DRINFELD-STUHLER MODULES AND THE HASSE PRINCIPLE

KEISUKE ARAI, SATOSHI KONDO, AND MIHRAN PAPIKIAN

ABSTRACT. We develop a theory of canonical isogeny characters of Drinfeld-Stuhler modules similar to the theory of canonical isogeny characters of abelian surfaces with quaternionic multiplication. We then apply this theory to give explicit criteria for the non-existence of rational points on Drinfeld-Stuhler modular varieties over finite extensions of $\mathbb{F}_q(T)$. This allows us to produce explicit examples of Drinfeld-Stuhler curves violating the Hasse principle.

1. INTRODUCTION

Drinfeld-Shutler modules are function field analogues of abelian surfaces equipped with an action of an indefinite quaternion algebra over $\mathbb{Q}$. The idea of these objects was proposed in the language of shtukas by Ulrich Stuhler under the name of *$\mathscr{D}$-elliptic sheaf* as a natural generalization of Drinfeld modules. The modular varieties of $\mathscr{D}$-elliptic sheaves were studied by Laumon, Rapoport and Stuhler in [18], with the aim of proving the local Langlands correspondence for $\mathrm{GL}(n)$ in positive characteristic.

Over the years, the third author of this paper has studied the arithmetic properties of $\mathscr{D}$-elliptic sheaves and their modular varieties, trying to extend to this setting the rich theory of abelian surfaces with quaternionic multiplication and Shimura curves; see, for example, [21], [22], [23], [24]. The current paper is a natural continuation of [24].

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a power of a prime number. Let $A = \mathbb{F}_q[T]$ be the ring of polynomials in indeterminate T with coefficients in $\mathbb{F}_q$, and $F = \mathbb{F}_q(T)$ be the field of fractions of A. Let $d \geq 2$ be an integer and D be a central division algebra over F of dimension d^2, which is split at $1/T$. Fix a maximal A-order O_D in D. The modular variety of Drinfeld-Stuhler O_D-modules X^D is a projective geometrically connected variety of dimension $d-1$ defined over F.

This paper has three main objectives:

(1) Develop a theory of canonical isogeny characters of Drinfeld-Stuhler modules similar to the theory of canonical isogeny characters of abelian surfaces with quaternionic multiplication given in [13].
(2) Apply (1) to give explicit criteria for the non-existence of rational points on X^D over finite extensions of F.
(3) Combine (2) with the results in [23] to produce explicit examples of Drinfeld-Stuhler curves violating the Hasse principle.

The major inspiration for this paper has been the work of Bruce Jordan in [13] (which itself was inspired by the work of Mazur [19]). One significant difference between our work and [13]

2010 *Mathematics Subject Classification.* 11G09, 11R52.
Key words and phrases. Drinfeld-Stuhler modules; $\mathscr{D}$-elliptic sheaves; Hasse principle; canonical isogeny character.

is that we are able to carry out (1) and (2) for arbitrary $d \geq 2$, not just quaternion algebras and curves. In principle, (3) also can be extended to the higher dimensional Drinfeld-Stuhler varieties once the results in [23] are extended to these higher dimensional varieties. We also mention that the results of Jordan in [13] have been generalized in the case of Shimura curves by the first author in [2], [3].

Next we give a more detailed description of the results in this paper. Let K be a field equipped with an A-algebra structure $\gamma\colon A \to K$. Note that $\mathbb{F}_q$ is a subfield of K. Let τ be the $\mathbb{F}_q$-linear Frobenius endomorphism of the additive group-scheme $\mathbb{G}_{a,K} = \mathrm{Spec}(K[x])$ over K; the morphism τ is given on the underlying ring by $x \mapsto x^q$. The ring of $\mathbb{F}_q$-linear endomorphisms $\mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,K})$ is canonically isomorphic to the skew polynomial ring $K[\tau]$ with the commutation relation $\tau\alpha = \alpha^q\tau$, $\alpha \in K$. Given a unitary ring R, let $M_d(R)$ denote the ring of $d \times d$ matrices with entries from R. A Drinfeld-Stuhler O_D-module over K is a homomorphism of $\mathbb{F}_q$-algebras

$$\phi : O_D \longrightarrow \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,K}^d) \cong M_d(K[\tau]), \qquad b \longmapsto \phi_b,$$

such that:

(i) For any nonzero $b \in O_D$, the kernel of ϕ_b as an endomorphism of $\mathbb{G}_{a,K}^d$ is a finite group scheme of order $\#O_D/O_Db$;
(ii) For any $a \in A$, substituting 0 for τ in ϕ_a one obtains the scalar matrix $\gamma(a)I_d$.

Assume $\mathfrak{p}$ is a prime of A such that the Hasse invariant $\mathrm{inv}_\mathfrak{p}(D)$ of D at $\mathfrak{p}$ is $1/d$. Denote $\mathbb{F}_\mathfrak{p} = A/\mathfrak{p}$ and let $\mathbb{F}_\mathfrak{p}^{(d)}$ be the degree d extension of the finite field $\mathbb{F}_\mathfrak{p}$. Let ϕ be a Drinfeld-Stuhler O_D-module over K. Assume $\mathfrak{p} \neq \ker(\gamma)$. In Section 4, we show that $\ker \phi_\mathfrak{p} \cong O_D/\mathfrak{p}$ has a canonical subgroup $\mathcal{C}_{\phi,\mathfrak{p}} \cong \mathbb{F}_\mathfrak{p}^{(d)}$ which is O_D-invariant and rational over K. Following the terminology in [13], we call the associated Galois representation

$$\varrho_{\phi,\mathfrak{p}} : \mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{Aut}_{O_D}(\mathcal{C}_{\phi,\mathfrak{p}}) \approx (\mathbb{F}_\mathfrak{p}^{(d)})^\times$$

a *canonical isogeny character* of ϕ at $\mathfrak{p}$. We then study the properties of $\varrho_{\phi,\mathfrak{p}}$. To prove some of these properties, one needs to know that Drinfeld-Stuhler modules have potentially good reduction over local fields. This foundational result is proved in [18] in the language of $\mathscr{D}$-elliptic sheaves; in Section 3 we give a more precise information about the extension over which a Drinfeld-Stuhler module acquires good reduction.

Now let K be a degree d extension of F which splits D, i.e., $D \otimes_F K \cong M_d(K)$. Assume there is a Drinfeld-Stuhler O_D-module ϕ defined over K. The canonical isogeny character of ϕ forces the coefficients of the characteristic polynomials of the Frobenius automorphisms acting on a Tate module of ϕ to satisfy certain congruences modulo $\mathfrak{p}$ (this is proved in Section 5). We use this information in Section 6 to show that if certain explicit conditions are satisfied, then the Drinfeld-Stuhler variety X^D has no K-rational points. These conditions are listed in Theorems 6.6 and 6.9, which are the main results of this paper. A technical issue arises here from the fact that X^D is only a coarse moduli scheme, so the K-rational points on X^D may not be represented by Drinfeld-Stuhler O_D-modules defined over K. Fortunately, a result from [24] partly resolves this: Assume $X^D(K) \neq \emptyset$. Then there is a Drinfeld-Stuhler O_D-module defined over K if and only if K splits D.

Remark 1.1. Let K be a degree d extension of F which splits D. Assume there is a unique place $\widetilde{\infty}$ of K over $\infty = 1/T$. Let H_K be the maximal unramified abelian extension of K in which $\widetilde{\infty}$ splits completely (i.e., H_K is the Hilbert class field of K). The Galois group $\mathrm{Gal}(H_K/K)$ is isomorphic to the class group of the integral closure B of A in K. By developing a theory of "complex multiplication" for Drinfeld-Stuhler modules, the third author has shown that $X^D(H_K) \neq \emptyset$; see [24, Thm. 4.10]. In particular, if B is a principal ideal domain, then $X^D(K) \neq \emptyset$.

In Section 7, we assume that $d = 2$, so X^D is a curve. The paper [23] contains comprehensive results about the existence of rational points on X^D over finite extensions of completions of F. We combine these results with the results of Section 6 to construct explicit examples of pairs (X^D, K), such that

(i) $[K : F] = 2$,
(ii) $X^D(K) = \emptyset$,
(iii) $X^D(K_v) \neq \emptyset$ for all places v of K, where K_v denotes the completion of K at v.

In other words, X^D violates the Hasse principle over K. Part of the calculations required for checking that the conditions of [23], as well as the conditions of Theorem 6.9, are satisfied for a given pair (X^D, K) were performed on a computer using the program `Magma`. One such example is the following:

Example 1.2. Let $q = 3$ and D be the quaternion algebra over F ramified at two primes $\{\mathfrak{p}, \mathfrak{q}\}$ of A, and unramified at all other places of F. Let $K = F(\sqrt{\mathfrak{d}})$. The Hasse principle is violated for the following choices: $\mathfrak{p} = T^2 + T + 2$, $\mathfrak{q} = T^2 + 1$, $\mathfrak{d} = T\mathfrak{p}\mathfrak{q}$.

Remark 1.3. We should mention the following relevant result:

Assume D is a quaternion division algebra whose discriminant has degree ≥ 20. Then there are infinitely many quadratic extensions K/F such that X^D violates the Hasse principle over K.

This is proved in [23] by adapting a method of Clark [5] to the function field setting, but this method does not give an effective procedure for finding the field extensions K/F over which X^D violates the Hasse principle.

2. Notation and terminology

We start by fixing the notation that will be used throughout the paper. As in the introduction, $\mathbb{F}_q$ will denote a finite field with q elements, $A = \mathbb{F}_q[T]$ the polynomial ring, and $F = \mathbb{F}_q(T)$ the field of fractions of A. For a nonzero ideal $\mathfrak{n} \lhd A$, by abuse of notation, we denote by the same symbol the unique monic polynomial in A generating $\mathfrak{n}$. (It will always be specified or clear from the context whether $\mathfrak{n}$ denotes the ideal or its monic generator.) We define

$$|\mathfrak{n}| = \#(A/\mathfrak{n}). \tag{2.1}$$

We will call a nonzero prime ideal of A simply a *prime* of A. Given a prime $\mathfrak{p}$ of A, we denote by $A_\mathfrak{p}$ (resp. $F_\mathfrak{p}$) the completion of A at $\mathfrak{p}$ (resp. the field of fractions of $A_\mathfrak{p}$). We denote by $\mathbb{F}_\mathfrak{p} = A/\mathfrak{p}$ the residue field of $A_\mathfrak{p}$, and by $\mathbb{F}_\mathfrak{p}^{(m)}$ the extension of $\mathbb{F}_\mathfrak{p}$ of degree $m \geq 1$.

The degree $\deg(a)$ of $0 \neq a \in A$ is its degree as a polynomial in T. The degree function extends to a valuation of F. The corresponding place of F is called the *place at infinity*, and denoted by ∞. The normalized absolute value on F at ∞ is given by

$$|a| = q^{\deg(a)} \quad \text{for } 0 \neq a \in A.$$

Note that the normalized absolute value at ∞ is closely related with (2.1) via $|a| = |(a)|$, where (a) denotes the ideal of A generated by a. Since $1/T$ is a uniformizer at ∞, the completion F_∞ of F at ∞ is isomorphic to $\mathbb{F}_q(\!(1/T)\!)$. We identify the places of F not equivalent to ∞ with the primes of A.

Let D be a central simple algebra over F of dimension d^2 such that $D \otimes F_\infty \cong M_d(F_\infty)$. Let $\mathrm{Ram}(D)$ be the set of primes of A which ramify in D, i.e., $\mathfrak{p} \in \mathrm{Ram}(D)$ if and only if $D_\mathfrak{p} := D \otimes_F F_\mathfrak{p}$ is not isomorphic to $M_d(F_\mathfrak{p})$. Fix a maximal A-order O_D in D; see [26] for the definitions. Note that A is the center of O_D. Because A is a principal ideal domain and D is split at ∞, any two maximal A-orders are conjugate in D; see [26, §34].

Given a field K we denote by $\overline{K}$ (resp. K^{sep}) its algebraic (resp. separable) closure, and put $\mathrm{G}_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$.

Let K be a field equipped with an A-algebra structure $\gamma\colon A \to K$. The A-characteristic of K is $\mathrm{char}_A(K) := \ker(\gamma) \lhd A$. We will always implicitly consider F, and its extensions, as A-fields via the natural injective homomorphism of A into its field of fractions.

Let $K[\tau]$ be the skew polynomial ring with the commutation relation $\tau\alpha = \alpha^q\tau$, $\alpha \in K$. One can write the elements of $M_d(K[\tau])$ as finite sums $\sum_{i\geq 0} B_i\tau^i$, where $B_i \in M_d(K)$. Using this, we define a homomorphism

$$\begin{aligned} \partial\colon M_d(K[\tau]) &\longrightarrow M_d(K) \\ \sum_{i\geq 0} B_i\tau^i &\longmapsto B_0. \end{aligned} \tag{2.2}$$

A *Drinfeld-Stuhler O_D-module* defined over K is an injective $\mathbb{F}_q$-algebra homomorphism

$$\begin{aligned} \phi : O_D &\longrightarrow \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,K}^d) \cong M_d(K[\tau]) \\ b &\longmapsto \phi_b \end{aligned}$$

satisfying the following conditions:

(i) For any $b \in O_D \cap D^\times$, the kernel $\phi[b]$ of the endomorphism ϕ_b of $\mathbb{G}_{a,K}^d$ is a finite group scheme over K of order $\#(O_D/O_D \cdot b)$.

(ii) The composition

$$A \longrightarrow O_D \xrightarrow{\phi} M_d(K[\tau]) \xrightarrow{\partial} M_d(K)$$

maps $a \in A$ to the scalar matrix $\gamma(a)I_d$, where I_d denotes the $d \times d$ identity matirx.

A *morphism* $u\colon \phi \to \psi$ between two Drinfeld-Stuhler O_D-modules over K is $u \in M_d(K[\tau])$ such that $u\phi_b = \psi_b u$ for all $b \in O_D$. A morphism u is an *isomorphism* if u is invertible in the ring $M_d(K[\tau])$. The set of morphisms $\phi \to \psi$ over K is an A-module $\mathrm{Hom}_K(\phi, \psi)$, where A acts by $a \circ u := u\phi_a$. It can be shown that the kernel of any nonzero morphism u is a finite group scheme over K (i.e., a nonzero morphism is an isogeny), and $\mathrm{Hom}_K(\phi, \psi)$ is a free A-module of rank $\leq d^2$; cf. [24]. We denote $\mathrm{End}_K(\phi) = \mathrm{Hom}_K(\phi, \phi)$ and $\mathrm{Aut}_K(\phi) = \mathrm{End}_K(\phi)^\times$.

Let $\mathfrak{p}$ be a prime of A. The $\mathfrak{p}$-adic Tate module of ϕ is

$$T_{\mathfrak{p}}(\phi) = \varprojlim_{n} \phi[\mathfrak{p}^n](K^{\mathrm{sep}}).$$

$T_{\mathfrak{p}}(\phi)$ is a free $A_{\mathfrak{p}}$-module of rank $\leq d^2$; cf. [1]. Moreover, if $\mathfrak{p} \neq \mathrm{char}_A(K)$, from [24, Lem. 2.10], one deduces an isomorphism

$$T_{\mathfrak{p}}(\phi) \cong O_D \otimes_A A_{\mathfrak{p}} \tag{2.3}$$

of left O_D-modules.

Example 2.1. In the special case when $D = M_d(F)$ and $O_D = M_d(A)$, Drinfeld-Stuhler modules can be obtained from Drinfeld modules by the following construction. Let

$$\Phi\colon A \longrightarrow K[\tau], \quad a \longmapsto \Phi_a,$$

be a Drinfeld A-module over L of rank d. Such a module is uniquely determined by the image of T:

$$\Phi_T = \gamma(T) + g_1\tau + \cdots + g_d\tau^d, \quad g_d \neq 0.$$

Define

$$\begin{aligned} \phi\colon O_D &\longrightarrow M_d(K[\tau]) \\ (a_{ij}) &\longmapsto \left(\Phi_{a_{ij}}\right). \end{aligned}$$

It is easy to check that ϕ is a Drinfeld-Stuhler module. In fact, every Drinfeld-Stuhler $M_d(A)$-module arises from some Drinfeld module Φ via this construction. This is a consequence of the Morita equivalence for Drinfeld-Stuhler modules; see [24, §2.4] for the details.

3. Potentially good reduction property

Let K be a local field of positive characteristic, complete with respect to a discrete valuation v. Let R be the ring of integers of K, π a uniformizer of K, and $k = R/(\pi)$ the residue field. Assume $\gamma\colon A \to R$ is an injective homomorphism. Extending this homomorphism to $\gamma\colon A \to K$, we consider K as an A-field with $\mathrm{char}_A(K) = 0$. (A typical case is when K is a finite extension of the completion $F_{\mathfrak{p}}$ of F at a prime $\mathfrak{p} \lhd A$ and $A \hookrightarrow A_{\mathfrak{p}} \hookrightarrow R$ are the natural embeddings.)

In this section, we discuss an analogue for Drinfeld-Stuhler modules of a well-known fact that abelian surfaces with quaternionic multiplication have potentially good reduction over local fields; cf. [13, §3]. Initially we will work in the category of $\mathscr{D}$-elliptic sheaves and then explain the connection to Drinfeld-Stuhler modules.

First, we briefly recall the concept of a $\mathscr{D}$-elliptic sheaf. Let $C := \mathbb{P}^1_{\mathbb{F}_q}$. Fix a maximal $\mathcal{O}_C$-order $\mathscr{D}$ in D such that $H^0(C \setminus \infty, \mathscr{D}) = O_D$. Let S be an $\mathbb{F}_q$-scheme. Let Frob_S be its Frobenius morphism, which is the identity on the points and the q-th power map on the functions. A $\mathscr{D}$-elliptic sheaf over S is a sequence $(\mathcal{E}_i, j_i, t_i)_{i\in\mathbb{Z}}$, where each $\mathcal{E}_i$ is a locally free $\mathcal{O}_{C\times_{\mathbb{F}_q}S}$-module of rank d^2 equipped with a right action of $\mathscr{D}$ extending the action of $\mathcal{O}_C$, and $j_i\colon \mathcal{E}_i \to \mathcal{E}_{i+1}$, $t_i\colon (\mathrm{id}_C \otimes \mathrm{Frob}_S)^*\mathcal{E}_i \to \mathcal{E}_{i+1}$ are injective $\mathscr{D}$-linear homomorphisms satisfying certain conditions. We refer to [18, §2] for the precise definition. A morphism

$f\colon (\mathcal{E}_i, j_i, t_i)_{i\in\mathbb{Z}} \to (\mathcal{E}'_i, j'_i, t'_i)_{i\in\mathbb{Z}}$ between two $\mathscr{D}$-elliptic sheaves is a sequence of sheaf morphisms $f_i\colon \mathcal{E}_i \to \mathcal{E}'_{i+n}$ for some fixed $n \in \mathbb{Z}$, which are compatible with the action of $\mathscr{D}$ and the morphisms j_i, t_i; cf. [24, p. 13].

Definition 3.1. Let $\mathbb{E} = (\mathcal{E}_i, j_i, t_i)_{i\in\mathbb{Z}}$ be a $\mathscr{D}$-elliptic sheaf over K. We say that $\mathbb{E}$ has *good reduction* if there is a $\mathscr{D}$-elliptic sheaf over R whose restriction to K is isomorphic to $\mathbb{E}$.

Let $\mathbb{E} = (\mathcal{E}_i, j_i, t_i)_{i\in\mathbb{Z}}$ be a $\mathscr{D}$-elliptic sheaf over K (resp. R). Then $M := \mathcal{E}_i|_{C^0}$, the restriction of $\mathcal{E}_i$ to C^0, is independent of i and is equipped with an $(\mathrm{id}_F \otimes \mathrm{Frob}_K)$-linear (resp. $(\mathrm{id}_F \otimes \mathrm{Frob}_R)$-linear) endomorphism φ; see [18, (6.5)]. The pair (M, φ) is a *τ-sheaf* over K (resp. R) in the sense of [7, 1.1]. This construction gives functors $\mathcal{F}_K$ and $\mathcal{F}_R$, and a commutative diagram

$$\begin{array}{ccc} (\mathscr{D}\text{-elliptic sheaves over } R) & \xrightarrow{\mathcal{F}_R} & (\tau\text{-sheaves over } R) \\ \Big\downarrow{\scriptstyle \mathrm{res}} & & \Big\downarrow{\scriptstyle \mathrm{res}} \\ (\mathscr{D}\text{-elliptic sheaves over } K) & \xrightarrow{\mathcal{F}_K} & (\tau\text{-sheaves over } K), \end{array}$$

where the vertical arrows are restrictions. It is easy to see that the functors $\mathcal{F}_K$ and $\mathcal{F}_R$ are faithful. Moreover, one can check that the functors $\mathcal{F}_K$ and $\mathcal{F}_R$ are full by checking the construction in [18, (6.7)] (see also [4, Rem. 3.2.4]).

Lemma 3.2. *Let $\tilde{\mathbb{E}}$ be a $\mathscr{D}$-elliptic sheaf over R and set $\mathbb{E} = \mathrm{res}(\tilde{\mathbb{E}})$. A morphism $f\colon \mathbb{E} \to \mathbb{E}$ uniquely extends to a morphism $\tilde{f}\colon \tilde{\mathbb{E}} \to \tilde{\mathbb{E}}$.*

Proof. For simplicity denote $M = \mathcal{F}_K(\mathbb{E})$ and $\mathcal{M} = \mathcal{F}_R(\tilde{\mathbb{E}})$. Then $\mathrm{res}(\mathcal{M}) = M$. Note that M has a good model (namely $\mathcal{M}$) in the sense of [7, p. 448]. We have a morphism $\mathcal{F}_K(f)\colon M \to M$. By Definition 2.3 and Proposition 2.13(ii) of [8], there exists a unique morphism $g\colon \mathcal{M} \to \mathcal{M}$ such that $\mathrm{res}(g) = \mathcal{F}_K(f)$. By the fullness of $\mathcal{F}_R$, there exists $\tilde{f}\colon \tilde{\mathbb{E}} \to \tilde{\mathbb{E}}$ such that $\mathcal{F}_R(\tilde{f}) = g$. Moreover, $\tilde{f}$ is unique by the faithfulness of $\mathcal{F}_R$. □

Let $\mathfrak{l} \lhd A$ be a prime different from $\ker(A \xrightarrow{\gamma} R \to k)$.

Lemma 3.3. *Let $\mathbb{E}$ be a $\mathscr{D}$-elliptic sheaves over K and $M := \mathcal{F}_K(\mathbb{E})$. The Tate module $T_{\mathfrak{l}}(M)$ of M is unramified if and only if $\mathbb{E}$ has good reduction.*

Proof. For the definition of the Tate module $T_{\mathfrak{l}}(M)$ of M we refer to [7]. By [7, Thm. 1.1], $T_{\mathfrak{l}}(M)$ is unramified if and only if there is a τ-sheaf $\mathcal{M}$ over R such that $\mathrm{res}(\mathcal{M}) = M$. The $\mathscr{D}$-elliptic sheaf over R which extends $\mathbb{E}$ is the $\mathscr{D}$-elliptic sheaf $\tilde{\mathbb{E}}$ such that $\mathcal{F}_R(\tilde{\mathbb{E}}) = \mathcal{M}$. □

Proposition 3.4. *Assume D is a central division algebra and $\mathbb{E}$ is a $\mathscr{D}$-elliptic sheaf over K. Then there exists a totally tamely ramified extension of K of degree dividing $q^d - 1$ over which $\mathbb{E}$ has good reduction.*

Proof. In [18, §6], using a result of Drinfeld, the authors prove that $\mathbb{E}$ acquires good reduction over some finite extension L of K. Moreover, looking more carefully at the proof of Drinfeld's result, one sees that the extension L/K can be taken to be any extension whose ramification index is divisible by a certain implicit integer depending on $\mathbb{E}$; see the proof of Lemma 3 in [16]. Therefore, by choosing an appropriate Eisenstein polynomial, we may assume that L/K is Galois.

Now we proceed similarly to the proof of [13, Prop. 3.2]. Let R_L be the ring of integers of L and let l be the residue field of R_L. Let $\tilde{\mathbb{E}}$ be the extension of $\mathbb{E} \otimes_K L$ over R_L. Let $I \subseteq \mathrm{Gal}(L/K)$ be the inertia group. Then $\sigma \in I$ induces a morphism $\mathbb{E} \otimes_K L \to \mathbb{E} \otimes_K L$ of $\mathscr{D}$-elliptic sheaves via its action on L. By Lemma 3.2, this morphism uniquely extends to a morphism $\tilde{\sigma} : \tilde{\mathbb{E}} \to \tilde{\mathbb{E}}$. Then $\tilde{\sigma}$ acts on the closed fibre $\tilde{\mathbb{E}} \otimes l$ of $\tilde{\mathbb{E}}$. Since σ acts trivially on l, $\tilde{\sigma}$ is an l-automorphism of $\tilde{\mathbb{E}} \otimes l$. There are canonical isomorphisms $T_{\mathfrak{l}}(\mathcal{F}_K(\mathbb{E})) \cong T_{\mathfrak{l}}(\mathcal{F}_L(\mathbb{E} \otimes L)) \cong T_{\mathfrak{l}}(\mathcal{F}_l(\tilde{\mathbb{E}} \otimes l))$. Hence the action of I on $T_{\mathfrak{l}}(\mathcal{F}_K(\mathbb{E}))$ factors through the group of l-automorphisms of $\tilde{\mathbb{E}} \otimes l$. By Theorems 3.2 and 3.4 in [24], there is a Drinfeld-Stuhler module ϕ functorially associated to $\tilde{\mathbb{E}} \otimes l$, so the action of I on $T_{\mathfrak{l}}(\mathcal{F}_K(\mathbb{E}))$ factors through $\mathrm{Aut}_l(\phi)$. Let N be the kernel of $I \to \mathrm{Aut}_l(\phi)$. By [24, Thm. 4.1 (4)], $\mathrm{Aut}_l(\phi) \cong \mathbb{F}_{q^s}$ for some s dividing d. Hence, $\#(I/N)$ divides $q^d - 1$.

Let $\theta \in \mathrm{Gal}(L/K)$ be a Frobenius element, i.e., an element which generates $\mathrm{Gal}(l/k)$ under the quotient map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(l/k)$. Let $\Gamma \subset \mathrm{Gal}(L/K)$ be the subgroup generated by N and θ. Let L' be the subfield of L fixed by Γ. Then L'/K is a totally tamely ramified extension with ramification index dividing $q^d - 1$. The action of the inertia subgroup of G_L on $T_{\mathfrak{l}}(\mathcal{F}_L(\mathbb{E} \otimes L))$ is trivial by Lemma 3.3, so the action of the inertia subgroup of $\mathrm{G}_{L'}$ on $T_{\mathfrak{l}}(\mathcal{F}_{L'}(\mathbb{E} \otimes L'))$ is also trivial. Now, using Lemma 3.3 again, we conclude that $\mathbb{E}$ has good reduction over L'. □

The group $\mathbb{Z}$ acts freely on the objects of the category of $\mathscr{D}$-elliptic sheaves by shifting indices, i.e., $n \in \mathbb{Z}$ acts by $n(\mathcal{E}_i, j_i, t_i) = (\mathcal{E}'_i, j'_i, t'_i)$, where $\mathcal{E}'_i = \mathcal{E}_{i+n}$, $j'_i = j_{i+n}$, $t'_i = t_{i+n}$. The quotient of the category of $\mathscr{D}$-elliptic sheaves over a field by this action is equaivalent to the category of Drinfeld-Stuhler O_D-modules over the same field; cf. [24, §3]. (Note that we have used this fact in the proof of Proposition 3.4.)

Definition 3.5. Let ϕ be a Drinfeld-Stuhler O_D-module over K. We will say that ϕ has *good reduction over* K if its corresponding $\mathscr{D}$-elliptic sheaf $\mathbb{E}$ has good reduction over K. In that case, the Drinfeld-Stuhler O_D-module $\bar{\phi}$ over k corresponding to $\tilde{\mathbb{E}} \otimes k$ will be called the *reduction of* ϕ.

Theorem 3.6. *Assume D is a central division algebra and ϕ is a Drinfeld-Stuhler O_D-module over K. There is a totally tamely ramified extension L/K of degree dividing $q^d - 1$ over which ϕ has good reduction. Moreover, the inertia subgroup of G_L acts trivially on $T_{\mathfrak{l}}(\phi)$.*

Proof. This follows from Lemma 3.3 and Proposition 3.4. □

4. Canonical isogeny characters

Let $\mathfrak{p} \in \mathrm{Ram}(D)$. In this section we assume that $D_{\mathfrak{p}} := D \otimes_F F_{\mathfrak{p}}$ is a division algebra with Hasse invariant $\mathrm{inv}_{\mathfrak{p}}(D) = 1/d$.

We start by examining the reduction of O_D modulo $\mathfrak{p}$. Note that

$$O_D \otimes_A \mathbb{F}_{\mathfrak{p}} = (O_D \otimes_A A_{\mathfrak{p}}) \otimes_{A_{\mathfrak{p}}} \mathbb{F}_{\mathfrak{p}}.$$

Since $\mathcal{D}_{\mathfrak{p}} := O_D \otimes_A A_{\mathfrak{p}}$ is a maximal order in the central division algebra $D_{\mathfrak{p}}$ over $F_{\mathfrak{p}}$, it can be explicitly described as follows (cf. [17, Appendix A]): Let $\mathbb{F}_{\mathfrak{p}}^{(d)}$ be the degree d extension of $\mathbb{F}_{\mathfrak{p}}$. Let $F_{\mathfrak{p}}^{(d)} = \mathbb{F}_{\mathfrak{p}}^{(d)} F_{\mathfrak{p}}$ be the unramified extension of $F_{\mathfrak{p}}$ of degree d and $A_{\mathfrak{p}}^{(d)}$ be the ring of integers of $F_{\mathfrak{p}}^{(d)}$. Let $\sigma \in \mathrm{Gal}(F_{\mathfrak{p}}^{(d)}/F_{\mathfrak{p}})$ be the lifting of the Frobenius automorphism $\alpha \mapsto \alpha^{|\mathfrak{p}|}$ in $\mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}^{(d)}/\mathbb{F}_{\mathfrak{p}})$. By [26, §14],

$$D_{\mathfrak{p}} \cong F_{\mathfrak{p}}^{(d)}[\Pi]/(\Pi^d - \mathfrak{p}),$$

where $F_{\mathfrak{p}}^{(d)}[\Pi]$ is the non-commutative polynomial ring in Π over $F_{\mathfrak{p}}^{(d)}$ with commutation rule

$$\Pi\alpha = \sigma(\alpha)\Pi, \qquad \alpha \in F_{\mathfrak{p}}^{(d)}.$$

The maximal order of $D_{\mathfrak{p}}$ is

$$\mathcal{D}_{\mathfrak{p}} = A_{\mathfrak{p}}^{(d)}[\Pi]/(\Pi^d - \mathfrak{p})$$

and $\Pi\mathcal{D}_{\mathfrak{p}} = \mathcal{D}_{\mathfrak{p}}\Pi$ is the maximal ideal of $\mathcal{D}_{\mathfrak{p}}$. To make this description even more explicit, note that $A_{\mathfrak{p}}^{(d)}$ may be identified with the ring $\mathbb{F}_{\mathfrak{p}}^{(d)}[\![\mathfrak{p}]\!]$ of formal series with coefficients in $\mathbb{F}_{\mathfrak{p}}^{(d)}$, where we consider $\mathfrak{p}$ as a uniformizer of $F_{\mathfrak{p}}$; cf. [29, §II.4]. From this description we obtain

$$\begin{aligned} O_D/\mathfrak{p}O_D &\cong \mathcal{D}_{\mathfrak{p}}/\mathfrak{p}\mathcal{D}_{\mathfrak{p}} \\ &\cong \mathbb{F}_{\mathfrak{p}}^{(d)}[\Pi]/\Pi^d \\ &\cong \mathbb{F}_{\mathfrak{p}}^{(d)} \oplus \mathbb{F}_{\mathfrak{p}}^{(d)}\Pi \oplus \cdots \oplus \mathbb{F}_{\mathfrak{p}}^{(d)}\Pi^{d-1}, \quad \Pi^d = 0, \quad \Pi\alpha = \alpha^{|\mathfrak{p}|}\Pi. \end{aligned} \tag{4.1}$$

Now let K be an A-field $\gamma\colon A \to K$ such that $\mathrm{char}_A(K) \neq \mathfrak{p}$. Let ϕ be a Drinfeld-Stuhler O_D-module over K. By [24, Lem. 2.10], we have an isomorphism of left O_D-modules

$$\phi[\mathfrak{p}] \cong O_D/\mathfrak{p}O_D. \tag{4.2}$$

It is easy to see from (4.1) and (4.2) that $\phi[\mathfrak{p}]$ has exactly one O_D-submodule which is a 1-dimensional $\mathbb{F}_{\mathfrak{p}}^{(d)}$-vector space, namely the $\mathbb{F}_{\mathfrak{p}}^{(d)}$-vector space spanned by Π^{d-1}. We shall denote this submodule by $\mathcal{C}_{\phi,\mathfrak{p}}$ and call it the *canonical subgroup* of $\phi[\mathfrak{p}]$. Note that the canonical subgroup can be equivalently described as the kernel of Π acting on $\phi[\mathfrak{p}]$. Since the action of G_K on $\phi[\mathfrak{p}]$ commutes with the action of O_D, the canonical subgroup $\mathcal{C}_{\phi,\mathfrak{p}}$ is rational over K.

The action of G_K on the subgroup $\mathcal{C}_{\phi,\mathfrak{p}}$ yields a character

$$\varrho_{\phi,\mathfrak{p}} : \mathrm{G}_K \longrightarrow \mathrm{Aut}_{O_D}(\mathcal{C}_{\phi,\mathfrak{p}}) \approx (\mathbb{F}_{\mathfrak{p}}^{(d)})^\times.$$

This character depends on an identification $\mathcal{D}_{\mathfrak{p}}/\Pi\mathcal{D}_{\mathfrak{p}} \cong \mathbb{F}_{\mathfrak{p}}^{(d)}$; such identifications differ by automorphisms of $\mathbb{F}_{\mathfrak{p}}^{(d)}$ given by powers of the Frobenius $\alpha \mapsto \alpha^{|\mathfrak{p}|}$.

Definition 4.1. The characters $\varrho_{\phi,\mathfrak{p}}^{|\mathfrak{p}|^i}$, $0 \le i \le d-1$, will be called the *canonical isogeny characters* associated to ϕ at $\mathfrak{p}$.

For the rest of this section we study the properties of canonical isogeny characters. By (4.1) and (4.2), $\phi[\mathfrak{p}]$ is a d-dimensional vector space over $\mathbb{F}_{\mathfrak{p}}^{(d)}$, so from the action of G_K on $\phi[\mathfrak{p}]$ one obtains a representation

$$\pi_{\phi,\mathfrak{p}} : \mathrm{G}_K \longrightarrow \mathrm{Aut}_{O_D}(\phi[\mathfrak{p}]) \subset \mathrm{GL}_d(\mathbb{F}_{\mathfrak{p}}^{(d)}). \tag{4.3}$$

Lemma 4.2. *We have*

$$\det(\pi_{\phi,\mathfrak{p}}) = \varrho_{\phi,\mathfrak{p}}^{1+|\mathfrak{p}|+\cdots+|\mathfrak{p}|^{d-1}} = \mathrm{Nr}_{\mathbb{F}_{\mathfrak{p}}^{(d)}/\mathbb{F}_{\mathfrak{p}}}\left(\varrho_{\phi,\mathfrak{p}}\right).$$

Proof. Fix $\{1, \Pi, \dots, \Pi^{d-1}\}$ as a basis of $O_D/\mathfrak{p}O_D$ considered as an $\mathbb{F}_\mathfrak{p}^{(d)}$-vector space. Let $g \in \mathrm{G}_K$ and

$$g \circ 1 = \alpha_1 + \alpha_2\Pi + \cdots + \alpha_d\Pi^{d-1},$$

where $\alpha_1, \alpha_2, \dots, \alpha_d \in \mathbb{F}_\mathfrak{p}^{(d)}$. Since the action of Π commutes with the action of g, we get

$$g \circ \Pi = \Pi(g \circ 1) = \alpha_1^{|\mathfrak{p}|}\Pi + \alpha_2^{|\mathfrak{p}|}\Pi^2 + \cdots + \alpha_{d-1}^{|\mathfrak{p}|}\Pi^{d-1}.$$

Continuing in this manner, we obtain

$$\pi_{\phi,\mathfrak{p}}(g) = \begin{pmatrix} \alpha_1 & 0 & 0 & \cdots & 0 \\ \alpha_2 & \alpha_1^{|\mathfrak{p}|} & 0 & \cdots & 0 \\ \alpha_3 & \alpha_2^{|\mathfrak{p}|} & \alpha_1^{|\mathfrak{p}|^2} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_d & \alpha_{d-1}^{|\mathfrak{p}|} & \alpha_{d-2}^{|\mathfrak{p}|^2} & \cdots & \alpha_1^{|\mathfrak{p}|^{d-1}} \end{pmatrix}. \tag{4.4}$$

The canonical isogeny characters are the diagonal entries of $\pi_{\phi,\mathfrak{p}}$. Now the claim of the lemma is clear. □

Let $M(\phi)$ be the O_D-motive associated to ϕ; cf. [24, §3]. Recall that $M(\phi)$ is a left $O_D^{\mathrm{opp}} \otimes_{\mathbb{F}_q} K[\tau]$-module, which is a locally free $O_D^{\mathrm{opp}} \otimes_{\mathbb{F}_q} K$-module of rank 1 and a free $K[\tau]$-module of rank d. A construction of Lafforgue [15, p. 26] associates to $M(\phi)$ an A-motive $\det(M(\phi))$ of rank 1 and dimension 1, along with a map $\det : M(\phi) \to \det(M(\phi))$ which on $M(\phi)$ as a locally free $O_D^{\mathrm{opp}} \otimes K$-module of rank 1 is given by the reduced norm on D^{opp}. Anderson's duality [1, Thm. 1] associates to $\det(M(\phi))$ a Drinfeld A-module of rank 1, which we will call the *determinant* of ϕ and denote by $\det(\phi)$. Let

$$\chi_{\phi,\mathfrak{p}} : \mathrm{G}_K \longrightarrow \mathrm{Aut}(\det(\phi)[\mathfrak{p}]) \cong \mathbb{F}_\mathfrak{p}^\times$$

be the character by which G_K acts on the $\mathfrak{p}$-torsion of $\det(\phi)$.

Proposition 4.3. *We have*

$$\chi_{\phi,\mathfrak{p}} = \mathrm{Nr}_{\mathbb{F}_\mathfrak{p}^{(d)}/\mathbb{F}_\mathfrak{p}}(\varrho_{\phi,\mathfrak{p}}).$$

Proof. By (4.1), the map

$$\iota : O_D/\mathfrak{p}O_D \longrightarrow M_d(\mathbb{F}_\mathfrak{p}^{(d)})$$

$$\alpha_1 + \alpha_2\Pi + \cdots + \alpha_d\Pi^{d-1} \longmapsto \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_d \\ 0 & \alpha_1^{|\mathfrak{p}|} & \alpha_2^{|\mathfrak{p}|} & \cdots & \alpha_{d-1}^{|\mathfrak{p}|} \\ 0 & 0 & \alpha_1^{|\mathfrak{p}|^2} & \cdots & \alpha_{d-2}^{|\mathfrak{p}|^2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \alpha_1^{|\mathfrak{p}|^{d-1}} \end{pmatrix}$$

is an injective ring homomorphism. (As an algebra, $O_D/\mathfrak{p}O_D$ is generated by $\mathbb{F}_\mathfrak{p}^{(d)}$ and Π and, as one easily checks, $\iota(\Pi)\iota(\alpha) = \iota(\alpha)^{|\mathfrak{p}|}\iota(\Pi)$ for any $\alpha \in \mathbb{F}_\mathfrak{p}^{(d)}$.) Hence the reduced norm

$\mathrm{Nr}: O_D \to A$ induces the map

$$\mathrm{Nr}: O_D/\mathfrak{p}O_D \longrightarrow \mathbb{F}_\mathfrak{p}, \tag{4.5}$$

$$\alpha_1 + \alpha_2\Pi + \cdots + \alpha_d\Pi^{d-1} \longmapsto \alpha_1^{1+|\mathfrak{p}|+\cdots+|\mathfrak{p}|^{d-1}} = \mathrm{Nr}_{\mathbb{F}_\mathfrak{p}^{(d)}/\mathbb{F}_\mathfrak{p}}(\alpha_1).$$

By [1, Prop. 1.8.3], $\phi[\mathfrak{p}]$ is dual to $M(\phi)/\mathfrak{p}M(\phi)$, hence the reduced norm

$$M(\phi)/\mathfrak{p}M(\phi) \longrightarrow \det(M(\phi))/\mathfrak{p}\det(M(\phi))$$

corresponds to the map

$$\mathrm{Nr}\colon \phi[\mathfrak{p}] \cong O_D/\mathfrak{p}O_D \longrightarrow \mathbb{F}_\mathfrak{p} \cong \det(\phi)[\mathfrak{p}]$$

constructed in (4.5). Comparing this with Lemma 4.2, we see that the following diagram commutes

$$\begin{array}{ccc} \phi[\mathfrak{p}] & \xrightarrow{\pi_{\phi,\mathfrak{p}}(g)} & \phi[\mathfrak{p}] \\ \downarrow{\scriptstyle \mathrm{Nr}} & & \downarrow{\scriptstyle \mathrm{Nr}} \\ \det(\phi)[\mathfrak{p}] & \xrightarrow{\mathrm{Nr}_{\mathbb{F}_\mathfrak{p}^{(d)}/\mathbb{F}_\mathfrak{p}}(\varrho_{\phi,\mathfrak{p}}(g))} & \det(\phi)[\mathfrak{p}]. \end{array}$$

Since Lafforgue's determinant construction is equivariant with respect to the action of G_K, we conclude that $\chi_{\phi,\mathfrak{p}}(g) = \mathrm{Nr}_{\mathbb{F}_\mathfrak{p}^{(d)}/\mathbb{F}_\mathfrak{p}}(\varrho_{\phi,\mathfrak{p}}(g))$ for all $g \in \mathrm{G}_K$. □

Lemma 4.4. *Let $C : A \to K[\tau]$, $C_T = \gamma(T) + \tau$, be the Carlitz module over K. Let*

$$\chi_{C,\mathfrak{p}}\colon\ \mathrm{G}_K \longrightarrow \mathrm{Aut}(C[\mathfrak{p}]) \cong \mathbb{F}_\mathfrak{p}^\times.$$

Then,

$$\chi_{\phi,\mathfrak{p}}^{q-1} = \chi_{C,\mathfrak{p}}^{q-1}.$$

Proof. Denote $\rho = \det(\phi)$. Then ρ is defined by $\rho_T = \gamma(T) + b\tau$ for some $0 \neq b \in K$. Let β be a fixed $(q-1)$-th root of b, so that $\beta\rho_T\beta^{-1} = C_T$. Denote by $C_\mathfrak{p}(x)$ the $\mathbb{F}_q$-linear polynomial whose roots constitute $C[\mathfrak{p}]$ (for example, $C_T(x) = \gamma(T)x + x^q$), and similarly for $\rho_\mathfrak{p}(x)$. Then $\beta\rho_\mathfrak{p}(x) = C_\mathfrak{p}(\beta x)$. This implies that multiplication by β gives an isomorphism

$$\rho[\mathfrak{p}] \xrightarrow{\sim} C[\mathfrak{p}],$$
$$\alpha \longmapsto \beta\alpha.$$

Let $\chi_b\colon\ \mathrm{G}_K \to \mathbb{F}_q^\times$ be the character $g \mapsto g(\beta)/\beta$, which is independent of the choice of the $(q-1)$-th root β of b. We see from the above isomorphism that $\chi_{C,\mathfrak{p}} = \chi_{\phi,\mathfrak{p}} \otimes \chi_b$. Finally, since $\chi_b^{q-1} = 1$, we get $\chi_{C,\mathfrak{p}}^{q-1} = \chi_{\phi,\mathfrak{p}}^{q-1}$. □

Corollary 4.5. *We have*

$$\mathrm{Nr}_{\mathbb{F}_\mathfrak{p}^{(d)}/\mathbb{F}_\mathfrak{p}}(\varrho_{\phi,\mathfrak{p}})^{q-1} = \chi_{C,\mathfrak{p}}^{q-1}.$$

Proof. Follows from Proposition 4.3 and Lemma 4.4. □

Now suppose that K, the field over which the Drinfeld-Stuhler O_D-module ϕ is defined, is a finite extension of F. Denote by K^{ab} the maximal abelian extension of K in K^{sep}. Let $\mathrm{G}_K^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{ab}}/K)$. Note that a canonical isogeny claracter factors through $\varrho_{\phi,\mathfrak{p}} : \mathrm{G}_K^{\mathrm{ab}} \to (\mathbb{F}_\mathfrak{p}^{(d)})^\times$.

Given a place v of K, denote by K_v (resp. O_v) the completion of K at v (resp. the ring of integers in K_v). Let

$$\omega_v\colon K_v^\times \longrightarrow \mathrm{G}_K^{\mathrm{ab}}$$

be the *local Artin homomorphism* (mapping $K_v^\times$ to the decomposition group of v in $\mathrm{G}_K^{\mathrm{ab}}$). Let $\widetilde{r}_{\phi,\mathfrak{p}}(v)\colon K_v^\times \to (\mathbb{F}_\mathfrak{p}^{(d)})^\times$ be the composition

$$K_v^\times \xrightarrow{\omega_v} \mathrm{G}_K^{\mathrm{ab}} \xrightarrow{\varrho_{\phi,\mathfrak{p}}} (\mathbb{F}_\mathfrak{p}^{(d)})^\times, \tag{4.6}$$

and let $r_{\phi,\mathfrak{p}}(v)\colon O_v^\times \to (\mathbb{F}_\mathfrak{p}^{(d)})^\times$ be the restriction of $\widetilde{r}_{\phi,\mathfrak{p}}(v)$ to $O_v^\times$.

Proposition 4.6. *With notation as above, we have:*

1. *If v does not lie over $\mathfrak{p}$ or ∞, then $r_{\phi,\mathfrak{p}}(v)^{q^d-1} = 1$.*
2. *If v lies over ∞, then $\widetilde{r}_{\phi,\mathfrak{p}}(v)^{\frac{|\mathfrak{p}|^d-1}{|\mathfrak{p}|-1}(q-1)} = 1$.*

Proof. By Theorem 3.6, ϕ acquires good reduction over a totally tamely ramified extension L of K_v of degree dividing q^d-1. If v does not lie over $\mathfrak{p}$ or ∞, then $\phi[\mathfrak{p}]$ is unramified over L. Hence $\varrho_{\phi,\mathfrak{p}}^{q^d-1}$ is the trivial character when restricted to the inertia group at v. Since by local class field theory ω_v maps $O_v^\times$ into the inertia group at v, we conclude that $r_{\phi,\mathfrak{p}}(v)^{q^d-1}$ is the trivial homomorphism. This proves (1).

To prove (2), first observe that by Corollary 4.5 we have

$$\varrho_{\phi,\mathfrak{p}}^{\frac{|\mathfrak{p}|^d-1}{|\mathfrak{p}|-1}(q-1)} = \chi_{C,\mathfrak{p}}^{q-1}.$$

Hence it is enough to show that $\chi_{C,\mathfrak{p}}^{q-1}$ is trivial when considered as a character of G_{F_∞}. Let $\Lambda_C \subset \mathbb{C}_\infty$ be the A-lattice of rank 1 corresponding to the Carlitz module C, where $\mathbb{C}_\infty$ is the completion of $\overline{F}_\infty$; cf. [6, §3]. Carlitz explicitly computed Λ_C, and from that calculation one easily deduces that $F_\infty(\Lambda_C) = F_\infty(\sqrt[q-1]{T-T^q})$; see [27, p. 236]. In particular, $[F_\infty(\Lambda_C) : F_\infty] = q-1$. On the other hand, any torsion point of C is rational over $F_\infty(\Lambda_C)$; cf. [27, Exercise 13.10]. This implies that $\chi_{C,\mathfrak{p}}$ restricted to G_{F_∞} has order dividing $q-1$. Hence $\chi_{C,\mathfrak{p}}^{q-1} = 1$ on G_{F_∞}. □

Fix a prime $\mathfrak{P}$ of K over $\mathfrak{p}$. Let $f_\mathfrak{P}$ be the residue degree of $\mathfrak{P}$ over $\mathfrak{p}$, i.e., the residue field $\mathbb{F}_\mathfrak{P} = \mathbb{F}_\mathfrak{p}^{(f_\mathfrak{P})}$ of $\mathfrak{P}$ is a degree $f_\mathfrak{P}$ extension of $\mathbb{F}_\mathfrak{p}$. Let

$$t_\mathfrak{P} = \gcd(f_\mathfrak{P}, d).$$

For $u \in O_\mathfrak{P}^\times$ denote by $\bar{u} \in \mathbb{F}_\mathfrak{P}^\times$ the reduction of u modulo $\mathfrak{P}$.

Lemma 4.7. *There is a unique integer $0 \le c_\mathfrak{P} \le |\mathfrak{p}|^{t_\mathfrak{P}} - 2$ such that*

$$r_{\phi,\mathfrak{p}}(\mathfrak{P})(u) = \mathrm{Nr}_{\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}^{(t_\mathfrak{P})}}(\bar{u})^{-c_\mathfrak{P}}$$

for all $u \in O_\mathfrak{P}^\times$.

Proof. The Artin homomorphism $\omega_\mathfrak{P}$ maps $O_\mathfrak{P}^\times$ into the inertia subgroup $I_\mathfrak{P} \subset \mathrm{G}_K^{\mathrm{ab}}$ of $\mathfrak{P}$. Since $K(\mathcal{C}_{\phi,\mathfrak{p}})/K$ is tamely ramified, $r_{\phi,\mathfrak{p}}(\mathfrak{P})$ factors through the tame quotient of $I_\mathfrak{P}$, which is isomorphic to $(O_{\mathfrak{P}}/\mathfrak{P})^\times \cong \mathbb{F}_{\mathfrak{P}}^\times$; cf. [29, §IV. 2]. The image of any homomorphism $\mathbb{F}_{\mathfrak{P}}^\times \to (\mathbb{F}_{\mathfrak{p}}^{(d)})^\times$ is contained in the unique cyclic subgroup of $(\mathbb{F}_{\mathfrak{p}}^{(d)})^\times$ of order

$$\gcd(|\mathfrak{p}|^{f_{\mathfrak{P}}}-1, |\mathfrak{p}|^d-1) = |\mathfrak{p}|^{\gcd(f_{\mathfrak{P}},d)}-1 = |\mathfrak{p}|^{t_{\mathfrak{P}}}-1.$$

Thus, $r_{\phi,\mathfrak{p}}(\mathfrak{P})$ is a homomorphism $O_{\mathfrak{P}}^\times \xrightarrow{(\mathrm{mod}\ \mathfrak{P})} \mathbb{F}_{\mathfrak{P}}^\times \to (\mathbb{F}_{\mathfrak{p}}^{(t_{\mathfrak{P}})})^\times$. Finally, observe that the norm homomorphism $\mathrm{Nr}_{\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}^{(t_{\mathfrak{P}})}}\colon \mathbb{F}_{\mathfrak{P}}^\times \to (\mathbb{F}_{\mathfrak{p}}^{(t_{\mathfrak{P}})})^\times$ is surjective, and, since both groups are cyclic, basic group theory implies that there is a unique $0 \le c_{\mathfrak{P}} \le |\mathfrak{p}|^{t_{\mathfrak{P}}}-2$ such that $r_{\phi,\mathfrak{p}}(\mathfrak{P})(u) = \mathrm{Nr}_{\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}^{(t_{\mathfrak{P}})}}(\bar{u})^{-c_{\mathfrak{P}}}$ for all $u \in O_{\mathfrak{P}}^\times$. □

Lemma 4.8. *Let $e_{\mathfrak{P}}$ be the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$. Let $\chi_{\mathfrak{P}}\colon O_{\mathfrak{P}}^\times \to \mathbb{F}_{\mathfrak{p}}^\times$ be the composition*

$$O_{\mathfrak{P}}^\times \xrightarrow{\omega_{\mathfrak{P}}} \mathrm{G}_K^{\mathrm{ab}} \xrightarrow{\chi_{C,\mathfrak{p}}} \mathrm{Aut}(C[\mathfrak{p}]) \cong \mathbb{F}_{\mathfrak{p}}^\times.$$

Then $\chi_{\mathfrak{P}}(u) = \mathrm{Nr}_{\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}}(\bar{u})^{-e_{\mathfrak{P}}}$ for all $u \in O_{\mathfrak{P}}^\times$.

Proof. Let $C_{\mathfrak{p}}(x) = \mathfrak{p}x + \cdots + x^{|\mathfrak{p}|}$ be the linearized polynomial corresponding to $C_{\mathfrak{p}}$, where $C_{\mathfrak{p}}$ is the image of $\mathfrak{p}$ under the Carlitz module homomorphism $C\colon A \to K[\tau]$. By [12], $f(x) = C_{\mathfrak{p}}(x)/x$ is irreducible and separable over F, and the splitting field L of f is totally tamely ramified over $\mathfrak{p}$. Let v denote the unique extension of the normalized valuation on $K_{\mathfrak{P}}$ to $K_{\mathfrak{P}}^{\mathrm{sep}}$. For any root α of f we have $v(\alpha) = e_{\mathfrak{P}}/(|\mathfrak{p}|-1)$. Let π be a uniformizer of $K_{\mathfrak{P}}$. Let $\theta_{|\mathfrak{p}|-1}\colon I_{\mathfrak{P}} \to \mathbb{F}_{\mathfrak{p}}^\times$ be the character $g \mapsto g(\pi^{1/(|\mathfrak{p}|-1)})/\pi^{1/(|\mathfrak{p}|-1)}$ of the inertia subgroup $I_{\mathfrak{P}} \subseteq \mathrm{G}_K^{\mathrm{ab}}$ of $\mathfrak{P}$. This character factors through the tame quotient I_t of $I_{\mathfrak{P}}$. According to [28, Prop. 7], because $v(\alpha) = e_{\mathfrak{P}}/(|\mathfrak{p}|-1)$,

$$g(\alpha)/\alpha = \theta_{|\mathfrak{p}|-1}(g)^{e_{\mathfrak{P}}} \quad \text{for all } g \in I_t,$$

i.e., I_t acts on the roots of $f(x)$ by the character $\theta_{|\mathfrak{p}|-1}^{e_{\mathfrak{P}}}$. Thus,

$$\chi_{C,\mathfrak{p}} = \theta_{|\mathfrak{p}|-1}^{e_{\mathfrak{P}}}. \tag{4.7}$$

Next, by [28, §1.3], for $\bar{u} \in \mathbb{F}_{\mathfrak{P}}^\times \subset I_t$, we have

$$\theta_{|\mathfrak{p}|-1}(\bar{u})^{e_{\mathfrak{P}}} = \mathrm{Nr}_{\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}}(\bar{u})^{e_{\mathfrak{P}}}. \tag{4.8}$$

Finally, by [28, Prop. 3], for $u \in O_{\mathfrak{P}}^\times$, we have

$$\theta_{|\mathfrak{p}|-1}(\omega_{\mathfrak{P}}(u)) = \theta_{|\mathfrak{p}|-1}(\bar{u}^{-1}). \tag{4.9}$$

Combining (4.7), (4.8), (4.9), we arrive at the formula of the lemma. □

Proposition 4.9. *We have*

$$\frac{d}{t_{\mathfrak{P}}}(q-1)c_{\mathfrak{P}} \equiv (q-1)e_{\mathfrak{P}} \mod (|\mathfrak{p}|-1).$$

Proof. By Corollary 4.5, $\mathrm{Nr}_{\mathbb{F}_{\mathfrak{p}}^{(d)}/\mathbb{F}_{\mathfrak{p}}}(\varrho_{\phi,\mathfrak{p}})^{q-1} = \chi_{C,\mathfrak{p}}^{q-1}$. Hence

$$\mathrm{Nr}_{\mathbb{F}_{\mathfrak{p}}^{(d)}/\mathbb{F}_{\mathfrak{p}}}(\varrho_{\phi,\mathfrak{p}}(\omega_{\mathfrak{P}}(u)))^{q-1} = \chi_{C,\mathfrak{p}}(\omega_{\mathfrak{P}}(u))^{q-1}.$$

On one hand, by Lemma 4.7,

$$\begin{aligned}\mathrm{Nr}_{\mathbb{F}_{\mathfrak{p}}^{(d)}/\mathbb{F}_{\mathfrak{p}}}(\varrho_{\phi,\mathfrak{p}}(\omega_{\mathfrak{P}}(u)))^{q-1} &= \mathrm{Nr}_{\mathbb{F}_{\mathfrak{p}}^{(d)}/\mathbb{F}_{\mathfrak{p}}}(\mathrm{Nr}_{\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}^{(t_{\mathfrak{P}})}}(\bar{u}))^{-c_{\mathfrak{P}}(q-1)} \\ &= \mathrm{Nr}_{\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}}(\bar{u})^{-\frac{d}{t_{\mathfrak{P}}}(q-1)c_{\mathfrak{P}}}.\end{aligned}$$

On the other hand, by Lemma 4.8,

$$\chi_{C,\mathfrak{p}}(\omega_{\mathfrak{P}}(u))^{q-1} = \mathrm{Nr}_{\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}}(\bar{u})^{-e_{\mathfrak{P}}(q-1)}.$$

Combining these two expressions, we get

$$\mathrm{Nr}_{\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}}(\bar{u})^{-e_{\mathfrak{P}}(q-1)} = \mathrm{Nr}_{\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}}(\bar{u})^{-\frac{d}{t_{\mathfrak{P}}}(q-1)c_{\mathfrak{P}}}$$

for all $\bar{u} \in \mathbb{F}_{\mathfrak{P}}^{\times}$. Since the norm $\mathrm{Nr}_{\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}}\colon \mathbb{F}_{\mathfrak{P}}^{\times} \to \mathbb{F}_{\mathfrak{p}}^{\times}$ is surjective and $\mathbb{F}_{\mathfrak{p}}^{\times}$ is cyclic, it follows that $\frac{d}{t_{\mathfrak{P}}}(q-1)c_{\mathfrak{P}} \equiv (q-1)e_{\mathfrak{P}} \mod (|\mathfrak{p}|-1)$, as was claimed. □

Corollary 4.10. *Let $\mathfrak{q} \lhd A$ be a prime different from $\mathfrak{p}$. Then*

$$r_{\phi,\mathfrak{p}}(\mathfrak{P})(\mathfrak{q}^{-1})^{d(q-1)} \equiv \mathfrak{q}^{e_{\mathfrak{P}}f_{\mathfrak{P}}(q-1)} \pmod{\mathfrak{p}}.$$

Proof. By Lemma 4.7,

$$r_{\phi,\mathfrak{p}}(\mathfrak{P})(\mathfrak{q}^{-1})^{d(q-1)} = \mathrm{Nr}_{\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}^{(t_{\mathfrak{P}})}}(\bar{\mathfrak{q}}^{-1})^{-c_{\mathfrak{P}}d(q-1)} = \mathrm{Nr}_{\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}^{(t_{\mathfrak{P}})}}(\bar{\mathfrak{q}})^{c_{\mathfrak{P}}d(q-1)}.$$

Since the image $\bar{\mathfrak{q}}$ of $\mathfrak{q}$ under $O_{\mathfrak{P}}^{\times} \to \mathbb{F}_{\mathfrak{P}}^{\times}$ lies in $\mathbb{F}_{\mathfrak{p}}^{\times}$, we have

$$\mathrm{Nr}_{\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}^{(t_{\mathfrak{P}})}}(\bar{\mathfrak{q}})^{c_{\mathfrak{P}}d(q-1)} = \bar{\mathfrak{q}}^{c_{\mathfrak{P}}\frac{f_{\mathfrak{P}}}{t_{\mathfrak{P}}}d(q-1)}.$$

Finally, by Proposition 4.9, in $\mathbb{F}_{\mathfrak{p}}^{\times}$ we have the equality

$$\bar{\mathfrak{q}}^{c_{\mathfrak{P}}\frac{f_{\mathfrak{P}}}{t_{\mathfrak{P}}}d(q-1)} = \bar{\mathfrak{q}}^{e_{\mathfrak{P}}f_{\mathfrak{P}}(q-1)}.$$

□

5. Drinfeld-Stuhler modules over finite fields

Let $\mathfrak{y} \lhd A$ be a prime. Let k be a field extension of $\mathbb{F}_{\mathfrak{y}}$ of degree m. Hence k is a finite field of order q^n, where $n = m \cdot \deg(\mathfrak{y})$. Let $\pi = \tau^n$ be the associated Frobenius morphism. With abuse of notation, denote by π also the scalar matrix $\pi I_d \in M_d(k[\tau])$. Note that π is in the center of $M_d(k[\tau])$ since $\tau^n\alpha = \alpha\tau^n$ for all $\alpha \in k$.

Let $\gamma\colon A \to k$ be the composition $A \to A/\mathfrak{y} \hookrightarrow k$; in particular, $\mathrm{char}_A(k) = \mathfrak{y}$. Let ϕ be a Drinfeld-Stuhler O_D-module defined over k. In this section we assume that $\mathfrak{y} \notin \mathrm{Ram}(D)$. Since π commutes with $\phi(O_D)$, we have $\pi \in \mathrm{End}_k(\phi)$.

Theorem 5.1. *Let $\widetilde{F} := F(\pi)$ be the subfield of $D' := \mathrm{End}_k(\phi) \otimes_A F$ generated over F by π. Then:*

1. *The degree $[\widetilde{F} : F]$ divides d.*
2. *There is a unique place $\widetilde{\infty}$ of $\widetilde{F}$ over ∞.*
3. *There is a unique prime $\tilde{\mathfrak{y}} \neq \widetilde{\infty}$ of $\widetilde{F}$ that divides π. Moreover, $\tilde{\mathfrak{y}}$ lies above $\mathfrak{y}$.*

(4) *The algebra D' is a central division algebra over $\widetilde{F}$ of dimension $(d/[\widetilde{F}:F])^2$ and with invariants*

$$\mathrm{inv}_{\tilde{v}}(D') = \begin{cases} -[\widetilde{F}:F]/d & \text{if } \tilde{v} = \widetilde{\infty}, \\ [\widetilde{F}:F]/d & \text{if } \tilde{v} = \tilde{\mathfrak{y}}, \\ -[\widetilde{F}_{\tilde{v}}:F_v]\cdot \mathrm{inv}_v(D) & \text{otherwise,} \end{cases}$$

for each place v of F and each place $\tilde{v}$ of $\widetilde{F}$ dividing v.

(5) *The field $\widetilde{F}$ is isomorphic to a subfield of D.*

Proof. See [18, (9.10)] and [24, Thm. 5.1]. Note that (5) is not explicitly stated in previous references, but it can be easily deduced from (4) as follows. Indeed, (4) implies that for each place v of F and each place $\tilde{v}$ of $\widetilde{F}$ dividing v, we have

$$d\frac{[\widetilde{F}_{\tilde{v}}:F_v]}{[\widetilde{F}:F]}\cdot \mathrm{inv}_v(D) \in \mathbb{Z}.$$

Now the fact that $\widetilde{F}$ embeds into D follows from a well-known characterization of commutative subfields of central simple algebras; see, for example, Corollary A.3.4 in [17]. □

Let $\mathfrak{l}\lhd A$ be a prime different from $\mathfrak{y}$. By (2.3), we have $T_\mathfrak{l}(\phi)\cong O_D\otimes A_\mathfrak{l}$. Thus, $T_\mathfrak{l}(\phi)\otimes_{A_\mathfrak{l}} F_\mathfrak{l}\cong D\otimes_{A_\mathfrak{l}} F_\mathfrak{l} =: D_\mathfrak{l}$. The action of G_k on torsion points of ϕ gives an $\mathfrak{l}$-adic representation

$$i_\mathfrak{l} : \mathrm{G}_k \to \mathrm{Aut}_{O_D}(T_\mathfrak{l}(\phi)\otimes_{A_\mathfrak{l}} F_\mathfrak{l}) \cong D_\mathfrak{l}^\times.$$

Let $\mathrm{Fr}_k\in \mathrm{G}_k$ be the Frobenius automorphism $\alpha\mapsto\alpha^{q^n}$ of $\bar{k}$. Let

$$P_{\phi,k}(X) = \mathrm{Nr}_{D_\mathfrak{l}/F_\mathfrak{l}}(X - i_\mathfrak{l}(\mathrm{Fr}_k)) \tag{5.1}$$

be the reduced characteristic polynomial of $i_\mathfrak{l}(\mathrm{Fr}_k)$.

Proposition 5.2. *Let $M_{\phi,k}(X)\in A[X]$ be the minimal polynomial of $\pi\in \mathrm{End}_k(\phi)$ over A. Then*

$$P_{\phi,k}(X) = M_{\phi,k}(X)^{d/[\widetilde{F}:F]}.$$

In particular, $P_{\phi,k}(X)$ has coefficients in A that are independent of $\mathfrak{l}$.

Proof. This can be proved by an argument similar to the argument in the proof of the corresponding fact for Drinfeld modules; cf. [9, Lem. 3.3]. For the sake of completeness, we give that argument in the setting of Drinfeld-Stuhler modules.

The endomorphisms of ϕ act on $T_\mathfrak{l}(\phi)$, and, by definition of endmorphisms, the actions of $\mathrm{End}_k(\phi)$ and $\phi(O_D)$ on $T_\mathfrak{l}(\phi)$ commute with each other. Since any nonzero endomorphism has finite kernel, the associated homomorphism

$$j_\mathfrak{l}\colon\ \mathrm{End}_k(\phi)\otimes A_\mathfrak{l} \longrightarrow \mathrm{End}_{O_D\otimes A_\mathfrak{l}}(T_\mathfrak{l}(\phi))$$

is injective. Hence we get an injective homomorphism

$$j_\mathfrak{l}\colon D'\otimes_F F_\mathfrak{l} \longrightarrow \mathrm{End}_{D_\mathfrak{l}}(T_\mathfrak{l}(\phi)\otimes_{A_\mathfrak{l}} F_\mathfrak{l})\cong D_\mathfrak{l}.$$

Let $\mathcal{N} : D'\to F$ be the map obtained by composing the reduced norm $\mathrm{Nr}_{D'/\widetilde{F}}\colon D'\to\widetilde{F}$ with the field norm $\mathrm{Nr}_{\widetilde{F}/F}\colon \widetilde{F}\to F$. Let L be a maximal commutative subfield of D'; in particular, L is a field extension of F of degree d. The restriction of $\mathcal{N}$ to L agrees with the field norm

$\mathrm{Nr}_{L/F}$. On the other hand, $j_\mathfrak{l}(L \otimes_F F_\mathfrak{l})$ is a maximal commutative $F_\mathfrak{l}$-subalgebra of $D_\mathfrak{l}$ whose norm mapping to $F_\mathfrak{l}$ is given by the reduced norm on $D_\mathfrak{l}$. Therefore, $\mathcal{N}|_L = (\mathrm{Nr}_{D_\mathfrak{l}/F_\mathfrak{l}} \circ j_\mathfrak{l})|_L$ for every maximal commutative subfield L of D', so $\mathcal{N} = \mathrm{Nr}_{D_\mathfrak{l}/F_\mathfrak{l}} \circ j_\mathfrak{l}|_{D'}$.

To prove the claim of the proposition, since $\widetilde{F}$ is an infinite set, it suffices to show that $P_{\phi,k}(\alpha) = M_{\phi,k}(\alpha)^{d/[\widetilde{F}:F]}$ for all $\alpha \in \widetilde{F}$. The action Fr_k on $T_\mathfrak{l}(\phi) \otimes_{A_\mathfrak{l}} F_\mathfrak{l}$ agrees with the action of the endomorphism $\pi \in \mathrm{End}_k(\phi)$, so we have

$$\begin{aligned} P_{\phi,k}(\alpha) = \mathrm{Nr}_{D_\mathfrak{l}/F_\mathfrak{l}}(\alpha - j_\mathfrak{l}(\pi)) &= \mathrm{Nr}_{\widetilde{F}/F} \circ \mathrm{Nr}_{D'/\widetilde{F}}(\alpha - \pi) \\ &= (\mathrm{Nr}_{\widetilde{F}/F}(\alpha - \pi))^{d/[\widetilde{F}:F]} \\ &= M_{\phi,k}(\alpha)^{d/[\widetilde{F}:F]}, \end{aligned}$$

the last equality coming from $\widetilde{F} = F(\pi)$. □

Theorem 5.3. *Let $|\cdot|_\infty$ be the unique extension to $\widetilde{F}$ of the normalized absolute value on F corresponding to ∞. Then $|\pi|_\infty = (\#k)^{1/d}$.*

Proof. This is the analogue of the Riemann hypothesis for Drinfeld-Stuhler modules. As the Anderson motive associated to a Drinfeld-Stuhler module is pure of weight $1/d$, Theorem 5.3 follows from a more general statement for Anderson T-modules [10, Thm. 5.6.10]. □

Proposition 5.4. *The ideal generated by $P_{\phi,k}(0)$ in A is $\mathfrak{y}^{[k:\mathbb{F}_\mathfrak{y}]}$.*

Proof. As follows from Proposition 5.2, the constant term of $P_{\phi,k}(X)$, up to an $\mathbb{F}_q^\times$ multiple, is equal to $\mathrm{Nr}_{\widetilde{F}/F}(\pi)^{d/[\widetilde{F}:F]}$. On the other hand, by Theorem 5.1, the only prime divisor of $\mathrm{Nr}_{\widetilde{F}/F}(\pi)$ in A is $\mathfrak{y}$. Thus, $(P_{\phi,k}(0)) = \mathfrak{y}^s$ for some $s \geq 0$.

Since $\widetilde{\infty}$ is the unique place of $\widetilde{F}$ over ∞, the minimal polynomial $M_{\phi,k}(X)$ is irreducible over F_∞, so all its roots have the same absolute value. Combined with Theorem 5.3, this implies that $\deg(P_{\phi,k}(0)) = \deg(\mathfrak{y}) \cdot [k : \mathbb{F}_\mathfrak{y}]$. Hence $s = [k : \mathbb{F}_\mathfrak{y}]$.

□

Corollary 5.5. *Assume $k = \mathbb{F}_\mathfrak{y}$. Then $P_{\phi,k}(X) = M_{\phi,k}(X)$ and $\mathrm{End}_k(\phi) \otimes_A F = \widetilde{F}$ is an imaginary field extension of F of degree d. Moreover, if we write*

$$P_{\phi,k}(X) = X^d + a_1 X^{d-1} + \cdots + a_d$$

then $\deg(a_i) \leq i \cdot \deg(\mathfrak{y})/d$ for all $1 \leq i \leq d$, and $a_d = \mu\mathfrak{y}$ for some $\mu \in \mathbb{F}_q^\times$.

Proof. By Proposition 5.4, if $k = \mathbb{F}_\mathfrak{y}$, then the constant term of $P_{\phi,k}(X)$ is irreducible in A. Since $P_{\phi,k}(0) = M_{\phi,k}(0)^{d/[\widetilde{F}:F]}$, we conclude that $[\widetilde{F} : F] = d$. Now the equality $\mathrm{End}_k(\phi) \otimes_A F = \widetilde{F}$ easily follows from Theorem 5.1. The claim about the degrees of a_i is a consequence of Theorem 5.3. □

Since $P_{\phi,k}(X)$ is a polynomial with coefficients in A, we can reduce the coefficients $P_{\phi,k}(X)$ modulo $\mathfrak{p}$ for any prime $\mathfrak{p} \lhd A$.

Proposition 5.6. *Assume $\mathrm{inv}_\mathfrak{p}(D) = 1/d$. Then*

$$P_{\phi,k}(X) \equiv \prod_{i=0}^{d-1} \left(X - \varrho_{\phi,\mathfrak{p}}(\mathrm{Fr}_k)^{|\mathfrak{p}|^i} \right) \mod \mathfrak{p}.$$

Proof. If in (5.1) we take $\mathfrak{l} = \mathfrak{p}$, then $P_{\phi,k}(X)$ modulo $\mathfrak{p}$ is equal to $\det(X - \pi_{\phi,\mathfrak{p}}(\mathrm{Fr}_k))$, where $\pi_{\phi,\mathfrak{p}}$ is the representation from (4.3). The claim now follows from (4.4). □

6. Global points on Drinfeld-Stuhler varieties

As we have mentioned in Section 3, the category of Drinfeld-Stuhler modules over an A-field K is equivalent to the category of $\mathscr{D}$-elliptic sheaves over K (modulo a certain action of $\mathbb{Z}$ on the latter category). The functor which associates to an $\mathbb{F}_q$-scheme S the set of isomorphism classes of $\mathscr{D}$-elliptic sheaves over S (modulo the action of $\mathbb{Z}$) possesses a coarse moduli scheme X^D over $C' := \mathbb{P}^1_{\mathbb{F}_q} - \mathrm{Ram}(D) - \{\infty\}$ of relative dimension $(d-1)$; this follows from [18, Thm. 4.1], combined with the Keel-Mori theorem. Up to isomorphism, X^D does not depend on the choice of a maximal order O_D in D. Moreover, X^D is geometrically connected since the class number of A is 1. If D is a central division algebra, then X^D is proper over C' by [18, Thm. 6.1]. We call X^D the *Drinfeld-Stuhler variety*. Assume $\mathrm{char}_A(K) \notin \mathrm{Ram}(D)$, so that $\gamma\colon A \to K$ corresponds to a morphism $\mathrm{Spec}(K) \to C'$. Let $X^D_K := X^D \times_{C'} \mathrm{Spec}(K)$. We will denote the set of K-rational points on X^D_K by $X^D(K)$.

In this section we assume that D is a central division algebra over F of dimension d^2, $d \geq 2$. The goal will be to use the canonical isogeny characters to prove that for certain degree d extensions K of F the set of K-rational points $X^D(K)$ of the Drinfeld-Stuhler variety X^D is empty.

A Drinfeld-Stuhler module defined over K corresponds to a K-rational point on X^D_K, so a natural approach to proving that $X^D(K)$ is empty for a specific A-field K is to show that there are no Drinfeld-Stuhler O_D-modules defined over K. But a technical issue arises in this approach from the fact X^D is only a coarse moduli scheme, so the points $X^D(K)$ may not be represented by Drinfeld-Stuhler O_D-modules defined over K, i.e., the field of moduli of a Drinfeld-Stuhler O_D-module might not be a field of definition. Fortunately, the results from [23] and [24] resolve this issue in certain cases.

Let K be an A-field such that $\mathrm{char}_A(K) \notin \mathrm{Ram}(D)$, i.e., either $\mathrm{char}_A(K) = 0$ or $\mathrm{char}_A(K)$ is a prime of A which does not ramify in D. Let ϕ be a Drinfeld-Stuhler O_D-module defined over K. The composition $\partial \circ \phi$ gives a homomorphism $\partial_\phi\colon O_D \to M_d(K)$, which extends linearly to a homomorphism

$$\partial_{\phi,K}\colon O_D \otimes_A K \to M_d(K).$$

It is not hard to show that $\partial_{\phi,K}$ is in fact an isomorphism; see [24, Lem. 2.5]. This implies that if a K-rational point on X^D corresponds to a Drinfeld-Stuhler module defined over K, then necessarily $O_D \otimes_A K \cong M_d(K)$. (If $\mathrm{char}_A(K) = 0$ this is equivalent to $D \otimes_F K \cong M_d(K)$, so K splits D.) Conversely, we have the following:

Theorem 6.1. *Let K be an A-field such that $\mathrm{char}_A(K) \notin \mathrm{Ram}(D)$. If $O_D \otimes_A K \cong M_d(K)$, then a K-rational point on X^D corresponds to a Drinfeld-Stuhler O_D-module defined over K.*

Proof. See [24, Cor. 6.17]. □

Theorem 6.1 does not rule out the possibility that $X^D(K) \neq \emptyset$ but $O_D \otimes_A K \ncong M_d(K)$, in which case the K-rational points on X^D would not correspond to Drinfeld-Stuhler O_D-modules defined over K. This unpleasant phenomenon does occur for Shimura curves associated with indefinite quaternion division algebras over $\mathbb{Q}$. For example, if X^6 denotes the Shimura curve associated to the indefinite quaternion algebra $B(6)$ over $\mathbb{Q}$ of discriminant 6, then $X^6(\mathbb{Q}(\sqrt{-7}))\neq\emptyset$ although $\mathbb{Q}(\sqrt{-7})$ does not split $B(6)$; see Example 1.2 in [13]. On the other hand, for Drinfeld-Stuhler curves we have the following:

Theorem 6.2. *Assume K is a finite extension of F, $d=2$, and $O_D\otimes_F K\not\cong M_d(K)$. Then $X^D(K)=\emptyset$.*

Proof. Since $D\otimes_F K\not\cong M_d(K)$, there is at least one prime $\mathfrak{P}$ of K lying over some $\mathfrak{p}\in\mathrm{Ram}(D)$ such that the ramification index $e(\mathfrak{P}|\mathfrak{p})$ and the residual degree $f(\mathfrak{P}|\mathfrak{p})$ are both odd. Let $K_\mathfrak{P}$ be the completion of K at $\mathfrak{P}$. By [23, Thm. 4.1], we have $X^D(K_\mathfrak{P})=\emptyset$. Since $X^D(K)\subseteq X^D(K_\mathfrak{P})$, the claim follows. □

Remark 6.3. Another result relevant to the above discussion is the following (see [24, Cor. 6.17]): Assume d and q^d-1 are coprime, and $\mathrm{char}_A(K)\notin\mathrm{Ram}(D)$. If $O_D\otimes_A K\not\cong M_d(K)$, then $X^D(K)=\emptyset$. Because of this fact and Theorems 6.1, 6.2, we are inclined to believe that a K-rational point on X^D always corresponds to a Drinfeld-Stuhler O_D-module defined over K.

For the rest of this section let K be an extension of F of degree d such that $D\otimes_F K\cong M_d(K)$. Assume $\mathfrak{y}\lhd A$ is a prime that totally ramifies in K. (In general, such a prime need not exist.) Assume $\mathfrak{y}\notin\mathrm{Ram}(D)$. Let $\mathfrak{Y}$ be the prime of K lying over $\mathfrak{y}$, so $\mathfrak{Y}^d=\mathfrak{y}$. Assume $\mathfrak{p}\in\mathrm{Ram}(D)$ and $\mathrm{inv}_\mathfrak{p}(D)=1/d$. Due to $D\otimes_F K\cong M_d(K)$, the prime $\mathfrak{p}$ does not split in K. Denote by $\mathfrak{P}$ the unique prime of K lying over $\mathfrak{p}$. Denote

$$n=d\frac{|\mathfrak{p}|^d-1}{|\mathfrak{p}|-1}(q^d-1).$$

Assume there is a Drinfeld-Stuhler O_D-module ϕ defined over K. Consider the character $\varrho^n_{\phi,\mathfrak{p}}:\mathrm{G}_K\to(\mathbb{F}_\mathfrak{p}^{(d)})^\times$. Note that $\varrho^n_{\phi,\mathfrak{p}}$ takes values in $\mathbb{F}_\mathfrak{p}^\times$, and is independent of the choice of a canonical isogeny character. By Proposition 4.6 (or rather by its proof), $\varrho^n_{\phi,\mathfrak{p}}$ is unramified at $\mathfrak{Y}$, so $\varrho^n_{\phi,\mathfrak{p}}(\mathrm{Fr}^d_\mathfrak{Y})$ is well-defined, i.e., is independent ot the choice a Frobenius automorphism $\mathrm{Fr}_\mathfrak{Y}$ at $\mathfrak{Y}$.

Proposition 6.4. *We have*

$$\varrho^n_{\phi,\mathfrak{p}}(\mathrm{Fr}^d_\mathfrak{Y})\equiv\mathfrak{y}^n \pmod{\mathfrak{p}}.$$

Proof. By class field theory, one can consider $\varrho^n_{\phi,\mathfrak{p}}$ as a character of the idèle class group $\mathbb{A}_K^\times/K^\times$ of K. Then

$$\varrho^n_{\phi,\mathfrak{p}}(\mathrm{Fr}^d_\mathfrak{Y})=\varrho^n_{\phi,\mathfrak{p}}((\varpi^d_\mathfrak{Y})_\mathfrak{Y},(1)^\mathfrak{Y})=\varrho^n_{\phi,\mathfrak{p}}((u\mathfrak{y})_\mathfrak{Y},(1)^\mathfrak{Y})=\varrho^n_{\phi,\mathfrak{p}}((u)_\mathfrak{Y},(\mathfrak{y}^{-1})^\mathfrak{Y}),$$

where $\varpi_\mathfrak{Y}$ is a uniformizer of $K_\mathfrak{Y}$; u is a unit in $O_\mathfrak{Y}$; $((\varpi^d_\mathfrak{Y})_\mathfrak{Y},(1)^\mathfrak{Y})$ is the idèle of K where the component at the place $\mathfrak{Y}$ is $\varpi^d_\mathfrak{Y}$ and 1 at all other places; $((u)_\mathfrak{Y},(\mathfrak{y}^{-1})^\mathfrak{Y})$ is the idèle where the component at the place $\mathfrak{Y}$ is u and $\mathfrak{y}^{-1}$ at all other places. Now

$$\varrho^n_{\phi,\mathfrak{p}}((u)_\mathfrak{Y},(\mathfrak{y}^{-1})^\mathfrak{Y})=r_{\phi,\mathfrak{p}}(\mathfrak{Y})^n(u)\cdot\prod_{v\neq\mathfrak{Y}}\widetilde{r}_{\phi,\mathfrak{p}}(v)^n(\mathfrak{y}^{-1}),$$

where $\widetilde{r}_{\phi,\mathfrak{p}}(v)$ is the character defined in (4.6), and $r_{\phi,\mathfrak{p}}(v)$ is its restriction to $O_v^\times$. Note that at all places v of K that do not divide $\mathfrak{y}$ or ∞, the element $\mathfrak{y}^{-1}$ is a unit. Hence by Proposition

4.6 we have

$$r_{\phi,\mathfrak{p}}(\mathfrak{Y})^n(u)\cdot\prod_{v\neq\mathfrak{Y}}\widetilde{r}_{\phi,\mathfrak{p}}(v)^n(\mathfrak{y}^{-1})=r_{\phi,\mathfrak{p}}(\mathfrak{P})^n(\mathfrak{y}^{-1}).$$

Finally, since $e_{\mathfrak{P}}f_{\mathfrak{P}}=[K:F]=d$, Corollary 4.10 implies

$$r_{\phi,\mathfrak{p}}(\mathfrak{P})^n(\mathfrak{y}^{-1})\equiv\mathfrak{y}^{e_{\mathfrak{P}}f_{\mathfrak{P}}\frac{n}{d}}=\mathfrak{y}^{d\frac{n}{d}}=\mathfrak{y}^n\pmod{\mathfrak{p}}.$$

□

Definition 6.5. Let $\mathcal{W}(\mathfrak{y})$ be the set of elements π of $\overline{F}$ such that

(1) π is integral over A.
(2) $[F(\pi):F]=d$.
(3) There is only one place $\widetilde{\infty}$ of $F(\pi)$ lying over ∞.
(4) There is a unique prime $\tilde{\mathfrak{y}}\neq\widetilde{\infty}$ of $F(\pi)$ that divides π. This prime lies above $\mathfrak{y}$.
(5) $|\pi|_\infty=|\mathfrak{y}|^{1/d}$, where $|\cdot|_\infty$ is the unique extension to $F(\pi)$ of the normalized absolute value of F corresponding to ∞.

Note that if $\pi\in\mathcal{W}(\mathfrak{y})$, then the minimal polynomial of π

$$M_\pi(X)=X^d+a_1X^{d-1}+\cdots+a_d$$

has the following properties

(1) $a_i\in A$ and $\deg(a_i)\leq i\cdot\deg(\mathfrak{y})/d$ for all $1\leq i\leq d$.
(2) $a_d=\mu\mathfrak{y}$ for some $\mu\in\mathbb{F}_q^\times$.

In particular, $\mathcal{W}(\mathfrak{y})$ is a finite set.

For $s\geq 1$, let $n'=d\frac{q^{sd}-1}{q^s-1}(q^d-1)$ and

$$\mathcal{D}'(\mathfrak{y},s)=\left\{\mathrm{Nr}_{F(\pi)/F}(\pi^{dn'}-\mathfrak{y}^{n'})\mid\pi\in\mathcal{W}(\mathfrak{y})\right\}.$$

Let $\mathcal{P}'(\mathfrak{y},s)$ be the set of prime divisors of nonzero elements of $\mathcal{D}'(\mathfrak{y},s)$.

Theorem 6.6. *Let K/F be a field extension of degree d. Assume*

- $D\otimes_F K\cong M_d(K)$,
- $\mathfrak{y}\lhd A$ *is a prime that totally ramifies in* K,
- $\mathfrak{y}\notin\mathrm{Ram}(D)$,
- $\mathrm{inv}_{\mathfrak{p}}(D)=1/d$,
- $\mathfrak{p}\notin\mathcal{P}'(\mathfrak{y},\deg(\mathfrak{p}))$,
- $D\otimes_F F(\sqrt[d]{\mu\mathfrak{y}})\ncong M_d(F(\sqrt[d]{\mu\mathfrak{y}}))$ *for any* $\mu\in\mathbb{F}_q^\times$.

Then $X^D(K)=\emptyset$.

Proof. Suppose $X^D(K)\neq\emptyset$. Since $D\otimes_F K\cong M_d(K)$, Theorem 6.1 implies that there exists a Drinfeld-Stuhler O_D-module ϕ defined over K. Consider ϕ over $K_{\mathfrak{Y}}$. By Theorem 3.6, ϕ has good reduction over a totally tamely ramified extension L of $K_{\mathfrak{Y}}$ of degree q^d-1. Denote by $\bar{\phi}$ the reduction of ϕ modulo the maximal ideal of L. Note that the residue field of L is $\mathbb{F}_{\mathfrak{y}}$. By Theorem 5.1, Theorem 5.3, and Corollary 5.5, the roots of $P_{\bar{\phi},\mathbb{F}_{\mathfrak{y}}}(X)$ are in $\mathcal{W}(\mathfrak{y})$. If we decompose

$$P_{\bar{\phi},\mathbb{F}_{\mathfrak{y}}}(X)=\prod_{i=1}^d(X-\pi_i)$$

over $\overline{F}$, then from (5.1) it is easy to see that

$$P_{\bar{\phi},\mathbb{F}_{\mathfrak{y}}^{(dn)}}(X)=\prod_{i=1}^{d}(X-\pi_i^{dn}).$$

On the other hand, by Proposition 5.6

$$P_{\bar{\phi},\mathbb{F}_{\mathfrak{y}}^{(dn)}}(X)\equiv\prod_{i=0}^{d-1}\left(X-\varrho_{\bar{\phi},\mathfrak{p}}(\mathrm{Fr}_{\mathbb{F}_{\mathfrak{y}}}^{dn})^{|\mathfrak{p}|^i}\right)=\prod_{i=0}^{d-1}\left(X-\varrho_{\bar{\phi},\mathfrak{p}}(\mathrm{Fr}_{\mathbb{F}_{\mathfrak{y}}}^{dn})\right)\mod \mathfrak{p},$$

where the second equality follows from the fact that $\varrho_{\bar{\phi},\mathfrak{p}}^n$ takes values in $\mathbb{F}_{\mathfrak{p}}^\times$.

Since L is totally ramified over $F_{\mathfrak{y}}$, we have $\varrho_{\phi,\mathfrak{p}}(\mathrm{Fr}_{\mathfrak{Y}}^{nd})=\varrho_{\bar{\phi},\mathfrak{p}}(\mathrm{Fr}_{\mathbb{F}_{\mathfrak{y}}}^{nd})$. By Proposition 6.4,

$$\varrho_{\phi,\mathfrak{p}}(\mathrm{Fr}_{\mathfrak{Y}}^{nd})\equiv\mathfrak{y}^n\ (\mathrm{mod}\ \mathfrak{p}).$$

Thus,

$$\prod_{i=1}^{d}(X-\pi_i^{dn})\equiv\prod_{i=1}^{d}(X-\mathfrak{y}^n)\mod \mathfrak{p}.$$

This congruence implies that for any $1\le i\le d$ we have $\pi_i^{dn}\equiv\mathfrak{y}^n\ (\mathrm{mod}\ \mathfrak{P})$ for the prime $\mathfrak{P}$ in $F(\pi_i)$ lying over $\mathfrak{p}$. Therefore, $\mathfrak{p}$ divides $\mathrm{Nr}_{F(\pi_i)/F}(\pi_i^{dn}-\mathfrak{y}^n)$. This contradicts the assumption $\mathfrak{p}\notin\mathcal{P}'(\mathfrak{y},\deg(\mathfrak{p}))$, unless $\pi_i^{dn}=\mathfrak{y}^n$ for all i. On the other hand, if $\pi_i^{dn}=\mathfrak{y}^n$, then $\bar{\phi}$ is supersingular and there is a unique place of $\widetilde{F}$ lying over $\mathfrak{y}$; see [24, Prop. 5.3]. By Corollary 5.5, the polynomial $P_{\bar{\phi},\mathbb{F}_{\mathfrak{y}}}(X)$ is irreducible over F, and, since only one place of $\widetilde{F}$ lies over $\mathfrak{y}$, it remains irreducible over the completion $F_{\mathfrak{y}}$ of F at $\mathfrak{y}$. Hence the Newton polygon of $P_{\bar{\phi},\mathbb{F}_{\mathfrak{y}}}(X)$ over $F_{\mathfrak{y}}$ must have only one slope. Let $P_{\bar{\phi},\mathbb{F}_{\mathfrak{y}}}(X)=X^d+a_1X^{d-1}+\cdots+a_d$. By Corollary 5.5, $a_d=-\mu\mathfrak{y}$ for some $\mu\in\mathbb{F}_q^\times$ and any other coefficient a_i is not divisible by $\mathfrak{y}$, unless it is zero. If $a_i\neq 0$ for some $1\le i\le d-1$, then the Newton polygon of $P_{\bar{\phi},\mathbb{F}_{\mathfrak{y}}}(X)$ has at least two slopes, contradicting our earlier conclusion. Thus, $P_{\bar{\phi},\mathbb{F}_{\mathfrak{y}}}(X)=X^d-\mu\mathfrak{y}$ for some $\mu\in\mathbb{F}_q^\times$. But now, in the notation of Theorem 5.1, the field $\widetilde{F}=F(\sqrt[d]{\mu\mathfrak{y}})$ embeds into D. We conclude that in our case $\widetilde{F}$ is a maximal commutative subfield of D, so $\widetilde{F}$ splits D. This contradicts one of our assumptions. Therefore $X^D(K)=\emptyset$. □

Example 6.7. Let $q=3$, $d=2$, $s=3$, and $\mathfrak{y}=T$. A computer calculation using `Magma` shows that T^3+T^2+2 and T^3+2T^2+1 are not in $\mathcal{P}'(\mathfrak{y},3)$. Let $\mathfrak{p}$ be one of these primes. Let $\mathfrak{q}$ be a prime different from $\mathfrak{p}$ which splits in both $F(\sqrt{T})$ and $F(\sqrt{-T})$. Let D be the quaternion division algebra over F with $\mathrm{Ram}(D)=\{\mathfrak{p},\mathfrak{q}\}$. Let $K=F(\sqrt{T\mathfrak{m}})$, where $\mathfrak{m}$ is square-free and $T\nmid\mathfrak{m}$. If $\mathfrak{m}$ is chosen so that $\left(\frac{T\mathfrak{m}}{\mathfrak{p}}\right)\neq 1$ and $\left(\frac{T\mathfrak{m}}{\mathfrak{q}}\right)\neq 1$, then K splits D. For example, one can take $\mathfrak{q}=T^2+1$ and $\mathfrak{m}=\mathfrak{p}\mathfrak{q}$. Therefore, by Theorem 6.6, $X^D(K)=\emptyset$.

Let $m=d(q^d-1)$. Fix a canonical isogeny claracter $\varrho_{\phi,\mathfrak{p}}$. Denote by $\bar{\mathfrak{y}}$ the image of $\mathfrak{y}$ under the reduction homomorphism $A\to\mathbb{F}_{\mathfrak{p}}$. By Proposition 6.4,

$$\varepsilon:=\varrho_{\phi,\mathfrak{p}}(\mathrm{Fr}_{\mathfrak{Y}}^{dm})/\bar{\mathfrak{y}}^m\in\mathbb{F}_{\mathfrak{p}}^{(d)}$$

satisfies

$$\mathrm{Nr}_{\mathbb{F}_{\mathfrak{p}}^{(d)}/\mathbb{F}_{\mathfrak{p}}}(\varepsilon)=\varepsilon^{1+|\mathfrak{p}|+\cdots+|\mathfrak{p}|^{d-1}}=1.$$

As in the proof of Theorem 6.6 one deduces that

$$P_{\bar{\phi},\mathbb{F}_{\mathfrak{y}}^{(dm)}}(X) \mod \mathfrak{p} = \prod_{i=0}^{d-1}\left(X - \varrho_{\phi,\mathfrak{p}}(\mathrm{Fr}_{\mathfrak{Y}}^{dm})^{|\mathfrak{p}|^i}\right) = \prod_{i=0}^{d-1}\left(X - \varepsilon^{|\mathfrak{p}|^i}\bar{\mathfrak{y}}^m\right) \in \mathbb{F}_{\mathfrak{p}}[X]$$

is independent of the choice of a canonical isogeny claracter. We use this expression to strengthen Theorem 6.6 when $d = 2$. This will give us a congruence condition which is more amenable to explicit verification, and thus construction of explicit examples.

Until the end of this section assume $d = 2$. For $r \geq 1$ denote

$$P_{\bar{\phi},\mathbb{F}_{\mathfrak{y}}^{(r)}}(X) = X^2 - a(r)X + b(r) \in A[X].$$

For $\pi \in \mathcal{W}(\mathfrak{y})$, let π' be its conjugate over F (keep in mind that $[F(\pi) : F] = d = 2$). Define

$$\mathcal{C}(\mathfrak{y}) = \{\pi^{dm} + (\pi')^{dm} \mid \pi \in \mathcal{W}(\mathfrak{y})\}.$$

Note that $\mathcal{C}(\mathfrak{y})$ is a finite subset of A, and $a(dm) \in \mathcal{C}(\mathfrak{y})$. For $s \geq 1$, let

$$\mathcal{D}(\mathfrak{y}, s) = \left\{\mathrm{Nr}_{\mathbb{F}_{q^s}(T)/F}\left(c - (\varepsilon + \varepsilon^{-1})\mathfrak{y}^m\right) \mid c \in \mathcal{C}(\mathfrak{y}), \varepsilon \in \mathbb{F}_{q^{2s}}, \varepsilon^{1+q^s} = 1\right\}.$$

Note that $\varepsilon + \varepsilon^{-1} = \varepsilon + \varepsilon^{q^s} = \mathrm{Tr}_{\mathbb{F}_{q^{2s}}/\mathbb{F}_{q^s}}(\varepsilon) \in \mathbb{F}_{q^s}$, so the norm above makes sense. The set $\mathcal{D}(\mathfrak{y}, s)$ is again a finite subset of A. Let $\mathcal{P}(\mathfrak{y}, s)$ be the set of prime divisors of nonzero elements of $\mathcal{D}(\mathfrak{y}, s)$.

Now let $s = \deg(\mathfrak{p})$ and identify $\mathbb{F}_{q^{2s}}$ with $\mathbb{F}_{\mathfrak{p}}^{(d)}$. From our earlier discussion,

$$a(dm) \equiv (\varepsilon + \varepsilon^{-1})\bar{\mathfrak{y}}^m \mod \mathfrak{p}.$$

This implies that either $\mathfrak{p} \in \mathcal{P}(\mathfrak{y}, s)$ or $a(dm) = (\varepsilon + \varepsilon^{-1})\mathfrak{y}^m$. In the second case, $\mathfrak{y}$ divides $a(dm)$.

Lemma 6.8. *The prime $\mathfrak{y}$ divides $a(dm)$ if and only if $a(1) = 0$.*

Proof. Write $a(1) = \pi + \pi'$ for some $\pi \in \mathcal{W}(\mathfrak{y})$. Then $a(r) = \pi^r + (\pi')^r$ for all $r \geq 1$. Since

$$a(1)^r = (\pi + \pi')^r = \pi^r + (\pi')^r + \pi\pi' c = \pi^r + (\pi')^r + \mathfrak{y}\mu c = a(r) + \mathfrak{y}\mu c$$

for some $c \in A$ and $\mu \in \mathbb{F}_q^\times$, we see that $\mathfrak{y}$ divides $a(r)$ if and only if $\mathfrak{y}$ divides $a(1)$. On the other hand, $\deg(a(1)) \leq \deg(\mathfrak{y})/2$, so $\mathfrak{y}$ divides $a(1)$ if and only if $a(1) = 0$. □

By Lemma 6.8, if $\mathfrak{y}$ divides $a(dm)$ then $a(1) = 0$. But if $a(1) = 0$, then the minimal polynomial of the Frobenius endomorphism of $\bar{\phi}$ over $\mathbb{F}_{\mathfrak{y}}$ is $X^2 - \mu\mathfrak{y}$ for some $\mu \in \mathbb{F}_q^\times$. Thus, $\widetilde{F} = F(\sqrt{\mu\mathfrak{y}})$. By Theorem 5.1, $\widetilde{F}$ embeds into D, so $\widetilde{F}$ splits D. Thus, we proved the following:

Theorem 6.9. *Let $d = 2$ and K/F be a quadratic extension. Assume*

- $D \otimes_F K \cong M_2(K)$,
- $\mathfrak{y} \lhd A$ *is a prime that ramifies in K,*
- $\mathfrak{y} \notin \mathrm{Ram}(D)$,
- $\mathfrak{p} \in \mathrm{Ram}(D)$,
- $\mathfrak{p} \notin \mathcal{P}(\mathfrak{y}, \deg(\mathfrak{p}))$,
- $D \otimes_F F(\sqrt{\mu\mathfrak{y}}) \ncong M_2(F(\sqrt{\mu\mathfrak{y}}))$ *for any $\mu \in \mathbb{F}_q^\times$.*

Then $X^D(K) = \emptyset$.

Note that the last assumption $D\otimes_F F(\sqrt{\mu\mathfrak{y}})\not\cong M_2(F(\sqrt{\mu\mathfrak{y}}))$ is equivalent to the existence of $\mathfrak{q}\in\mathrm{Ram}(D)$ which splits in $F(\sqrt{\mu\mathfrak{y}})$. Also, ∞ should not split in $\widetilde{F}$, which is equivalent to μ being a non-square in $\mathbb{F}_q^\times$ when $\deg(\mathfrak{y})$ is even and q is odd.

Remark 6.10. Theorem 6.6 specialized to $d=2$ is a weaker theorem than Theorem 6.9 because $\mathcal{P}(\mathfrak{y},s)$ is a smaller set than $\mathcal{P}'(\mathfrak{y},s)$. For example, if $q=3$, $\mathfrak{y}=T$ and $s=2$, then T^2+T+2 and T^2+2T+2 are not in $\mathcal{P}(\mathfrak{y},2)$ but they are both in $\mathcal{P}'(\mathfrak{y},2)$.

Example 6.11. Let $q=3$, $d=2$, $\mathfrak{y}=T$. Let

$$S:=\{T^2+T+2,\quad T^2+2T+2,\quad T^3+T^2+2,\quad T^3+2T^2+1\}.$$

A computer calculation shows that if $\mathfrak{p}\in S$, then $\mathfrak{p}\notin\mathcal{P}(\mathfrak{y},\deg(\mathfrak{p}))$.

Let $\mathfrak{q}$ be a prime different from $\mathfrak{p}$ which splits in both $F(\sqrt{T})$ and $F(\sqrt{-T})$, i.e., $\left(\frac{\pm T}{\mathfrak{q}}\right)=1$. For example, one can take $\mathfrak{q}=T^2+1$. Let D be the quaternion algebra over F with $\mathrm{Ram}(D)=\{\mathfrak{p},\mathfrak{q}\}$. Since $\mathfrak{q}$ splits in $F(\sqrt{\pm T})$, the last assumption of Theorem 6.9 is satisfied, i.e., $D\otimes_F F(\sqrt{\pm T})\not\cong M_2(F(\sqrt{\pm T}))$.

Let $K=F(\sqrt{T\mathfrak{m}})$, where $\mathfrak{m}\in A$ is a square-free, but not necessarily monic, polynomial not divisible by T. If $\mathfrak{m}$ is chosen so that $\left(\frac{T\mathfrak{m}}{\mathfrak{p}}\right)\neq 1$ and $\left(\frac{T\mathfrak{m}}{\mathfrak{q}}\right)\neq 1$, then K splits D. (For example, one can take $\mathfrak{m}=\mathfrak{p}\mathfrak{q}\mathfrak{m}_1$, where $\mathfrak{m}_1$ is an arbitrary square-free polynomial coprime to $T\mathfrak{p}\mathfrak{q}$.) With previous choices, Theorem 6.9 implies that $X^D(K)=\emptyset$.

Example 6.12. Let $q=5$, $d=2$, $\mathfrak{y}=T$. Let

$$\begin{aligned}S:=\{&T^3+2T+4,\quad T^3+3T+3,\quad T^3+T^2+T+4,\quad T^3+T^2+3T+1,\\ &T^3+2T^2+T+3,\quad T^3+2T^2+2T+3,\quad T^3+3T^2+2T+3,\\ &T^3+3T^2+4T+3,\quad T^3+4T^2+T+1,\quad T^3+4T^2+3T+4\}.\end{aligned}$$

A computer calculation shows that if $\mathfrak{p}\in S$, then $\mathfrak{p}\notin\mathcal{P}(\mathfrak{y},\deg(\mathfrak{p}))$. Fix a prime $\mathfrak{p}\in S$.

Let $\mathfrak{q}\lhd A$ be a prime such that

(i) $\mathfrak{q}\neq T,\mathfrak{p}$;
(ii) $\deg(\mathfrak{q})$ is odd;
(iii) $\left(\frac{\mathfrak{p}}{T}\right)=-\left(\frac{\mathfrak{q}}{T}\right)$.

Let D be the quaternion algebra over F with $\mathrm{Ram}(D)=\{\mathfrak{p},\mathfrak{q}\}$. We claim that $F(\sqrt{\mu T})$ does not split D for any $\mu\in\mathbb{F}_q^\times$. It is enough to prove this for $\mu=1,2$ (since $3=2\cdot 4$ and $4=1\cdot 4$). Assume first that $\left(\frac{\mathfrak{p}}{T}\right)=1$. Then, by the Quadratic Reciprocity (cf. [27, Thm. 3.5]), we have $\left(\frac{T}{\mathfrak{p}}\right)=\left(\frac{\mathfrak{p}}{T}\right)(-1)^{\frac{5-1}{2}\deg(T)\deg(\mathfrak{p})}=1$. Hence $\mathfrak{p}$ splits in $F(\sqrt{T})$, and therefore $D\otimes_F F(\sqrt{T})\not\cong M_2(F(\sqrt{T}))$. Since $\left(\frac{\mathfrak{q}}{T}\right)=-1$, we have $\left(\frac{T}{\mathfrak{q}}\right)=-1$. Since $\deg(\mathfrak{q})$ is odd and $2\in\mathbb{F}_q^\times$ is not a square, we have $\left(\frac{2}{\mathfrak{q}}\right)=-1$. Therefore $\left(\frac{2T}{\mathfrak{q}}\right)=1$, and so $\mathfrak{q}$ splits in $F(\sqrt{2T})$. As before, this implies $D\otimes_F F(\sqrt{2T})\not\cong M_2(F(\sqrt{2T}))$. If $\left(\frac{\mathfrak{p}}{T}\right)=-1$, then a similar argument applies.

Now, as in Example 6.11, let $K=F(\sqrt{T\mathfrak{m}})$, where $\mathfrak{m}\in A$ is a square-free, but not necessarily monic, polynomial not divisible by T. If $\mathfrak{m}$ is chosen so that $\left(\frac{T\mathfrak{m}}{\mathfrak{p}}\right)\neq 1$ and $\left(\frac{T\mathfrak{m}}{\mathfrak{q}}\right)\neq 1$, then K splits D. With previous choices, Theorem 6.9 implies that $X^D(K)=\emptyset$.

7. Counterexamples to the Hasse principle

In this section, we extend Examples 6.11 and 6.12 to construct explicit examples of curves violating the Hasse principle. The main auxiliary tool that we will use are the results from [23] on the existence of local points on Drinfeld-Stuhler curves, which are the function field analogues of the results of Jordan and Livné for Shimura curves [14]. For the convenience of the reader, we summarize these results specialized to the case that will be of particular interest for us.

Let K/F be a quadratic extension. Let D be the quaternion algebra over F with $\mathrm{Ram}(D) = \{\mathfrak{p}, \mathfrak{q}\}$, where $\mathfrak{p}$ and $\mathfrak{q}$ are two distinct primes of A. For a place v of K denote by K_v the completion of K at v.

Theorem 7.1. *Let $\widetilde{\infty}$ be a place of K over ∞.*

1. *If ∞ does not split in K, then $X^D(K_{\widetilde{\infty}}) \neq \emptyset$.*
2. *If ∞ splits in K, then $X^D(K_{\widetilde{\infty}}) = \emptyset$ if and only if either $\deg(\mathfrak{p})$ or $\deg(\mathfrak{q})$ is even.*

Proof. This is a consequence of Theorem 5.10 in [23]. □

Remark 7.2. Assume q is odd and $K = F(\sqrt{\mathfrak{d}})$ for a square-free polynomial $\mathfrak{d} \in A$. It is easy to show that ∞ splits in K if and only if $\deg(\mathfrak{d})$ is even and its leading coefficient is a square in $\mathbb{F}_q^\times$.

Theorem 7.3. *Let $\mathfrak{P}$ be a place of K over $\mathfrak{p}$. Let f and e be the residual degree and the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$, respectively.*

1. *If $f = 2$, then $X^D(K_{\mathfrak{P}}) \neq \emptyset$.*
2. *If $e = 2$, then $X^D(K_{\mathfrak{P}}) = \emptyset$ if and only if in every quadratic extension $F(\sqrt{\mu\mathfrak{p}})$, with $\mu \in \mathbb{F}_q^\times$, at least one of the places $\mathfrak{q}, \infty$ splits.*
3. *If $\mathfrak{p}$ splits in K, then $X^D(K_{\mathfrak{P}}) = \emptyset$.*

Proof. This is a consequence of Theorem 4.1 in [23]. □

In this section, we are only interested in quadratic extensions K which split D. In such extensions neither $\mathfrak{p}$ nor $\mathfrak{q}$ can split, so (3) of Theorem 7.3 does not occur.

Theorem 7.4. *Let $\mathfrak{l} \notin \{\mathfrak{p}, \mathfrak{q}, \infty\}$ be a place of F and $\mathfrak{L}$ be a place of K over $\mathfrak{l}$. Let f be the residual degree of $\mathfrak{L}$ over $\mathfrak{l}$.*

1. *If $f = 2$, then $X^D(K_{\mathfrak{L}}) \neq \emptyset$.*
2. *If $f = 1$, then $X^D(K_{\mathfrak{L}}) = \emptyset$ if and only if for all $a \in A$ and $c \in \mathbb{F}_q^\times$ such that $a^2 + c\mathfrak{l}$ is not a square in A at least one of the places $\{\mathfrak{p}, \mathfrak{q}, \infty\}$ splits in $F(\sqrt{a^2 + c\mathfrak{l}})$.*

Proof. This is a consequence of Theorem 3.1 in [23]. □

Remark 7.5. If q is odd, then to determine whether $X^D(K_{\mathfrak{L}}) = \emptyset$ one needs to examine only a finite number of quadratic extensions $F(\sqrt{a^2 + c\mathfrak{l}})$. Indeed, if $\deg(a) > \deg(\mathfrak{l})/2$, then $a^2 + c\mathfrak{l}$ has even degree and its leading coefficient is a square in $\mathbb{F}_q^\times$, so ∞ splits in $F(\sqrt{a^2 + c\mathfrak{l}})$. If q is even, then $X^D(K_{\mathfrak{L}}) \neq \emptyset$ since the places $\{\mathfrak{p}, \mathfrak{q}, \infty\}$ ramify in the inseparable extension $F(\sqrt{\mathfrak{l}})$.

Let $\mathfrak{l}$ be as in Theorem 7.4. By [18] and [11], X^D has good reduction at $\mathfrak{l}$ (and bad reduction at $\mathfrak{p}, \mathfrak{q}, \infty$). From a geometric version of Hensel's Lemma (see [14]) it follows that $X^D(K_{\mathfrak{L}}) \neq \emptyset$ if and only if $X^D(k_{\mathfrak{L}}) \neq \emptyset$, where $k_{\mathfrak{L}}$ is the residue field at $\mathfrak{L}$. If $\mathfrak{l}$ is not inert in K (i.e., $f = 1$), then $k_{\mathfrak{L}} = \mathbb{F}_{\mathfrak{l}}$. Now by the Weil bound

$$\# X^D(\mathbb{F}_{\mathfrak{l}}) \geq |\mathfrak{l}| + 1 - 2g(X^D)\sqrt{|\mathfrak{l}|},$$

where $g(X^D)$ is the genus of X^D. On the other hand, by [20],

$$g(X^D) = 1 + \frac{(|\mathfrak{p}|-1)(|\mathfrak{q}|-1)}{q^2-1} - \begin{cases} 0 & \text{if } \deg(\mathfrak{p}) \text{ or } \deg(\mathfrak{q}) \text{ is even;} \\ \frac{2q}{q+1} & \text{if } \deg(\mathfrak{p}) \text{ and } \deg(\mathfrak{q}) \text{ are odd.} \end{cases} \tag{7.1}$$

This implies that $X^D(\mathbb{F}_{\mathfrak{l}}) \neq \emptyset$ once $\deg(\mathfrak{l}) \geq 2(\deg(\mathfrak{p}) + \deg(\mathfrak{q}))$. Hence, to decide whether a given X^D has rational points over all completions of K, we need to examine only finitely many places.

Example 7.6. Let $q = 3$,

$$\mathfrak{p} \in \{T^2 + T + 2, \quad T^2 + 2T + 2\}, \qquad \mathfrak{q} = T^2 + 1,$$

and $K = F(\sqrt{\mathfrak{d}})$, where $\mathfrak{d} = \pm T\mathfrak{p}\mathfrak{q}\mathfrak{m}$ for some monic square-free polynomial $\mathfrak{m}$ coprime to $T\mathfrak{p}\mathfrak{q}$. Further assume that either $\deg(\mathfrak{m})$ is even or the leading coefficient of $\mathfrak{d}$ is -1. Note that this last assumption implies that ∞ does not split in K. Let D be the quaternion algebra over F with $\mathrm{Ram}(D) = \{\mathfrak{p}, \mathfrak{q}\}$. By Example 6.11, $X^D(K) = \emptyset$.

Since ∞ does not split in K, by Theorem 7.1, we have $X^D(K_{\widetilde{\infty}}) \neq \emptyset$.

The places $\mathfrak{p}$ and $\mathfrak{q}$ ramify in K. By Theorem 7.3, we have $X^D(K_{\mathfrak{P}}) \neq \emptyset$ and $X^D(K_{\mathfrak{Q}}) \neq \emptyset$ for the unique places $\mathfrak{P}$ and $\mathfrak{Q}$ of K over $\mathfrak{p}$ and $\mathfrak{q}$, respectively. (Note that $\mathfrak{q}$ and ∞ are inert in $F(\sqrt{-\mathfrak{p}})$, and similarly $\mathfrak{p}$ and ∞ are inert in $F(\sqrt{-\mathfrak{q}})$.)

It remains to examine the places of F where X^D has good reduction. By Theorem 7.4, we can restrict ourselves to those $\mathfrak{l}$ that split or ramify in K. Using (7.1) one computes that $g(X^D) = q^2$. From the Weil bound, $X^D(\mathbb{F}_{\mathfrak{l}}) \neq \emptyset$ once $\deg(\mathfrak{l}) \geq 6$. Hence, we need to examine $X^D(K_{\mathfrak{L}})$ for primes $\mathfrak{l} \lhd A$ of degree ≤ 5 which split or ramify in K; here $\mathfrak{L}$ is a place of K over $\mathfrak{l}$. By Theorem 7.4, to show that $X^D(K_{\mathfrak{L}}) \neq \emptyset$ we need to find $a \in A$ with $\deg(a) \leq \deg(\mathfrak{l})/2$ and $c \in \mathbb{F}_q^\times$ such that

- $a^2 + c\mathfrak{l}$ has odd degree or its leading coefficient is not a square in $\mathbb{F}_q^\times$, and
- $$\left(\frac{a^2 + c\mathfrak{l}}{\mathfrak{p}}\right) \neq 1, \qquad \left(\frac{a^2 + c\mathfrak{l}}{\mathfrak{q}}\right) \neq 1.$$

For this we use computer calculations. (It is important here that places $\mathfrak{l}$ have relatively small degree, which is a consequence of choosing $\mathfrak{q}$ of small degree so that the genus of X^D is small.) Using `Magma`, we simply run through all possible a and c and check the conditions. For the following $\mathfrak{m}$ our program confirms that a and c for which the necessary conditions are satisfied always exist:

$$\begin{aligned}\mathfrak{m} \in \{1,\quad & T+1,\quad T+2,\quad T^2+T+2,\quad T^2+2T+2,\quad T^3+T^2+2,\\ & T^3+2T^2+1,\quad T^3+2T+1,\quad T^3+2T+2,\quad T^3+T^2+2T+1,\\ & T^3+T^2+T+2,\quad T^4+T+2,\quad T^4+2T+2,\quad T^4+T^2+2,\\ & T^4+2T^2+2,\quad T^4+T^2+T+1,\quad T^4+T^2+2T+1\}\\ & \text{(where the case } \mathfrak{m}=\mathfrak{p} \text{ is excluded).}\end{aligned}$$

Thus, we obtain counterexamples to the Hasse principle.

Remark 7.7. In Example 6.11 we also had $\mathfrak{p} \in \{T^3+T^2+2, T^3+2T^2+1\}$ and $\mathfrak{q} = T^2+1$ as possible ramification places of a quaternion algebra D for which $X^D(K) = \emptyset$, where $K = F(\sqrt{\pm T\mathfrak{p}\mathfrak{q}\mathfrak{m}})$. But these $\mathfrak{p}$ do not lead to counterexamples to the Hasse principle since in these cases $X^D(K_{\mathfrak{Q}}) = \emptyset$. This follows from Theorem 7.3, as ∞ splits in $F(\sqrt{\mathfrak{q}})$ and $\mathfrak{p}$ splits in $F(\sqrt{-\mathfrak{q}})$.

Example 7.8. Let $q = 5$, $\mathfrak{p} = T^3+2T+4$, and $\mathfrak{q} = T+2$. Note that this puts us in the setup of Example 6.12 since $\deg(\mathfrak{q})$ is odd and $\left(\frac{\mathfrak{p}}{T}\right) = 1 = -\left(\frac{\mathfrak{q}}{T}\right)$. Let $\mathfrak{m} \in A$ be a monic square-free polynomial coprime to $T\mathfrak{p}\mathfrak{q}$. Let $\mathfrak{d} = T\mathfrak{p}\mathfrak{q}\mathfrak{m}$ or $\mathfrak{d} = 2T\mathfrak{p}\mathfrak{q}\mathfrak{m}$ if $\deg(\mathfrak{m})$ is even, and $\mathfrak{d} = 2T\mathfrak{p}\mathfrak{q}\mathfrak{m}$ if $\deg(\mathfrak{m})$ is odd. Let D be the quaternion algebra over F with $\mathrm{Ram}(D) = \{\mathfrak{p}, \mathfrak{q}\}$. Then, by Example 6.12, we have $X^D(K) = \emptyset$ for $K = F(\sqrt{\mathfrak{d}})$.

Since ∞ does not split in K, we have $X^D(K_{\widetilde{\infty}}) \neq \emptyset$.

The places $\mathfrak{p}$ and $\mathfrak{q}$ ramify in K. Since $\deg(\mathfrak{p}) = 3$ is odd, ∞ ramifies in both $F(\sqrt{\mathfrak{p}})$ and $F(\sqrt{2\mathfrak{p}})$. The prime $\mathfrak{q}$ is inert in $F(\sqrt{\mathfrak{p}})$. Thus, $X^D(K_{\mathfrak{P}}) \neq \emptyset$ for the unique prime $\mathfrak{P}$ of K over $\mathfrak{p}$. Similarly, ∞ ramifies in both $F(\sqrt{\mathfrak{q}})$ and $F(\sqrt{2\mathfrak{q}})$, and $\mathfrak{p}$ is inert in $F(\sqrt{\mathfrak{q}})$. Thus, $X^D(K_{\mathfrak{Q}}) \neq \emptyset$.

Next, we compute $g(X^D) = q(q-1)$ and use the Weil bound to conclude that $X^D(F_{\mathfrak{l}}) \neq \emptyset$ if $\deg(\mathfrak{l}) \geq 5$. Finally, we examine places $\mathfrak{l}$ of degree ≤ 4 using a computer program. For the following $\mathfrak{m}$ our program confirms that the conditions for the existence of $K_{\mathfrak{L}}$-rational points are satisfied for all $\mathfrak{l}$:

$$\mathfrak{m} \in \{1,\quad T+1,\quad T+3,\quad T+4,\quad T^2+2,\quad T^2+3,\quad T^2+T+1,\quad T^2+T+2\}.$$

Thus, we obtain counterexamples to the Hasse principle.

Remark 7.9. By Theorem 7.3, for $\mathfrak{p} \in \mathrm{Ram}(D)$ we have $X^D(F_{\mathfrak{p}}) = \emptyset$. Thus, $X^D(F) = \emptyset$ but X^D does not violate the Hasse principle over F.

Remark 7.10. If X^D embeds into its Jacobian J^D over a finite extension K of F (e.g., there is a K-rational divisor of degree 1 on X^D), then the Brauer-Manin obstruction is the only obstruction to the Hasse principle over K. This follows from a result of Poonen and Voloch [25, Thm. D]. There are two conditions that need to be satisfied in order to apply [25]. These conditions are

(1) J^D has no nonzero isotrivial quotients;
(2) $J^D(F^{\mathrm{sep}})[p^\infty]$ is finite (p is the characteristic of F).

These are satisfied since J^D has split purely multiplicative reduction at ∞ (cf. [23]). Indeed, the first claim is clear from the theory of Néron models. The second claim can be seen from the rigid-analytic uniformization $J^D(\overline{F}_\infty) \cong (\overline{F}_\infty^\times)^{g(X^D)}/\Lambda$ of J^D over F_∞ since the extension of F_∞ obtained by adjoining $J^D(\overline{F}_\infty)[p^n]$ is the same as the extension obtained by adjoining p^n-th roots of the generators of the lattice Λ.

Acknowledgements. Keisuke Arai thanks Shin Hattori for a discussion and suggestive comments. Satoshi Kondo thanks Kürşat Aker for a computation and Shin Hattori in general. Mihran Papikian thanks the National Center for Theoretical Sciences in Hsinchu, where part of this work was carried out, for its hospitality and excellent working conditions.

References

[1] Anderson, G. W. t-motives. *Duke Math. J. 53*, 2 (1986), 457–502.

[2] Arai, K. Non-existence of points rational over number fields on Shimura curves. *Acta Arith. 172*, 3 (2016), 243–250.

[3] Arai, K. Rational points on Shimura curves and the Manin obstruction. *Nagoya Math. J. 230* (2018), 144–159.

[4] Blum, A., and Stuhler, U. Drinfeld modules and elliptic sheaves. In *Vector bundles on curves—new directions (Cetraro, 1995)*, vol. 1649 of *Lecture Notes in Math.* Springer, 1997, pp. 110–193.

[5] Clark, P. L. On the Hasse principle for Shimura curves. *Israel J. Math. 171* (2009), 349–365.

[6] Drinfeld, V. G. Elliptic modules. *Mat. Sb. (N.S.) 94* (1974), 594–627.

[7] Gardeyn, F. A Galois criterion for good reduction of τ-sheaves. *J. Number Theory 97*, 2 (2002), 447–471.

[8] Gardeyn, F. The structure of analytic τ-sheaves. *J. Number Theory 100*, 2 (2003), 332–362.

[9] Gekeler, E.-U. On finite Drinfeld modules. *J. Algebra 141*, 1 (1991), 187–203.

[10] Goss, D. *Basic structures of function field arithmetic*, vol. 35 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*. Springer-Verlag, Berlin, 1996.

[11] Hausberger, T. Uniformisation des variétés de Laumon-Rapoport-Stuhler et conjecture de Drinfeld-Carayol. *Ann. Inst. Fourier (Grenoble) 55*, 4 (2005), 1285–1371.

[12] Hayes, D. R. Explicit class field theory in global function fields. In *Studies in algebra and number theory*, vol. 6 of *Adv. in Math. Suppl. Stud.* Academic Press, New York-London, 1979, pp. 173–217.

[13] Jordan, B. W. Points on Shimura curves rational over number fields. *J. Reine Angew. Math. 371* (1986), 92–114.

[14] Jordan, B. W., and Livné, R. A. Local Diophantine properties of Shimura curves. *Math. Ann. 270*, 2 (1985), 235–248.

[15] Lafforgue, L. Chtoucas de Drinfeld et conjecture de Ramanujan-Petersson. *Astérisque*, 243 (1997), ii+329.

[16] Lafforgue, L. Une compactification des champs classifiant les chtoucas de Drinfeld. *J. Amer. Math. Soc. 11*, 4 (1998), 1001–1036.

[17] Laumon, G. *Cohomology of Drinfeld modular varieties. Part I*, vol. 41 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1996. Geometry, counting of points and local harmonic analysis.

[18] Laumon, G., Rapoport, M., and Stuhler, U. $\mathscr{D}$-elliptic sheaves and the Langlands correspondence. *Invent. Math. 113*, 2 (1993), 217–338.

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

[20] Papikian, M. Genus formula for modular curves of $\mathscr{D}$-elliptic sheaves. *Arch. Math. (Basel) 92*, 3 (2009), 237–250.

[21] Papikian, M. On hyperelliptic modular curves over function fields. *Arch. Math. (Basel) 92*, 4 (2009), 291–302.

[22] Papikian, M. Endomorphisms of exceptional $\mathscr{D}$-elliptic sheaves. *Math. Z. 266*, 2 (2010), 407–423.

[23] Papikian, M. Local Diophantine properties of modular curves of $\mathscr{D}$-elliptic sheaves. *J. Reine Angew. Math. 664* (2012), 115–140.

[24] Papikian, M. Drinfeld-Stuhler modules. *Res. Math. Sci. 5*, 4 (2018), Paper No. 40, 33.

[25] Poonen, B., and Voloch, J. F. The Brauer-Manin obstruction for subvarieties of abelian varieties over function fields. *Ann. of Math. (2) 171*, 1 (2010), 511–532.

[26] Reiner, I. *Maximal orders*, vol. 28 of *London Mathematical Society Monographs. New Series*. The Clarendon Press, Oxford University Press, Oxford, 2003. Corrected reprint of the 1975 original, With a foreword by M. J. Taylor.

[27] Rosen, M. *Number theory in function fields*, vol. 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

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

[29] Serre, J.-P. *Local fields*, vol. 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979.

[30] Taelman, L. *On t-motifs*. 2007. Thesis (Ph.D.)–The University of Groningen.

Department of Mathematics, School of Science and Technology for Future Life, Tokyo Denki University, 5 Senju Asahi-cho, Adachi-ku, Tokyo 120-8551, Japan

E-mail address: araik@mail.dendai.ac.jp

Middle East Technical University, Northern Cyprus Campus, 99738 Kalkanli, Guzelyurt, Mersin 10, Turkey

Kavli Institute for the Physics and Mathematics of the Universe, University of Tokyo, Kashiwa-no-ha 5-1-5, 277-8583, Japan

E-mail address: satoshi.kondo@gmail.com

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, U.S.A.

E-mail address: papikian@psu.edu