Volume 133, Issue 3, March 2013 ISSN 0022-314X

ELSEVIER

JOURNAL OF
NUMBER
THEORY

Special Issue: In Honor of David Hayes

Editors:
Michael Rosen, Matthew Papanikolas, Dinesh Thakur

Journal of Number Theory 133 (2013) 897–914

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

An average Chebotarev Density Theorem for generic rank 2 Drinfeld modules with complex multiplication [☆]

Alina Carmen Cojocaru [a,b,*], Andrew Michael Shulman [a]

[a] Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S. Morgan St., 322 SEO, Chicago, 60607 IL, USA
[b] Institute of Mathematics "Simion Stoilow" of the Romanian Academy, 21 Calea Grivitei St., Bucharest, 010702, Sector 1, Romania

ARTICLE INFO

Article history:
Received 26 September 2011
Revised 25 July 2012
Accepted 25 July 2012
Available online 13 August 2012
Communicated by David Goss

Keywords:
Drinfeld module
Weil number
Density theorem
Prime distribution

ABSTRACT

Let q be an odd prime power and let $A = \mathbb{F}_q[T]$, $k = \mathbb{F}_q(T)$. Let ψ be a Drinfeld A-module over k, of rank 2 and with a non-trivial endomorphism ring. We prove an average effective Chebotarev Density Theorem for the primes splitting completely in the division fields $k(\psi[d])$ of ψ, with a very small error term. We also apply our techniques to study the primes of good reduction for ψ for which the reduced A-module is cyclic.

Published by Elsevier Inc.

Contents

[☆] 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. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

[*] Corresponding author at: Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S. Morgan St., 322 SEO, Chicago, 60607 IL, USA.

E-mail addresses: cojocaru@math.uic.edu (A.C. Cojocaru), ashulm2@uic.edu (A.M. Shulman).

0022-314X/$ – see front matter Published by Elsevier Inc.
http://dx.doi.org/10.1016/j.jnt.2012.07.001

1. Introduction and statement of results

It is a classical result, proven by Dirichlet, that, given any coprime integers a, d, there exist infinitely many primes $p \equiv a \pmod d$. The most precise version of this result, due to de la Vallée Poussin, assumes the Generalized Riemann Hypothesis (GRH) for Dirichlet L-functions and states that the function

$$\pi(x; d, a) := \#\{p \leqslant x:\ p \text{ prime},\ p \equiv a \ (\text{mod}\ d)\}$$

satisfies

$$\pi(x; d, a) = \frac{1}{\phi(d)} \operatorname{li} x + \mathrm{O}\big(x^{\frac{1}{2}} \log(dx)\big), \tag{1}$$

where $\phi(d)$ is the Euler function of d and $\operatorname{li} x$ is the logarithmic integral. The O-constant is absolute and the GRH assumption is reflected in the exponent of x in the O-term; in fact, GRH is *equivalent* to this exponent being $\frac{1}{2}$. Moreover, in order for (1) to be meaningful, d should be such that the main term dominates the remainder; for instance, $d \leqslant x^{\frac{1}{2}-\varepsilon}$ for any $\varepsilon > 0$.

The importance of (1) cannot be overstated. Indeed, the study of many of the major conjectures in classical number theory reduces to fine questions about the distribution of primes in arithmetic progressions, for *infinitely many* progressions. The size of the error term in statements such as (1) is then essential. Without GRH, the analogue of (1), known as the Siegel–Walfisz Theorem, states that, for any $A > 0$, there exists a positive constant $c(A)$ such that

$$\pi(x; d, a) = \frac{1}{\phi(d)} \operatorname{li} x + \mathrm{O}\big(x \exp\big(-c(A)\sqrt{\log x}\big)\big). \tag{2}$$

Here, the modulus d should satisfy $d \leqslant (\log x)^A$. This very restricted range of d makes (2) quite unsatisfactory, despite the result being unconditional.

In many cases, to compensate for the lack of a good unconditional error term, one can appeal to *average results*, such as the now standard Bombieri–Vinogradov Theorem: for any $A > 0$, there exists $B > 0$ such that

$$\sum_{d \leqslant \frac{x^{\frac{1}{2}}}{(\log x)^B}} \max_{y \leqslant x} \max_{\substack{a \\ (a,d)=1}} \left| \pi(y; d, a) - \frac{1}{\phi(d)} \operatorname{li} y \right| \ll_A \frac{x}{(\log x)^A}. \tag{3}$$

We may interpret (3) as saying that (1) holds on average, without any unproven hypothesis.

While this is a very powerful result, let us note that the possible range of the modulus d is $(1, x)$, and (3) handles only $(1, x^{\frac{1}{2}}/(\log x)^B)$. Enlarging this range is a major open problem in analytic number theory, as illustrated by the notoriously difficult Elliott–Halberstam Conjecture: for any $A, \varepsilon > 0$, we expect that

$$\sum_{d \leqslant x^{1-\varepsilon}} \max_{y \leqslant x} \max_{\substack{a \\ (a,d)=1}} \left| \pi(y; d, a) - \frac{1}{\phi(d)} \operatorname{li} y \right| \ll_{A,\varepsilon} \frac{x}{(\log x)^A}. \tag{4}$$

Dirichlet's Theorem and its refined formulations (1), (2) are only basic instances of the more general Chebotarev Density Theorem applied to the cyclotomic field $\mathbb{Q}(\zeta_d)$. Versions of (1) and (2) in the general Chebotarev situation of Galois extensions of number fields were proven by Lagarias and Odlyzko [LaOd] and assume, as in the classical case, *strong restrictions* in terms of x on the size of the arithmetic invariants of the number fields considered, even under the assumption of GRH (for

Dedekind zeta functions). At the same time, no general version of (3) for an arbitrary families of Galois extensions of number fields is yet known.

In spite of these deficits, for some special families of number fields, closely related to cyclotomic fields, some average versions of the Chebotarev Density Theorem can be proven. For example, by considering an elliptic curve E defined over $\mathbb{Q}$, with a non-trivial endomorphism ring, and by focusing on its division fields $\mathbb{Q}(E[d])$, the results of M.R. Murty [Mu, Theorem 3] may be restated as saying that the function

$$\pi_1\big(x, \mathbb{Q}\big(E[d]\big)/\mathbb{Q}\big) := \#\big\{p \leqslant x:\ p \text{ prime},\ p \text{ splits completely in } \mathbb{Q}\big(E[d]\big)\big\}$$

satisfies

$$\sum_{\substack{d\geqslant 1\\ d \text{ squarefree}}} \pi_1\big(x, \mathbb{Q}\big(E[d]\big)/\mathbb{Q}\big) \sim \Bigg(\sum_{\substack{d\geqslant 1\\ d \text{ squarefree}}} \frac{1}{[\mathbb{Q}(E[d]):\mathbb{Q}]}\Bigg) \operatorname{li} x \tag{5}$$

as $x \to \infty$. By assuming GRH for Dedekind zeta functions, this result can be much improved; indeed, the results of this paper's first author and M.R. Murty [CoMu, Theorem 1.2] may be restated as

$$\sum_{\substack{d\geqslant 1\\ d \text{ squarefree}}} \bigg(\pi_1\big(x, \mathbb{Q}\big(E[d]\big)/\mathbb{Q}\big) - \frac{1}{[\mathbb{Q}(E[d]):\mathbb{Q}]} \operatorname{li} x\bigg) \ll_E x^{\frac{3}{4}} (\log x)^{\frac{1}{2}}. \tag{6}$$

Note that in both (5) and (6) the range of d is the *maximal* allowable as a function of x. This turns out to be $d \leqslant x^{\frac{1}{2}} + 1$, which is much shorter than in the classical situation, and thus easier to handle.

Over the years, it has been a fruitful theme of research to explore parallels and differences between the number field and function field situations. The study of this theme in the case of primes in arithmetic progressions is already abundant in both analogies and non-analogies. Our goal in this paper is to continue this study and *explore function field analogues of* (5) *and* (6) *in the context of Drinfeld modules*. For this purpose, let us introduce some notation and a brief context.

We let q be an odd prime power, fixed throughout the paper. We denote by $\mathbb{F}_q$ the finite field with q elements, by $\mathbb{F}_q^*$ its group of units, by $\bar{\mathbb{F}}_q$ an algebraic closure of $\mathbb{F}_q$, and by $\tau : x \mapsto x^q$ the q-th power Frobenius automorphism. We denote by $A := \mathbb{F}_q[T]$ the polynomial ring over $\mathbb{F}_q$, by $A^{(1)}$ the set of monic polynomials in A, by $k := \mathbb{F}_q(T)$ its field of fractions, by $\bar{k}$ an algebraic closure of k, and by k^{sep} a separable closure of k in $\bar{k}$.

We recall that $\frac{1}{T}$ identifies with the "prime at infinity" of k, while the monic irreducible polynomials of A identify with the "finite primes" of k. We will simply refer to the latter as the **primes of** k. We recall that a finite field extension k' of k is called **imaginary** if there is only one prime in k' lying above the infinite prime in k.

We shall denote the elements of A (mostly) by d, the elements of $A^{(1)}$ (mostly) by m, the irreducible elements of $A^{(1)}$ by p and ℓ, and the (finite) primes of k by $\mathfrak{p} = pA$, $\mathfrak{l} = \ell A$, with $p, \ell \in A^{(1)}$. For $d \in A$, we use the standard notation:

- $\deg d$ for the degree of d as a polynomial in T;
- $|d|_\infty := q^{\deg d}$ if $d \neq 0$, and $|0|_\infty := 0$.

As with rational primes in arithmetic progression, given any coprime $a, d \in A$ with d non-constant, there exist infinitely many primes $p \in A^{(1)}$ with $p \equiv a \pmod d$. Moreover, the function

$$\pi_A(x; d, a) := \#\big\{p \in A^{(1)}:\ \deg p = x,\ p \equiv a \ (\mathrm{mod}\ d)\big\}$$

satisfies

$$\pi_A(x; d, a) = \frac{1}{\phi_A(d)} \cdot \frac{q^x}{x} + \mathrm{O}\left(\frac{q^{\frac{x}{2}}}{x} \deg d\right), \tag{7}$$

where $\phi_A(d) := \#(A/dA)^*$ is the Euler function of d, $\frac{q^x}{x}$ is the growth of the prime counting function $\pi_A(x) := \#\{p \in A^{(1)}\colon \deg p = x\}$, and the O-constant is absolute. As in the classical case (1), this asymptotic is meaningful provided $|d|_\infty < q^{\frac{x}{2}-\varepsilon}$ for any $\varepsilon > 0$. However, unlike the classical case, this holds *unconditionally*, thanks to Weil's proof of the Riemann Hypothesis for curves over finite fields (reflected in the exponent $\frac{x}{2}$ of q in the error term).

Once again, (7) is only a particular case of the more general Chebotarev Density Theorem for Galois extensions of global function fields. As with rational primes, it is natural to consider this theorem not only for one extension (e.g. one d), but for infinitely many extensions (e.g. infinitely many d), and also to enlarge the range of d to the maximum allowable. We will prove such a statement by focusing on a special family of function fields, as follows.

We denote by $\mathrm{Drin}_A(k)$ the category of Drinfeld A-modules over k (necessarily of generic A-characteristic). For $\psi : A \longrightarrow k\{\tau\}$ an object in $\mathrm{Drin}_A(k)$, we denote by

$$\mathrm{End}_{\bar{k}}(\psi) := \left\{f \in \bar{k}\{\tau\}\colon f\psi_d = \psi_d f \ \forall d \in A\right\}$$

the endomorphism ring of ψ over $\bar{k}$, and for each non-zero $d \in A$, we denote by $k(\psi[d])$ the **d-division field** obtained by adjoining to k the **d-division module of** ψ, that is,

$$\psi[d] := \left\{\lambda \in \bar{k}\colon \psi_d(\lambda) = 0\right\}.$$

We denote by

$$c_d := \left[k\big(\psi[d]\big) \cap \bar{\mathbb{F}}_q : \mathbb{F}_q\right]$$

the degree of the constant field of $k(\psi[d])$ over $\mathbb{F}_q$, and we define, for any arbitrary positive integer x,

$$c_d(x) := \begin{cases} c_d & \text{if } c_d | x, \\ 0 & \text{otherwise.} \end{cases} \tag{8}$$

Our main result is:

Theorem 1. *Let q be an odd prime power and, as above, let $A := \mathbb{F}_q[T]$, $k := \mathbb{F}_q(T)$. Let $\psi \in \mathrm{Drin}_A(k)$ be of rank 2. We assume that $\mathrm{End}_{\bar{k}}(\psi)$ is the full ring of integers of an imaginary quadratic extension of k. Then, as $x \to \infty$,*

$$\sum_{m \in A^{(1)}} \left(\#\left\{p \in A^{(1)}\colon \deg p = x,\ pA \text{ splits completely in } k\big(\psi[m]\big)/k\right\} - \frac{c_m(x)}{[k(\psi[m]) : k]}\pi_A(x)\right)$$
$$\ll_\psi q^{\frac{3}{4}x} \log x.$$

Note that this is an analogue of (6), which is obtained unconditionally. A similar, but weaker, result was obtained in [CoSh] in the setting of Theorem 1, without fully using the assumption on the endomorphism ring of ψ; specifically, the authors proved that, as $x \to \infty$,

$$\sum_{m\in A^{(1)}}\left(\#\bigl\{p\in A^{(1)}\colon \deg p = x,\ pA \text{ splits completely in } k\bigl(\psi[m]\bigr)/k\bigr\} - \frac{c_m(x)}{[k(\psi[m]):k]}\pi_A(x)\right)$$
$$\ll_\psi q^{\frac{5}{6}x}.$$

On the other hand, the strength of the results of [CoSh] is that they apply to Drinfeld modules in higher generality (higher rank and more general function fields).

As an application to the (proof of) Theorem 1, we obtain that

$$\#\bigl\{p\in A^{(1)}\colon \deg p = x,\ \psi(\mathbb{F}_\mathfrak{p}) \text{ is } A\text{-cyclic}\bigr\} = \left(\sum_{m\in A^{(1)}}\frac{\mu_A(m)c_m(x)}{[k(\psi[m]):k]}\right)\cdot\frac{q^x}{x} + \mathrm{O}_\psi\bigl(q^{\frac{3x}{4}}\log x\bigr), \tag{9}$$

where $\mathbb{F}_\mathfrak{p}$ is the residue field of $\mathfrak{p} = pA$, $\psi(\mathbb{F}_\mathfrak{p})$ is the A-module structure on $\mathbb{F}_\mathfrak{p}$ defined by the reduction of ψ modulo $\mathfrak{p}$, and $\mu_A(\cdot)$ is the Möbius function of A.

To prove these results, we do use an effective version of the Chebotarev Density Theorem. The application of Chebotarev requires, in particular, estimates for the size of the Galois groups of the division fields of ψ, for which, in our present situation, we rely on results of Hayes from his celebrated paper [Ha].

As usual in such problems, we must find adhoc ways to extend the range of applicability of Chebotarev, which is where the main contributions to the proof methods lie. For Theorem 1, we make use of both the average over m and of the *rank* 2 and *CM* assumptions on the Drinfeld module. These assumptions lead to a very convenient reinterpretation of the splitting completely property: an *ordinary* prime p splits completely in $k(\psi[m])$ if and only if the Weil root $\pi = \pi_{\psi,pA}$ of the reduction of ψ at p has the property that $\frac{\pi-1}{m}$ is an algebraic integer in $\mathrm{End}_{\bar{k}}(\psi)\otimes_A k$. We then use elementary sieving to average such primes over m. Since there are no *supersingular* primes p which split completely in $k(\psi[m])$ for m of sufficiently large degree and since the primes of good reduction of a *rank* 2 (generic) Drinfeld module ψ are either ordinary or supersingular, there is nothing left to estimate.

It is natural to consider the analogue of Theorem 1 (that is, an improvement of the error terms in some of the results of [CoSh]) for Drinfeld modules of higher rank, a task which we relegate to a future study. Since the size of the error terms in such density estimates is intimately connected to the zeroes of the L-functions involved, it is also natural to investigate the meaning of our small error term $\mathrm{O}_\psi(q^{\frac{3}{4}x}\log x)$ in terms of the zeroes of the Artin L-functions associated to the family $(k(\psi[m]))_{m\in A^{(1)}}$; this, again, we relegate to a future study.

2. Preliminaries

Throughout the paper, we shall use the notation introduced in Section 1 and the auxiliary standard notation and results below. We reserve the notation ψ for Drinfeld A-modules over k (not necessarily of rank 2), and Ψ for Drinfeld modules over more general rings $\mathscr{A}$ and $\mathscr{A}$-fields $\mathscr{L}$. As for k, the letters $\mathfrak{p}$ and $\mathfrak{l}$ will denote finite primes of $\mathscr{L}$.

For a more comprehensive treatment of some of the material in Section 2, we refer the reader to [Go,Ro] and [Th].

2.1. *Division fields*

We record below the properties of the division fields of a Drinfeld module that will be used in the proof of Theorem 1. Since these properties span a vast part of the theory of Drinfeld modules, our presentation may seem slightly intricate.

2.1.1. *Ramification*

Let $\mathscr{K}$ be an arbitrary function field, ∞ a fixed prime of $\mathscr{K}$, $\mathscr{A}$ the ring of functions on $\mathscr{K}$ regular away from ∞, and $\mathscr{L}$ an $\mathscr{A}$-field of generic $\mathscr{A}$-characteristic.

Let Ψ be a Drinfeld $\mathscr{A}$-module over $\mathscr{L}$, of rank r. Let $\mathfrak{p}$ be a prime of $\mathscr{L}$, of good reduction for Ψ, and let

$$\Psi \otimes \mathbb{F}_{\mathfrak{p}} : \mathscr{A} \longrightarrow \mathbb{F}_{\mathfrak{p}}\{\tau\}$$

be the reduction of Ψ modulo $\mathfrak{p}$, where $\mathbb{F}_{\mathfrak{p}}$ is the residue field of $\mathfrak{p}$. We denote by

$$\Psi(\mathbb{F}_{\mathfrak{p}})$$

the $\mathscr{A}$-module structure on $\mathbb{F}_{\mathfrak{p}}$ defined by $\Psi \otimes \mathbb{F}_{\mathfrak{p}}$.

By classical theory, all but finitely many primes of $\mathscr{L}$ are of good reduction for Ψ. We denote their set by

$$\mathcal{P}_{\Psi}.$$

For the purpose of our paper, these primes are relevant in the following way:

Proposition 2 *(Ramification criterion). (See [Ta, Theorem 1, p. 477].) Let $\mathscr{K}$ be an arbitrary function field, ∞ a fixed prime of $\mathscr{K}$, $\mathscr{A}$ the ring of functions on $\mathscr{K}$ regular away from ∞, and $\mathscr{L}$ an $\mathscr{A}$-field of generic $\mathscr{A}$-characteristic. Let Ψ be a Drinfeld $\mathscr{A}$-module over $\mathscr{L}$. Let $\mathfrak{p} \neq \mathfrak{l}$ be primes of $\mathscr{L}$. Then Ψ has good reduction at $\mathfrak{p}$ if and only if the Galois module $\Psi[\mathfrak{l}^{\infty}] := \bigcup_{n \geqslant 1} \Psi[\mathfrak{l}^n]$ is unramified at $\mathfrak{p}$. If Ψ has rank 1, then $\Psi[\mathfrak{l}^{\infty}]$ is totally ramified at $\mathfrak{l}$.*

Note that the last assertion is not stated explicitly in the theorem cited, but can be derived from its proof.

2.1.2. Algebraic properties

In this subsection, we restrict our attention to Drinfeld A-modules ψ over k. Moreover, for the result on the degree of the division fields (Proposition 5), we shall make an additional assumption on the endomorphism ring of ψ.

Proposition 3 *(Size of constant field). (See [Go, Remark 7.1.9, p. 196].) Let $\psi \in \mathrm{Drin}_A(k)$, and let*

$$k_{\psi,\mathrm{tors}} := \bigcup_{d \in A \setminus \{0\}} k\bigl(\psi[d]\bigr).$$

Then

$$[k_{\psi,\mathrm{tors}} \cap \overline{\mathbb{F}}_q : \mathbb{F}_q] < \infty.$$

In particular, there exists a positive constant $C(\psi)$, depending on ψ, such that, for any $d \in A \setminus \mathbb{F}_q$,

$$c_d \leqslant C(\psi),$$

where, we recall, $c_d := [k(\psi[d]) \cap \overline{\mathbb{F}}_q : \mathbb{F}_q]$.

Proposition 4 *(Growth of genus). (See [Ga, Corollary 7, p. 248].) Let $\psi \in \mathrm{Drin}_A(k)$. Then there exists a positive constant $G(\psi)$, depending on ψ, such that, for any $d \in A \setminus \mathbb{F}_q$, the genus g_d of $k(\psi[d])$ satisfies*

$$g_d \leqslant G(\psi) \cdot \bigl[k\bigl(\psi[d]\bigr) : k\bigr] \cdot \deg d.$$

Proposition 5 *(Size of degree). Let $\psi \in \mathrm{Drin}_A(k)$ of rank $r \geqslant 2$. Assume that $\mathrm{End}_{\bar{k}}(\psi)$ is the maximal A-order in an imaginary Galois extension k' of k satisfying $[k' : k] = r$. Then, for any non-zero $d \in A$,*

$$\bigl[k\bigl(\psi[d]\bigr) : k\bigr] \gg_{k'} \frac{q^{r \deg d}}{\log(r \deg d) + \log\log q}.$$

Proof. This is, essentially, a consequence of the important work of David Hayes, more precisely of [Ha, Theorem 9.2, p. 206], as we explain below.

First, we recall:

Proposition 6. *Let $\psi \in \mathrm{Drin}_A(k)$ of rank $r \geqslant 2$. Assume that $\mathscr{A} := \mathrm{End}_{\bar{k}}(\psi)$ is the maximal A-order in an imaginary Galois extension k' of k satisfying $[k' : k] = r$. Then there exists a Drinfeld $\mathscr{A}$-module ψ' over $\bar{k}$, of generic $\mathscr{A}$-characteristic, such that*:

(i) *ψ' has rank 1;*
(ii) *$\psi'_d = \psi_d$ for all non-zero $d \in A$.*

Part (ii) is [Ha, Prop. 3.2, p. 182] and part (i) is derived by comparing the size of the division modules $\psi'[d]$, $\psi[d]$, equality coming from part (ii). We include more details below.

Proof of Proposition 6. Since $A \subseteq \mathscr{A} \subseteq \bar{k}\{\tau\}$, we have the commutative diagram

$$\begin{tikzcd}
A \arrow[r, "\psi"] \arrow[dr, hook] & k\{\tau\} \arrow[r, hook] & \bar{k}\{\tau\} \\
& \mathscr{A} \arrow[ur, hook, "\psi' \text{ (by definition)}"'] &
\end{tikzcd}$$

As shown above, we define ψ' to be the low right-hand map and claim that it is a Drinfeld $\mathscr{A}$-module over $\bar{k}$, of generic characteristic, satisfying (i) and (ii).

To see this, observe first that $\mathscr{A} \subseteq \bar{k}$, hence $\bar{k}$ is naturally a field with generic $\mathscr{A}$-characteristic. We also observe that, by its definition, ψ' is an $\mathbb{F}_q$-algebra for which the differentiation with respect to x map,

$$D : \bar{k}\{\tau\} \longrightarrow \bar{k},\ D\left(\sum_{0 \leqslant i \leqslant n} c_i \tau^i\right) = c_0,$$

satisfies $D(\psi'_d) = d$ for any $d \in A$. Moreover, since $A \subsetneq \mathscr{A}$, ψ' satisfies $\mathrm{Im}\,\psi' \not\subseteq \bar{k}$. Hence, indeed, ψ' is a generic Drinfeld $\mathscr{A}$-module over $\bar{k}$.

From the definition of ψ', property (ii) is immediate. It remains to prove (i), that is, that the rank r' of ψ' is 1. For this, let $d \in A$ be non-zero. By classical theory,

$$\psi'[d] \simeq_{\mathscr{A}} (\mathscr{A}/d\mathscr{A})^{r'} \tag{10}$$

and

$$\psi[d] \simeq_A (A/dA)^r. \tag{11}$$

By our assumption on $\mathscr{A}$, we have

$$\mathscr{A} \simeq_A A^r. \tag{12}$$

Putting together (10)–(12) and using (ii), we deduce that $r' = 1$. This *completes the proof of Proposition* 6. □

Continuing the preparation for the proof of Proposition 5, we next recall:

Proposition 7. *(See [Ha, Theorem 9.2, p. 206].) Let $\mathscr{K}$ be an arbitrary function field, ∞ a fixed prime of $\mathscr{K}$, $\mathscr{A}$ the ring of functions on $\mathscr{K}$ regular away from ∞, and $(\mathscr{L}, \delta)$ an $\mathscr{A}$-field. Denote by $H_{\mathscr{K}}$ the Hilbert class field of $\mathscr{K}$ with respect to $\mathscr{A}$, that is, the maximal abelian extension of $\mathscr{K}$, unramified everywhere and split completely at ∞. The following statements hold*:

(i) *$H_{\mathscr{K}}/\mathscr{K}$ is a finite Galois extension with*

$$\mathrm{Gal}(H_{\mathscr{K}}/\mathscr{K}) \simeq \mathrm{Pic}(\mathscr{A}),$$

the Picard group of $\mathscr{A}$, that is, the group of classes of degree zero divisors of $\mathscr{K}$ supported away from $\mathscr{A}$, modulo principal divisors.

(ii) *Let $\Psi \in \mathrm{Drin}_{\mathscr{A}}(\mathscr{L})$ of rank 1 and of generic $\mathscr{A}$-characteristic. Then, for any non-zero $d \in \mathscr{A}$,*

$$\mathrm{Gal}\big(H_{\mathscr{K}}\big(\Psi[d]\big)/H_{\mathscr{K}}\big) \simeq (\mathscr{A}/d\mathscr{A})^*.$$

We are now ready to prove Proposition 5. For this, let $\psi \in \mathrm{Drin}_A(k)$ be of rank $r \geqslant 2$ and assume that $\mathscr{A} := \mathrm{End}_{\bar{k}}(\psi)$ is the maximal A-order in an imaginary Galois extension k' of k satisfying $[k' : k] = r$. By Proposition 6, there exists a generic Drinfeld $\mathscr{A}$-module ψ' over $\bar{k}$, of rank 1, such that $\psi'_d = \psi_d$ for all non-zero $d \in A$.

Let $d \in A\backslash\{0\}$ be fixed. Then the Hilbert class field $H_{k'}$ of k' satisfies

$$H_{k'} \cap k'\big(\psi'[d]\big) = k'. \tag{13}$$

This follows from the ramification properties of the fields involved: by definition, $H_{k'}$ is unramified everywhere, while, by Proposition 2, $k'(\psi'[d])$ is totally ramified at the primes dividing d.

Using (13) and Proposition 7, we obtain the following field diagram:

$$\begin{tikzcd}
 & H_{k'}(\psi'[d]) \arrow[dl, dash, "\#(\mathscr{A}/d\mathscr{A})^*"'] \arrow[dr, dash, "\#\,\mathrm{Pic}(\mathscr{A})"] & & \\
H_{k'} \arrow[dr, dash, "\#\,\mathrm{Pic}(\mathscr{A})"'] & & k'(\psi'[d]) \arrow[dl, dash, "\#(\mathscr{A}/d\mathscr{A})^*"'] \arrow[dr, dash] & \\
 & k' \arrow[dr, dash] & & k(\psi'[d]) \arrow[dl, dash, "\#(\mathscr{A}/d\mathscr{A})^*"'] \\
 & & k' \cap k(\psi'[d]) \arrow[d, dash] & \\
 & & k &
\end{tikzcd}$$

We immediately deduce that

$$\big[k\big(\psi'[d]\big) : k\big] = \#(\mathscr{A}/d\mathscr{A})^* \cdot \big[k' \cap k\big(\psi'[d]\big) : k\big] \in \big\{n\#(\mathscr{A}/d\mathscr{A})^*\colon\ n \in \mathbb{N}\backslash\{0\}, n|r\big\},$$

and, recalling part (ii) of Proposition 6, that

$$\left[k\bigl(\psi[d]\bigr):k\right]\in\left\{n\#(\mathscr{A}/d\mathscr{A})^{*}\colon n\in\mathbb{N}\backslash\{0\},n|r\right\}. \tag{14}$$

Finally, by invoking [Br, Lemma 2.2, p. 1243] and our assumption on $\mathscr{A}$ (in particular, that we work with a Dedekind domain satisfying (12)), we deduce that

$$\#(\mathscr{A}/d\mathscr{A})^{*}=\#\,\mathrm{GL}_1(\mathscr{A}/d\mathscr{A})\gg_{k'}\frac{q^{r\deg d}}{\log\log q^{r\deg d}}. \tag{15}$$

By putting together (14) and (15), *we complete the proof of Proposition* 5. □

2.1.3. Arithmetic in division fields

In this subsection, let $\psi\in\mathrm{Drin}_A(k)$ be of rank $r\geqslant 1$, and let $\mathcal{P}_\psi$ be the set of primes of good reduction for ψ.

For $\mathfrak{p}\in\mathcal{P}_\psi$, by the torsion theory of $\psi\otimes\mathbb{F}_\mathfrak{p}$, there exist uniquely determined monic polynomials $m_1(\psi,\mathfrak{p}),\dots,m_r(\psi,\mathfrak{p})\in A^{(1)}$ such that

$$m_1(\psi,\mathfrak{p})|\dots|m_r(\psi,\mathfrak{p})$$

and

$$\psi(\mathbb{F}_\mathfrak{p})\simeq_A A/m_1(\psi,\mathfrak{p})A\times\cdots\times A/m_r(\psi,\mathfrak{p})A. \tag{16}$$

We define the **Euler–Poincaré characteristic of** $\psi(\mathbb{F}_\mathfrak{p})$ as the principal ideal

$$\chi\bigl(\psi(\mathbb{F}_\mathfrak{p})\bigr):=m_1(\psi,\mathfrak{p})\dots m_r(\psi,\mathfrak{p})A$$

and note that

$$\bigl|\chi\bigl(\psi(\mathbb{F}_\mathfrak{p})\bigr)\bigr|_\infty=|\mathfrak{p}|_\infty. \tag{17}$$

For $\mathfrak{l}=\ell A$ a prime of k, let

$$T_\mathfrak{l}(\psi):=\mathrm{Hom}_{A_\mathfrak{l}}\bigl(k_\mathfrak{l}/A_\mathfrak{l},\psi\bigl[\ell^\infty\bigr]\bigr),$$
$$V_\mathfrak{l}(\psi):=T_\mathfrak{l}(\psi)\otimes_{A_\mathfrak{l}}k_\mathfrak{l}$$

be the $\mathfrak{l}$-adic Tate module and the $\mathfrak{l}$-adic Tate algebra, respectively, of ψ, where, as usual, $A_\mathfrak{l}$ and $k_\mathfrak{l}$ are the completions of A and k at $\mathfrak{l}$.

By the torsion theory of ψ,

$$T_\mathfrak{l}(\psi)\simeq_{A_\mathfrak{l}}A_\mathfrak{l}^r,$$
$$V_\mathfrak{l}(\psi)\simeq_{k_\mathfrak{l}}k_\mathfrak{l}^r.$$

Moreover, the absolute Galois group $G_k:=\mathrm{Gal}(k^{\mathrm{sep}}/k)$ of k acts continuously on these structures, giving rise to continuous Galois representations

$$\rho_{\psi,\mathfrak{l}}:G_k\longrightarrow\mathrm{Aut}_{A_\mathfrak{l}}\bigl(T_\mathfrak{l}(\psi)\bigr)\simeq\mathrm{GL}_r(A_\mathfrak{l}),$$
$$\rho_{\psi,\mathfrak{l}}\otimes k_\mathfrak{l}:G_k\longrightarrow\mathrm{Aut}_{k_\mathfrak{l}}\bigl(V_\mathfrak{l}(\psi)\bigr)\simeq\mathrm{GL}_r(k_\mathfrak{l}).$$

For the purpose of our paper, these two aspects of the theory of ψ (reductions and Galois representations) are related through the important properties of the **characteristic polynomial of the Frobenius $\sigma_{\mathfrak{p}}$ at** $\mathfrak{p}$,

$$\begin{aligned} P^{\mathfrak{l}}_{\psi,\mathfrak{p}}(X) &:= \det\bigl(X\,\mathrm{Id} - \rho_{\psi,\mathfrak{l}}(\sigma_{\mathfrak{p}})\bigr) \\ &= X^r + a_{r-1}(\psi,\mathfrak{p})X^{r-1} + \cdots + a_1(\psi,\mathfrak{p})X + a_0(\psi,\mathfrak{p}) \in A_{\mathfrak{l}}[X], \end{aligned}$$

as will be discussed below.

We recall the basic properties of this polynomial:

Proposition 8. *(See [Ge, Corollary 3.4, p. 193; Theorem 5.1, p. 199].) Let $\psi \in \mathrm{Drin}_A(k)$ of rank $r \geqslant 1$. Let $\mathfrak{p} = pA \in \mathcal{P}_\psi$ and $\mathfrak{l}$ be primes of k such that $\mathfrak{l} \neq \mathfrak{p}$. Then:*

- (i) *$P^{\mathfrak{l}}_{\psi,\mathfrak{p}}(X) \in A[x]$; in particular, $P^{\mathfrak{l}}_{\psi,\mathfrak{p}}(X)$ is independent of $\mathfrak{l}$, and, as such, we will drop the superscript $\mathfrak{l}$ from notation and simply write $P_{\psi,\mathfrak{p}}(X)$.*
- (ii) *$a_0(\psi,\mathfrak{p}) = u(\psi,\mathfrak{p})p$ for some $u(\psi,\mathfrak{p}) \in \mathbb{F}_q^*$.*
- (iii) *The roots of $P_{\psi,\mathfrak{p}}(X)$ have $|\cdot|_\infty$-norm less than or equal to $|\mathfrak{p}|_\infty^{\frac{1}{r}}$.*
- (iv) *$|a_i(\psi,\mathfrak{p})|_\infty \leqslant |\mathfrak{p}|_\infty^{\frac{r-i}{r}}$ for all $0 \leqslant i \leqslant r-1$.*
- (v) *$P_{\psi,\mathfrak{p}}(1)A = \chi(\psi(\mathbb{F}_{\mathfrak{p}}))$.*

Next we focus on characterizing the primes splitting completely in a division field of ψ. We start with:

Proposition 9. *Let $\psi \in \mathrm{Drin}_A(k)$ of rank $r \geqslant 1$. Let $\mathfrak{p} = pA \in \mathcal{P}_\psi$ and let $d \in A\backslash\{0\}$ be coprime to p. If $\mathfrak{p}$ splits completely in $k(\psi[d])$, then $d^r | P_{\psi,\mathfrak{p}}(1)$.*

Proof. Let $\mathfrak{p}$ be as in the statement of the proposition. Since it splits completely in $k(\psi[d])$, $\sigma_{\mathfrak{p}}$ acts trivially on $\psi[d]$, and so $(\psi \otimes \mathbb{F}_{\mathfrak{p}})[d] \leqslant_A \mathrm{Ker}(\pi_{\mathfrak{p}} - 1)$, where $\pi_{\mathfrak{p}}$ is the $|\mathfrak{p}|_\infty$-power Frobenius of $\mathbb{F}_{\mathfrak{p}}$. By invoking the structure of the torsion of $\psi \otimes \mathbb{F}_{\mathfrak{p}}$, we deduce that $\psi(\mathbb{F}_{\mathfrak{p}})$ contains an isomorphic copy of $(A/dA)^r$. By taking the Euler–Poincaré characteristic and by invoking part (v) of Proposition 8, we then deduce the desired divisibility relation. □

We devote the rest of this subsection to proving one of the key ingredients of the proof of Theorem 1:

Proposition 10 *(Properties of primes splitting completely in division fields). Let $\psi \in \mathrm{Drin}_A(k)$ of rank $r \geqslant 2$. There exists $\psi^1 \in \mathrm{Drin}_A(k)$, of rank 1, uniquely determined up to $\bar{k}$-isomorphism, such that:*

- (i) *$\mathcal{P}_\psi \subseteq \mathcal{P}_{\psi^1}$;*
- (ii) *for any $\mathfrak{p} \in \mathcal{P}_\psi$, the characteristic polynomials of ψ and ψ^1 at $\mathfrak{p}$ satisfy the relation:*

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

$$P_{\psi^1,\mathfrak{p}}(X) = X + (-1)^{r-1}u(\psi,\mathfrak{p})p,$$

  where, we recall, $u(\psi,\mathfrak{p}) \in \mathbb{F}_q^*$;
- (iii) *for any $\mathfrak{p} = pA \in \mathcal{P}_\psi$ and any non-zero $d \in A$ coprime to p we have that, if $\mathfrak{p}$ splits completely in $k(\psi[d])$, then*
  - (iii1) *$\mathfrak{p}$ also splits completely in $k(\psi^1[d])$;*
  - (iii2) *$d^r | P_{\psi,\mathfrak{p}}(1)$;*
  - (iii3) *$d | P_{\psi^1,\mathfrak{p}}(1)$.*

Proof. Let $\psi \in \mathrm{Drin}_A(k)$ be defined by

$$\psi_T = T\tau^0 + c_1(\psi)\tau + \cdots + c_{r-1}(\psi)\tau^{r-1} + \Delta(\psi)\tau^r \in k\{\tau\}, \tag{18}$$

where $\Delta(\psi) \neq 0$.

Let $\psi^1 \in \mathrm{Drin}_A(k)$ be defined by

$$\psi_T^1 = T\tau^0 + (-1)^{r-1}\Delta(\psi)\tau. \tag{19}$$

Using [He, Theorems 3.1 and 6.3], we obtain that, for any prime $\mathfrak{l}$ of k, the Tate algebras of ψ and ψ^1 satisfy the G_k-isomorphism

$$V_{\mathfrak{l}}(\psi^1) \simeq_{G_k} \Lambda^r V_{\mathfrak{l}}(\psi). \tag{20}$$

Thus, if the representation $\rho_{\psi,\mathfrak{l}} \otimes k_{\mathfrak{l}}$ is unramified at some prime $\mathfrak{p}$, so is the representation $\rho_{\psi^1,\mathfrak{l}} \otimes k_{\mathfrak{l}}$. Using Proposition 2, we then deduce part (i) of the theorem.

Part (ii) is an immediate consequence of [HsYu, Theorem 3.2] and the relation between ψ and ψ^1 exhibited in (18)–(19).

To prove part (iii), let $\mathfrak{p} = pA \in \mathcal{P}_\psi$ and $d \in A$ coprime to p be such that $\mathfrak{p}$ splits completely in $k(\psi[d])$. Then the residual representation

$$\bar{\rho}_{\psi,d} : \mathrm{Gal}\big(k\big(\psi[d]\big)/k\big) \hookrightarrow \mathrm{GL}_r(A/dA)$$

satisfies

$$\bar{\rho}_{\psi,d}(\sigma_{\mathfrak{p}}) = \mathrm{Id},$$

and so

$$P_{\psi,\mathfrak{p}}(X) \equiv (X-1)^r \pmod{dA}.$$

Using part (ii), we deduce that

$$P_{\psi^1,\mathfrak{p}}(X) \equiv X - 1 \pmod{dA};$$

recalling that ψ^1 has rank 1, we deduce further that the residual representation

$$\bar{\rho}_{\psi^1,d} : \mathrm{Gal}\big(k\big(\psi^1[d]\big)/k\big) \hookrightarrow \mathrm{GL}_1(A/dA)$$

satisfies

$$\bar{\rho}_{\psi^1,d}(\sigma_{\mathfrak{p}}) = \mathrm{Id}.$$

In other words, $\mathfrak{p}$ splits completely in $k(\psi^1[d])$, proving (iii1). Parts (iii2) and (iii3) are then immediate applications of Proposition 9. □

By specializing to the case of a rank 2 Drinfeld module, we obtain:

Corollary 11. *Let $\psi \in \mathrm{Drin}_A(k)$ of rank 2. Let $\mathfrak{p} = pA \in \mathcal{P}_\psi$ and $d \in A$ non-zero, coprime to p. If $\mathfrak{p}$ splits completely in $k(\psi[d])$, then either of the roots $\pi_{\psi,\mathfrak{p}} \in \bar{k}$ of $P_{\psi,\mathfrak{p}}$ has the property that*

$$\frac{\pi_{\psi,\mathfrak{p}} - 1}{d} \quad \textit{is an algebraic integer.}$$

Proof. Let $\overline{\pi}_{\psi,\mathfrak{p}} \in \bar{k}$ be the Galois conjugate of $\pi_{\psi,\mathfrak{p}}$. We consider the polynomial

$$\left(X - \frac{\pi_{\psi,\mathfrak{p}} - 1}{d}\right)\left(X - \frac{\overline{\pi}_{\psi,\mathfrak{p}} - 1}{d}\right) = X^2 + \frac{a_1(\psi,\mathfrak{p}) + 2}{d} X + \frac{P_{\psi,\mathfrak{p}}(1)}{d^2} \in k[X]$$

and show that it has coefficients in A.

Since $\mathfrak{p}$ splits completely in $k(\psi[d])$, parts (ii)–(iii) of Proposition 10 give $d^2 | P_{\psi,\mathfrak{p}}(1) = 1 + a_1(\psi,\mathfrak{p}) + u(\psi,\mathfrak{p})p$ and $d | P_{\psi^1,\mathfrak{p}}(1) = 1 - u(\psi,\mathfrak{p})p$, and so also $d | a_1(\psi,\mathfrak{p}) + 2$. This completes the proof. □

2.2. *Reduction types*

Let $\psi \in \mathrm{Drin}_A(k)$ of rank 2. We recall that a prime $\mathfrak{p} \in \mathcal{P}_\psi$ is called **supersingular** if $\mathrm{End}_{\overline{\mathbb{F}}_\mathfrak{p}}(\psi \otimes \mathbb{F}_\mathfrak{p})$ has rank 4, and is called **ordinary** if $\mathrm{End}_{\overline{\mathbb{F}}_\mathfrak{p}}(\psi \otimes \mathbb{F}_\mathfrak{p})$ has rank 2, these being the only possibilities. Here, $\overline{\mathbb{F}}_\mathfrak{p}$ is an algebraic closure of $\mathbb{F}_\mathfrak{p}$.

As in the previous section, let

$$\begin{aligned} P_{\psi,\mathfrak{p}}(X) &= X^2 + a_1(\psi,\mathfrak{p})X + u(\psi,\mathfrak{p})p \in A[X] \\ &= (X - \pi_{\psi,\mathfrak{p}})(X - \overline{\pi}_{\psi,\mathfrak{p}}) \in \bar{k}[X] \end{aligned}$$

be the characteristic polynomial of ψ at $\mathfrak{p}$, where $u(\psi,\mathfrak{p}) \in \mathbb{F}_q^*$.

Proposition 12. *Let $\psi \in \mathrm{Drin}_A(k)$ be of rank 2 and let $\mathfrak{p} \in \mathcal{P}_\psi$.*

(i) *If $\mathfrak{p}$ is supersingular, then $a_1(\psi,\mathfrak{p}) = 0$, i.e.*

$$P_{\psi,\mathfrak{p}}(X) = X^2 + u(\psi,\mathfrak{p})p.$$

(ii) *If $\mathfrak{p}$ is ordinary and $\mathrm{End}_{\bar{k}}(\psi)$ is non-trivial, then*

$$k(\pi_{\psi,\mathfrak{p}}) \simeq \mathrm{End}_{\bar{k}}(\psi) \otimes_A k.$$

Proof. (i) Assume that $\mathfrak{p} = pA$ is supersingular. By classical theory, this is equivalent to $p | a_1(\psi,\mathfrak{p})$. Provided $a_1(\psi,\mathfrak{p}) \neq 0$, we obtain that $\deg p \leqslant \deg a_1(\psi,\mathfrak{p})$. On the other hand, by part (iv) of Proposition 8, $\deg a_1(\psi,\mathfrak{p}) \leqslant \frac{\deg p}{2}$, leading to a contradiction. This shows that $a_1(\psi,\mathfrak{p}) = 0$.

(ii) Let $\mathfrak{p} = pA \in \mathcal{P}_\psi$ be ordinary. Then, by classical theory (see, in particular, [Yu]), $k(\pi_{\psi,\mathfrak{p}})$ is an imaginary quadratic extension of k, satisfying

$$k \subsetneq k(\pi_{\psi,\mathfrak{p}}) = \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\psi \otimes \mathbb{F}_\mathfrak{p}) \otimes_A k \subseteq \mathrm{End}_{\overline{\mathbb{F}}_\mathfrak{p}}(\psi \otimes \mathbb{F}_\mathfrak{p}) \otimes_A k,$$

with the latter a rank 2 k-algebra, since $\mathfrak{p}$ is ordinary.

On the other hand,

$$\mathrm{End}_{\bar{k}}(\psi) \otimes_A k \subseteq \mathrm{End}_{\overline{\mathbb{F}}_\mathfrak{p}}(\psi \otimes \mathbb{F}_\mathfrak{p}) \otimes_A k,$$

with the former also a rank 2 k-algebra, from our hypothesis on ψ. By putting everything together, we obtain the desired isomorphism. □

2.3. The Chebotarev Density Theorem

Let K be a finite Galois extension of k. In this section, we recall an effective version of the Chebotarev Density Theorem for K/k proven in [MuSc], and apply it in the context of division fields of Drinfeld modules.

Let g_K be the genus of K and let c_K denote the degree of the constant field of K, that is,

$$c_K := [K \cap \overline{\mathbb{F}}_q : \mathbb{F}_q].$$

Let

$$D := \sum_{\mathfrak{p} \text{ ramified in } K/k} \deg \mathfrak{p}.$$

For $x \in \mathbb{N} \backslash \{0\}$, define

$$\Pi(x; K/k) := \#\{\mathfrak{p} \text{ unramified in } K/k\colon \deg \mathfrak{p} = x\},$$

and for $C \subseteq \mathrm{Gal}(K/k)$ a conjugacy class, define

$$\Pi_C(x; K/k) := \#\{\mathfrak{p} \text{ unramified in } K/k\colon \deg \mathfrak{p} = x,\ \sigma_{\mathfrak{p}} = C\},$$

where $\sigma_{\mathfrak{p}}$ is the Frobenius at $\mathfrak{p}$ in K/k. In particular,

$$\Pi_1(x; K/k)$$

defines the number of primes of k, of degree x, which split completely in K. Define $a_C \in \mathbb{N}$ by the property that the restriction to $K \cap \overline{\mathbb{F}}_q$ of C is τ^{a_C}.

Theorem 13. *(See [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*

$$\left|\Pi_C(x; K/k) - c_K \frac{|C|}{[K:k]} \Pi(x; K/k)\right| \leqslant 2g_K \frac{|C|}{[K:k]} \frac{q^{\frac{x}{2}}}{x} + 6|C| \frac{q^{\frac{x}{2}}}{x} + \left(1 + \frac{|C|}{x}\right) D.$$

The application of Theorem 13 relevant to us is when K is a division field of $\psi \in \mathrm{Drin}_A(k)$ and $C = \{1\}$. Here is a restatement of this theorem in our desired setting:

Theorem 14. *Let* $\psi \in \mathrm{Drin}_A(k)$ *of rank* $r \geqslant 1$. *Let* $d \in A \backslash \mathbb{F}_q$. *Then, for any positive integer* x, *we have*

$$\Pi_1\big(x; k\big(\psi[d]\big)/k\big) = \frac{c_d(x)}{[k(\psi[d]):k]} \cdot \frac{q^x}{x} + \mathrm{O}_\psi\left(\frac{q^{\frac{x}{2}}}{x} \deg d\right),$$

where $c_d(x)$ *is defined in* (8).

Proof. Using the effective Prime Number Theorem for k and Theorem 13 with $K = k(\psi[d])$, $C = \{1\}$, and hence $a_C = 0$, we obtain

$$\Pi_1\big(x; k\big(\psi[d]\big)/k\big) = \frac{c_d(x)}{[k(\psi[d]):k]} \cdot \frac{q^x}{x} + \mathrm{O}\left(\left(2g_d \cdot \frac{1}{[k(\psi[d]):k]} + 6\right) \cdot \frac{q^{\frac{x}{2}}}{x} + \left(1 + \frac{1}{x}\right) D\right),$$

where

$$D := \sum_{\mathfrak{p} \text{ ramified in } k(\psi[d])/k} \deg \mathfrak{p}.$$

By Proposition 2, $D \ll_\psi \deg d$. Combining this with Proposition 4, we deduce that

$$\left(2g_d \cdot \frac{1}{[k(\psi[d]) : k]} + 6\right) \cdot \frac{q^{\frac{x}{2}}}{x} + \left(1 + \frac{1}{x}\right) D \ll_\psi \frac{q^{\frac{x}{2}}}{x} \cdot \deg d,$$

completing the proof. □

3. Proof of Theorem 1

Let $\psi \in \mathrm{Drin}_A(k)$ be of rank 2 and such that $\mathscr{A} := \mathrm{End}_{\bar{k}}(\psi)$ is the full ring of integers in an imaginary quadratic extension k' of k. We keep all the associated notation introduced in the previous sections.

Let x be a fixed positive integer, to be thought of as large (approaching infinity). The goal of the theorem is to obtain an *effective asymptotic formula* for

$$\mathscr{S}(\psi, x) := \sum_{m \in A^{(1)}} \Pi_1\bigl(x; k\bigl(\psi[m]\bigr)/k\bigr),$$

with an *optimal error term*.

By Proposition 10, for any prime $\mathfrak{p} \in \mathcal{P}_\psi$ which splits completely in some $k(\psi[m])$ we have $m^2 | P_{\psi,\mathfrak{p}}(1)$. Using part (v) of Proposition 8 and (17), this implies that $\deg m \leqslant \frac{\deg \mathfrak{p}}{2}$. In other words, the range of $m \in A^{(1)}$ in the definition of $\mathscr{S}(\psi, x)$ restricts to

$$\mathscr{S}(\psi, x) = \sum_{\substack{m \in A^{(1)} \\ \deg m \leqslant \frac{x}{2}}} \Pi_1\bigl(x; k\bigl(\psi[m]\bigr)/k\bigr).$$

To evaluate the sum, we split the range of m into

$$\begin{aligned} \mathscr{S}(\psi, x) &= \sum_{\substack{m \in A^{(1)} \\ \deg m \leqslant y}} \Pi_1\bigl(x; k\bigl(\psi[m]\bigr)/k\bigr) + \sum_{\substack{m \in A^{(1)} \\ y < \deg m \leqslant \frac{x}{2}}} \Pi_1\bigl(x; k\bigl(\psi[m]\bigr)/k\bigr) \\ &=: \mathscr{S}_1(\psi, x, y) + \mathscr{S}_2(\psi, x, y) \end{aligned} \tag{21}$$

for some $y = y(x) \geqslant 1$, to be chosen optimally later, and we apply the effective Chebotarev Density Theorem when $\deg m \leqslant y$. When $y < \deg m \leqslant \frac{x}{2}$, we use adhoc methods to obtain a satisfactory upper bound. The details follow.

A direct application of Theorem 14 and of the elementary estimate

$$\sum_{\substack{m \in A^{(1)} \\ \deg m \leqslant y}} \deg m \leqslant y \frac{q^{y+1} - 1}{q - 1}$$

yields

$$\mathcal{S}_1(\psi, x, y) = \left(\sum_{\substack{m \in A^{(1)} \\ \deg m \leqslant y}} \frac{c_m(x)}{[k(\psi[m]) : k]} \right) \frac{q^x}{x} + \mathrm{O}_\psi\left(q^{\frac{x}{2}+y}\right). \tag{22}$$

To estimate $\mathcal{S}_2(\psi, x, y)$, we make use of our assumptions on ψ. More specifically, we make use of Corollary 11 and Proposition 12, as follows.

Since ψ has rank 2, we can write

$$\mathcal{S}_2(\psi, x, y) = \mathcal{S}_2^{ss}(\psi, x, y) + \mathcal{S}_2^{o}(\psi, x, y), \tag{23}$$

where

$$\mathcal{S}_2^{ss}(\psi, x, y) := \sum_{\substack{m \in A^{(1)} \\ y < \deg m \leqslant \frac{x}{2}}} \#\bigl\{\mathfrak{p}\colon \deg \mathfrak{p} = x,\ \mathfrak{p} \text{ splits completely in } k\bigl(\psi[m]\bigr)/k, \\ \mathfrak{p} \text{ supersingular for } \psi\bigr\},$$

$$\mathcal{S}_2^{o}(\psi, x, y) := \sum_{\substack{m \in A^{(1)} \\ y < \deg m \leqslant \frac{x}{2}}} \#\bigl\{\mathfrak{p}\colon \deg \mathfrak{p} = x,\ \mathfrak{p} \text{ splits completely in } k\bigl(\psi[m]\bigr)/k,\ \mathfrak{p} \text{ ordinary for } \psi\bigr\}.$$

To estimate $\mathcal{S}_2^{ss}(\psi, x, y)$, let $\mathfrak{p} \in \mathcal{P}_\psi$ be supersingular and split completely in $k(\psi[m])$ for some $m \in A^{(1)}$ with $y < \deg m \leqslant \frac{x}{2}$. Using Proposition 9 and part (i) of Proposition 12, we obtain

$$m^2 | P_{\psi,\mathfrak{p}}(1) = 1 + u(\psi, \mathfrak{p})p.$$

At the same time, using parts (ii) and (iii) of Proposition 10, we obtain

$$m | P_{\psi^1,\mathfrak{p}}(1) = 1 - u(\psi, \mathfrak{p})p.$$

Combining the two, we obtain

$$m|2.$$

Since $\deg m \geqslant y \geqslant 1$, we reach a contradiction. Consequently,

$$\mathcal{S}_2^{ss}(\psi, x, y) = 0. \tag{24}$$

To estimate $\mathcal{S}_2^{o}(\psi, x, y)$, let $\mathfrak{p} \in \mathcal{P}_\psi$ be ordinary and split completely in $k(\psi[m])$ for some $m \in A^{(1)}$ with $y < \deg m \leqslant \frac{x}{2}$. Using our assumptions on k and $\mathrm{End}_{\bar{k}}(\psi)$, we write

$$\mathrm{End}_{\bar{k}}(\psi) = A + A\sqrt{f(T)},$$

and so

$$k' = k\bigl(\sqrt{f(T)}\bigr),$$

for some squarefree polynomial $f \in A$ of odd degree, or of even degree and with leading coefficient *not* a square in $\mathbb{F}_q^*$ (see, for example, [Ro, p. 248]).

Using Corollary 11 and part (ii) of Proposition 12, we deduce that

$$\frac{\pi_{\psi,\mathfrak{p}} - 1}{m} = d_1 + d_2\sqrt{f}$$

for some $d_1, d_2 \in A$, and so

$$N_{k'/k}(\pi_{\psi,\mathfrak{p}}) = N_{k'/k}\bigl((1 + md_1) + md_2\sqrt{f}\,\bigr)$$

for some $d_1, d_2 \in A$. Recalling part (ii) of Proposition 8, this gives

$$u(\psi,\mathfrak{p})p = (1 + md_1)^2 - f(md_2)^2$$

for some $u(\psi,\mathfrak{p}) \in \mathbb{F}_q^*$ and $d_1, d_2 \in A$. Therefore

$$\mathscr{S}_2^o(\psi,x,y) \leqslant \sum_{\substack{m\in A^{(1)}\\ y<\deg m\leqslant \frac{x}{2}}} \#\bigl\{(d_1,d_2) \in A\times A\colon \deg\bigl((1+md_1)^2 - f(md_2)^2\bigr) = x\bigr\}.$$

To estimate the size of the set inside the sum above, we use the aforementioned properties of f to infer that

$$\deg\bigl((1+md_1)^2 - f(md_2)^2\bigr) = \max\bigl\{\deg(1+md_1)^2, \deg\bigl(f(md_2)^2\bigr)\bigr\}.$$

Consequently,

$$\begin{aligned}
&\#\bigl\{(d_1,d_2) \in A\times A\colon \deg\bigl((1+md_1)^2 - f(md_2)^2\bigr) = x\bigr\}\\
&\quad\leqslant \#\left\{d_1 \in A\colon \deg d_1 \leqslant \frac{x}{2} - \deg m\right\}\cdot\#\left\{d_2 \in A\colon \deg d_2 \leqslant \frac{x}{2} - \frac{\deg f}{2} - \deg m\right\}\\
&\quad= q^{x-\frac{\deg f}{2}-2\deg m+2},
\end{aligned}$$

and so

$$\begin{aligned}
\mathscr{S}_2^o(\psi,x,y) &\leqslant \sum_{\substack{m\in A^{(1)}\\ y<\deg m\leqslant \frac{x}{2}}} q^{x-\frac{\deg f}{2}-2\deg m+2}\\
&= q^{x-\frac{\deg f}{2}+2}\cdot\frac{q^{-(y+1)} - q^{-(\frac{x}{2}+1)}}{1-q^{-1}}\\
&\leqslant q^{x-y}\cdot\frac{q^{2-\frac{\deg f}{2}}}{1-q^{-1}}. \qquad (25)
\end{aligned}$$

Putting together (21), (22), (23), (24), (25), we obtain

$$\mathscr{S}(\psi,x) = \Biggl(\sum_{\substack{m\in A^{(1)}\\ \deg m\leqslant y}} \frac{c_m(x)}{[k(\psi[m]):k]}\Biggr)\frac{q^x}{x} + \mathrm{O}_\psi\bigl(q^{\frac{x}{2}+y}\bigr) + \mathrm{O}_\psi\bigl(q^{x-y}\bigr).$$

Upon choosing

$$y := \frac{x}{4},$$

we obtain further that

$$\mathscr{S}(\psi, x) = \left(\sum_{\substack{m \in A^{(1)} \\ \deg m \leqslant y}} \frac{c_m(x)}{[k(\psi[m]) : k]} \right) \frac{q^x}{x} + \mathrm{O}_\psi\left(q^{\frac{3x}{4}}\right). \tag{26}$$

To estimate the tail

$$\sum_{\substack{m \in A^{(1)} \\ \deg m \geqslant \frac{x}{4}}} \frac{c_m(x)}{[k(\psi[m]) : k]},$$

we use Propositions 3 and 5, as well as elementary estimates. We obtain

$$\sum_{\substack{m \in A^{(1)} \\ \deg m \geqslant \frac{x}{4}}} \frac{c_m(x)}{[k(\psi[m]) : k]} \ll_\psi \sum_{\substack{m \in A^{(1)} \\ \deg m \geqslant \frac{x}{4}}} \frac{\log(2 \deg m) + \log\log q}{q^{2 \deg m}}$$
$$\ll \frac{\log x}{q^{\frac{x}{4}+1} \log q}.$$

Plugging this in (26), we deduce

$$\mathscr{S}(\psi, x) = \left(\sum_{m \in A^{(1)}} \frac{c_m(x)}{[k(\psi[m]) : k]} \right) \frac{q^x}{x} + \mathrm{O}_\psi\left(q^{\frac{3x}{4}} \log x\right),$$

completing the proof of Theorem 1.

To prove (9), we start with the key remark that the A-module $\psi(\mathbb{F}_\mathfrak{p})$ contains a copy of $(A/mA)^2$ if and only if $\mathfrak{p}$ splits completely in $k(\psi[m])$ (by arguing as in the proof of Proposition 9, emphasizing the two-way implications). Therefore, keeping in mind the A-module structure of $\psi(\mathbb{F}_\mathfrak{p})$ described in (16) and using the inclusion–exclusion formula, we obtain that

$$\begin{aligned} &\#\left\{p \in A^{(1)} \colon \deg p = x,\ \psi(\mathbb{F}_\mathfrak{p}) \text{ is } A\text{-cyclic}\right\} \\ &\quad = \#\left\{p \in A^{(1)} \colon \deg p = x,\ pA \text{ does not split completely in } k\big(\psi[\ell]\big)/k \text{ for any } \ell \in A^{(1)}\right\} \\ &\quad = \sum_{m \in A^{(1)}} \mu_A(m) \Pi_1\big(x, k\big(\psi[m]\big)/k\big), \end{aligned}$$

where, we recall, $\mu_A(\cdot)$ is the Möbius function of A. This sum is now estimated, asymptotically, exactly as $\mathscr{S}(\psi, x)$, leading to (9).

Acknowledgments

The authors are grateful to Florian Breuer, Jing Long-Hoelscher, Nathan Jones, and the anonymous referees for helpful comments and suggestions towards the final version of the paper.

References

[Br] F. Breuer, Torsion bounds for elliptic curves and Drinfeld modules, J. Number Theory 130 (5) (2010) 1241–1250.

[CoMu] A.C. Cojocaru, M.R. Murty, Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem, Math. Ann. 330 (2004) 601–625.

[CoSh] A.C. Cojocaru, A.M. Shulman, Elementary divisors of Drinfeld modules of arbitrary rank, preprint.

[Ga] F. Gardeyn, Une borne pour l'action de l'inertie sauvage sur la torsion d'un module de Drinfeld, Arch. Math. 79 (2002) 241–251.

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

[Go] D. Goss, Basic Structures of Function Field Arithmetic, Ergeb. Math. Grenzgeb. (3), vol. 35, Springer, Berlin, 1996.

[Ha] D. Hayes, Explicit class field theory in global function fields, in: Studies in Algebra and Number Theory, vol. 6, 1979, pp. 173–217.

[He] G.-J. van der Heiden, Weil pairing for Drinfeld modules, Monatschefte Math. 143 (2004) 115–143.

[HsYu] L.-C. Hsia, J. Yu, On characteristic polynomials of geometric Frobenius associated to Drinfeld modules, Compos. Math. 122 (3) (2000) 261–280.

[LaOd] J.C. Lagarias, A.M. Odlyzko, Effective versions of the Chebotarev density theorem, in: A. Fröhlich (Ed.), Algebraic Number Fields, Academic Press, New York, 1977, pp. 409–464.

[Mu] M.R. Murty, On Artin's conjecture, J. Number Theory 16 (1983) 147–168.

[MuSc] V.K. Murty, J. Scherk, Effective versions of the Chebotarev density theorem for function fields, C. R. Acad. Sci. Paris 319 (1994) 523–528.

[Ro] M. Rosen, Number Theory in Function Fields, Grad. Texts in Math., vol. 201, Springer-Verlag, New York, 2002.

[Ta] T. Takahashi, Good reduction of elliptic modules, J. Math. Soc. Japan 34 (3) (1982) 475–487.

[Th] D. Thakur, Function Field Arithmetic, World Scientific Publishing, 2004.

[Yu] J.-K. Yu, Isogenies of Drinfeld modules, J. Number Theory 54 (1995) 161–171.