 309–321

[Zas69] Hans Zassenhaus, *Characterization of unipotent matrices*, J. Number Theory **1**, (1969), 222–230