Nagoya Math. J., **234** (2019), 17–45
DOI 10.1017/nmj.2017.26

EXPLICIT SURJECTIVITY RESULTS FOR DRINFELD MODULES OF RANK 2

IMIN CHEN AND YOONJIN LEE

Abstract. Let $K=\mathbb{F}_q(T)$ and $A=\mathbb{F}_q[T]$. Suppose that ϕ is a Drinfeld A-module of rank 2 over K which does not have complex multiplication. We obtain an explicit upper bound (dependent on ϕ) on the degree of primes $\wp$ of K such that the image of the Galois representation on the $\wp$-torsion points of ϕ is not surjective, in the case of q odd. Our results are a Drinfeld module analogue of Serre's explicit large image results for the Galois representations on p-torsion points of elliptic curves (Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. **15** (1972), 259–331; Serre, Quelques applications du théorème de densité de Chebotarev, Inst. Hautes Etudes Sci. Publ. Math. **54** (1981), 323–401.) and are unconditional because the generalized Riemann hypothesis for function fields holds. An explicit isogeny theorem for Drinfeld A-modules of rank 2 over K is also proven.

§1. Introduction

It is well known that there is a close analogy between the arithmetic of Drinfeld A-modules of rank 2 over $K=\mathbb{F}_q(T)$ (where $A=\mathbb{F}_q[T]$ and $\mathbb{F}_q$ is a finite field of order q), and elliptic curves over $\mathbb{Q}$, and that considering arithmetical problems from both perspectives enhances our understanding of the intrinsic difficulty of the problems in question. In this paper, we investigate the problem of obtaining explicit large image results for the fields generated by torsion points of Drinfeld modules.

Serre proved in [24] that if E is an elliptic curve over a number field K without complex multiplication, then there is a constant $c_{K,E}$ dependent only on K and E such that the Galois representation $\rho_{E,p}$ on the p-torsion points of E is surjective for any prime number $p>c_{K,E}$. There has been

Received July 22, 2016. Revised July 1, 2017. Accepted July 1, 2017.
2010 Mathematics subject classification. Primary 11G09; Secondary 11R58.
Imin Chen is supported by an NSERC Discovery Grant and Yoonjin Lee is a corresponding author and supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2009-0093827) and also by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (NRF-2017R1A2B2004574).

© 2017 *Foundation Nagoya Mathematical Journal*

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

some work on obtaining explicit values for the constants $c_{K,E}$ when $K = \mathbb{Q}$ (Serre [26], Kraus [14], Cojocaru–Hall [4], Lombardo [16]). The assumption of the generalized Riemann hypothesis allows one to considerably improve these bounds [26].

In the case $K = \mathbb{Q}$, the analysis normally proceeds by dividing the argument into which type of maximal proper subgroup contains the image of $\rho_{E,p}$. The most difficult case is when the image of $\rho_{E,p}$ lies in the normalizer of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. In all other cases, one in fact has a uniform bound on $c_{K,E}$ which is independent of the elliptic curve E without complex multiplication, by work of Mazur [17] on rational points on modular curves.

The analogue of Serre's result [24] for Drinfeld A-modules of rank 2 was proved by Gardeyn [11], using the earlier work of Pink on the Mumford–Tate conjecture for Drinfeld modules [20]. In detail, if ϕ is a Drinfeld module of rank 2 without complex multiplication over a fixed finite extension of K, then there are only finitely many primes $\wp$ such that the image of the Galois representation $\rho_{\phi,\wp}$ on the $\wp$-torsion points of ϕ is not surjective. The case of general rank was recently proven in [21].

In this paper, we obtain an explicit upper bound on the degree of primes $\wp$ of K such that $\rho_{\phi,\wp}$ is not surjective, for any Drinfeld A-module ϕ of rank 2 over $K = \mathbb{F}_q(T)$ without complex multiplication, in the case when q is odd.

The proof is modeled on the strategy of [24] and [26], some parts of which were made effective, though not explicit in [12].

New difficulties arise however in carrying out the strategy of [24, 26] in the setting of Drinfeld modules. One of these is obtaining an explicit bound on the degree of the different divisor of division fields of ϕ, which in the function field case does not follow immediately from algebraic considerations. For this, we rely heavily on the results in [2, 3] to make explicit the bounds on the different divisor and constant field extensions of torsion fields of Drinfeld A-modules over K.

On the other hand, the generalized Riemann hypothesis holds for function fields, so we are entitled to use better effective Chebotarev density theorems, which makes the final results unconditional and stronger when compared to the number field setting. In the Drinfeld module setting, we do not have uniform bounds in the Borel case because Mazur's method has not yet been successfully adapted to work with Drinfeld modular curves in general. However, there are some partial results in this direction [1, 19].

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

As part of the proof of the Cartan case, we also derive an explicit isogeny theorem for Drinfeld modules of rank 2 over K which uses the explicit bounds on the different divisor and constant field extensions obtained in [2]. A partially explicit isogeny theorem valid for general rank r and K is proven in [3].

§2. Main result

Let $\mathbb{F}_q$ be a finite field of order q, $A = \mathbb{F}_q[T]$, and $K = \mathbb{F}_q(T)$. Throughout the paper, for the sake of simplicity, $:=$ is denoted to mean "is defined to be".

Let L be a finite extension of K, $\mathcal{O}_L$ be the maximal order of L, that is, the integral closure of A in L, and $\mathbb{F}_L$ be the constant field of L. For a prime ideal $\mathfrak{B}$ of $\mathcal{O}_L$, we let $\deg_L \mathfrak{B}$ be the $\mathbb{F}_L$-dimension of the residue class field $\mathbb{F}_{L,\mathfrak{B}} := \mathcal{O}_L/\mathfrak{B}$ of $\mathfrak{B}$, extending this to a general ideal I of $\mathcal{O}_L$ by additivity on products. For a in $\mathcal{O}_L$, we define the *degree* of a by $\deg_L a := \deg_L(a)$, where (a) is the principal ideal of $\mathcal{O}_L$ generated by a.

By a prime $\wp$ (or place) of K, we mean a discrete valuation ring with field of fractions K and maximal ideal $\wp$, and v denotes the discrete valuation associated to a prime $\wp$ of K. Let ∞ be the infinite prime of K with corresponding discrete valuation $v_\infty(f/g) = \deg_K g - \deg_K f$, where $f, g \in A$.

Let τ be the map which raises an element to its qth power. A *Drinfeld A-module ϕ over K* is given by an $\mathbb{F}_q$-algebra homomorphism

$$\phi : A \to K\{\tau\}$$

such that $\phi(a)$ has constant term a for any $a \in A$, and the image of ϕ is not contained in K.

A Drinfeld A-module ϕ of rank r over K is completely determined by

$$\phi(T) = T + a_1(\phi)\tau + a_2(\phi)\tau^2 + \cdots + a_r(\phi)\tau^r,$$

where $a_j(\phi) \in K$ for $j = 1, 2, \ldots, r$ and $a_r(\phi)$ is nonzero. For any *monic* $a \in \mathbb{F}_q[T]$, we then have

$$\phi(a) = a + \sum_{j=1}^{M-1} a_j(\phi, a)\tau^j + \Delta(\phi)^{(q^M-1)/(q^r-1)}\tau^M, \tag{1}$$

for some $a_j(\phi, a) \in K$, where $M = r \deg_K a$ and $\Delta(\phi) := a_r(\phi)$.

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

For any nonzero $a \in A$, we define the A-module of *a-torsion points* as

$$\phi[a] = \{\lambda \in \overline{K} \mid \phi_a(\lambda) = 0\},$$

where ϕ_a denotes $\phi(a)$ and $\overline{K}$ is a fixed separable algebraic closure of K. We have that $\phi[a] \simeq (A/aA)^r$ (see for instance, [23, Proposition 12.4]). If I is a nonzero ideal of A, we similarly define the A-module of *I-torsion points*

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

Let $K(\phi[a])$ be the field obtained by adjoining a-torsion points of ϕ to K, and let $K_{\phi,I} := K(\phi[I])$.

Let $\mathfrak{L}$ be a finite prime of K. The $\mathfrak{L}$-torsion points of ϕ in $\overline{K}$ give rise to a representation

$$\rho_{\phi,\mathfrak{L}} : G_K \to \mathrm{Aut}_{A/\mathfrak{L}}(\phi[\mathfrak{L}]) \cong \mathrm{GL}_r(A/\mathfrak{L}A),$$

where G_K is the absolute Galois group of K. For a prime $\wp$ of K, if ϕ has good reduction at $\wp$, then $\rho_{\phi,\mathfrak{L}}$ is unramified at $\wp$ if $\wp \neq \mathfrak{L}$.

If ϕ is a Drinfeld A-module defined over K, and all its defining coefficients $a_i(\phi)$ lie in A, then we say that ϕ is *integral over A*. If ϕ is integral over A, then it has good reduction outside any set of primes S of K which includes the prime at ∞ and the primes dividing the discriminant $\Delta(\phi)$ of ϕ. In particular, the G_K-modules $\phi[\mathfrak{L}^\infty] := \bigcup_{m \geqslant 1} \phi[\mathfrak{L}^m]$ and $\phi[\mathfrak{L}]$ are unramified outside $S \cup \{\mathfrak{L}\}$.

For a prime $\wp$ of K, let $\mathrm{Frob}_\wp \in G_K$ denote a Frobenius conjugacy class at $\wp$, and let $T_{\mathfrak{L}}(\phi)$ be the *$\mathfrak{L}$-adic Tate module* of ϕ, which is defined as an inverse limit of the $\phi[\mathfrak{L}^n]$, that is, $\varprojlim_n \phi[\mathfrak{L}^n]$.

Let $a_\wp(\phi)$ denote the trace of $\mathrm{Frob}_\wp$ on the $T_{\mathfrak{L}}(\phi)$ and $P_\wp(\phi)(X)$ the characteristic polynomial of $\mathrm{Frob}_\wp$ on the $T_{\mathfrak{L}}(\phi)$ (when the Frobenius conjugacy class is unramified in the relevant extensions). It is known that $a_\wp(\phi)$ and $P_\wp(\phi)(X)$ are independent of $\mathfrak{L}$ [9, Theorem 4.12.12].

The *ring of K-isogenies* of ϕ is denoted by $\mathrm{End}_K(\phi)$, and the *ring of $\overline{K}$-isogenies* is denoted by $\mathrm{End}(\phi)$. We have that $\phi(A) \subseteq \mathrm{End}_K(\phi)$. When ϕ is a Drinfeld A-module of rank 2 over K, $\mathrm{End}(\phi)$ is either $\phi(A)$ or an order $\mathcal{O}$ in some quadratic imaginary extension over K. In the latter case, we say that ϕ has *complex multiplication* (by $\mathcal{O}$).

We use the following notation for Theorem 2.1 and throughout the paper.

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

Notation 1:

$\ln x =$ the natural logarithm of x, $\log_q x =$ the logarithm of x to base q,
$\log_q^* x = \log_q \max\{x, 1\}$,
$c_0 = 9 + \log_q \dfrac{64}{3}$,
$s_q = \dfrac{9\ln(qc_0)}{\ln(qc_0) - 1}$,
$C_q = c_0 + 9\log_q c_0 + s_q\left(\log_q 4 + \log_q(1 + \log_q c_0)\right)$,
ϕ is a Drinfeld A-module over K,
S_ϕ is the set of primes of bad reduction of ϕ over K,
$j(\phi) = \dfrac{a_1(\phi)^{q+1}}{a_2(\phi)}$,
$m =$ the least positive integer such that $-v_\infty(j(\phi)) \leqslant q^{m+1}$,

$$\kappa_\phi = \begin{cases} \dfrac{-v_\infty(j(\phi)) - q^m}{q^m(q-1)} + m - 1 & \text{if } -v_\infty(j(\phi)) > q, \\ 0 & \text{if } -v_\infty(j(\phi)) \leqslant q, \end{cases}$$

$s_1(\phi) = \dfrac{v_\infty(a_1(\phi)) + q}{q - 1}$,
$\tilde{s}_1(\phi) = \dfrac{v_\infty(a_2(\phi)) + q^2}{q^2 - 1}$,
$\delta_\phi =$ the (monic) denominator of $j(\phi)$ as represented by a fraction in reduced form,
$\eta_\phi =$ the product of finite primes $\mathfrak{p}$ of K such that ϕ has bad reduction over $K_\mathfrak{p}$, where $K_\mathfrak{p}$ is the completion at $\mathfrak{p}$ of K.

We state the main result of this paper as follows.

THEOREM 2.1. *Let ϕ be a Drinfeld A-module of rank 2 over K without complex multiplication with $\phi(T) = i(T) + a_1(\phi)\tau + a_2(\phi)\tau^2$, and let q be odd. Let S_ϕ be the set of primes of bad reduction of ϕ over K. Let $\rho_{\phi,\wp}$ be the Galois representation on the $\wp$-torsion points of ϕ, where $\wp$ is a finite prime of K. Let $q_\wp$ be the cardinality of the residue field $A/\wp$. We use notation given in Notation 1.*

If $\rho_{\phi,\wp}$ is not surjective, then either:

(1) $q_\wp \leqslant 5$ *or* $\wp \in S_\phi$,
(2) *or, the image of $\rho_{\phi,\wp}$ lies in the normalizer of a Cartan subgroup of $\mathrm{GL}_2(A/\wp)$ but not in the Cartan subgroup and*

$$\deg_K \wp \leqslant 2(C_q + \widetilde{W} + s_q \log_q(c_0 + \widetilde{W})),$$

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

where

$$\widetilde{W} := \log_q^* 2 \left(\deg_K \eta_\phi + \frac{2}{q-1} \deg_K \delta_\phi + 1 + \kappa_\phi \left(q^{\kappa_\phi + 1} - 1 \right) \right) + \frac{1}{4}((q^2-1)(q^2-q))^2 \left(1 + \frac{\kappa_\phi}{s_1(\phi)} \right)^2,$$

(3) *or, the image of* $\rho_{\phi,\wp}$ *lies in a Borel subgroup of* $\mathrm{GL}_2(A/\wp)$ *and*

$$\deg_K \wp \leqslant \varphi((q-1)(q^2-1)n_\phi) \deg_K P,$$

where φ *denotes the Euler-phi function,* P *is the least degree prime of* K *at which* ϕ *has good reduction, and* $n_\phi \leqslant (q^2-1)(q^2-q)(1+\kappa_\phi/s_1(\phi))$ *is a positive integer.*

This paper is organized as follows. We establish an explicit isogeny theorem for Drinfeld modules of rank 2 in Section 3 which is used in the Cartan case. Some ingredients needed to set up the proof of the main theorem are discussed in Sections 4 and 5. Section 6 (Section 7, respectively) deals with the Cartan case (the Borel case, respectively). The proof of Theorem 2.1 is then given in Section 8.

§3. An explicit isogeny theorem for rank 2

Let L/K be a finite extension. Writing divisors in terms of places instead of primes, the *different divisor* $\mathfrak{D}(L/K)$ of L/K is defined as

$$\mathfrak{D}(L/K) = \sum_w w(D(L_w/K_v))w,$$

and its degree is given by

$$\deg_L \mathfrak{D}(L/K) = \sum_w w(D(L_w/K_v)) \deg_L w,$$

where w ranges through all normalized places of L, and $D(L_w/K_v)$ is the *different ideal* of L_w/K_v. For convenience, we define *the degree with respect to* K of $\mathfrak{D}(L/K)$ as

$$\deg_K \mathfrak{D}(L/K) = \sum_v \max\{v(D(L_w/K_v)) : w|v\} \deg_K v,$$

where v ranges through all normalized places of K.

The following theorem presents an upper bound on the degree of the different divisor $\mathfrak{D}(K(\phi[a])/K)$ of $K(\phi[a])$ over K based on work from [2, 3].

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

THEOREM 3.1. *Let ϕ be a Drinfeld A-module of rank 2 over K with $\phi(T) = i(T) + a_1(\phi)\tau + a_2(\phi)\tau^2$ and a be nonzero in A. Let $j(\phi)$, m, κ_ϕ, δ_ϕ and η_ϕ be the same as given in Notation 1. Let $\mathfrak{D}(K(\phi[a])/K)$ be the different divisor of the torsion field $K(\phi[a])$ over K. Then*

$$\deg_K \mathfrak{D}(K(\phi[a])/K) \leqslant 2\deg_K a + \deg_K \eta_\phi + \frac{2}{q-1} \times \deg_K \delta_\phi + 1 + \kappa_\phi(q^{\kappa_\phi+1} - 1). \tag{2}$$

Proof. See [2, 3]. □

We have an upper bound on the extension degree of the constant field of $K(\phi[a])$ over $\mathbb{F}_q$ as follows.

THEOREM 3.2. *Let ϕ be a Drinfeld A-module of rank 2 over K with $\phi(T) = i(T) + a_1(\phi)\tau + a_2(\phi)\tau^2$ and a be nonzero in A. Let $j(\phi)$, m and κ_ϕ be the same as given in Notation 1. Let $\gamma_{\phi,a} := [\mathbb{F}_{K(\phi[a])} : \mathbb{F}_q]$, where $\mathbb{F}_{K(\phi[a])}$ denotes the algebraic closure of $\mathbb{F}_q$ in $K(\phi[a])$ (that is, $\mathbb{F}_{K(\phi[a])}$ is the constant field of $K(\phi[a])$). Then we have*

$$\gamma_{\phi,a} \leqslant (q^2-1)(q^2-q)(1 + \frac{\kappa_\phi}{s_1(\phi)}), \tag{3}$$

where $s_1(\phi) = (v_\infty(a_1(\phi)) + q)/(q-1)$.

Proof. Let $g_{\phi,\infty} = [K_\infty(\Lambda_{\phi,\infty}) : K_\infty]$, where K_∞ denotes the completion at ∞ of K, C_∞ denotes the completion of an algebraic closure of K_∞ and $\Lambda_{\phi,\infty}$ is the lattice associated to the uniformization of ϕ over C_∞. As $K_\infty(\Lambda_{\phi,\infty})$ contains $\phi[a]$ and $\mathbb{F}_{K_\infty} = \mathbb{F}_K$, we have that

$$[\mathbb{F}_{K(\phi[a])} : \mathbb{F}_K] \leqslant [\mathbb{F}_{K_\infty(\Lambda_{\phi,\infty})} : \mathbb{F}_{K_\infty}] \leqslant [K_\infty(\Lambda_{\phi,\infty}) : K_\infty].$$

Hence, $\gamma_{\phi,a} \leqslant g_{\phi,\infty}$.

One can bound $g_{\phi,\infty}$ using knowledge of the successive minima of the lattice $\Lambda_{\phi,\infty}$ associated to ϕ [12, Proposition 4(i)]. Concerning the term $g_{\phi,\infty}$, we have from [12] that

$$g_{\phi,\infty} \leqslant (q^2-1)(q^2-q)\nu_{2,\infty}(\phi)/\nu_{1,\infty}(\phi),$$

where $\nu_{i,\infty}(\phi)$ is the *ith successive minima* of ϕ associated to its uniformization over C_∞. From [2], an explicit bound for these successive minima $\nu_{i,\infty}(\phi)$ is determined as follows:

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

Case 1: If $-v_\infty(j(\phi)) \leqslant q$, then $\nu_{1,\infty}(\phi) = \nu_{2,\infty}(\phi) = -\tilde{s}_1(\phi)$,

Case 2: If $q < -v_\infty(j(\phi)) \leqslant q^{m+1}$, then $\nu_{1,\infty}(\phi) = -s_1(\phi)$ and $\nu_{2,\infty}(\phi) = -s_1(\phi) - \kappa_\phi$, where notations for $s_1(\phi)$ and $\tilde{s}_1(\phi)$ are given in Notation 1.

Combining all these yields the result. □

REMARK 3.3. Under the assumptions of Theorem 3.2, if $-v_\infty(j(\phi)) \leqslant q$, then $\gamma_\phi \leqslant (q^2-1)(q^2-q)$, and if $q < -v_\infty(j(\phi)) \leqslant q^{m+1}$, then we see that

$$\gamma_{\phi,a} \leqslant (q^2-1)(q^2-q)\left(1 + \frac{m(q-1)}{v_\infty(a_1(\phi)) + q}\right).$$

Recall the isogeny theorem for Drinfeld A-modules, proven in [27, Proposition 3.1].

THEOREM 3.4. *Let ϕ and ϕ' be rank r Drinfeld A-modules over K. Then ϕ and ϕ' are K-isogenous if and only if $P_\wp(\phi)(X) = P_\wp(\phi')(X)$ for all but finitely many primes $\wp$ of K.*

The following theorem is an explicit and effective version of the isogeny theorem for rank 2 Drinfeld A-modules over K. The proof of Theorem 3.5 is similar to that of [3, Theorem 1.2], except that it uses more refined and explicit bound on the different divisor and the degree of constant field extensions given in Theorems 3.1 and 3.2. For completeness, we summarize the proof to explain and justify all the new constants, for example, c_0, s_q, C_q, κ_{ϕ_i}, $s_1(\phi_i)$, δ_{ϕ_i}, which arise.

THEOREM 3.5. *Let ϕ_1 and ϕ_2 be Drinfeld A-modules of rank 2 over K which are not K-isogenous with $\phi_i(T) = T + a_1(\phi_i)\tau + a_2(\phi_i)\tau^2$ for $i = 1, 2$. Let $j(\phi_i) = a_1(\phi_i)^{q+1}/a_2(\phi_i)$ and m_i be the least positive integer such that $-v_\infty(j(\phi_i)) \leqslant q^{m_i+1}$ for $i = 1, 2$. Let $S = S_{\phi_1} \cup S_{\phi_2} \cup \{\infty\}$ be the set of primes of bad reduction of ϕ_1 or ϕ_2 over K together with the infinite prime ∞ of K.*

Assume that $\wp \notin S$ is a prime of K of least degree such that $P_\wp(\phi_1) \neq P_\wp(\phi_2)$. Then we have

$$\deg_K \wp \leqslant 4\left(C_q + W + s_q \log_q(c_0 + W)\right), \tag{4}$$

where we let c_0, s_q, C_q, $\kappa_{\phi_i}, s_1(\phi_i), \delta_{\phi_i}$ and η_{ϕ_i} for each ϕ_i, $i = 1, 2$ be the same as given in Notation 1, and

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

$$W = \log_q^* \Bigg(\deg_K \eta_{\phi_1}\eta_{\phi_2} + \frac{2}{q-1}\deg_K \delta_{\phi_1}\delta_{\phi_2} + 2 + \kappa_{\phi_1}\left(q^{\kappa_{\phi_1}+1}-1\right) + \kappa_{\phi_2}\left(q^{\kappa_{\phi_2}+1}-1\right)\Bigg) + \frac{1}{4}((q^2-1)(q^2-q))^2\left(1+\frac{\kappa_{\phi_1}}{s_1(\phi_1)}\right)\left(1+\frac{\kappa_{\phi_2}}{s_1(\phi_2)}\right).$$

Proof. Let $\wp \notin S$ be a prime of K with least degree such that $P_\wp(\phi_1) \neq P_\wp(\phi_2)$ (which exists from the hypotheses and Theorem 3.4). Let α_0 be a nonzero coefficient of $P_\wp(\phi_1) - P_\wp(\phi_2)$. It is known that a root γ of $P_\wp(\phi_1)$ or $P_\wp(\phi_2)$ satisfies

$$v_\infty(\gamma) = -\tfrac{1}{2}\deg_K \wp,$$

(cf. [10, Theorem 3.2.3(c)(d)], [12, Proposition 9]). This implies that each coefficient β of $P_\wp(\phi_1)$ and $P_\wp(\phi_2)$ satisfies $\deg_K \beta \leqslant \deg_K \wp$, and hence each coefficient α of $P_\wp(\phi_1) - P_\wp(\phi_2)$ also satisfies $\deg_K \alpha \leqslant \deg_K \wp$, in particular $\deg_K \alpha_0 \leqslant \deg_K \wp$.

We choose a finite prime $\mathfrak{L}$ of K by [3, Lemma 5.2] such that

$$\alpha_0 \not\equiv 0 \pmod{\mathfrak{L}} \quad \text{and} \quad \deg_K \mathfrak{L} \leqslant 1 + \log_q \deg_K \wp, \tag{5}$$

and write $\mathfrak{L} = (a)$, where a is monic in A. Note that either $\deg_K \wp \leqslant 2$ or $\mathfrak{L} \neq \wp$ by the above inequality.

Suppose we are now in the latter case where $\mathfrak{L} \neq \wp$. Consider the representation

$$\psi_\mathfrak{L} : G_K \to \mathrm{Aut}_{A/\mathfrak{L}}(\phi_1[\mathfrak{L}]) \times \mathrm{Aut}_{A/\mathfrak{L}}(\phi_2[\mathfrak{L}]) \cong \mathrm{GL}_2(A/\mathfrak{L}) \times \mathrm{GL}_2(A/\mathfrak{L}),$$

where $\psi_\mathfrak{L} = \rho_{\phi_1,\mathfrak{L}} \times \rho_{\phi_2,\mathfrak{L}}$. Let $G_\mathfrak{L}$ be the image of this homomorphism. Let $C_\mathfrak{L}$ be the subset of $G_\mathfrak{L}$ consisting of pairs $(\mathfrak{a}, \mathfrak{b})$ such that the characteristic polynomials of $\mathfrak{a}$ and $\mathfrak{b}$ are not equal. Note that $C_\mathfrak{L}$ is invariant under conjugation, so it is a union of conjugacy classes in $G_\mathfrak{L}$. Since $\mathfrak{L} \neq \wp$, we have that $C_\mathfrak{L} \neq \emptyset$, and in particular, there is some conjugacy class $\mathcal{C} \subseteq C_\mathfrak{L}$ in $G_\mathfrak{L}$ with $\mathcal{C} \neq \emptyset$.

Let $S_\mathfrak{L} = S \cup \{\mathfrak{L}\}$. Then the Galois representation $\psi_\mathfrak{L}$ is unramified outside $S_\mathfrak{L}$. We have that $A/\mathfrak{L} \cong \mathbb{F}_\ell$ where $\ell = q^{\deg_K \mathfrak{L}}$. Let $\widetilde{K}/K$ be the field extension associated to $\psi_\mathfrak{L}$, and let n (resp. n') be its extension degree (resp. geometric extension degree). By an explicit Chebotarev argument

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

as in [3, Theorem 1.2], we deduce that there is a prime $P \notin S_{\mathfrak{L}}$ such that $\mathrm{Frob}_P = \mathcal{C} \subseteq C_{\mathfrak{L}}$ and

$$\deg_K P \leqslant 4 \log_q \tfrac{4}{3}(B+3) + m, \tag{6}$$

where

$$\Sigma' := \sum_{\mathfrak{p} \in S_{\mathfrak{L}}} \mathfrak{p} \geqslant \Sigma := \sum_{\mathfrak{p} \in S} \mathfrak{p}, \quad m = [\mathbb{F}_{\widetilde{K}} : \mathbb{F}_K],$$

$$\deg_K \Sigma' \leqslant \deg_K \eta_{\phi_1}\eta_{\phi_2} + \deg_K \mathfrak{L} + 1, \tag{7}$$

$$\mathfrak{D} = \mathfrak{D}(\widetilde{K}/K) \text{ is the different divisor } of \widetilde{K}/K,$$

$$B = \max\left\{\deg_K \Sigma', \deg_{\widetilde{K}} \mathfrak{D}, 2\right\}.$$

By using the explicit bound on the different divisor $\mathfrak{D}$ in Theorem 3.1, we obtain

$$\deg_{\widetilde{K}} \mathfrak{D} \leqslant n' \left(4 \deg_K a + \deg_K \eta_{\phi_1}\eta_{\phi_2} + \frac{2}{q-1} \deg_K \delta_{\phi_1}\delta_{\phi_2} + \epsilon_{\phi_1,\phi_2}\right), \tag{8}$$

$$\text{where} \quad \epsilon_{\phi_1,\phi_2} := 2 + \kappa_{\phi_1}\left(q^{\kappa_{\phi_1}+1} - 1\right) + \kappa_{\phi_2}\left(q^{\kappa_{\phi_2}+1} - 1\right).$$

Then from (6) and (7), we note that B is bounded above by the upper bound of $\deg_{\widetilde{K}} \mathfrak{D}$ in (8); thus we have that

$$\log_q \frac{4}{3}B \leqslant \log_q n' + \log_q \frac{16}{3} + \log_q(\log_q \ell) + \log_q^* \times \left(\deg_K \eta_{\phi_1}\eta_{\phi_2} + \frac{2}{q-1} \deg_K \delta_{\phi_1}\delta_{\phi_2} + \epsilon_{\phi_1,\phi_2}\right).$$

(We use the inequality $\log_q(x+y) \leqslant \log_q x + \log_q y$ for $x, y \geqslant 2$; in more detail, in (8), both $4 \deg_K a$ and the other terms, $\deg_K \eta_{\phi_1}\eta_{\phi_2} + (2/(q-1)) \deg_K \delta_{\phi_1}\delta_{\phi_2} + \epsilon_{\phi_1,\phi_2}$, are greater than 2 since $\epsilon_{\phi_1,\phi_2} > 2$.)

We note that $n' \leqslant n = |G_{\mathfrak{L}}| < \ell^8$, so $\log_q n' < 8 \log_q \ell$. Returning to (6), we obtain

$$\begin{aligned}
\deg_K P &\leqslant 4\Bigg(\log_q \frac{64}{3} + \log_q(\log_q \ell) + 8 \log_q \ell \\
&\quad + \log_q^*\left(\deg_K \eta_{\phi_1}\eta_{\phi_2} + \frac{2}{q-1} \deg_K \delta_{\phi_1}\delta_{\phi_2} + \epsilon_{\phi_1,\phi_2}\right)\Bigg) + m \\
&\leqslant 4\Bigg(\log_q \frac{64}{3} + 9 \log_q \ell + \log_q^*\Bigg(\deg_K \eta_{\phi_1}\eta_{\phi_2} \\
&\quad + \frac{2}{q-1} \deg_K \delta_{\phi_1}\delta_{\phi_2} + \epsilon_{\phi_1,\phi_2}\Bigg)\Bigg) + m.
\end{aligned}$$

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

By construction of $C_{\mathfrak{L}}$, we have that $P_P(\phi_1) \not\equiv P_P(\phi_2) \pmod{\mathfrak{L}}$. Thus, we have $\deg_K \wp \leqslant \deg_K P$, and from (5), it follows that

$$\begin{aligned}\deg_K \wp \leqslant 4\Bigg(&\log_q \frac{64}{3} + 9(1 + \log_q \deg_K \wp) + \log_q^* \\ &\times \left(\deg_K \eta_{\phi_1}\eta_{\phi_2} + \frac{2}{q-1} \deg_K \delta_{\phi_1}\delta_{\phi_2} + \epsilon_{\phi_1,\phi_2} \right) + \frac{m}{4} \Bigg).\end{aligned} \tag{9}$$

As $1 + \log_q y \geqslant 1$ and $(\log_q y)/y \leqslant 1$, we have that

$$\frac{\deg_K \wp}{1 + \log_q(\deg_K \wp)} \leqslant 4(c_0 + W_0),$$

where $c_0 := 9 + \log_q (64/3)$ and $W_0 := \log_q^*(\deg_K \eta_{\phi_1}\eta_{\phi_2} + (2/(q-1)) \deg_K \delta_{\phi_1}\delta_{\phi_2} + \epsilon_{\phi_1,\phi_2}) + m/4$.

Thus, (9) can be written as follows:

$$\deg_K \wp \leqslant 4(c_0 + W_0 + 9 \log_q \deg_K \wp). \tag{10}$$

Let $t^* = (\ln(qc_0) - 1)/\ln(qc_0)$ and $s^* = 1/t^* = \ln(qc_0)/(\ln(qc_0) - 1)$. If $x := \deg_K \wp \geqslant c_0$, then using [3, Lemma 5.3 and the calculation in (32)] with $c^* = c_0$, we see that

$$\begin{aligned}\log_q \deg_K \wp = \log_q x &\leqslant \frac{1}{t^*} \log_q \left(4(c_0 + W_0) \frac{1 + \log_q c_0}{c_0^{1/\ln(qc_0)}} \right) \\ &\leqslant s^* \left(\log_q 4 + \log_q(c_0 + W_0) + \log_q(1 + \log_q c_0) \right) \\ &\quad + \left(\frac{1}{1 - \ln(qc_0)} \right) \log_q c_0 \\ &\leqslant s^* \left(\log_q 4 + \log_q(c_0 + W_0) + \log_q(1 + \log_q c_0) \right) \\ &\quad + \log_q c_0. \end{aligned} \tag{11}$$

Substitution of (11) into (10) yields

$$\tfrac{1}{4} \deg_K \wp \leqslant C_q + W_0 + 9s^* \log_q(c_0 + W_0), \tag{12}$$

where $C_q := c_0 + 9 \log_q c_0 + 9s^* \left(\log_q 4 + \log_q(1 + \log_q c_0) \right)$.

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

Finally, from Theorem 3.2, it follows that $m \leqslant \gamma_{\phi_1}\gamma_{\phi_2}$ and

$$\gamma_{\phi_1}\gamma_{\phi_2} \leqslant ((q^2-1)(q^2-q))^2 \left(1+\frac{\kappa_{\phi_1}}{s_1(\phi_1)}\right)\left(1+\frac{\kappa_{\phi_2}}{s_1(\phi_2)}\right).$$

Therefore, we either have the above upper bound (12) on $\deg_K \wp$ or $\deg_K \wp \leqslant c_0 \leqslant C_q$; so in the end, we get

$$\deg_K \wp \leqslant 4\left(C_q + W + s_q \log_q(c_0+W)\right), \tag{13}$$

where $s_q = 9s^*$. The result thus follows as desired. □

§4. Twists of Drinfeld modules

Let L/K be an extension where $K = \mathbb{F}_q(T)$. Suppose that ϕ and ϕ' are rank r Drinfeld A-modules over K given by

$$\phi(T) = \sum_{j=0}^{r} a_j \tau^j \qquad \text{and} \qquad \phi'(T) = \sum_{j=0}^{r} a'_j \tau^j.$$

Then ϕ and ϕ' are isomorphic over L if and only if there is a $c \in L^*$ such that

$$\phi'(T)c = \left(\sum_{i=0}^{r} a'_j \tau^j\right) c = c\left(\sum_{j=0}^{r} c^{q^j-1} a'_j \tau^j\right) = c\phi(T).$$

Explicitly, this implies that $a'_j = a_j/c^{q^j-1}$ for any $j = 0, 1, \ldots, r$. Here $c \in L^*$ is regarded as an element of $\mathrm{Hom}_L(\phi, \phi')$ and induces a map $L \to L$ as Drinfeld A-modules by $x \mapsto cx$, where the first L is an A-module under ϕ and the second under ϕ'.

LEMMA 4.1. *Let $K = \mathbb{F}_q(T)$ and q be odd. For Drinfeld A-modules ϕ, ϕ' of rank r over K, suppose there is an isomorphism $f(x) = cx$ from ϕ to ϕ' given by $c\phi_a = \phi'_a c$, where $c = \delta^{1/(q-1)}$ for some $\delta \in K^*$. Let $\epsilon : G_K \to \mathbb{F}_q^\times$ denote the Galois character such that $\sigma(c) = \epsilon(\sigma)c$ for $\sigma \in G_K$. Let $\phi[a]$ and $\phi'[a]$ be the A-modules of a-torsion points of ϕ, ϕ' with $a \in A$ nonzero and let*

$$\rho_{\phi,a} : G_K \to \mathrm{GL}(\phi[a]), \quad \rho_{\phi',a} : G_K \to \mathrm{GL}(\phi'[a])$$

be their associated mod a representations. Then $\rho_{\phi',a} \cong \rho_{\phi,a} \otimes \epsilon$.

Proof. Let $\psi : \phi[a] \to \phi'[a]$ be the isomorphism induced by f, namely $P \mapsto cP$, where $P \in \phi[a]$. For $P \in \phi[a]$, we then have that $\rho_{\phi',a}(\sigma)(\psi(P)) = \rho_{\phi',a}(\sigma)cP = \sigma(cP) = \sigma(c)\sigma(P) = \epsilon(\sigma)c\sigma(P) = \epsilon(\sigma)\psi(\rho_{\phi,a}(\sigma)(P))$, hence the result follows. □

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

In the above lemma, we call the resulting ϕ' *the twist* of ϕ by ϵ.

LEMMA 4.2. *Let ϕ, ϕ' be Drinfeld A-modules of rank r over $K = \mathbb{F}_q(T)$, and suppose that ϕ' is the twist of ϕ by a nontrivial character $\epsilon : G_K \to \mathbb{F}_q^\times$. Assume that* $\mathrm{End}(\phi) = \phi(A)$ *(that is, ϕ has no complex multiplication). Then ϕ and ϕ' are not K-isogenous.*

Proof. We note that there is an isomorphism $\psi : \phi' \to \phi$ defined over $\overline{K}$ but not over K. Explicitly, it is given by the element $c \in \overline{K}^*$ but not in K^* such that $c\phi'(a) = \phi(a)c$ for all $a \in A$.

Suppose there is a K-isogeny $\lambda : \phi \to \phi'$. Explicitly, there is a $g \in K\{\tau\}$ such that $g\phi(a) = \phi'(a)g$ for all $a \in A$. Hence, $\psi \circ \lambda : \phi \to \phi$ is given by cg so that $(cg)\phi(a) = \phi(a)(cg)$ for all $a \in A$. We may assume now that $cg \in \phi(A)$ or else $\mathrm{End}(\phi)$ is strictly bigger than $\phi(A)$. Hence, $cg = \phi(m)$ for some $m \in A$. But this means that $c \in K\{\tau\}$, contradicting the fact that $c \in \overline{K}^*$ but not in K^*. □

LEMMA 4.3. *Let ϕ_1, ϕ_2 be Drinfeld A-modules of rank 2 over $K = \mathbb{F}_q(T)$, and suppose ϕ_2 is the twist of ϕ_1 by a nontrivial character $\epsilon : G_K \to \mathbb{F}_q^\times$ which is ramified on a subset of the set of primes of bad reduction of ϕ_1. Then the bound on the different divisor for $K(\phi_2[a])/K$ from Theorem 3.1 can be taken to be the bound on the different divisor for $K(\phi_1[a])/K$ from Theorem 3.1.*

Proof. This follows from the fact that the dependence of the bounds from Theorem 3.1 on ϕ is only through the j-invariant of ϕ and the set of primes of bad reduction of ϕ. □

§5. Semi-stable reduction in rank 2 and Weil pairings

Let P be a finite prime of K, K_P be the completion at P of K and $\mathcal{O}_P \subseteq K_P$ be the valuation ring of P. We say that a Drinfeld A-module ϕ of rank 2 over K has *stable reduction* at P if there exists a Drinfeld module ϕ' over K_P which is integral over $\mathcal{O}_P$ such that its reduction modulo P defines a Drinfeld module over $\mathcal{O}_P/P$ and ϕ' is isomorphic to ϕ over K_P. Furthermore, we say that ϕ has *good reduction* at P if ϕ has stable reduction at P such that $P \nmid a_2(\phi)$, otherwise we say that ϕ has *bad reduction* at P. If ϕ has bad reduction at P, but has stable reduction over $\mathcal{O}_P$ such that $P \nmid a_1(\phi)$, we say that ϕ has *bad Tate reduction* at P. If ϕ has good reduction, or bad Tate reduction at P, we say that ϕ is *semi-stable reduction* at P.

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

LEMMA 5.1. *Let P be a finite prime of K and $\mathcal{O}_P \subseteq K_P$ be the valuation ring of P. Let ϕ be a Drinfeld A-module of rank 2 over K, with $\phi(T) = i(T) + a_1(\phi)\tau + a_2(\phi)\tau^2$, and $a_1(\phi), a_2(\phi) \in \mathcal{O}_P$. Then there is a finite tamely ramified extension K'/K_P such that ϕ attains semi-stable reduction over K' and the degree of $K_P^{nr} \cdot K'/K_P^{nr}$ divides $q^2 - 1$, where K_P^{nr} is the maximal unramified extension of K_P.*

Proof. A twist ϕ' of ϕ has the form:

$$\begin{aligned}\phi'(T) &= T + a_1(\phi')\tau + a_2(\phi')\tau^2 \\ &= T + a_1(\phi)c^{q-1}\tau + a_2(\phi)c^{q^2-1}\tau^2.\end{aligned}$$

Let $\pi \in \mathcal{O}_P$ be a uniformizer, and let v be the corresponding valuation at P of K which we extend to $\overline{K}$.

Recall $j(\phi) = a_1(\phi)^{q+1}/a_2(\phi)$.

Case $v(j(\phi)) \geqslant 0$: Let $c = 1/\pi^{v(a_2(\phi))/(q^2-1)}$. The corresponding twist ϕ' over K' then has $v(a_1(\phi')) = v(a_1(\phi)c^{q-1}) \geqslant 0$ and $v(a_2(\phi')) = v(a_2(\phi)c^{q^2-1}) = 0$, where $K' = K_P(\pi^{v(a_2(\phi))/(q^2-1)})$. Hence, ϕ' has good reduction over K'.

Case $v(j(\phi)) < 0$: Let $c = 1/\pi^{v(a_1(\phi))/(q-1)}$. The corresponding twist ϕ' then has $v(a_1(\phi')) = v(a_1(\phi)c^{q-1}) = 0$ and $v(a_2(\phi')) = v(a_2(\phi)c^{q^2-1}) > 0$, where $K' = K_P(\pi^{v(a_1(\phi))/(q-1)})$. Hence, ϕ' has bad Tate reduction over K'.

In both cases, K'/K_P is tamely ramified and the degree of $K_P^{\mathrm{nr}} \cdot K'/K_P^{\mathrm{nr}}$ divides $q^2 - 1$. □

THEOREM 5.2. *Let ϕ be a Drinfeld A-module over K of rank 2 with $\phi(T) = i(T) + a_1(\phi)\tau + a_2(\phi)\tau^2$, q be odd, and let ψ be the Drinfeld A-module over K of rank 1 defined by $\psi(T) = T - a_2(\phi)\tau$. If $\wp$ is a finite prime of K, then we have that*

$$\det \rho_{\phi,\wp} = \rho_{\psi,\wp}.$$

Proof. This follows by combining the second part of [31, Theorem 5.3] and [31, Proposition 7.4], under the assumption that ϕ has rank 2 and $A = \mathbb{F}_q[T]$. It can also be deduced by showing that $\det \rho_{\phi,\wp}$ and $\rho_{\psi,\wp}$ coincide on Frobenius elements using [8, Theorem 2.11], again under the assumption that ϕ has rank 2 and $A = \mathbb{F}_q[T]$, so by the Chebotarev density theorem, the two Galois characters are the same. □

For a definition of the Weil pairing between a Drinfeld A-module and its dual, see [22].

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

We use the convention $\chi(P) := \chi(\mathrm{Frob}_P)$ for a Galois character $\chi : G_K \to (A/\wp)^\times$.

PROPOSITION 5.3. *Under the hypothesis of Theorem 5.2, we have that*

$$\det \rho_{\phi,\wp}(\mathrm{Frob}_P) = \rho_{\psi,\wp}(\mathrm{Frob}_P) \equiv \epsilon_0(P)P \pmod{\wp},$$

for all P not in S_ϕ and $P \neq \wp, \infty$, where $\epsilon_0 : G_K \to \mathbb{F}_q^\times \subseteq (A/\wp)^\times$ is a Galois character.

Proof. Note that ψ is isomorphic to the Carlitz module $C(T) = T + \tau$ over $K(c)$, where $c = (-a_2(\phi))^{1/(q-1)}$, that is, $C \circ f = f \circ \psi$ where $f(z) = cz$. Thus, we have that $\rho_{\psi,\wp} = \rho_{C,\wp} \otimes \epsilon_0$, where $\epsilon_0 : G_K \to \mathbb{F}_q^\times$ giving the action of G_K on c.

Now, $C[P] \cong A/P$ and the elements of $(A/P)^\times$ correspond to the roots of $C(P)(X)/X$.

Furthermore, from [23, Theorem 12.10], we have that $C(P)(X)/X \in A[X]$ is an Eisenstein polynomial for the prime P. Hence, $C(P)(X) \equiv X^{|P|} \pmod{P}$, where $|P| = q^{\deg_K P}$.

Let $\mathfrak{P}$ be a prime of $K(C[\wp])$ lying above P. We then have that $C(P)(X) \equiv X^{|P|} \pmod{\mathfrak{P}}$.

Let λ be a generator for $C[\wp]$. Since $\mathrm{Frob}_P(\lambda) \equiv \lambda^{|P|} \pmod{\mathfrak{P}}$ and $C(P)(\lambda) \equiv \lambda^{|P|} \pmod{\mathfrak{P}}$, we have that $\rho_{C,\wp}(\mathrm{Frob}_P) \equiv P \pmod{\wp}$.

Thus, we get that $\det \rho_{\phi,\wp}(\mathrm{Frob}_P) = \rho_{\psi,\wp}(\mathrm{Frob}_P) = \rho_{C,\wp} \otimes \epsilon_0(\mathrm{Frob}_P) \equiv \epsilon_0(P)P \pmod{\wp}$. ∎

§6. The Cartan case

In this section, we assume throughout that *q is odd*.

Let ϕ be a Drinfeld A-module of rank 2 over K without complex multiplication, and let $\wp$ be a finite prime of K. In this section, we suppose throughout that the image of $\rho_{\phi,\wp}$ lies in the normalizer $\mathcal{N}$ of a Cartan subgroup $\mathcal{C}$ of $\mathrm{GL}_2(A/\wp)$ but not in $\mathcal{C}$.

Consider the associated character $\epsilon_\wp : G_K \to \{\pm 1\}$ obtained by applying $\rho_{\phi,\wp}$ and then the quotient map $\mathcal{N}/\mathcal{C} \cong \{\pm 1\}$. Let K'/K be the quadratic extension associated to $\epsilon_\wp$.

Gardeyn studies the image of the inertia group $I_{K_\wp}$ of $\rho_{\phi,\wp}$ at the finite prime $\wp$ of K [11, Theorem 2.23, Corollary 2.24]. He shows the following theorem, where we do not need the assumption that the image of $\rho_{\phi,\wp}$ lies in the normalizer $\mathcal{N}$ of a Cartan subgroup $\mathcal{C}$ of $\mathrm{GL}_2(A/\wp)$ but not in $\mathcal{C}$.

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

THEOREM 6.1. *Let ϕ be a Drinfeld A-module of rank 2 over K with good reduction at $\wp$ and $I_{K_\wp}$ be the inertia group at $\wp$ of K. Then $\rho_{\phi,\wp}(I_{K_\wp})$ is*

(1) *a nonsplit Cartan subgroup of order $q_\wp^2 - 1$ (if ϕ has good reduction at $\wp$ of height 2);*
(2) *a semisplit Cartan or semisplit Borel subgroup of order divisible by $q_\wp - 1$ (if ϕ has good reduction at $\wp$ of height 1),*

where $q_\wp$ is the size of the residue field $A/\wp$.

Proof. See [21, Proposition 2.7], [11, Theorem 2.23, Corollary 2.24], [24, Proposition 11, 12, 13]. □

REMARK 6.2. The elliptic curve analogue of the above theorem is described in [24, Proposition 11, 12, 13]. The reader may be curious about the situation of bad Tate reduction at $\wp$. For elliptic curves, one knows by [24, Proposition 13], that $\rho_{E,p}(I_p)$ lies in a semisplit Borel subgroup if E has bad multiplicative reduction at p. However, for Drinfeld modules, we only have that $\rho_{\phi,\wp}(I_\wp)$ lies in a Borel subgroup, for reasons that we explain below.

If ϕ has bad Tate reduction at $\wp$, then over $C_\wp$, where $C_\wp$ is the completion of an algebraic closure of $K_\wp$, we have a uniformization [6] given by a surjective analytic map $e_\wp : C_\wp \to C_\wp$ which relates ϕ to a Drinfeld A-module ψ of rank 1 with good reduction at $\wp$ via the relation $\psi_a \circ e_\wp = e_\wp \circ \phi_a$. Let $\Lambda_\wp$ be the set of zeros of $e_\wp$. Then by [6], $\Lambda_\wp = A \cdot \lambda_1$ is an A-lattice in $C_\wp$ of rank 1, where the A-module structure on $C_\wp$ is given by $\alpha \cdot x := \psi_\alpha(x)$.

Write $\wp = (a)$. The analytic map $e_\wp$ is $G_{K_\wp}$-equivariant and induces an isomorphism $\psi_\wp^{-1}(\Lambda_\wp)/\Lambda_\wp \cong \phi[\wp]$. We also have an exact sequence

$$0 \to \psi[\wp] \to \psi_a^{-1}(\Lambda_\wp)/\Lambda_\wp \to \Lambda_\wp/a \cdot \Lambda_\wp \to 0.$$

Thus, $\rho_{\phi,\wp}$ has the form

$$\rho_{\phi,\wp} = \begin{pmatrix} \chi' & * \\ 0 & \chi'' \end{pmatrix},$$

where $\chi' \cong \rho_{\psi,\wp}$. Since ψ is of rank 1 and has good reduction at $\wp$, by application of [21, Proposition 2.7], we see that $\chi'_{|I_\wp}$ has image $\mathbb{F}_\wp^\times = (A/\wp)^\times$.

Since $\Lambda_\wp$ is $G_{K_\wp}$-invariant, we have that

$$\sigma(\lambda_1) = \chi''(\sigma)\lambda_1,$$

where $\sigma \in G_{K,\wp}$ and $\chi''(\sigma) \in A^\times = \mathbb{F}_q^\times$. This implies that $\lambda_1^{q-1} = c \in K_\wp^*$. Now, χ'' is unramified at $\wp$ if and only if $v_\wp(c) \equiv 0 \pmod{q-1}$:

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

Write $c = u\pi^{(q-1)k+r}$, where $0 \leqslant r < q-1$, π is a uniformizer for $K_\wp$, and u is a unit in $K_\wp$. Then $\lambda_1 = u^{1/(q-1)}\pi^k\pi^{r/(q-1)}$, which lies in $K_\wp^{\mathrm{nr}}$ or $K_\wp^{\mathrm{nr}}(\pi^{r/(q-1)}) = K_\wp^{\mathrm{nr}}(\pi^{1/(q-1)})$ accordingly as $r = 0$ or $r \neq 0$. In the former case, $K_\wp^{\mathrm{nr}}(\lambda_1) = K_\wp^{\mathrm{nr}}$ is unramified, and in the latter case, $K_\wp^{\mathrm{nr}}(\lambda_1) = K_\wp^{\mathrm{nr}}(\pi^{1/(q-1)})$ is tamely ramified.

Thus, in general both χ' and χ'' are ramified at $\wp$.

LEMMA 6.3. *Suppose $\wp \notin S_\phi$ and $q_\wp \geqslant 5$. Then the character $\epsilon_\wp$ is unramified at $\wp$.*

Proof. Using Theorem 6.1, $\rho_{\phi,\wp}(I_{K_\wp})$ is a nonsplit Cartan subgroup, semisplit Cartan subgroup, or semisplit Borel subgroup. In the first case, we obtain that $\epsilon_\wp(I_{K_\wp}) = 1$ by definition of $\epsilon_\wp$.

Recall we are under the running assumption that $\rho_{\phi,\wp}$ has image contained in the normalizer of a Cartan subgroup $\mathcal{N}$. Hence, the last case does not occur as no semisplit Borel subgroup can be contained in $\mathcal{N}$.

In the second case, $\rho_{\phi,\wp}(I_{K_\wp})$ is a semisplit Cartan subgroup contained in $\mathcal{N}$. As $q_\wp \geqslant 5$, it follows that $\rho_{\phi,\wp}(I_{K_\wp})$ is the unique such semisplit Cartan subgroup in $\mathcal{N}$ (the proof in [24, Proposition 14] works for general finite fields). Since this semisplit Cartan subgroup is contained in $\mathcal{C}$, we have that $\epsilon_\wp(I_{K_\wp}) = 1$. □

COROLLARY 6.4. *Assume the notation and hypotheses of Lemma 6.3. Let ϕ' be the twist of ϕ by the character $\epsilon_\wp$. Then*

$$\deg_K \eta_\phi\eta_{\phi'} = \deg_K \eta_\phi^2 = 2\deg_K \eta_\phi,$$

and in fact, $\eta_\phi = \eta_{\phi'}$.

Proof. The character $\epsilon_\wp$ is unramified outside the set of primes containing ∞ and the primes which divide η_ϕ. Thus, $\eta_{\phi'} \mid \eta_\phi$ from Lemma 4.1. On the other hand, ϕ is the twist of ϕ' by $\epsilon_\wp$ as well, so we obtain $\eta_\phi \mid \eta_{\phi'}$. □

Let ϕ' be the twist of ϕ by the character $\epsilon_\wp$, and let S denote a set of primes outside of which both ϕ and ϕ' have good reduction. We have that

$$\rho_{\phi',\wp} \cong \rho_{\phi,\wp} \otimes \epsilon_\wp \tag{14}$$

by Lemma 4.1 as ϕ' is the twist of ϕ by $\epsilon_\wp$. Thus, $a_P(\phi') = a_P(\phi)\epsilon_\wp(\mathrm{Frob}_P)$, where $a_\wp(\phi)$ denotes the trace of a Frobenius conjugacy class $\mathrm{Frob}_\wp$ at $\wp$ on the Tate module $T_{\mathfrak{L}}(\phi)$, and similarly for $a_P(\phi')$. Also, $\rho_{\phi',\wp}\,|_{G_{K'}} \cong \rho_{\phi,\wp}\,|_{G_{K'}} \cong \sigma$ for a 1-dimensional representation $\sigma : G_{K'} \to \overline{\mathbb{F}}_q^\times$, so we have

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

$\rho_{\phi',\wp} \cong \mathrm{Ind}_{G_{K'}}^{G_K} \sigma \cong \rho_{\phi,\wp}$. Hence, we have $a_P(\phi') \equiv a_P(\phi) \pmod{\wp}$ for all primes $P \notin S$. Now, if $\epsilon_\wp(\mathrm{Frob}_P) = -1$, we get that

$$\wp \mid 2a_P(\phi) \tag{15}$$

by the relationship between $a_P(\phi')$ and $a_P(\phi)$ following (14). Since ϕ does not have complex multiplication and $\epsilon_\wp$ is nontrivial, by Lemma 4.2 we have that ϕ and ϕ' are not K-isogenous. Hence, by the isogeny theorem [27, Proposition 3.1], there are only finitely many $P \notin S$ such that $\epsilon_\wp(\mathrm{Frob}_P) = -1$ and $a_P(\phi) = 0$.

We now use Theorem 3.5 with ϕ' being the twist of ϕ by $\epsilon_\wp$ to obtain the following result.

THEOREM 6.5. *Assume that q is odd, $\wp \notin S_\phi$, and $q_\wp \geqslant 5$. Let ϕ be a Drinfeld A-module of rank 2 over K without complex multiplication, and let $\wp$ be a finite prime of K. Suppose that the image of $\rho_{\phi,\wp}$ lies in the normalizer of a Cartan subgroup of $\mathrm{GL}_2(A/\wp)$ but not in the Cartan subgroup. Let $\epsilon_\wp : G_K \to \mathbb{F}_q^\times$ be the associated Galois character as before.*

Let $\mathfrak{p} \notin S = S_\phi \cup \{\infty\}$ be a prime of least degree such that $\epsilon_\wp(\mathrm{Frob}_\mathfrak{p}) = -1$ and $a_\mathfrak{p}(\phi) \neq 0$; such a prime exists since ϕ has no complex multiplication. Then

$$\deg_K \mathfrak{p} \leqslant 4(C_q + \widetilde{W} + s_q \log_q(c_0 + \widetilde{W})), \tag{16}$$

where

$$\begin{aligned} \widetilde{W} := \log_q^* 2 \left(\deg_K \eta_\phi + \frac{2}{q-1} \deg_K \delta_\phi + 1 + \kappa_\phi \left(q^{\kappa_\phi + 1} - 1 \right) \right) \\ + \frac{1}{4}((q^2-1)(q^2-q))^2 \left(1 + \frac{\kappa_\phi}{s_1(\phi)} \right)^2, \end{aligned} \tag{17}$$

and the notation is taken from Notation 1.

Proof. Let ϕ' be the twist of ϕ by $\epsilon_\wp$ over K given explicitly by $c\phi_a = \phi'_a c$, where $c = \sqrt{\delta}$ for some $\delta \in K^*$ with $v_\infty(\delta) \leqslant 0$.

We note that if $\epsilon_\wp(\mathrm{Frob}_\mathfrak{p}) = 1$ then $a_\mathfrak{p}(\phi) = a_\mathfrak{p}(\phi')$. Therefore, if $a_\mathfrak{p}(\phi) \neq a_\mathfrak{p}(\phi')$, we have that $\epsilon_\wp(\mathrm{Frob}_\mathfrak{p}) = -1$ and $a_\mathfrak{p}(\phi) \neq 0$.

Since $\wp \notin S_\phi$ and $q_\wp \geqslant 5$, by Corollary 6.4, we have that $\eta_\phi = \eta_{\phi'}$. Furthermore, as $j(\phi) = j(\phi')$, we have that $\delta_\phi = \delta_{\phi'}$. We thus have $s_1(\phi') = s_1(\phi) - \frac{1}{2} v_\infty(\delta)$ since $a_1(\phi') = a_1(\phi)/c^{q-1}$.

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

By taking $\phi_2 = \phi'$ to be the twist of $\phi_1 = \phi$ by $\epsilon_\wp$ and $S_\phi \cup S_{\phi'} \cup \{\infty\} = S_\phi \cup \{\infty\} = S$, we deduce from Theorem 3.5 that

$$\deg_K \mathfrak{p} \leqslant 4\left(C_q + W + s_q \log_q(c_0 + W)\right), \tag{18}$$

where

$$W = \log_q^* 2\left(\deg_K \eta_\phi + \frac{2}{q-1}\deg_K \delta_\phi + 1 + \kappa_\phi\left(q^{\kappa_\phi+1} - 1\right)\right) + \frac{1}{4}((q^2-1)(q^2-q))^2\left(1 + \frac{\kappa_\phi}{s_1(\phi)}\right)\left(1 + \frac{\kappa_\phi}{s_1(\phi) - \frac{1}{2}v_\infty(\delta)}\right).$$

Since $1/(s_1(\phi) - \frac{1}{2}v_\infty(\delta)) \leqslant 1/s_1(\phi)$, the result follows. □

The above theorem implies the following bound on the degree of $\wp$ in the Cartan case:

THEOREM 6.6. *Assume that q is odd. Let ϕ be a Drinfeld A-module of rank 2 over K without complex multiplication, and let $\wp$ be a finite prime of K. Suppose that the image of $\rho_{\phi,\wp}$ lies in the normalizer of a Cartan subgroup of $\mathrm{GL}_2(A/\wp)$ but not in the Cartan subgroup.*

Then either $\wp \in S_\phi$, or

$$\deg_K \wp \leqslant 2\left(C_q + \widetilde{W} + s_q \log_q(c_0 + \widetilde{W})\right),$$

where

$$\widetilde{W} := \log_q^* 2\left(\deg_K \eta_\phi + \frac{2}{q-1}\deg_K \delta_\phi + 1 + \kappa_\phi\left(q^{\kappa_\phi+1} - 1\right)\right) + \frac{1}{4}((q^2-1)(q^2-q))^2\left(1 + \frac{\kappa_\phi}{s_1(\phi)}\right)^2, \tag{19}$$

and the quantities in the above formula are as given in Notation 1.

Proof. Note that if $q_\wp < 5$, then the conclusion follows as the bounds on $\wp$ are larger than 1, so we may assume without generality from now on that $\wp \notin S_\phi$ and $q_\wp \geqslant 5$.

As ϕ has no complex multiplication, there exists a prime $\mathfrak{p} \notin S_\phi \cup \{\infty\}$ of least degree such that $\epsilon_\wp(\mathrm{Frob}_\mathfrak{p}) = -1$ and $a_\mathfrak{p}(\phi) \neq 0$. Then applying Theorem 6.5, it follows that

$$\deg_K \mathfrak{p} \leqslant 4\left(C_q + \widetilde{W} + s_q \log_q(c_0 + \widetilde{W})\right), \tag{20}$$

where the quantities in the above formula are as given in Notation 1.

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

Then $\wp \mid 2a_{\mathfrak{p}}(\phi)$ by (15). Since the analogue of Hasse's Theorem [7] gives

$$\deg_K a_{\mathfrak{p}}(\phi) \leqslant \tfrac{1}{2} \deg_K \mathfrak{p},$$

we obtain

$$\deg_K \wp \leqslant 2\left(C_q + \widetilde{W} + s_q \log_q(c_0 + \widetilde{W})\right). \tag{21}$$

Hence, the assertion follows. □

§7. The Borel case

The arguments in this section are Drinfeld module analogues of the arguments in [24, Section 5.6] for elliptic curves.

In this section, let $K = \mathbb{F}_q(T)$. Let ϕ be a Drinfeld A-module of rank 2 over K without complex multiplication, and let $\wp$ be a finite prime of K such that $\rho_{\phi,\wp}$ is not surjective.

We also suppose that the image of $\rho_{\phi,\wp}$ lies in a Borel subgroup of $\mathrm{GL}_2(A/\wp)$.

Let $\chi', \chi'' : G_K \to (A/\wp)^\times$ be the characters of G_K such that

$$\rho_{\phi,\wp}(g) = \begin{pmatrix} \chi'(g) & * \\ 0 & \chi''(g) \end{pmatrix}.$$

We use the convention $\chi(P) := \chi(\mathrm{Frob}_P)$ for a Galois character $\chi : G_K \to (A/\wp)^\times$.

We fix $\overline{K} \subseteq \overline{K}_P$ for each prime P of K.

Recall we let S_ϕ be the set of primes of bad reduction of ϕ over K. Let S'_ϕ be the subset of S_ϕ of primes where ϕ does not have bad Tate reduction.

PROPOSITION 7.1. *We assume that the image of $\rho_{\phi,\wp}$ lies in a Borel subgroup of $\mathrm{GL}_2(A/\wp)$.*

(1) *The characters χ' and χ'' are unramified outside $S_\phi \cup \{\wp, \infty\}$.*
(2) *For all primes $P \notin S_\phi \cup \{\wp, \infty\}$, we have that*

$$a_P(\phi) \equiv \chi'(P) + \chi''(P) \pmod{\wp} \text{ and}$$
$$\epsilon_0(P)P \equiv \chi'(P)\chi''(P) \pmod{\wp},$$

where $a_P(\phi)$ is the trace of $\rho_{\phi,\wp}(\mathrm{Frob}_P)$ and $\epsilon_0 : G_K \to (A/\wp)^\times$ is some character.

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

(3) *Suppose $\wp \notin S_\phi$. Then one of χ' or χ'' is unramified at $\wp$. Denoting this by $\alpha_\wp$, we have that*

$$a_P(\phi) \equiv \alpha_\wp(P) + \epsilon_0(P) P \alpha_\wp(P)^{-1} \pmod{\wp},$$

for all primes $P \notin S_\phi \cup \{\infty\}$.

(4) *Suppose $\wp \notin S_\phi$. Then we have that $\alpha_\wp^{(q-1)(q^2-1)n_\phi} = 1$,*

where $n_\phi \leqslant (q^2-1)(q^2-q)(1+\kappa_\phi/s_1(\phi))$ is a positive integer, and $s_1(\phi)$ and κ_ϕ are the same as given in Notation 1.

Proof. Since $\rho_{\phi,P}$ is unramified for $P \notin S_\phi \cup \{\wp, \infty\}$, the same is true for χ' and χ''; hence, the part (1) follows.

If $P \notin S_\phi \cup \{\wp, \infty\}$, then from Proposition 5.3, we obtain that $\epsilon_0(P)P \equiv \chi'(P)\chi''(P) \pmod{\wp}$, and hence

$$a_P(\phi) \equiv \chi'(P) + \chi''(P) \pmod{\wp}.$$

Suppose $\wp \notin S_\phi$. Then $\rho_{\phi,\wp}(I_{K_\wp})$ is a semisplit Cartan or semisplit Borel subgroup from Theorem 6.1 (the image of $\rho_{\phi,\wp}$ is assumed to lie in a Borel subgroup, which does not contain any nonsplit Cartan subgroup, so the case of a nonsplit Cartan subgroup in Theorem 6.1 does not occur under the hypotheses of this proposition). From Theorem 6.1, we also know that χ' can be assumed to be unramified at $\wp$, which we now denote by $\alpha_\wp$. Thus, we have

$$a_P(\phi) \equiv \alpha_\wp(P) + \epsilon_0(P) P \alpha_\wp(P)^{-1} \pmod{\wp},$$

for all $P \notin S_\phi \cup \{\wp, \infty\}$.

Now, if $P = \wp$, then we still have

$$a_P(\phi) = a_\wp(\phi) \equiv \alpha_\wp(\wp) \pmod{\wp}$$

by the following argument. Note that we now define $a_\wp(\phi)$ as the trace of $\rho_{\phi,\wp}(\mathrm{Frob}_\wp)$ on inertial invariants. The inertial invariants under $\rho_{\phi,\wp}$ are spanned by the vector ${}^T(1,0)$. Then we have that $\mathrm{Frob}_\wp$ acts on the vector ${}^T(1,0)$ via $\alpha_\wp$, hence $a_\wp(\phi) \equiv \alpha_\wp(\wp) \pmod{\wp}$.

Thus, parts (2) and (3) follow.

For the part (4), suppose that $\wp \notin S_\phi$, so as before $\alpha_\wp$ is unramified at $\wp$.

We show that $\alpha_\wp^{(q-1)(q^2-1)}$ is unramified at every prime $P \neq \wp$. This will be done according to each of the following cases:

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

(i) $P \in S_\phi \setminus S'_\phi$ with $P \neq \wp$,
(ii) $P \in S'_\phi$.

In the case (i), P is a prime of bad Tate reduction of ϕ over K and $P \neq \wp$. Then over C_P, where C_P is the completion of an algebraic closure of K_P, we have a uniformization [6] given by a surjective analytic map $e_P : C_P \to C_P$ which relates ϕ to a Drinfeld A-module ψ of rank 1 via the relation $\psi_a \circ e_P = e_P \circ \phi_a$. Let Λ_P be the set of zeros of e_P. Then by [6], $\Lambda_P = A \cdot \lambda_1$ is an A-lattice in C_P of rank 1, where the A-module structure on C_P is given by $\alpha \cdot x := \psi_\alpha(x)$.

Let $K_P^0 = K_P(\Lambda_P, \psi[\wp])$. Then Gardeyn [12, pp. 247–248] shows that:

(1) $K_P(\phi[\wp]) \subseteq K_P^0(\psi_P^{-1}(\Lambda_P)) = K_P^0(s_1)$, where $s_1 \in \psi_P^{-1}(\lambda_1)$;
(2) the conjugates of s_1 over K_P^0 lie in $s_1 + \psi[\wp]$.

The equality $K_P^0(\psi_P^{-1}(\Lambda_P)) = K_P^0(s_1)$ can be seen as follows. Pick a $s_1 \in C_P$ such that $\psi_P(s_1) = \lambda_1$. Then if $\alpha \in A$, $\alpha \cdot s_1 := \psi_\alpha(s_1)$ so that $\psi_P(\alpha \cdot s_1) = \psi_P \circ \psi_\alpha(s_1) = \psi_\alpha \circ \psi_P(s_1) = \psi_\alpha(\lambda_1) = \alpha \cdot \lambda_1$. Hence, $\psi_P^{-1}(\Lambda_P) \supseteq A \cdot s_1$. If $x \in \psi_P^{-1}(\Lambda_P)$, then $\psi_P(x) = \alpha \cdot \lambda_1 = \psi_P(\alpha \cdot s_1)$ for some $\alpha \in A$. Hence, $x \in A \cdot s_1 + \Lambda_P$. Since $K_P^0 \supseteq \Lambda_P$, we have $K_P^0(\psi_P^{-1}(\Lambda_P)) = K_P^0(s_1)$.

The above properties yield a representation $\rho : \mathrm{Gal}(K_P^0(s_1)/K_P^0) \to \psi[\wp]$ from the formula $\sigma(s_1) = s_1 + \rho(\sigma)$. Hence, the image of $\rho_{\phi,\wp}$ consists only of elements of order a power of p when $\rho_{\phi,\wp}$ is restricted to $G_{K_P^0}$.

Finally, since $P \neq \wp$, we have that $K_P^0/K_P(\Lambda_P)$ is unramified, so the inertia subgroup $I_{K_P(\Lambda_P)}$ of $K_P(\Lambda_P)$ is contained in $G_{K_P^0}$. Hence, the image $\rho_{\phi,\wp}(I_{K_P(\Lambda_P)})$ consists only of elements of order a power of p. It follows that χ', χ'' are unramified when restricted to $G_{K_P(\Lambda_P)}$.

Since ϕ has bad Tate reduction at the finite prime P, by [12, Proposition 4(i)], we have that $[K_P(\Lambda_P) : K_P]$ is bounded above by $g_P = \#\,\mathrm{GL}(1, \mathbb{F}_q) = q - 1$. In fact, the proof in [12, Proposition 4(i)] shows that $[K_P(\Lambda_P) : K_P] \mid q - 1$. Thus, $\alpha_\wp^{q-1}$ is unramified when restricted to G_{K_P}.

In the case (ii), $P \in S_\phi$ (we then have that $P \neq \wp$ because $\wp \notin S_\phi \supseteq S'_\phi$). We know that there exists an extension K' of K_P such that ϕ attains semi-stable reduction over K' by Lemma 5.1, and the extension degree $[K_P^{\mathrm{nr}} \cdot K' : K_P^{\mathrm{nr}}]$ divides $q^2 - 1$.

Let P' denote the prime of K' above the prime P. If P' is a bad Tate reduction prime of ϕ over K', we thus have $P' \neq \wp'$, where $\wp'$ is a prime of K' lying above $\wp$, so the same argument as above shows (by replacing K by

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

K', P by P') that $\alpha_\wp^{q-1}$ is unramified when restricted to $G_{K'_{P'}}$ (the results from [12] used above apply equally well over the extension $K'_{P'}$).

Now $K_P^{\mathrm{nr}} \cdot K'$ is Galois over K_P^{nr} of degree dividing q^2-1, where K_P^{nr} is the maximal unramified extension of K_P. Also, $\alpha_\wp^{(q-1)(q^2-1)}$ is unramified when restricted to G_{K_P} if and only if $\alpha_\wp^{(q-1)(q^2-1)}$ is unramified when restricted to $G_{K_P^{\mathrm{nr}}}$, which is the case.

Finally, $\alpha_\wp^{(q-1)(q^2-1)}$ is unramified at every finite prime of K.

Furthermore, we claim that as a character of G_K, we have that $\alpha_\wp^{(q-1)(q^2-1)n_\phi} = 1$, where $n_\phi \leqslant (q^2-1)(q^2-q)(1+\frac{\kappa_\phi}{s_1(\phi)})$ is a positive integer.

Let L be a finite, separable, tamely ramified, and geometric extension of K (recall L is a *geometric extension* of K if and only if the algebraic closure of $\mathbb{F}_K$ in L is $\mathbb{F}_K$ itself). Suppose that M is a field with $K \subset M \subset L$ and L/M is unramified except possibly at the primes ∞_i lying above a prime ∞ of M. From Riemann–Hurwitz, since L/K is tamely ramified, we have the following equality:

$$2g_L - 2 = m(2g_K - 2) + \sum_{i=1}^{t}(e_i - 1)f_i,$$

where $m := [L:K]$, g_L (resp. g_M) is the genus of L (resp. M), and e_i (resp. f_i) denotes the ramification index (resp. the inertial degree) of ∞_i over ∞. This implies that $2g_L = 2 - m - \sum_{i=1}^{t} f_i$ since $g_M = 0$ and $\sum_{i=1}^{t} e_i f_i = m$. Thus, we have $m \leqslant 2 - \sum_{i=1}^{t} f_i \leqslant 1$ as $g_L \geqslant 0$, and hence $m = 1$, that is, $L = M$.

Suppose that a Galois character $\psi : G_K \to \mathbb{F}_\wp^\times$ is unramified at every finite prime of K. Let L be the field cut out by ψ and $M = \mathbb{F}_L \cdot K = \mathbb{F}_{q^n} \cdot K$ (where $\mathbb{F}_L = \mathbb{F}_{q^n}$ is the algebraic closure of $\mathbb{F}_K = \mathbb{F}_q$ in L) so L/M is a geometric extension. Applying the previous paragraph, we deduce that $L = M$. It thus follows that a Galois character $\psi : G_K \to \mathbb{F}_\wp^\times$ which is unramified at every finite prime of K must factor through the Galois group of a finite constant field extension $\mathbb{F}_{q^n}K/K$ for some positive integer n, where $n = [\mathbb{F}_L : \mathbb{F}_K]$.

Applying the above to the character $\alpha_\wp^{(q-1)(q^2-1)}$ (which is unramified at every finite prime of K) and using Theorem 3.2, we get $\alpha_\wp^{(q-1)(q^2-1)n_\phi} = 1$, where $n_\phi \leqslant (q^2-1)(q^2-q)(1+\kappa_\phi/s_1(\phi))$ is a positive integer as claimed. ∎

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

THEOREM 7.2. *Let $K = \mathbb{F}_q(T)$ and ϕ be a Drinfeld A-module of rank 2 over K without complex multiplication and $\wp$ be a finite prime of K. Let P be the least degree prime of K where ϕ has good reduction.*

Suppose that the image of $\rho_{\phi,\wp}$ lies in a Borel subgroup of $\mathrm{GL}_2(A/\wp)$.

Then either

$$\wp \in S_\phi \quad \text{or} \quad \deg_K \wp \leqslant \varphi((q-1)(q^2-1)n_\phi)\ \deg_K P,$$

where φ is the Euler-phi function, $s_1(\phi)$ and κ_ϕ are the same as given in Notation 1, and $n_\phi \leqslant (q^2-1)(q^2-q)(1+\kappa_\phi/s_1(\phi))$ is a positive integer.

Proof. Suppose $\wp \notin S_\phi$. From Proposition 7.1, we have that

$$a_P(\phi) \equiv z + \epsilon_0(P)Pz^{-1} \pmod{\wp}, \tag{22}$$

where z is a $(q-1)(q^2-1)n_\phi$th root of unity in $A/\wp$.

Let d be the order of z, $S_d(X)$ the dth cyclotomic polynomial, and $F_P(X) = X^2 - a_P(\phi)X + \epsilon_0(P)P$.

The congruence in (22) implies that S_d and F_P have a common root mod $\wp$, hence their resultant $R \in A$ is divisible by $\wp$. The resultant R is given by

$$R = \prod (x-\zeta)(x'-\zeta),$$

where x and x' are the two roots of $F_P(X)$ and ζ runs through the set of primitive dth roots of unity.

Let $|x| = q^{-v_\infty(x)}$ denote the absolute value of x associated to the prime ∞. Then we have that

$$|x| = |x'| = q^{(1/2)\deg_K P} \quad \text{and}$$
$$|\zeta| = 1.$$

Hence, we have that

$$\begin{aligned} 0 < |R| &\leqslant \max\{q^{(1/2)\deg_K P}, 1\}^{2n} \\ &= q^{n \deg_K P}, \end{aligned}$$

where $n = \deg S_d(X) = \varphi(d)$. Since d divides $(q-1)(q^2-1)n_\phi$, we have that $n \leqslant \varphi((q-1)(q^2-1)n_\phi)$.

Now, $\wp$ divides R, so we get that

$$\deg_K \wp \leqslant \varphi((q-1)(q^2-1)n_\phi) \deg_K P.$$

The result thus follows. ∎

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

§8. Proof of Theorem 2.1

Let ϕ be a Drinfeld A-module of rank 2 over $K = \mathbb{F}_q(T)$ without complex multiplication, and $\wp$ be a finite prime of K such that $\rho_{\phi,\wp}$ is not surjective.

We first recall a classification of the proper maximal subgroups of $\mathrm{PGL}_2(k)$, where k is a finite field of characteristic p.

THEOREM 8.1. *The maximal proper subgroups of* $\mathrm{PGL}_2(k)$*, where* k *is a finite field of characteristic* p*, are:*

(i) *the projective image of a Borel subgroup of* $\mathrm{GL}_2(k)$*;*
(ii) *the projective image of the normalizer of a Cartan subgroup of* $\mathrm{GL}_2(k)$*;*
(iii) $\mathrm{PSL}_2(k)$*;*
(iv) *isomorphic to the subgroup* $\mathrm{PGL}_2(k')$ *for some proper subfield* k' *of* k*;*
(v) *isomorphic to one of the groups* A_4*,* S_4*, or* A_5*.*

Proof. This result is stated in [11, Proposition 3.12] as being deduced from the version of Dickson's classification of the subgroups of $\mathrm{PSL}_2(k)$ proven in [13, Theorem 8.27, Chapter II]. For completeness, we explain how to deduce the above classification. In order to shorten the arguments, we also rely on [24, Proposition 16] (or [15, Chapter XI, §2, Theorem 2.3]).

Let K be a finite field of order p^f. From [13, Theorem 8.27], a subgroup of $\mathrm{PSL}_2(K)$ is one of:

(1) an elementary abelian p-group;
(2) a cyclic group of order $n \mid (p^f \pm 1)/w$ where $w = (p^f - 1, 2)$;
(3) a dihedral group of order $2n$ with n as in (2);
(4) isomorphic to A_4;
(5) isomorphic to S_4;
(6) isomorphic to A_5;
(7) a semidirect product of an elementary abelian p-group of order p^m with a cyclic subgroup of order t with $t \mid (p^m - 1, p^f - 1)$;
(8) isomorphic to $\mathrm{PSL}_2(K')$, where K' is a subfield of K, or $\mathrm{PGL}_2(K')$, where a quadratic extension of K' is a subfield of K.

We note that the proof of [13, Theorem 8.27] shows that the subgroups in the case (8) are in fact $\mathrm{PGL}_2(K)$-conjugate to $\mathrm{PSL}_2(K')$ or $\mathrm{PGL}_2(K')$. However, since we do not need this additional information for the proof of our results, we omit further discussion of this point.

Let $\bar{H}$ be a maximal proper subgroup of $\mathrm{PGL}_2(k)$. If $p \nmid \left|\bar{H}\right|$, then we have that $\bar{H}$ is

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

(1) the projective image of the normalizer of a Cartan subgroup of $\mathrm{GL}_2(k)$;
(2) isomorphic to A_4, S_4, or A_5

by [24, Proposition 16]. Thus, let us now assume that we are in the case $p \mid |\bar{H}|$.

If $p = 2$, then $\mathrm{PGL}_2(k) = \mathrm{PSL}_2(k)$. If p is odd, then $\mathrm{PGL}_2(k)$ is a subgroup of $\mathrm{PSL}_2(K)$ where $[K : k] = 2$. Hence, applying [13, Theorem 8.27] to $\mathrm{PSL}_2(K)$, $\bar{H}$ is isomorphic to one of the eight types of subgroups listed above.

Cases (2) and (3): The condition $p \mid |\bar{H}|$ implies that we are not in the case (2). If $\bar{H}$ is in the case (3), then $p = 2$. Consider the cyclic subgroup $\bar{Z}$ of order n of $\bar{H}$. If $n = 1$, then $\bar{H}$ is generated by a unipotent element of order 2 and hence lies in a Borel subgroup of $\mathrm{GL}_2(k)$.

Assume now that $n > 1$. Since $p \nmid n$, we have that $\bar{Z}$ is contained in the projective image of a Cartan subgroup $\bar{C}$ of $\mathrm{GL}_2(k)$ by [24, Proposition 16]. An element of $\mathrm{GL}_2(k)$ which conjugates a nontrivial element of $\bar{C}$ to another nontrivial element of $\bar{C}$ must in fact normalize all of $\bar{C}$. Hence $\bar{H}$ is contained in the projective image of the normalizer of a Cartan subgroup of $\mathrm{GL}_2(k)$.

Cases (1) and (7): We show here that $\bar{H}$ is contained in the projective image of a Borel subgroup of $\mathrm{GL}_2(k)$. Let $\bar{E}$ be the elementary abelian p-subgroup of the case (1) or the case (7). Let E be the inverse image of $\bar{E}$ under the homomorphism $\pi : \mathrm{SL}_2(K) \to \mathrm{PSL}_2(K)$. Note that E is abelian and $E = E_0 \times E'$ for a unique elementary abelian p-group E_0 which is isomorphic to $\bar{E}$ under π and an abelian group E' of order coprime to p. Since every element in E_0 has order dividing p and E_0 is abelian, it follows that E_0 up to conjugation is contained in the subgroup

$$U = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}$$

of $\mathrm{SL}_2(K)$ which has order p^f.

An element of $\mathrm{SL}_2(K)$ which conjugates a nontrivial element of U to another nontrivial element of U must in fact normalize U. Let H be the inverse image of $\bar{H}$ under π. Then H is contained in the normalizer of U in $\mathrm{SL}_2(K)$ which is given by

$$\left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} : a \in K^*, b \in K \right\}.$$

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

It follows that the line that is fixed by E is also fixed by all of H. Hence, $\bar{H}$ is contained in the projective image of a Borel subgroup of $\mathrm{GL}_2(k)$.

Case (8): Here, $\bar{H}$ is isomorphic to $\mathrm{PGL}_2(k')$ for some proper subfield k' of k, or $\mathrm{PSL}_2(k)$. □

Assume that $q_\wp > 5$. Suppose also that $\wp \notin S_\phi$, so that $\rho_\wp(I_{K_\wp})$ contains a nonsplit Cartan subgroup or a semisplit Cartan subgroup by Theorem 6.1. The projective image of a nonsplit Cartan subgroup and of a semisplit Cartan subgroup has a cyclic subgroup of order at least $q_\wp \pm 1 > 5$, which rules out the case (v). On the other hand, the order of the projective image of a nonsplit Cartan subgroup or of a semisplit Cartan subgroup does not divide the order of $\mathrm{PGL}_2(k')$ for a proper subfield k' of k, ruling out the case (iv). Since the image of the determinant map on a nonsplit Cartan and semisplit Cartan subgroup is $(A/\wp)^\times$, the case (iii) is ruled out.

Thus, we are in one of the following cases:

(1) Image of $\rho_{\phi,\wp}$ is contained in the normalizer $\mathcal{N}$ of a Cartan subgroup $\mathcal{C}$, but not in $\mathcal{C}$;
(2) Image of $\rho_{\phi,\wp}$ is contained in a Borel subgroup;
(3) Image of $\rho_{\phi,\wp}$ is contained in a nonsplit Cartan subgroup.

PROPOSITION 8.2. *Assume q is odd. The representation $\rho_{\phi,\wp}$ cannot have image contained in a nonsplit Cartan subgroup.*

Proof. Let $\bar{c}$ be an element of $G(K(C[\wp])/K) \cong (A/\wp)^\times$ of order $q_\wp - 1$, where $q_\wp = q^{\deg_K \wp}$ and C is the Carlitz module as in Proposition 5.3. Extend $\bar{c}$ to an element $c \in G_K$ of order $q_\wp - 1$.

From Proposition 5.3, there is a Galois character $\epsilon_0 : G_K \to \mathbb{F}_q^\times$ and a rank 1 Drinfeld A-module ψ such that $\det \rho_{\phi,\wp}(\mathrm{Frob}_P) = \rho_{\psi,\wp}(\mathrm{Frob}_P) \equiv \epsilon_0(P)P \pmod{\wp}$ for all primes P of K such that $P \notin S_\phi$ and $P \neq \wp, \infty$.

Let ϕ' be the twist of ϕ by ϵ_0^{-1}. From the proof of Proposition 5.3, we have that $\det \rho_{\phi',\wp} = \rho_{C,\wp}$. If $\rho_{\phi,\wp}$ has image lying in a nonsplit Cartan subgroup, then $\rho_{\phi',\wp}$ also has image in a nonsplit Cartan subgroup. Therefore, $\rho_{\phi',\wp}(c)$ is contained in the scalars, and hence $\det \rho_{\phi',\wp}(c)$ is a square; thus, the order of $\det \rho_{\phi',\wp}(c)$ divides $(q_\wp - 1)/2$. But $\det \rho_{\phi',\wp}(c) = \rho_{C,\wp}(c) = \bar{c}$ has order $q_\wp - 1$, yielding a contradiction. □

Thus, Case (3) is ruled out. We dealt with Case (1) in Section 6, and with Case (2) in Section 7. Combining all the results together, we obtain Theorem 2.1.

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

Acknowledgments. We would like to thank C. David and A. Cojocaru for useful initial discussions pertaining to the subject of this paper. We also thank the referee for a careful reading, which improved this paper greatly.

References

[1] C. Armana, *Torsion des modules de Drinfeld de rang 2 et formes modulaires de Drinfeld (French)*, Algebra Number Theory **6**(6) (2012), 1239–1288.
[2] I. Chen and Y. Lee, *Newton polygons of exponential functions attached to Drinfeld modules of rank 2*, Proc. Amer. Math. Soc. **141** (2013), 83–91.
[3] I. Chen and Y. Lee, *Explicit isogeny theorems for Drinfeld modules*, Pac. J. Math. **263**(1) (2013), 87–116.
[4] A. Cojocaru and C. Hall, *Uniform results for Serre's theorem for elliptic curves*, Int. Math. Res. Not. **50** (2005), 3065–3080.
[5] C. David, *Frobenius distributions of Drinfeld modules of any rank*, J. Number Theory **90**(2) (2001), 329–340.
[6] V. G. Drinfeld, *Elliptic modules*, Math. USSR Sb. **31** (1977), 159–170.
[7] E.-U. Gekeler, *On finite Drinfeld modules*, J. Algebra **141** (1991), 167–182.
[8] E. Gekeler, *Frobenius distributions of Drinfeld modules over finite fields*, Trans. Amer. Math. Soc. **360**(4) (2008), 1695–1721.
[9] D. Goss, *Basic Structures of Function Field Arithmetic*, Springer, Berlin, 1996.
[10] D. Goss, "*L-series of t-motives and Drinfeld modules*", in *The Arithmetic of Function Fields: Proceedings of the Workshop at Ohio State University 1991* (eds. D. Goss et al.) Berlin-New York, 1992, 313–402.
[11] F. Gardeyn, *t-motives and Galois representations*, Ph.D Thesis, ETH Zurich, 2001.
[12] F. Gardeyn, *Une borne pour l'action de l'inertie sauvage sur la torsion d'un module de Drinfeld*, Arch. Math. **79** (2002), 241–251.
[13] B. Huppert, *Endliche Gruppen I*, Grundlehren der Mathematischen Wissenschaften **134**, Springer, Berlin, 1967.
[14] A. Kraus, *Une remarque sur les points de torsion des courbes elliptiques*, C. R. Acad. Sci. Paris Sér. I Math. **321**(9) (1995), 1143–1146.
[15] S. Lang, *Introduction to Modular Forms*, Grundlehren der Mathematischen Wissenschaften **222**, Springer, Berlin, 1976, ix+261.
[16] D. Lombardo, *Bounds for Serre's open image theorem for elliptic curves over number fields*, Algebra Number Theory **9**(10) (2015), 2347–2395.
[17] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44**(2) (1978), 129–162.
[18] V. K. Murty and J. Scherk, *Effective versions of the Chebotarev density theorem for function fields*, C. R. Acad. Sci. Paris Sr. I Math. **319**(6) (1994), 523–528.
[19] A. Pál, *On the torsion of Drinfeld modules of rank two*, J. Reine Angew. Math. **640** (2010), 1–45.
[20] R. Pink, *The Mumford–Tate Conjecture for Drinfeld Modules*, Publ. Res. Inst. Math. Sci. **33** (1997), 393–425.
[21] R. Pink and E. Rütsche, *Image of the group ring of the Galois representation associated to Drinfeld modules*, J. Number Theory **129** (2009), 866–881.
[22] B. Poonen, *Fractional power series and pairings on Drinfeld modules*, J. Amer. Math. Soc. **9**(3) (1996), 783–812.
[23] M. Rosen, *Number Theory in Function Fields*, Springer, 2002.
[24] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press

[25] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics, Springer, New York, 1979.
[26] J-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Etudes Sci. Publ. Math. **54** (1981), 323–401.
[27] Y. Taguchi, "*Ramifications arising from Drinfeld modules*", in *The Arithmetic of Function Fields (Columbus, OH, 1991)*, Ohio State Univ. Math. Res. Inst. Publ. **2**, de Gruyter, Berlin, 1992, 171–187.
[28] Y. Taguchi, *On ϕ-modules*, J. Number Theory **60** (1996), 124–141.
[29] T. Takahashi, *Good reduction of elliptic modules*, J. Math. Soc. Japan **34** (1982), 475–487.
[30] D.S. Thakur, *Function Field Arithmetic*, World Scientific Publishing Co., Inc., 2004.
[31] G.-J. van der Heiden, *Weil pairing for Drinfeld modules*, Monatsch. Math. **143** (2004), 115–143.

Imin Chen
Department of Mathematics
Simon Fraser University
Burnaby
British Columbia
CANADA V5A 1S6
ichen@math.sfu.ca

Yoonjin Lee
Department of Mathematics
Ewha Womans University
52 Ewhayeodae-gil
Seodaemun-gu
Seoul
03760
South Korea
yoonjinl@ewha.ac.kr

https://doi.org/10.1017/nmj.2017.26 Published online by Cambridge University Press