Journal of Number Theory ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

Endomorphism rings of reductions of Drinfeld modules

Sumita Garai, Mihran Papikian [*]

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA

ARTICLE INFO

Article history:
Received 30 April 2018
Received in revised form 7 February 2019
Accepted 11 February 2019
Available online xxxx
Communicated by A. Pal

In memory of David Goss

MSC:
11G09
11R58

Keywords:
Drinfeld modules
Endomorphism rings

ABSTRACT

Let $A = \mathbb{F}_q[T]$ be the polynomial ring over $\mathbb{F}_q$, and F be the field of fractions of A. Let ϕ be a Drinfeld A-module of rank $r \geq 2$ over F. For all but finitely many primes $\mathfrak{p} \lhd A$, one can reduce ϕ modulo $\mathfrak{p}$ to obtain a Drinfeld A-module $\phi \otimes \mathbb{F}_\mathfrak{p}$ of rank r over $\mathbb{F}_\mathfrak{p} = A/\mathfrak{p}$. The endomorphism ring $\mathcal{E}_\mathfrak{p} = \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\phi \otimes \mathbb{F}_\mathfrak{p})$ is an order in an imaginary field extension K of F of degree r. Let $\mathcal{O}_\mathfrak{p}$ be the integral closure of A in K, and let $\pi_\mathfrak{p} \in \mathcal{E}_\mathfrak{p}$ be the Frobenius endomorphism of $\phi \otimes \mathbb{F}_\mathfrak{p}$. Then we have the inclusion of orders $A[\pi_\mathfrak{p}] \subset \mathcal{E}_\mathfrak{p} \subset \mathcal{O}_\mathfrak{p}$ in K. We prove that if $\mathrm{End}_{F^{\mathrm{alg}}}(\phi) = A$, then for arbitrary non-zero ideals $\mathfrak{n}, \mathfrak{m}$ of A there are infinitely many $\mathfrak{p}$ such that $\mathfrak{n}$ divides the index $\chi(\mathcal{E}_\mathfrak{p}/A[\pi_\mathfrak{p}])$ and $\mathfrak{m}$ divides the index $\chi(\mathcal{O}_\mathfrak{p}/\mathcal{E}_\mathfrak{p})$. We show that the index $\chi(\mathcal{E}_\mathfrak{p}/A[\pi_\mathfrak{p}])$ is related to a reciprocity law for the extensions of F arising from the division points of ϕ. In the rank $r = 2$ case we describe an algorithm for computing the orders $A[\pi_\mathfrak{p}] \subset \mathcal{E}_\mathfrak{p} \subset \mathcal{O}_\mathfrak{p}$, and give some computational data.

[*] Corresponding author.
E-mail addresses: sxg386@psu.edu (S. Garai), papikian@psu.edu (M. Papikian).

https://doi.org/10.1016/j.jnt.2019.02.008
0022-314X/© 2019 Elsevier Inc. All rights reserved.

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements and of characteristic p. Let $A = \mathbb{F}_q[T]$ be the polynomial ring over $\mathbb{F}_q$ in an indeterminate T, and $F = \mathbb{F}_q(T)$ be the field of fractions of A. In this paper we study the endomorphism rings of the reductions of a fixed Drinfeld module defined over F. We are interested in theoretical, as well as computational, aspects of the theory of these rings. To state the main results of the paper, we first need to introduce some notation and terminology.

1.1. Notation and terminology

The degree $\deg(a)$ of $0 \neq a \in A$ is its degree as a polynomial in T. The degree function extends to a valuation of F; the corresponding place of F is denoted by ∞. Let $F_\infty = \mathbb{F}_q(\!(1/T)\!)$ be the completion of F at ∞. For a non-zero ideal $\mathfrak{n} \lhd A$, by abuse of notation, we denote by the same symbol the unique monic polynomial in A generating $\mathfrak{n}$. We will call a non-zero prime ideal of A simply a *prime* of A. Given a prime $\mathfrak{p}$ of A, we denote by $A_\mathfrak{p}$ (resp. $F_\mathfrak{p}$) the completion of A at $\mathfrak{p}$ (resp. the fraction field of $A_\mathfrak{p}$); we also denote $\mathbb{F}_\mathfrak{p} = A/\mathfrak{p}$. Given a field L, we denote by L^{alg} (resp. L^{sep}) an algebraic (resp. separable) closure of L, and $G_L = \mathrm{Gal}(L^{\mathrm{sep}}/L)$.

Let K be a field extension of F of degree $r \geq 2$. Let $\mathcal{O}_K$ be the integral closure of A in K. An *A-order* $\mathcal{O}$ in K is a subring of K such that

(i) $A \subset \mathcal{O}$;
(ii) $\mathcal{O}$ is a finitely generated A-module (equiv. $\mathcal{O}$ is an A-subalgebra of $\mathcal{O}_K$);
(iii) $\mathcal{O}$ contains an F-basis of K (equiv. the quotient module $\mathcal{O}_K/\mathcal{O}$ has finite cardinality).

Since A is a PID, $\mathcal{O}$ is a free A-module of rank

$$\mathrm{rank}_A \mathcal{O} = \dim_F(\mathcal{O} \otimes_A F) = \dim_F K = r.$$

Let $\mathcal{O} \subset \mathcal{O}'$ be two A-orders in K. Since both modules $\mathcal{O}$ and $\mathcal{O}'$ have the same rank over A, and both contain 1, we have

$$\mathcal{O}'/\mathcal{O} \cong A/\mathfrak{b}_1 \times A/\mathfrak{b}_2 \times \cdots \times A/\mathfrak{b}_{r-1}, \tag{1.1}$$

for uniquely determined non-zero ideals $\mathfrak{b}_1, \ldots, \mathfrak{b}_{r-1} \lhd A$ such that

$$\mathfrak{b}_1 \mid \mathfrak{b}_2 \mid \cdots \mid \mathfrak{b}_{r-1}.$$

We call

$$\chi(\mathcal{O}'/\mathcal{O}) = \prod_{i=1}^{r-1} \mathfrak{b}_i$$

the *index* of $\mathcal{O}$ in $\mathcal{O}'$, and $(\mathfrak{b}_1, \dots, \mathfrak{b}_{r-1})$ the *refined index.* (Note that $\chi(\mathcal{O}'/\mathcal{O})$ is the Fitting ideal of the A-module $\mathcal{O}'/\mathcal{O}$.) The *conductor* of $\mathcal{O}$ in $\mathcal{O}'$ is

$$\mathfrak{c} = \{c \in K \mid c\mathcal{O}' \subset \mathcal{O}\}.$$

This is the largest ideal in $\mathcal{O}'$ which is also an ideal in $\mathcal{O}$. The conductor is related to the refined index by $\mathfrak{c} \cap A = \mathfrak{b}_{r-1}$.

1.2. Drinfeld modules

Let L be a field provided with a structure $\gamma : A \to L$ of an A-algebra. Note that either γ is injective or γ factors through the quotient map $A \to \mathbb{F}_\mathfrak{p} \hookrightarrow L$ for some prime $\mathfrak{p}$. Let τ be the Frobenius endomorphism of L relative to $\mathbb{F}_q$, that is, the map $\alpha \mapsto \alpha^q$, and let $L\{\tau\}$ be the noncommutative ring of polynomials in τ with coefficients in L and the commutation rule $\tau c = c^q \tau$ for any $c \in L$.

A *Drinfeld A-module over L of rank* $r \geq 1$ is a ring homomorphism

$$\phi : A \longrightarrow L\{\tau\}$$

$$a \mapsto \phi_a = \gamma(a) + \sum_{i=1}^{r\cdot \deg(a)} g_i(a)\tau^i$$

uniquely determined through

$$\phi_T = \gamma(T) + \sum_{i=1}^{r} g_i(T)\tau^i, \quad g_r(T) \neq 0.$$

A *morphism* from the Drinfeld module ϕ to the Drinfeld module ψ over L is some $u \in L\{\tau\}$ such that $u\phi_a = \psi_a u$ for all $a \in A$ (it suffices to require this for $a = T$); u is an *isomorphism* if $u \in L\{\tau\}^\times = L^\times$. With this definition, the *endomorphism ring*

$$\mathrm{End}_L(\phi) = \{u \in L\{\tau\} \mid u\phi_T = \phi_T u\}$$

is the centralizer of $\phi(A)$ in $L\{\tau\}$. It is clear that $\mathrm{End}_L(\phi)$ contains in its center the subring $\phi(A) \cong A$, hence is an A-algebra. It can be shown that $\mathrm{End}_L(\phi)$ is a free A-module of rank $\leq r^2$, and $\mathrm{End}_L(\phi) \otimes_A F_\infty$ is a division algebra over F_∞; see [7].

The Drinfeld module ϕ endows L^{alg} with an A-module structure, where $a \in A$ acts by ϕ_a. The *a-torsion* $\phi[a] \subset L^{\mathrm{alg}}$ of ϕ is the kernel of ϕ_a, that is, the set of zeros of the polynomial

$$\phi_a(x) = \gamma(a)x + \sum_{i=1}^{r\cdot\deg(a)} g_i(a)x^{q^i} \in L[x]. \tag{1.2}$$

It is clear that $\phi[a]$ has a natural structure of an A-module. If a is not divisible by $\ker(\gamma)$, then $\phi[a] \cong (A/aA)^{\oplus r}$ and $\phi[a] \subset L^{\mathrm{sep}}$ (since $\phi'_a(x) = \gamma(a) \neq 0$). For a prime $\mathfrak{l} \lhd A$ different from $\ker(\gamma)$, the *$\mathfrak{l}$-adic Tate module of ϕ*,

$$T_{\mathfrak{l}}(\phi) = \varprojlim \phi[\mathfrak{l}^n] \cong A_{\mathfrak{l}}^{\oplus r},$$

carries a continuous Galois representation

$$\rho_{\phi,\mathfrak{l}} : G_L \to \mathrm{Aut}_{A_{\mathfrak{l}}}(T_{\mathfrak{l}}(\phi)) \cong \mathrm{GL}_r(A_{\mathfrak{l}}).$$

1.3. Main results

Let $\phi : A \to F\{\tau\}$ be a Drinfeld module of rank r over F defined by

$$\phi_T = T + g_1\tau + \cdots + g_r\tau^r.$$

(We will always implicitly assume that $\gamma : A \to F$ is the canonical embedding of A into its field of fractions.) We say that a prime $\mathfrak{p} \lhd A$ is a *prime of good reduction* for ϕ if $\mathrm{ord}_{\mathfrak{p}}(g_i) \geq 0$ for $1 \leq i \leq r-1$, and $\mathrm{ord}_{\mathfrak{p}}(g_r) = 0$. In that case, we can consider $g_1, \dots, g_r$ as elements of $A_{\mathfrak{p}}$; denote by $\overline{g}$ the image of $g \in A_{\mathfrak{p}}$ under the canonical homomorphism $A_{\mathfrak{p}} \to A_{\mathfrak{p}}/\mathfrak{p}$. The *reduction of ϕ at $\mathfrak{p}$* is the Drinfeld module $\phi \otimes \mathbb{F}_{\mathfrak{p}}$ over $\mathbb{F}_{\mathfrak{p}}$ given by

$$(\phi \otimes \mathbb{F}_{\mathfrak{p}})_T = \overline{T} + \overline{g_1}\tau + \cdots + \overline{g_r}\tau^r.$$

Note that $\phi \otimes \mathbb{F}_{\mathfrak{p}}$ has rank r since $\overline{g_r} \neq 0$. All but finitely many primes of A are primes of good reduction for a given Drinfeld module ϕ; we denote the set of these primes by $\mathcal{P}(\phi)$.

Let $\mathfrak{p} \in \mathcal{P}(\phi)$ and $d = \deg(\mathfrak{p})$. Let $\mathcal{E}_{\mathfrak{p}} := \mathrm{End}_{\mathbb{F}_{\mathfrak{p}}}(\phi \otimes \mathbb{F}_{\mathfrak{p}})$. It is easy to see that $\pi_{\mathfrak{p}} := \tau^d$ is in the center of $\mathbb{F}_{\mathfrak{p}}\{\tau\}$, hence $\pi_{\mathfrak{p}} \in \mathcal{E}_{\mathfrak{p}}$. Using the theory of Drinfeld modules over finite fields it is easy to show that $A[\pi_{\mathfrak{p}}] \subset \mathcal{E}_{\mathfrak{p}}$ are A-orders in an *imaginary* field extension $K := F(\pi_{\mathfrak{p}})$ of F of degree r ("imaginary" means that there is a unique place of K over ∞); see Proposition 2.1. Denote by $\mathcal{O}_{\mathfrak{p}}$ the integral closure of A in K. Thus, we have the inclusion of A-orders

$$A[\pi_{\mathfrak{p}}] \subset \mathcal{E}_{\mathfrak{p}} \subset \mathcal{O}_{\mathfrak{p}}.$$

The endomorphism rings (and algebras) of Drinfeld modules over finite fields have been extensively studied; cf. [8], [2], [11], [12], [22]. They play an important role in the theory of Drinfeld modules, as well as their applications to other areas, such as the theory of central simple algebras (cf. [10]) or the Langlands conjecture over function fields (cf.

[8], [15]). In this paper, we are primarily interested in the indices of $\mathcal{E}_\mathfrak{p}/A[\pi_\mathfrak{p}]$ and $\mathcal{O}_\mathfrak{p}/\mathcal{E}_\mathfrak{p}$ as $\mathfrak{p}$ varies. We prove the following:

Theorem 1.1. *Let ϕ be a Drinfeld A-module of rank $r \geq 2$ over F. Let $\mathfrak{n}$ and $\mathfrak{m}$ be arbitrary non-zero elements of A.*

(1) *The subset of primes $\mathfrak{p} \in \mathcal{P}(\phi)$ such that $\mathfrak{n}$ divides $\chi(\mathcal{E}_\mathfrak{p}/A[\pi_\mathfrak{p}])$ has positive density.*
(2) *If $\mathrm{End}_{F^{\mathrm{alg}}}(\phi) = A$, then the subset of primes $\mathfrak{p} \in \mathcal{P}(\phi)$ such that $\mathfrak{n}$ divides $\chi(\mathcal{E}_\mathfrak{p}/A[\pi_\mathfrak{p}])$ and, simultaneously, $\mathfrak{m}$ divides $\chi(\mathcal{O}_\mathfrak{p}/\mathcal{E}_\mathfrak{p})$ has positive density.*

We prove (1) as Corollary 3.2, and the proof of (2) is given at the end of Section 4.2. In fact, we prove stronger results about the refined indices from which this theorem follows. Our proof is modeled on the proof of an analogous result for abelian varieties by Zarhin [23].

Next, let $\mathfrak{p} \in \mathcal{P}(\phi)$ and $(\mathfrak{b}_{\mathfrak{p},1}, \dots, \mathfrak{b}_{\mathfrak{p},r-1})$ be the refined index of $\mathcal{E}_\mathfrak{p}/A[\pi_\mathfrak{p}]$. Let

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

the minimal polynomial of $\pi_\mathfrak{p}$ over F. We show that $\mathfrak{b}_{\mathfrak{p},1}$ and $a_{\mathfrak{p},1}$ produce an interesting reciprocity law (see Section 3).

Theorem 1.2. *Let ϕ be a Drinfeld A-module of rank $r \geq 2$ over F. Let $0 \neq \mathfrak{n} \lhd A$. Assume the characteristic p of F does not divide r and the prime $\mathfrak{p} \in \mathcal{P}(\phi)$ does not divide $\mathfrak{n}$. Then $\mathfrak{p}$ splits completely in the Galois extension $F(\phi[\mathfrak{n}])$ of F if and only if*

$$a_{\mathfrak{p},1} + r \equiv 0 \pmod{\mathfrak{n}} \quad \textit{and} \quad \mathfrak{b}_{\mathfrak{p},1} \equiv 0 \pmod{\mathfrak{n}}.$$

Theorem 1.2 for $r = 2$ was proved in [4]. Here we give a somewhat different and simpler proof which works for any r. The restriction on r being coprime to p can be removed if $\mathfrak{n}$ is prime; see Remark 3.1. The primes which split completely in $F(\phi[\mathfrak{n}])$ have been studied before, in particular in papers by Cojocaru and Shulman [5], [6], and Kuo and Liu [14]. We also note that the argument of the proof of Theorem 1.2 can be adapted to the setting of elliptic curves over $\mathbb{Q}$ to give a different (simpler) proof of [9, Cor. 2.2] which does not rely on Deuring's Lifting Theorem.

In Section 5, we discuss how to compute in practice the endomorphism ring $\mathcal{E}_\mathfrak{p}$ and the indices $\chi(\mathcal{E}_\mathfrak{p}/A[\pi_\mathfrak{p}])$ and $\chi(\mathcal{O}_\mathfrak{p}/\mathcal{E}_\mathfrak{p})$. The calculation of the characteristic polynomial of the Frobenius $P_\mathfrak{p}(X)$ is fairly straightforward, and easier than Schoof's algorithm [18] for elliptic curves over $\mathbb{F}_p$. We describe an algorithm for calculating $P_\mathfrak{p}(X)$ in polynomial time in d and r. Then, assuming the rank of ϕ is 2, we describe an algorithm for computing $\mathcal{E}_\mathfrak{p}$. The algorithm actually computes all three rings $A[\pi_\mathfrak{p}] \subset \mathcal{E}_\mathfrak{p} \subset \mathcal{O}_\mathfrak{p}$, and the corresponding indices. In comparison to the known algorithms for computing the endomorphism rings of elliptic curves over finite fields, cf. [9], [3], our algorithm is quite different and more elementary. The difference stems from the fact that we crucially use the fact that $\mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\phi)$ is a subring of the larger ambient space $\mathbb{F}_\mathfrak{p}\{\tau\}$. We have implemented our algorithms in `Magma`, and the examples presented in Section 5 are based on computer calculations.

2. Drinfeld modules over $\mathbb{F}_\mathfrak{p}$

In this section we collect some facts about Drinfeld modules over finite fields that are used throughout the paper.

Let $\mathfrak{p} \lhd A$ be a prime of degree d. Let $\phi : A \to \mathbb{F}_\mathfrak{p}\{\tau\}$ be a Drinfeld A-module over $\mathbb{F}_\mathfrak{p}$ of rank r determined by

$$\phi_T = \gamma(T) + g_1\tau + \cdots + g_{r-1}\tau^{r-1} + g_r\tau^r, \quad g_r \neq 0,$$

where $\gamma : A \to \mathbb{F}_\mathfrak{p} = A/\mathfrak{p}$ is the quotient map. It is easy to see that $\pi := \tau^d$ is in the center of $\mathbb{F}_\mathfrak{p}\{\tau\}$, hence $\pi \in \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\phi)$. Denote by $P(X) \in A[X]$ the minimal polynomial of π over $\phi(A)$.

Proposition 2.1. *Let $K = F(\pi) \cong F[X]/(P(X))$.*

(1) *The field extension K/F is imaginary of degree r.*
(2) *$\mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\phi)$ is an A-order in K.*

Proof. Let r_1 be the degree of $P(X)$. By Theorem 2.9 in [11], r_1 divides r. Let $r_2 = r/r_1$. Let $P_1(X) = P(X)^{r_2}$. By Lemma 3.3 and Theorem 5.1 (ii) in [11], we have $(P_1(0)) = \mathfrak{p}$. Thus, if $c = P(0)$ is the constant term of $P(X)$, then c^{r_2}, up to $\mathbb{F}_q^\times$ multiple, is equal to the irreducible monic polynomial $\mathfrak{p}$. This implies $r_2 = 1$, or equivalently $r = r_1$. By [11, (2.3)], K/F is imaginary. This proves (1).

By Theorem 2.9 in [11], $\mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\phi) \otimes_A F$ is a central division algebra over K of dimension $r_2^2 = 1$. Thus, $\mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\phi) \otimes_A F = K$. This proves (2). □

The previous proposition implies that $P(X)$ has degree r. Write

$$P(X) = X^r + a_1X^{r-1} + \cdots + a_r.$$

Proposition 2.2. *For $1 \leq i \leq r$, we have*

$$\deg(a_i) \leq \frac{i \cdot d}{r}.$$

Proof. This follows from [22, Thm. 1 (f)]. □

Proposition 2.3. *Let*

$$\varepsilon(\phi) := (-1)^r(-1)^{d(r+1)}\mathrm{Nr}_{\mathbb{F}_\mathfrak{p}/\mathbb{F}_q}(g_r)^{-1} \in \mathbb{F}_q^\times.$$

Then

$$a_r = \varepsilon(\phi)\mathfrak{p}.$$

Proof. This follows from [13, p. 268]. □

We can consider $\mathbb{F}_\mathfrak{p}$ as an A-module via ϕ; this module will be denoted ${}^\phi\mathbb{F}_\mathfrak{p}$. Then

$$ {}^\phi\mathbb{F}_\mathfrak{p} \cong A/\mathfrak{d}_1 \times \cdots \times A/\mathfrak{d}_r, \tag{2.1}$$

for uniquely determined non-zero ideals $\mathfrak{d}_1, \dots, \mathfrak{d}_r \lhd A$ such that $\mathfrak{d}_1 \mid \mathfrak{d}_2 \mid \cdots \mid \mathfrak{d}_r$. There are at most r terms because ${}^\phi\mathbb{F}_\mathfrak{p}$ is a finite A-module so for some $\mathfrak{d} \lhd A$ we have ${}^\phi\mathbb{F}_\mathfrak{p} \subset \phi[\mathfrak{d}] \cong (A/\mathfrak{d})^r$. Denote $\chi(\phi) := \mathfrak{d}_1 \cdots \mathfrak{d}_r$. It is clear that $\deg \chi(\phi) = \deg \mathfrak{p}$. It is also easy to see the following:

Lemma 2.4. $\mathfrak{d}_1 \in A$ *is the monic polynomial of largest degree such that* $\mathfrak{p}$ *does not divide* $\mathfrak{d}_1$ *and all the roots of* $\phi_{\mathfrak{d}_1}(x)$ *are in* $\mathbb{F}_\mathfrak{p}$.

Proposition 2.5. *We have*

$$\chi(\phi) = P(1)A = (1 + a_1 + a_2 + \cdots + a_r)A.$$

Proof. See [11, Thm. 5.1 (i)]. □

Proposition 2.6. *Let* $\mathrm{Frob}_\mathfrak{p} \in G_{\mathbb{F}_\mathfrak{p}}$ *be the Frobenius automorphism* $\alpha \mapsto \alpha^{q^d}$. *Let* $\mathfrak{l} \lhd A$ *be a prime different from* $\mathfrak{p}$.

(1) *The characteristic polynomial of* $\rho_{\phi,\mathfrak{l}}(\mathrm{Frob}_\mathfrak{p})$ *is* $P(X)$*; in particular, the characteristic polynomial of* $\rho_{\phi,\mathfrak{l}}(\mathrm{Frob}_\mathfrak{p})$ *has coefficients in* A *and does not depend on* $\mathfrak{l}$.
(2) *The natural map*

$$\mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\phi) \otimes_A A_\mathfrak{l} \to \mathrm{End}_{A_\mathfrak{l}[G_{\mathbb{F}_\mathfrak{p}}]}(T_\mathfrak{l}(\phi))$$

is an isomorphism.

Proof. See [11, §3] or [22, Thm. 2]. □

3. Reciprocity law: proof of Theorem 1.2

Let ϕ be a Drinfeld A-module over F of rank $r \geq 2$. For $\mathfrak{n} \lhd A$, let $F(\phi[\mathfrak{n}])$ be the splitting field of the polynomial $\phi_\mathfrak{n}(x)$ in (1.2). This is a Galois extension whose Galois group is naturally a subgroup of $\mathrm{GL}_r(A/\mathfrak{n})$. A prime $\mathfrak{p} \lhd A$ is unramified in $F(\phi[\mathfrak{n}])/F$ if $\mathfrak{p} \in \mathcal{P}(\phi)$ and $\mathfrak{p}$ does not divide $\mathfrak{n}$; cf. [21]. Theorem 1.2 describes those primes which split completely in $F(\phi[\mathfrak{n}])$ in terms of congruences modulo $\mathfrak{n}$; such theorems are usually called "reciprocity laws". Recall that the set of all but finitely many primes which split completely in a given Galois extension uniquely determines that extension. In the following proof we keep the notion introduced right before Theorem 1.2.

Proof of Theorem 1.2. To simplify the notation, denote $\overline{\phi} = \phi \otimes \mathbb{F}_\mathfrak{p}$. The prime $\mathfrak{p}$ is unramified in $F(\phi[\mathfrak{n}])$. Reducing $\phi_\mathfrak{n}(x)$ modulo $\mathfrak{p}$ we get a canonical isomorphism $\phi[\mathfrak{n}] \cong \overline{\phi}[\mathfrak{n}]$ of A-modules. The prime $\mathfrak{p}$ splits completely in $F(\phi[\mathfrak{n}])$ if and only if $\mathrm{Frob}_\mathfrak{p} \in G_{\mathbb{F}_\mathfrak{p}}$ acts as the identity on $\overline{\phi}[\mathfrak{n}]$. On the other hand, the action of $\mathrm{Frob}_\mathfrak{p}$ on $\overline{\phi}[\mathfrak{n}]$ agrees with the action of $\pi_\mathfrak{p}$ as an endomorphism of $\overline{\phi}$. Thus, we need to show that $\pi_\mathfrak{p}$ acts as the identity on $\overline{\phi}[\mathfrak{n}]$ if and only if the congruences of the theorem hold.

First, we prove that $w \in \mathcal{E}_\mathfrak{p}$ acts as 0 on $\overline{\phi}[\mathfrak{n}]$ if and only if $w \in \mathfrak{n}\mathcal{E}_\mathfrak{p}$. If $w \in \mathfrak{n}\mathcal{E}_\mathfrak{p}$ then $w = v\overline{\phi}_\mathfrak{n}$ for some $v \in \mathcal{E}_\mathfrak{p}$, so it obviously acts as 0 on $\overline{\phi}[\mathfrak{n}]$. Conversely, suppose w acts as 0 on $\overline{\phi}[\mathfrak{n}]$. By the division algorithm in $\mathbb{F}_\mathfrak{p}\{\tau\}$, we can write $w = v\overline{\phi}_\mathfrak{n} + u$ for some $v, u \in \mathbb{F}_\mathfrak{p}\{\tau\}$ with $u = 0$ or $\deg_\tau(u) < \deg_\tau(\overline{\phi}_\mathfrak{n})$. Since w and $\overline{\phi}_\mathfrak{n}$ act as 0 on $\overline{\phi}[\mathfrak{n}]$, so does u. On the other hand, the polynomial $\overline{\phi}_\mathfrak{n}(x)$ is separable. This implies $\deg_\tau(u) \geq \deg_\tau(\overline{\phi}_\mathfrak{n})$ or $u = 0$. Thus, $u = 0$ and $w = v\overline{\phi}_\mathfrak{n}$. We need to show that $v \in \mathcal{E}_\mathfrak{p}$, i.e., v commutes with $\overline{\phi}(A)$. Now $w\overline{\phi}_b = v\overline{\phi}_\mathfrak{n}\overline{\phi}_b = v\overline{\phi}_b\overline{\phi}_\mathfrak{n}$ and $w\overline{\phi}_b = \overline{\phi}_b w = \overline{\phi}_b v\overline{\phi}_\mathfrak{n}$. Thus, $(v\overline{\phi}_b - \overline{\phi}_b v)\overline{\phi}_\mathfrak{n} = 0$. Since $\mathbb{F}_\mathfrak{p}\{\tau\}$ has no zero-divisors and $\overline{\phi}_\mathfrak{n} \neq 0$, we must have $v\overline{\phi}_b = \overline{\phi}_b v$ for all $b \in A$, so $v \in \mathcal{E}_\mathfrak{p}$.

Suppose $\pi_\mathfrak{p}$ acts as a scalar on $\overline{\phi}[\mathfrak{n}]$. This means that there is $c \in A$ such that $\pi_\mathfrak{p} - c$ annihilates $\overline{\phi}[\mathfrak{n}]$. By the previous paragraph, this is equivalent to $\pi_\mathfrak{p} - c$ being in $\mathfrak{n}\mathcal{E}_\mathfrak{p}$; this is equivalent to $A[\pi_\mathfrak{p}] \subset A + \mathfrak{n}\mathcal{E}_\mathfrak{p}$. We can choose an A-basis $1, e_1, \dots, e_{r-1}$ of $\mathcal{E}_\mathfrak{p}$ such that $A[\pi_\mathfrak{p}] = A + \mathfrak{b}_{\mathfrak{p},1}e_1 + \cdots + \mathfrak{b}_{\mathfrak{p},r-1}e_{r-1}$. Since $\mathfrak{b}_{\mathfrak{p},1}$ divides $\mathfrak{b}_{\mathfrak{p},2}, \dots, \mathfrak{b}_{\mathfrak{p},r-1}$, the inclusion $A[\pi_\mathfrak{p}] \subset A + \mathfrak{n}\mathcal{E}_\mathfrak{p}$ is equivalent to $\mathfrak{n} \mid \mathfrak{b}_{\mathfrak{p},1}$. Thus, $\pi_\mathfrak{p}$ acts as a scalar on $\overline{\phi}[\mathfrak{n}]$ if and only if $\mathfrak{n}$ divides $\mathfrak{b}_{\mathfrak{p},1}$.

Now note that $\pi_\mathfrak{p}$ acts as the identity on $\overline{\phi}[\mathfrak{n}]$ if and only if $\pi_\mathfrak{p}$ acts as a scalar c on $\overline{\phi}[\mathfrak{n}]$ and $c \equiv 1 \pmod{\mathfrak{n}}$. If $\pi_\mathfrak{p}$ acts as a scalar then the characteristic polynomial of $\pi_\mathfrak{p}$ satisfies $P_\mathfrak{p}(X) \equiv (X - c)^r \pmod{\mathfrak{n}}$. (This congruence is not sufficient for $\pi_\mathfrak{p}$ to act as a scalar on $\overline{\phi}[\mathfrak{n}]$, if the action is not semi-simple.) We have

$$(X - c)^r = X^r - rcX^{r-1} + \cdots .$$

Since p does not divide r by assumption, we see that $c \equiv 1 \pmod{\mathfrak{n}}$ if and only if $rc \equiv r \pmod{\mathfrak{n}}$. Hence $c \equiv 1 \pmod{\mathfrak{n}}$ if and only if $a_{\mathfrak{p},1} \equiv -rc \equiv -r \pmod{\mathfrak{n}}$. □

Remark 3.1. If $\mathfrak{n}$ itself is prime, then in Theorem 1.2 one can dispose with the assumption that $p \nmid r$ as follows: Decompose $r = p^s r'$, $s \geq 0$ with $p \nmid r'$. Then $\mathfrak{p} \nmid \mathfrak{n}$ splits completely in $F(\phi[\mathfrak{n}])$ if and only if

$$a_{\mathfrak{p},p^s} + r' \equiv 0 \pmod{\mathfrak{n}} \quad \text{and} \quad \mathfrak{b}_{\mathfrak{p},1} \equiv 0 \pmod{\mathfrak{n}}.$$

The proof is essentially the same except at the end we have

$$(X-c)^r = (X^{p^s} - c^{p^s})^{r'} = X^r - r'c^{p^s}X^{p^s(r'-1)} + \cdots .$$

If $\mathfrak{n}$ is prime, then the pth power map is an automorphism of $(A/\mathfrak{n})^\times$. Thus, $c \equiv 1 \pmod{\mathfrak{n}}$ if and only if $c^{p^s} \equiv 1 \pmod{\mathfrak{n}}$; thus, $c \equiv 1 \pmod{\mathfrak{n}}$ if and only if $a_{\mathfrak{p},p^s} \equiv -r'c^{p^s} \equiv -r' \pmod{\mathfrak{n}}$.

Corollary 3.2. *Let ϕ be a Drinfeld A-module over F of rank $r \geq 2$. For a given $\mathfrak{n} \in A$, the set of primes $\mathfrak{p} \in \mathcal{P}(\phi)$ such that $\mathfrak{n}$ divides $\mathfrak{b}_{\mathfrak{p},1}$ has positive density. In particular, for any $\mathfrak{n} \in A$ there are infinitely many $\mathfrak{p} \in \mathcal{P}(\phi)$ such that $\mathfrak{n}$ divides the index $\chi(\mathcal{E}_\mathfrak{p}/A[\pi_\mathfrak{p}])$.*

Proof. From the proof of Theorem 1.2 we see that for any prime $\mathfrak{p}$ for which $\pi_\mathfrak{p}$ acts as a scalar on $(\phi \otimes \mathbb{F}_\mathfrak{p})[\mathfrak{n}]$ we have $\mathfrak{n} \mid \mathfrak{b}_{\mathfrak{p},1}$ (this part does not use the assumption that r is coprime to p). The set of primes that split completely in $F(\phi[\mathfrak{n}])$ have this property and positive density $1/[F(\phi[\mathfrak{n}]) : F]$ by Chebotarev. □

Let $\mathfrak{p} \in \mathcal{P}(\phi)$. As in Section 2, we can consider $\mathbb{F}_\mathfrak{p}$ as an A-module via $\phi \otimes \mathbb{F}_\mathfrak{p}$. Let

$${}^{\phi\otimes\mathbb{F}_\mathfrak{p}}\mathbb{F}_\mathfrak{p} \cong A/\mathfrak{d}_{\mathfrak{p},1} \times \cdots \times A/\mathfrak{d}_{\mathfrak{p},r}$$

be the isomorphism of (2.1). (Keep in mind that ϕ in Section 2 is over $\mathbb{F}_\mathfrak{p}$, whereas in this section ϕ is over F.)

Corollary 3.3. *With notation and assumptions of Theorem 1.2, we have*

$$\mathfrak{d}_{\mathfrak{p},1} = \gcd(\mathfrak{b}_{\mathfrak{p},1}, a_{\mathfrak{p},1} + r).$$

Proof. From the proof of Theorem 1.2 we see that $(\phi \otimes \mathbb{F}_\mathfrak{p})[\mathfrak{n}] \subset \mathbb{F}_\mathfrak{p}$ if and only if $\mathfrak{p}$ splits completely in $F(\phi[\mathfrak{n}])$. The claim then follows from Lemma 2.4 and Theorem 1.2. □

The previous corollary for $r = 2$ already appears in [4]. In the $r = 2$ case, from Corollary 3.3, Proposition 2.3 and Proposition 2.5 we also get that

$$\frac{1 + a_{\mathfrak{p},1} + \varepsilon(\phi \otimes \mathbb{F}_\mathfrak{p})\mathfrak{p}}{\gcd(\mathfrak{b}_{\mathfrak{p},1}, a_{\mathfrak{p},1} + r)} \in A,$$

and this polynomial generates $\mathfrak{d}_{\mathfrak{p},2}$.

4. Large indices: proof of Theorem 1.1

4.1. Preliminaries

Fix a prime $\mathfrak{l} \lhd A$ and denote $K = F_\mathfrak{l}$. Let V be a vector space of dimension r over K. For $u \in \mathrm{End}_K(V)$, denote by $\Delta(u)$ the discriminant of the characteristic polynomial of u. Note that the characteristic polynomial of u has no multiple roots over K^{alg} if and only if $\Delta(u) \neq 0$.

Denote by $Z(u)$ the centralizer of u in $\mathrm{End}_K(V)$. Assume $\Delta(u) \neq 0$. Obviously, $K[u] \subseteq Z(u)$, but since $K[u]$ is a maximal torus in $\mathrm{End}_K(V)$ and $Z(u) = Z(K[u])$, we in fact have $K[u] = Z(u)$. Denote

$$Z(u)^\circ = \{w \in Z(u) \mid \Delta(w) \neq 0\}.$$

Since the complement of $Z(u)^\circ$ in $Z(u)$ is the locus of vanishing of Δ, $Z(u)^\circ$ is open and everywhere dense in $Z(u)$ with respect to the $\mathfrak{l}$-adic topology. It is clear that for any $w \in Z(u)^\circ$ we have $Z(w) = Z(u)$.

Lemma 4.1. *The map*

$$\Psi_u : \mathrm{Aut}_K(V) \times Z(u)^\circ \to \mathrm{Aut}_K(V), \quad (g, w) \mapsto gwg^{-1}$$

is an open map with respect to the $\mathfrak{l}$-adic topology, i.e., the image under Ψ_u of any open subset of $\mathrm{Aut}_K(V) \times Z(u)^\circ$ is open in $\mathrm{Aut}_K(V)$.

Proof. It is enough to prove that the induced map on tangent spaces of the corresponding $\mathfrak{l}$-adic manifolds is surjective; cf. [17, Cor. 4.5]. Since the map on tangent spaces is a homomorphism of vector spaces over K, the property of this map being surjective is invariant under base change. Thus, after possibly extending the base field K, we can assume that u has all its eigenvalues in K, so $Z(u)$ is a split torus. Then, after fixing an appropriate basis of V, we identify $\mathrm{Aut}_K(V)$ with $\mathrm{GL}_r(K)$ and $Z(u)$ with diagonal matrices in $M_r(K)$. We show that for any $(g, t) \in \mathrm{Aut}_K(V) \times Z(u)^\circ$, the derivative

$$d\Psi_u\big|_{(g,t)} : M_r(K) \times Z(u) \to M_r(K)$$

is surjective.

A small calculation shows that $d\Psi_u\big|_{(g,t)}(M, N) = gNg^{-1} + Mtg^{-1} - gtg^{-1}Mg^{-1}$. Substituting $M' = g^{-1}M$, we can write $d\Psi_u\big|_{(g,t)}(M, N) = g(N + [M', t])g^{-1}$. Since we assumed u to be diagonal, t is also a diagonal matrix with *distinct* entries. It would be enough to show that for any $X \in M_r(K)$, we can find M' and N, such that $(N+[M', t]) = g^{-1}Xg =: X'$. Any $X' \in M_r(K)$ can be written as $X' = X_1 + X_2$, where X_1 is a diagonal matrix and X_2 has zeros on the diagonal. We can solve for $M' = (m_{ij})$ such that $[M', t] = (m_{ij}(t_i - t_j)) = X_2$ since $t_i \neq t_j$ for $i \neq j$. Finally, if we take $M = gM'$ and $N = X_1$ then we get $d\Psi_u\big|_{(g,t)}(M, N) = gX'g^{-1} = X$. □

Let Λ be an $A_{\mathfrak{l}}$-lattice in V of maximal rank r. Consider the intersection

$$\mathcal{Z}(u) := Z(u) \bigcap \mathrm{End}_{A_{\mathfrak{l}}}(\Lambda) \subset \mathrm{End}_{A_{\mathfrak{l}}}(\Lambda) \subset \mathrm{End}_K(V).$$

It is clear that $\mathcal{Z}(u)$ coincides with the centralizer of u in $\mathrm{End}_{A_\mathfrak{l}}(\Lambda)$ and is an $A_\mathfrak{l}$-order in $Z(u)$.

Proposition 4.2. *Let G be an open compact subgroup of $\mathrm{Aut}_{A_\mathfrak{l}}(\Lambda)$. The set*

$$U = \{\gamma \in G \mid \mathcal{Z}(\gamma) \cong \mathcal{Z}(u)\}$$

is open in G.

Proof. Since G is an open compact subgroup of $\mathrm{Aut}_K(V)$, the intersection

$$Z(u)^\circ_G := G \bigcap Z(u)^\circ$$

is an open subset in $Z(u)^\circ$. (This subset is non-empty since its closure contains the identity.) Therefore, by Lemma 4.1, $G' := \Psi_u(G \times Z(u)^\circ_G)$ is an open subset of $\mathrm{Aut}_K(V)$. On the other hand, obviously, $G' \subset G$.

Note that for any $g \in G$ and $w \in Z(u)^\circ$, we have

$$Z(gwg^{-1}) = gZ(w)g^{-1} = gZ(u)g^{-1}.$$

Since G is a subgroup of $\mathrm{Aut}_{A_\mathfrak{l}}(\Lambda)$, this implies

$$\mathcal{Z}(gwg^{-1}) = g\mathcal{Z}(w)g^{-1} = g\mathcal{Z}(u)g^{-1}.$$

In particular, $\mathcal{Z}(\gamma) \cong \mathcal{Z}(u)$ for $\gamma = gwg^{-1}$. Since every element in G' is of this form, we conclude that $\mathcal{Z}(\gamma) \cong \mathcal{Z}(u)$ for all $\gamma \in G'$. As G' is open in G, this finishes the proof. □

4.2. Main theorem

Let ϕ be a Drinfeld A-module of rank $r \geq 2$ over F. Let $\mathfrak{p} \in \mathcal{P}(\phi)$ and $\mathcal{E}_\mathfrak{p} := \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\phi \otimes \mathbb{F}_\mathfrak{p})$. Let $\mathfrak{l} \lhd A$ be a prime different from $\mathfrak{p}$. By [21], the Tate module $T_\mathfrak{l}(\phi)$ is unramified at $\mathfrak{p}$, i.e., for any place $\bar{\mathfrak{p}}$ in F^{sep} extending $\mathfrak{p}$, the inertia group of $\bar{\mathfrak{p}}$ acts trivially on $T_\mathfrak{l}(\phi)$. There is a canonical isomorphism $T_\mathfrak{l}(\phi) \cong T_\mathfrak{l}(\phi \otimes \mathbb{F}_\mathfrak{p})$ which is compatible with the action of a Frobenius element $\sigma_\mathfrak{p}$ in the decomposition group of $\bar{\mathfrak{p}}$ on $T_\mathfrak{l}(\phi)$ and the action of $\mathrm{Frob}_\mathfrak{p} \in G_{\mathbb{F}_\mathfrak{p}}$ on $T_\mathfrak{l}(\phi \otimes \mathbb{F}_\mathfrak{p})$; cf. [21, p. 479]. Hence using Proposition 2.6, we get

$$\begin{aligned}
\mathcal{E}_\mathfrak{p} \otimes_A A_\mathfrak{l} &\cong \mathrm{End}_{A_\mathfrak{l}[G_{\mathbb{F}_\mathfrak{p}}]}(T_\mathfrak{l}(\phi \otimes \mathbb{F}_\mathfrak{p})) \\
&\cong \text{Centralizer of } \mathrm{Frob}_\mathfrak{p} \text{ in } \mathrm{End}_{A_\mathfrak{l}}(T_\mathfrak{l}(\phi \otimes \mathbb{F}_\mathfrak{p})) \\
&\cong \text{Centralizer of } \sigma_\mathfrak{p} \text{ in } \mathrm{End}_{A_\mathfrak{l}}(T_\mathfrak{l}(\phi)).
\end{aligned}$$

Now let $C_\mathfrak{l}$ be a fixed commutative semi-simple $F_\mathfrak{l}$-algebra of dimension r and let $R_\mathfrak{l}$ be an $A_\mathfrak{l}$-order in $C_\mathfrak{l}$. Fix an isomorphism of free $A_\mathfrak{l}$-modules $R_\mathfrak{l} \cong T_\mathfrak{l}(\phi)$ and extend it linearly to an isomorphism $R_\mathfrak{l} \otimes_{A_\mathfrak{l}} F_\mathfrak{l} = C_\mathfrak{l} \cong V_\mathfrak{l}(\phi) := T_\mathfrak{l}(\phi) \otimes_{A_\mathfrak{l}} F_\mathfrak{l}$. Let

$$C_\mathfrak{l} \xrightarrow{\iota} \mathrm{End}_{F_\mathfrak{l}}(C_\mathfrak{l}) \cong \mathrm{End}_{F_\mathfrak{l}}(V_\mathfrak{l}(\phi))$$

be the embedding given by multiplication, i.e., $\iota(\alpha)(x) = \alpha x$. We identify $C_\mathfrak{l}$ with its image in $\mathrm{End}_{F_\mathfrak{l}}(V_\mathfrak{l}(\phi))$. Since $C_\mathfrak{l}$ is a maximal torus, it coincides with its own centralizer $Z(C_\mathfrak{l})$ in $\mathrm{End}_{F_\mathfrak{l}}(V_\mathfrak{l}(\phi))$.

Lemma 4.3. *We have:*

(i) $R_\mathfrak{l} = \{u \in C_\mathfrak{l} \mid u(T_\mathfrak{l}(\phi)) \subset T_\mathfrak{l}(\phi)\}$.
(ii) $R_\mathfrak{l} = \{u \in \mathrm{End}_{A_\mathfrak{l}}(T_\mathfrak{l}(\phi)) \mid u \in Z(C_\mathfrak{l})\}$.

Proof. (i) We clearly have the inclusion $R_\mathfrak{l} \subset \{u \in C_\mathfrak{l} \mid u(T_\mathfrak{l}(\phi)) \subset T_\mathfrak{l}(\phi)\}$. For the reverse inclusion, assume $u \in C_\mathfrak{l}$ is such that $u(T_\mathfrak{l}(\phi)) \subset T_\mathfrak{l}(\phi)$. Then $u \cdot 1 = u \in R_\mathfrak{l}$. (ii) This follows from (i) since $Z(C_\mathfrak{l}) = C_\mathfrak{l}$. □

A simple finite-dimensional commutative algebra over $F_\mathfrak{l}$ is just a field extension of $F_\mathfrak{l}$. Thus $C_\mathfrak{l} = \prod_{i=1}^{h} K_i$ where each K_i is a finite algebraic field extension of $F_\mathfrak{l}$. We will assume from now on that each $K_i/F_\mathfrak{l}$ is a *separable* extension. Then we have the Primitive Element Theorem, so can use Lemma 2.3 in [23] to prove that (use A instead of $\mathbb{Z}$ in the proof).

Lemma 4.4. *There exists an invertible element u_0 of $C_\mathfrak{l}$ such that $C_\mathfrak{l} = F_\mathfrak{l}[u_0]$.*

Note that the centralizer $Z(u_0)$ of u_0 in $\mathrm{End}_{F_\mathfrak{l}}(C_\mathfrak{l})$ is $Z(C_\mathfrak{l}) = C_\mathfrak{l}$. Hence by Lemma 4.3 the centralizer $\mathcal{Z}(u_0)$ of u_0 in $\mathrm{End}_{A_\mathfrak{l}}(T_\mathfrak{l}(\phi))$ is $R_\mathfrak{l}$. Let G be an open subgroup of $\mathrm{Aut}_{A_\mathfrak{l}}(T_\mathfrak{l}(\phi))$. By Proposition 4.2, the set

$$U = \{u \in G \mid \mathcal{Z}(u) \cong \mathcal{Z}(u_0)\}$$

is open in G.

We will need the following result of Pink [16]:

Theorem 4.5. *If $\mathrm{End}_{F^{\mathrm{alg}}}(\phi) = A$, then for any finite set S of primes of A the image of the homomorphism*

$$G_F \to \prod_{\mathfrak{l} \in S} \mathrm{Aut}_{A_\mathfrak{l}}(T_\mathfrak{l}(\phi))$$

is open.

Assume $\mathrm{End}_{F^{\mathrm{alg}}}(\phi) = A$. Let $S = \{\mathfrak{l}_1, \dots, \mathfrak{l}_m\}$ be a set of distinct primes. Choose a commutative separable semi-simple $F_\mathfrak{l}$-algebra $C_\mathfrak{l}$ of dimension r for each $\mathfrak{l} \in S$. Choose an $A_\mathfrak{l}$-order $R_\mathfrak{l} \subset C_\mathfrak{l}$ for each $\mathfrak{l} \in S$. Let

$$\rho : G_F \to \prod_{\mathfrak{l}\in S} \mathrm{Aut}_{A_\mathfrak{l}}(T_\mathfrak{l}(\phi))$$

be the Galois representation arising from the action on $T_\mathfrak{l}(\phi)$. Let $\prod_{\mathfrak{l}\in S} G_\mathfrak{l}$ be the image of ρ. By Theorem 4.5, $G_\mathfrak{l}$ is an open subgroup of $\mathrm{Aut}_{A_\mathfrak{l}}(T_\mathfrak{l}(\phi))$. Let $U_\mathfrak{l} \subset G_\mathfrak{l}$ be the open subset provided by Proposition 4.2. Since by Chebotarev's theorem the Frobenius elements are dense in G_F, they are also dense in $\prod_{\mathfrak{l}\in S} U_\mathfrak{l}$. In particular, there are infinitely many $\mathfrak{p}$ such that the conjugacy class of $\sigma_\mathfrak{p}$ lies in $\prod_{\mathfrak{l}\in S} U_\mathfrak{l}$. Even stronger, the set of such primes has positive density by Corollary 2 (b) on page I-8 of [20]. Thus, we have proved the following:

Theorem 4.6. *Assume* $\mathrm{End}_{F^{\mathrm{alg}}}(\phi) = A$. *The set of primes* $\mathfrak{p} \in \mathcal{P}(\phi)$ *such that* $\mathcal{E}_\mathfrak{p} \otimes_A A_\mathfrak{l} \cong R_\mathfrak{l}$ *for all* $\mathfrak{l} \in S$ *has positive density.*

Finally, we are ready to prove Theorem 1.1.

Proof of Theorem 1.1. Part (1) of the theorem was already proved as Corollary 3.2. Moreover, it easy to see from the proof of Corollary 3.2 that to prove part (2) it is enough to show that for a subset of primes $\mathfrak{p} \in \mathcal{P}(\phi)$ of positive density $\sigma_\mathfrak{p}$ acts trivially on $\phi[\mathfrak{n}]$, simultaneously with the condition of Theorem 4.6.

Let $\mathfrak{n} = \mathfrak{q}_1^{s_1} \cdots \mathfrak{q}_d^{s_d}$ be the prime decomposition of a given element $\mathfrak{n} \in A$. Let $S' = \{\mathfrak{q}_1, \dots, \mathfrak{q}_d\}$. Let $\prod_{\mathfrak{l}\in S\cup S'} G_\mathfrak{l}$ be the image of $G_F \to \prod_{\mathfrak{l}\in S\cup S'} \mathrm{Aut}_{A_\mathfrak{l}}(T_\mathfrak{l}(\phi))$ For $\mathfrak{q} \in S'$, let $G'_\mathfrak{q}$ be the intersection of $G_\mathfrak{q}$ with the principal congruence subgroup of $\mathrm{GL}_r(A_\mathfrak{q})$ of level $\mathfrak{q}^s$ consisting of matrices which are congruent to 1 modulo $\mathfrak{q}^s$. Note that $G'_\mathfrak{q}$ is still open in $\mathrm{Aut}_{A_\mathfrak{q}}(T_\mathfrak{q}(\phi))$. For $\mathfrak{l} \in S \setminus S'$, let $G'_\mathfrak{l} = G_\mathfrak{l}$. Now to achieve our goal we can simply apply the argument in the proof of Theorem 4.6 to $\prod_{\mathfrak{l}\in S\cup S'} G'_\mathfrak{l}$. □

5. Algorithms

In this section we describe algorithms for computing some of the invariants of Drinfeld modules over finite fields discussed in Section 2. We have implemented these algorithms in Magma. The examples presented in this section are based on computer calculations.

Throughout this section $\phi : A \to \mathbb{F}_\mathfrak{p}\{\tau\}$ is a Drinfeld module of rank r, $\mathfrak{p} \lhd A$ is a prime of degree d, and $\gamma : A \to \mathbb{F}_\mathfrak{p} = A/\mathfrak{p}$ is the reduction modulo $\mathfrak{p}$.

5.1. Characteristic polynomial of the Frobenius

Let

$$P(X) = X^r + a_1 X^{r-1} + \cdots + a_r$$

be the characteristic polynomial of $\mathrm{Frob}_\mathfrak{p}$ acting on $T_\mathfrak{l}(\phi)$; cf. Proposition 2.6. From Proposition 2.2 we know that $a_1, \dots, a_r \in A$ and $\deg(a_i) \leq i \cdot \frac{d}{r}$. In particular, $a_1, \dots, a_{r-1}$ are uniquely determined by their residues modulo $\mathfrak{p}$. We also know from Proposition 2.3 that $a_r = \varepsilon(\phi)\mathfrak{p}$. Now since $P(X)$ is also the minimal polynomial of $\pi = \tau^d$, we have

$$\tau^{dr} + \phi_{a_1}\tau^{d(r-1)} + \cdots + \phi_{a_{r-1}}\tau^d + \phi_{a_r} = 0.$$

Denote

$$f_i = \phi_{a_i}\tau^{d(r-i)} + \phi_{a_{i+1}}\tau^{d(r-i-1)} + \cdots + \phi_{a_r} \in \mathbb{F}_\mathfrak{p}\{\tau\}$$

and

$$f_i^\dagger = \tau^{dr} + \phi_{a_1}\tau^{d(r-1)} + \cdots + \phi_{a_{i-1}}\tau^{d(r-i+1)}.$$

Note that $\deg_\tau \phi_{a_j}\tau^{d(r-j)} \geq d(r-j)$, so the coefficient of $\tau^{d(r-i+1)}$ in $f_i^\dagger$ is the constant term of $\phi_{a_{i-1}}$, i.e., $\gamma(a_{i-1})$. Therefore,

$$\gamma(a_{i-1}) = -\text{Coefficient of } \tau^{d(r-i+1)} \text{ in } f_i.$$

Since we know f_r explicitly, we can compute all a_i recursively, where we use $a_r, a_{r-1}, \dots, a_{r-i}$ to calculate a_{r-i-1}.

Computing ϕ_a takes approximately $r\deg(a)^2$ operations (computing ϕ_{T^n} recursively via $\phi_T\phi_{T^{n-1}}$ takes $\approx nr$ operations, so computing ϕ_a takes $r(\deg(a) + (\deg(a)-1) + \cdots + 1 \approx r\deg(a)^2$ operations). We conclude that the amount of work involved in the calculation of $P(X)$ is $O(r^2d^2)$, so this is a “polynomial time” algorithm; cf. [18].

Example 5.1. Let $q = 3$, $\mathfrak{p} = T^7 - T^2 + 1$, and $\phi_T = T + (T^2+1)\tau + T\tau^2 + \tau^3$. Then

$$P(X) = X^3 + (-T+1)X^2 + (T^3+T-1)X - \mathfrak{p}.$$

Remark 5.2. For rank $r = 2$ there is a different recursive procedure for computing $P(X)$ based on the properties of Eisenstein series; see [12, Prop. 3.7]. In practice, Gekeler's algorithm seems to have the same efficiency as what was presented above (the amount of computer time it took to execute both in `Magma` were almost identical in our tests).

5.2. Exponent of ${}^\phi\mathbb{F}_\mathfrak{p}$

Let

$${}^\phi\mathbb{F}_\mathfrak{p} \cong A/\mathfrak{d}_1 \times \cdots \times A/\mathfrak{d}_r,$$

be the isomorphism of (2.1). We call $\mathfrak{d}_r$ the *exponent* of ${}^\phi\mathbb{F}_\mathfrak{p}$, since the fact that $\mathfrak{d}_1 \mid \cdots \mid \mathfrak{d}_r$ implies that $\mathfrak{d}_r$ is the smallest degree element of A such that $\phi_{\mathfrak{d}_r}$ annihilates $\mathbb{F}_\mathfrak{p}$. The exponent was studied in prior papers by Cojocaru and Shulman [5], [6].

Denote $\theta = \gamma(T)$. Then $\mathbb{F}_\mathfrak{p} = A/\mathfrak{p}$ is an $\mathbb{F}_q$-vector space with basis $1, \theta, \theta^2, \dots, \theta^{d-1}$. Put

$$\mathfrak{d} = x_0 + x_1 T + \cdots + x_{d-1}T^{d-1} + T^d$$

for a hypothetical annihilator of ${}^\phi\mathbb{F}_\mathfrak{p}$, i.e., $\phi_\mathfrak{d}$ acts as zero on $\mathbb{F}_\mathfrak{p}$. Let $k \in \{0, \dots, d-1\}$. Compute

$$\phi_{T^i}(\theta^k) = \alpha_{i,1} + \alpha_{i,2}\theta + \cdots + \alpha_{i,d}\theta^{d-1}$$

for $i = 1, 2, \dots, d$, which can be easily done by repeated application of ϕ_T. Let M_k be the $d \times d$ matrix whose first row consists of zeros except at position $k+1$ where it is 1, and the $(i+1)$-th row is $[\alpha_{i,1}, \alpha_{i,2}, \dots, \alpha_{i,d}]$ for $1 \leq i \leq d-1$. Let $N_k = -[\alpha_{d,1}, \dots, \alpha_{d,d}]^t$. Then $\phi_\mathfrak{d}$ acting as 0 on $A/\mathfrak{p}$ is equivalent to $\phi_\mathfrak{d}(\theta^k) = 0$ for all $k = 0, \dots, d-1$, which itself is equivalent to

$$[x_0, \dots, x_{d-1}]M_k = N_k \quad \text{for all} \quad k = 0, \dots, d-1.$$

This system of linear equations always has a solution (since ${}^\phi\mathbb{F}_\mathfrak{p}$ has exponent). Find a particular solution $\mathbf{x}$ and find a basis $\mathbf{b}_1, \dots, \mathbf{b}_h$ for the intersection of null-spaces of all M_k, so that every other solution is of the form $\mathbf{x} + \mathrm{span}(\mathbf{b}_1, \dots, \mathbf{b}_h)$. It is easy to see that the exponent of ${}^\phi\mathbb{F}_\mathfrak{p}$ is the gcd of $f_\mathbf{x}, f_{\mathbf{x}+\mathbf{b}_1}, \dots, f_{\mathbf{x}+\mathbf{b}_h}$, where $f_\mathbf{y} := y_0 + \cdots + y_{d-1}T^{d-1} + T^d$ for $\mathbf{y} = (y_0, \dots, y_{d-1})$. This can be easily computed. Computing all $\phi_{T^i}(\theta^k)$ can be done in polynomial time in d, solving the system of linear equations also can be done in polynomial time in d. Hence we can find the exponent $\mathfrak{d}_r$ of ${}^\phi\mathbb{F}_\mathfrak{p}$ in polynomial time in d.

Example 5.3. Suppose we want to compute all $\mathfrak{d}_1, \dots, \mathfrak{d}_r$. The previous algorithm allows us to computed $\mathfrak{d}_r$. Since $\mathfrak{d}_1 \mid \mathfrak{d}_2 \mid \cdots \mid \mathfrak{d}_r$, this already gives us only finitely many possibilities for these invariants. To further restrict the possibilities, one can compute $P(x)$, which then allows to compute the product $\mathfrak{d}_1 \cdot \mathfrak{d}_2 \cdots \mathfrak{d}_r = P(1)A = \chi(\phi)$, thanks to Proposition 2.5. One can also uniquely determine $\mathfrak{d}_1$ using Lemma 2.4. In practice, knowing $\mathfrak{d}_1, \mathfrak{d}_r$, and the product $\prod_{i=1}^r \mathfrak{d}_r$ is usually sufficient to uniquely determine all $\mathfrak{d}_i$'s. (Obviously, this is always the case when $r \leq 3$.) When this is not sufficient, one can determine these invariants by computing the dimension of the null space of possible $\phi_{\mathfrak{d}_i}$ by an argument used in the algorithm for computing $\mathfrak{d}_r$.

In this example we take $q = 3$ and compute $\mathfrak{d}_1, \mathfrak{d}_2, \mathfrak{d}_3$ for the Drinfeld A-module

$$\phi_T = \theta + \theta\tau + \tau^3$$

over $\mathbb{F}_\mathfrak{p}$ for varying primes $\mathfrak{p}$, which are chosen specifically to demonstrate different possible situations.

Please cite this article in press as: S. Garai, M. Papikian, Endomorphism rings of reductions of Drinfeld modules, J. Number Theory (2019), https://doi.org/10.1016/j.jnt.2019.02.008

First, let $\mathfrak{p} = T^7 + T^5 + T - 1$. Then the exponent is $\mathfrak{d}_3 = T^3(T+1)(T-1)$. We also have $P(X) = X^3 - X^2 - (T^3 - T + 1)X - \mathfrak{p}$. Hence $\chi(\phi) = T^3(T+1)^2(T-1)^2$. This implies $\mathfrak{d}_2 = (T+1)(T-1)$ and $\mathfrak{d}_1 = 1$.

Next, let $\mathfrak{p} = T^8 + T^7 + T^6 + T^4 - T^3 - T^2 - 1$. Then $\mathfrak{d}_3 = (T+1)^2(T-1)^3$ and $\chi(\phi) = (T+1)^3(T-1)^5$. Hence either

$$\mathfrak{d}_2 = (T+1)(T-1)^2, \quad \mathfrak{d}_1 = 1,$$

or

$$\mathfrak{d}_2 = (T+1)(T-1), \quad \mathfrak{d}_1 = (T-1).$$

If $\mathfrak{d}_1$ is not 1, then, by Lemma 2.4, $\phi_{T-1}(x) = (T-1)x + Tx^3 + x^{27}$ splits completely modulo $\mathfrak{p}$. This is easy to check on a computer to be false, hence $\mathfrak{d}_2 = (T+1)(T-1)^2$ and $\mathfrak{d}_1 = 1$.

Finally, let $\mathfrak{p} = T^{14} + T^{13} + T^{12} + T^5 - T^2 + T + 1$. Then

$$\mathfrak{d}_3 = T(T+1)(T-1)(T^2+1)^2(T^4 - T - 1).$$

and

$$\chi(\phi) = T^3(T+1)^2(T-1)(T^2+1)^2(T^4 - T - 1).$$

One checks that $\phi[T]$ is rational over $\mathbb{F}_\mathfrak{p}$. Hence we must have

$$\mathfrak{d}_1 = T, \qquad \mathfrak{d}_2 = T(T+1).$$

5.3. Endomorphism ring

Now assume $r = 2$. Let

$$P(X) = X^2 - aX + \varepsilon(\phi)\mathfrak{p},$$

be the characteristic polynomial of the Frobenius, so a is the trace of $\rho_{\phi,\mathfrak{l}}(\mathrm{Frob}_\mathfrak{p})$. Let π be a root of $P(X)$. Then $K = F(\pi)$ is an imaginary quadratic extension of F. Let $\mathcal{O}_K$ be the integral closure of A in K. Denote $\mathcal{E}_\phi := \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\phi)$. By Proposition 2.1, we have the inclusion of orders,

$$A[\pi] \subset \mathcal{E}_\phi \subset \mathcal{O}_K.$$

Let c_π (resp. c_ϕ) be the index of $A[\pi]$ (resp. $\mathcal{E}_\phi$) in $\mathcal{O}_K$. These are monic polynomials in A such that c_ϕ divides c_π; note that $b = c_\pi/c_\phi$ is the (refined) index of $A[\pi]$ in $\mathcal{E}_\phi$ that appears in Theorem 1.2. Orders in quadratic extensions are uniquely determined by their indices:

$$A[\pi] = A + c_\pi \mathcal{O}_K, \qquad \mathcal{E}_\phi = A + c_\phi \mathcal{O}_K,$$

so to determine $\mathcal{E}_\phi$ it is enough to determine c_ϕ.

We have $\mathcal{O}_K = A[\alpha]$ for some α satisfying a monic quadratic polynomial $f(X) \in A[X]$. Note that $A[c_\pi \alpha] = A[\pi]$, so $c_\pi \alpha = m + n\pi$, where $m \in A$ and $n \in \mathbb{F}_q^\times$. Suppose we are able to do the following:

(i) Compute $f(X)$.
(ii) Compute c_π.
(iii) Compute m, n such that $c_\pi \alpha = m + n\pi$.

Then c_ϕ can be computed using the following process: Initially, put $c_1 = c_\pi$. Let $c \neq 1$ run through monic divisors of c_1. For a given c we look for $x \in \mathbb{F}_\mathfrak{p}\{\tau\}$ such that

$$x\phi_c = \phi_m + n\tau^d. \tag{5.1}$$

If we write $x = x_0 + x_1\tau + \cdots + x_s\tau^s$, where $s = \deg_\tau(n\tau^d + \phi_m) - 2\deg(c)$, then (5.1) gives a system of *linear* equations in $x_0, \dots, x_m$, so can be easily solved. Of course, this system of linear equations might not have any solutions, but when it does, the solution x is unique. For such a solution we check whether $x\phi_T = \phi_T x$. If this condition holds (so $x \in \mathcal{E}_\phi$) then we replace c_1 by c_1/c and repeat the process. Eventually, we will either end up with $c_1 = 1$ or will not find any x satisfying the necessary conditions. In that case, the process terminates and the index of $\mathcal{E}_\phi$ is $c_\phi = c_1$. Note that this process also computes a generator of $\mathcal{E}_\phi$ over A. Indeed, it is easy to see that $\mathcal{E}_\phi = A[x]$, where x is the solution of $x\phi_{c_\pi/c_\phi} = n\tau^d + \phi_m$.

Now we address the question of how to carry out (i)-(iii). There are three cases, which need to be treated separately:

$\boxed{\text{Case 1: } q \text{ is odd.}}$ Let $\Delta_\pi := a^2 - 4\varepsilon(\phi)\mathfrak{p}$. Note that $\Delta_\pi \in A$ has degree $\leq d$. We can decompose any polynomial $h(T) \in A$ as $h(T) = c^2 e$, where c is monic and e is square-free. Decompose Δ_π in this manner

$$\Delta_\pi := c^2 \cdot \Delta_{\max}.$$

Then $f(X) = X^2 - \Delta_{\max}$ and $c_\pi = c$; this gives (i) and (ii). If we fix a root α of $f(X)$, then (iii) follows from the quadratic formula: $2\pi = a + c_\pi \alpha$.

$\boxed{\text{Case 2: } q \text{ is even and } a = 0.}$ This is equivalent to K/F being inseparable. Let $g := \varepsilon(\phi)\mathfrak{p}$. Then K is defined by the equation $X^2 = g$. The polynomial g decomposes (uniquely) as $g = g_e + g_o$, where g_e (resp. g_o) is a polynomial in T whose terms all have even degrees (resp. odd degrees). Then $g_e = s^2$ and $g_o = Tc^2$ for uniquely determined $s, c \in A$. After a change of variables $X \mapsto X + s$, we see that $A[\sqrt{g}] = A[c\sqrt{T}]$. Hence $\mathcal{O}_K = A[\sqrt{T}]$, $f(X) = X^2 + T$, $c_\pi = c$, and $\pi + s = c_\pi \sqrt{T}$.

$\boxed{\text{Case 3: } q \text{ is even and } a \neq 0.}$ This is the most complicated case; it is equivalent to K/F being separable in characteristic 2. By [19, III.6, Cor. 1], we have an equality of ideals

$$(P'(\pi)) = (a) = (\mathcal{D}_K \cdot c_\pi),$$

where $\mathcal{D}_K$ is the different of $\mathcal{O}_K$ over A. Thus, to compute c_π we need to compute $\mathcal{D}_K$. To do this, we first recall some facts about Artin-Schreier extensions.

Any quadratic separable extension K/F is the splitting field of a polynomial

$$X^2 + X = \mathfrak{n}/\mathfrak{m}$$

for some $\mathfrak{n}, \mathfrak{m} \in A$ coprime to each other. Suppose $\mathfrak{m} = \mathfrak{q}^{2e}\mathfrak{m}_1$, where $e \geq 1$, $\mathfrak{q}$ is a prime, and $\mathfrak{q} \nmid \mathfrak{m}_1$. After a change of variables, $X \mapsto X + b/\mathfrak{p}^e$, $b \in A$, we get

$$X^2 + X = \frac{\mathfrak{n} + b^2\mathfrak{m}_1 + \mathfrak{q}^e\mathfrak{m}_1 b}{\mathfrak{m}}.$$

Since $\mathfrak{n}$ and $\mathfrak{m}_1$ are coprime to $\mathfrak{q}$, and squaring is an automorphism of $A/\mathfrak{q}$, we can choose b such that $\mathfrak{n} + b^2\mathfrak{m}_1 + \mathfrak{q}^e\mathfrak{m}_1 b$ is divisible by $\mathfrak{q}$. Repeating this process finitely many times, we can assume that

$$\mathfrak{m} = \mathfrak{q}_1^{2e_1-1} \cdots \mathfrak{q}_s^{2e_s-1}, \quad e_1, \dots, e_s \geq 1.$$

Then, by [1, Cor. 2.3],

$$\mathcal{D}_K = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_s^{e_s}.$$

After a change of variables $X \mapsto X/\epsilon\mathcal{D}_K$, we can rewrite $X^2 + X = \mathfrak{n}/\mathfrak{m} = \mathfrak{q}_1 \cdots \mathfrak{q}_s\mathfrak{n}/\mathcal{D}_K^2$ as

$$X^2 + \epsilon\mathcal{D}_K X = \epsilon^2\mathfrak{q}_1 \cdots \mathfrak{q}_s\mathfrak{n},$$

where $\epsilon \in \mathbb{F}_q^\times$ is arbitrary.

Lemma 5.4. *Let α be a root of $f(X) = X^2 + \epsilon\mathcal{D}_K X + \epsilon^2\mathfrak{q}_1 \cdots \mathfrak{q}_s\mathfrak{n}$. Then $\mathcal{O}_K = A[\alpha]$.*

Proof. It is clear from the construction that $K = F(\alpha)$. Since $f(X) \in A[X]$ is monic, we have $A[\alpha] \subset \mathcal{O}_K$. On the other hand, $f'(X) = \epsilon\mathcal{D}_K$, so $A[\alpha] = \mathcal{O}_K$ by [19, III.6, Cor. 2]. □

To compute the different of the extension defined by the characteristic polynomial of the Frobenius $X^2 + aX = \varepsilon(\phi)\mathfrak{p}$, we first make a change of variables $X \mapsto aX$, then divide both sides by a^2, obtaining $X^2 + X = \varepsilon(\phi)\mathfrak{p}/a^2$. Then we apply the process of the previous paragraph. Let ϵ be the leading coefficient of a as a polynomial in T.

We have computed the minimal polynomial $f(X) = X^2 + \epsilon\mathcal{D}_K X + b$ of an element α generating $\mathcal{O}_K$. Then $c_\pi\alpha$ is a root of $X^2 + aX + c_\pi^2 b = 0$. This implies that $c_\pi\alpha = m + \pi$, where $m \in A$ is such that

$$m^2 + am = c_\pi^2 b + \varepsilon(\phi)\mathfrak{p}.$$

If we write $m = m_0 + m_1 T + \cdots$ as a polynomial in T whose coefficients m_i are unknowns, then the previous equality reduces to solving a system of quadratic equations over $\mathbb{F}_q$, which can be done recursively starting with the constant term m_0. In fact, the first non-zero coefficient m_h of m is determined from a quadratic equation over $\mathbb{F}_q$, while every other m_i, $i \geq h$, can be deduced from a linear equation in m_i with coefficients involving $m_h, \dots, m_{i-1}$.

Example 5.5. Let $q = 3$ and ϕ be a Drinfeld A-module of rank 2 over F given by

$$\phi_T = T + g_1\tau + g_2\tau^2.$$

Tables 1 and 2 list the invariants of $\phi \otimes \mathbb{F}_\mathfrak{p}$ for primes $\mathfrak{p}$ of degree 6 in cases when $A[\pi_\mathfrak{p}] \neq \mathcal{E}_\pi$. The total number of primes of degree 6 in $\mathbb{F}_3[T]$ is 116, while the number of primes in Table 1 (resp. Table 2) is 24 (resp. 20).

Example 5.6. $\mathbb{F}_4$ is generated over $\mathbb{F}_2$ by w satisfying $w^2 + w + 1 = 0$. Table 3 lists computational data for

$$\phi_T = T + T\tau + \tau^2,$$

which involves Cases 2 and 3 of the algorithm computing $\mathcal{E}_\phi$.

Example 5.7. Let $q = 3$ and $\phi_T = T + \tau + T\tau^2$. We know from Theorem 1.1 that for any fixed prime $\mathfrak{q}$ there exist infinitely many $\mathfrak{p}$ such that $c_{\phi\otimes\mathbb{F}_\mathfrak{p}} = \chi(\mathcal{O}_{\mathfrak{p},K}/\mathcal{E}_{\phi\otimes\mathbb{F}_\mathfrak{p}})$ is divisible by $\mathfrak{q}$. We compute that:

If $\mathfrak{q} = T^2 - T - 1$, then the smallest degree $\mathfrak{p}$ is $T^6 + T^5 + T^3 - 1$.
If $\mathfrak{q} = T^3 - T + 1$, then the smallest degree $\mathfrak{p}$ is $T^6 + T^4 + T^3 + T^2 - T - 1$.
If $\mathfrak{q} = T^4 - T^3 - 1$, then the smallest degree $\mathfrak{p}$ is $T^{10} + T^9 - T^7 + T^5 - T + 1$.

By the same corollary, we can also fix two primes $\mathfrak{q}_1$ and $\mathfrak{q}_2$ and find infinitely many $\mathfrak{p}$ such that $\mathfrak{q}_1$ divides $c_{\pi_\mathfrak{p}}/c_{\phi\otimes\mathbb{F}_\mathfrak{p}} = \chi(\mathcal{E}_{\phi\otimes\mathbb{F}_\mathfrak{p}}/A[\pi_\mathfrak{p}])$ and $\mathfrak{q}_2$ divides $c_{\phi\otimes\mathbb{F}_\mathfrak{p}} = \chi(\mathcal{O}_{\mathfrak{p},K}/\mathcal{E}_{\phi\otimes\mathbb{F}_\mathfrak{p}})$. If $\mathfrak{q}_1 = T$ and $\mathfrak{q}_2 = T^2 - T - 1$, then such a prime of smallest degree is $\mathfrak{p} = T^7 - T^5 - T^4 - 1$. On the other hand, if $\mathfrak{q}_1 = T^2 - T - 1$ and $\mathfrak{q}_2 = T$, then the smallest degree $\mathfrak{p}$ is $T^9 + T^5 + T^4 + T^2 - T + 1$.

Please cite this article in press as: S. Garai, M. Papikian, Endomorphism rings of reductions of Drinfeld modules, J. Number Theory (2019), https://doi.org/10.1016/j.jnt.2019.02.008

Table 1
$q = 3,\ g_1 = T,\ g_2 = 1.$

$\mathfrak{p}$	a	$\varepsilon(\phi)$	c_π	c_ϕ	$\Delta_{\max}$
$T^6+2T^5+2T^3+T^2+2T+2$	$2T^3+T^2+2$	1	$T+2$	1	$2T^3+2T^2+2T+2$
$T^6+T^5+T^4+1$	$2T^3+2T^2+2T+2$	1	$T+2$	1	T^3+T^2+2T
$T^6+2T^5+2T^4+2T^3+2T^2+2T+2$	$2T^3$	1	T^2+2	$T+1$	$T+1$
$T^6+T^5+2T^4+2T^2+2T+2$	$2T^3+T+2$	1	T^2+2	$T+2$	$2T+2$
$T^6+T^5+T^4+T^3+T+2$	$2T^3+2T^2+1$	1	$T+2$	1	T^3+2T^2+2
$T^6+T^5+T^4+2T^2+2$	$2T^3+T+2$	1	$T+2$	1	$2T^3+T^2+2T+2$
$T^6+T^5+T^3+T^2+T+2$	$2T^3+T+2$	1	$T+1$	1	$2T^3+2T+2$
$T^6+T^5+T^4+T^3+2T^2+2T+2$	$2T^3$	1	T^2+T+1	$T+2$	$2T+1$
$T^6+2T^4+T^2+T+2$	$2T^3+T^2+2$	1	$T+2$	1	T^3+T^2+2
$T^6+T^5+2T^4+2T^3+2T^2+2$	$2T^3+2T+1$	1	$T+2$	1	$2T^3+T^2+2T+2$
$T^6+T^4+T^3+2T+2$	$2T^3+T^2+T+1$	1	$T+2$	1	T^3+T+2
$T^6+2T^4+2T^3+T+1$	$2T^3+T^2+T+1$	1	T^2+2	$T+1$	T
$T^6+2T^4+T^3+T^2+2$	$2T^3+T^2+2T$	1	$T+2$	1	T^3+2T+1
$T^6+T^3+T^2+1$	$2T^3+2T+1$	1	$T+2$	1	$2T^2+T$
T^6+2T^3+2T+2	$2T^3+T^2+2$	1	$T+2$	1	T^3+2T+2
$T^6+T^3+2T^2+2T+1$	$2T^3+T^2+T+1$	1	T^2+2T	$T+2$	$T+1$
$T^6+T^5+2T^4+T^3+T^2+2$	$2T^3+2T+2$	1	$T+1$	1	$2T^3+2T^2+T+2$
$T^6+T^5+2T^3+1$	$2T^3+1$	1	T	1	$2T^3+2T$
$T^6+2T^3+2T^2+T+1$	$2T^3+T^2+2$	1	$T+2$	1	T^3+2T
$T^6+2T^5+T^4+2T+1$	$2T^3+T^2+2T$	1	$T+2$	1	$2T^3+2T+2$
T^6+T^2+2T+1	$2T^3+2T+2$	1	T	1	$2T^2+2T$
T^6+2T^5+2T+2	$2T^3$	1	$T+2$	1	T^3+2T^2+1
$T^6+2T^5+T^2+2T+1$	$2T^3+T^2+2$	1	$T+2$	1	$2T^3+2T^2+T$
$T^6+2T^5+2T^4+T^3+1$	$2T^3+T^2+2$	1	T^2+T	T	$2T+1$

Please cite this article in press as: S. Garai, M. Papikian, Endomorphism rings of reductions of Drinfeld modules, J. Number Theory (2019), https://doi.org/10.1016/j.jnt.2019.02.008

Table 2
$q = 3,\ g_1 = 1,\ g_2 = T$.

$\mathfrak{p}$	a	$\varepsilon(\phi)$	c_π	c_ϕ	$\Delta_{\max}$
$T^6 + 2T^5 + 2T^4 + T^3 + T^2 + T + 2$	$2T^3 + T + 1$	2	$T^3 + 2T^2 + T$	$T^2 + 2T + 1$	2
$T^6 + 2T^5 + 2T^4 + T^2 + T + 1$	$T^3 + T + 1$	1	$T^2 + 1$	1	T
$T^6 + T^5 + 2$	$2T^3 + 2T^2 + 2$	2	T	1	$2T^4 + T^2 + 2T + 2$
$T^6 + 2T^5 + 2$	$T^3 + 2T^2 + 2$	2	T	1	$2T^4 + T^2 + T + 2$
$T^6 + 2T^5 + T^4 + T^2 + T + 2$	$T^3 + T$	2	$T + 2$	1	$2T^4 + T^2 + 2T + 2$
$T^6 + 2T^5 + 2T^4 + 2T^3 + 2T + 2$	$T^3 + 2T^2 + 1$	2	$T + 1$	1	$2T^4 + 2T^3 + 2T$
$T^6 + 2T^4 + 1$	$T^2 + 1$	1	$T^3 + 2T$	$T^2 + 2$	2
$T^6 + T^5 + 2T^4 + T^2 + 2T + 1$	$2T^3 + 2T + 1$	1	$T^2 + 1$	1	$2T$
$T^6 + 2T^4 + T^2 + T + 2$	$T^3 + T^2 + 2T + 2$	2	T	1	$2T^4 + 2T^3 + T^2 + 2T$
$T^6 + T^5 + T^4 + T^2 + 2T + 2$	$2T^3 + 2T$	2	$T + 1$	1	$2T^4 + T^2 + T + 2$
$T^6 + T^5 + 2T^4 + T^3 + T + 2$	$2T^3 + 2T^2 + 1$	2	$T + 2$	1	$2T^4 + T^3 + T$
$T^6 + T^3 + T^2 + 2T + 2$	$T^3 + 2T^2 + 2T + 1$	2	T	1	$2T^4 + T^3 + 2T^2 + 2T$
$T^6 + 2T^2 + 1$	$T^2 + 2$	1	$T^3 + T$	T	2
$T^6 + T^3 + 2T^2 + 2T + 1$	$T^3 + 2T^2$	1	$T + 1$	1	$T^3 + 2T^2 + 2$
$T^6 + 2T^4 + 2T^3 + T^2 + 2T + 2$	$2T^3 + 2T^2 + 2T$	2	$T^2 + 2T + 1$	$T + 1$	$2T^2 + 2$
$T^6 + T^5 + 2T^4 + 2T^3 + T^2 + 2T + 2$	$T^3 + 2T + 1$	2	$T^3 + T^2 + T$	$T^2 + T + 1$	2
$T^6 + 2T^3 + T^2 + T + 2$	$2T^3 + 2T^2 + T + 1$	2	T	1	$2T^4 + 2T^3 + 2T^2 + T$
$T^6 + 2T^3 + 2T^2 + T + 1$	$2T^3 + 2T^2$	1	$T + 2$	1	$2T^3 + 2T^2 + 2$
$T^6 + 2T^4 + T^2 + 2T + 2$	$2T^3 + T^2 + T + 2$	2	T	1	$2T^4 + T^3 + T^2 + T$
$T^6 + 2T^4 + T^3 + T^2 + T + 2$	$T^3 + 2T^2 + T$	2	$T^2 + T + 1$	$T + 2$	$2T^2 + 2$

Table 3
$q = 4,\ g_1 = T,\ g_2 = 1$.

$\mathfrak{p}$	a	$\varepsilon(\phi)$	c_π	c_ϕ	$\mathcal{D}_K$
$T^5 + wT^2 + w^2T + w$	$T + w$	1	$T + w$	1	1
$T^5 + wT^4 + w^2T^3 + w^2T^2 + wT + w^2$	$wT^2 + T$	1	T	1	$T + w^2$
$T^6 + T^5 + w^2T^4 + w^2T^3 + T^2 + w^2T + w^2$	$w^2T^2 + T + w$	1	$T^2 + wT + w^2$	$T + w^2$	1
$T^7 + T^6 + T^5 + wT^4 + wT + w$	$T^3 + wT^2 + wT + w^2$	1	$T + w^2$	1	$T^2 + T + 1$
$T^7 + T^5 + w^2T^4 + w^2T^2 + 1$	0	1	$T^3 + T^2$	T^2	$\sqrt{T}$
$T^7 + w^2T^5 + T^4 + T^3 + wT^2 + w^2T + w$	$wT^2 + w$	1	$T^2 + 1$	$T + 1$	1
$T^8 + T^6 + wT^5 + w^2T^4 + wT^2 + T + w^2$	0	1	$T^2 + w$	$T + w + 1$	$\sqrt{T}$
$T^9 + T^8 + wT^5 + w^2T^4 + wT^3 + w$	$T^4 + T^3 + T^2 + 1$	1	$T + 1$	1	$T^3 + T + 1$
$T^{11} + wT^{10} + w^2T^9 + wT^8 + w^2T^7 + wT^4 + wT^3 + wT^2 + T + w^2$	$wT^5 + wT^4 + T^2 + 1$	1	$T + 1$	1	$T^4 + w^2T + w^2$

References

[1] N. Anbar, H. Stichtenoth, S. Tutdere, On ramification in the compositum of function fields, Bull. Braz. Math. Soc. (N.S.) 40 (4) (2009) 539–552.

[2] B. Anglès, On some subrings of Ore polynomials connected with finite Drinfeld modules, J. Algebra 181 (2) (1996) 507–522.

[3] T. Centeleghe, Integral Tate modules and splitting of primes in torsion fields of elliptic curves, Int. J. Number Theory 12 (1) (2016) 237–248.

[4] A. Cojocaru, M. Papikian, Drinfeld modules, Frobenius endomorphisms, and CM-liftings, Int. Math. Res. Not. IMRN (17) (2015) 7787–7825.

[5] A. Cojocaru, A. Shulman, An average Chebotarev density theorem for generic rank 2 Drinfeld modules with complex multiplication, J. Number Theory 133 (3) (2013) 897–914.

[6] A. Cojocaru, A. Shulman, The distribution of the first elementary divisor of the reductions of a generic Drinfeld module of arbitrary rank, Canad. J. Math. 67 (6) (2015) 1326–1357.

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

[8] V. Drinfeld, Elliptic modules. II, Mat. Sb. (N.S.) 102 (1977) 182–194.

[9] W. Duke, Á. Tóth, The splitting of primes in division fields of elliptic curves, Exp. Math. 11 (4) (2002) 555–565, (2003).

[10] E.-U. Gekeler, Sur les classes d'idéaux des ordres de certains corps gauches, C. R. Acad. Sci. Paris, Sér. I Math. 309 (1989) 577–580.

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

[12] E.-U. Gekeler, Frobenius distributions of Drinfeld modules over finite fields, Trans. Amer. Math. Soc. 360 (4) (2008) 1695–1721.

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

[14] W. Kuo, Y.-R. Liu, Cyclicity of finite Drinfeld modules, J. Lond. Math. Soc. (2) 80 (3) (2009) 567–584.

[15] G. Laumon, Cohomology of Drinfeld Modular Varieties. Part I, Cambridge Studies in Advanced Mathematics, vol. 41, Cambridge University Press, Cambridge, 1996.

[16] R. Pink, The Mumford-Tate conjecture for Drinfeld-modules, Publ. Res. Inst. Math. Sci. 33 (3) (1997) 393–425.

[17] P. Schneider, p-Adic Lie Groups, Grundlehren der Mathematischen Wissenschaften (Fundamental Principles of Mathematical Sciences), vol. 344, Springer, Heidelberg, 2011.

[18] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, Math. Comp. 44 (170) (1985) 483–494.

[19] J.-P. Serre, Local Fields, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979.

[20] J.-P. Serre, Abelian l-Adic Representations and Elliptic Curves, Research Notes in Mathematics, vol. 7, A K Peters, Ltd., Wellesley, MA, 1998, With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

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

[22] J.-K. Yu, Isogenies of Drinfeld modules over finite fields, J. Number Theory 54 (1) (1995) 161–171.

[23] Yu. Zarhin, Endomorphism rings of reductions of elliptic curves and Abelian varieties, Algebra i Analiz 29 (1) (2017) 110–144.

Please cite this article in press as: S. Garai, M. Papikian, Endomorphism rings of reductions of Drinfeld modules, J. Number Theory (2019), https://doi.org/10.1016/j.jnt.2019.02.008