Journal of Algebra 644 (2024) 381–410

Contents lists available at ScienceDirect

Journal of Algebra

journal homepage: www.elsevier.com/locate/jalgebra

Research Paper

Isomorphism classes of Drinfeld modules over finite fields

Valentijn Karemaker [a,*], Jeffrey Katen [b], Mihran Papikian [b]

[a] *Mathematical Institute, Utrecht University, Utrecht, the Netherlands*
[b] *Department of Mathematics, Pennsylvania State University, University Park, PA, United States of America*

ARTICLE INFO

Article history:
Received 23 January 2023
Available online 22 January 2024
Communicated by Eamonn O'Brien

MSC:
11G09
11R58

Keywords:
Drinfeld modules
Endomorphism rings
Isogeny classes
Gorenstein rings
Algorithms for Drinfeld modules

ABSTRACT

We study isogeny classes of Drinfeld A-modules over finite fields k with commutative endomorphism algebra D, in order to describe the isomorphism classes in a fixed isogeny class. We study when the minimal order $A[\pi]$ of D generated by the Frobenius π occurs as an endomorphism ring by proving when it is locally maximal at π, and show that this happens if and only if the isogeny class is ordinary or k is the prime field. We then describe how the monoid of fractional ideals of the endomorphism ring $\mathcal{E}$ of a Drinfeld module ϕ up to D-linear equivalence acts on the isomorphism classes in the isogeny class of ϕ, in the spirit of Hayes. We show that the action is free when restricted to kernel ideals, of which we give three equivalent definitions, and determine when the action is transitive. In particular, the action is free and transitive on the isomorphism classes in an isogeny class which is either ordinary or defined over the prime field, yielding a complete and explicit description in these cases, which can be implemented as a computer algorithm.

* Corresponding author.
E-mail addresses: V.Z.Karemaker@uu.nl (V. Karemaker), jmk1097@psu.edu (J. Katen), papikian@psu.edu (M. Papikian).

https://doi.org/10.1016/j.jalgebra.2023.12.037

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements. Let F be a function field of transcendence degree 1 over $\mathbb{F}_q$; we assume that $\mathbb{F}_q$ is algebraically closed in F. Fix a place ∞ of F. Let

$$A = \{a \in F \mid \mathrm{ord}_v(a) \geq 0 \text{ for all places } v \neq \infty\}$$

be the ring of elements of F regular outside of ∞. On A, the degree function $\deg\colon A \to \mathbb{Z}$ is defined by $\deg(a) = \log_q \#A/(a)$. We use "prime", "nonzero prime ideal", and "place" of A as synonyms. Given a prime $\mathfrak{p}$ of A, we denote $\mathbb{F}_\mathfrak{p} = A/\mathfrak{p}$. Let $k \cong \mathbb{F}_{q^n}$ be a finite extension of $\mathbb{F}_\mathfrak{p}$. We consider k as an A-field via $\gamma\colon A \to A/\mathfrak{p} \hookrightarrow k$.

Let τ be the Frobenius automorphism of k relative to $\mathbb{F}_q$, that is, the map $\alpha \mapsto \alpha^q$. Let $k\{\tau\}$ be the noncommutative ring of polynomials in τ with coefficients in k and commutation rule $\tau\alpha = \alpha^q\tau$, $\alpha \in k$. A Drinfeld module of rank $r \geq 1$ over k is a ring homomorphism $\phi\colon A \to k\{\tau\}$, $a \mapsto \phi_a$, such that

$$\phi_a = \gamma(a) + g_1(a)\tau + \cdots + g_n(a)\tau^n, \quad n = r \cdot \deg(a).$$

An isogeny $u\colon \phi \to \psi$ between two Drinfeld modules over k is a nonzero element $u \in k\{\tau\}$ such that $u\phi_a = \psi_a u$ for all $a \in A$.

The endomorphism ring $\mathcal{E} := \mathrm{End}_k(\phi)$ of ϕ consists of the zero map and all isogenies $\phi \to \phi$; it is the centralizer of $\phi(A)$ in $k\{\tau\}$. It is known that $\mathcal{E}$ is a projective finitely generated A-module with $r \leq \mathrm{rank}_A\, \mathcal{E} \leq r^2$. We introduce a special element, $\pi = \tau^n$, the so-called Frobenius of k. Note that π lies in the center of $k\{\tau\}$, and hence belongs to $\mathcal{E}$.

Isogenies define an equivalence relation on the set of isomorphism classes of Drinfeld modules over k. The isogeny class of ϕ is determined by the minimal polynomial of π over $F = \phi(F)$, cf. [14, Theorem 3.5]. Since the properties of these polynomials are well understood, it is known how to classify Drinfeld modules over finite fields up to isogeny.

In this article, we investigate the isomorphism classes within a fixed isogeny class. This is an important and difficult question in the theory of Drinfeld modules, which can be approached from different viewpoints, cf. [23,15]. Our approach is inspired by the work of Waterhouse [28] in the case of abelian varieties over finite fields and is partly aimed at producing efficient algorithms for explicitly computing a representative of each isomorphism class. We refer to Section 7 for a more in-depth comparison of our results to known results for abelian varieties.

When $\mathcal{E}$ is commutative, the endomorphism ring of a Drinfeld module isogenous to ϕ is an A-order in $F(\pi)$ containing $A[\pi]$. We start by investigating the natural question of when $A[\pi]$ itself is an endomorphism ring of a Drinfeld module isogenous to ϕ. We prove the following:

Theorem A. *Let ϕ be a Drinfeld module over k such that $\mathrm{End}_k(\phi)$ is commutative. Then $A[\pi]$ is the endomorphism ring of a Drinfeld module isogenous to ϕ if and only if either ϕ is ordinary or $k = \mathbb{F}_{\mathfrak{p}}$.*

Next, we study isogenies from ϕ to other Drinfeld modules using the ideals of $\mathcal{E}$. Let $I \trianglelefteq \mathcal{E}$ be a nonzero ideal. Since $k\{\tau\}$ has a right division algorithm, there exists $u_I \in k\{\tau\}$ such that $k\{\tau\}I = k\{\tau\}u_I$. This element defines an isogeny $u_I \colon \phi \to \psi$, where ψ is the Drinfeld module determined by $\psi_a = u_I \phi_a u_I^{-1}$ for all $a \in A$; we denote $\psi = I * \phi$. The map $I \mapsto I * \phi$ induces a map S from the linear equivalences classes of ideals of $\mathcal{E}$ to the isomorphism classes of Drinfeld modules isogenous to ϕ. Generally, S is neither injective nor surjective.

It was observed by Waterhouse [28] in the setting of abelian varieties that S is injective when restricted to ideals of a special type, called *kernel ideals*. Kernel ideals were introduced in the context of Drinfeld modules by Yu [29]. In Sections 3 and 4, we revisit Yu's definition, give two other equivalent definitions, and prove several general facts about kernel ideals. We also give an explicit example (Example 3.10) of a rank 3 Drinfeld module ϕ and an ideal $I \trianglelefteq \mathrm{End}_k(\phi)$ which is not kernel; as far as we know, this is the first such explicit example in the literature.

In general $\mathrm{End}_k(I * \phi) \supseteq u_I \mathcal{O}_I u_I^{-1} \cong \mathcal{O}_I$, where

$$\mathcal{O}_I := \{g \in F(\pi) \mid Ig \subseteq I\}.$$

(Equality holds when I is a kernel ideal; cf. Lemma 4.2.) Note that $\mathcal{O}_I$ is an overorder of $\mathcal{E}$, so S can be surjective only when $\mathcal{E}$ is the smallest order among the endomorphism rings of Drinfeld modules isogenous to ϕ. When $\mathcal{E}$ is a Gorenstein ring, we prove that any isogeny $\phi \to \psi$ such that $\mathrm{End}_k(\psi) \cong \mathcal{O}_I$ for some (necessarily kernel) ideal $I \trianglelefteq \mathcal{E}$ arises from the map S via $I \mapsto I * \phi = \psi$. In other words, when $\mathcal{E}$ is Gorenstein, the image of S is the set of isomorphism classes in the isogeny class of ϕ whose endomorphism rings are overorders of $\mathcal{E}$. Since $A[\pi]$ is a Gorenstein ring, we arrive at the following:

Theorem B. *Assume that either $k = \mathbb{F}_{\mathfrak{p}}$ or the isogeny class that we consider is ordinary, so that there is a Drinfeld module ϕ with $\mathrm{End}_k(\phi) = A[\pi]$. Then the map $I \mapsto I * \phi$ from the linear equivalences classes of ideals of $A[\pi]$ to the isomorphism classes of Drinfeld modules isogenous to ϕ is a bijection.*

In [24], an algorithm is presented for computing the ideal class monoid of an order in a number field. We have adapted that algorithm to orders in function fields. Since computing $I * \phi$ for a given ideal $I \trianglelefteq \mathcal{E}$ is fairly straightforward, Theorem B combined with this algorithm provides an efficient method for computing explicit representatives of isomorphism classes of all Drinfeld modules isogenous to ϕ such that $\mathrm{End}_k(\phi) \cong A[\pi]$. Section 6 discusses the details of this algorithm and provides an explicit example computed using the algorithm implemented in MAGMA [6], see [19].

Let us mention that Assong [3] has described a brute-force algorithm to list isomorphism classes, based on a theoretical classification in terms of j-invariants and "fine isomorphy invariants", and implemented this for certain examples of isogeny classes of Drinfeld modules of rank 3. Our methods involve fractional ideals in endomorphism rings rather than invariants and explicit expressions for the coefficients of the Drinfeld module.

The outline of the paper is as follows. Section 2 contains our analysis of local maximality of $A[\pi]$ at π, including a key result (Theorem 2.5) for the proof of Theorem A. Section 3 gives the definitions of kernel ideals and proves their equivalence, and Section 4 gives properties of kernel ideals and proves that every ideal is a kernel ideal when $\mathcal{E}$ is Gorenstein (Proposition 4.5). Section 5 contains our main results: we find which endomorphism rings can occur in a fixed isogeny class (Proposition 5.1), study the injectivity and surjectivity of the map $I \mapsto I * \phi$ (Theorem 5.4), and prove when $A[\pi]$ occurs as an endomorphism ring (Corollary 5.3), to obtain Theorem B (cf. Corollary 5.5). Section 6 discusses the algorithm based on Corollary 5.5 for computing representatives of the isomorphism classes in a given isogeny class, and the implementation of that algorithm in Magma. Finally, Section 7 contains a comparison between the results obtained in this paper and the results from the literature ([28,10,7]) on abelian varieties over finite fields.

Acknowledgments

The first author was supported by the Dutch Research Council (NWO) through grant VI.Veni.192.038. Part of this work was carried out while the third author was visiting Utrecht University and the Max Planck Institute for Mathematics in Bonn. He thanks these institutions for their hospitality and financial support. He was also supported in part by a Collaboration Grant for Mathematicians from the Simons Foundation, Award No. 637364. The authors thank Stefano Marseglia for helpful discussions related to the topics of this paper, and thank the referee for helpful comments that led to improvements of the initial version of the paper.

2. Local maximality at π of the Frobenius order

As in the introduction, let F be a function field of transcendence degree 1 over $\mathbb{F}_q$ (in which $\mathbb{F}_q$ is algebraically closed), let ∞ be a fixed place of F, and let

$$A = \{a \in F \mid \mathrm{ord}_v(a) \geq 0 \text{ for all places } v \neq \infty\}.$$

For $a \in A$, we define $\deg(a) = \log_q \#A/(a)$. Let $k = \mathbb{F}_{q^n}$ be a finite A-field, i.e., a field equipped with a homomorphism $\gamma\colon A \to k$. Let $\mathfrak{p} \trianglelefteq A$ be the kernel of γ. Then $\mathfrak{p}$ is a maximal ideal such that $\mathbb{F}_\mathfrak{p} := A/\mathfrak{p} \cong \mathbb{F}_{q^d}$ is a subfield of $\mathbb{F}_{q^n}$. We call d the degree of $\mathfrak{p}$; note that d divides n.

Let $\phi\colon A \to k\{\tau\}$ be a Drinfeld module of rank r, and let $\pi = \tau^n$. The results about the endomorphism algebra of ϕ that we use in this section are well-known and can be found, for example, in [11,14,16,17,25].

Let $K := \mathbb{F}_q(\pi)$ be the fraction field of $\mathbb{F}_q[\pi] \subseteq k\{\tau\}$ and define

$$k(\tau) = k\{\tau\} \otimes_{\mathbb{F}_q[\pi]} K.$$

Then $k(\tau)$ is a central division algebra over K of dimension n^2, split at all places of K except at (π) and $(1/\pi)$, where its invariants are $1/n$ and $-1/n$, respectively. Extend ϕ to an embedding $\phi\colon F \to k(\tau)$. Then

$$\mathcal{E} := \mathrm{End}_k(\phi) = \mathrm{Cent}_{k\{\tau\}}(\phi(A)),$$
$$D := \mathrm{End}_k(\phi) \otimes_{\phi(A)} \phi(F) = \mathrm{Cent}_{k(\tau)}(\phi(F)),$$

where $\mathrm{Cent}_R(S) = \{x \in R \mid xs = sx \text{ for all } s \in S\}$ denotes the centralizer of a subset S of a ring R. To simplify the notation, we will denote $\phi(A)$ by A and $\phi(F)$ by F, with ϕ being fixed. Let

$$A' := \mathbb{F}_q[\pi], \quad \widetilde{F} := F(\pi).$$

Let B be the integral closure of A in $\widetilde{F}$. There is a unique place $\widetilde{\mathfrak{p}}$ in $\widetilde{F}$ over the place (π) of K, and this $\widetilde{\mathfrak{p}}$ lies above the place $\mathfrak{p}$ of F; see [16, Theorem 3.8]. Let

$$\widetilde{F}_{\widetilde{\mathfrak{p}}} := \widetilde{F} \otimes_K \mathbb{F}_q(\!(\pi)\!)$$

be the completion of $\widetilde{F}$ at $\widetilde{\mathfrak{p}}$, and let $B_{\widetilde{\mathfrak{p}}}$ be the ring of integers of $\widetilde{F}_{\widetilde{\mathfrak{p}}}$.

Definition 2.1. Given an A-order R in B containing π, let

$$R_{\widetilde{\mathfrak{p}}} := R \otimes_{\mathbb{F}_q[\pi]} \mathbb{F}_q[\![\pi]\!] \subseteq B_{\widetilde{\mathfrak{p}}}.$$

We say that R is *locally maximal* at π if $R_{\widetilde{\mathfrak{p}}} = B_{\widetilde{\mathfrak{p}}}$; cf. [1, Definition 3.1].

Remark 2.2.

(1) For an A-order R in B, its *conductor* is defined as

$$\mathfrak{C} = \{c \in \widetilde{F} \mid cB \subseteq R\}.$$

One can show that $\mathfrak{C} = \mathrm{Ann}_R(B/R)$ and $\mathfrak{C}$ is the largest ideal of B that is contained in R. One can moreover show that R is locally maximal at π if and only if $\mathfrak{C}$ is relatively prime to $\widetilde{\mathfrak{p}}$; see [8, Corollary 6.2]. This is a weaker condition than requiring $\mathfrak{C}$ to be relatively prime to $\mathfrak{p}$; see Example 2.17.

(2) Suppose $\mathcal{E}$ is commutative. Then $\mathcal{E}$ can be considered as an A'-order in $\widetilde{F}$. It is observed in [29, p. 164] and [1, p. 514] that $\mathcal{E}$ is locally maximal at π. Therefore, for $A[\pi]$ to be an endomorphism ring of a Drinfeld module isogenous to ϕ it is necessary for $A[\pi]$ to be locally maximal at π. We investigate this condition in this section; later we will show that it is also sufficient; cf. Proposition 5.1.

Lemma 2.3. *The following hold:*

(1) The completion $A_{\mathfrak{p}}$ is a subring of $A[\pi]_{\widetilde{\mathfrak{p}}}$.
(2) The ideal $\mathcal{M}$ of $A[\pi]_{\widetilde{\mathfrak{p}}}$ generated by π and $\mathfrak{p}$ is maximal, and $A[\pi]_{\widetilde{\mathfrak{p}}}/\mathcal{M} \cong \mathbb{F}_{\mathfrak{p}}$.

Proof. Note that $A[\pi]_{\widetilde{\mathfrak{p}}}$ is an order in $B_{\widetilde{\mathfrak{p}}}$ (because $A[\pi]$ is an order in B). Hence $A[\pi]_{\widetilde{\mathfrak{p}}}$ is open and closed with respect to the $\widetilde{\mathfrak{p}}$-adic topology on $B_{\widetilde{\mathfrak{p}}}$. In particular, $A[\pi]_{\widetilde{\mathfrak{p}}}$ is complete. Now the topology on A induced by the embedding $A \to A[\pi] \to B_{\widetilde{\mathfrak{p}}}$ is the $\mathfrak{p}$-adic topology. Hence $A \hookrightarrow B_{\widetilde{\mathfrak{p}}}$ extends to an embedding $A_{\mathfrak{p}} \hookrightarrow B_{\widetilde{\mathfrak{p}}}$. Since $A[\pi]_{\widetilde{\mathfrak{p}}}$ is complete, the image of $A_{\mathfrak{p}}$ lies in $A[\pi]_{\widetilde{\mathfrak{p}}}$. This proves (1). Next, note that $B_{\widetilde{\mathfrak{p}}}/(\pi)$ is a finite local ring, and the natural homomorphism

$$A[\pi]_{\widetilde{\mathfrak{p}}} \to B_{\widetilde{\mathfrak{p}}}/(\pi)$$

factors through $A/\mathfrak{p}^s$ for some $s \geq 1$. Thus, $A[\pi]_{\widetilde{\mathfrak{p}}}/(\pi, \mathfrak{p}) \cong \mathbb{F}_{\mathfrak{p}}$. This proves (2). □

Let

$$[\widetilde{F}_{\widetilde{\mathfrak{p}}} : K_\pi] = e_K \cdot f_K,$$
$$[\widetilde{F}_{\widetilde{\mathfrak{p}}} : F_{\mathfrak{p}}] = e_F \cdot f_F,$$

where $F_{\mathfrak{p}}$ (resp. K_π) denotes the completion of F (resp. K) at $\mathfrak{p}$ (resp. (π)), and where e and f denote the ramification index and the residue degree of the corresponding extension, respectively.

Proposition 2.4. $A[\pi]$ *is locally maximal at π if and only if one of the following holds:*

- $f_F = 1$ *and* $e_F = 1$*;*
- $f_F = 1$ *and* $e_K = 1$*.*

Proof. Let $\mathrm{ord}_{\widetilde{\mathfrak{p}}}$ be the normalized valuation on $\widetilde{F}$ corresponding to the place $\widetilde{\mathfrak{p}}$. Then

$$e_K = \mathrm{ord}_{\widetilde{\mathfrak{p}}}(\pi),$$
$$e_F = \mathrm{ord}_{\widetilde{\mathfrak{p}}}(\mathfrak{p}).$$

Suppose that $A[\pi]_{\widetilde{\mathfrak{p}}} = B_{\widetilde{\mathfrak{p}}}$. Then, using the notation of Lemma 2.3, $\mathcal{M} = \widetilde{\mathfrak{p}}$ and $\mathbb{F}_{\widetilde{\mathfrak{p}}} := B_{\widetilde{\mathfrak{p}}}/\widetilde{\mathfrak{p}} = A[\pi]_{\widetilde{\mathfrak{p}}}/\mathcal{M} = \mathbb{F}_{\mathfrak{p}}$. Since π and $\mathfrak{p}$ generate $\mathcal{M}$, at least one of them must have $\mathrm{ord}_{\widetilde{\mathfrak{p}}}$ equal to 1. Hence, either $e_K = 1$ or $e_F = 1$. Next, f_F, by definition, is the degree of the extension $\mathbb{F}_{\widetilde{\mathfrak{p}}}/\mathbb{F}_{\mathfrak{p}}$. Hence $f_F = 1$.

Conversely, suppose that one of the given conditions holds. Then the residue field of $B_{\widetilde{\mathfrak{p}}}$ is $\mathbb{F}_{\mathfrak{p}}$ and either $\mathfrak{p}$ or π is a uniformizer of $B_{\widetilde{\mathfrak{p}}}$. Then $B_{\widetilde{\mathfrak{p}}} = \mathbb{F}_{\mathfrak{p}}[\![\mathfrak{p}]\!]$ or $B_{\widetilde{\mathfrak{p}}} = \mathbb{F}_{\mathfrak{p}}[\![\pi]\!]$, by the structure theorem of local fields of positive characteristic. On the other hand, by Lemma 2.3,

$$\mathbb{F}_{\mathfrak{p}} \subseteq A_{\mathfrak{p}} \cong \mathbb{F}_{\mathfrak{p}}[\![\mathfrak{p}]\!] \subseteq A[\pi]_{\widetilde{\mathfrak{p}}},$$

and $\mathfrak{p}, \pi \in A[\pi]_{\widetilde{\mathfrak{p}}}$. Hence $B_{\widetilde{\mathfrak{p}}} \subseteq A[\pi]_{\widetilde{\mathfrak{p}}}$, which implies that $B_{\widetilde{\mathfrak{p}}} = A[\pi]_{\widetilde{\mathfrak{p}}}$. □

For $f = \sum_{i=h}^{n} a_i \tau^i \in k\{\tau\}$ with $a_h \neq 0$, define $\mathrm{ht}(f) = h$. There is an integer $1 \leq H(\phi) \leq r$, called the *height of* ϕ, such that

$$\mathrm{ht}(\phi_a) = H(\phi) \cdot \mathrm{ord}_{\mathfrak{p}}(a) \cdot d$$

for all $0 \neq a \in A$ (cf. [17, Lemma 4.5.6]).

Theorem 2.5. *Let H be the height of ϕ. Then*

$$\left\lceil \frac{n}{H \cdot d} \right\rceil \leq \frac{[\widetilde{F} : K]}{d},$$

with equality if and only if $A[\pi]$ is locally maximal at π.

Proof. The following equalities hold:

$$\frac{[\widetilde{F} : F]}{[\widetilde{F} : K]} = \frac{r}{n} \qquad \text{(see [16, (3.7)])},$$

$$[\widetilde{F} : K] = e_K \cdot f_K \qquad \text{(because } \widetilde{\mathfrak{p}} \text{ is the only place of } \widetilde{F} \text{ over } (\pi)\text{)},$$

$$f_K = f_F \cdot d \qquad \text{(see [25, (4.1.6)])}.$$

On the other hand, by [16, p. 75],

$$H = \frac{r}{[\widetilde{F} : F]} [\widetilde{F}_{\widetilde{\mathfrak{p}}} : F_{\mathfrak{p}}]. \tag{1}$$

Hence

$$H = \frac{n}{[\widetilde{F} : K]} e_F f_F = \frac{n e_F f_F}{e_K f_K} = \frac{n}{d} \frac{e_F}{e_K}.$$

This implies that

$$\frac{n}{H \cdot d} = \frac{e_K}{e_F}.$$

On the other hand,

$$\frac{[\widetilde{F}:K]}{d} = \frac{e_K f_K}{d} = e_K \cdot f_F.$$

Thus, the inequality of the theorem is equivalent to

$$\left\lceil \frac{e_K}{e_F} \right\rceil \leq e_K \cdot f_F.$$

Since e_K, e_F, f_F are positive integers, the above inequality always holds, with equality if and only if $f_F = 1$ and either $e_K = 1$ or $e_F = 1$. Now the theorem follows from Proposition 2.4. □

Remark 2.6. The advantage of having the inequality of Theorem 2.5, rather than the statement of Proposition 2.4, is that instead of computing each of e_K, e_F, f_F individually it combines these numbers into quantities that are easier to compute.

Corollary 2.7. *If $H \leq r/[\widetilde{F}:F]$, then $A[\pi]$ is locally maximal at π. In particular, if ϕ is ordinary, i.e., $H = 1$, then $A[\pi]$ is locally maximal at π.*

Proof. Since $r/[\widetilde{F}:F] = n/[\widetilde{F}:K]$, the assumption is equivalent to $n/H \geq [\widetilde{F}:K]$, which implies that equality in Theorem 2.5 holds. □

Corollary 2.8. *If $k = \mathbb{F}_\mathfrak{p}$, i.e., if $d = n$, then $A[\pi]$ is locally maximal at π.*

Proof. Let $P_\phi(x)$ be the characteristic polynomial of π acting on the Tate module $T_\mathfrak{l}(\phi)$ of ϕ for some prime $\mathfrak{l} \neq \mathfrak{p}$. Then $P_\phi(x)$ is a monic polynomial in $A[x]$ of degree r whose coefficients do not depend on $\mathfrak{l}$; moreover, if $M_\phi(x)$ is the minimal polynomial of π over A, then $P_\phi(x) = M_\phi(x)^{r/[\widetilde{F}:F]}$; see [14, Lemma 3.3]. Denote the constant term of $P_\phi(x)$ by $a_0 = P_\phi(0)$. It is known that $\deg(a_0) = n$; see [17, Theorem 4.12.8]. Thus, by our assumption, $\deg(a_0) = d$. On the other hand, it is known that $a_0 \in \mathfrak{p}$, so $\deg(a_0) = \mathrm{ord}_\mathfrak{p}(a_0) \cdot d$; see [2, Theorem 4.2]. We see that $\mathrm{ord}_\mathfrak{p}(a_0) = 1$. Since $a_0 = M_\phi(0)^{r/[\widetilde{F}:F]}$, we also have $\mathrm{ord}_\mathfrak{p}(a_0) \geq r/[\widetilde{F}:F]$. Therefore, $[\widetilde{F}:F] = r$. But $[\widetilde{F}:F] = r$ is equivalent to $[\widetilde{F}:K] = n$, so $[\widetilde{F}:K] = d$. Thus, the inequality of Theorem 2.5 becomes

$$1 = \left\lceil \frac{1}{H} \right\rceil \leq \frac{[\widetilde{F}:K]}{d} = 1,$$

so it is an equality. □

Corollary 2.9. *Assume* $\mathrm{End}_k(\phi)$ *is commutative. Then $A[\pi]$ is locally maximal at π if and only if either ϕ is ordinary or $k = \mathbb{F}_\mathfrak{p}$.*

Proof. By [14, Theorem 2.9], $\mathrm{End}_k(\phi)$ is commutative if and only if $[\widetilde{F}:F]=r$. Now, as in the previous proof, $[\widetilde{F}:K]=n$. The inequality of Theorem 2.5 becomes

$$\left\lceil \frac{n}{Hd} \right\rceil \leq \frac{n}{d}.$$

Since n/d is a positive integer, equality holds if and only if either $H=1$ or $n=d$. $\square$

In all examples below, we let $A=\mathbb{F}_q[T]$ and $t:=\gamma(T)$. We also denote the monic polynomial in T generating the ideal $\mathfrak{p}$ by the same symbol $\mathfrak{p}$.

Example 2.10. Let $\mathfrak{p}=T$, $r=2$, and $n=3$. Let $\phi_T=\tau^2$, so ϕ is supersingular. In this case, the characteristic polynomial of the Frobenius is $P_\pi(x)=x^2-T^3$ (since $\pi^2=\tau^6=\phi_T^3$), so $[\widetilde{F}:F]=2$. Thus, $[\widetilde{F}:K]=3$. Since $H=2$ and $d=1$, the inequality of Theorem 2.5 becomes strict:

$$2=\left\lceil \frac{3}{2\cdot 1} \right\rceil < \frac{3}{1}=3.$$

Thus, $A[\pi]$ is *not* maximal at π. One can also see that $A[\pi]$ is not maximal at π by directly computing $A[\pi]_{\tilde{\mathfrak{p}}}$. Indeed, $A[\pi]=A[T\sqrt{T}]$ and $B=A[\sqrt{T}]$. Since $\sqrt{T}$ is the unique prime over T, $A[\pi]_{\tilde{\mathfrak{p}}}=A_T[T\sqrt{T}]\neq A_T[\sqrt{T}]=B_{\tilde{\mathfrak{p}}}$. Also, note that $\mathrm{End}_k(\phi)=\mathbb{F}_q[\tau]\cong A[\sqrt{T}]$ is the maximal A-order in $\widetilde{F}$.

Example 2.11. Suppose $n=6$ and $d=2$. Note that $[\widetilde{F}:K]$ is divisible by d and divides n, (since $r/[\widetilde{F}:F]=n/[\widetilde{F}:K]$ and $[\widetilde{F}:F]$ divides r). Hence, $[\widetilde{F}:K]=2$ or 6. The inequality of the theorem becomes

$$\left\lceil \frac{3}{H} \right\rceil \leq \frac{[\widetilde{F}:K]}{2}.$$

Hence $A[\pi]$ is locally maximal at π if and only if either $H=1$ or $[\widetilde{F}:K]=2$.

For example, when $q=3$, $\mathfrak{p}=T^2+T+2$, $\phi_T=t+\tau^4$, we calculate that $\phi_{\mathfrak{p}}=(2t+1)\tau^2+\tau^8$, which tells us that $H=2$. We also calculate the minimal polynomial for T over K, which is given by $\widetilde{m}_T(x)=x^6+(\pi^2+1)x^3+(\pi^4-\pi^2+2)$. (The minimal polynomial $\widetilde{m}_T(x)$ can be obtained from the minimal polynomial $M_\phi(x)$ of π over F by viewing $M_\phi(\pi)$ as a polynomial in T with coefficients in $\mathbb{F}_q[\pi]$; see [25, Lemma 4.3.1].) Hence, $[\widetilde{F}:K]=6$, so $A[\pi]$ is not locally maximal at π.

Example 2.12. Suppose $q=3$, $n=8$, and $\mathfrak{p}=T^2+T+2$. Let

$$\phi_T=t+\tau+(2t+1)\tau^2+2\tau^3+\tau^4.$$

Then, $H = 2$ and $\widetilde{m}_T(x) = x^4 + 2x^3 + 2x^2 + (2\pi + 1)x + \pi^2 + \pi + 1$, so $[\widetilde{F} : K] = 4$. Thus,

$$\frac{n}{Hd} = 2 = \frac{[\widetilde{F} : K]}{d},$$

so equality in Theorem 2.5 holds. In this case, $A[\pi]$ is locally maximal at π.

The next four examples show that the quantities in Proposition 2.4 are essentially independent of each other.

Example 2.13 *(Local maximality despite $e_K \neq 1$).* Let $q = 3$, $\mathfrak{p} = T^2 + T + 2$, and $k = \mathbb{F}_{q^4}$. Let $\phi_T = t + \tau^2$. By computation, we see that $H = 1$ and the minimal polynomial for T over K is given by $\widetilde{m}_T(x) = x^4 - x^3 + (\pi + 2)x^2 + (\pi + 1)x + \pi^2 + 1$. In particular, $n/(Hd) = 2$ and $[\widetilde{F} : K]/d = 2$. Therefore, $A[\pi]$ is locally maximal at π.

Notice that $e_K/e_F = 2$ and $e_K f_F = 2$ imply that $e_K = 2$, $e_F = 1$, $f_F = 1$, and $f_K = 2$.

Example 2.14 *(Local maximality despite $e_F \neq 1$).* Let $q = 3$, $\mathfrak{p} = T^2 + T + 2$, and $k = \mathbb{F}_{q^4}$. Let $\phi_T = t + (t + 1)\tau + (t + 2)\tau^2 + \tau^3$. By computation, we see that $H = 3$ and the minimal polynomial for T over K is given by $\widetilde{m}_T(x) = x^2 + x + 2\pi^3 + 2$. In particular, $n/(Hd) = 1/3$ and $[\widetilde{F} : K]/d = 1$. Therefore, $A[\pi]$ is locally maximal at π.

Notice that $e_K/e_F = 1/3$ and $e_K f_F = 2$ imply that $e_K = 1$, $e_F = 3$, $f_F = 1$, and $f_K = 2$.

Example 2.15 *(Not locally maximal despite $f_F = 1$).* Let $q = 3$, $\mathfrak{p} = T^2 + T + 2$, and $k = \mathbb{F}_{q^6}$. Let $\phi_T = t + \tau + (2t + 1)\tau^2$. By computation, we see that $H = 2$ and the minimal polynomial for T over K is given by $\widetilde{m}_T(x) = x^6 + x^3 + \pi^2 + 2$. In particular, $n/(Hd) = 3/2$ and $[\widetilde{F} : K]/d = 3$. Therefore, $A[\pi]$ is not locally maximal at π.

Notice that $e_K/e_F = 3/2$ and $e_K f_F = 3$ imply that $e_K = 3$, $e_F = 2$, $f_F = 1$, and $f_K = 2$.

Example 2.16 *(Not locally maximal despite $e_F = e_K = 1$).* Assume d is odd, q is odd, and $n/d = [k : \mathbb{F}_\mathfrak{p}] = 2$. Then there is a supersingular Drinfeld module of rank 2 over k whose minimal polynomial of π is $M_\phi(x) = x^2 + c\mathfrak{p} + c'\mathfrak{p}^2$, where $c, c' \in \mathbb{F}_q^\times$ are such that $c^2 - 4c'$ is not a square in $\mathbb{F}_q^\times$; see [25, Example 4.3.6]. In this case, $\mathfrak{p}$ remains inert in $\widetilde{F}$, so $e_F = 1$ and $f_F = 2$. Since $n/Hd = e_K/e_F$ and $H = 2$, we see that $e_K = 1$.

We conclude this section by pointing out that $A[\pi]$ might be locally maximal at π without being locally maximal at the other primes of $\widetilde{F}$ over $\mathfrak{p}$. The next example demonstrates this phenomenon.

Example 2.17. Let $q = 3$, $\mathfrak{p} = T^2 + T + 2$, and $n = 6$. Let $\phi_T = t + \tau + \tau^3$. Notice that $\phi_\mathfrak{p} = \tau^2 + 2\tau^4 + \tau^6$, so $H(\phi) = 1$, i.e., ϕ is ordinary. By Corollary 2.7, $A[\pi]$ is locally maximal at π.

Since ϕ is ordinary, we have $A[\pi] \subseteq \mathcal{E} \subseteq B \subset \widetilde{F}$ (the fact that $\mathcal{E}$ is an A-order in $\widetilde{F}$ follows from (1)). Let $\mathrm{Fitt}_A(\mathcal{E}/A[\pi])$ denote the Fitting ideal of $\mathcal{E}/A[\pi]$, and $\mathrm{disc}(A[\pi])$ (resp. $\mathrm{disc}(\mathcal{E})$) denote the discriminant of $A[\pi]$ (resp. the discriminant of $\mathcal{E}$). Then (cf. [26, p. 49])

$$\mathrm{disc}(A[\pi]) = \mathrm{Fitt}_A(\mathcal{E}/A[\pi])^2 \cdot \mathrm{disc}(\mathcal{E}).$$

The minimal polynomial of π is $M_\phi(x) = x^3+2x^2+x+2\mathfrak{p}^3$, so $\mathrm{disc}(A[\pi]) = \mathfrak{p}^3$. Therefore, either $\mathcal{E} = A[\pi]$ or $\mathrm{Fitt}_A(\mathcal{E}/A[\pi]) = \mathfrak{p}$.

Note that $M_\phi(x) \equiv x(x+1)^2$ modulo $\mathfrak{p}$. Let $m_\mathfrak{p}(x)$ be the minimal polynomial over $A/\mathfrak{p}$ of π acting on $\phi[\mathfrak{p}] \cong (A/\mathfrak{p})^2$. Then $m_\mathfrak{p}(x)$ must divide $x(x+1)^2$. In fact, $m_\mathfrak{p}(x)$ must divide either $(x+1)$ or $(x+1)^2$ since $\ker(\pi) = 0$. Suppose $u \in \mathcal{E}$ is such that $\mathfrak{p}u \in A[\pi]$. Then, $u = g(\pi)/\mathfrak{p}$ for some g with $\deg g(x) < 3$, and $g(\pi)$ acts as zero on $\phi[\mathfrak{p}]$. Furthermore, since $\phi_\mathfrak{p}$ divides $g(\pi)$ in $k\{\tau\}$, we must have $\mathrm{ht}(g(\pi)) \geq 2$. Thus, x divides $g(x)$ modulo $\mathfrak{p}$. Since the minimal polynomial of π acting on $\phi[\mathfrak{p}]$ must divide both $m_\mathfrak{p}(x)$ and $g(x)$ modulo $\mathfrak{p}$, it follows that

$$g(x) \equiv c \cdot x(x+1) \pmod{\mathfrak{p}} \quad \text{for some } c \in \mathbb{F}_q^\times.$$

On the other hand, by the division algorithm, we compute that

$$\frac{\pi(\pi+1)}{\mathfrak{p}} = \tau^4 + \tau^6.$$

Thus, the $\mathfrak{p}$-torsion of $\mathcal{E}/A[\pi]$ is the 1-dimensional span of $\pi(\pi+1)/\mathfrak{p}$ (and, in fact, $m_\mathfrak{p}(x) = x+1$), and we get $\mathcal{E}/A[\pi] \cong A/\mathfrak{p}$ and $\mathrm{disc}(\mathcal{E}) = \mathfrak{p}$. Since we also have $\mathrm{disc}(\mathcal{E}) = \mathrm{Fitt}_A(B/\mathcal{E})^2\,\mathrm{disc}(B)$, we conclude that $B = \mathcal{E}$.

Because $H = 1$, from equation (1) we get $\widetilde{F}_{\widetilde{\mathfrak{p}}} = F_\mathfrak{p}$; in particular, $\widetilde{\mathfrak{p}}$ is unramified over $\mathfrak{p}$. On the other hand, $\mathfrak{p}$ ramifies in B because $\mathrm{disc}(B) = \mathfrak{p}$. This implies that $\mathfrak{p}B = \widetilde{\mathfrak{p}} \cdot \mathfrak{P}^2$ for some prime $\mathfrak{P} \neq \widetilde{\mathfrak{p}}$.

Next, we note that the conductor $\mathfrak{C}$ of $A[\pi]$ in B has the property that $\mathfrak{C} \cap A = \mathrm{Ann}_A(B/A[\pi])$. Thus, $\mathfrak{C} \cap A = \mathfrak{p}$. This implies that $\mathfrak{C} \mid \widetilde{\mathfrak{p}} \cdot \mathfrak{P}^2$. By the local maximality of $A[\pi]$ at π, we know that $\widetilde{\mathfrak{p}} \nmid \mathfrak{C}$. Therefore, $\mathfrak{C} \mid \mathfrak{P}^2$. We also have the following equality (see [9, p. 78])

$$\mathrm{disc}(A[\pi]) = \mathrm{Nr}_{\widetilde{F}/F}(\mathfrak{C}) \cdot \mathrm{disc}(B).$$

Since $\mathrm{Nr}_{\widetilde{F}/F}(\mathfrak{P}) = \mathfrak{p}$, we see that $\mathfrak{C} = \mathfrak{P}^2$.

3. Kernel ideals: definitions

We keep the notation of the previous section but from now on we assume that $\mathcal{E} = \mathrm{End}_k(\phi)$ is commutative. Moreover, we no longer insist that $A = \mathbb{F}_q[T]$.

Let $I \trianglelefteq \mathcal{E}$ be a nonzero ideal. Let $k\{\tau\}\, I$ be the left ideal of $k\{\tau\}$ generated by the elements of I. Then $k\{\tau\}\, I$ is generated by a single element $u_I \in k\{\tau\}$ since $k\{\tau\}$ has a right division algorithm. Thus, $k\{\tau\}\, I = k\{\tau\}\, u_I$. It follows that

$$k\{\tau\}\, u_I \phi(A) = k\{\tau\}\, I\phi(A) = k\{\tau\}\, I = k\{\tau\}\, u_I.$$

Therefore, $u_I \phi(A) u_I^{-1} \subseteq k\{\tau\}$. If we set $\psi_a = u_I \phi_a u_I^{-1}$ for all $a \in A$, then ψ is a Drinfeld module over k of rank r and $u_I \colon \phi \to \psi$ is an isogeny. We denote $\psi = I * \phi$.

As before, let $D = \mathcal{E} \otimes_A F$ be the endomorphism algebra of ϕ. Note that $\mathcal{E} = D \cap k\{\tau\}$. Hence

$$k\{\tau\}\, I \cap D \subseteq k\{\tau\} \cap D = \mathcal{E}.$$

This implies that

$$k\{\tau\}\, I \cap D = (k\{\tau\}\, I \cap D) \cap \mathcal{E} = k\{\tau\}\, I \cap (D \cap \mathcal{E}) = k\{\tau\}\, I \cap \mathcal{E}. \tag{2}$$

Definition 3.1. We say that I is a *kernel ideal* if $(k\{\tau\}\, I) \cap D = I$. This definition is the one in [29, p. 167].

Next, define

$$\phi[I] = \bigcap_{\alpha \in I} \ker(\alpha),$$

where $\ker(\alpha)$ denotes the kernel (as a group-scheme) of the twisted polynomial $\alpha \in k\{\tau\}$ acting on the additive group scheme $\mathbb{G}_{a,k}$.

Lemma 3.2. *We have* $\phi[I] = \ker(u_I)$.

Proof. Suppose $\alpha \in I$. Then $\alpha \in k\{\tau\}\, I$, so $\alpha = f u_I$. Thus, $\ker(u_I) \subseteq \ker(\alpha)$. Since α is an arbitrary element of I, we get $\ker(u_I) \subseteq \phi[I]$. Conversely, we can write

$$u_I = f_1 \alpha_1 + \cdots + f_m \alpha_m,$$

for suitable $f_1, \ldots, f_m \in k\{\tau\}$ and $\alpha_1, \ldots, \alpha_m \in I$. This implies that $\phi[I] \subseteq \ker(u_I)$. $\square$

Each $\ker(\alpha)$, $\alpha \in I$, is an $\mathcal{E}$-module scheme, so $\phi[I]$ is an $\mathcal{E}$-module scheme. The annihilator $\mathrm{Ann}_{\mathcal{E}}(\phi[I])$ of this module scheme is an ideal of $\mathcal{E}$. It follows immediately from the definition that $I \subseteq \mathrm{Ann}_{\mathcal{E}}(\phi[I])$.

Definition 3.3. We say that I is a *kernel ideal* if $I = \mathrm{Ann}_{\mathcal{E}}(\phi[I])$. This definition is the analogue of the definition of this concept in the setting of abelian varieties; see [28, p. 533].

Lemma 3.4. *We have* $\mathrm{Ann}_{\mathcal{E}}(\phi[I]) = k\{\tau\}\, I \cap D$*, so Definitions 3.1 and 3.3 are equivalent.*

Proof. Let $J := k\{\tau\}\, I \cap D$ and $J' := \mathrm{Ann}_{\mathcal{E}}(\phi[I])$. Suppose $u \in J$. Then $u \in \mathcal{E}$ and $u = wu_I$ for some $w \in k\{\tau\}$. But wu_I annihilates $\ker(u_I) = \phi[I]$, so $u \in J'$. This implies that $J \subseteq J'$. Conversely, if $u \in J'$, then $u = wu_I$ for some $w \in k\{\tau\}$, by [23, Lemma 2.1.1]. Hence $u \in k\{\tau\}\, u_I \cap \mathcal{E} = J$, so $J' \subseteq J$. □

Let ϕ and ψ be two Drinfeld module over k of rank r. Let $\mathfrak{l}$ be a prime not equal to $\mathfrak{p} = \mathrm{char}_A(k)$. Let $u\colon \phi \to \psi$ be an isogeny. Then u induces a surjective homomorphism ${}^{\phi}\bar{k} \xrightarrow{u} {}^{\psi}\bar{k}$ of A-modules with finite kernel, where the notation ${}^{\phi}\bar{k}$ means that the A-module structure on $\bar{k}$ is induced from $\phi\colon A \to k\{\tau\}$ and likewise for ψ. From this, we get the short exact sequence

$$0 \longrightarrow \mathrm{Hom}_{A_{\mathfrak{l}}}(F_{\mathfrak{l}}/A_{\mathfrak{l}}, {}^{\phi}\bar{k}) \longrightarrow \mathrm{Hom}_{A_{\mathfrak{l}}}(F_{\mathfrak{l}}/A_{\mathfrak{l}}, {}^{\psi}\bar{k}) \longrightarrow \mathrm{Ext}^1_{A_{\mathfrak{l}}}(F_{\mathfrak{l}}/A_{\mathfrak{l}}, \ker(u)_{\mathfrak{l}}) \longrightarrow 0,$$

where $\ker(u)_{\mathfrak{l}}$ denotes the $\mathfrak{l}$-primary part of $\ker(u)$ (this is an étale group scheme). Note that $T_{\mathfrak{l}}(\phi) := \mathrm{Hom}_{A_{\mathfrak{l}}}(F_{\mathfrak{l}}/A_{\mathfrak{l}}, {}^{\phi}\bar{k})$ is the $\mathfrak{l}$-adic Tate module of ϕ and that

$$\mathrm{Ext}^1_{A_{\mathfrak{l}}}(F_{\mathfrak{l}}/A_{\mathfrak{l}}, \ker(u)_{\mathfrak{l}}) \cong \mathrm{Hom}_{A_{\mathfrak{l}}}(A_{\mathfrak{l}}, \ker(u)_{\mathfrak{l}}) \cong \ker(u)_{\mathfrak{l}}.$$

Hence, u induces an injective homomorphism

$$u_{\mathfrak{l}}\colon T_{\mathfrak{l}}(\phi) \longrightarrow T_{\mathfrak{l}}(\psi)$$

whose cokernel is isomorphic to $\ker(u)_{\mathfrak{l}}$. On the other hand, on $V_{\mathfrak{l}}(\phi) := T_{\mathfrak{l}}(\phi) \otimes_{A_{\mathfrak{l}}} F_{\mathfrak{l}}$, $u_{\mathfrak{l}}$ induces an isomorphism $V_{\mathfrak{l}}(\phi) \xrightarrow{\sim} V_{\mathfrak{l}}(\psi)$. Pulling back $T_{\mathfrak{l}}(\psi) \subseteq V_{\mathfrak{l}}(\psi)$ via $u_{\mathfrak{l}}^{-1}$ we get an $A_{\mathfrak{l}}$-lattice $u_{\mathfrak{l}}^{-1} T_{\mathfrak{l}}(\psi)$ in $V_{\mathfrak{l}}(\phi)$ which contains $T_{\mathfrak{l}}(\phi)$ and a short exact sequence

$$0 \longrightarrow T_{\mathfrak{l}}(\phi) \longrightarrow u_{\mathfrak{l}}^{-1} T_{\mathfrak{l}}(\psi) \longrightarrow \ker(u)_{\mathfrak{l}} \longrightarrow 0. \tag{3}$$

Following [23, (2.3.6)], we denote

$$H_{\mathfrak{l}}(\phi) = \mathrm{Hom}_{A_{\mathfrak{l}}}(T_{\mathfrak{l}}(\phi), A_{\mathfrak{l}}). \tag{4}$$

Taking the $A_{\mathfrak{l}}$-duals of (3), we obtain

$$0 \longrightarrow \mathrm{Hom}_{A_{\mathfrak{l}}}(u_{\mathfrak{l}}^{-1} T_{\mathfrak{l}}(\psi), A_{\mathfrak{l}}) \longrightarrow H_{\mathfrak{l}}(\phi) \longrightarrow \mathrm{Ext}^1_{A_{\mathfrak{l}}}(\ker(u)_{\mathfrak{l}}, A_{\mathfrak{l}}) \longrightarrow 0.$$

Note that $\mathrm{Ext}^1_{A_{\mathfrak{l}}}(\ker(u)_{\mathfrak{l}}, A_{\mathfrak{l}}) \cong \mathrm{Hom}_{A_{\mathfrak{l}}}(\ker(u)_{\mathfrak{l}}, F_{\mathfrak{l}}/A_{\mathfrak{l}}) \cong \ker(u)_{\mathfrak{l}}$. Hence to the isogeny u there corresponds a canonical sublattice of $H_{\mathfrak{l}}(\phi)$ whose cokernel is isomorphic to $\ker(u)_{\mathfrak{l}}$.

Now given a nonzero ideal $I \trianglelefteq \mathcal{E}$, we would like to describe the sublattice of $H_{\mathfrak{l}}(\phi)$ corresponding to u_I. Before doing so we recall an elementary result about the duals of intersections of lattices.

Let R be a PID with field of fractions K. Let $V = K^n$. A lattice in V is the R-span of a basis of V, i.e., a lattice is a free R-submodule $\Lambda \subseteq V$ of rank n such that $\Lambda K = V$. Fix a basis $\{e_1, \dots, e_n\}$ of V and define a symmetric K-bilinear pairing $\langle \cdot, \cdot \rangle \colon V \times V \to K$ by defining $\langle e_i, e_j \rangle = \delta_{ij} (=$ Kronecker symbol) and extending it bilinearly to $V \times V$. We identify $V^* := \mathrm{Hom}_K(V, K)$ with the linear functionals on V and take $e_i^*(v) = \langle e_i, v \rangle$ as a basis of V^*. For a lattice Λ in V, the *dual lattice* $\Lambda^* \subseteq V^*$ is the lattice defined by

$$\Lambda^* = \{f \in V^* \mid f(\lambda) \in R \text{ for all } \lambda \in \Lambda\}.$$

If we identify V^* with V by mapping $e_i^* \mapsto e_i$ for all $1 \le i \le n$, then

$$\Lambda^* = \{v \in V \mid \langle v, \lambda \rangle \in R \text{ for all } \lambda \in \Lambda\}.$$

Given two lattices Λ_1, Λ_2 in V, it is easy to check that

$$\Lambda_1 + \Lambda_2 = \{\lambda_1 + \lambda_2 \mid \lambda_1 \in \Lambda_1, \lambda_2 \in \Lambda_2\}$$

is a lattice, and so is

$$\Lambda_1 \cap \Lambda_2 = \{\lambda \mid \lambda \in \Lambda_1, \lambda \in \Lambda_2\}.$$

Lemma 3.5. *We have*

$$(\Lambda_1 \cap \Lambda_2)^* = \Lambda_1^* + \Lambda_2^*.$$

Proof. The proof is straightforward and is omitted. □

Now returning to u_I, let $\alpha, \beta \in I$ be nonzero elements. The overlattice of $T_{\mathfrak{l}}(\phi)$ corresponding to $\ker(\alpha) \cap \ker(\beta)$ is $\alpha^{-1} T_{\mathfrak{l}}(\phi) \cap \beta^{-1} T_{\mathfrak{l}}(\phi)$. The sublattice of $H_{\mathfrak{l}}(\phi)$ corresponding to $\ker(\alpha)_{\mathfrak{l}}$ is $\alpha H_{\mathfrak{l}}(\phi)$, so $(\alpha^{-1} T_{\mathfrak{l}}(\phi))^* = \alpha H_{\mathfrak{l}}(\phi)$. From the previous lemma, we conclude that the sublattice of $H_{\mathfrak{l}}(\phi)$ corresponding to $\ker(\alpha) \cap \ker(\beta)$ is $\alpha H_{\mathfrak{l}}(\phi) + \beta H_{\mathfrak{l}}(\phi)$. Thus, the dual of $u_I^{-1} T_{\mathfrak{l}}(I * \phi)$ is $I H_{\mathfrak{l}}(\phi)$ and we have proved:

Lemma 3.6. *The sublattice of $H_{\mathfrak{l}}(\phi)$ corresponding to $\ker(u_I)_{\mathfrak{l}}$ is $I H_{\mathfrak{l}}(\phi)$.*

Let $\mathcal{O}_k$ be the ring of integers of the unramified extension F_k of $F_{\mathfrak{p}}$ with residue field k. Let $H_{\mathfrak{p}}(\phi)$ be the Dieudonné module of ϕ as defined in [23, Sec. 2.5]. Recall that $H_{\mathfrak{p}}(\phi)$ is a free $\mathcal{O}_k$-module of rank r equipped with a $\tau^{\deg(\mathfrak{p})}$-linear map $f_{\phi,\mathfrak{p}} \colon H_{\mathfrak{p}}(\phi) \to H_{\mathfrak{p}}(\phi)$ such that

$$\begin{cases} \mathfrak{p} H_{\mathfrak{p}}(\phi) \subseteq f_{\phi,\mathfrak{p}}(H_{\mathfrak{p}}(\phi)) \subseteq H_{\mathfrak{p}}(\phi), \\ \dim_k(H_{\mathfrak{p}}(\phi)/f_{\phi,\mathfrak{p}}(H_{\mathfrak{p}}(\phi))) = 1. \end{cases}$$

Let

$$\mathbb{H}(\phi) = \prod_{\mathfrak{l} \trianglelefteq A} H_{\mathfrak{l}}(\phi),$$

where the product is over all primes of A, including $\mathfrak{p}$. According to [23, Lemma 2.6.2], there is a bijection between the kernels of isogenies $u\colon \phi \to \psi$ and sublattices $M = \prod_{\mathfrak{l} \trianglelefteq A} M_{\mathfrak{l}} \subseteq \mathbb{H}(\phi)$ such that $M_{\mathfrak{l}} = H_{\mathfrak{l}}(\phi)$ for all but finitely many primes $\mathfrak{l}$ and $M_{\mathfrak{p}}$ is a free $\mathcal{O}_k$-submodule of rank r of $H_{\mathfrak{p}}(\phi)$ such that

$$\begin{cases} \mathfrak{p} M_{\mathfrak{p}} \subseteq f_{\phi,\mathfrak{p}}(M_{\mathfrak{p}}) \subseteq M_{\mathfrak{p}}, \\ \dim_k(M_{\mathfrak{p}}/f_{\phi,\mathfrak{p}}(M_{\mathfrak{p}})) = 1. \end{cases} \tag{5}$$

The quotient $\prod_{\mathfrak{l} \neq \mathfrak{p}} (H_{\mathfrak{l}}(\phi)/M_{\mathfrak{l}})$ defines a unique finite étale k-subscheme $G^{\mathfrak{p}} \subseteq \mathbb{G}_{a,k}$ in $\phi(A)$-modules. Similarly, the quotient $\mathcal{O}_k$-module $H_{\mathfrak{p}}(\phi)/M_{\mathfrak{p}}$ endowed with the $\tau^{\deg(\mathfrak{p})}$-linear map induced by $f_{\phi,\mathfrak{p}}$ defines a unique k-subscheme $G_{\mathfrak{p}} \subseteq \mathbb{G}_{a,k}$ in $\phi(A)$-modules. The quotient of ϕ by $G^{\mathfrak{p}} \times G_{\mathfrak{p}}$ is the isogeny corresponding to M.

Proposition 3.7. *The sublattice of $\mathbb{H}(\phi)$ corresponding to u_I is $I\mathbb{H}(\phi) := \prod_{\mathfrak{l}} IH_{\mathfrak{l}}(\phi)$.*

Proof. We already proved this for $\mathfrak{l} \neq \mathfrak{p}$. On the other hand, $H_{\mathfrak{p}}(\phi)$ is the contravariant Dieudonné module, so $u_I(H_{\mathfrak{p}}(I * \phi))$ is the submodule generated by all $\alpha H_{\mathfrak{p}}(\phi)$, $\alpha \in I$. Hence $u_I(H_{\mathfrak{p}}(I * \phi)) = IH_{\mathfrak{p}}(\phi)$. $\square$

Definition 3.8. Let I be a nonzero ideal of $\mathcal{E}$. We say that I is a *kernel ideal* if for any ideal $J \trianglelefteq \mathcal{E}$ the inclusion $J\mathbb{H}(\phi) \subseteq I\mathbb{H}(\phi)$ implies $J \subseteq I$.

Lemma 3.9. *Definitions 3.3 and 3.8 are equivalent.*

Proof. Note that by the previous discussion, $J\mathbb{H}(\phi) \subseteq I\mathbb{H}(\phi)$ if and only if $\phi[I] \subseteq \phi[J]$.

Suppose I is a kernel ideal in the sense of Definition 3.3 and $\phi[I] \subseteq \phi[J]$. Then

$$J \subseteq \operatorname{Ann}_{\mathcal{E}} \phi[J] \subseteq \operatorname{Ann}_{\mathcal{E}} \phi[I] = I.$$

Hence I is a kernel ideal in the sense of Definition 3.8.

Conversely, suppose that I is a kernel ideal in the sense of Definition 3.8. Denote $J = \operatorname{Ann}_{\mathcal{E}} \phi[I]$. We know that $I \subseteq J$, and we need to show that this is an equality. For any $\alpha \in J$, $\ker(\alpha)$ contains $\phi[I]$, so $\phi[I] \subseteq \phi[J]$. This implies $J\mathbb{H}(\phi) \subseteq I\mathbb{H}(\phi)$. Hence $J \subseteq I$. $\square$

The next example shows that in general not every ideal of $\mathcal{E}$ is a kernel ideal.

Example 3.10. As in the examples in Section 2, let $A = \mathbb{F}_q[T]$ and $t = \gamma(T)$. Let $q = 2$, $\mathfrak{p} = T^4 + T + 1$, and $n = d = 4$. Set $\phi_T = t + t^3\tau^2 + \tau^3$. The minimal polynomial of π is given by

$$M_\phi(x) = x^3 + Tx^2 + x + \mathfrak{p}.$$

We algorithmically compute, cf. [13], that an A-basis for $\mathcal{E}$ is given by e_1, e_2, e_3, where

$$e_1 = 1, \qquad e_2 = \pi + 1, \qquad e_3 = \frac{(\pi+1)^2}{T+1}.$$

We also compute that

$$\begin{aligned} e_2e_3 = e_3e_2 &= (T+1)^3 + (T+1)e_3, \\ e_2^2 &= (T+1)e_3, \\ e_3^2 &= (T+1)^3 + (T+1)^2e_2 + (T+1)e_3. \end{aligned}$$

Let $\mathfrak{l} = T + 1$. We observe that an argument similar to the argument in [13, Example 4.12] implies that $\mathcal{E}_\mathfrak{l}$ is not Gorenstein, cf. Definition 4.4.

Consider the ideal $I = (e_2, e_3)$ in $\mathcal{E}$. An arbitrary element of I is of the following form:

$$\begin{aligned} &(a_1 + a_2e_2 + a_3e_3)e_2 + (b_1 + b_2e_2 + b_3e_3)e_3 \\ &= (a_3 + b_2 + b_3)(T+1)^3 + (a_1 + b_3(T+1)^2)e_2 + (b_1 + (a_3 + b_2 + b_3)(T+1))e_3, \end{aligned}$$

where $a_i, b_i \in A$. Hence

$$I = A(T+1)^3 + Ae_2 + Ae_3.$$

In $k\{\tau\}$, we have

$$\begin{aligned} e_2 &= 1 + \tau^4, \\ e_3 &= t^3 + t^2 + t + (t^3 + t^2 + 1)\tau^2 + (t^3 + t)\tau^3 + (t^3 + t^2)\tau^4 + \tau^5. \end{aligned}$$

These polynomials satisfy the equation

$$w = ue_2 + ve_3,$$

where

$$\begin{aligned} w &:= t^3 + t + 1 + (t^3 + t^2)\tau + (t+1)\tau^2 + \tau^3, \\ u &:= (t^3 + t^2)^2 + (t^3 + t^2)\tau, \\ v &:= t^3 + t^2. \end{aligned}$$

We also have

$$\begin{aligned}\phi_{(T+1)^2} &= (t^2+1) + t^3\tau^2 + (t^2+t+1)\tau^3 + \tau^4 + t\tau^5 + \tau^6\\ &= (t + (t^2+1)\tau + (t^2+t)\tau^2 + \tau^3)w.\end{aligned}$$

Hence, $(T+1)^2 \in k\{\tau\}\, w \subseteq k\{\tau\}\, I$. But $I \cap A = (T+1)^3 A$, so $(T+1)^2 \notin I$. Thus, I is not a kernel ideal.

4. Kernel ideals: properties

We keep the notation and assumptions of the previous section. In particular, ϕ is a Drinfeld module over k such that $\mathcal{E} := \mathrm{End}_k(\phi)$ is commutative, and $D := \mathcal{E} \otimes_A F$.

The next lemma is the analogue of [28, Theorem 3.11].

Lemma 4.1. *Let I and J be nonzero ideals in $\mathcal{E}$.*

(1) If $I = Ju$ for some $u \in D$, then $I * \phi \cong J * \phi$.
(2) If $I * \phi \cong J * \phi$ and I, J are kernel ideals, then $I = Ju$ for some $u \in D$.

Proof. (1) Let $k\{\tau\}\, I = k\{\tau\}\, u_I$ and $k\{\tau\}\, J = k\{\tau\}\, u_J$. By definition, for any $a \in A$, $(I * \phi)_a = u_I \phi_a u_I^{-1}$ and $(J * \phi)_a = u_J \phi_a u_J^{-1}$. Then

$$\begin{aligned} I * \phi \cong J * \phi \quad &\iff \quad c u_I \phi_a u_I^{-1} c^{-1} = u_J \phi_a u_J^{-1} \qquad \text{for some } c \in k^\times \text{ and all } a \in A,\\ &\iff u_J^{-1} c u_I \in D\\ &\iff c u_I = u_J u \qquad\qquad\qquad\qquad \text{for some } u \in D.\end{aligned}$$

If $I = Ju$, then $u_I = u_J u$, so $I * \phi \cong J * \phi$.

(2) Now assume that $I * \phi \cong J * \phi$, or equivalently $c u_I = u_J u$. Then

$$k\{\tau\}\, c u_I = k\{\tau\}\, u_I = k\{\tau\}\, I$$

and

$$k\{\tau\}\, u_J u = k\{\tau\}\, Ju.$$

Note that $k\{\tau\}\, Ju \cap D = (k\{\tau\}\, J \cap D)u$, so if I and J are kernel ideals, then

$$Ju = (k\{\tau\}\, J \cap D)u = k\{\tau\}\, Ju \cap D = k\{\tau\}\, I \cap \mathcal{E} = I. \quad \square$$

Let

$$\mathcal{O}_I := \{g \in D \mid Ig \subseteq I\} \tag{6}$$

be the (right) order of I in D. The next lemma is the analogue of [28, Proposition 3.9].

Lemma 4.2. *Let I be a nonzero ideal in $\mathcal{E}$ and write $k\{\tau\}\, I = k\{\tau\}\, u_I$ with $u_I \in k\{\tau\}$.*

(1) We have $u_I \mathcal{O}_I u_I^{-1} \subseteq \mathrm{End}_k(I * \phi)$.
(2) If I is a kernel ideal, then $u_I \mathcal{O}_I u_I^{-1} = \mathrm{End}_k(I * \phi)$.

Proof. (1) Let $u \in \mathcal{O}_I$. By definition, $u \in D$, so it commutes with ϕ_a in $k(\tau)$ for all $a \in A$. Therefore,

$$(u_I u u_I^{-1})(u_I \phi_a u_I^{-1}) = u_I u \phi_a u_I^{-1} = u_I \phi_a u u_I^{-1} = (u_I \phi_a u_I^{-1})(u_I u u_I^{-1}).$$

On the other hand, because $u \in \mathcal{O}_I$,

$$k\{\tau\}\, u_I u = k\{\tau\}\, I u \subseteq k\{\tau\}\, I = k\{\tau\}\, u_I.$$

Thus, $k\{\tau\}\, u_I u u_I^{-1} \subseteq k\{\tau\}$, so $u_I u u_I^{-1} \in k\{\tau\}$. It follows that $(u_I u u_I^{-1}) \in \mathrm{End}_k(I * \phi)$. Hence $u_I \mathcal{O}_I u_I^{-1} \subseteq \mathrm{End}_k(I * \phi)$.

(2) Now let $w \in \mathrm{End}_k(I * \phi)$. Then $w \in k\{\tau\}$ and $w(u_I \phi_a u_I^{-1})w^{-1} = u_I \phi_a u_I^{-1}$. This implies that $u_I^{-1} w u_I \in D$. Then

$$k\{\tau\}\, I(u_I^{-1} w u_I) = k\{\tau\}\, u_I(u_I^{-1} w u_I) = k\{\tau\}\, w u_I \subseteq k\{\tau\}\, u_I = k\{\tau\}\, I$$

Assume I is a kernel ideal. Then $k\{\tau\}\, I \cap D = I$ and

$$(k\{\tau\}\, I(u_I^{-1} w u_I)) \cap D = (k\{\tau\}\, I \cap D)(u_I^{-1} w u_I) = I(u_I^{-1} w u_I),$$

where the first equality follows from the fact that $u_I^{-1} w u_I \in D$. We see that

$$I(u_I^{-1} w u_I) \subseteq I,$$

so $u_I^{-1} w u_I \in \mathcal{O}_I$. This proves that $\mathrm{End}_k(I * \phi) \subseteq u_I \mathcal{O}_I u_I^{-1}$, which combined with the reverse inclusion proved earlier implies that $\mathrm{End}_k(I * \phi) = u_I \mathcal{O}_I u_I^{-1}$. $\square$

The next lemma is the analogue of [28, Theorem 3.15].

Lemma 4.3. *Assume $\mathcal{E}$ is the maximal A-order in D. Then every nonzero ideal of $\mathcal{E}$ is a kernel ideal.*

Proof. First, consider a nonzero principal ideal $\alpha\mathcal{E}$. Then $k\{\tau\}\, \alpha\mathcal{E} = k\{\tau\}\, \alpha$. Suppose that $u = g\alpha \in k\{\tau\}\, \alpha$ and $u \in D$. Then $g = u\alpha^{-1} \in D$ and $g \in k\{\tau\}$, so $g \in \mathcal{E}$. Therefore, $u \in \alpha\mathcal{E}$. This implies that

$$\alpha\mathcal{E} \subseteq k\{\tau\}\, \alpha \cap D \subseteq \alpha\mathcal{E},$$

so $(k\{\tau\}\, (\alpha\mathcal{E})) \cap D = \alpha\mathcal{E}$, i.e., $\alpha\mathcal{E}$ is a kernel ideal.

Now let $I \trianglelefteq \mathcal{E}$ be an arbitrary nonzero ideal. Since $\mathcal{E}$ is maximal, there is an ideal $J \trianglelefteq \mathcal{E}$ such that $IJ = \alpha\mathcal{E}$ is principal. Then

$$(k\{\tau\}\, I \cap D)J \subseteq k\{\tau\}\, IJ \cap D = IJ,$$

where the last equality follows from the earlier considered case of principal ideals. Now $I' := k\{\tau\}\, I \cap D$ is an ideal of $\mathcal{E}$, and $I'J \subseteq IJ$. Multiplying both sides by $J^{-1} \subseteq D$, we get $I' \subseteq I$. Since $I \subseteq I'$, we find that $I' = I$, so I is a kernel ideal. $\square$

Definition 4.4. We say that $\mathcal{E}$ is Gorenstein if $\mathcal{E}_{\mathfrak{l}} := \mathcal{E} \otimes_A A_{\mathfrak{l}}$ is a Gorenstein ring for all primes $\mathfrak{l} \trianglelefteq A$, i.e., $\mathrm{Hom}_{A_{\mathfrak{l}}}(\mathcal{E}_{\mathfrak{l}}, A_{\mathfrak{l}})$ is a free $\mathcal{E}_{\mathfrak{l}}$-module of rank 1; cf. [5].

Note that the maximal A-order in D is Gorenstein, so the next proposition implies Lemma 4.3.

Proposition 4.5. *If $\mathcal{E}$ is Gorenstein then every nonzero ideal of $\mathcal{E}$ is a kernel ideal.*

Proof. Let I and J be nonzero ideals of $\mathcal{E}$ such that $JH_{\mathfrak{l}}(\phi) \subseteq IH_{\mathfrak{l}}(\phi)$. Assume $\mathfrak{l} \neq \mathfrak{p}$. Because $\mathcal{E}_{\mathfrak{l}}$ is Gorenstein, $T_{\mathfrak{l}}(\phi)$ is a free $\mathcal{E}_{\mathfrak{l}}$-module of rank 1; cf. [13, Theorem 4.9]. But then, again because $\mathcal{E}_{\mathfrak{l}}$ is Gorenstein, $H_{\mathfrak{l}}(\phi) = \mathrm{Hom}_{A_{\mathfrak{l}}}(T_{\mathfrak{l}}(\phi), A_{\mathfrak{l}})$ is also a free $\mathcal{E}_{\mathfrak{l}}$-module of rank 1; cf. [13, Def. 4.8]. Hence, the inclusion $JH_{\mathfrak{l}}(\phi) \subseteq IH_{\mathfrak{l}}(\phi)$ implies that $J_{\mathfrak{l}} \subseteq I_{\mathfrak{l}}$, where $J_{\mathfrak{l}} := J \otimes_A A_{\mathfrak{l}}$ and $I_{\mathfrak{l}} := I \otimes_A A_{\mathfrak{l}}$.

At $\mathfrak{p}$ we consider the decomposition

$$H_{\mathfrak{p}}(\phi) = H^c_{\mathfrak{p}}(\phi) \oplus H^{\text{ét}}_{\mathfrak{p}}(\phi) \tag{7}$$

of the Dieudonné module into its connected component $H^c_{\mathfrak{p}}(\phi)$ and maximal étale quotient $H^{\text{ét}}_{\mathfrak{p}}(\phi)$. Let

$$D_{\mathfrak{p}} := D \otimes_F F_{\mathfrak{p}} = \bigoplus_{\nu | \mathfrak{p}} D_\nu, \tag{8}$$

where the sum is over the places of $\widetilde{F} = D$ lying over $\mathfrak{p}$ and D_ν is the completion of D at ν. There is a natural isomorphism (cf. [23, Theorem 2.5.6])

$$\mathcal{E}_{\mathfrak{p}} \simeq \mathrm{End}(H_{\mathfrak{p}}(\phi)),$$

where $\mathrm{End}(H_{\mathfrak{p}}(\phi))$ denotes the ring of endomorphisms of $H_{\mathfrak{p}}(\phi)$ compatible with the action of the Frobenius $f_{\phi,\mathfrak{p}}$. By [23, Corollary 2.5.8], the splitting (8) induces a compatible splitting $\mathcal{E}_{\mathfrak{p}} = \mathcal{E}_{\tilde{\mathfrak{p}}} \oplus \mathcal{E}'_{\mathfrak{p}}$ such that

$$\mathcal{E}_{\tilde{\mathfrak{p}}} \simeq \mathrm{End}(H^c_{\mathfrak{p}}(\phi)), \tag{9}$$

$$\mathcal{E}'_{\mathfrak{p}} \simeq \mathrm{End}(H^{\text{ét}}_{\mathfrak{p}}(\phi)) \simeq \mathrm{End}_{A_{\mathfrak{p}}[G_k]}(T_{\mathfrak{p}}(\phi)). \tag{10}$$

Here $\mathcal{E}_{\tilde{\mathfrak{p}}}$ is the completion of $\mathcal{E}$ in $B_{\tilde{\mathfrak{p}}}$, and $\mathcal{E}'_{\mathfrak{p}} = \oplus_j \mathcal{E}_j$ is a direct sum of finitely many local rings corresponding to places $\nu \neq \tilde{\mathfrak{p}}$ lying over $\mathfrak{p}$, and $T_{\mathfrak{p}}(\phi) = \varprojlim \phi[\mathfrak{p}^n](\bar{k})$ denotes the $\mathfrak{p}$-adic Tate module of ϕ. By [29, Corollary, p. 164] we find that $\mathcal{E}_{\tilde{\mathfrak{p}}} = B_{\tilde{\mathfrak{p}}}$ is maximal, hence a DVR, which implies that $H^c_{\mathfrak{p}}(\phi)$ is a free $\mathcal{E}_{\tilde{\mathfrak{p}}}$-module. Further, since $\mathcal{E}'_{\mathfrak{p}}$ is Gorenstein by assumption, one can apply the argument in the proof of [13, Theorem 4.9] to (10) to conclude that $H^{\text{ét}}_{\mathfrak{p}}(\phi)$ is a free $\mathcal{E}'_{\mathfrak{p}}$-module. Combining these statements yields that $JH_{\mathfrak{p}}(\phi) \subseteq IH_{\mathfrak{p}}(\phi)$ also implies that $J_{\mathfrak{p}} \subseteq I_{\mathfrak{p}}$.

Finally, consider $I_{\mathfrak{l}}$ as an $A_{\mathfrak{l}}$-submodule of $D \otimes_F F_{\mathfrak{l}}$ for any prime $\mathfrak{l}$ including $\mathfrak{p}$. Then

$$J = \bigcap_{\mathfrak{l}} (D \cap J_{\mathfrak{l}}) \subseteq \bigcap_{\mathfrak{l}} (D \cap I_{\mathfrak{l}}) = I.$$

Hence I is a kernel ideal by Definition 3.8. $\square$

5. Endomorphism rings and ideal actions

We keep the notation and assumptions of the previous section. In particular, ϕ is a Drinfeld module over k of rank r such that $\mathcal{E} = \mathrm{End}_k(\phi)$ is commutative.

Given an A-order R in $\widetilde{F} = D = \mathcal{E} \otimes_A F$ and a prime $\mathfrak{l} \lhd A$, we denote $R_{\mathfrak{l}} = R \otimes_A A_{\mathfrak{l}}$. Also, given a prime ν of B, we denote by B_ν the completion of B at ν and by R_ν the completion of R in B_ν.

The following result is modeled on [28, Porism 4.3].

Proposition 5.1. *Let R be an A-order in D containing π. Then there is a Drinfeld module ψ in the isogeny class of ϕ such that* $\mathrm{End}_k(\psi) = R$ *if and only if R is locally maximal at π.*

Proof. This is proved in [4, Theorem 1.5]. We present a slightly different argument.

If R is the endomorphism ring of a Drinfeld module isogenous to ϕ, then R contains π and is locally maximal at π by [29, Corollary, p. 164].

Conversely, assume R is locally maximal at π. It is enough to show that there is a Drinfeld module ψ in the isogeny class of ϕ such that $\mathrm{End}_k(\psi)_{\mathfrak{l}} = R_{\mathfrak{l}}$ for all the primes $\mathfrak{l}$ of A.

Pick any Drinfeld module ϕ_0 in the isogeny class. For any $\mathfrak{l} \neq \mathfrak{p}$, it follows from our assumptions that the rational Tate module $V_{\mathfrak{l}}(\phi_0)$ is free of rank 1 over $D_{\mathfrak{l}}$. It therefore contains lattices L with any order $\mathcal{O}_L = \{x \in D : xL \subseteq L\}$ (cf. (6)), and, identifying $V_{\mathfrak{l}}(\phi_0) \simeq D_{\mathfrak{l}}$, we see that such a lattice is Galois invariant if and only if its order contains π.

For any prime $\mathfrak{l} \neq \mathfrak{p}$, we view both $\mathrm{End}_k(\phi_0)_{\mathfrak{l}} = \mathrm{End}_k(\phi_0) \otimes A_{\mathfrak{l}} \simeq \mathrm{End}_{A_{\mathfrak{l}}[G_k]}(T_{\mathfrak{l}}(\phi_0))$ and $R_{\mathfrak{l}}$ as lattices in $V_{\mathfrak{l}}(\phi_0)$. Hence, both $\mathrm{End}_k(\phi_0)$ and R are maximal at all but finitely many primes $\mathfrak{l}$. In particular, there exist only finitely many primes, $\mathfrak{l}_1, \ldots, \mathfrak{l}_n$ say, at which $\mathrm{End}_k(\phi_0)_{\mathfrak{l}} \neq R_{\mathfrak{l}}$.

The lattice $R_{\mathfrak{l}_1}$ has order $\{x \in D : xR_{\mathfrak{l}_1} \subseteq R_{\mathfrak{l}_1}\} = R_{\mathfrak{l}_1}$, and so does its dual $R^*_{\mathfrak{l}_1} \simeq R_{\mathfrak{l}_1}$. As in (4), let $H_{\mathfrak{l}_1}(\phi_0)$ denote the dual of $T_{\mathfrak{l}_1}(\phi_0)$ and consider the intersection $H_{\mathfrak{l}_1}(\phi_0) \cap R^*_{\mathfrak{l}_1}$. This is an order contained in $R^*_{\mathfrak{l}_1}$ and we consider the Fitting ideal $\chi := \mathrm{Fitt}_A(R^*_{\mathfrak{l}_1}/(H_{\mathfrak{l}_1}(\phi_0) \cap R^*_{\mathfrak{l}_1}))$, which is a product of nonzero A-ideals. Then

$$\chi \cdot R^*_{\mathfrak{l}_1} \subseteq H_{\mathfrak{l}_1}(\phi_0) \cap R^*_{\mathfrak{l}_1} \subseteq H_{\mathfrak{l}_1}(\phi_0)$$

by definition. So we have obtained an integral lattice $L_{\mathfrak{l}_1} := \chi \cdot R^*_{\mathfrak{l}_1}$ inside $H_{\mathfrak{l}_1}(\phi_0)$, or equivalently, a lattice in $V_{\mathfrak{l}_1}(\phi_0)$ containing $T_{\mathfrak{l}_1}(\phi_0)$, with order

$$\{x \in D : x\chi R^*_{\mathfrak{l}_1} \subseteq \chi R^*_{\mathfrak{l}_1}\} = \{x \in D : xR^*_{\mathfrak{l}_1} \subseteq R^*_{\mathfrak{l}_1}\} = R_{\mathfrak{l}}.$$

Similar constructions yield sublattices $L_{\mathfrak{l}_i}$ of $H_{\mathfrak{l}_i}(\phi_0)$ for all $i = 2, \ldots, n$. At all other $\mathfrak{l} \neq \mathfrak{p}$ we set $L_{\mathfrak{l}} = H_{\mathfrak{l}}(\phi_0)$.

At $\mathfrak{p}$, write $D_{\mathfrak{p}} = \oplus_{\nu|\mathfrak{p}} D_\nu = D_{\tilde{\mathfrak{p}}} \oplus \left(\oplus_{\nu \neq \tilde{\mathfrak{p}}} D_\nu\right) =: D_{\tilde{\mathfrak{p}}} \oplus D'_{\mathfrak{p}}$, cf. (8). In this case, the rational Dieudonné module $H^{\text{ét}}_{\mathfrak{p}}(\phi_0) \otimes F_{\mathfrak{p}} = \oplus_{\nu \neq \tilde{\mathfrak{p}}} (H_{\mathfrak{p}}(\phi_0) \otimes F_{\mathfrak{p}})_\nu$ is free over $D'_{\mathfrak{p}}$, where each summand $(H_{\mathfrak{p}}(\phi_0) \otimes F_{\mathfrak{p}})_\nu$ is free over D_ν, and therefore contains lattices with any order. Comparing $\mathrm{End}(\phi_0)_\nu$ and R_ν at each $\nu \neq \tilde{\mathfrak{p}}$ over $\mathfrak{p}$ as lattices in D_ν, and adjusting the former if necessary via an analogous procedure to that in the previous paragraph, yields a sublattice $\oplus_{\nu \neq \tilde{\mathfrak{p}}} L_\nu$ of $H^{\text{ét}}_{\mathfrak{p}}(\phi_0)$. At $\tilde{\mathfrak{p}}$, we set $L_{\tilde{\mathfrak{p}}} = H^c_{\mathfrak{p}}(\phi_0)$.

By the dictionary between sublattices of $\mathbb{H}(\phi_0) = \prod_{\mathfrak{l} \trianglelefteq A} H_{\mathfrak{l}}(\phi_0)$ and isogenies, the quotient of $\prod_{\mathfrak{l} \neq \mathfrak{p}} H_{\mathfrak{l}}(\phi_0) \times H_{\mathfrak{p}}(\phi_0)$ by $\prod_{\mathfrak{l} \neq \mathfrak{p}} L_{\mathfrak{l}} \times \prod_{\nu|\mathfrak{p}} L_\nu$ yields a finite A-invariant subgroup G; cf. [23, Section 2.6]. The quotient ϕ_0/G in turn yields a Drinfeld module ψ isogenous to ϕ_0, for which $\mathrm{End}_k(\psi)_{\mathfrak{l}} = R_{\mathfrak{l}}$ at all places $\mathfrak{l} \neq \mathfrak{p}$ of A, and $\mathrm{End}_k(\psi)_\nu = R_\nu$ at all primes $\nu|\mathfrak{p}$ of $\tilde{F}$ with $\nu \neq \tilde{\mathfrak{p}}$. Finally, by [29, Corollary, p. 164], $\mathrm{End}_k(\psi)$ is locally maximal at π, so we also have $\mathrm{End}_k(\psi)_{\tilde{\mathfrak{p}}} = R_{\tilde{\mathfrak{p}}}$. □

Remark 5.2.

(1) Proposition 5.1 implies that if $A[\pi]$ is locally maximal at π, then any order between (and including) $A[\pi]$ and the maximal order B of $F(\pi)$ appears as an endomorphism ring of a Drinfeld module isogenous to ϕ.

(2) The problem of describing endomorphism rings of Drinfeld modules has been considered by several authors, see e.g. [14,29] and in particular [1], in which it is shown that for a fixed finite extension $L/\mathbb{F}_q$, any subring U of $L\{\tau\}$ containing $\mathbb{F}_q[\pi]$ such that the commutator of its center equals U is the endomorphism ring of some Drinfeld module over L. We should mention a caveat for this last result, which is not explicitly stated in [1]: the A-characteristic of L is not fixed and the construction of a Drinfeld module ϕ with $\mathrm{End}_L(\phi) = U$ involves an appropriate choice of $\gamma\colon A \to L$. In our setting, the A-characteristic of k is fixed from the beginning.

(3) Explicit algorithms to compute endomorphism rings were developed in [12] for Drinfeld $\mathbb{F}_q[T]$-modules of rank 2 over $\mathbb{F}_{\mathfrak{p}}$ and in [13] for any Drinfeld $\mathbb{F}_q[T]$-module with

commutative endomorphism algebra; in [21], the existence of an effective general algorithm is shown.

Corollary 5.3. *The ring $A[\pi]$ is the endomorphism ring of a Drinfeld module isogenous to ϕ if and only if either ϕ is ordinary or $k = \mathbb{F}_{\mathfrak{p}}$.*

Proof. By Proposition 5.1, $A[\pi]$ is the endomorphism ring of a Drinfeld module in the isogeny class of ϕ if and only if $A[\pi]$ is locally maximal at π. On the other hand, Corollary 2.9 states that $A[\pi]$ is locally maximal at π if and only if either ϕ is ordinary or $k = \mathbb{F}_{\mathfrak{p}}$. $\square$

We saw in Section 3 that, given a Drinfeld module ϕ over k and an ideal $I \trianglelefteq \mathcal{E} = \mathrm{End}_k(\phi)$, we can construct an isogenous Drinfeld module $\psi = I * \phi$, which is determined by $\psi_a = u_I \phi_a u_I^{-1}$ for all $a \in A$ and which satisfies $\mathrm{End}_k(\psi) \supseteq u_I \mathcal{O}_I u_I^{-1} \simeq \mathcal{O}_I \supseteq \mathcal{E}$ by Lemma 4.2.(2).

Theorem 5.4. *Consider the isogeny class of a Drinfeld module ϕ over k with commutative endomorphism algebra.*

(1) The map $I \mapsto I * \phi$ defines an action of the monoid of fractional ideals of $\mathcal{E}$ up to linear equivalence on the set of isomorphism classes of Drinfeld modules in the isogeny class of ϕ whose endomorphism ring is the order of an $\mathcal{E}$-ideal (and hence an overorder of $\mathcal{E}$).
(2) Upon restricting to kernel ideals, the action is free.
(3) If $\mathcal{E}$ is Gorenstein, then the action is also transitive on the set of all Drinfeld modules whose endomorphism ring is the order of an $\mathcal{E}$-ideal. In other words, if $\mathcal{E}$ is Gorenstein, then every submodule M of $\mathbb{H}(\phi)$ is of the form $I\mathbb{H}(\phi)$ for some nonzero ideal $I \trianglelefteq \mathcal{E}$.

Proof. (1) By Lemma 4.1.(1), we may consider the fractional ideals of $\mathcal{E}$ up to linear equivalence. The trivial ideal $I = \mathcal{E}$, considered as a $k\{\tau\}$-ideal, is generated by the trivial element, so $\mathcal{E} * \phi = \phi$ for any ϕ. For two ideals I, J it follows from the definition and commutativity that $(I \cdot J) * \phi = I * (J * \phi)$. As remarked above, for any ideal I, the Drinfeld modules ϕ and $I * \phi$ are isogenous via the generator u_I of $k\{\tau\}I$.
(2) This follows from Lemma 4.1.(2).
(3) The proof is inspired by [28, Proofs of Theorem 4.5 and Theorem 5.1]. Suppose that ϕ and ψ are isogenous and that $R := \mathrm{End}_k(\psi)$ is the order of an $\mathcal{E}$-ideal, i.e., $R \simeq \mathcal{O}_I$ for some ideal $I \trianglelefteq \mathcal{E}$. We may write $\psi = \phi/G$ where the finite subgroup scheme G is the kernel of the isogeny. We want to show that $\psi \cong I * \phi$. Since I is a kernel ideal by Proposition 4.5, by Proposition 3.7 this amounts to showing that the sublattice corresponding to the isogeny $\phi \to \psi$ with kernel G is $I\mathbb{H}(\phi)$, up to linear equivalence.

(Note also that the Drinfeld module $I * \phi$ indeed has endomorphism ring $u_I \mathcal{O}_I u_I^{-1} \simeq \mathcal{O}_I$ by Lemma 4.2.(2).)

By the dictionary between lattices and isogenies given above, the kernel G gives rise to a sublattice of $N_\mathfrak{l} \subseteq H_\mathfrak{l}(\phi)$ such that $H_\mathfrak{l}(\phi)/N_\mathfrak{l} \simeq G_\mathfrak{l}$ for each $\mathfrak{l} \neq \mathfrak{p}$ and a sublattice $N_\mathfrak{p} \subseteq H_\mathfrak{p}(\phi)$ satisfying (5) such that $H_\mathfrak{p}(\phi)/N_\mathfrak{p} \simeq G_\mathfrak{p}$. The lattice $N_\mathfrak{p}$ in $H_\mathfrak{p}(\phi)$ is both a free left $\mathcal{O}_k$-module and a right $\mathcal{E}_\mathfrak{p}$-module; by the splittings of $\mathcal{E}_\mathfrak{p} = \mathcal{E}_{\tilde{\mathfrak{p}}} \oplus \mathcal{E}'_\mathfrak{p}$ and $H_\mathfrak{p}(\phi) = H^c_\mathfrak{p}(\phi) \oplus H^{\text{ét}}_\mathfrak{p}(\phi)$ in (7) and their compatibility in (9) and (10), we must have that $N_\mathfrak{p} = N_{\tilde{\mathfrak{p}}} \oplus N'_\mathfrak{p}$ splits as well, where $N_{\tilde{\mathfrak{p}}}$ is a sublattice of $H^c_\mathfrak{p}(\phi)$ and an $\mathcal{O}_k \otimes \mathcal{E}_{\tilde{\mathfrak{p}}}$-module, and $N'_\mathfrak{p}$ is a sublattice of $H^{\text{ét}}_\mathfrak{p}(\phi)$ and an $\mathcal{O}_k \otimes \mathcal{E}'_\mathfrak{p}$-module.

As remarked in the proof of Proposition 4.5, the Gorenstein property implies that $H_\mathfrak{l}(\phi)$ is free over $\mathcal{E}_\mathfrak{l}$ of rank 1 for all $\mathfrak{l} \neq \mathfrak{p}$, and $H^{\text{ét}}_\mathfrak{p}(\phi)$ is free over $\mathcal{E}'_\mathfrak{p}$. Hence, any sublattice of $H_\mathfrak{l}(\phi)$ is of the form $I_\mathfrak{l} \cdot H_\mathfrak{l}(\phi)$ for some local ideal $I_\mathfrak{l} \trianglelefteq \mathcal{E}_\mathfrak{l}$, and any sublattice of $H^{\text{ét}}_\mathfrak{p}(\phi)$ is of the form $I'_\mathfrak{p} \cdot H^{\text{ét}}_\mathfrak{p}(\phi)$ for some ideal $I'_\mathfrak{p} \trianglelefteq \mathcal{E}'_\mathfrak{p}$. Since G is finite, we know that $I_\mathfrak{l} = \mathcal{E}_\mathfrak{l}$ for all but finitely many $\mathfrak{l}$; note also that there are only finitely many $\nu \neq \tilde{\mathfrak{p}}$ over $\mathfrak{p}$ that contribute to $I'_\mathfrak{p}$. Recall that $\mathcal{E}_{\tilde{\mathfrak{p}}}$ is maximal by [29, Corollary, p. 164], hence a PID, so again any sublattice of $H^c_\mathfrak{p}(\phi) = (H_\mathfrak{p}(\phi))_{\tilde{\mathfrak{p}}}$ is of the form $I_{\tilde{\mathfrak{p}}} \cdot H^c_\mathfrak{p}(\phi)$ for a local principal ideal $I_{\tilde{\mathfrak{p}}} \trianglelefteq \mathcal{E}_{\tilde{\mathfrak{p}}}$. Note that at all places we may scale the ideal generators to lie in the local endomorphism ring. We conclude that

$$N_\mathfrak{p} = \left(I_{\tilde{\mathfrak{p}}} \cdot H^c_\mathfrak{p}(\phi)\right) \oplus \left(I'_\mathfrak{p} \cdot H^{\text{ét}}_\mathfrak{p}(\phi)\right) = I_\mathfrak{p} \cdot H_\mathfrak{p}(\phi)$$

for some local ideal $I_\mathfrak{p} = I_{\tilde{\mathfrak{p}}} \oplus I'_\mathfrak{p}$ of $\mathcal{E}_\mathfrak{p}$.

These local ideals $I_\mathfrak{p}$ and $I_\mathfrak{l}$ for all $\mathfrak{l} \neq \mathfrak{p}$, i.e., local integral lattices, are the localizations of a global lattice (again since $I_\mathfrak{l} = \mathcal{E}_\mathfrak{l}$ for all but finitely many $\mathfrak{l}$), which is closed under the action of $\mathcal{E}$ since it is so everywhere locally by construction. Hence, it is a global ideal I, as we had to show. □

Corollary 5.5. *Suppose that $\mathcal{E} = A[\pi]$ (so that either ϕ is ordinary or $k = \mathbb{F}_\mathfrak{p}$, by Lemma 5.3). Then the action $I \mapsto I * \phi$ of the monoid of fractional ideals of $A[\pi]$ is free and transitive on the isomorphism classes in the isogeny class of ϕ.*

Proof. Since we consider the fractional ideals up to linear equivalence, we may without loss of generality consider only integral $A[\pi]$-ideals. If $\mathcal{E}_\mathfrak{l}$ is generated over $A_\mathfrak{l}$ by one element, then $\mathcal{E}_\mathfrak{l}$ is Gorenstein; cf. [27, p. 329]. Thus, $A[\pi]$ is Gorenstein, so every $A[\pi]$-ideal is a kernel ideal by Proposition 4.5. The statement now follows from Theorem 5.4 since every endomorphism ring is an overorder of $A[\pi]$; note that all such overorders occur as endomorphism rings by Proposition 5.1. □

Remark 5.6.

(1) The ideal action already appears in [18, Section 3] in a slightly different setting: fix an A-order $\mathcal{O}$ and consider the Picard group $\mathrm{Pic}(\mathcal{O})$, i.e., the quotient group of invertible

$\mathcal{O}$-ideals modulo principal ideals. Hayes shows that $\mathrm{Pic}(\mathcal{O})$ acts on the isomorphism classes of Drinfeld modules whose endomorphism ring contains $\mathcal{O}$. Invertible $\mathcal{O}$-ideals are proper and therefore have order $\mathcal{O}$; so this statement is consistent with the statement $\mathrm{End}_k(I * \phi) \supseteq u_I \mathcal{O}_I u_I^{-1} \cong \mathcal{O}_I$ which we prove in Lemma 4.2.

(2) It follows from Theorem 5.4 that the number of isomorphism classes in the isogeny class is bounded below by the sum of the class numbers of the overorders of $\mathcal{E}$ and that equality holds if $\mathcal{E}$ is minimal and Bass, so that every overorder is Gorenstein. For rank 2 Drinfeld modules, this result can also be found in [15, §6] where the class numbers are given as products involving Dirichlet characters. In higher rank, analogous expressions for the class numbers of the orders in D could be given.

6. Algorithms

In this section, we describe three algorithms which together compute representatives of each isomorphism class within the isogeny class of some Drinfeld module $\phi : A \to k\{\tau\}$ whose endomorphism ring we assume to be $A[\pi]$. While these algorithms will work for general A, our code written in Magma [6] implementing the algorithms works for the case $A = \mathbb{F}_q[T]$. The code is publicly available at https://github.com/JeffKaten/DrinfeldModules [19]. At the end of the section, an example is given for which the calculations are done by a computer.

The first algorithm is based on the work of Klüners and Pauli [20], who describe a method for computing the Picard group of an order in a global field. The second algorithm is based on the work of Marseglia [24], who describes a way of extending the computation of the Picard groups of each overorder of some fixed order $\mathcal{O}$ to the full ideal class monoid of $\mathcal{O}$. The third algorithm takes the representatives for the elements of the ideal class monoid $\mathrm{ICM}(A[\pi])$ and uses the built-in Magma functions for right division and greatest common right divisors in twisted polynomial rings to calculate u_I and $I * \phi$ for each $I \in \mathrm{ICM}(A[\pi])$ in order to generate a list of unique representatives for the isomorphism classes within the isogeny class of ϕ by way of Corollary 5.5.

Algorithm 1. Computing the Picard group of an order.

Starting with an A-basis for an order $\mathcal{O}$, we use the built-in Magma functions for computing the maximal order B, the class group $\mathrm{Cl}(B)$ of B, the unit group B^*, and the conductor $\mathcal{F}$ of $\mathcal{O}$ in B. Then there is an exact sequence

$$1 \longrightarrow \mathcal{O}^* \longrightarrow B^* \longrightarrow \frac{(B/\mathcal{F})^*}{(\mathcal{O}/\mathcal{F})^*} \longrightarrow \mathrm{Pic}(\mathcal{O}) \longrightarrow \mathrm{Cl}(B) \longrightarrow 1.$$

If we then compute representatives for the elements of $\frac{(B/\mathcal{F})^*}{(\mathcal{O}/\mathcal{F})^*}$, we can build a list of representatives for the elements of $\mathrm{Pic}(\mathcal{O})$ using the above sequence of finite abelian groups. That is, we use the following algorithm:

Step 1: Calculate a list of representatives in B for $\frac{(B/\mathcal{F})^*}{(\mathcal{O}/\mathcal{F})^*}$ using the method described in [20].
Step 2: Let $f : B^* \to \frac{(B/\mathcal{F})^*}{(\mathcal{O}/\mathcal{F})^*}$ be the above map. Compute a sublist L_0 of representatives for $\frac{(B/\mathcal{F})^*}{(\mathcal{O}/\mathcal{F})^*}$ modulo $\mathrm{Im}(f)$.
Step 3: Compute $L_1 := \{lB \cap \mathcal{O} | l \in L_0\}$.
Step 4: Compute $L_2 := \{I \cap \mathcal{O} | I \in \mathrm{Cl}(B)\}$.
Step 5: Output $L_3 := \{I_1 I_2 | I_1 \in L_1, I_2 \in L_2\}$.

Algorithm 2. Computing the ideal class monoid of $A[\pi]$.

Given two fractional ideals I_1, I_2 of an overorder $\mathcal{O}$, we denote by $(I_1 : I_2)$ the *ideal quotient* $\{x \in B : xI_2 \subseteq I_1\}$. Then for a single fractional ideal I it can be shown that the quotient $(I : I)$ is closed under multiplication, and we call $(I : I)$ the *multiplicator ring* of I. Simple algorithms which take as input an A-basis for each of two fractional ideals and output their ideal quotient are known and built into Magma.

Fix two fractional ideals I_1 and I_2 of $A[\pi]$. As in [24], we say that I_1 is *weakly equivalent* to I_2 if the multiplicator ring of I_1 and the multiplicator ring of I_2 are equal to the same order $\mathcal{O}$, and there exists an invertible fractional ideal L of $\mathcal{O}$ such that $I_2 = LI_1$. It is proved in [24, Proposition 4.1] that I_1 and I_2 are weakly equivalent if and only if $1 \in (I_1 : I_2)(I_2 : I_1)$.

For each overorder $\mathcal{O}$ of $A[\pi]$, we denote by $W_{\mathcal{O}}(A[\pi])$ the set of weak equivalence classes of fractional ideals whose multiplicator rings are $\mathcal{O}$. Finally, define $\mathrm{ICM}_{\mathcal{O}}(A[\pi])$ to be the subset consisting of those ideal classes whose multiplicator ring is $\mathcal{O}$,

$$\mathrm{ICM}_{\mathcal{O}}(A[\pi]) := \{[I] \in \mathrm{ICM} : (I : I) = \mathcal{O}\}.$$

Then,

$$\mathrm{ICM}(A[\pi]) = \bigsqcup \mathrm{ICM}_{\mathcal{O}}(A[\pi]).$$

As in [24, Theorem 4.6], it can be shown that if we have lists of unique representatives

$$W_{\mathcal{O}}(A[\pi]) = \{[I_1], \dots, [I_s]\} \qquad \text{and} \qquad \mathrm{Pic}(\mathcal{O}) = \{[J_1], \dots, [J_v]\}$$

then

$$\mathrm{ICM}(A[\pi]) = \{I_i J_j | 1 \le i \le s, 1 \le j \le v\}.$$

This leads to following algorithm, which computes a list of unique representatives for $\mathrm{ICM}(A[\pi])$.

Step 1: Calculate the overorders of $A[\pi]$. See [24, Section 6, Algorithm 1].
Step 2: For each overorder $\mathcal{O}$, calculate a list $L_1(\mathcal{O})$ of unique representatives for

$W_{\mathcal{O}}(A[\pi])$ using the method described in [24, Section 5].
Step 3: For each overorder $\mathcal{O}$, calculate a list $L_2(\mathcal{O})$ of unique representatives for $\mathrm{Pic}(\mathcal{O})$ using Algorithm 1.
Step 4: For each overorder calculate $\mathrm{ICM}_{\mathcal{O}}(A[\pi]) = \{IJ | I \in L_1(\mathcal{O}), J \in L_2(\mathcal{O})$.
Step 5: Output $\bigsqcup \mathrm{ICM}_{\mathcal{O}}$.

Algorithm 3. Computing the isomorphism classes of the isogeny class of ϕ.

Fix a Drinfeld module ϕ with $\mathrm{End}_k(\phi) = A[\pi]$. We use the following algorithm to compute a list $\{\psi_T\}$ defining unique representatives $\{[\psi]\}$ for the isomorphism classes within the isogeny class of ϕ.

Step 1: Compute a list L of unique representatives of ideals in $\mathrm{ICM}(A[\pi])$ using Algorithm 2. We may scale by an appropriate element of $A[\pi]$ if necessary to make each fractional ideal integral.
Step 2: For each $I \in L$, embed the basis elements of I into $k\{\tau\}$ using the map ϕ, and compute u_I by taking the greatest common right divisor of these elements. A function for computing greatest common right divisors of twisted polynomials (the classical Euclidean algorithm) is built into Magma.
Step 3: For each $I \in L$, compute the polynomial $I * \phi = u_I \phi_T u_I^{-1}$. Multiplication and right division of twisted polynomials are built into Magma.
Step 4: Output the list $\{I * \phi_T | I \in L\}$.

Example 6.1. Let $A = \mathbb{F}_q[T]$, $q = 2$, $k = \mathbb{F}_4$, $\mathfrak{p} = T$. Fix $\alpha \in k \setminus \mathbb{F}_q$. Let $\phi_1 \colon A \to k\{\tau\}$ be the Drinfeld module of rank 7 given by $(\phi_1)_T = \alpha\tau + \tau^2 + \tau^7$. The height of ϕ_1 is 1, i.e., it is ordinary. The minimal polynomial of $\pi = \tau^2$ over A is given by $m(x) = x^7 + x^4 + x^2 + x + T^2$, which has discriminant $T^4(T+1)^8$. The endomorphism ring of ϕ_1 is $A[\pi]$, and the maximal order in $F(\pi)$ containing A is

$$B = A\left[\frac{\pi^6 + \pi^5 + \pi^4 + \pi}{T}, \frac{\pi^5 + \pi^4 + 1}{T+1}\right].$$

Moreover,

$$B/A[\pi] \cong \frac{A}{T} \times \frac{A}{T+1} \times \frac{A}{T+1}.$$

We compute that there are exactly 4 overorders of $A[\pi]$, given by

$$\mathcal{O}_1 = A[\pi], \quad \mathcal{O}_2 = A\left[\pi, \frac{\pi^6 + \pi^5 + \pi^4 + \pi}{T}\right], \quad \mathcal{O}_3 = A\left[\pi, \frac{\pi^5 + \pi^4 + 1}{T+1}\right], \quad \mathcal{O}_4 = B.$$

In this case, $\mathrm{Cl}(B) = \mathrm{Pic}(\mathcal{O}_4)$ and the unit group of each overorder is trivial. We then compute the conductors $\mathcal{F}_i$, $1 \leq i \leq 4$ and see the following results as we calculate the Picard group of each of these orders.

Table 1
Ideal classes of $A[\pi]$.

I	u_I	$I * \phi_1$
(1)	1	ϕ_1
(T, π)	τ	ϕ_2
$(T^2 + T, \pi^3 + 1)$	$\alpha + \tau^3$	ϕ_3
$(T^2, \pi^2 + T + 1)$	$(\alpha + 1) + (\alpha + 1)\tau + \tau^3$	ϕ_4
$(T, \pi^4 + \pi^2 + \pi + 1)$	$1 + \alpha\tau^2 + \tau^3 + \tau^4$	ϕ_5
$(T + 1, \pi^3 + \pi + 1)$	$1 + (\alpha + 1)\tau + \tau^2 + \tau^3$	ϕ_6
$(T, \pi^2 + 1)$	$(\alpha + 1) + \tau + \tau^2$	ϕ_7
$(T^2 + T, \pi^3 + \pi^2 + \pi)$	$\tau + \alpha\tau^2 + \tau^3$	ϕ_8
$(T^2, \pi^2 + \pi + T)$	$(\alpha + 1)\tau + (\alpha + 1)\tau^2 + \tau^3$	ϕ_9
$(T, \pi^6 + \pi^5 + \pi^4 + \pi)$	$(\alpha + 1)\tau + \tau^2 + \alpha\tau^3 + \tau^4 + \alpha\tau^5 + \tau^6$	ϕ_{10}
$(T, \pi^3 + \pi^2 + 1)$	$(\alpha + 1) + \tau + \alpha\tau^2 + \tau^3$	ϕ_{11}
$(T^2, \pi + T + 1)$	$\alpha + \alpha\tau + \tau^2$	ϕ_{12}
$(T + 1, \pi^5 + \pi^4 + 1)$	$1 + \tau + (\alpha + 1)\tau^2 + (\alpha + 1)\tau^4 + \tau^5$	ϕ_{13}
$(T, \pi^4 + \pi^3 + \pi)$	$\alpha\tau + \tau^2 + (\alpha + 1)\tau^3 + \tau^4$	ϕ_{14}
$(T, \pi^2 + \pi)$	$(\alpha + 1)\tau + \tau^2$	ϕ_{15}

$$\# \frac{(B/\mathcal{F}_1)^*}{(\mathcal{O}_1/\mathcal{F}_1)^*} = 8 = \#\mathrm{Pic}(\mathcal{O}_1);$$
$$\# \frac{(B/\mathcal{F}_2)^*}{(\mathcal{O}_2/\mathcal{F}_2)^*} = 4 = \#\mathrm{Pic}(\mathcal{O}_2);$$
$$\# \frac{(B/\mathcal{F}_3)^*}{(\mathcal{O}_3/\mathcal{F}_3)^*} = 2 = \#\mathrm{Pic}(\mathcal{O}_3);$$
$$\# \frac{(B/\mathcal{F}_4)^*}{(\mathcal{O}_4/\mathcal{F}_4)^*} = 1 = \#\mathrm{Pic}(\mathcal{O}_4).$$

Next, we compute the weak equivalence classes of fractional ideals for each overorder, and see they are all trivial (hence $A[\pi]$ is Bass, see [24, Proposition 3.7]):

$$\#W_{\mathcal{O}_1}(A[\pi]) = \#W_{\mathcal{O}_2}(A[\pi]) = \#W_{\mathcal{O}_3}(A[\pi]) = \#W_{\mathcal{O}_4}(A[\pi]) = 1.$$

We list representatives of the $1 + 2 + 4 + 8 = 15$ ideal classes I_j within $\mathrm{ICM}(A[\pi])$ in Table 1 and the corresponding generator u_{I_j} of $k\{\tau\}I_j$ under the embedding ϕ_1. We also list the 15 distinct isomorphism classes of Drinfeld modules isogenous to ϕ_1; representatives of these isomorphism classes are listed in Table 2, along with their endomorphism rings $\mathcal{E}$.

7. Comparison with abelian varieties over finite fields

There are striking resemblances of the theory of Drinfeld modules over finite fields with the theory of abelian varieties over finite fields. Isogeny classes of such abelian varieties are also determined by the minimal or characteristic polynomial of their Frobenius endomorphism π, and it is an important open problem to describe the isomorphism classes within a fixed isogeny class. Indeed, precisely when the varieties are ordinary or

Table 2
Isomorphism classes of Drinfeld modules isogenous to ϕ_1.

ϕ_i	$(\phi_i)_T$	$\mathcal{E}$
ϕ_1	$\alpha\tau + \tau^2 + \tau^7$	$\mathcal{O}_1$
ϕ_2	$(\alpha+1)\tau + \tau^2 + \tau^7$	$\mathcal{O}_1$
ϕ_3	$\tau + \tau^2 + \tau^4 + \tau^7$	$\mathcal{O}_4$
ϕ_4	$(\alpha+1)\tau + \alpha\tau^3 + \tau^4 + \tau^5 + \tau^7$	$\mathcal{O}_1$
ϕ_5	$\alpha\tau + \alpha\tau^2 + \alpha\tau^3 + \tau^4 + \tau^5 + \tau^7$	$\mathcal{O}_2$
ϕ_6	$\alpha\tau + (\alpha+1)\tau^3 + \tau^4 + \tau^5 + \tau^7$	$\mathcal{O}_1$
ϕ_7	$(\alpha+1)\tau + \tau^2 + (\alpha+1)\tau^3 + \tau^4 + \tau^5 + \tau^7$	$\mathcal{O}_2$
ϕ_8	$(\alpha+1)\tau + \alpha\tau^3 + \tau^6 + \tau^7$	$\mathcal{O}_3$
ϕ_9	$\tau + (\alpha+1)\tau^3 + \alpha\tau^5 + \tau^6 + \tau^7$	$\mathcal{O}_1$
ϕ_{10}	$\tau + \alpha\tau^3 + \tau^4 + \alpha\tau^5 + \tau^6 + \tau^7$	$\mathcal{O}_2$
ϕ_{11}	$(\alpha+1)\tau + \tau^2 + (\alpha+1)\tau^3 + \tau^4 + \alpha\tau^5 + \tau^6 + \tau^7$	$\mathcal{O}_1$
ϕ_{12}	$\tau + \alpha\tau^3 + (\alpha+1)\tau^5 + \tau^6 + \tau^7$	$\mathcal{O}_1$
ϕ_{13}	$\alpha\tau + (\alpha+1)\tau^3 + (\alpha+1)\tau^5 + \tau^6 + \tau^7$	$\mathcal{O}_3$
ϕ_{14}	$\alpha\tau + \tau^2 + \alpha\tau^3 + \tau^4 + (\alpha+1)\tau^5 + \tau^6 + \tau^7$	$\mathcal{O}_1$
ϕ_{15}	$\tau + (\alpha+1)\tau^3 + \tau^4 + (\alpha+1)\tau^5 + \tau^6 + \tau^7$	$\mathcal{O}_2$

defined over the prime field $\mathbb{F}_p$, there exist categorical equivalences between isomorphism classes of abelian varieties over $\mathbb{F}_q$ and certain $\mathbb{Z}[\pi, \bar{\pi}]$-ideals, where $\bar{\pi} = q/\pi$ is the dual of the Frobenius, also called the Verschiebung.

First, consider an isogeny class of simple ordinary abelian varieties over $\mathbb{F}_q$ determined by a Frobenius endomorphism π. It is known that any ordinary variety $A/\mathbb{F}_q$ admits a (Serre-Tate) canonical lifting $\tilde{A}$ to the Witt vectors $W = W(\overline{\mathbb{F}}_q)$, which may be embedded into $\mathbb{C}$. In [10], Deligne shows that the functor $A \mapsto H_1(\tilde{A} \otimes_W \mathbb{C})$ induces an equivalence of categories between isomorphism classes in the isogeny class determined by π and free $\mathbb{Z}$-modules of rank $2\dim(A)$ equipped with an endomorphism F acting as π and an endomorphism V such that $FV = q$ playing the role of Verschiebung; these modules are often called Deligne modules. On the other hand, complex abelian varieties $A_\mathbb{C}$ are determined by lattices via the equivalence $A_\mathbb{C} \mapsto A_\mathbb{C}(\mathbb{C}) \cong \mathbb{C}^g/\Lambda$ induced from complex uniformization, and when $A_\mathbb{C}$ has CM through a CM-type Φ, we may write $\Lambda = \Phi(I)$ for some fractional $\mathrm{End}(A_\mathbb{C})$-ideal I. In this way, we may associate a fractional ideal I to each ordinary abelian variety $A/\mathbb{F}_q$, since each variety over $\mathbb{F}_q$ has CM and therefore so does its canonical lifting $\tilde{A}$. Linearly equivalent fractional ideals yield homothetic lattices and hence isomorphic abelian varieties, and homomorphisms between abelian varieties are described by quotient ideals. Put differently, fractional ideals up to linear equivalence act on the isomorphism classes in the ordinary isogeny class.

By comparison, it should follow with a similar proof that ordinary Drinfeld modules over k admit a canonical lifting to $\mathbb{C}_\infty$ of A-characteristic zero. On the one hand, Drinfeld modules over $\mathbb{C}_\infty$ admit analytic uniformization by lattices $\Lambda \subseteq \mathbb{C}_\infty$ (where homothetic lattices describe isomorphic Drinfeld modules), which yields a bijection between lattices in $\mathbb{C}_\infty$ and Drinfeld modules over $\mathbb{C}_\infty$. On the other hand, the ideal action $\phi \mapsto I * \phi$ may be defined for arbitrary Drinfeld modules over any A-field (i.e., of any characteristic).

Indeed, as alluded to above, the monoid of fractional ideals of an order $\mathcal{O}$ up to linear equivalence acts simply transitively on the isomorphism classes of Drinfeld modules over $\mathbb{C}_\infty$ with CM by $\mathcal{O}$. Ideals of $\mathcal{E}$ may be embedded in $\mathbb{C}_\infty$ as lattices, and every lattice $\Lambda \subseteq \mathbb{C}_\infty$ yields an ideal $\mathrm{Fitt}_A(\Lambda/\mathcal{E})\Lambda \trianglelefteq \mathcal{E}$. One can show that if $u_I\colon \phi \to I * \phi$ is an isogeny and ϕ corresponds to the lattice Λ, then $I * \phi$ corresponds to the lattice $I^{-1}\Lambda$, where $I^{-1} = (\mathcal{E} : I)$. This shows that, as for abelian varieties, the ideal action for ordinary Drinfeld modules can equivalently be described in terms of lattices via analytic uniformization on the lifted modules.

Next, consider an isogeny class of simple abelian varieties over $\mathbb{F}_p$, determined by a characteristic polynomial of π which does not have real roots, to ensure the endomorphism rings are all commutative. In [7], the authors show that such an isogeny class contains an element A_w with minimal endomorphism ring, i.e., $\mathrm{End}_{\mathbb{F}_p}(A_w) = \mathbb{Z}[\pi, \bar{\pi}]$, which is Gorenstein. They then use this variety to show that the functor $A \mapsto \mathrm{Hom}(A, A_w)$ induces a contravariant equivalence between isomorphism classes in the isogeny class and reflexive $\mathbb{Z}[\pi, \bar{\pi}]$-modules, which are in turn equivalent to finite free $\mathbb{Z}$-modules with an endomorphism F acting as π and an endomorphism V such that $FV = p$ which plays the role of $\bar{\pi}$. When the varieties are also ordinary, the authors also prove that their functor is equivalent to that of Deligne.

By comparison, for Drinfeld modules over $k = \mathbb{F}_\mathfrak{p}$, the existence of an isomorphism class ϕ_w with minimal endomorphism ring $\mathrm{End}_k(\phi_w) = A[\pi]$ is guaranteed by Corollary 2.8 and Lemma 5.3. The functor $\phi \mapsto \mathrm{Hom}_k(\phi, \phi_w)$ from isomorphism classes in the isogeny class of ϕ_w to reflexive $A[\pi]$-modules can be proven to be fully faithful by using Tate's theorems for Drinfeld modules and mimicking the proof of fully faithfulness in [7, Theorem 25]. Essential surjectivity follows from the main result in [22], when we view an $A[\pi]$-module as an A-matrix with characteristic polynomial determined by that of π. Moreover, suppose that $\phi = I * \phi_w$ for some (necessarily kernel) ideal $I \trianglelefteq \mathcal{E} = A[\pi]$ and recall that $\phi_a = u_I(\phi_w)_a u_I^{-1}$ for $u_I \in k\{\tau\}$ with $k\{\tau\}I = k\{\tau\}u_I$. Then, using that $A[\pi] = \mathrm{End}_k(\phi_w) = \{v \in k\{\tau\} : v(\phi_w)_a = (\phi_w)_a v \text{ for all } a \in A\}$, we see that

$$\begin{aligned}\mathrm{Hom}_k(\phi, \phi_w) &= \{u \in k\{\tau\} : u\phi_a = (\phi_w)_a u \text{ for all } a \in A\}\\ &= \{u \in k\{\tau\} : uu_I(\phi_w)_a = (\phi_w)_a uu_I \text{ for all } a \in A\}\\ &= \{u \in k\{\tau\} : uu_I \in A[\pi]\}\\ &= k\{\tau\}u_I \cap A[\pi] = I,\end{aligned}$$

where the last equality follows from the definition of a kernel ideal, see Definition 3.1 above and cf. Equation (2). This shows that the two constructions are in fact equivalent for Drinfeld modules.

Data availability

We have shared a link to our code on GitHub in the body of the paper and included the citation [19].

References

[1] Bruno Anglès, On some subrings of Ore polynomials connected with finite Drinfeld modules, J. Algebra 181 (2) (1996) 507–522.
[2] Bruno Anglès, On some characteristic polynomials attached to finite Drinfeld modules, Manuscr. Math. 93 (3) (1997) 369–379.
[3] Sedric Nkotto Nkung Assong, Explicit description of isogeny and isomorphism classes of Drinfeld modules over finite field, arXiv e-prints, arXiv:2009.02533, 2020.
[4] Sedric Nkotto Nkung Assong, Orders occurring as endomorphism ring of a Drinfeld module in some isogeny classes of Drinfeld modules of higher ranks, arXiv e-prints, arXiv:2009.11578, 2020.
[5] Hyman Bass, On the ubiquity of Gorenstein rings, Math. Z. 82 (1963) 8–28.
[6] Wieb Bosma, John Cannon, Catherine Playoust, The Magma algebra system. I. The user language, in: Computational Algebra and Number Theory, London, 1993, J. Symb. Comput. 24 (3–4) (1997) 235–265.
[7] Tommaso Giorgio Centeleghe, Jakob Stix, Categories of abelian varieties over finite fields, I: Abelian varieties over $\mathbb{F}_p$, Algebra Number Theory 9 (1) (2015) 225–265.
[8] Keith Conrad, The conductor ideal of an order, available at https://kconrad.math.uconn.edu/blurbs/.
[9] Ilaria Del Corso, Roberto Dvornicich, Relations among discriminant, different, and conductor of an order, J. Algebra 224 (1) (2000) 77–90.
[10] Pierre Deligne, Variétés abéliennes ordinaires sur un corps fini, Invent. Math. 8 (1969) 238–243.
[11] Vladimir G. Drinfeld, Elliptic modules. II, Mat. Sb. (N.S.) 102(144) (2) (1977) 182–194, 325.
[12] Sumita Garai, Mihran Papikian, Endomorphism rings of reductions of Drinfeld modules, J. Number Theory 212 (2020) 18–39.
[13] Sumita Garai, Mihran Papikian, Computing endomorphism rings and Frobenius matrices of Drinfeld modules, J. Number Theory 237 (2022) 145–164.
[14] Ernst-Ulrich Gekeler, On finite Drinfeld modules, J. Algebra 141 (1) (1991) 187–203.
[15] Ernst-Ulrich Gekeler, Frobenius distributions of Drinfeld modules over finite fields, Trans. Am. Math. Soc. 360 (4) (2008) 1695–1721.
[16] Ernst-Ulrich Gekeler, Brian A. Snyder, Drinfeld modules over finite fields, in: Drinfeld Modules, Modular Schemes and Applications, Alden-Biesen, 1996, World Sci. Publ., River Edge, NJ, 1997, pp. 66–87.
[17] David Goss, Basic Structures of Function Field Arithmetic, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 35, Springer-Verlag, Berlin, 1996.
[18] David Hayes, Explicit class field theory in global function fields, in: Studies in Algebra and Number Theory, in: Adv. in Math. Suppl. Stud., vol. 6, Academic Press, New York-London, 1979, pp. 173–217.
[19] Jeffrey Katen, DrinfeldModules, GitHub repository, available at https://github.com/JeffKaten/DrinfeldModules, 2023.
[20] Jürgen Klüners, Sebastian Pauli, Computing residue class rings and Picard groups of orders, J. Algebra 292 (1) (2005) 47–64.
[21] Nikolas Kuhn, Richard Pink, Finding endomorphisms of Drinfeld modules, J. Number Theory 232 (2022) 118–154.
[22] Claiborne Latimer, Cyrus C. MacDuffee, A correspondence between classes of ideals and classes of matrices, Ann. Math. (2) 34 (1933) 313–316.
[23] Gérard Laumon, Cohomology of Drinfeld Modular Varieties. Part I, Cambridge Studies in Advanced Mathematics, vol. 41, Cambridge University Press, Cambridge, 1996.
[24] Stefano Marseglia, Computing the ideal class monoid of an order, J. Lond. Math. Soc. (2) 101 (3) (2020) 984–1007.
[25] Mihran Papikian, Drinfeld Modules, Graduate Texts in Mathematics, vol. 296, Springer, Cham, 2023.
[26] Jean-Pierre Serre, Local Fields, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979.
[27] Jacques Tilouine, Hecke algebras and the Gorenstein property, in: Modular Forms and Fermat's Last Theorem, Boston, MA, 1995, Springer, New York, 1997, pp. 327–342.
[28] William C. Waterhouse, Abelian varieties over finite fields, Ann. Sci. Éc. Norm. Supér. (4) 2 (1969) 521–560.
[29] Jiu-Kang Yu, Isogenies of Drinfeld modules over finite fields, J. Number Theory 54 (1) (1995) 161–171.