Canad. J. Math. Vol. **67** (6), 2015 pp. 1326–1357
http://dx.doi.org/10.4153/CJM-2015-006-9

The Distribution of the First Elementary Divisor of the Reductions of a Generic Drinfeld Module of Arbitrary Rank

Alina Carmen Cojocaru and Andrew Michael Shulman

Abstract. Let ψ be a generic Drinfeld module of rank $r \geq 2$. We study the first elementary divisor $d_{1,\wp}(\psi)$ of the reduction of ψ modulo a prime $\wp$, as $\wp$ varies. In particular, we prove the existence of the density of the primes $\wp$ for which $d_{1,\wp}(\psi)$ is fixed. For $r = 2$, we also study the second elementary divisor (the exponent) of the reduction of ψ modulo $\wp$ and prove that, on average, it has a large norm. Our work is motivated by J.-P. Serre's study of an elliptic curve analogue of Artin's Primitive Root Conjecture, and, moreover, by refinements to Serre's study developed by the first author and M. R. Murty.

1 Introduction and Statement of Results

A beautiful and fruitful theme in number theory is that of exploring versions of one given problem in both the number field and function field settings. In many instances, such explorations unravel striking analogies, shedding light to deep basic principles underlying the problem. In other instances, the number field and function field versions of the same problem turn out to be surprisingly different.

This article is part of such dual investigations, where the problem is that of Frobenius distributions in GL-extensions, generated by elliptic curves over number fields and by Drinfeld modules over function fields. In particular, the article focuses on the problem of determining the distribution of the first elementary divisor of the reduction modulo a prime of a generic Drinfeld module, as the prime varies. Our main result is analogous to a generalization of a result of J.-P. Serre [Se], proved in [CoMu] and [Co3], for the reductions modulo primes of an elliptic curve over $\mathbb{Q}$. The techniques used in proving our main result lead to further applications, such as to Drinfeld module analogues of a result of W. Duke [Du] and of a recent result of T. Freiberg and P. Kurlberg [FrKu], as we now explain.

Let $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$, and for a prime p of good reduction, let $E_p/\mathbb{F}_p$ be the reduction of E modulo p. By the theory of torsion points of elliptic curves, there exist uniquely determined positive integers $d_{1,p}(E), d_{2,p}(E)$ such that

$$E_p(\mathbb{F}_p) \simeq_{\mathbb{Z}} \mathbb{Z}/d_{1,p}(E)\mathbb{Z} \times \mathbb{Z}/d_{2,p}(E)\mathbb{Z} \quad \text{and} \quad d_{1,p}(E) \mid d_{2,p}(E).$$

Received by the editors November 12, 2014; revised February 4, 2015.
Published electronically July 28, 2015.
A. C. Cojocaru's work on this material was partially supported by the National Science Foundation under agreements No. DMS-0747724 and No. DMS-0635607, and by the European Research Council under Starting Grant 258713.
AMS subject classification: **11R45**, 11G09, 11R58.
Keywords: Drinfeld modules, density theorems.

In the theory of $\mathbb{Z}$-modules, the integers $d_{1,p}(E), d_{2,p}(E)$ are called the *elementary divisors* of $E_p(\mathbb{F}_p)$, with the largest of them, $d_2 = d_{2,p}(E)$, called the *exponent*, having the property that $d_2 x = 0$ for all $x \in E_p(\mathbb{F}_p)$ (see the general definition in [La, p. 149]).

The study of the growth of $d_{2,p}(E)$, as the prime p varies and $E/\mathbb{Q}$ is fixed, was initiated by R. Schoof [Sc], who showed that if $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$, then

$$d_{2,p}(E) \gg \frac{\log p}{(\log\log p)^2}\sqrt{p}.$$

W. Duke [Du] improved this bound substantially, but in an "almost all" sense. To be precise, Duke showed that, given any positive function f with $\lim_{x\to\infty} f(x) = \infty$, then, as $x \to \infty$,

$$\#\Big\{ p \le x : d_{2,p}(E) > \frac{p}{f(p)} \Big\} \sim \pi(x), \tag{1.1}$$

unconditionally if $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \not\simeq \mathbb{Z}$, and conditionally upon the Generalized Riemann Hypothesis (GRH) if $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$. Here, $\pi(x)$ denotes the number of primes $p \le x$. By the "Riemann hypothesis for curves over finite fields" (Hasse's bound in this case), the numerator p in the growth $\frac{p}{f(p)}$ of $d_{2,p}(E)$ above is very close to the order of magnitude of $\#E_p(\mathbb{F}_p)$. Thus, roughly, Duke's result says that for almost all p, the exponent of $E_p(\mathbb{F}_p)$ is almost as large as the order of $E_p(\mathbb{F}_p)$. This behaviour is also confirmed by a recent result of T. Freiberg and P. Kurlberg [FrKu] (see also the follow up papers by S. Kim [Ki] and J. Wu [Wu]), in the following sense. Under the same assumptions as Duke's, Freiberg and Kurlberg showed that, as $x \to \infty$,

$$\frac{1}{\pi(x)} \sum_{p \le x} d_{2,p}(E) \sim c(E)x \tag{1.2}$$

for some explicit constant $c(E) \in (0,1)$, depending on E.

The proofs of (1.1) and (1.2) reduce to the analysis of sums of the form

$$\sum_{y<d<z} \#\big\{ p \le x : d \mid d_{1,p}(E) \big\}$$

for suitable parameters $y = y(x), z = z(x)$. In particular, they reduce to an understanding of the first elementary divisor $d_{1,p}(E)$.

The study of $d_{1,p}(E)$, as the prime p varies and $E/\mathbb{Q}$ is fixed, has been carried out for over four decades and precedes the study of $d_{2,p}(E)$. Most notably, J.-P. Serre [Se] studied the distribution of the primes p for which $d_{1,p}(E) = 1$ in analogy to the study of the Artin primitive root conjecture, while M. R. Murty [Mu] and, later, the first author of this paper, refined and strengthened Serre's result, proving the following (see [Co1, Co2, CoMu, Co3]): for any $d \in \mathbb{N}$, there exists an explicit constant $\delta_{E,\mathbb{Q}}(d) \ge 0$ such that, as $x \to \infty$,

$$\#\big\{ p \le x : d_{1,p}(E) = d \big\} \sim \delta_{E,\mathbb{Q}}(d)\pi(x), \tag{1.3}$$

unconditionally if $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \not\simeq \mathbb{Z}$, and conditionally upon GRH if $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$. Under GRH, Cojocaru and Murty [CoMu] (see also [Co3]) showed that the error term in this asymptotic is $\mathrm{O}_{E,d}(x^{\frac{3}{4}}(\log x)^{\frac{1}{2}})$ if $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \not\simeq \mathbb{Z}$, and $\mathrm{O}_{E,d}(x^{\frac{5}{6}}(\log x)^{\frac{2}{3}})$ if $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$.

When considering the function field analogue of these problems, we are naturally led to Drinfeld modules. Indeed, the role played by elliptic curves over $\mathbb{Q}$ in number field arithmetic is similar to the one played by rank 2 Drinfeld modules over $\mathbb{F}_q(T)$ in function field arithmetic. Drinfeld modules also come in higher generalities, for example in higher ranks, and, as such, when suitable, we may focus on Drinfeld modules of arbitrary rank.

To state our main results, we fix the following: q a prime power, $A := \mathbb{F}_q[T]$, $k := \mathbb{F}_q(T)$, $K \supseteq k$ a finite field extension, $\psi\colon A \to K\{\tau\}$ a generic Drinfeld A-module over K of rank $r \geq 2$. Here, $\tau\colon x \mapsto x^q$ is the q-th power Frobenius automorphism and $K\{\tau\}$ is the skew-symmetric polynomial ring in τ over K (we will review definitions and basic properties in Sections 2 and 3).

By classical theory, all but finitely many of the primes $\wp$ of K are of good reduction for ψ. We denote by $\mathcal{P}_\psi$ the collection of these primes, and for each $\wp \in \mathcal{P}_\psi$, we consider the residue field $\mathbb{F}_\wp$ at $\wp$ and the A-module structure on $\mathbb{F}_\wp$, denoted $\psi(\mathbb{F}_\wp)$, defined by the reduction $\psi \otimes \wp : A \to \mathbb{F}_\wp\{\tau\}$ of ψ modulo $\wp$.

By the theory of torsion points for Drinfeld modules and that of finitely generated modules over a PID, there exist uniquely determined monic polynomials $d_{1,\wp}(\psi), \dots, d_{r,\wp}(\psi) \in A$ such that

$$\psi(\mathbb{F}_\wp) \simeq_A A/d_{1,\wp}(\psi)A \times \cdots \times A/d_{r,\wp}(\psi)A \tag{1.4}$$

and $d_{1,\wp}(\psi) | \cdots | d_{r,\wp}(\psi)$. The polynomials $d_{1,\wp}(\psi), \dots, d_{r,\wp}(\psi)$ are the *elementary divisors* of the A-module $\psi(\mathbb{F}_\wp)$, with the largest of them, $d_r = d_{r,\wp}(\psi)$, the *exponent*, having the property that $d_r x = 0$ for all $x \in \psi(\mathbb{F}_\wp)$. Here, $d_r x := (\psi \otimes \mathbb{F}_\wp)(d_r)(x)$.

Associated with this setting, we introduce the following additional notation. We let $\mathbb{F}_K$ denote the constant field of K and $c_K := [\mathbb{F}_K : \mathbb{F}_q]$; thus $\mathbb{F}_K = \mathbb{F}_{q^{c_K}}$. For a non-zero $a \in A$, we let $|a|_\infty := q^{\deg a}$, where $\deg a$ is the degree of a as a polynomial in T. For a prime $\wp$ of K, we let $\deg_K \wp := [\mathbb{F}_\wp : \mathbb{F}_K]$ and $|\wp|_\infty := q^{c_K \deg_K \wp}$. We set

$$\pi_K(x) := \#\{\wp \text{ prime of } K : \deg_K \wp = x\}$$

and recall the effective Prime Number Theorem for K:

$$\pi_K(x) = \frac{q^{c_K x}}{x} + \mathrm{O}_K\Big(\frac{q^{\frac{c_K x}{2}}}{x}\Big). \tag{1.5}$$

The first main result of the paper follows.

Theorem 1.1 *Let q be a prime power, $A := \mathbb{F}_q[T]$, $k := \mathbb{F}_q(T)$ and let K/k be a finite field extension. Let $\psi\colon A \to K\{\tau\}$ be a generic Drinfeld A-module over K, of rank $r \geq 2$. Let $d \in A$ be monic. Then, as $x \to \infty$,*

$$\#\big\{\wp \in \mathcal{P}_\psi : \deg_K \wp = x, d_{1,\wp}(\psi) = d\big\} \sim \pi_K(x) \sum_{\substack{m \in A \\ m \text{ monic}}} \frac{\mu_A(m) c_{md}(x)}{[K(\psi[md]) : K]}, \tag{1.6}$$

where $\mu_A(\cdot)$ is the Möbius function on A, $K(\psi[md])$ is the md-division field of ψ, and

$$c_{md}(x) := \begin{cases} [K(\psi[md]) \cap \overline{\mathbb{F}}_K : \mathbb{F}_K] & \textit{if } [K(\psi[md]) \cap \overline{\mathbb{F}}_K : \mathbb{F}_K] \,|\, x, \\ 0 & \textit{otherwise.} \end{cases}$$

Moreover, the Dirichlet density of the set $\{\wp \in \mathcal{P}_\psi : d_{1,\wp}(\psi) = d\}$ *exists and is given by*

$$\delta_{\psi,K}(d) := \sum_{\substack{m \in A \\ m \text{ monic}}} \frac{\mu_A(m)}{[K(\psi[md]) : K]}.$$

This is a large generalization of a result proved independently in [KuLi] for $d = 1$ and for Drinfeld modules ψ having a trivial endomorphism ring. Note that the proofs of both Theorem 1.1 and [KuLi, Theorem 1] are based on the main ideas introduced by Cojocaru and Murty in [CoMu].

The essence of the proof of this theorem can be summarized as a Chebotarev Density Theorem for infinitely many Galois extensions generated by the generic Drinfeld module ψ.

Theorem 1.2 *Let q be a prime power, $A := \mathbb{F}_q[T]$, $k := \mathbb{F}_q(T)$, and let K/k be a finite field extension. Let $\psi\colon A \to K\{\tau\}$ be a generic Drinfeld A-module over K, of rank $r \geq 2$. Then, as $x \to \infty$,*

$$\sum_{\substack{m \in A \\ m \text{ monic}}} \#\big\{\wp \in \mathcal{P}_\psi : \deg_K \wp = x, \wp \text{ splits completely in } K(\psi[m])\big\} \sim \pi_K(x) \sum_{\substack{m \in A \\ \text{monic}}} \frac{c_m(x)}{[K(\psi[m]) : K]},$$

with notation as in Theorem 1.1.

As a consequence of the techniques used in proving Theorems 1.1 and 1.2, we obtain the following analogues of the results of [Du] and [FrKu] in the case of a rank 2 generic Drinfeld module over K.

Theorem 1.3 *Let q be a prime power, $A := \mathbb{F}_q[T]$, $k := \mathbb{F}_q(T)$, and let K/k be a finite field extension. Let $\psi\colon A \to K\{\tau\}$ be a generic Drinfeld A-module over K, of rank 2.*

(i) *Let $f\colon (0,\infty) \to (0,\infty)$ be such that $\lim_{x\to\infty} f(x) = \infty$. Then, as $x \to \infty$,*

$$\#\Big\{\wp \in \mathcal{P}_\psi : \deg_K \wp = x, |d_{2,\wp}(\psi)|_\infty > \frac{|\wp|_\infty}{q^{c_K f(x)}}\Big\} \sim \pi_K(x).$$

Moreover, the Dirichlet density of the set

$$\Big\{\wp \in \mathcal{P}_\psi : |d_{2,\wp}(\psi)|_\infty > \frac{|\wp|_\infty}{q^{c_K f(\deg_K \wp)}}\Big\}$$

exists and equals 1.

(ii) *As $x \to \infty$, we have*

$$\frac{1}{\pi_K(x)} \sum_{\substack{\wp \in \mathcal{P}_\psi \\ \deg_K \wp = x}} |d_{2,\wp}(\psi)|_\infty \sim q^{c_K x} \sum_{\substack{m \in A \\ m \text{ monic}}} \frac{c_m(x)}{[K(\psi[m]) : K]} \sum_{\substack{a,b \in A \\ a,b \text{ monic} \\ ab = m}} \frac{\mu_A(a)}{|b|_\infty}.$$

https://doi.org/10.4153/CJM-2015-006-9 Published online by Cambridge University Press

The structure of the paper is as follows. In Section 2, we review standard notation and terminology for the arithmetic of A and that of A-fields, and we include a few lemmas on elementary function field arithmetic that will be used in Sections 5 and 6. In Section 3, we discuss definitions and main results from the theory of Drinfeld modules, with a focus on properties of division fields of Drinfeld modules. These properties will be relevant in the proofs of Theorems 1.1, 1.2, and 1.3. In Section 4, we recall an effective version of the Chebotarev density theorem, which we apply to division fields of generic Drinfeld modules, using results from Section 3; this application of Chebotarev is the first key ingredient in the proofs of our main theorems. In Section 5, we present the proofs of Theorems 1.1 and 1.2, while in Section 6 we present the proof of Theorem 1.3. With the algebraic background from Sections 3–5 in place, the general flavour of our proofs is analytic. We conclude the paper with remarks on the error terms and the densities appearing in our main theorems.

2 Notation and Basic Facts

Throughout the paper, we will use the following notation and basic results.

2.1 Basic Notation

We use $\mathbb{N}$ for the set of natural numbers $\{1, 2, 3, \dots\}$, and $\mathbb{R}$, $\mathbb{C}$ for the sets of real and complex numbers, respectively.

For two functions $f, g\colon D \to \mathbb{R}$, with $D \subseteq \mathbb{C}$ and g positive, we write $f(x) = \mathrm{O}(g(x))$ or $f(x) \ll g(x)$ if there is a positive constant C such that $|f(x)| \le Cg(x)$ for all $x \in D$. If C depends on another specified object C', we write $f(x) = \mathrm{O}_{C'}(g(x))$ or $f(x) \ll_{C'} g(x)$. We write $f(x) = \mathrm{o}(g(x))$, or sometimes $f(x) \sim 0 \cdot g(x)$, if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$, and $f(x) \sim \delta g(x)$ for $\delta > 0$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = \delta$ (whenever the limits exist).

2.2 Elementary Arithmetic

We let q be a prime power, fixed throughout the paper. Our implied O-constants may depend on q without any additional specification.

We denote by $\mathbb{F}_q$ the finite field with q elements, by $\mathbb{F}_q^*$ its group of units, by $\overline{\mathbb{F}}_q$ an algebraic closure, and by $\tau\colon x \mapsto x^q$ the q-th power Frobenius automorphism.

As in Section 1, we denote by $A := \mathbb{F}_q[T]$ the polynomial ring over $\mathbb{F}_q$ and by $k := \mathbb{F}_q(T) = \mathrm{Quot}(A)$ its field of fractions; we denote by $A^{(1)}$ the set of monic polynomials in A.

We recall that A is a Euclidean domain, hence the greatest common divisor, denoted gcd, and the least common multiple, denoted lcm, exist in A. We recall that $\frac{1}{T}$ plays the role of the "prime at infinity" of k, while the "finite primes" of k are identified with monic irreducible polynomials of A. We will simply refer to the latter as the *primes of* k.

We denote the monic irreducible elements of A by p or ℓ. We denote the primes of k by $\mathfrak{p} = pA$, with $p \in A^{(1)}$, or by $\mathfrak{l} = \ell A$, with $\ell \in A^{(1)}$. For such primes, we

https://doi.org/10.4153/CJM-2015-006-9 Published online by Cambridge University Press

denote their residue fields by $\mathbb{F}_{\mathfrak{p}}$, $\mathbb{F}_{\mathfrak{l}}$, and the completions of A, respectively of k, by $A_{\mathfrak{p}}$, $A_{\mathfrak{l}}$, and $k_{\mathfrak{p}}$, $k_{\mathfrak{l}}$.

For $a \in A$, we use the following standard notation:

- $\deg a$ for the degree of $a \neq 0$ as a polynomial in T, and $\deg 0 := -\infty$;
- $|a|_\infty := q^{\deg a}$ if $a \neq 0$, and $|0|_\infty := 0$;
- $\operatorname{sgn}(a) \in \mathbb{F}_q$ for the leading coefficient of a;
- $\mu_A(a)$ for the Möbius function of a on A, that is, letting $a = \operatorname{sgn}(a) \cdot p_1^{e_1} \dots p_t^{e_t}$ be the prime decomposition of $a \in A \backslash \mathbb{F}_q$, we have

$$\mu_A(a) := \begin{cases} 1 & \text{if } a \in \mathbb{F}_q^*, \\ (-1)^t & \text{if } a \in A\backslash\mathbb{F}_q \text{ and } e_1 = e_2 = \cdots = e_t = 1, \\ 0 & \text{otherwise;} \end{cases}$$

- $(A/aA)^*$ for the group of units of A/aA;
- $\phi_A(a)$ for the Euler function of a on A, that is,

$$\begin{aligned}\phi_A(a) &:= \#(A/aA)^* \\ &= \#\{a' \in A\backslash\{0\} : \deg a' < \deg a, \gcd(a, a') = 1\} \\ &= |a|_\infty \prod_{\substack{p \in A^{(1)} \\ p \mid a}} \Big(1 - \frac{1}{|p|_\infty}\Big);\end{aligned}$$

- $\mathrm{GL}_r(A/aA) := \{(a_{ij})_{1 \le i,j \le r} : a_{ij} \in A/aA, \det(a_{ij})_{i,j} \in (A/aA)^*\}$.

We record below a few arithmetic results needed in the proofs of our main theorems.

Lemma 2.1 *Let $y \in \mathbb{N}$. Then*

(i) $$\sum_{\substack{a \in A^{(1)} \\ 0 \le \deg a \le y}} 1 = \frac{q^{y+1} - 1}{q - 1};$$

(ii) $$\sum_{\substack{a \in A^{(1)} \\ 0 \le \deg a \le y}} \deg a \le y \frac{q^{y+1} - 1}{q - 1}.$$

Proof Part (i) is easily deduced by partitioning the polynomials a under summation according to their degrees. Part (ii) follows from this. ■

Lemma 2.2 *Let $y \in \mathbb{N}\backslash\{1, 2\}$ and let $\alpha > 1$. Then*

(i) $$\sum_{\substack{a \in A \\ \deg a > y}} \frac{1}{q^{\alpha \deg a}} = \frac{q}{(1 - \frac{1}{q^{\alpha-1}}) q^{(\alpha-1)(y+1)}};$$

(ii) $$\sum_{\substack{a \in A \\ \deg a > y}} \frac{\log \deg a}{q^{\alpha \deg a}} \le \frac{(q-1)\log y}{q(\log q)(\alpha - 1) q^{(\alpha-1)y}} + \frac{q-1}{q(\log q)^2(\alpha-1)^2 y} \cdot q^{(1-\alpha)y},$$

provided y is sufficiently large (specifically, $(\alpha - 1)(\log q) y (\log y) > 1$).

https://doi.org/10.4153/CJM-2015-006-9 Published online by Cambridge University Press

Proof As in the proof of Lemma 2.1, (i) is deduced easily by partitioning the polynomials a under summation according to their degrees. Part (ii) is deduced proceeding similarly, and also by using integration by parts. ∎

Lemma 2.3 *Let $a \in A\backslash\{0\}$. Then*

$$\sum_{\substack{d\in A\\ d|a}} \mu_A(d) = \begin{cases} q-1 & \text{if } a \in \mathbb{F}_q^*,\\ 0 & \text{otherwise.}\end{cases}$$

Proof If $a \in \mathbb{F}_q^*$, then

$$\sum_{\substack{d\in A\\ d|a}} \mu_A(d) = \sum_{d\in\mathbb{F}_q^*} 1 = q-1.$$

If $a \notin \mathbb{F}_q^*$, let $a = \operatorname{sgn}(a)\cdot p_1^{e_1}\cdots p_t^{e_t}$ be the prime factorization of a and let $\operatorname{rad}(a) := \operatorname{sgn}(a)\cdot p_1\cdots p_t$ be the radical of a. Then

$$\sum_{\substack{d\in A\\ d|a}} \mu_A(d) = \sum_{\substack{d\in A\\ d|\operatorname{rad}(a)}} \mu_A(d).$$

Note that if $\mathbb{F}_q^* = \langle u\rangle$, then the divisors $d\,|\operatorname{rad}(a)$ are of the form: u^α for some $1\le\alpha\le q-1$; or $u^\alpha p_i$ for some $1\le\alpha\le q-1$ and some $1\le i\le t$; or $u^\alpha p_{i_1}p_{i_2}$ for some $1\le\alpha\le q-1$ and some $1\le i_1<i_2\le t$; etc. There are $(q-1)\binom{t}{0}$ possibilities for the first type, $(q-1)\binom{t}{1}$ possibilities for the second, $(q-1)\binom{t}{2}$ possibilities for the third, etc. In summary, we have

$$\sum_{\substack{d\in A\\ d|\operatorname{rad}(a)}} \mu_A(d) = \sum_{0\le i\le t}(q-1)\binom{t}{i}(-1)^i = (q-1)(1-1)^t = 0.$$

This completes the proof. ∎

Lemma 2.4 *Let $d \in A\backslash\{0\}$. Then*

$$\frac{1}{|d|_\infty} = \frac{1}{(q-1)^2}\sum_{\substack{a,b\in A\\ ab|d}} \frac{\mu_A(a)}{|b|_\infty}.$$

Proof By using Lemma 2.3, we have

$$\frac{1}{(q-1)^2}\sum_{\substack{a,b\in A\\ ab|d}} \frac{\mu_A(a)}{|b|_\infty} = \frac{1}{(q-1)^2}\sum_{b\in A}\frac{1}{|b|_\infty}\sum_{\substack{a\in A\\ a|\frac{d}{b}}}\mu_A(a)$$
$$= \frac{1}{q-1}\sum_{\substack{b\in A\\ \frac{d}{b}\in\mathbb{F}_q^*}}\frac{1}{|b|_\infty} = \frac{1}{|d|_\infty}.$$ ∎

Lemma 2.5 *Let $d \in A^{(1)}$. Then*

$$\sum_{\substack{m,n\in A^{(1)}\\ mn=d}} \frac{\mu_A(m)}{|n|_\infty} = \frac{(-1)^{\omega(d)}\phi_A(\operatorname{rad}(d))}{|d|_\infty},$$

https://doi.org/10.4153/CJM-2015-006-9 Published online by Cambridge University Press

where $\omega(d)$ is the number of all monic prime divisors of d (counted without multiplicities) and $\operatorname{rad}(d)$ *is the radical of d.*

Proof By multiplicativity, we have

$$\sum_{\substack{m,n\in A^{(1)}\\ mn=d}} \frac{\mu_A(m)}{|n|_\infty} = \prod_{\substack{p\in A^{(1)}\\ p^t||d}} \sum_{\substack{n\in A^{(1)}\\ n|p^t}} \frac{\mu_A(\frac{p^t}{n})}{|n|_\infty} = \prod_{\substack{p\in A^{(1)}\\ p^t||d}} \frac{1-|p|_\infty}{|p|_\infty^t} = \frac{(-1)^{\omega(d)}\phi_A(\operatorname{rad}(d))}{|d|_\infty}. \qquad \blacksquare$$

2.3 A-modules

For A-modules M_1, M_2, we write $M_1 \simeq_A M_2$ to mean that M_1, M_2 are isomorphic over A, and $M_1 \leq_A M_2$ to mean that M_1 is an A-submodule of M_2.

For a non-zero finite A-module M, we let $\chi(M)$ be its *Euler-Poincaré characteristic*, defined as the ideal of A uniquely determined by the following conditions:

(a) if $M \simeq_A A/\mathfrak{p}$ for a prime ideal $\mathfrak{p}$ of A, then $\chi(M) := \mathfrak{p}$;
(b) if $0 \to M_1 \to M \to M_2 \to 0$ is an exact sequence of A-modules, then $\chi(M) = \chi(M_1)\chi(M_2)$.

We let $|\chi(M)|_\infty := |m|_\infty$ for some generator $m \in A$ of $\chi(M)$.

2.4 A-fields

We reserve the notation (L,δ) for *A-fields*, that is, pairs consisting of a field $L \supseteq \mathbb{F}_q$ and an $\mathbb{F}_q$-algebra homomorphism $\delta\colon A \to L$. We recall that the kernel of δ is called the *A-characteristic of L*; in particular, if $\operatorname{Ker}\delta = (0)$, L is said to have *generic A-characteristic*, and if $\operatorname{Ker}\delta \neq (0)$, L is said to have *finite A-characteristic*.

We denote by $\overline{L}$ an algebraic closure of L, by L^{sep} the separable closure of L in $\overline{L}$, and by $G_L := \operatorname{Gal}(L^{\mathrm{sep}}/L)$ the absolute Galois group of L. We also denote by $L\{\tau\}$ the *skew-symmetric polynomial ring in τ over L*, that is,

$$L\{\tau\} := \Big\{ \sum_{0\leq i\leq n} c_i\tau^i : c_i \in L \ \forall\, 0 \leq i \leq n, n \in \mathbb{N}\cup\{0\}\Big\},$$

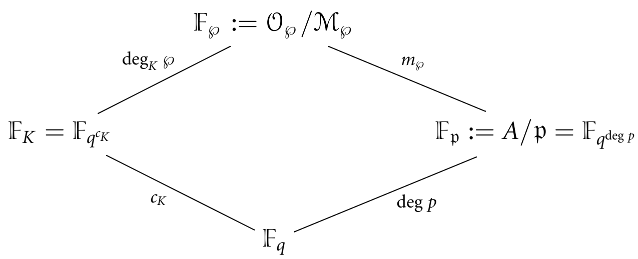
with the multiplication rule $\tau c = c^q\tau \ \forall c \in L$. For an element $f \in L\{\tau\}$, we denote by $\deg_\tau(f)$ its degree as a polynomial in τ. We recall that $L\{\tau\}$ is isomorphic to the $\mathbb{F}_q$-endomorphism ring $\operatorname{End}_{\mathbb{F}_q}(\mathbb{G}_a/L)$ of the additive group scheme $\mathbb{G}_a$ over L.

2.5 Finite Field Extensions of k

We reserve the notation K for a finite field extension of k of genus g_K. Note that the inclusions $A \subseteq k$ and $k \subseteq K$ give K an A-field structure of generic A-characteristic. We denote by $\mathbb{F}_K$ the constant field of K (that is, $\mathbb{F}_K = K\cap\overline{\mathbb{F}}_q$), and by $\overline{\mathbb{F}}_K$ an algebraic closure of $\mathbb{F}_K$. We set $c_K := [\mathbb{F}_K : \mathbb{F}_q]$.

By a *prime of K* we mean a discrete valuation ring $\mathcal{O}$ with maximal ideal $\mathcal{M}$ such that the quotient field $\operatorname{Quot}(\mathcal{O})$ of $\mathcal{O}$ equals K. In particular, for a prime $\wp$ of K, we denote by $(\mathcal{O}_\wp, \mathcal{M}_\wp)$ the associated discrete valuation ring, by $\mathbb{F}_\wp := \mathcal{O}_\wp/\mathcal{M}_\wp$ the associated residue field, by $\deg_K \wp := [\mathbb{F}_\wp : \mathbb{F}_K]$ the degree of $\wp$ in K, and by $\overline{\mathbb{F}}_\wp$ an algebraic closure of $\mathbb{F}_\wp$. We denote the prime $\wp \cap A$ of A by $\mathfrak{p}$, and we denote by p the monic generator of $\mathfrak{p}$. We set $m_\wp := [\mathbb{F}_\wp : A/\mathfrak{p}]$ and record the following diagram:

(2.1)



Hence the relationship between the $|\cdot|_\infty$-norm of a prime $\wp$ of K and that of its associated prime $\mathfrak{p} = pA$ in k is

$$|\wp|_\infty = \#\mathbb{F}_K = |p|_\infty^{m_\wp}.$$

Finally, for a finite Galois extension K' of K, we write $\sigma_\wp$ for the Artin symbol ("the Frobenius") at $\wp$ in K'/K.

3 Drinfeld Modules

3.1 Basic Definitions

Let (L, δ) be an A-field. A *Drinfeld A-module over L* is an $\mathbb{F}_q$-algebra homomorphism

$$\psi\colon A \longrightarrow L\{\tau\}$$
$$a \longmapsto \psi_a$$

such that:

(a) for all $a \in A$, $D(\psi_a) = \delta(a)$, where $D\colon L\{\tau\} \to L$, $D(\sum_{0\le i\le n} c_i\tau^i) = c_0$ is the differentiation with respect to x map;

(b) $\operatorname{Im}\psi \not\subseteq L$.

A homomorphism ψ as above induces a nontrivial A-module structure on L, or, more generally, on any L-algebra Ω; we denote this structure by $\psi(\Omega)$.

Associated with a Drinfeld A-module ψ over L we have two important invariants, called the rank and the height. We define the *rank* of ψ as the unique positive integer r such that

$$\deg_\tau(\psi_a) = r \deg a \quad \forall a \in A.$$

If L has generic A-characteristic, we define the *height* of ψ as zero. If L is of finite A-characteristic $\mathfrak{p} = pA$, we define the *height* of ψ as the unique positive integer h such that

$$\min\{0 \le i \le r \deg a : c_{i,a}(\psi) \ne 0\} = h \operatorname{ord}_\mathfrak{p}(a) \deg p \quad \forall a \in A, a \ne 0,$$

where

$$\psi_a = \sum_{0\le i\le r\deg a} c_{i,a}(\psi)\tau^i$$

and $\operatorname{ord}_\mathfrak{p}(a) := t$ with $p^t || a$.

https://doi.org/10.4153/CJM-2015-006-9 Published online by Cambridge University Press

For the purpose of this paper, the rank and the height are particularly relevant in determining the structure (1.4) of the reductions modulo primes of a Drinfeld A-module in generic characteristic.

3.2 Endomorphism Rings

Let (L, δ) be an A-field. Given $\psi, \psi' \colon A \to L\{\tau\}$ Drinfeld A-modules over L, a *morphism from ψ to ψ' over L* is an element $f \in L\{\tau\}$ such that

$$f\psi_a = \psi'_a f \quad \forall a \in A.$$

An *isogeny from ψ to ψ' over L* is a non-zero morphism as above. An *isomorphism from ψ to ψ' over L* is an element $f \in L^*$ such that $f\psi_a = \psi'_a f$ for all $a \in A$. Finally, $\mathrm{End}_L(\psi)$ and $\mathrm{End}_{\overline{L}}(\psi)$ are the rings of endomorphisms of ψ over L and over $\overline{L}$, respectively.

We remark that

$$\psi(A) \subseteq \mathrm{End}_L(\psi) \subseteq \mathrm{End}_{\overline{L}}(\psi)$$

and that isogenous Drinfeld modules have the same rank and height.

For ease of notation, we shall henceforth denote the category of Drinfeld A-modules over L (with a fixed A-field structure (L, δ)) by $\mathrm{Drin}_A(L)$.

Note that, in the setting of our main theorems, $K \supseteq k$ a fixed field extension and $\psi \colon A \to K\{\tau\}$ a generic Drinfeld A-module over K, we are implicitly working with the structure on K arising from the injective homomorphism $D \circ \psi \colon A \to K$.

Remark 3.1 The category $\mathrm{Drin}_A(L)$ of Drinfeld A-modules over L may be defined in greater generality. Indeed, we may fix an arbitrary function field $\mathscr{K}$ and a prime ∞ of $\mathscr{K}$. We then take $\mathscr{A}$ as the ring of functions on $\mathscr{K}$ regular away from ∞ and define the category $\mathrm{Drin}_{\mathscr{A}}(\mathscr{L})$ of Drinfeld $\mathscr{A}$-modules over $\mathscr{A}$-fields $\mathscr{L}$ exactly as we did above.

The endomorphism rings introduced here have important properties:

Theorem 3.2 ([Go, Prop. 4.7.6, p. 80, Theorem 4.7.8, p. 81, Prop. 4.7.17, p. 84], [Th, Theorem 2.7.2, p. 50]) *Let (L, δ) be an A-field with generic A-characteristic. Let $\psi \in \mathrm{Drin}_A(L)$ be of rank $r \geq 1$. Then $\mathrm{End}_{\overline{L}}(\psi)$ has the following properties:*

(i) $\mathrm{End}_{\overline{L}}(\psi)$ *is commutative;*

(ii) $\mathrm{End}_{\overline{L}}(\psi)$ *is a finitely generated projective A-module of rank at most r;*

(iii) *if we let k' denote $\mathrm{End}_{\overline{L}}(\psi) \otimes_A k$, then k' is a finite field extension of k satisfying $[k' : k] \leq r$.*

3.3 Division Points

Let (L, δ) be an A-field and let $\psi \in \mathrm{Drin}_A(L)$. Let $a \in A \backslash \mathbb{F}_q$. We define the *$a$-division module of ψ* by

$$\psi[a] := \left\{ \lambda \in \overline{L} : \psi_a(\lambda) = 0 \right\}.$$

When $a = \ell$ is irreducible, we define the *ℓ^∞-division module of ψ* by

$$\psi[\ell^\infty] := \bigcup_{n \geq 1} \psi[\ell^n].$$

Note that $\psi[a]$ is a torsion A-module via ψ. As we recall below, its A-module structure is well determined by a and ψ.

Theorem 3.3 ([Ro, Theorem 13.1 p. 221]) *Let (L, δ) be an A-field with A-characteristic $\mathfrak{p}$ (possibly zero). Let $\psi \in \mathrm{Drin}_A(L)$ be of rank $r \geq 1$ and height h. Let $\mathfrak{l} \neq \mathfrak{p}$ be a non-zero prime ideal of A with $\mathfrak{l} = \ell A$, and let $e \geq 1$ be an integer. Then*

$$\psi[\ell^e] \simeq_A (A/\ell^e A)^r.$$

If $\mathfrak{p} = pA$ is non-zero, then

$$\psi[p^e] \simeq_A (A/p^e A)^{r-h}.$$

Corollary 3.4 *Let (L, δ) be an A-field with A-characteristic $\mathfrak{p}$ (possibly zero). Let $\psi \in \mathrm{Drin}_A(L)$ be of rank $r \geq 1$ and height h. Let $a \in A \backslash \mathbb{F}_q$ and write the ideal aA uniquely as the product of ideals $\mathfrak{a}_1, \mathfrak{a}_2$ of A such that $\mathfrak{a}_1$ is relatively prime to $\mathfrak{p}$ and $\mathfrak{a}_2$ is composed of prime divisors of $\mathfrak{p}$. Then*

$$\psi[a] \simeq_A (A/\mathfrak{a}_1)^r \oplus (A/\mathfrak{a}_2)^{r-h} \leq_A (A/aA)^r.$$

Remark 3.5 Theorem 3.3 and Corollary 3.4 hold in greater generality. In particular, the results hold for a Drinfeld module $\psi \in \mathrm{Drin}_{\mathscr{A}}(\mathscr{L})$, where $\mathscr{A}$ is the ring of functions on an arbitrary function field $\mathscr{K}$ which are regular away from some fixed prime in $\mathscr{K}$, and where $\mathscr{L}$ is any $\mathscr{A}$-field.

3.4 Reductions Modulo Primes

Let (L, δ) be an A-field and let $\psi \in \mathrm{Drin}_A(L)$ be of rank $r \geq 1$. Let $\wp$ be a prime of L.

We say that ψ *has integral coefficients at* $\wp$ if

(a) $\psi_a \in \mathcal{O}_\wp\{\tau\}$ for all $a \in A$, and
(b) $\psi \otimes \mathbb{F}_\wp : A \to \mathbb{F}_\wp\{\tau\}$, defined by $a \mapsto \psi_a \pmod{\wp}$, is a Drinfeld A-module over $\mathbb{F}_\wp$ (of some rank $0 < r_1 \leq r$).

In this case, we also say that $\psi \otimes \mathbb{F}_\wp$ is the *reduction of ψ modulo $\wp$*.

We say that ψ *has good reduction at* $\wp$ if there exists $\psi' \in \mathrm{Drin}_A(L)$ such that

(i) $\psi' \simeq_K \psi$,
(ii) ψ' has integral coefficients at $\wp$, and
(iii) $\psi' \otimes \mathbb{F}_\wp$ has rank r.

For the remainder of this subsection, we assume that $L = K$ is a finite field extension of k and that $\psi \in \mathrm{Drin}_A(K)$ has generic characteristic. There are only finitely many primes of K that are not of good reduction for $\psi \in \mathrm{Drin}_A(K)$. As in Section 1, we let $\mathcal{P}_\psi$ denote the set of (finite) primes of K of good reduction for ψ.

Note that, for a prime $\wp \in \mathcal{P}_\psi$, Corollary 3.4 gives the structure (1.4) of the A-module $\psi(\mathbb{F}_\wp)$. Indeed, $\psi(\mathbb{F}_\wp)$ is a finite A-module, and since A is a PID, there exist unique polynomials $d_{1,\wp}(\psi), d_{2,\wp}(\psi), \dots, d_{s,\wp}(\psi) \in A^{(1)}$ such that

$$\psi(\mathbb{F}_\wp) \simeq_A A/d_{1,\wp}(\psi)A \times \cdots \times A/d_{s,\wp}(\psi)A,$$

with $d_{i,\wp}(\psi)|d_{i+1,\wp}(\psi)$ for all $i = 1, \dots, s-1$. That $s = r$ follows from the fact that $\psi(\mathbb{F}_\wp)$ is a torsion module, and hence, by Corollary 3.4, from the existence of some $a \in A\backslash\mathbb{F}_q$ such that $\psi(\mathbb{F}_\wp) \leq_A \psi[a] \leq_A (A/aA)^r$.

The following analogue of the Néron–Ogg–Shafarevich criterion for elliptic curves holds.

Theorem 3.6 ([Tak, Theorem 1, p. 477]) *Let K be a finite extension of k. Let $\psi \in \mathrm{Drin}_A(K)$ be of generic characteristic. Let $\wp$ be a prime of K and let $\mathfrak{l} = \ell A$ be a prime ideal different from $\mathfrak{p} := \wp \cap A$. Then ψ has good reduction at $\wp$ if and only if the Galois module $\psi[\ell^\infty]$ is unramified at $\wp$. Moreover, if ψ has rank 1, then $\psi[\ell^\infty]$ is totally ramified at $\mathfrak{l}$.*

Note that while the last assertion of the theorem is not stated explicitly in [Tak, Theorem 1, p. 477], its proof is given during the course of the proof of the cited theorem.

Remark 3.7 The notion of good reduction can be introduced for a general $\psi \in \mathrm{Drin}_{\mathscr{A}}(\mathscr{L})$, where $\mathscr{A}$ is the ring of functions on an arbitrary function field $\mathscr{K}$ that are regular away from some fixed prime in $\mathscr{K}$, and $\mathscr{L}$ is a generic $\mathscr{A}$-field. Theorem 3.6 holds in this general setting also.

3.5 Division Fields

Let K be a finite field extension of k and let $\psi \in \mathrm{Drin}_A(K)$ be of generic characteristic. For $a \in A$, we define the *a-division field of ψ* as $K(\psi[a])$. This is a Galois extension of K, which plays a crucial role in our study of the elementary divisors of the reductions of ψ. We denote the genus of $K(\psi[a])$ by g_a and the degree of the constant field of $K(\psi[a])$ over $\mathbb{F}_K$ by c_a, that is,

$$c_a := \left[K(\psi[a]) \cap \overline{\mathbb{F}}_K : \mathbb{F}_K\right]. \tag{3.1}$$

Here are some important properties of these division fields.

Proposition 3.8 ([Go, Remark 7.1.9, p. 196]) *Let K be a finite field extension of k and let $\psi \in \mathrm{Drin}_A(K)$ be of generic characteristic. Let*

$$K_{\psi,\mathrm{tors}} := \bigcup_{a \in A\backslash\mathbb{F}_q} K(\psi[a]).$$

Then $[K_{\psi,\mathrm{tors}} \cap \overline{\mathbb{F}}_K : \mathbb{F}_K] < \infty$. In particular, there exists a constant $C(\psi, K) \in \mathbb{N}$, depending on K and ψ, such that, for any $a \in A\backslash\mathbb{F}_q$, $c_a \leq C(\psi, K)$.

Proposition 3.9 ([Ga, Corollary 7, p. 248]) *Let K be a finite field extension of k and let $\psi \in \mathrm{Drin}_A(K)$ be of generic characteristic. Then there exists a constant $G(\psi, K) \in \mathbb{N}$, depending on K and ψ, such that for any $a \in A\backslash\mathbb{F}_q$,*

$$g_a \leq G(\psi, K) \cdot [K(\psi[a]) : K] \cdot \deg a.$$

3.6 Galois Representations

We start with a more general setting. Let $\mathscr{K}$ be a finitely generated field of transcendence degree 1 over $\mathbb{F}_q$, let ∞ be a fixed prime of $\mathscr{K}$, and let $\mathscr{A}$ be the ring of functions on $\mathscr{K}$ regular away from ∞. Let $\mathscr{L}$ be a finitely generated extension of $\mathscr{K}$. Let $\psi \in \mathrm{Drin}_{\mathscr{A}}(\mathscr{L})$ be of rank $r \geq 1$, automatically of generic characteristic.

Using the general notions of division points on Drinfeld modules, for any non-zero prime $\mathfrak{l}$ of $\mathscr{A}$ we define the $\mathfrak{l}$*-adic Tate module of* ψ by

$$T_{\mathfrak{l}}(\psi) := \mathrm{Hom}_A\big(\mathscr{L}_{\mathfrak{l}}/\mathscr{A}_{\mathfrak{l}}, \psi[\mathfrak{l}^{\infty}]\big),$$

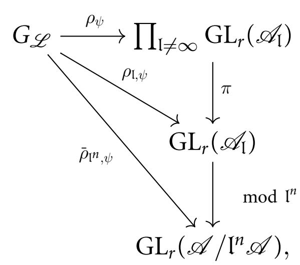
where: for a non-zero ideal $\mathfrak{a}$ of $\mathscr{A}$, $\psi[\mathfrak{a}] := \{\lambda \in \mathscr{L}^{\mathrm{sep}} : \psi_a(\lambda) = 0 \ \forall a \in \mathfrak{a}\}$, $\psi[\mathfrak{l}^{\infty}] := \bigcup_{n\geq 1} \psi[\mathfrak{l}^n]$, and $\mathscr{L}_{\mathfrak{l}}$, $\mathscr{A}_{\mathfrak{l}}$ are the respective $\mathfrak{l}$-completions.

The $\mathfrak{l}$-adic Tate module of ψ is a free $\mathscr{A}_{\mathfrak{l}}$-module of rank r. Moreover, it gives rise to continuous Galois representations

$$\rho_{\mathfrak{l},\psi} \colon G_{\mathscr{L}} \longrightarrow \mathrm{Aut}_{\mathscr{A}_{\mathfrak{l}}}(T_{\mathfrak{l}}(\psi)) \simeq \mathrm{GL}_r(\mathscr{A}_{\mathfrak{l}}),$$
$$\rho_{\psi} \colon G_{\mathscr{L}} \longrightarrow \prod_{\mathfrak{l}\neq\infty} \mathrm{Aut}_{\mathscr{A}_{\mathfrak{l}}}(T_{\mathfrak{l}}(\psi)) \simeq \prod_{\mathfrak{l}\neq\infty} \mathrm{GL}_r(\mathscr{A}_{\mathfrak{l}}) \simeq \mathrm{GL}_r(\widehat{\mathscr{A}})$$

of the absolute Galois group $G_{\mathscr{L}} := \mathrm{Gal}(\mathscr{L}^{\mathrm{sep}}/\mathscr{L})$ of $\mathscr{L}$. Here, $\widehat{\mathscr{A}} := \varprojlim_{\mathfrak{a}} \mathscr{A}/\mathfrak{a}$, where $\mathfrak{a}$ are non-zero ideals of $\mathscr{A}$ ordered by divisibility.

These representations fit into a commutative diagram



with π denoting the natural projection and mod $\mathfrak{l}^n$ denoting the reduction modulo $\mathfrak{l}^n$ map.

Since the *residual* representation $\bar{\rho}_{\mathfrak{l}^n,\psi}$ gives rise to an *injective* representation

$$\bar{\rho}_{\mathfrak{l}^n,\psi} \colon \mathrm{Gal}\big(\mathscr{L}\big(\psi[\mathfrak{l}^n]\big)/\mathscr{L}\big) \hookrightarrow \mathrm{GL}_r(\mathscr{A}/\mathfrak{l}^n\mathscr{A}),$$

we immediately deduce the upper bound

$$\big[\mathscr{L}(\psi[\mathfrak{l}^n]) : \mathscr{L}\big] \leq \#\,\mathrm{GL}_r(\mathscr{A}/\mathfrak{l}^n\mathscr{A}).$$

This bound can be better understood using the following lemma.

Lemma 3.10 *Let $\mathscr{A}$ be a Dedekind domain whose field of fractions is a global field $\mathscr{K}$. Let $\mathfrak{a}$ be a non-zero ideal of $\mathscr{A}$. Define*

$$|\mathfrak{a}| := \#(\mathscr{A}/\mathfrak{a}).$$

https://doi.org/10.4153/CJM-2015-006-9 Published online by Cambridge University Press

Then for any $r \in \mathbb{N}$, we have

$$\# \operatorname{GL}_r(\mathscr{A}/\mathfrak{a}) = |\mathfrak{a}|^{r^2} \prod_{\substack{\mathfrak{l} \mid \mathfrak{a} \\ \mathfrak{l} \text{ prime}}} \Big(1 - \frac{1}{|\mathfrak{l}|}\Big)\Big(1 - \frac{1}{|\mathfrak{l}|^2}\Big) \cdots \Big(1 - \frac{1}{|\mathfrak{l}|^r}\Big)$$
$$\gg_{\mathscr{K}} \frac{|\mathfrak{a}|^{r^2}}{\log\log|\mathfrak{a}|}.$$

Proof This is deduced from [Br, Lemmas 2.2 & 2.3, pp. 1243–1244]. ■

For the main results of this paper we require more precise information about the degree $[\mathscr{L}(\psi[\mathfrak{l}^n]) : \mathscr{L}]$, which we deduce from the following important results of R. Pink and E. Rütsche [PiRu].

Theorem 3.11 ([PiRu, Theorem 0.1, p. 883]) *We keep the setting introduced at the beginning of Section 3.6 and assume that $\operatorname{End}_{\overline{\mathscr{L}}}(\psi) = \mathscr{A}$. Then the image of the representation ρ_ψ is open in $\operatorname{GL}_r(\widehat{\mathscr{A}})$, that is,*

$$\left| \operatorname{GL}_r(\widehat{\mathscr{A}}) : \operatorname{Im} \rho_\psi \right| < \infty.$$

In particular, there exists an integer $i_1(\psi, \mathscr{L}) \in \mathbb{N}$ such that, for any non-zero $a \in \mathscr{A}$,

$$\left| \operatorname{GL}_r(\mathscr{A}/a\mathscr{A}) : \operatorname{Gal}(\mathscr{L}(\psi[a])/\mathscr{L}) \right| \le i_1(\psi, \mathscr{L}),$$

and there exists an ideal $I_1(\psi, \mathscr{L})$ of $\mathscr{A}$ such that for any non-zero $a \in \mathscr{A}$ with $(a\mathscr{A}, I_1(\psi, \mathscr{L})) = 1$,

$$\operatorname{Gal}\big(\mathscr{L}(\psi[a])/\mathscr{L}\big) \simeq \operatorname{GL}_r(\mathscr{A}/a\mathscr{A}).$$

Note that ψ may have a non-trivial endomorphism ring. If all endomorphisms of ψ are actually defined over $\mathscr{L}$, then the image of $\rho_{\mathfrak{l},\psi}$ lies in the centralizer $\operatorname{Centr}_{\operatorname{GL}_r(\mathscr{A}_\mathfrak{l})}\big(\operatorname{End}_{\overline{\mathscr{L}}}(\psi)\big)$. In this case, we focus on the representations

$$\rho_{\mathfrak{l},\psi} \colon G_{\mathscr{L}} \longrightarrow \operatorname{Centr}_{\operatorname{GL}_r(\mathscr{A}_\mathfrak{l})}\big(\operatorname{End}_{\overline{\mathscr{L}}}(\psi)\big),$$
$$\rho_\psi \colon G_{\mathscr{L}} \longrightarrow \prod_{\mathfrak{l} \neq \infty} \operatorname{Centr}_{\operatorname{GL}_r(\mathscr{A}_\mathfrak{l})}\big(\operatorname{End}_{\overline{\mathscr{L}}}(\psi)\big).$$

Theorem 3.12 ([PiRu, Theorem 0.2, p. 883]) *We keep the setting introduced at the beginning of Section 3.6 and assume that*

$$\operatorname{End}_{\overline{\mathscr{L}}}(\psi) = \operatorname{End}_{\mathscr{L}}(\psi).$$

Then the image of the representation ρ_ψ is open in $\prod_{\mathfrak{l}\neq\infty} \operatorname{Centr}_{\operatorname{GL}_r(\mathscr{A}_\mathfrak{l})}(\operatorname{End}_{\overline{\mathscr{L}}}(\psi))$, that is,

$$\left| \prod_{\mathfrak{l} \neq \infty} \operatorname{Centr}_{\operatorname{GL}_r(\mathscr{A}_\mathfrak{l})}\big(\operatorname{End}_{\overline{\mathscr{L}}}(\psi)\big) : \operatorname{Im} \rho_\psi \right| < \infty.$$

In particular, there exists an integer $i_2(\psi, \mathscr{L}) \in \mathbb{N}$ such that, for any non-zero $a \in \mathscr{A}$,

$$\left| \operatorname{Centr}_{\operatorname{GL}_r(\mathscr{A}/a\mathscr{A})}\big(\operatorname{End}_{\overline{\mathscr{L}}}(\psi)\big) : \operatorname{Gal}(\mathscr{L}(\psi[a])/\mathscr{L}) \right| \le i_2(\psi, \mathscr{L}),$$

and there exists an ideal $I_2(\psi, \mathscr{L})$ of $\mathscr{A}$ such that for any non-zero $a \in \mathscr{A}$ with $(a\mathscr{A}, I_2(\psi, \mathscr{L})) = 1$,

$$\operatorname{Gal}(\mathscr{L}(\psi[a])/\mathscr{L}) \simeq \operatorname{Centr}_{\operatorname{GL}_r(\mathscr{A}/a\mathscr{A})}\big(\operatorname{End}_{\overline{\mathscr{L}}}(\psi)\big).$$

We will apply these results to deduce a lower bound for the degree $[K(\psi[a]):K]$ of the a-division field of a generic Drinfeld module $\psi \in \mathrm{Drin}_A(K)$ of rank $r \geq 2$, where K is a finite extension of k; see Theorem 3.14. Before we state and prove this bound, let us recall the Drinfeld module analogue of the Tate Conjecture, proven in [Tag1, Tag2].

Theorem 3.13 (The Tate Conjecture for Drinfeld module) *We keep the previous general setting $\mathscr{K}$, $\mathscr{A}$, $\mathscr{L}$. Let $\psi_1, \psi_2 \in \mathrm{Drin}_{\mathscr{A}}(\mathscr{L})$. Then, for any prime $\mathfrak{l}$ of $\mathscr{A}$, the natural map*

$$\mathrm{Hom}_{\mathscr{L}}(\psi_1, \psi_2) \otimes_{\mathscr{A}} (\mathscr{A}_{\mathfrak{l}}) \longrightarrow \mathrm{Hom}_{\mathscr{A}_{\mathfrak{l}}[G_{\mathscr{L}}]}\big(T_{\mathfrak{l}}(\psi_1), T_{\mathfrak{l}}(\psi_2)\big)$$

is an isomorphism.

Theorem 3.14 *Let K be a finite extension of k and let $\psi \in \mathrm{Drin}_A(K)$ be of rank $r \geq 2$ and of generic characteristic. Let $\gamma := \mathrm{rank}_A \mathrm{End}_{\overline{K}}(\psi)$. Then, for any $a \in A \backslash \mathbb{F}_q$, we have*

$$\frac{|a|_{\infty}^{\frac{r^2}{\gamma}}}{\log\gamma + \log\deg a + \log\log q} \ll_{\psi,K} [K(\psi[a]):K] \leq |a|_{\infty}^{\frac{r^2}{\gamma}}.$$

Proof We base the proof on a strategy used in [Pi]. Let $\widetilde{A} := \mathrm{End}_{\overline{K}}(\psi)$ and let F be the field of fractions of $\widetilde{A}$. By Theorem 3.2, all endomorphisms $f \in \widetilde{A}$ are defined over a finite extension $\widetilde{K}$ of K. Thus, after identifying A with its image $\psi(A) \subseteq \widetilde{A}$, we can extend $\psi\colon A \to K\{\tau\}$ tautologically to a homomorphism

$$\widetilde{\psi}\colon \widetilde{A} \to \widetilde{K}\{\tau\}.$$

This is again a Drinfeld module, with the difference that $\widetilde{A}$ may not be a maximal order in $\widetilde{K}$. To fix this, we modify $\widetilde{\psi}$ by a suitable isogeny, using results of D. Hayes [Ha].

Indeed, we let $\mathscr{A}$ be the normalization of $\widetilde{A}$ in $\widetilde{K}$. Then, by [Ha, Proposition 3.2, p. 182], there exists a Drinfeld module

$$\overline{\psi}\colon \mathscr{A} \longrightarrow \overline{K}\{\tau\}$$

such that $\overline{\psi}|_{\widetilde{A}}$ is K-isogenous to $\widetilde{\psi}$. Moreover, $\overline{\psi}$ may be chosen such that the restriction $\overline{\psi}|_{\widetilde{A}}$ is defined over K.

Let $\mathscr{K}$ be the finite field extension of K generated by the coefficients of all endomorphisms in $\mathrm{End}_{\overline{K}}(\overline{\psi})$. By Theorem 3.13, all the endomorphisms of $\overline{\psi}$ over $\overline{K}$ are defined already over K^{sep}. Thus $\mathscr{K}$ is a separable Galois extension of K. Moreover, by construction, the Galois group $\mathrm{Gal}(\mathscr{K}/K)$ acts on F and, again by Theorem 3.13, it acts faithfully.

Let $\Psi\colon \mathscr{A} \to \mathscr{K}\{\tau\}$ be the tautological extension of $\overline{\psi}$. This is a generic Drinfeld module of rank $R := \frac{r}{\gamma}$ satisfying $\mathrm{End}_{\overline{\mathscr{K}}}(\Psi) = \mathrm{End}_{\mathscr{K}}(\Psi) = \mathscr{A}$. By Theorem 3.12, the image of the representation

$$\rho_{\Psi}\colon G_{\mathscr{K}} \longrightarrow \prod_{\mathfrak{l}\neq\infty} \mathrm{Centr}_{\mathrm{GL}_R(\mathscr{A}_{\mathfrak{l}})}(\mathscr{A}) \simeq \prod_{\mathfrak{l}\neq\infty} \mathrm{GL}_R(\mathscr{A}_{\mathfrak{l}})$$

is open. In particular, there exists an integer $i(\Psi, \mathscr{K}) \in \mathbb{N}$ such that, for any non-zero $a \in \mathscr{A}$,

$$\left| \mathrm{GL}_R(\mathscr{A}/a\mathscr{A}) : \mathrm{Gal}(\mathscr{K}(\Psi[a])/\mathscr{K}) \right| \leq i(\Psi, \mathscr{K}). \tag{3.2}$$

Since $\mathscr{A}$ is a Dedekind domain, by Lemma 3.10 we deduce that, for any non-zero $a \in \mathscr{A}$,

$$\frac{|a\mathscr{A}|^{R^2}}{\log\log |a\mathscr{A}|} \ll_{\mathscr{K}} \#\,\mathrm{GL}_R(\mathscr{A}/a\mathscr{A}) \leq |a\mathscr{A}|^{R^2}, \tag{3.3}$$

where $|a\mathscr{A}| := \#(\mathscr{A}/a\mathscr{A})$.

Now let $a \in A\backslash\mathbb{F}_q$ and remark that $\#(\mathscr{A}/a\mathscr{A}) = \#(A/aA)^{\gamma} = |a|_{\infty}^{\gamma}$. Therefore, (3.2) and (3.3) imply that

$$\frac{|a|_{\infty}^{\frac{r^2}{\gamma}}}{\log\gamma + \log\deg a + \log\log q} \ll_{\Psi,\mathscr{K}} \left[\mathscr{K}(\Psi[a]) : \mathscr{K}\right] \leq |a|_{\infty}^{\frac{r^2}{\gamma}}.$$

Finally, recalling the construction and properties of $\widetilde{\psi}, \overline{\psi}$, and Ψ in relation to ψ, these bounds imply the ones stated in the theorem. ■

3.7 Arithmetic in Division Fields

Let K be a finite field extension of k and let $\psi \in \mathrm{Drin}_A(K)$ be of generic characteristic and rank $r \geq 1$. We focus on providing properties of the primes splitting completely in the division fields of ψ.

Let $\wp \in \mathcal{P}_{\psi}$ and let $\mathfrak{l} = \ell A$ be a prime of k such that $\mathfrak{l} \neq \wp \cap A$. Let $\sigma_{\wp}$ denote the Frobenius at $\wp$ in $K(\psi[\ell])/K$. The *characteristic polynomial of the Frobenius* $\sigma_{\wp}$ *at* $\wp$, defined by

$$\begin{aligned} P_{\psi,\wp}^{\mathfrak{l}}(X) &:= \det\big(X\,\mathrm{Id} - \rho_{\psi,\mathfrak{l}}(\sigma_{\wp})\big) \\ &= X^r + a_{r-1,\wp}(\psi)X^{r-1} + \cdots + a_{1,\wp}(\psi)X + a_{0,\wp}(\psi) \in A_{\mathfrak{l}}[X], \end{aligned}$$

is very useful in describing further properties of $\wp$ when it splits completely in a division field of K. We recall the basic properties of this polynomial.

Theorem 3.15 ([Ge, Corollary 3.4, p. 193; Theorem 5.1, p. 199]) *Let K be a finite field extension of k and let $\psi \in \mathrm{Drin}_A(K)$ be of generic characteristic and rank $r \geq 1$. Let $\wp \in \mathcal{P}_{\psi}$ and let $\mathfrak{l} = \ell A$ be a prime of k such that $\mathfrak{l} \neq \wp \cap A$. The characteristic polynomial of the Frobenius at $\wp$ has the following properties.*

(i) $P_{\psi,\wp}^{\mathfrak{l}}(X) \in A[X]$; *in particular,* $P_{\psi,\wp}^{\mathfrak{l}}(X)$ *is independent of* $\mathfrak{l}$, *and, as such, we may drop the superscript* $\mathfrak{l}$ *from notation and simply write* $P_{\psi,\wp}(X)$.

(ii) *There exists* $u_{\wp}(\psi) \in \mathbb{F}_q^*$ *such that* $a_{0,\wp}(\psi) = u_{\wp}(\psi)p^{m_{\wp}}$, *where, we recall,* $m_{\wp} := [\mathbb{F}_{\wp} : \mathbb{F}_{\mathfrak{p}}]$.

(iii) *The roots of* $P_{\psi,\wp}(X)$ *have* $|\cdot|_{\infty}$*-norm less than or equal to* $|\wp|_{\infty}^{\frac{1}{r}}$.

(iv) $|a_{i,\wp}(\psi)|_{\infty} \leq |\wp|_{\infty}^{\frac{r-i}{r}}$ *for all* $0 \leq i \leq r-1$.

(v) $P_{\psi,\wp}(1)A = \chi(\psi(\mathbb{F}_{\wp}))$, *where, we recall,* $\chi(\psi(\mathbb{F}_{\wp}))$ *denotes the Euler–Poincaré characteristic of* $\psi(\mathbb{F}_{\wp})$.

Proposition 3.16 (Characterization of primes splitting completely in division fields) *Let K be a finite field extension of k and let $\psi \in \mathrm{Drin}_A(K)$ be of generic characteristic and rank $r \geq 1$. Let $\wp \in \mathcal{P}_\psi$ and let $m \in A^{(1)}$ be such that $\gcd(m, p) = 1$, where $\wp \cap A = pA$. Then $\psi(\mathbb{F}_\wp)$ contains an A-submodule isomorphic to $(A/mA)^r$ if and only if $\wp$ splits completely in $K(\psi[m])/K$. Consequently, given $d \in A^{(1)}$ with $\gcd(d, p) = 1$, we have that $d_{1,\wp}(\psi) = d$ if and only if $\wp$ splits completely in $K(\psi[d])/K$ and $\wp$ does not split completely in $K(\psi[d\ell])/K$ for any prime $\ell \in A$ such that $\ell \neq p$.*

Proof Let $\pi_\wp$ be the Frobenius automorphism of $\psi(\mathbb{F}_\wp)$, which may also be viewed as a root of $P_{\psi,\wp}$. Note that $\mathrm{Ker}(\pi_\wp - 1) = \psi(\mathbb{F}_\wp)$. Since $\gcd(m, p) = 1$, Theorem 3.3 tells us that $(\psi \otimes \mathbb{F}_\wp)[m] \simeq_A (A/mA)^r$. Therefore, $\psi(\mathbb{F}_\wp)$ contains an isomorphic copy of $(A/mA)^r$ if and only if $(\psi \otimes \mathbb{F}_\wp)[m] \leq_A \psi(\mathbb{F}_\wp) = \mathrm{Ker}(\pi_\wp - 1)$.

If $\sigma_\wp$ denotes the Frobenius at $\wp$ in $K(\psi[m])/K$, then

$$(\psi \otimes \mathbb{F}_\wp)[m] \leq_A \mathrm{Ker}(\pi_\wp - 1)$$

if and only if $\psi[m] \leq_A \mathrm{Ker}(\sigma_\wp - 1)$. This last statement is equivalent to $\sigma_\wp$ acting trivially on $\psi[m]$, and hence to $\wp$ splitting completely in $K(\psi[m])/K$. ■

Proposition 3.17 *Let K be a finite field extension of k and let $\psi \in \mathrm{Drin}_A(K)$ be of generic characteristic and rank $r \geq 1$. Let $\wp \in \mathcal{P}_\psi$ and let $a \in A \backslash \mathbb{F}_q$ be such that $\gcd(a, p) = 1$, where $\wp \cap A = pA$. If $\wp$ splits completely in $K(\psi[a])$, then $a^r \mid P_{\psi,\wp}(1)$.*

Proof Again, let $\pi_\wp$ be the Frobenius automorphism of $\psi(\mathbb{F}_\wp)$. Since $\wp$ splits completely in $K(\psi[a])$, $\sigma_\wp$ acts trivially on $\psi[a]$, and so $(\psi \otimes \mathbb{F}_\wp)[a] \leq_A \mathrm{Ker}(\pi_\wp - 1)$. Recalling the structure of the torsion of $\psi \otimes \mathbb{F}_\wp$, we deduce that $\psi(\mathbb{F}_\wp)$ contains an isomorphic copy of $(A/aA)^r$. By taking the Euler–Poincaré characteristic and invoking Proposition 3.15(v), we infer the desired divisibility relation. ■

By combining Proposition 3.17 with the results of [He] providing a Drinfeld module analogue of the Weil pairing for elliptic curves, we obtain the following theorem.

Theorem 3.18 (Properties of primes splitting completely in division fields) *Let K be a finite field extension of k and let $\psi \in \mathrm{Drin}_A(K)$ be of generic characteristic and rank $r \geq 2$. Then there exists $\psi^1 \in \mathrm{Drin}_A(K)$, of generic characteristic and of rank 1, uniquely determined up to $\overline{K}$-isomorphism, such that:*

(i) $\mathcal{P}_\psi \subseteq \mathcal{P}_{\psi^1}$;

(ii) *for any $\wp \in \mathcal{P}_\psi$, the characteristic polynomials of ψ and ψ^1 at $\wp$ are such that*

$$P_{\psi,\wp}(X) = X^r + a_{r-1,\wp}(\psi)X^{r-1} + \cdots + a_1(\psi,\wp)X + u_\wp(\psi)p^{m_\wp},$$
$$P_{\psi^1,\wp}(X) = X + (-1)^{r-1}u_\wp(\psi)p^{m_\wp},$$

where $u_\wp(\psi) \in \mathbb{F}_q^*$;

(iii) *for any $\wp \in \mathcal{P}_\psi$ and any $a \in A\backslash\mathbb{F}_q$ coprime to p, where $\wp \cap A = pA$, if $\wp$ splits completely in $K(\psi[a])$, then*

(a) *$\wp$ also splits completely in $K(\psi^1[a])$;*

(b) *$a^r | P_{\psi,\wp}(1)$;*

(c) *$a | P_{\psi^1,\wp}(1)$.*

https://doi.org/10.4153/CJM-2015-006-9 Published online by Cambridge University Press

Proof See [CoSh, Proposition 10]. ∎

4 The Chebotarev Density Theorem

Let K be a finite field extension of k and let K'/K be a finite Galois extension. In this section, we recall an effective version of the Chebotarev Density Theorem for K'/K, as proved in [MuSc].

Let $g_{K'}$ and g_K be the genera of K' and K, respectively, and let $c_{K'}$ denote the degree of the constant field $\mathbb{F}_{K'}$ of K' over $\mathbb{F}_K$, that is,

$$c_{K'} := [K' \cap \overline{\mathbb{F}}_K : \mathbb{F}_K].$$

Let

$$D := \sum_{\wp \text{ ramified in } K'/K} \deg_K \wp .$$

Let $x \in \mathbb{N}$ and set

$$\Pi(x; K'/K) := \#\{\wp \text{ unramified in } K'/K : \deg_K \wp = x\}.$$

For $C \subseteq \mathrm{Gal}(K'/K)$ a conjugacy class, set

$$\Pi_C(x; K'/K) := \#\{\wp \text{ unramified in } K'/K : \deg_K \wp = x, \sigma_\wp = C\},$$

where $\sigma_\wp$ is the Frobenius at $\wp$ in K'/K. Note that, in particular, $\Pi_1(x; K'/K)$ denotes the number of degree x primes of K that split completely in K'. Let $a_C \in \mathbb{N}$ be defined by the property that the restriction of C to $\mathbb{F}_{K'}$ is τ^{a_C}.

Theorem 4.1 ([MuSc, Theorem 1, p. 524]) *We keep the above setting and notation.*

(i) *If $x \not\equiv a_C \pmod{c_{K'}}$, then $\Pi_C(x; K'/K) = 0$.*

(ii) *If $x \equiv a_C \pmod{c_{K'}}$, then*

$$\Big| \Pi_C(x; K'/K) - c_{K'} \frac{|C|}{|G|} \Pi(x; K'/K) \Big| \le 2 g_{K'} \frac{|C|}{|G|} \frac{q^{\frac{c_K x}{2}}}{x} + 2(2g_K + 1)|C| \frac{q^{\frac{c_K x}{2}}}{x} + \Big(1 + \frac{|C|}{x}\Big) D.$$

Our main application of Theorem 4.1 is when K' is a division field of a generic Drinfeld module $\psi \in \mathrm{Drin}_A(K)$ and $C = \{1\}$. We record a restatement of this theorem in our desired setting.

Theorem 4.2 *Let K be a finite field extension of k and let $\psi \in \mathrm{Drin}_A(K)$ be of generic characteristic. Let $a \in A \backslash \mathbb{F}_q$. Let $x \in \mathbb{N}$ and define*

$$c_a(x) := \begin{cases} c_a & \text{if } c_a | x, \\ 0 & \text{else}, \end{cases} \tag{4.1}$$

where c_a denotes the degree of the constant field extension of $K(\psi[a])$ over $\mathbb{F}_K$ (see (3.1)). Then

$$\Pi_1(x; K(\psi[a])/K) = \frac{c_a(x)}{[K(\psi[a]) : K]} \cdot \frac{q^{c_K x}}{x} + \mathrm{O}_{\psi,K}\Big(\frac{q^{\frac{c_K x}{2}}}{x} \deg a \Big).$$

https://doi.org/10.4153/CJM-2015-006-9 Published online by Cambridge University Press

Proof Using the effective Prime Number Theorem for K (see (1.5)) and Theorem 4.1 with $K' = K(\psi[a])$, $C = \{1\}$, and hence with $a_C = 0$, we obtain

$$\Pi_1(x; K(\psi[a])/K) = \frac{c_a(x)}{[K(\psi[a]) : K]} \cdot \frac{q^{c_K x}}{x} + \mathrm{O}\bigg(\Big(2g_a \cdot \frac{1}{[K(\psi[a]):K]} + 2(2g_K + 1) \Big) \cdot \frac{q^{\frac{c_K x}{2}}}{x} + \Big(1 + \frac{1}{x}\Big) D \bigg),$$

where

$$D := \sum_{\substack{\wp \in \mathcal{P}_\psi \\ \wp \text{ ramified in } K(\psi[a])/K}} \deg_K \wp .$$

By Theorem 3.6, $D \ll_K \deg a$. Combining this with Proposition 3.9, we obtain

$$\begin{aligned} &\Big(2g_a \cdot \frac{1}{[K(\psi[a]):K]} + 2(2g_K + 1) \Big) \cdot \frac{q^{\frac{c_K x}{2}}}{x} + \Big(1 + \frac{1}{x}\Big) D \\ &\ll_K \frac{G(\psi, K) \cdot [K(\psi[a]):K] \cdot \deg a}{[K(\psi[a]):K]} \cdot \frac{q^{\frac{c_K x}{2}}}{x} + \frac{x+1}{x} \cdot \deg a \\ &\ll_K G(\psi, K) \cdot \frac{q^{\frac{c_K x}{2}}}{x} \cdot \deg a. \end{aligned}$$

■

5 Proofs of Theorems 1.1 and 1.2

Let K/k be a finite field extension and let $\psi\colon A \to K\{\tau\}$ be a generic Drinfeld A-module over K, of rank $r \geq 2$. Let $d \in A^{(1)}$. For a fixed $x \in \mathbb{N}$, let

$$\mathscr{D}(\psi, x) := \#\{\wp \in \mathcal{P}_\psi : \deg_K \wp = x,\ d_{1,\wp}(\psi) = d\}.$$

Our first goal is to derive an asymptotic formula for this function, as $x \to \infty$.

We start by noting that, for any prime $\wp \in \mathcal{P}_\psi$ such that $\gcd(d, p) = 1$ (where, as usual, $\wp \cap A = pA$), we have $d = d_{1,\wp}(\psi)$ if and only if $\psi(\mathbb{F}_\wp) \geq_A (A/dA)^r$ and $\psi(\mathbb{F}_\wp) \not\geq_A (A/\ell dA)^r$ for all primes $\ell \in A^{(1)}$. Hence, by the inclusion-exclusion principle and by Proposition 3.16,

$$\mathscr{D}(\psi, x) = \sum_{\substack{m \in A^{(1)} \\ \deg m \leq \frac{c_K x}{r}}} \mu_A(m) \Pi_1\big(x; K(\psi[md])/K\big), \tag{5.1}$$

where, for square-free m, the field extension $K(\psi[md])/K$ is obtained via field composition

$$\prod_{\substack{\ell | m \\ \ell \text{ prime}}} K(\psi[\ell d]) = K\big(\psi[\operatorname{lcm}(\ell d : \ell | m)]\big) = K(\psi[md]),$$

and where, we recall,

$$\Pi_1(x; K(\psi[md])/K) := \#\big\{ \wp \in \mathcal{P}_\psi : \deg_K \wp = x, \wp \text{ splits completely in } K(\psi[md])/K \big\}.$$

https://doi.org/10.4153/CJM-2015-006-9 Published online by Cambridge University Press

The range of $\deg m$ in the summation on the right-hand side of (5.1) is derived from the condition that if $\wp$ splits completely in $K(\psi[md])$, then

$$(A/mdA)^r \leq_A \psi(\mathbb{F}_\wp).$$

This gives the divisibility relation $m^r d^r \mid \chi(\psi(\mathbb{F}_\wp))$ obtained by taking Euler–Poincaré characteristic on both sides. Indeed, since $|\chi(\psi(\mathbb{F}_\wp))|_\infty = |\wp|_\infty = q^{c_K x}$, the above gives

$$\deg m \leq \frac{c_K x}{r}. \tag{5.2}$$

The obvious tool in estimating $\mathscr{D}(\psi, x)$ is the effective Chebotarev Density Theorem (Theorem 4.2). However, for $r = 2$, this is insufficient. As such, we split the sum into two parts, apply Theorem 4.2 to the first, and find a different approach for the second. To be precise, we write

$$\mathscr{D}(\psi, x) = \mathscr{D}_1(\psi, x, y) + \mathscr{D}_2(\psi, x, y) \tag{5.3}$$

for some positive real number $y = y(x)$, to be chosen optimally later, where

$$\mathscr{D}_1(\psi, x, y) := \sum_{\substack{m\in A^{(1)}\\ \deg m \leq y}} \mu_A(m)\Pi_1\big(x; K(\psi[md])/K\big),$$

$$\mathscr{D}_2(\psi, x, y) := \sum_{\substack{m\in A^{(1)}\\ y<\deg m \leq \frac{c_K x}{r}}} \mu_A(m)\Pi_1\big(x; K(\psi[md])/K\big).$$

By applying Theorem 4.2 and Lemma 2.1, we obtain

$$\mathscr{D}_1(\psi, x, y) = \frac{q^{c_K x}}{x} \sum_{\substack{m\in A^{(1)}\\ \deg m \leq y}} \frac{\mu_A(m) c_{md}(x)}{[K(\psi[md]):K]} + \mathrm{O}_{\psi,K,d}\Big(\frac{q^{\frac{c_K x}{2}+y} y}{x}\Big).$$

Now let $\gamma := \operatorname{rank}_A \operatorname{End}_{\overline{K}}(\psi)$. By Proposition 3.8, Theorem 3.14, and Lemma 2.2 (for which we are also using that $\gamma \leq r$), we obtain

$$\sum_{\substack{m\in A^{(1)}\\ \deg m > y}} \frac{\mu_A(m) c_{md}(x)}{[K(\psi[md]):K]} \ll_{\psi,K,d} \sum_{\substack{m\in A^{(1)}\\ \deg m > y}} \frac{\log\deg(md) + \log\log q}{q^{\frac{r^2 \deg(md)}{\gamma}}} \ll \frac{\log y}{q^{(\frac{r^2}{\gamma}-1)y}}. \tag{5.4}$$

Thus,

$$\mathscr{D}_1(\psi, x, y) = \frac{q^{c_K x}}{x} \sum_{m\in A^{(1)}} \frac{\mu_A(m) c_{md}(x)}{[K(\psi[md]):K]} + \mathrm{O}_{\psi,K,d}\Big(\frac{q^{\frac{c_K x}{2}+y} y}{x}\Big) + \mathrm{O}_{\psi,K}\Big(q^{c_K x - (\frac{r^2}{\gamma}-1)y} \log y\Big). \tag{5.5}$$

Observe that by choosing $y := \frac{1}{r} c_K x$, if $r \geq 4$, then the above estimate already proves the first part of the theorem. The following discussion thus pertains to the case $r \leq 3$.

To estimate $\mathscr{D}_2(\psi, x, y)$ from above, we make use of van der Heiden's construction of the analogue of the Weil pairing for ψ, as well as of the average over m. More precisely, we appeal to Theorem 3.18 and rely on the properties of the rank 1 Drinfeld A-module $\psi^1 \in \operatorname{Drin}_A(K)$ associated with ψ, as follows.

By Theorem 3.18(iii), if $\wp$ splits completely in $K(\psi[md])/K$, then $\wp$ splits completely in $K(\psi^1[md])/K$. Using the characteristic polynomials at $\wp$ associated with ψ and ψ^1, by Theorem 3.18(ii), this implies that

$$m^r d^r \mid 1 + a_\wp(\psi) + u_\wp(\psi) p^{m_\wp} \quad \text{and} \quad md \mid 1 + (-1)^{r-1} u_\wp(\psi) p^{m_\wp},$$

where, we recall,

$$P_{\wp,\psi}(X) = X^r + a_{r-1,\wp}(\psi) X^{r-1} + \cdots + a_{1,\wp}(\psi) X + u_\wp(\psi) p^{m_\wp} \in A[X]$$

with $u_\wp(\psi) \in \mathbb{F}_q^*$, and where we define

$$a_\wp(\psi) := a_{r-1,\wp}(\psi) + \cdots + a_{1,\wp}(\psi).$$

By Theorem 3.15(iv), we obtain that

$$\deg a_\wp(\psi) \leq \frac{(r-1) c_K \deg_K \wp}{r}.$$

Therefore,

$$\left| \mathscr{D}_2(\psi, x, y) \right| \leq \sum_{\substack{m \in A^{(1)} \\ y < \deg m \leq \frac{c_K x}{r}}} \sum_{u \in \mathbb{F}_q^*} \sum_{\substack{a \in A \\ \deg a \leq \frac{(r-1) c_K x}{r}}} \sum_{\substack{\wp \in \mathcal{P}_\psi \\ \deg_K \wp = x \\ a_\wp(\psi) = a, u_\wp(\psi) = u \\ m^r d^r | 1 + a_\wp(\psi) + u_\wp(\psi) p^{m_\wp} \\ md | 1 + (-1)^{r-1} u_\wp(\psi) p^{m_\wp}}} 1.$$

To simplify notation, for each $a \in A$ let us define

$$\widetilde{a} := \begin{cases} 2 + a & \text{if } r \text{ even}, \\ a & \text{if } r \text{ odd}. \end{cases}$$

Thus

$$\left| \mathscr{D}_2(\psi, x, y) \right| \leq \sum_{\substack{m \in A^{(1)} \\ y < \deg m \leq \frac{c_K x}{r}}} \sum_{u \in \mathbb{F}_q^*} \sum_{\substack{a \in A \\ \deg a \leq \frac{(r-1) c_K x}{r} \\ md | \widetilde{a}}} \sum_{\substack{\wp \in \mathcal{P}_\psi \\ \deg_K \wp = x \\ m^r d^r | 1 + a + u p^{m_\wp}}} 1.$$

We now consider the innermost sum above. Using diagram (2.1), we see that

$$\deg p^{m_\wp} = m_\wp \deg p = c_K \deg_K \wp = c_K x.$$

We also see that, by Lemma 2.1(i), for fixed $a \in A$ and $u \in \mathbb{F}_q^*$, there exist at most $q^{c_K x - r \deg m + 1}$ primes $p \in A$ of degree $\frac{c_K x}{m_\wp}$ such that $m^r | 1 + a + u p^{m_\wp}$. Indeed, this reduces to counting polynomials in A of degree $\deg(1 + a + u p^{m_\wp}) - r \deg m = c_K x - r \deg m$. But there are at most $[K : k]$ primes in K lying above a fixed prime $p \in A$. Therefore,

$$\sum_{\substack{\wp \in \mathcal{P}_\psi \\ \deg_K \wp = x \\ m^r | 1 + a + u p^{m_\wp}}} 1 \ll_K q^{c_K x - r \deg m + 1} \ll q^{c_K x - r \deg m}.$$

https://doi.org/10.4153/CJM-2015-006-9 Published online by Cambridge University Press

Continuing, we deduce that

$$\begin{aligned}
\mathscr{D}_2(\psi, x, y) &\ll_{K,d} \sum_{\substack{m \in A^{(1)} \\ y < \deg m \leq \frac{c_K x}{r}}} \sum_{u \in \mathbb{F}_q^*} \sum_{\substack{a \in A \\ \deg a \leq \frac{(r-1)c_K x}{r} \\ m \mid \widetilde{a}}} q^{c_K x - r \deg m} \\
&= q^{c_K x} \sum_{\substack{m \in A^{(1)} \\ y < \deg m \leq \frac{c_K x}{r}}} q^{-r \deg m} \sum_{u \in \mathbb{F}_q^*} \sum_{\substack{a \in A \\ \deg a \leq \frac{(r-1)c_K x}{r} \\ \widetilde{a} \neq 0 \\ m \mid \widetilde{a}}} 1 \\
&\quad + q^{c_K x} \sum_{\substack{m \in A^{(1)} \\ y < \deg m \leq \frac{c_K x}{r}}} q^{-r \deg m} \sum_{u \in \mathbb{F}_q^*} \sum_{\substack{a \in A \\ \deg a \leq \frac{(r-1)c_K x}{r} \\ \widetilde{a} = 0}} 1 \\
&=: \mathscr{D}_{2,1}(\psi, x, y) + \mathscr{D}_{2,2}(\psi, x, y).
\end{aligned}$$

We will estimate these two sums from above using Lemmas 2.1 and 2.2, where, for the latter, we will be implicitly also using that $\gamma \leq r$.

To estimate $\mathscr{D}_{2,1}(\psi, x, y)$ from above, we note that

$$\mathscr{D}_{2,1}(\psi, x, y) \leq q^{c_K x + 1} \sum_{\substack{m \in A^{(1)} \\ y < \deg m \leq \frac{c_K x}{r}}} q^{-r \deg m} \sum_{\substack{\alpha \in A \\ \deg \alpha \leq \frac{(r-1)c_K x}{r} - \deg m}} 1,$$

which, by Lemmas 2.1(i) and 2.2(i), is

$$\ll q^{c_K x + 1} \sum_{\substack{m \in A^{(1)} \\ y < \deg m \leq \frac{c_K x}{r}}} q^{-r \deg m} q^{\frac{(r-1)c_K x}{r} - \deg m} \ll q^{\frac{(2r-1)c_K x}{r} - r y}.$$

To estimate $\mathscr{D}_{2,2}(\psi, x, y)$ from above, we note that its innermost sum has only one term, hence, by Lemma 2.2(i),

$$\mathscr{D}_{2,2}(\psi, x, y) \ll q^{c_K x - (r-1) y}.$$

Combining these estimates, we obtain that

$$\mathscr{D}_2(\psi, x, y) \ll_{K,d} q^{\frac{(2r-1)c_K x}{r} - r y} + q^{c_K x - (r-1) y}.$$

Plugging this back into (5.3) and appealing to (5.5), we deduce that

$$\begin{aligned}
(5.6) \quad \mathscr{D}(\psi, x) = \frac{q^{c_K x}}{x} \sum_{m \in A^{(1)}} \frac{\mu_A(m) c_{md}(x)}{[K(\psi[md]) : K]} &+ \mathrm{O}_{\psi,K,d}\Big(\frac{q^{\frac{c_K x}{2} + y} y}{x}\Big) \\
&+ \mathrm{O}_{\psi,K}\Big(q^{c_K x - (\frac{r^2}{\gamma} - 1) y} \log y\Big) + \mathrm{O}_{K,d}\Big(q^{\frac{(2r-1)c_K x}{r} - r y} + q^{c_K x - (r-1) y}\Big).
\end{aligned}$$

Finally, we choose y as follows:

$$y := \begin{cases} \frac{3r-2}{2r(r+1)} c_K x & \text{if } r = 2, 3, \\ \frac{1}{r} c_K x & \text{if } r \geq 4. \end{cases}$$

https://doi.org/10.4153/CJM-2015-006-9 Published online by Cambridge University Press

We plug this into (5.6) if $r = 2, 3$, and into (5.5) if $r \geq 4$ (note that in this case $\mathscr{D}(\psi, x) = \mathscr{D}_1(\psi, x, y)$), obtaining the effective asymptotic formulae

$$\mathscr{D}(\psi, x) = \frac{q^{c_K x}}{x} \sum_{m \in A^{(1)}} \frac{\mu_A(m) c_{md}(x)}{[K(\psi[md]):K]} + \begin{cases} \mathrm{O}_{\psi,K,d}(q^{\frac{5c_K x}{6}}) & \text{if } r = 2, \\ \mathrm{O}_{\psi,K,d}(q^{\frac{19c_K x}{24}}) & \text{if } r = 3, \\ \mathrm{O}_{\psi,K,d}(q^{\frac{(r+2)c_K x}{2r}}) & \text{if } r \geq 4. \end{cases} \tag{5.7}$$

This completes the first part of Theorem 1.1.

Remark 5.1 (i) Formula (5.7) is stronger than the asymptotic formula (1.6) stated in Theorem 1.1, as it provides us with explicit error terms. Moreover, these error terms carry significant savings in powers of $q^{c_K x}$.

(ii) For $r \geq 4$, the splitting of $\mathscr{D}(\psi, x)$ into two parts, as in (5.3), is unnecessary. The proof of Theorem 1.1 in this case is solely an application of the effective Chebotarev Density Theorem for the division fields of ψ.

(iii) For $r = 3$, the splitting of $\mathscr{D}(\psi, x)$ into two parts, as in (5.3), is also unnecessary in order to obtain the asymptotic formula (1.6). In our proof, we do so in order to obtain a saving in the final error term: $\mathrm{O}_{\psi,K,d}(q^{\frac{19c_K x}{24}})$ using (5.3) and the approach therein for estimating $\mathscr{D}_2(\psi, x, y)$, versus $\mathrm{O}_{\psi,K,d}(q^{\frac{5c_K x}{6}})$ using only the effective Chebotarev Density Theorem (and the choice $y := \frac{1}{3} c_K x$).

(iv) The error terms in (5.7) may be improved with additional techniques. For example, for the case q odd, $r = 2$, $\gamma = 2$, and $K = k$, in [CoSh] we proved the formula

$$\mathscr{D}(\psi, x) = \frac{q^x}{x} \sum_{m \in A^{(1)}} \frac{\mu_A(m) c_{md}(x)}{[k(\psi[md]):k]} + \mathrm{O}_{\psi,k,d}(q^{\frac{3x}{4}}).$$

Our second goal is to prove that the Dirichlet density of the set

$$\left\{ \wp \in \mathcal{P}_\psi : d_{1,\wp}(\psi) = d \right\}$$

exists and equals $\sum_{m \in A^{(1)}} \frac{\mu_A(m)}{[K(\psi[md]):K]}$. For this, let $s > 1$ and consider the sum

$$\begin{aligned} \sum_{\substack{\wp \in \mathcal{P}_\psi \\ d_{1,\wp}(\psi) = d}} q^{-sc_K \deg_K \wp} &= \sum_{x \geq 1} q^{-sc_K x} \mathscr{D}(\psi, x) \\ &= \sum_{m \in A^{(1)}} \frac{\mu_A(m)}{[K(\psi[md]):K]} \sum_{x \geq 1} \frac{q^{(1-s)c_K x} c_{md}(x)}{x} + \mathrm{O}_{\psi,K}\Big(\sum_{x \geq 1} q^{(\theta(r)-s)c_K x} \Big), \end{aligned} \tag{5.8}$$

where we used (5.7) with

$$\theta(r) := \begin{cases} \frac{5}{6} & \text{if } r = 2, \\ \frac{19}{24} & \text{if } r = 3, \\ \frac{r+2}{2r} & \text{if } r \geq 4. \end{cases}$$

By the definition (4.1) of $c_{md}(x)$, (5.8) becomes

$$= \sum_{m \in A^{(1)}} \frac{\mu_A(m)}{[K(\psi[md]):K]} \sum_{j \geq 1} \frac{q^{(1-s)c_K c_{md} j}}{j} + \mathrm{O}_{\psi,K}\Big(\sum_{x \geq 1} q^{(\theta(r)-s)c_K x} \Big).$$

Since $s > 1$, this can be written as

$$= -\sum_{m \in A^{(1)}} \frac{\mu_A(m)}{[K(\psi[md]):K]} \log\big(1 - q^{(1-s)c_K c_{md}}\big) + \mathrm{O}_{\psi,K}\Big(\frac{q^{(\theta(r)-s)c_K}}{1 - q^{(\theta(r)-s)c_K}}\Big).$$

We now calculate

$$\begin{aligned}
&\lim_{s \to 1+} \frac{\sum_{\substack{\wp \in \mathcal{P}_\psi \\ d_{1,\wp}(\psi)=d}} q^{-sc_K \deg_K \wp}}{-\log(1 - q^{(1-s)c_K})} \\
&\quad = \lim_{s \to 1+} \Big[\sum_{m \in A^{(1)}} \frac{\mu_A(m)}{[K(\psi[md]):K]} \frac{\log(1 - q^{(1-s)c_K c_{md}})}{\log(1 - q^{(1-s)c_K})} \\
&\qquad\qquad + \mathrm{O}_{\psi,K}\Big(\frac{q^{(\theta(r)-s)c_K}}{(1 - q^{(\theta(r)-s)c_K}) \log(1 - q^{(1-s)c_K})}\Big)\Big] \\
&\quad = \sum_{m \in A^{(1)}} \frac{\mu_A(m)}{[K(\psi[md]):K]},
\end{aligned}$$

obtained after an application of l'Hospital and elementary manipulations. This completes the proof of Theorem 1.1.

The proof of Theorem 1.2 proceeds in the same way as that of the first part of Theorem 1.1, after replacing with 1 the factor $\mu_A(m)$ appearing in (5.1), and, henceforth, in $\mathcal{D}_1(\psi, x, y)$ and $\mathcal{D}_2(\psi, x, y)$ of (5.3). In particular, this approach leads to the asymptotic formulae

$$\begin{aligned}
(5.9)\quad &\sum_{m \in A^{(1)}} \Pi_1(x, K(\psi[m])/K) \\
&= \sum_{\substack{m \in A^{(1)} \\ \deg m \le \frac{c_K x}{r}}} \Pi_1(x, K(\psi[m])/K) \\
&= \frac{q^{c_K x}}{x} \sum_{\substack{m \in A^{(1)} \\ \deg m \le \frac{c_K x}{r}}} \frac{c_m(x)}{[K(\psi[m]):K]} + \begin{cases} \mathrm{O}_{\psi,K}(q^{\frac{5c_K x}{6}}) & \text{if } r = 2, \\ \mathrm{O}_{\psi,K}(q^{\frac{19c_K x}{24}}) & \text{if } r = 3, \\ \mathrm{O}_{\psi,K}(q^{\frac{(r+2)c_K x}{2r}}) & \text{if } r \ge 4 \end{cases} \\
&= \frac{q^{c_K x}}{x} \sum_{m \in A^{(1)}} \frac{c_m(x)}{[K(\psi[m]):K]} + \begin{cases} \mathrm{O}_{\psi,K}(q^{\frac{5c_K x}{6}}) & \text{if } r = 2, \\ \mathrm{O}_{\psi,K}(q^{\frac{19c_K x}{24}}) & \text{if } r = 3, \\ \mathrm{O}_{\psi,K}(q^{\frac{(r+2)c_K x}{2r}}) & \text{if } r \ge 4. \end{cases} \qquad \blacksquare
\end{aligned}$$

6 Proof of Theorem 1.3

Let K/k be a finite field extension and let $\psi\colon A \to K\{\tau\}$ be a generic Drinfeld A-module over K, of rank 2. Let $\gamma := \operatorname{rank}_A \operatorname{End}_{\overline{K}}(\psi)$.

(i) Let $f\colon (0,\infty) \to (0,\infty)$ be such that $\lim_{x\to\infty} f(x) = \infty$. For a fixed $x \in \mathbb{N}$, let

$$\mathcal{E}(\psi, x) = \mathcal{E}_f(\psi, x) := \#\Big\{\wp \in \mathcal{P}_\psi : \deg_K \wp = x, |d_{2,\wp}(\psi)|_\infty > \frac{|\wp|_\infty}{q^{c_K f(x)}}\Big\},$$

$$e(\psi, x) = e_f(\psi, x) := \#\Big\{\wp \in \mathcal{P}_\psi : \deg_K \wp = x, |d_{2,\wp}(\psi)|_\infty < \frac{|\wp|_\infty}{q^{c_K f(x)}}\Big\}.$$

https://doi.org/10.4153/CJM-2015-006-9 Published online by Cambridge University Press

Our goal is to derive an asymptotic formula for $\mathcal{E}(\psi, x)$, as $x \to \infty$. More precisely, our goal is to show that $\mathcal{E}(\psi, x) \sim \pi_K(x)$, which is equivalent to showing that

$$e(\psi, x) = \mathrm{o}\big(\pi_K(x)\big).$$

Note that, without loss of generality, we may assume that $f(x) < \frac{x}{2}$ for all x. Indeed, if $f_1, f_2 \colon (0, \infty) \to (0, \infty)$ satisfy $f_2 \le f_1$ and $\lim_{x\to\infty} f_2(x) = \infty$, then $\mathcal{E}_{f_2}(\psi, x) \le \mathcal{E}_{f_1}(\psi, x) \le \pi_K(x)$. Thus, for the purpose of proving Theorem 1.3(i), we may replace $f(x)$ by $\min\big\{f(x), \frac{x}{2} - 1\big\}$.

We start with the partition

$$e(\psi, x) = \sum_{d \in A^{(1)}} \sum_{\substack{\wp \in \mathcal{P}_\psi \\ \deg_K \wp = x \\ d_{1,\wp}(\psi) = d \\ |d_{2,\wp}(\psi)|_\infty < \frac{|\wp|_\infty}{q^{c_K f(x)}}}} 1,$$

and remark that, as in the deduction of (5.1) in the proof of Theorem 1.1, the condition $d = d_{1,\wp}(\psi)$ imposes the restriction $\deg d \le \frac{c_K x}{2}$. Moreover, the conditions $d_{1,\wp}(\psi) = d$ and $|d_{2,\wp}(\psi)|_\infty < \frac{|\wp|_\infty}{q^{c_K f(x)}}$, coupled with the remark

$$|\wp|_\infty = |\chi(\psi(\mathbb{F}_\wp))|_\infty = |d_{1,\wp}(\psi)|_\infty |d_{2,\wp}(\psi)|_\infty, \tag{6.1}$$

impose the restriction $c_K f(x) < \deg d$. Thus,

$$\begin{aligned} e(\psi, x) &\le \sum_{\substack{d \in A^{(1)} \\ c_K f(x) < \deg d \le \frac{c_K x}{2}}} \#\{\wp \in \mathcal{P}_\psi : \deg_K \wp = x, d \mid d_{1,\wp}(\psi)\} \\ &= \sum_{\substack{d \in A^{(1)} \\ c_K f(x) < \deg d \le \frac{c_K x}{2}}} \Pi_1(x, K(\psi[d])/K), \end{aligned}$$

by also using Proposition 3.16. Using version (5.9) of Theorem 1.2 for the range $\deg d \le \frac{c_K x}{2}$ and Theorem 4.2 for the range $\deg d \le c_K f(x)$, the above is

$$= \frac{q^{c_K x}}{x} \sum_{\substack{d \in A^{(1)} \\ c_K f(x) < \deg d \le \frac{c_K x}{2}}} \frac{c_d(x)}{[K(\psi[d]) : K]} + \mathrm{O}_{\psi,K}\Big(q^{\frac{5 c_K x}{6}}\Big) + \mathrm{O}_{\psi,K}\Big(\frac{q^{\frac{c_K x}{2} + c_K f(x)} f(x)}{x}\Big). \tag{6.2}$$

Reasoning as for (5.4) in the proof of Theorem 1.1 and using that now $\gamma \le 2$, the first term becomes

$$\ll_{\psi,K} q^{c_K (x - (\frac{4}{\gamma} - 1) f(x))} \frac{\log f(x)}{x}.$$

Since $\lim_{x\to\infty} f(x) = \infty$ and $f(x) < \frac{x}{2}$, we deduce that $e(\psi, x) = \mathrm{o}(\pi_K(x))$.

Remark 6.1 The same proof can be carried through in the case $r = 3$, leading to a weaker result. For $r \ge 4$, however, one requires a more careful analysis, which should also take into consideration the behaviour of the intermediate elementary divisors.

Reasoning as at the beginning of the proof, without loss of generality we may assume that there is $0 < \theta < 1$ such that $f(x) \le \frac{\theta x}{2}$ for all x. We now show that the Dirichlet density of the set $\{\wp \in \mathcal{P}_\psi : |d_{2,\wp}|_\infty < \frac{|\wp|_\infty}{q^{c_K f(\deg_K \wp)}}\}$ equals 0.

Let $s > 1$ and consider the sum

$$
\begin{aligned}
(6.3)\qquad & \sum_{\substack{\wp \in \mathcal{P}_\psi \\ |d_{2,\wp}(\psi)|_\infty < \frac{|\wp|_\infty}{q^{c_K f(\deg_K \wp)}}}} q^{-sc_K \deg_K \wp} \\
&= \sum_{x\geq 1} q^{-sc_K x} e(\psi, x) \\
&\ll \sum_{x\geq 1} \frac{q^{(1-s)c_K x}}{x} \sum_{\substack{d\in A^{(1)} \\ c_K f(x) < \deg d \leq \frac{c_K x}{2}}} \frac{c_d(x)}{[K(\psi[d]) : K]} + \sum_{x\geq 1} q^{(\frac{5}{6}-s)c_K x} \\
&\quad + \sum_{x\geq 1} \frac{q^{(\frac{1}{2}-s)c_K x + c_K f(x)} f(x)}{x} \\
&=: T_1 + T_2 + T_3;
\end{aligned}
$$

here we have also used the prior estimate (6.2).

First we focus on T_1. By the definition of $c_d(x)$, we obtain

$$
\begin{aligned}
(6.4)\qquad T_1 &:= \sum_{x\geq 1} \frac{q^{(1-s)c_K x}}{x} \sum_{\substack{d\in A^{(1)} \\ c_K f(x) < \deg d \leq \frac{c_K x}{2}}} \frac{c_d(x)}{[K(\psi[d]):K]} \\
&= \sum_{d\in A^{(1)}} \sum_{\substack{j\geq 1 \\ c_K f(c_d j) < \deg d \leq \frac{c_K c_d j}{2}}} \frac{q^{(1-s)c_K c_d j}}{j[K(\psi[d]):K]}.
\end{aligned}
$$

Let $M > 0$. Since $\lim_{x\to\infty} f(x) = \infty$, there exists $n(M) \in \mathbb{N}$ such that $f(n) > M$ for all $n \geq n(M)$. We split the inner sum in (6.4) according to whether $c_d j \geq n(M)$ and $c_d j < n(M)$, and consider each of the two emerging sums.

By the above and Theorem 3.14, we have

$$
\begin{aligned}
T_{1,1} &:= \sum_{d\in A^{(1)}} \sum_{\substack{j\geq 1 \\ c_d j \geq n(M) \\ c_K f(c_d j) < \deg d \leq \frac{c_K c_d j}{2}}} \frac{q^{(1-s)c_K c_d j}}{j[K(\psi[d]):K]} \\
&\leq \sum_{d\in A^{(1)}} \sum_{\substack{j\geq 1 \\ c_K M < \deg d \leq \frac{c_K c_d j}{2}}} \frac{q^{(1-s)c_K c_d j}}{j[K(\psi[d]) : K]} \\
&\ll_{\psi,K} \sum_{\substack{d\in A^{(1)} \\ c_K M < \deg d}} \frac{\log \deg d}{|d|_\infty^{\frac{4}{\gamma}}} \sum_{j\geq 1} \frac{q^{(1-s)c_K c_d j}}{j} \\
&\leq \sum_{\substack{d\in A^{(1)} \\ c_K M < \deg d}} \frac{\log \deg d}{|d|_\infty^{\frac{4}{\gamma}}} \sum_{j\geq 1} \frac{q^{(1-s)c_K j}}{j}.
\end{aligned}
$$

https://doi.org/10.4153/CJM-2015-006-9 Published online by Cambridge University Press

Since $s > 1$, the latter becomes

$$= - \sum_{\substack{d \in A^{(1)} \\ c_K M < \deg d}} \frac{\log \deg d}{|d|_\infty^{\frac{4}{\gamma}}} \log\big(1 - q^{(1-s)c_K}\big).$$

By Lemma 2.2, this is

$$\ll \frac{\log(c_K M)}{q^{\left(\frac{4}{\gamma}-1\right)c_K M}\log q} \left|\log\left(1 - q^{(1-s)c_K}\right)\right|,$$

which gives that

$$\lim_{s\to 1+} \frac{T_{1,1}}{-\log\left(1 - q^{(1-s)c_K}\right)} \ll \frac{\log(c_K M)}{q^{\left(\frac{4}{\gamma}-1\right)c_K M}\log q}. \tag{6.5}$$

We also have

$$T_{1,2} := \sum_{d \in A^{(1)}} \sum_{\substack{j \geq 1 \\ c_d j < n(M) \\ c_K f(c_d j) < \deg d \leq \frac{c_K c_d j}{2}}} \frac{q^{(1-s)c_K c_d j}}{j[K(\psi[d]):K]},$$

a finite sum. Since

$$\lim_{s\to 1+} \frac{q^{(1-s)c_K \alpha}}{\log(1 - q^{(1-s)c_K})} = 0$$

for any $\alpha \in \mathbb{N}$, we deduce that

$$\lim_{s\to 1+} \frac{T_{1,2}}{-\log(1 - q^{(1-s)c_K})} = 0. \tag{6.6}$$

By taking $M \to \infty$ and by using (6.5) and (6.6), we obtain that

$$\lim_{s\to 1+} \frac{T_1}{-\log(1 - q^{(1-s)c_K})} = 0. \tag{6.7}$$

We now focus on T_2 and note that

$$\lim_{s\to 1+} \frac{T_2}{-\log(1 - q^{(1-s)c_K})} = -\lim_{s\to 1+} \frac{q^{(\frac{5}{6}-s)c_K}}{(1 - q^{(\frac{5}{6}-s)c_K})\log(1 - q^{(1-s)c_K})} = 0. \tag{6.8}$$

It remains to focus on T_3. Recalling that now we are assuming that there exists $0 < \theta < 1$ such that $f(x) \leq \frac{\theta x}{2}\ \ \forall x$, we see that

$$\begin{aligned} \lim_{s\to 1+} \frac{T_3}{-\log(1 - q^{(1-s)c_K})} &= -\lim_{s\to 1+} \frac{\sum_{x\geq 1} \frac{q^{(\frac{1}{2}-s)c_K x + c_K f(x)} f(x)}{x}}{\log(1 - q^{(1-s)c_K})} \\ &\ll \left|\lim_{s\to 1+} \frac{\sum_{x\geq 1} q^{(\frac{1}{2}+\frac{\theta}{2}-s)c_K x}}{\log(1 - q^{(1-s)c_K})}\right| \\ &= \left|\lim_{s\to 1+} \frac{q^{(\frac{1}{2}+\frac{\theta}{2}-s)c_K}(1 - q^{(\frac{1}{2}+\frac{\theta}{2}-s)c_K})^{-1}}{\log(1 - q^{(1-s)c_K})}\right| = 0. \end{aligned} \tag{6.9}$$

https://doi.org/10.4153/CJM-2015-006-9 Published online by Cambridge University Press

By combining (6.3) with (6.7)–(6.9), we obtain

$$\lim_{s\to 1+} \sum_{\substack{\wp \in \mathcal{P}_\psi \\ |d_{2,\wp}(\psi)|_\infty < \frac{|\wp|_\infty}{q^{c_K f(\deg_K \wp)}}}} q^{-sc_K \deg_K \wp} \Big/ -\log(1-q^{(1-s)c_K}) = 0.$$

This completes the proof of the first part of Theorem 1.3.

(ii) In what follows, we investigate the average of $|d_{2,\wp}(\psi)|_\infty$ as $\wp \in \mathcal{P}_\psi$ varies over primes with $\deg_K \wp = x$. By using (6.1) and Lemma 2.4, and by partitioning the primes $\wp$ according to the divisors of $d_{1,\wp}(\psi)$, we obtain

$$\begin{aligned}
\mathcal{A}(\psi,x) &:= \frac{1}{q^{c_K x}} \sum_{\substack{\wp \in \mathcal{P}_\psi \\ \deg_K \wp = x}} |d_{2,\wp}(\psi)|_\infty = \frac{1}{q^{c_K x}} \sum_{\substack{\wp \in \mathcal{P}_\psi \\ \deg_K \wp = x}} \frac{|\wp|_\infty}{|d_{1,\wp}(\psi)|_\infty} \\
&= \sum_{\substack{\wp \in \mathcal{P}_\psi \\ \deg_K \wp = x}} \frac{1}{|d_{1,\wp}(\psi)|_\infty} = \frac{1}{(q-1)^2} \sum_{\substack{\wp \in \mathcal{P}_\psi \\ \deg_K \wp = x}} \sum_{\substack{a,b\in A \\ ab|d_{1,\wp}(\psi)}} \frac{\mu_A(a)}{|b|_\infty} \\
&= \sum_{\substack{\wp \in \mathcal{P}_\psi \\ \deg_K \wp = x}} \sum_{\substack{a,b\in A^{(1)} \\ ab|d_{1,\wp}(\psi)}} \frac{\mu_A(a)}{|b|_\infty} = \sum_{m\in A^{(1)}} \sum_{\substack{\wp \in \mathcal{P}_\psi \\ \deg_K \wp = x \\ m|d_{1,\wp}(\psi)}} \sum_{\substack{a,b\in A^{(1)} \\ ab|d_{1,\wp}(\psi)}} \frac{\mu_A(a)}{|b|_\infty} \\
&= \sum_{\substack{m\in A^{(1)} \\ \deg m \le \frac{c_K x}{2}}} \sum_{\substack{a,b\in A^{(1)} \\ ab=m}} \frac{\mu_A(a)}{|b|_\infty} \Pi_1(x, K(\psi[m])/K),
\end{aligned}$$

where in the last line we used Proposition 3.16 and the same derivation as (5.2) for the length of the sum over m.

Now we proceed similarly to the study of $\mathcal{D}(\psi,x)$ in the proof of Theorem 1.1. Specifically, we let $y := \frac{c_K x}{3}$ and write

$$\begin{aligned}
\mathcal{A}(\psi,x) = &\sum_{\substack{m\in A^{(1)} \\ \deg m \le y}} \sum_{\substack{a,b\in A^{(1)} \\ ab=m}} \frac{\mu_A(a)}{|b|_\infty} \Pi_1\big(x, K(\psi[m])/K\big) \\
&+ \sum_{\substack{m\in A^{(1)} \\ y<\deg m \le \frac{c_K x}{2}}} \sum_{\substack{a,b\in A^{(1)} \\ ab=m}} \frac{\mu_A(a)}{|b|_\infty} \Pi_1\big(x, K(\psi[m])/K\big) \\
=:& \mathcal{A}_1(\psi,x,y) + \mathcal{A}_2(\psi,x,y).
\end{aligned}$$

By Theorem 4.2,

$$\begin{aligned}
\mathcal{A}_1(\psi,x,y) = \frac{q^{c_K x}}{x} &\sum_{\substack{m\in A^{(1)} \\ \deg m \le y}} \frac{c_m(x)}{[K(\psi[m]):K]} \sum_{\substack{a,b\in A^{(1)} \\ ab=m}} \frac{\mu_A(a)}{|b|_\infty} \\
&+ \mathrm{O}_{\psi,K}\Bigg(\frac{q^{\frac{c_K x}{2}}}{x} \sum_{\substack{m\in A^{(1)} \\ \deg m \le y}} \deg m \sum_{\substack{a,b\in A^{(1)} \\ a \text{ squarefree} \\ ab=m}} \frac{1}{|b|_\infty} \Bigg).
\end{aligned}$$

https://doi.org/10.4153/CJM-2015-006-9 Published online by Cambridge University Press

By Lemma 2.5 and the observation that

$$\frac{\phi_A(\mathrm{rad}(m))}{|m|_\infty} \le 1, \tag{6.10}$$

the sum in the O-term of $\mathcal{A}_1(\psi, x, y)$ becomes

$$\ll \sum_{\substack{m\in A^{(1)}\\ \deg m\le y}} \frac{\phi_A(\mathrm{rad}(m))}{|m|_\infty} \deg m \ll q^y y,$$

upon also using Lemma 2.1(ii). Thus, recalling our choice of y, we obtain that

$$\mathcal{A}_1(\psi,x,y) = \frac{q^{c_K x}}{x} \sum_{\substack{m\in A^{(1)}\\ \deg m\le \frac{c_K x}{3}}} \frac{c_m(x)}{[K(\psi[m]):K]} \sum_{\substack{a,b\in A^{(1)}\\ ab=m}} \frac{\mu_A(a)}{|b|_\infty} + \mathrm{O}_{\psi,K}\big(q^{\frac{5c_K x}{6}}\big).$$

To extend the range of $\deg m$ in the above sum over m, we use Proposition 3.8, Theorem 3.14, Lemma 2.5, (6.10), and Lemma 2.2(ii). We obtain

$$\begin{aligned}
&\frac{q^{c_K x}}{x}\Big| \sum_{\substack{m\in A^{(1)}\\ \deg m> y}} \frac{c_m(x)}{[K(\psi[m]):K]} \sum_{\substack{a,b\in A^{(1)}\\ ab=m}} \frac{\mu_A(a)}{|b|_\infty}\Big| \\
&\quad \ll_\psi \frac{q^{c_K x}}{x} \sum_{\substack{m\in A^{(1)}\\ \deg m> y}} \frac{1}{[K(\psi[m]):K]} \sum_{\substack{a,b\in A^{(1)}\\ a \text{ squarefree}\\ ab=m}} \frac{1}{|b|_\infty} \\
&\quad \ll_\psi \frac{q^{c_K x}}{x} \sum_{\substack{m\in A^{(1)}\\ \deg m> y}} \frac{\log \deg m}{|m|_\infty^{\frac{4}{\gamma}}} \cdot \frac{\phi_A(\mathrm{rad}(m))}{|m|_\infty} \ll_\psi \frac{q^{c_K x - (\frac{4}{\gamma}-1)y} \log y}{xy},
\end{aligned}$$

using once again that $\gamma \le 2$. Recalling that $y = \frac{c_K x}{3}$, we deduce that

$$\mathcal{A}_1(\psi,x,y) = \frac{q^{c_K x}}{x} \sum_{m\in A^{(1)}} \frac{c_m(x)}{[K(\psi[m]):K]} \sum_{\substack{a,b\in A^{(1)}\\ ab=m}} \frac{\mu_A(a)}{|b|_\infty} + \mathrm{O}_{\psi,K}\big(q^{\frac{5c_K x}{6}}\big).$$

We now turn to $\mathcal{A}_2(\psi, x, y)$. By Lemma 2.5 and (6.10), we have

$$\begin{aligned}
|\mathcal{A}_2(\psi,x,y)| &\le \sum_{\substack{m\in A^{(1)}\\ y<\deg m\le \frac{c_K x}{2}}} \sum_{\substack{a,b\in A^{(1)}\\ a \text{ squarefree}\\ ab=m}} \frac{1}{|b|_\infty} \Pi_1(x, K(\psi[m])/K) \\
&\le \sum_{\substack{m\in A^{(1)}\\ y<\deg m\le \frac{c_K x}{2}}} \Pi_1(x, K(\psi[m])/K).
\end{aligned}$$

This is estimated exactly as $|\mathscr{D}_2(\psi, x, y)|$ in the proof of Theorem 1.1, giving the upper bound $\mathrm{O}_{\psi,K}(q^{\frac{5c_K x}{6}})$ (with $y = \frac{c_K x}{3}$).

Putting everything together, we deduce that

$$\mathcal{A}(\psi, x) = \frac{q^{c_K x}}{x} \sum_{m \in A^{(1)}} \frac{c_m(x)}{[K(\psi[m]):K]} \sum_{\substack{a,b \in A^{(1)} \\ ab=m}} \frac{\mu_A(a)}{|b|_\infty} + \mathrm{O}_{\psi,K}\big(q^{\frac{5c_K x}{6}}\big), \tag{6.11}$$

completing the proof of Theorem 1.3(ii).

Remark 6.2 As with Theorem 1.1, (6.11) is stronger than the asymptotic formula stated in Theorem 1.3(ii), as it provides us with explicit error terms. Moreover, when q is odd, $r = 2$, $\gamma = 2$, and $K = k$, the methods of [CoSh] lead to the improved formula

$$\frac{1}{q^x} \sum_{\substack{\wp \in \mathcal{P}_\psi \\ \deg \wp = x}} |d_{2,\wp}(\psi)|_\infty = \frac{q^x}{x} \sum_{d \in A^{(1)}} \frac{c_d(x)}{[k(\psi[d]) : k]} \sum_{\substack{m,n \in A^{(1)} \\ mn=d}} \frac{\mu_A(m)}{|n|_\infty} + \mathrm{O}_{\psi,k}\big(q^{\frac{3x}{4}}\big).$$

7 Concluding Remarks

Remark 7.1 Along with investigating the Drinfeld module analogues of (1.1) and (1.3), it is also natural to consider their analogues in the context of an elliptic curve E over a global function field. This is precisely the content of [CoTo]. For clarity, one of the results Cojocaru and Tóth prove is that, given an elliptic curve E over $K := \mathbb{F}_q(T)$ with $j(E) \notin \mathbb{F}_q$, then, provided $\operatorname{char} \mathbb{F}_q \geq 5$, for any $x \in \mathbb{N}$ such that $x \to \infty$ and for any $\varepsilon > 0$, we have

$$\#\{\mathfrak{p} \text{ prime of good reduction for } E : \deg(\mathfrak{p}) = x, E_\mathfrak{p}(\mathbb{F}_\mathfrak{p}) \text{ cyclic}\} = \sum_{\substack{m \geq 1 \\ (m, \operatorname{char} \mathbb{F}_q)=1 \\ m | q^x - 1}} \frac{\mu(m) c_m}{[K(E[m]):K]} \cdot \frac{q^x}{x} + \mathrm{O}_{E,\varepsilon}\Big(\frac{q^{x(\frac{1}{2}+\varepsilon)}}{x}\Big), \tag{7.1}$$

where $\mu(\cdot)$ is the Möbius function on $\mathbb{Z}$, $K(E[m])$ is the m-th division field of E, and c_m is the multiplicative order of q modulo m. The formula is unconditional. Unusually, it is a direct consequence of the effective Chebotarev Density Theorem for function fields, no extra sieving being required. This special simplification occurs thanks to the inclusion $K\mathbb{F}_{q^{c_m}} \subseteq K(E[m])$, and hence to the resulting strong restriction $m | q^x - 1$ in the sum over m.

Remark 7.2 It is natural to ask what the best error terms in the asymptotic (5.7) leading to Theorem 1.1 might be. For $r \geq 4$, our methods give rise to a dominant error term $\mathrm{O}_{\psi,K,d}(q^{(r+2)c_K x/2r})$, which, as $r \to \infty$, is of the same order of magnitude as the one in (7.1) and as the best error term with respect to x in the standard Chebotarev Density Theorem 4.2 applied to one (or finitely many) field(s). When $r = 2$, we obtain $\mathrm{O}_{\psi,K,d}(q^{\frac{5}{6}c_K x})$. Moreover, by making better use of the properties of Drinfeld modules with a non-trivial endomorphism ring, in [CoSh] we succeed in lowering this error term to $\mathrm{O}_{\psi,K,d}(q^{\frac{3}{4}x})$ if $\psi \in \operatorname{Drin}_A(k)$ has rank 2 and is such that $\operatorname{End}_{\overline{k}}(\psi)$ is a maximal A-order in a field extension of k of degree 2 (and provided q is odd). It remains to investigate the true order of magnitude of the error term for such small r.

https://doi.org/10.4153/CJM-2015-006-9 Published online by Cambridge University Press

Remark 7.3 It is also natural to investigate the positivity of the densities $\delta_{\psi,K}(d)$ in Theorem 1.1. The methods required for such a study are of a completely different nature than the ones used in this paper and, as such, this study is to be addressed separately. Nevertheless, we can already exhibit Drinfeld modules for which some of these densities are positive. For example, as a consequence of [CoPa, Theorem 5(b)], if q is odd, then any rank 2 Drinfeld module $\psi \in \mathrm{Drin}_A(k)$ with $\mathrm{End}_{\overline{k}}(\psi)$ isomorphic to the maximal order of an imaginary quadratic extension of k satisfies $\delta_{\psi,k}(1) \geq \frac{1}{2}$.

Acknowledgments Some of the work on this paper was done while A. C. Cojocaru was a member at the Institute for Advanced Study in Princeton, USA and a guest researcher at the Max Planck Institute for Mathematics in Bonn and the University of Göttingen, Germany. She is grateful to both these institutes for excellent work facilities and funding. In particular, she is grateful for research support from the National Science Foundation under agreements No. DMS-0747724 and No. DMS-0635607, and from the European Research Council under Starting Grant 258713.

Both authors are grateful to G. Böckle, F. Breuer, I. Chen, J. Long-Hoelscher, M. Papikian, and D. Thakur for helpful discussions related to the background on Drinfeld modules. They are also grateful to the anonymous referees for comments and suggestions.

References

[Br] F. Breuer, *Torsion bounds for elliptic curves and Drinfeld modules.* J. Number Theory **130**(2010), no. 5, 1241–1250. http://dx.doi.org/10.1016/j.jnt.2009.11.009

[Co1] A. C. Cojocaru, *On the cyclicity of the group of $\mathbb{F}_p$-rational points of non-CM elliptic curves.* J. Number Theory **96**(2002), no. 2, 335–350.

[Co2] ———, *Cyclicity of CM elliptic curves modulo p.* Trans. Amer. Math. Soc. **355**(2003), no. 7, 2651–2662. http://dx.doi.org/10.1090/S0002-9947-03-03283-5

[Co3] ———, *Questions about the reductions modulo primes of an elliptic curve.* In: Number theory, CRM Proc. Lecture Notes, 36, American Mathematical Society, Providence, RI, 2004, pp. 61–79.

[CoMu] A. C. Cojocaru and M. R. Murty, *Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem.* Math. Ann. **330**(2004), no. 3, 601–625. http://dx.doi.org/10.1007/s00208-004-0562-x

[CoPa] A. C. Cojocaru and M. Papikian, *Drinfeld modules, Frobenius endomorphisms, and CM liftings.* Int. Math. Res. Notices (2014). http://dx.doi.org/10.1093/imrn/rnu178

[CoSh] A. C. Cojocaru and A. M. Shulman, *An average Chebotarev density theorem for generic rank 2 Drinfeld modules with complex multiplication.* J. Number Theory **133**(2013), no. 3, 897–914. http://dx.doi.org/10.1016/j.jnt.2012.07.001

[CoTo] A. C. Cojocaru and Á. Tóth, *The distribution and growth of the elementary divisors of the reductions of an elliptic curve over a function field.* J. Number Theory **132**(2012), no. 5, 953–965. http://dx.doi.org/10.1016/j.jnt.2011.08.007

[Du] W. Duke, *Almost all reductions modulo p of an elliptic curve have large exponent.* C. R. Acad. Sci. Paris **337**(2003), no. 11, 689–692. http://dx.doi.org/10.1016/j.crma.2003.10.006

[FrKu] T. Freiberg and P. Kurlberg, *On the average exponent of elliptic curves modulo p.* Int. Math. Res. Not. IMRN **2014**, no. 8, 2265–2293.

[Ga] F. Gardeyn, *Une borne pour l'action de l'inertie sauvage sur la torsion d'un module de Drinfeld.* Arch. Math. **79**(2002), no. 4, 241–251. http://dx.doi.org/10.1007/s00013-002-8310-5

[Ge] E.-U. Gekeler, *On finite Drinfel'd modules.* J. Algebra **141**(1991), no. 1, 187–203. http://dx.doi.org/10.1016/0021-8693(91)90211-P

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

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

[He] G.-J. van der Heiden, *Weil pairing for Drinfeld modules.* Monatsh. Math. **143**(2004), no. 2, 115–143. http://dx.doi.org/10.1007/s00605-004-0261-4

[Ki] Sungjin Kim, *Average behaviors of invariant factors in Mordell–Weil groups of CM elliptic curves modulo p.* Finite Fields Appl. **30**(2014), 178–190. http://dx.doi.org/10.1016/j.ffa.2014.07.003

[KuLi] W. Kuo and Y.-R. Liu, *Cyclicity of finite Drinfeld modules.* J. Lond. Math. Soc. (2) **80**(2009), no. 3, 567–584. http://dx.doi.org/10.1112/jlms/jdp043

[La] S. Lang, *Algebra.* Third ed., Graduate Texts in Mathematics, 211, Spring-Verlag, New York, 2002.

[Mu] M. R. Murty, *On Artin's conjecture.* J. Number Theory **16**(1983), no. 2, 147–168. http://dx.doi.org/10.1016/0022-314X(83)90039-2

[MuSc] V. K. Murty and J. Scherk, *Effective versions of the Chebotarev density theorem for function fields* . C. R. Acad. Sci. Paris Sér. I **319**(1994), no. 6, 523–528.

[Pi] R. Pink, *The Mumford-Tate conjecture for Drinfeld modules.* Publ. Res. Inst. Math. Sci. **33**(1997), no. 3, 393–425. http://dx.doi.org/10.2977/prims/1195145322

[PiRu] R. Pink and E. Rütsche, *Adelic openness for Drinfeld modules in generic characteristic.* J. Number Theory **129**(2009), no. 4, 882–907. http://dx.doi.org/10.1016/j.jnt.2008.12.002

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

[Sc] R. Schoof, *The exponents of the groups of points on the reductions of an elliptic curve.* In: Arithmetic algebraic geometry (Texel, 1989), Prog. Math., 89, Birkhäuser Boston, Boston, MA, 1991, pp. 325–335.

[Se] J-P. Serre, *Summaries of courses of the 1977-78 academic year.* (French), Collège de France, Paris, 1978, pp. 67–71.

[Tag1] Y. Taguchi, *The Tate conjecture for t-motives.* Proc. Amer. Math. Soc. **123**(1995), no. 11, 3285–3287.

[Tag2] ———, *On Φ-modules.* J. Number Theory **60**(1996), no. 1, 124–411. http://dx.doi.org/10.1006/jnth.1996.0117

[Tak] ———, *Good reduction of elliptic modules.* J. Math. Soc. Japan **34**(1982), no. 3, 475–487. http://dx.doi.org/10.2969/jmsj/03430475

[Th] D. Thakur, *Function field arithmetic.* World Scientific Publishing Co. Inc., River Edge, NJ, 2004.

[Wu] J. Wu, *The average exponent of elliptic curves modulo p.* J. Number Theory **135**(2014), 28–35. http://dx.doi.org/10.1016/j.jnt.2013.08.009

(Cojocaru, Shulman) *Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, Chicago, 60607, IL, USA*
e-mail: cojocaru@math.uic.edu ashulm2@uic.edu

(Cojocaru) *Institute of Mathematics "Simion Stoilow" of the Romanian Academy, Bucharest, 010702, Sector 1, Romania*