RIMS-1947 revision

On Isogeny Characters of Drinfeld Modules of Rank Two

By

Shun ISHII

December 2021

京都大学　数理解析研究所

RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES

KYOTO UNIVERSITY, Kyoto, Japan

ON ISOGENY CHARACTERS OF DRINFELD MODULES OF RANK TWO

SHUN ISHII

Abstract. In this paper, we study cyclic torsion subgroups of Drinfeld $\mathbb{F}_q[T]$-modules of rank two over $\mathbb{F}_q(T)$ via isogeny characters associated to them. Among other things, we prove that such Drinfeld $\mathbb{F}_q[T]$-modules do not have a cyclic $\mathfrak{p}$-torsion subgroup defined over $\mathbb{F}_q(T)$ under various conditions, where $\mathfrak{p}$ is a maximal ideal of $\mathbb{F}_q[T]$. We also obtain some unconditional results.

1. Introduction

Let p be a prime, q a power of p, $A \coloneqq \mathbb{F}_q[T]$ a polynomial ring over $\mathbb{F}_q$, $K \coloneqq \mathbb{F}_q(T)$ and $\mathfrak{p}$ a maximal ideal of A. Let ϕ be a Drinfeld A-module of rank two over K. The purpose of this paper is to study the character associated to each cyclic subgroup of $\phi[\mathfrak{p}]$ (the $\mathfrak{p}$-torsion submodule of ϕ) which is defined over K. In particular, we show that such a cyclic subgroup does not exist under various assumptions. Such "various assumptions" are divided into the following three types of conditions:

($\dagger_q$) : conditions on q (e.g. q is even/odd).

($\dagger_{\mathfrak{p}}$) : conditions on $\mathfrak{p}$ (e.g. $\deg(\mathfrak{p})$ is even/odd, $\deg(\mathfrak{p})$ is greater than q, etc).

($\dagger_\phi$) : conditions on ϕ. Let S_ϕ be the set of all finite places of K at which ϕ has potentially good reduction. In this part, we assume that S_ϕ is sufficiently large (e.g. S_ϕ contains a prime of degree one, $S_\phi = \sum_K^{\mathrm{fin}} \coloneqq$ the set of all finite places of K, etc).

For example, we prove the following results:

Theorem 1.1 (=Theorem 4.2)**.** *Let ϕ be a Drinfeld A-module of rank two over K. Assume that the following conditions are satisfied:*

($\dagger_{\mathfrak{p}}$) $\deg(\mathfrak{p})$ *is even and greater than two.*

($\dagger_\phi$) $\mathfrak{p} \in S_\phi$ *and S_ϕ contains a prime of degree one.*

Then ϕ does not have a nontrivial cyclic $\mathfrak{p}$-torsion subgroup defined over K.

Theorem 1.2 (=Theorem 4.5)**.** *Let ϕ be a Drinfeld A-module of rank two over K. Assume that the following conditions are satisfied:*

($\dagger_q$) *q is even.*

($\dagger_{\mathfrak{p}}$) $\deg(\mathfrak{p})$ *is greater than q.*

($\dagger_\phi$) $\mathfrak{p} \in S_\phi$ *and S_ϕ contains a prime of degree one.*

Then ϕ does not have a nontrivial cyclic $\mathfrak{p}$-torsion subgroup defined over K.

Let us exlpain some previous results and their relations to our results. First, Pál proved that, if $q = 2$, no Drinfeld A-module of rank two over K admits a $\mathfrak{p}$-isogeny defined over K for any maximal ideal $\mathfrak{p}$ of A of degree greater than two [11, Theorem 1.2]. To prove this result, he proved a weaker assertion [11, Theorem 8.10], which states that no Drinfeld $\mathbb{F}_2[T]$-module of rank two over $\mathbb{F}_2(T)$ which has good reduction at every finite place admits a $\mathfrak{p}$-isogeny defined over K for any

Date: December 15, 2021.

maximal ideal $\mathfrak{p}$ of A of degree greater than two. In this paper, we prove the latter assertion for arbitrary q:

Theorem 1.3 (=Corollary 4.7)**.** *Let ϕ be a Drinfeld A-module of rank two over K. Assume that the following conditions are satisfied:*
($\dagger_{\mathfrak{p}}$) $\deg(\mathfrak{p})$ *is greater than q.*
($\dagger_{\phi}$) $S_{\phi} = \sum_{K}^{\mathrm{fin}}$.
Then ϕ does not have a nontrivial cyclic $\mathfrak{p}$-torsion subgroup defined over K.

Second, Armana proved that no Drinfeld A-module of rank two over K admits a nontrivial K-rational $\mathfrak{p}$-torsion point for any maximal ideal $\mathfrak{p}$ of A of degree three or four [1, Théorème 1.4]. We prove a stronger assertion when $\deg(\mathfrak{p})$ is equal to four:

Theorem 1.4 (= Corollary 5.3)**.** *Let $\mathfrak{p}$ be a maximal ideal of A of degree four. Then no Drinfeld A-module of rank two over K has a $\mathfrak{p}$-isogeny defined over K. Moreover, the set of K-rational points of the Drinfeld modular curve $Y_0(\mathfrak{p})$ is empty.*

We briefly explain the proof of these results. First, we prove a Drinfeld module analogue of Mazur's results in [9, §5 The Isogeny Character]. More precisely, let C be a cyclic $\mathfrak{p}$-torsion subgroup of ϕ defined over K and $r : \mathrm{Gal}(\overline{K}/K) \to \mathbb{F}_{\mathfrak{p}}^{*}(:= (A/\mathfrak{p})^{*})$ the character associated to C which we call the isogeny character associated to (ϕ, C). Assuming $\mathfrak{p} \in S_{\phi}$, we study ramification of r at $\mathfrak{p}$. Moreover, assuming $\mathfrak{l} \in S_{\phi}$, we obtain a nontrivial congruence which relates $\mathfrak{p}$ to $\mathfrak{l}$ by using traces of Frobenius endomorphisms of Drinfeld modules defined over finite fields. With some more assumptions, such a congruence (or, such congruences for various $\mathfrak{l}$) lead(s) us to conclude that C does not exist. Moreover, when $\deg(\mathfrak{p})$ is equal to three or four, we show that the existence of a cyclic $\mathfrak{p}$-torsion subgroup over K implies that ϕ has potentially good reduction at every finite place of K.

This paper is organized as follows. In section 2, we collect some lemmas on Drinfeld modules. In section 3, we study cyclic $\mathfrak{p}$-torsion subgroups of Drinfeld modules which are defined over finite extensions of $K_{\mathfrak{p}}^{\mathrm{ur}}$ (the maximal unramified extension of the $\mathfrak{p}$-adic completion of K), by using a result of Raynaud [12]. In section 4, we apply the result of section 3 and obtain certain local properties of isogeny characters. In the last section, we discuss some unconditional results. More precisely, we try to remove ($\dagger_{\phi}$) appearing in main results and prove that the set of K-rational points of the Drinfeld modular curve $Y_0(\mathfrak{p})$ is empty when $\deg(\mathfrak{p})$ is equal to four. We also give a conjecture which relates the divisibility of certain trinomials by $\mathfrak{p}$ to the non-existence of K-rational points of $Y_0(\mathfrak{p})$ when $\deg(\mathfrak{p})$ is equal to three.

Acknowledgement. The author deeply thanks Professor Akio Tamagawa for his many helpful comments and warm encouragements.

Notation and Definition

- p: a prime.
- $q := p^r$ for some $r \geq 1$.
- $K := \mathbb{F}_q(T)$.
- $A := \mathbb{F}_q[T]$.
- $\mathfrak{p}$: a maximal ideal of A of degree $d =: \deg(\mathfrak{p})$ with monic generator f.
- ∞: a place of K which corresponds to $\frac{1}{T}$ (the infinite place).
- $\mathbb{C}_{\infty}$: the completion of an algebraic closure of the ∞-adic completion K_{∞} of K.
- Let $\mathfrak{l}$ be a maximal ideal of A. We denote the $\mathfrak{l}$-adic completion of A by $A_{\mathfrak{l}}$. Its field of fraction and residue field are denoted by $K_{\mathfrak{l}}$ and $\mathbb{F}_{\mathfrak{l}}$, respectively.

- Let R be an A-algebra. R is called an A-field if R is a field.
- For a field R, we denote a separable closure of R by $\overline{R}$.
- Let R be a commutative $\mathbb{F}_q$-algebra. We define $R\{\tau\}$ as the skew polynomial ring over R defined by $\tau a = a^q\tau$ for every $a \in R$. This ring is naturally regarded as a subring of $\mathrm{End}(\mathbb{G}_{a,R})$, the endomorphism ring of the additive group scheme over R, via identifying τ with the q-th power Frobenius endomorphism. A natural homomorphism $R\{\tau\} \to R$ is defined by $\tau \mapsto 0$.
- Let R be an A-field with structure homomorphism $\iota : A \to R$. A Drinfeld A-module over R is defined to be a homomorphism $\phi : A \to R\{\tau\}$ such that the composite of $A \xrightarrow{\phi} R\{\tau\} \to R$ is equal to ι and the degree of ϕ_T as a polynomial in τ is positive. If ϕ is a Drinfeld A-module over R, the rank of ϕ is defined to be the degree of $\phi_T(:= \phi(T))$ as a polynomial in τ. By definition, for every Drinfeld A-module ϕ of rank two over R, ϕ_T can be written as $\phi_T = \iota(T) + a_1\tau + a_2\tau^2$ for some $a_1 \in R$ and $a_2 \in R^*$. Note that, if $R \subset S$ is a field extension, then ϕ is also naturally regarded as a Drinfeld A-module over S which is denoted by the same character ϕ.
- A homomorphism between two Drinfeld A-modules $\phi_1 \to \phi_2$ over R is defined to be an element $h \in R\{\tau\}$ such that $h\phi_{1,T} = \phi_{2,T}h$. An isomorphism between two Drinfeld A-modules is defined in the obvious manner.
- Let ϕ be a Drinfeld A-module over R and $\mathfrak{a}$ a nonzero ideal of A. The $\mathfrak{a}$-torsion subscheme of ϕ is defined to be the scheme theoretic intersection of $\{\ker(\phi_a : \mathbb{G}_{a,R} \to \mathbb{G}_{a,R})\}_{a\in\mathfrak{a}}$ and denoted by $\phi[\mathfrak{a}]$. This is a finite flat $(A/\mathfrak{a})$-module scheme over R. If $\ker(\iota)$ does not divide $\mathfrak{a}$, then $\phi[\mathfrak{a}]$ is étale and étale-locally isomorphic to the constant $(A/\mathfrak{a})$-module scheme with value in $(A/\mathfrak{a})^{\deg(\phi_T)}$. In this paper, we refer to a nonzero cyclic $(A/\mathfrak{a})$-module contained in $\phi[\mathfrak{a}](\overline{R})$ as a cyclic subgroup of $\phi[\mathfrak{a}]$. We say that a cyclic subgroup of $\phi[\mathfrak{a}](\overline{R})$ is defined over R if it is closed under the action of the absolute Galois group of R.
- Let $Y(\mathfrak{p})_A$ be the Drinfeld modular curve over $\mathrm{Spec}(A)$ of level $\Gamma(\mathfrak{p}) \subset \mathrm{GL}_2(A)$ and $X(\mathfrak{p})_A$ its compactification which are constructed by Gekeler in [4, 5.1] (where $Y(\mathfrak{p})_A$ and $X(\mathfrak{p})_A$ are denoted by $M(\mathfrak{p})$ and $\overline{M(\mathfrak{p})}$, respectively). Similarly, let $Y_0(\mathfrak{p})_A$ be the Drinfeld modular curve over $\mathrm{Spec}(A)$ of level $\Gamma_0(\mathfrak{p})$ and $X_0(\mathfrak{p})_A$ its compactification which are constructed in [4, 5.2] (where $Y_0(\mathfrak{p})_A$ and $X_0(\mathfrak{p})_A$ are denoted by $M_0(\mathfrak{p})$ and $\overline{M_0(\mathfrak{p})}$, respectively).
- We define the Drinfeld modular curve over $\mathrm{Spec}(A)$ of level $\Gamma_1(\mathfrak{p})$ which we denote by $Y_1(\mathfrak{p})_A$ as the quotient of $Y(\mathfrak{p})_A$ by the natural action of $\Gamma_1(\mathfrak{p})$. Similarly, we define $X_1(\mathfrak{p})_A$ to be the quotient of $X(\mathfrak{p})_A$ by the natural action of $\Gamma_1(\mathfrak{p})$.
- For an A-scheme X_A and an A-algebra R, $X_A \times_{\mathrm{Spec}(A)} \mathrm{Spec}(R)$ is denoted by X_R unless otherwise specified.

2. Preliminaries on Drinfeld modules of rank two

In this section, we prepare some lemmas used later. Let R be an A-field with structure homomorphism $\iota : A \to R$.

Automorphism.

Lemma 2.1. *Let ϕ be a Drinfeld A-module of rank two over R. Then $\mathrm{Aut}(\phi)$ is equal to $\mathbb{F}_q^*$ or $\mathbb{F}_{q^2}^*$.*

Proof. It is easy to see that $\mathrm{Aut}(\phi) = \{u \in R^* \mid u^{-1}\phi_T u = \phi_T\}$. The assertion follows by comparing the coefficients of τ and τ^2 in ϕ_T. □

Lemma 2.2. *Assume that R is separably closed and let ϕ be a Drinfeld A-module of rank two over R. Let C be a cyclic subgroup of $\phi[\mathfrak{p}](R)$ and $\mathrm{Aut}(\phi, C)$ the group of automorphisms of ϕ which preserves C. Then the natural map $\mathrm{Aut}(\phi, C) \to \mathrm{Aut}_{\mathbb{F}_\mathfrak{p}}(C) \cong \mathbb{F}_\mathfrak{p}^*$ is injective.*

Proof. Each element $h \in \mathrm{Aut}(\phi)$ induces an automorphism of $\phi[\mathfrak{p}]$ and is induced by an element u of R^* so the induced automorphism on $\phi[\mathfrak{p}]$ is simply the multiplication by u. Hence h is uniquely determined by its value at a nonzero element of $\phi[\mathfrak{p}](R)$. The assertion follows. □

Reduction.

Assume that R is equipped with a normalized discrete valuation v and $\iota(A)$ is contained in the discrete valuation ring $\mathcal{O}$ of v.

Let ϕ be a Drinfeld A-module of rank two over R defined by $\phi_T = \iota(T) + a_1\tau + a_2\tau^2$ for $a_1 \in R$ and $a_2 \in R^*$. We say ϕ has good reduction at v if there exists $u \in R^*$ such that all coefficients of $u^{-1}\phi_T u$ are contained in $\mathcal{O}$ and its leading coefficient is contained in $\mathcal{O}^*$. By definition, this is equivalent to saying that there exists $u \in R^*$ such that $v(u^{q-1}a_1) = (q-1)v(u) + v(a_1) \geq 0$ and $v(u^{q^2-1}a_2) = (q^2-1)v(u) + v(a_2) = 0$. We say ϕ has potentially good reduction at v if there exists a finite extension of discrete valuation fields (S, w) of (R, v) such that ϕ has good reduction at w. This is equivalent to saying that $\frac{v(a_1)}{q-1} \geq \frac{v(a_2)}{q^2-1}$.

Lemma 2.3. *Let ϕ be a Drinfeld A-module of rank two over R which has potentially good reduction at v. Then ϕ has good reduction at the unique extension of v to $R(\pi^{\frac{1}{q^2-1}})$ where π is a uniformizer of v.*

Proof. Let w be the discrete valuation on $R(\pi^{\frac{1}{q^2-1}})$ which extends v and $u \in R(\pi^{\frac{1}{q^2-1}})$ an element with $w(u) = -\frac{v(a_2)}{q^2-1}$. Then $u^{-1}\phi_T u$ satisfies the desired property. □

Let k be the residue field of $\mathcal{O}$ and assume that $\ker(A \xrightarrow{\iota} \mathcal{O} \to k)$ is equal to $\mathfrak{p}$. Let ϕ be a Drinfeld A-module of rank two which has good reduction at v. By replacing ϕ with $u^{-1}\phi u$ for suitable $u \in R^*$, we may assume that $\phi_T \in \mathcal{O}\{\tau\}$ and its leading coefficient is contained in $\mathcal{O}^*$. By reducing ϕ modulo the maximal ideal of $\mathcal{O}$, we obtain a Drinfeld A-module of rank two over k which we denote by $\overline{\phi}$.

Lemma 2.4. *The degree of the lowest nonzero term of $\overline{\phi}_f$ is equal to either d or $2d$.*

Proof. See Pál [11, Lemma 8.2]. □

If the first nonzero coefficient of $\overline{\phi}_f$ appears in τ^d, we say that ϕ has good ordinary reduction at v. Otherwise, we say that ϕ has good supersingular reduction at v.

Frobenius Trace.

Let $\mathfrak{l} \neq \mathfrak{p}$ be a maximal ideal of A with monic generator g and ϕ a Drinfeld A-module of rank two over $\mathbb{F}_\mathfrak{l}$ defined by $\phi_T = T + a_1\tau + a_2\tau^2$. Then $\tau^{\deg(g)}$ defines an endomorphism of ϕ called the Frobenius endomorphism of ϕ.

Lemma 2.5 (Gekeler [6, 1.8. Theorem], [5, 3.4. Corollary])**.** *There exists a quadratic polynomial $P_\phi \in A[X]$ which satisfies the following properties:*

1. *P_ϕ is equal to the characteristic polynomial of $\tau^{\deg(g)}$ with regard to its action on the $\mathfrak{p}$-adic Tate module of ϕ.*
2. *Write $P_\phi = X^2 - aX + b$ for some $a, b \in A$. Then $(b) = \mathfrak{l}$.*
3. *P_ϕ is irreducible over K_∞. In particular, $2\deg(a) \leq \deg(b) = \deg(g)$.*

We refer to this a as the Frobenius trace of ϕ.

Corollary 2.6. *Let l be a positive integer and $P_{\phi,l} = X^2 - a_l X + b_l$ the characteristic polynomial of $\tau^{l\deg(\mathfrak{l})} \in \mathrm{End}(\phi)$. Then $2\deg(a_l) \leq \deg(b_l) = l\deg(\mathfrak{l})$.*

Proof. See Gekeler [6, 1.8. Theorem (iii)]. □

3. Isogeny characters

3.1. **Ramification Arising from Cyclic Subgroups of Drinfeld Modules.** In this subsection, let L be a finite extension of the maximal unramified extension $K_{\mathfrak{p}}^{\mathrm{ur}}$ of the $\mathfrak{p}$-adic completion $K_{\mathfrak{p}}$ of K, e the degree of L over $K_{\mathfrak{p}}^{\mathrm{ur}}$, v the normalized discrete valuation on L, $\mathcal{O}$ the discrete valuation ring of L which corresponds to v and $\mathfrak{m}$ the maximal ideal of $\mathcal{O}$.

Let ϕ be a Drinfeld A-module of rank two over L which has good reduction and C a cyclic $\mathfrak{p}$-torsion subgroup of ϕ defined over L. We may assume that ϕ_T is contained in $\mathcal{O}\{\tau\}$ and its leading coefficient is contained in $\mathcal{O}^*$. Let $\phi[\mathfrak{p}]_{\mathcal{O}}$ be the $\mathfrak{p}$-torsion submodule scheme of ϕ which is a finite flat $\mathbb{F}_{\mathfrak{p}}$-module scheme over $\mathrm{Spec}(\mathcal{O})$ and $C_{\mathcal{O}}$ the scheme-theoretic closure of C in $\phi[\mathfrak{p}]_{\mathcal{O}}$. Then $C_{\mathcal{O}}$ is naturally equipped with a structure of finite flat $\mathbb{F}_{\mathfrak{p}}$-module scheme over $\mathrm{Spec}(\mathcal{O})$.

By a result of Raynaud [12, COROLLAIRE 1.5.1], we have the following isomorphism of $\mathbb{F}_{\mathfrak{p}}$-module schemes for some $(\delta_i)_{i\in\mathbb{Z}/rd\mathbb{Z}}$ contained in $\mathcal{O}$:

$$C_{\mathcal{O}} \cong \mathrm{Spec}(\mathcal{O}[\{X_i\}_{i\in\mathbb{Z}/rd\mathbb{Z}}]/(X_i^p - \delta_i X_{i+1})_{i\in\mathbb{Z}/rd\mathbb{Z}}). \tag{1}$$

Note that the group scheme structure of the right hand side is induced by the natural embedding into $\mathbb{G}_a^{rd}$. The $\mathbb{F}_{\mathfrak{p}}$-module scheme structure of the right hand side is, by rearranging $\{X_i\}_{i\in\mathbb{Z}/rd\mathbb{Z}}$, described as follows: For $a \in \mathbb{F}_{\mathfrak{p}}$, a acts on X_i by $a \cdot X_i := i(a^{p^i})X_i$. Here, $i : \mathbb{F}_{\mathfrak{p}} \to A_{\mathfrak{p}}$ is the section homomorphism of the natual surjection $A_{\mathfrak{p}} \to \mathbb{F}_{\mathfrak{p}}$.

In the following, we compute $(v(\delta_i))_{i\in\mathbb{Z}/rd\mathbb{Z}}$. First, assume that ϕ has good ordinary reduction. In this case, $\phi[\mathfrak{p}]_{\overline{\mathbb{F}}_{\mathfrak{p}}} := \phi[\mathfrak{p}]_{\mathcal{O}} \times_{\mathrm{Spec}(\mathcal{O})} \mathrm{Spec}(\overline{\mathbb{F}}_{\mathfrak{p}})$ is a direct sum of $\alpha_{q^d} := \mathrm{Spec}(\overline{\mathbb{F}}_{\mathfrak{p}}[X]/(X^{q^d}))$ and a finite étale group scheme over $\overline{\mathbb{F}}_{\mathfrak{p}}$. In particular, $C_{\overline{\mathbb{F}}_{\mathfrak{p}}} := C_{\mathcal{O}} \times_{\mathrm{Spec}(\mathcal{O})} \mathrm{Spec}(\overline{\mathbb{F}}_{\mathfrak{p}})$ is isomorphic to either α_{q^d} or a finite étale group scheme over $\overline{\mathbb{F}}_{\mathfrak{p}}$.

If $C_{\overline{\mathbb{F}}_{\mathfrak{p}}}$ is étale, it follows that $v(\delta_i) = 0$ for all i. If $C_{\overline{\mathbb{F}}_{\mathfrak{p}}} \cong \alpha_{q^d}$, by comparing the right hand side of (1) and α_{q^d}, it follows that there exists an index i such that $v(\delta_i) = 0$ and $v(\delta_j) > 0$ for all $j \neq i$. Therefore, by [12, COROLLAIRE 1.5.1] there exists an isomorphism of $\mathbb{F}_{\mathfrak{p}}$-module schemes for some $\delta \in \mathfrak{m}$:

$$C_{\mathcal{O}} \cong \mathrm{Spec}(\mathcal{O}[X]/(X^{q^d} - \delta X)).$$

We claim that $v(\delta) \leq e$. Since $C_{\mathcal{O}}$ is a closed subscheme of $\phi[\mathfrak{p}]_{\mathcal{O}}$, there exists an $h(X) \in \mathcal{O}[X]$ such that $h'(0) \in \mathcal{O}^*$ and $X^{q^d} - \delta X \mid \phi_f(h(X))$ in $\mathcal{O}[X]$. Since the coefficient of X in $\phi_f(h(X))$ is equal to $fh'(0)$ whose valuation is greater than $v(\delta)$, it follows that $v(\delta) \leq v(f) = e$.

Next, assume that ϕ has good supersingular reduction at $\mathfrak{p}$. Then it follows that $\phi[\mathfrak{p}]_{\overline{\mathbb{F}}_{\mathfrak{p}}} \cong \alpha_{q^{2d}}$ and $C_{\overline{\mathbb{F}}_{\mathfrak{p}}} \cong \alpha_{q^d}$. By the same argument as above, there exists $\delta \in \mathfrak{m}$ with $v(\delta) \leq e$ [1] and an isomorphism:

$$C_{\mathcal{O}} \cong \mathrm{Spec}(\mathcal{O}[X]/(X^{q^d} - \delta X)).$$

Summarizing the above, we proved the following:

Proposition 3.1. *Let L be a finite extension of the maximal unramified extension $K_{\mathfrak{p}}^{\mathrm{ur}}$, e the degree of L over $K_{\mathfrak{p}}^{\mathrm{ur}}$, v the normalized discrete valuation on L, $\mathcal{O}$ the discrete valuation ring of L which corresponds to v.*

[1] One can easily show that $v(\delta) < e$ by looking at the coefficient of X^{q^d} appearing in $\phi_f(h(X))$.

Let ϕ be a Drinfeld A-module of rank two over L which has good reduction and C a cyclic $\mathfrak{p}$-torsion subgroup of ϕ defined over L. Assume that ϕ_T is contained in $\mathcal{O}\{\tau\}$ and its leading coefficient is contained in $\mathcal{O}^*$. Then there exists a $\delta \in \mathcal{O}$ with $v(\delta) \leq e$ such that $C_{\mathcal{O}}$ is isomorphic to $\mathrm{Spec}(\mathcal{O}[X]/(X^{q^{\deg(\mathfrak{p})}} - \delta X))$ as $\mathbb{F}_{\mathfrak{p}}$-module schemes. In particular, the corresponding character $\mathrm{Gal}(\overline{K}_{\mathfrak{p}}/L) \to \mathbb{F}_{\mathfrak{p}}^*(\cong \mathbb{Z}/(q^{\deg(\mathfrak{p})} - 1)\mathbb{Z})$ is the Kummer character asscociated to $\delta \in L^*/(L^*)^{q^{\deg(\mathfrak{p})}-1}$.

3.2. **Properties of Isogeny Characters.** In this subsection and the next section, we prove natural Drinfeld-module analogues of results which are proved by Mazur in [9, §5 The Isogeny Character]. Let ϕ be a Drinfeld A-module of rank two over K which has a cyclic $\mathfrak{p}$-torsion subgroup C defined over K. We have the corresponding character

$$r : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}_{\mathbb{F}_{\mathfrak{p}}}(C) = \mathbb{F}_{\mathfrak{p}}^*$$

which is referred to as the isogeny character associated to (ϕ, C).

Lemma 3.2. *Let $\mathrm{Aut}_{\overline{K}}(\phi, C)$ be the group of automorphisms of ϕ over $\overline{K}$ which preserves C. Then the order of $\mathrm{Aut}_{\overline{K}}(\phi, C)$ divides $q^2 - 1$. Moreover, if $\deg(\mathfrak{p})$ is odd, $\mathrm{Aut}_{\overline{K}}(\phi, C)$ is equal to $\mathbb{F}_q^*$.*

Proof. By Lemma 2.1, $\mathrm{Aut}_{\overline{K}}(\phi)$ is equal to either $\mathbb{F}_q^*$ or $\mathbb{F}_{q^2}^*$. By Lemma 2.2, the natural homomorphism $\mathrm{Aut}_{\overline{K}}(\phi, C) \to \mathrm{Aut}_{\mathbb{F}_{\mathfrak{p}}, K}(C) = \mathbb{F}_{\mathfrak{p}}^* = \mathrm{Aut}_{\mathbb{F}_{\mathfrak{p}}, \overline{K}}(C)$ is injective. It follows that $\mathrm{Aut}_{\overline{K}}(\phi, C) = \mathrm{Aut}_K(\phi, C)$. If $\deg(\mathfrak{p})$ is odd, it holds that $\mathrm{Aut}_{\overline{K}}(\phi, C) = \mathbb{F}_q^*$ because of the injectivity of the above homomorphism. □

Recall that the Carlitz module is a Drinfeld A-module of rank one over K defined by $A \to K\{\tau\} : T \mapsto T + \tau$. Let $\chi = \chi_{\mathfrak{p}} : \mathrm{Gal}(\overline{K}/K) \to \mathbb{F}_{\mathfrak{p}}^*$ be the character associated to the $\mathfrak{p}$-torsion subgroup of the Carlitz module. It is known that χ is unramified outside $\mathfrak{p}$ and ∞, totally ramified at $\mathfrak{p}$ and ∞ splits into $|\mathbb{F}_{\mathfrak{p}}^*/\mathbb{F}_q^*| = \frac{q^d-1}{q-1}$ places with ramification index $q - 1$ on the field extension of K which corresponds to $\ker(\chi)$ (for a proof, see Hayes [8, Theorem 3.2]).

Lemma 3.3. *Let $L/K_{\mathfrak{p}}$ be a finite tamely ramified extension with ramification index e and $I \subset \mathrm{Gal}(\overline{L}/L)$ the inertia subgroup of L. Then $\chi|_I$ is equal to the e-th power of the fundamental character θ_{q^d-1} (for the definition of the fundamental character, see Serre* [15, §1, 1.3]*).*

Proof. The proof is essentially the same as the one in [15, §1, 1.8, Proposition 8]. Indeed, the $\mathfrak{p}$-torsion subgroup of the Carlitz module has a natural Galois-equivariant injection into $V_{\frac{e}{q^d-1}}$ which is defined at the beginning of [15, §1, 1.8]) and the tame inertia subgroup of L acts on $V_{\frac{e}{q^d-1}}$ by $\theta_{q^d-1}^e$ by [15, §1, 1.8, Proposition 6]. □

Lemma 3.4. *There exists a unique $k \in \mathbb{Z}/(q^d - 1)\mathbb{Z}$ such that $r = \alpha \cdot \chi^k$ where $\alpha : \mathrm{Gal}(\overline{K}/K) \to \mathbb{F}_{\mathfrak{p}}^*$ is unramified at $\mathfrak{p}$.*

Proof. Let $I_{\mathfrak{p}} \subset \mathrm{Gal}(\overline{K}/K)$ be the inertia subgroup at $\mathfrak{p}$ (which is determined up to conjugacy). Since r is tamely ramified at $\mathfrak{p}$, $r|_{I_{\mathfrak{p}}}$ factors through $I_{\mathfrak{p}}^{\mathrm{tr}}$, the maximal tame quotient of $I_{\mathfrak{p}}$. Since χ is equal to the fundamental character θ_{q^d-1} on I by Lemma 3.3, it holds that every homomorphism $I_{\mathfrak{p}}^{\mathrm{tr}} \to \mathbb{F}_{\mathfrak{p}}^*$ is a power of the Carlitz character. Hence the assertion follows. □

We use the following notations:

$$\begin{aligned} m &:= |\mathbb{F}_{\mathfrak{p}}^*/\mathbb{F}_q^*| = \frac{q^d-1}{q-1} \\ n &:= \begin{cases} \frac{q^d-1}{q-1} & (\text{if } d \text{ is odd}) \\ \frac{q^d-1}{q^2-1} & (\text{if } d \text{ is even}) \end{cases} \\ t &:= \frac{m}{n} = \begin{cases} 1 & (\text{if } d \text{ is odd}) \\ q+1 & (\text{if } d \text{ is even}) \end{cases} \end{aligned}$$

Proposition 3.5. *In the notation as above, $\alpha^{(q-1)t}$ is trivial.*

Proof. First of all, we prove that $\alpha^{(q-1)t}$ is unramified everywhere outside ∞. By construction, the natural morphism $X_1(\mathfrak{p})_{A[\frac{1}{\mathfrak{p}}]} \to X_0(\mathfrak{p})_{A[\frac{1}{\mathfrak{p}}]}$ is a finite flat Galois covering with Galois group isomorphic to $\mathbb{F}_{\mathfrak{p}}^*/\mathbb{F}_q^*$. Let $X_2(\mathfrak{p})_{A[\frac{1}{\mathfrak{p}}]} \to X_0(\mathfrak{p})_{A[\frac{1}{\mathfrak{p}}]}$ be the finite flat Galois covering which corresponds to the quotient of $\mathbb{F}_{\mathfrak{p}}^*/\mathbb{F}_q^*$ of order n. We claim that this morphism $X_2(\mathfrak{p})_{A[\frac{1}{\mathfrak{p}}]} \to X_0(\mathfrak{p})_{A[\frac{1}{\mathfrak{p}}]}$ is étale.

In the proof of [10, Lemma 8.17], it is proved that $X_2(\mathfrak{p})_K \to X_0(\mathfrak{p})_K$ is étale. Moreover, for every maximal ideal $\mathfrak{l} \neq \mathfrak{p}$ of A, $X_2(\mathfrak{p})_{A[\frac{1}{\mathfrak{p}}]} \to X_0(\mathfrak{p})_{A[\frac{1}{\mathfrak{p}}]}$ is étale over the generic point of $X_0(\mathfrak{p})_{\mathbb{F}_{\mathfrak{l}}}$. Indeed, let $Y_0(\mathfrak{p})^*_{A[\frac{1}{\mathfrak{p}}]}$ and $Y_1(\mathfrak{p})^*_{A[\frac{1}{\mathfrak{p}}]}$ be the inverse images of $\mathbb{A}^1_{A[\frac{1}{\mathfrak{p}}]} \setminus \{0\}$ with respect to j-invariant maps. Since $Y_1(\mathfrak{p})^*_{A[\frac{1}{\mathfrak{p}}]}$ is étale over $Y_0(\mathfrak{p})^*_{A[\frac{1}{\mathfrak{p}}]}$, $X_1(\mathfrak{p})_{A[\frac{1}{\mathfrak{p}}]} \to X_0(\mathfrak{p})_{A[\frac{1}{\mathfrak{p}}]}$ is étale over the generic point of $X_0(\mathfrak{p})_{\mathbb{F}_{\mathfrak{l}}}$. In particular, $X_2(\mathfrak{p})_{A[\frac{1}{\mathfrak{p}}]} \to X_0(\mathfrak{p})_{A[\frac{1}{\mathfrak{p}}]}$ is étale over the generic point of $X_0(\mathfrak{p})_{\mathbb{F}_{\mathfrak{l}}}$.

However, since $X_0(\mathfrak{p})_{A[\frac{1}{\mathfrak{p}}]}$ is smooth over $\mathrm{Spec}(A[\frac{1}{\mathfrak{p}}])$ by [4, (5.2) (i)], the branched locus of $X_2(\mathfrak{p})_{A[\frac{1}{\mathfrak{p}}]} \to X_0(\mathfrak{p})_{A[\frac{1}{\mathfrak{p}}]}$ consists of codimension 1 irreducible closed subschemes by Zariski-Nagata purity. Hence the branched locus of $X_2(\mathfrak{p})_{A[\frac{1}{\mathfrak{p}}]} \to X_0(\mathfrak{p})_{A[\frac{1}{\mathfrak{p}}]}$ must be empty.

Let x be the K-rational point of $X_0(\mathfrak{p})$ which corresponds to (ϕ, C). Let K_1/K be the finite Galois extension which corresponds to the kernel of $\mathrm{Gal}(\overline{K}/K) \xrightarrow{r} \mathbb{F}_{\mathfrak{p}}^* \to \mathbb{F}_{\mathfrak{p}}^*/\mathbb{F}_q^*$. This is a cyclic extension of degree dividing m and x admits a lift to a point of $Y_1(\mathfrak{p})(K_1)$. By the above argument, there exists a subextension K_2/K of K_1/K which is unramified outside $\mathfrak{p}$ and ∞ and such that $[K_1 : K_2]$ divides t. Hence $r^{(q-1)t}$ factors through $\mathrm{Gal}(K_2/K)$. This shows that $r^{(q-1)t}$ is unramified outside $\mathfrak{p}$ and ∞, so is $\alpha^{(q-1)t}$. Moreover, since α is also unramified at $\mathfrak{p}$, tamely ramified at ∞ and the geometric tame fundamental group of $\mathbb{A}^1_{\overline{\mathbb{F}}_q}$ is trivial, $\alpha^{(q-1)t}$ is also unramified at ∞. Hence $\alpha^{(q-1)t}$ factors through $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$.

Now we prove that $\alpha^{(q-1)t}$ is trivial. It suffices to prove that $r^{(q-1)t}|_{\mathrm{Gal}(\overline{K}_\infty/K_\infty)}$ is trivial since $\chi^{q-1}|_{\mathrm{Gal}(\overline{K}_\infty/K_\infty)}$ is trivial. Let Λ be a $\mathrm{Gal}(\overline{K}_\infty/K_\infty)$-stable discrete A-lattice of rank two in $\mathbb{C}_\infty$ which corresponds to ϕ via analytic uniformization (for the theory of analytic uniformization of Drinfeld modules over $\mathbb{C}_\infty$, see [7, 4.6]). Then the following commutative diagram exists:

$$\begin{array}{ccccc} & & \mathrm{Aut}_A(\Lambda) & \xrightarrow{\sim} & \mathrm{GL}_2(A) \\ & \nearrow & \downarrow & & \downarrow \\ \mathrm{Gal}(\overline{K}_\infty/K_\infty) & \longrightarrow & \mathrm{Aut}_{\mathbb{F}_{\mathfrak{p}}}(\mathfrak{p}^{-1}\Lambda/\Lambda) & \xrightarrow{\sim} & \mathrm{GL}_2(\mathbb{F}_{\mathfrak{p}}) \\ & \searrow & \downarrow\wr & \nearrow & \\ & & \mathrm{Aut}_{\mathbb{F}_{\mathfrak{p}}}(\phi[\mathfrak{p}](\overline{K}_\infty)) & & \end{array}$$

Since the image of $\mathrm{Gal}(\overline{K}_\infty/K_\infty) \to \mathrm{GL}_2(A)$ is finite, eigenvalues of each element in this image is contained in $\overline{\mathbb{F}}_q$. In particular, the characteristic polynomial of each element is contained in $(\overline{\mathbb{F}}_q \cap A)[T] = \mathbb{F}_q[T]$. This shows that the image of $r|_{\mathrm{Gal}(\overline{K}_\infty/K_\infty)}$ is contained in $\mathbb{F}_q^*$ if d is odd and in $\mathbb{F}_{q^2}^*$ if d is even. Hence $r^{(q-1)t}|_{\mathrm{Gal}(\overline{K}_\infty/K_\infty)}$ is trivial. □

Lemma 3.6. *In the notation as above, assume that ϕ has potentially good reduction at $\mathfrak{p}$. Then the element $k \in \mathbb{Z}/(q^d-1)\mathbb{Z}$ in the assertion of Lemma 3.4 takes only the following values modulo n:*

$$k = \begin{cases} \frac{x}{q+1} & \text{where } 0 \le x \le q+1 \text{ (if } \deg(\mathfrak{p}) \text{ is odd)} \\ 0, 1 & \text{(if } \deg(\mathfrak{p}) \text{ is even)} \end{cases}$$

Proof. Since ϕ has potentially good reduction at $\mathfrak{p}$, ϕ has good reduction over $L \coloneqq K_\mathfrak{p}(\pi^{\frac{1}{q^2-1}})$ where π is a uniformizer of $\mathfrak{p}$ by Lemma 2.3. We abbreviate the fundamental character θ_{q^d-1} as θ. By Lemma 3.3, it holds that $\chi = \theta^{q^2-1}$ as characters on the inertia subgroup I of L. So we have an equality $r = \theta^{k(q^2-1)}$ on I. Moreover, by Proposition 3.1, $r|_I$ is also equal to the Kummer character associated to some $\delta \in LK_\mathfrak{p}^{\mathrm{ur}}$ with $v(\delta) \le q^2-1$ and this character is equal to $\theta^{v(\delta)}$. Hence it follows that $0 \le \langle k(q^2-1)\rangle_{q^d-1} \le q^2-1$. Here, $\langle k(q^2-1)\rangle_{q^d-1}$ is defined to be the unique integer y with $0 \le y < q^d-1$ which satisfies $y \equiv k(q^2-1) \bmod q^d-1$. Since $q^2-1 \mid q^d-1$ if d is even, k is equal to 0 or 1 modulo m. If d is odd, since $q+1$ is relatively prime to $\frac{q^d-1}{q-1}$, it follows that $\langle k(q^2-1)\rangle_{q^d-1} = x(q-1)$ with some $0 \le x \le q+1$. □

4. Consequences

We use the same notation as in subsection 2.2.

Set $S_\phi \coloneqq \{\mathfrak{l} \mid \mathfrak{l} \text{ is a maximal ideal of } A \text{ at which } \phi \text{ has potentially good reduction}\}$. Assume that $\mathfrak{l} \in S_\phi$. By local class field theory, we have the following noncanonical isomorphism which depends on the choice of a uniformizer of $K_\mathfrak{l}$:

$$\mathrm{Gal}(\overline{K}_\mathfrak{l}/K_\mathfrak{l})^{\mathrm{ab}} \cong A_\mathfrak{l}^* \times \hat{\mathbb{Z}}.$$

We factorize $\alpha_\mathfrak{l} \coloneqq \alpha|_{\mathrm{Gal}(\overline{K}_\mathfrak{l}/K_\mathfrak{l})^{\mathrm{ab}}}$ as $\alpha_\mathfrak{l} = \gamma_\mathfrak{l} \cdot b_\mathfrak{l}$ where $\gamma_\mathfrak{l}$ factors through the projection to $A_\mathfrak{l}^*$ and $b_\mathfrak{l}$ is unramified. Moreover, by Lemma 3.5, the orders of $\gamma_\mathfrak{l}$ and $b_\mathfrak{l}$ divide $(q-1)t$ and the finite Galois field extension $L/K_\mathfrak{l}$ which corresponds to the kernel of $\gamma_\mathfrak{l}$ is totally tamely ramified.

We claim that ϕ_L has good reduction over L. Let M/L be the field extension corresponding to the kernel of $b_\mathfrak{l} \cdot \chi_\mathfrak{p}^k|_{\mathrm{Gal}(\overline{L}/L)}$, the isogeny character of ϕ over L. Now the claim follows from the following general lemma:

Lemma 4.1. *Let $\mathfrak{p}$ be a maximal ideal of A with $d \coloneqq \deg(\mathfrak{p}) \ge 2$. Let L be an A-field with complete discrete normalized valuation v which satisfies $v(A) \ge 0$ and the characteristic of the residue field of L is different from $\mathfrak{p}$, M/L a finite unramified extension and ϕ a Drinfeld A-module of rank two over L which has potentially good reduction. If ϕ has a nontrivial $\mathfrak{p}$-torsion over M, ϕ has good reduction over L.*

Proof. First, write $\phi_T = T + a_1\tau + a_2\tau^2$ where $a_1 \in L$ and $a_2 \in L^*$. Since ϕ has potentially good reduction over L, it holds that $\frac{v(a_1)}{q-1} \ge \frac{v(a_2)}{q^2-1}$. By replacing ϕ with $u\phi u^{-1}$ for a suitable $u \in L^*$, we may assume that $0 \le v(a_2) < q^2-1$ (hence $v(a_1) \ge 0$).

Since $\phi[\mathfrak{p}](\overline{L})$ is a two-dimensional $\mathbb{F}_\mathfrak{p}$-vector space, the Newton polygon of $\frac{\phi_f(X)}{X} \in L[X]$ has at most two line segments. Moreover, since $\phi_f(X)$ has a nonzero root in M, it follows that at least one of their slopes is an integer.

If the Newton polygon of $\frac{\phi_f(X)}{X} \in L[X]$ is a line, the unique slope is equal to $\frac{v(a_2)}{q^2-1}$, which is an integer if and only if $v(a_2) = 0$ i.e. ϕ has good reduction. On the other hand, if the Newton polygon of $\frac{\phi_f(X)}{X}$ consists of two line segments, some computations show that the maximal slope is smaller than $\frac{(q^d+1)v(a_2)}{q^d(q^2-1)}$. It follows that the valuation of each root of $\frac{\phi_f(X)}{X}$ is contained in $[-\frac{(q^d+1)v(a_2)}{q^d(q^2-1)}, 0]$. Moreover, if the minimal slope is zero, it holds that $v(a_2) = 0$ or $v(a_1) = 0$. Since $v(a_2) = 0$ holds in both cases, we may assume that the valuation of each root of $\frac{\phi_f(X)}{X}$ is contained in $[-\frac{(q^d+1)v(a_2)}{q^d(q^2-1)}, 0)$.

However, since $d \geq 2$, it holds that

$$\frac{(q^d+1)v(a_2)}{q^d(q^2-1)} \leq \frac{(q^d+1)(q^2-2)}{q^d(q^2-1)} < 1.$$

Hence the valuation cannot be an integer. □

Since $L/K_{\mathfrak{l}}$ is totally ramified, by reducing ϕ modulo the maximal ideal of L we obtain a Drinfeld A-module $\phi_{\mathbb{F}_{\mathfrak{l}}}$ over $\mathbb{F}_{\mathfrak{l}}$ with $\mathfrak{p}$-isogeny defined over $\mathbb{F}_{\mathfrak{l}}$ whose isogeny character is equal to $b_{\mathfrak{l}} \cdot \chi^k$.

Write ϕ_T as $T + a_1\tau + a_2\tau^2$ for $a_1 \in K$ and $a_2 \in K^*$. Let $\rho_{\mathfrak{p}} : G_K \to \mathrm{GL}_2(\mathbb{F}_{\mathfrak{p}})$ be the Galois representation associated to $\phi[\mathfrak{p}]$. It is known that $\det(\rho_{\mathfrak{p}})$ coincides with the Galois representation associated to the $\mathfrak{p}$-torsion submodule of the Drinfeld A-module ψ of rank one defined by $\psi_T = T - a_2\tau$ (see van der Heiden [17], for example). Therefore, if we denote a character $\mathrm{Gal}(\overline{K}/K) \to \mathbb{F}_q^*$ associated to $(-a_2)^{-1} \in K^*/(K^*)^{q-1}$ by $\epsilon : G_K \to \mathbb{F}_q^*$, it holds that $\det(\rho_{\mathfrak{p}}) = \epsilon \otimes \chi$.

The Frobenius trace of $\phi_{\mathbb{F}_{\mathfrak{l}}}$ modulo $\mathfrak{p}$ is expressed as $b_{\mathfrak{l}}(\mathrm{Frob}_{\mathfrak{l}})\chi^k(\mathrm{Frob}_{\mathfrak{l}}) + \epsilon(\mathrm{Frob}_{\mathfrak{l}})b_{\mathfrak{l}}(\mathrm{Frob}_{\mathfrak{l}})^{-1}\chi^{1-k}(\mathrm{Frob}_{\mathfrak{l}})$. Moreover, it is easily observed that $\chi(\mathrm{Frob}_{\mathfrak{l}}) = g \bmod \mathfrak{p}$. Hence the Frobenius trace of $\phi_{\mathbb{F}_{\mathfrak{l}}}$ modulo $\mathfrak{p}$ is equal to $b_{\mathfrak{l}}(\mathrm{Frob}_{\mathfrak{l}})g^k + \epsilon(\mathrm{Frob}_{\mathfrak{l}})b_{\mathfrak{l}}(\mathrm{Frob}_{\mathfrak{l}})^{-1}g^{1-k}$. In particular, it is contained in $\mathbb{F}_q^* \cdot g^k + \mathbb{F}_q^* \cdot g^{1-k}$ if $\deg(\mathfrak{p})$ is odd and in $\mathbb{F}_{q^2}^* \cdot g^k + \mathbb{F}_{q^2}^* \cdot g^{1-k}$ if $\deg(\mathfrak{p})$ is even. Similarly, one can calculate the trace of an arbitrary power of Frobenius endomorphism.

For each positive integer l, we define a certain set $a(\mathbb{F}_{\mathfrak{l}^l}/\mathbb{F}_{\mathfrak{l}}) \subset A$ as follows:

$$a(\mathbb{F}_{\mathfrak{l}^l}/\mathbb{F}_{\mathfrak{l}}) \coloneqq \{a \in A \mid a \text{ is the trace of } \tau^{\deg(\mathfrak{l})l} \text{ of some Drinfeld } A\text{-module of rank two over } \mathbb{F}_{\mathfrak{l}}\}.$$

Theorem 4.2. *Let ϕ be a Drinfeld A-module of rank two over K. Assume that the following conditions are satisfied:*

($\dagger_{\mathfrak{p}}$) $\deg(\mathfrak{p})$ *is even and greater than two.*

($\dagger_{\phi}$) $\mathfrak{p} \in S_\phi$ *and S_ϕ contains a prime of degree one.*

Then ϕ does not have a nontrivial cyclic $\mathfrak{p}$-torsion subgroup defined over K.

Proof. Let $\mathfrak{l}$ be an arbitrary prime of degree one contained in S_ϕ. By Lemma 3.6, we know that $(q^2-1)k \equiv 0$ or $q^2 - 1 \bmod q^d - 1$. By considering the trace of the Frobenius endomorphism $\tau \in \mathrm{End}(\phi_{\mathbb{F}_{\mathfrak{l}}})$, we see that one of the elements of $\mathbb{F}_{q^2}^* \cdot T + \mathbb{F}_{q^2}^* \bmod \mathfrak{p}$ is congruent to one of the elements of $a(\mathbb{F}_{\mathfrak{l}}/\mathbb{F}_{\mathfrak{l}})$. However, since $a(\mathbb{F}_{\mathfrak{l}}/\mathbb{F}_{\mathfrak{l}}) \subset \mathbb{F}_q$ by Lemma 2.5 (3), it follows that $T \in \mathbb{F}_{q^2} \subset \mathbb{F}_{\mathfrak{p}}$. This is impossible since $d \geq 4$ and T generates $\mathbb{F}_{\mathfrak{p}}$ as an $\mathbb{F}_q$-algebra. □

Proposition 4.3. *Let ϕ be a Drinfeld A-module of rank two over K. Assume that the following conditions are satisfied:*

($\dagger_q$) q *is odd.*

($\dagger_{\mathfrak{p}}$) $\deg(\mathfrak{p})$ *is odd and greater than q.*

($\dagger_{\phi}$) $\mathfrak{p} \in S_\phi$ *and S_ϕ contains a prime of degree one.*

Then ϕ does not have a nontrivial cyclic $\mathfrak{p}$-torsion subgroup defined over K with $k \not\equiv \frac{1}{2}$ mod $\frac{q^d-1}{q-1}$ (i.e. $x \neq \frac{q+1}{2}$), where k and x are defined as in the previous section.

Proof. Let $\mathfrak{l}$ be an arbitrary prime of degree one contained in S_ϕ. By considering the trace of the $(q+1)$-th power of Frobenius $\tau^{q+1} \in \mathrm{End}(\phi_{\mathbb{F}_\mathfrak{l}})$, it holds that one of the elements of

$$\mathbb{F}_q^* \cdot g^{(q+1)k} + \mathbb{F}_q^* \cdot g^{(q+1)(1-k)}$$

is congruent modulo $\mathfrak{p}$ to one of the elements of $a(\mathbb{F}_{\mathfrak{l}^{q+1}}/\mathbb{F}_\mathfrak{l})$. Here, g is the monic generator of $\mathfrak{l}$.

First, we claim that $(q+1)k$ is not equal to 0 mod $\frac{q^d-1}{q-1}$ (i.e. $x \neq 0$). Indeed, if this is the case, by considering the trace of $\tau \in \mathrm{End}(\phi_{\mathbb{F}_\mathfrak{l}})$ and Lemma 2.5 (3), it holds that one of the elements of $\mathbb{F}_q^* + \mathbb{F}_q^* \cdot g$ is congruent to one of the elements of $a(\mathbb{F}_\mathfrak{l}/\mathbb{F}_\mathfrak{l}) \subset \mathbb{F}_q$, which gives a contradiction. By the same argument, it holds that $(q+1)k$ is not equal to $q+1$ mod $\frac{q^d-1}{q-1}$ (i.e. $x \neq q+1$). Hence the degree of $\mathbb{F}_q^* \cdot g^{(q+1)k} + \mathbb{F}_q^* \cdot g^{(q+1)(1-k)} = \mathbb{F}_q^* \cdot g^x + \mathbb{F}_q^* \cdot g^{q+1-x}$ is greater than $\frac{q+1}{2}$ and less than or equal to q if k is not congruent modulo $\frac{q^d-1}{q-1}$ to $\frac{1}{2}$. On the other hand, the degree of each element of $a(\mathbb{F}_{\mathfrak{l}^{q+1}}/\mathbb{F}_\mathfrak{l})$ is less than or equal to $\frac{q+1}{2}$ by Corollary 2.6. Hence the assertion follows. □

Remark 4.4. *In the above Proposition, if $(\dagger_q)$ is replaced by the condition that q is even, the above proof shows that such k does not exist.*

Theorem 4.5. *Let ϕ be a Drinfeld A-module of rank two over K. Assume that the following conditions are satisfied:*

$(\dagger_q)$ q is even.

$(\dagger_\mathfrak{p})$ $\deg(\mathfrak{p})$ is greater than q.

$(\dagger_\phi)$ $\mathfrak{p} \in S_\phi$ and S_ϕ contains a prime of degree one.

Then ϕ does not have a nontrivial cyclic $\mathfrak{p}$-torsion subgroup defined over K.

Proof. This follows from Remark 4.4 and Theorem 4.2. □

The rest of this section is devoted to the proof of the following theorem.

Theorem 4.6. *Let ϕ be a Drinfeld A-module of rank two over K. Assume that the following conditions are satisfied:*

$(\dagger_q)$ q is odd.

$(\dagger_\mathfrak{p})$ $\deg(\mathfrak{p})$ is odd and greater than 1. If $q = 3$, then $\deg(\mathfrak{p}) > 3$.

$(\dagger_\phi)$ $S_\phi = \sum_K^{\mathrm{fin}}$.

Then ϕ does not have a nontrivial cyclic $\mathfrak{p}$-torsion subgroup defined over K with $k \equiv \frac{1}{2}$ mod $\frac{q^d-1}{q-1}$ (i.e. $x = \frac{q+1}{2}$), where k and x are defined as in the previous section.

Proof. By Proposition 3.5, α^{q-1} is trivial. Hence, by taking the twist of ϕ which corresponds to α^{-1}, we may assume that $r = \chi^k$.

Since we have reduced the situation to the case when $\alpha = 1$, ϕ has good reduction at every finite place outside $\mathfrak{p}$ by Lemma 4.1. In particular, $q-1 \mid q^2-1 \mid v_\mathfrak{l}(a_2)$ for every maximal ideal $\mathfrak{l} \neq \mathfrak{p}$. Here, $v_\mathfrak{l}$ is the normalized discrete valuation on K corresponding to $\mathfrak{l}$. Hence it holds that $(-a_2)^{-1} \in K^*$ modulo $(K^*)^{q-1}$ is equal to sf^u for some $s \in \mathbb{F}_q^*$ and some $0 \leq u < q-1$.

Write $2k \equiv 1 + v\frac{q^d-1}{q-1}$ mod q^d-1 for some $0 \leq v < q-1$ and fix an arbitrary maximal ideal $\mathfrak{l} \neq \mathfrak{p}$ of degree smaller than d with monic generator g. By considering the trace of $\tau^{2\deg(\mathfrak{l})} \in \mathrm{End}(\phi_{\mathbb{F}_\mathfrak{l}})$, it holds that $g^{2k} + \epsilon(\mathrm{Frob}_\mathfrak{l})^2 g^{2-2k}$ is congruent modulo $\mathfrak{p}$ to one of the elements of $a(\mathbb{F}_{\mathfrak{l}^2}/\mathbb{F}_\mathfrak{l})$.

Let $X^2 - aX + b$ be the characteristic polynomial of $\tau^{\deg(\mathfrak{l})} \in \mathrm{End}(\phi_{\mathbb{F}_\mathfrak{l}})$. By Lemma 2.5 (1), b is equal to the determinant of $\tau^{\deg(\mathfrak{l})}$ with regard to the $\mathfrak{p}$-adic representation associated to ϕ, which is equal to $\epsilon(\mathrm{Frob}_\mathfrak{l})g$.

The characteristic polynomial of $\tau^{2\deg(\mathfrak{l})} \in \mathrm{End}(\phi_{\mathbb{F}_\mathfrak{l}})$ is then equal to

$$X^2 - (a^2 - 2b)X + b^2.$$

Therefore, it holds that

$$g^{2k} + \epsilon(\mathrm{Frob}_\mathfrak{l})^2 g^{2-2k} \equiv a^2 - 2\epsilon(\mathrm{Frob}_\mathfrak{l})g \bmod \mathfrak{p}.$$

Since $\deg(\mathfrak{l}) < d$ and $\deg(a) \leq \frac{\deg(\mathfrak{l})}{2}$ by Lemma 2.5(3), it holds that $a^2 = gN_{\mathbb{F}_\mathfrak{p}/\mathbb{F}_q}(g)^{-v}(\epsilon(\mathrm{Frob}_\mathfrak{l}) + N_{\mathbb{F}_\mathfrak{p}/\mathbb{F}_q}(g)^v)^2$ where $N_{\mathbb{F}_\mathfrak{p}/\mathbb{F}_q}(g) \in \mathbb{F}_q^*$ is defined to be the unique element of $\mathbb{F}_q^*$ which satisfies $g^{\frac{q^d-1}{q-1}} \equiv N_{\mathbb{F}_\mathfrak{p}/\mathbb{F}_q}(g) \bmod \mathfrak{p}$. Since g is irreducible, it holds that $a = 0$ and $\epsilon(\mathrm{Frob}_\mathfrak{l}) + N_{\mathbb{F}_\mathfrak{p}/\mathbb{F}_q}(g)^v = 0$. In the following, we concentrate on the second equality. We have $\epsilon(\mathrm{Frob}_\mathfrak{l}) = N_{\mathbb{F}_\mathfrak{l}/\mathbb{F}_q}(sf^u)$ and, by the reciprocity law [13, Theorem 3.5], it holds that $N_{\mathbb{F}_\mathfrak{p}/\mathbb{F}_q}(g) = (-1)^{\deg(\mathfrak{l})} N_{\mathbb{F}_\mathfrak{l}/\mathbb{F}_q}(f)$. To sum it up, we have that $N_{\mathbb{F}_\mathfrak{l}/\mathbb{F}_q}(sf^{\langle u-v\rangle_{q-1}}) = (-1)^{v\deg(\mathfrak{l})+1}$ where $\langle u-v\rangle_{q-1}$ is defined to be the unique integer y with $0 \leq y < q-1$ which satisfies $y \equiv u - v \bmod q-1$.

Let $l \coloneqq \gcd(u-v, q-1)$. Then it holds that $N_{\mathbb{F}_\mathfrak{l}/\mathbb{F}_q}(f^{\langle u-v\rangle_{q-1}}) \in (\mathbb{F}_q^*)^l$. First, by taking $\mathfrak{l}$ to be a prime of degree one, it follows that $s \in (-1)^{v+1}(\mathbb{F}_q^*)^l$. Next, by taking $\mathfrak{l}$ to be a prime of degree two, it follows that $s^{q+1} = s^2 \in -(\mathbb{F}_q^*)^l$. From these facts, we obtain that $-1 \in (\mathbb{F}_q^*)^l$ (i.e. $l \mid \frac{q-1}{2}$) and $s \in (\mathbb{F}_q^*)^l$.

In the following, we assume that $\deg(\mathfrak{l})$ is odd.

Take arbitrary l-th roots of s and -1 and denote them by $s^{\frac{1}{l}}$ and $(-1)^{\frac{1}{l}}$, respectively. We take a $\frac{q-1}{2l}$-th power of $N_{\mathbb{F}_\mathfrak{l}/\mathbb{F}_q}(sf^{\langle u-v\rangle_{q-1}}) = (-1)^{v\deg(\mathfrak{l})+1}$. First, since $\deg(\mathfrak{l})$ is odd, it holds that $N_{\mathbb{F}_\mathfrak{l}/\mathbb{F}_q}(s)^{\frac{q-1}{2l}} = s^{\frac{q^{\deg(\mathfrak{l})}-1}{2l}} = (s^{\frac{1}{l}})^{\frac{q-1}{2}}$. Second, note that, since $\frac{\langle u-v\rangle_{q-1}}{l}$ is relatively prime to $\frac{q-1}{l}$ which is even, $\frac{\langle u-v\rangle_{q-1}}{l}$ is odd. Since $\frac{(q^{\deg(\mathfrak{l})}-1)\langle u-v\rangle_{q-1}}{q-1} \cdot \frac{q-1}{2l} = \frac{q^{\deg(\mathfrak{l})}-1}{2} \cdot \frac{\langle u-v\rangle_{q-1}}{l}$, it holds that $N_{\mathbb{F}_\mathfrak{l}/\mathbb{F}_q}(f^{\langle u-v\rangle_{q-1}})^{\frac{q-1}{2l}} = N_{\mathbb{F}_\mathfrak{l}/\mathbb{F}_q}(f)^{\frac{q-1}{2}}$. From these observations, we have the following equality:

$$\left(\frac{f}{\mathfrak{l}}\right) = \left(\frac{s^{\frac{1}{l}}(-1)^{\frac{v+1}{l}}}{\mathfrak{l}}\right).$$

Here, $\left(\frac{-}{\mathfrak{l}}\right)$ denotes the quadratic residue symbol for $\mathbb{F}_\mathfrak{l}$. Since v does not depend on $\mathfrak{l}$, by taking $\tilde{f}$ to be $s^{\frac{1}{l}}(-1)^{\frac{v+1}{l}}f$, it follows that the following condition (†) holds:

(†) Let C be a hyperelliptic curve over $\mathbb{F}_q$ whose affine equation is given by $y^2 = \tilde{f}(x)$ with natural double cover $C \to \mathbb{P}^1_{\mathbb{F}_q}$. For each odd positive integer $d' < d$, every $\mathbb{F}_{q^{d'}}$-rational point of $\mathbb{P}^1_{\mathbb{F}_q}$ admits a lift to an $\mathbb{F}_{q^{d'}}$-rational point of C.

Let d' be an odd integer in $(2\log_q(d-1), d)$ which exists under $(\dagger_q)$ and $(\dagger_\mathfrak{p})$. By the Weil estimate, it holds that $|C(\mathbb{F}_{q^{d'}})| \leq q^{d'} + 1 + 2g(C)q^{\frac{d'}{2}} = q^{d'} + 1 + (d-1)q^{\frac{d'}{2}}$. On the other hand, since (†) is satisfied, it holds that $|C(\mathbb{F}_{q^{d'}})| \geq 2q^{d'} + 1$. By combining these two inequalities, we have $d \geq 1 + q^{\frac{d'}{2}}$ so $d' \leq 2\log_q(d-1)$. This is a contradiction. □

Corollary 4.7. *Let ϕ be a Drinfeld A-module of rank two over K. Assume that the following conditions are satisfied:*

($\dagger_\mathfrak{p}$) $\deg(\mathfrak{p})$ *is greater than q.*

($\dagger_\phi$) $S_\phi = \sum_K^{\mathrm{fin}}$.
Then ϕ does not have a nontrivial cyclic $\mathfrak{p}$-torsion subgroup defined over K.

Proof. If q is even, the assertion follows from Theorem 4.5. So we may assume that q is odd. If d is even, the assertion follows from Theorem 4.2. Otherwise, the assertion follows from Proposition 4.3 and Theorem 4.6. □

Remark 4.8. *(1) The above Corollary 4.7 can be seen as a generalization of the result of Pál* [11, Theorem 8.10] *where he proved the case when $q = 2$ and ϕ (appears in the assertion of the corollary) has good reduction at every finite place, as is mentioned in the introduction.*

(2) In the above Corollary 4.7, we cannot replace the condition $d > q$ with $d \geq q$. For example, if $q = d = 3$, the Drinfeld modular curves $X_0(T^3 - T + 1)$ and $X_0(T^3 - T - 1)$ have K-rational CM points which arise as Drinfeld modules with cyclic torsion subgroups over K (see Lemma 5.4). Moreover, it is known that, if a Drinfeld modular curve $X_0(\mathfrak{p})$ with $\deg(\mathfrak{p}) \geq 3$ has a K-rational CM points, then $q = d = 3$ and $\mathfrak{p}$ is either $T^3 - T + 1$ or $T^3 - T - 1$ (see Schweizer [14, Remark 4.6]*). In the end of the next section, we shall discuss K-rational points of $X_0(\mathfrak{p})$ with $\deg(\mathfrak{p}) = 3$.*

5. Unconditional Results

In this section, we discuss how one can remove the conditions ($\dagger_\phi$) which appear in the main results proved in the previous section when $\deg(\mathfrak{p})$ is equal to three or four. First, we introduce a result of Armana:

Proposition 5.1 (Armana, [1, Proposition 7.6])**.** *Let ϕ be a Drinfeld A-module of rank two over K which has a $\mathfrak{p}$-isogeny defined over K. Suppose that $\deg(\mathfrak{p})$ is equal to three or four. Then ϕ has potentially good reduction at every finite place different from $\mathfrak{p}$.*

Additionally, we prove the following concerning potentially good reduction at $\mathfrak{p}$:

Proposition 5.2. *Let ϕ be a Drinfeld A-module of rank two over K which has a $\mathfrak{p}$-isogeny defined over K. Suppose that $\deg(\mathfrak{p})$ is equal to three or four. Then ϕ has potentially good reduction at $\mathfrak{p}$.*

Proof. Let $J_0(\mathfrak{p})$ be the Jacobian of $X_0(\mathfrak{p})_K$ and J' an optimal quotient of $J_0(\mathfrak{p})$ over K. By [11, Lemma 3.4], J' does not have a K-rational p-primary torsion. Suppose that the Mordell-Weil group of J' is finite. Let $\mathcal{J}'$ be the Neron model of J' over $A_\mathfrak{p}$ and set $\overline{\mathcal{J}}' \coloneqq \mathcal{J}' \times_{\mathrm{Spec}(A_\mathfrak{p})} \mathrm{Spec}(\mathbb{F}_\mathfrak{p})$. Since the torsion subgroup of the kernel of the specialization map $J'(K) \cong \mathcal{J}'(A_\mathfrak{p}) \to \overline{\mathcal{J}}'(\mathbb{F}_\mathfrak{p})$ is a finite p-group (for a proof, see [2, Proposition 3.2]), it follows that $J'(K) \to \overline{\mathcal{J}}'(\mathbb{F}_\mathfrak{p})$ is injective.

Next, let $X_0(\mathfrak{p})^{\mathrm{sm}}_{A_\mathfrak{p}}$ be the smooth locus of $X_0(\mathfrak{p})_{A_\mathfrak{p}}$ and $X_0(\mathfrak{p})^{\mathrm{sm}}_{\mathbb{F}_\mathfrak{p}} \coloneqq X_0(\mathfrak{p})^{\mathrm{sm}}_{A_\mathfrak{p}} \times_{\mathrm{Spec}(A_\mathfrak{p})} \mathrm{Spec}(\mathbb{F}_\mathfrak{p})$. Note that $\infty : \mathrm{Spec}(A_\mathfrak{p}) \to X_0(\mathfrak{p})_{A_\mathfrak{p}}$ factors through $X_0(\mathfrak{p})^{\mathrm{sm}}_{A_\mathfrak{p}}$. Let $x \in X_0(\mathfrak{p})$ be a K-rational point which reduces to ∞ after the reduction modulo $\mathfrak{p}$. Observe the following commutative diagram:

$$\begin{array}{ccc}
X_0(\mathfrak{p})(K) & \longrightarrow & J'(K) \\
\uparrow & & \wr\uparrow \\
X_0(\mathfrak{p})^{\mathrm{sm}}_{A_\mathfrak{p}}(A_\mathfrak{p}) & \longrightarrow & \mathcal{J}'(A_\mathfrak{p}) \\
\downarrow & & \downarrow \\
X_0(\mathfrak{p})^{\mathrm{sm}}_{\mathbb{F}_\mathfrak{p}}(\mathbb{F}_\mathfrak{p}) & \longrightarrow & \overline{\mathcal{J}}'(\mathbb{F}_\mathfrak{p})
\end{array}$$

Here, $X_0(\mathfrak{p})(K) \to J'(K)$ is a morphism induced by $X_0(\mathfrak{p})_K \hookrightarrow J_0(\mathfrak{p}) : y \mapsto [y - \infty]$ and $X_0(\mathfrak{p})^{\mathrm{sm}}_{A_\mathfrak{p}} \to \mathcal{J}'$ is a morphism induced by the Neron mapping property. Since ∞ is in the smooth locus of $X_0(\mathfrak{p})_{A_\mathfrak{p}}$, the morphism $x : \mathrm{Spec}(A_\mathfrak{p}) \to X_0(\mathfrak{p})_{A_\mathfrak{p}}$ also factors through $X_0(\mathfrak{p})^{\mathrm{sm}}_{A_\mathfrak{p}}$. So the above diagram shows that $[x - \infty] = 0$ in $J'(K)$. The rest of the proof follows from the same argument as in [1, Proposition 7.6]. □

Corollary 5.3. *Let $\mathfrak{p}$ be a maximal ideal of A of degree four. Then no Drinfeld A-module of rank two over K has a $\mathfrak{p}$-isogeny defined over K. Moreover, the set of K-rational points of the Drinfeld modular curve $Y_0(\mathfrak{p})$ is empty.*

Proof. The first half of the claim follows from Theorem 4.2, together with Proposition 5.1 and Proposition 5.2. To prove the last half of the claim, it suffices to show that each K-rational point of $Y_0(\mathfrak{p})$ comes from a Drinfeld module ϕ over K with a cyclic $\mathfrak{p}$-torsion subgroup C over K. This follows from Lemma 5.4 below. □

Lemma 5.4. *Let $(\overline{\phi}, \overline{C})$ be a Drinfeld A-module of rank two over $\overline{K}$ and a cyclic $\mathfrak{p}$-torsion subgroup of $\overline{\phi}$. Suppose that the isomorphism class of $(\overline{\phi}, \overline{C})$ is invariant under $\mathrm{Gal}(\overline{K}/K)$-action. Then there exists a pair (ϕ, C) of a Drinfeld A-module over K and a cyclic $\mathfrak{p}$-torsion subgroup of ϕ defined over K such that (ϕ, C) is isomorphic to $(\overline{\phi}, \overline{C})$ over $\overline{K}$.*

Proof. The proof of this lemma is essentially the same as the one in [3, Proposition 3.2] since $\mathrm{Aut}(\overline{\phi})$ is isomorphic to either μ_{q-1} or μ_{q^2-1} by Lemma 2.1. □

Corollary 5.5. *Assume q is even and let $\mathfrak{p}$ be a maximal ideal of degree four. Then the order of $\mathrm{Aut}(X_0(\mathfrak{p})_{\overline{K}})$ (the automorphism group of the Drinfeld modular curve $X_0(\mathfrak{p})_{\overline{K}}$) is two.*

Proof. In the proof of [11, Corollary 1.7], it is proved that the order of $\mathrm{Aut}_{\overline{K}}(X_0(\mathfrak{p}))$ is two if q is even and $Y_0(\mathfrak{p})(K)$ is empty (See the paragraph above [11, Remark 9.6]). Hence the assertion follows. □

Lastly, let us add some observations when $\deg(\mathfrak{p})$ is equal to three. Let (ϕ, C) be a pair of a Drinfeld A-module of rank two and a cyclic $\mathfrak{p}$-torsion subgroup defined over K. By Proposition 5.1 and Proposition 5.2, ϕ has potentially good reduction at every finite place of K. Let k be an element of $\mathbb{Z}/(q^3-1)\mathbb{Z}$ which is associated to the isogeny character of (ϕ, C) as is defined in section 3. By Lemma 3.6, k mod q^2+q+1 is equal to $\frac{x}{q+1}$ for some x with $0 \leq x \leq q+1$.

For each maximal ideal $\mathfrak{l}$ of degree one with monic generator g, we know that there exists $(a, b) \in \mathbb{F}_q^* \times \mathbb{F}_q$ such that $g^k + ag^{1-k} \equiv b \bmod \mathfrak{p}$, by taking the trace of the Frobenius at $\mathfrak{l}$ as in the previous section. Since the underlined condition is still true after we replace k with any element of $\mathbb{Z}/(q^3-1)\mathbb{Z}$ which is congruent to k modulo q^2+q+1, we may take k to be $\frac{q^4-1}{q^2-1}x = (q^2+1)x$. Then it is easy to observe that the underlined condition is equivalent to the condition that there exists $(a, b) \in \mathbb{F}_q \times \mathbb{F}_q^*$ such that $g^{2x+q^2} + ag^x + b \equiv 0 \bmod \mathfrak{p}$. Note that, if x is equal to $\frac{q+1}{2}$, then the condition is trivially true for $a = 0$ and some $b \in \mathbb{F}_q^*$ since $2x + q^2 = q^2 + q + 1$. We conjecture that this is the only case such that the underlined condition holds for every $\mathfrak{l}$:

Conjecture 5.6. *Suppose that q is odd. Let $\mathfrak{p}$ be a maximal ideal of A of degree three and x an integer with $0 \leq x \leq q+1$. Suppose that, for every maximal ideal $\mathfrak{l}$ of A of degree one with monic generator g, there exists $(a, b) \in \mathbb{F}_q \times \mathbb{F}_q^*$ such that $g^{2x+q^2} + ag^x + b \equiv 0$ mod $\mathfrak{p}$. Then x is equal to $\frac{q+1}{2}$.*

This conjecture has the following consequence:

Proposition 5.7. *Suppose q is odd and greater than three. Let $\mathfrak{p}$ be a maximal ideal of A of degree three. If Conjecture 5.6 is true, then no Drinfeld A-module of rank two over K has a $\mathfrak{p}$-isogeny defined over K. Moreover, then the set of K-rational points of the Drinfeld modular curve $Y_0(\mathfrak{p})$ is empty.*

Proof. Suppose that there exists a pair (ϕ, C) of a Drinfeld A-module of rank two defined over K and a cyclic $\mathfrak{p}$-torsion subgroup defined over K. If Conjectue 5.6 is true, it holds that $k \equiv \frac{1}{2} \bmod \frac{q^3-1}{q-1}$. However this contradicts Theorem 4.6. The rest of the assertion follows from Lemma 5.4. □

We confirmed that Conjecture 5.6 is true for odd primes $q = p \leq 181$, with the help of SageMath. However, at the writing of this paper, the author does not know how to prove this conjecture in general.

References

[1] Cécile Armana. Torsion des modules de Drinfeld de rang 2 et formes modulaires de Drinfeld. *Algebra & Number Theory*, 6(6):1239–1288, 2012.

[2] Pete L. Clark and Xavier Xarles. Local bounds for torsion points on abelian varieties. *Canad. J. Math.*, 60(3):532–555, 2008.

[3] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 143–316. Lecture Notes in Math., Vol. 349, 1973.

[4] Ernst-Ulrich Gekeler. Über Drinfeldsche Modulkurven vom Hecke-Typ. *Compositio Math.*, 57(2):219–236, 1986.

[5] Ernst-Ulrich Gekeler. On finite Drinfeld modules. *J. Algebra*, 141(1):187–203, 1991.

[6] Ernst-Ulrich Gekeler. Frobenius distributions of Drinfeld modules over finite fields. *Trans. Amer. Math. Soc.*, 360(4):1695–1721, 2008.

[7] David Goss. *Basic structures of function field arithmetic*, volume 35 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1996.

[8] D. R. Hayes. Explicit class field theory for rational function fields. *Trans. Amer. Math. Soc.*, 189:77–91, 1974.

[9] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[10] Ambrus Pál. On the torsion of the Mordell-Weil group of the Jacobian of Drinfeld modular curves. *Doc. Math.*, 10:131–198, 2005.

[11] Ambrus Pál. On the torsion of Drinfeld modules of rank two. *J. Reine Angew. Math.*, 640:1–45, 2010.

[12] Michel Raynaud. Schémas en groupes de type $(p, \ldots, p)$. *Bull. Soc. Math. France*, 102:241–280, 1974.

[13] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[14] Andreas Schweizer. On the uniform boundedness conjecture for Drinfeld modules. *Math. Z.*, 244(3):601–614, 2003.

[15] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[16] Jean-Pierre Serre. *Trees*. Springer-Verlag, Berlin-New York, 1980. Translated from the French by John Stillwell.

[17] Gert-Jan van der Heiden. Weil pairing for Drinfeld modules. *Monatsh. Math.*, 143(2):115–143, 2004.

Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606-8502, Japan

Email address: ishii@kurims.kyoto-u.ac.jp