arXiv:2209.15033v1 [math.NT] 29 Sep 2022

ISOMORPHISM CLASSES OF DRINFELD MODULES OVER FINITE FIELDS

VALENTIJN KAREMAKER, JEFFREY KATEN, AND MIHRAN PAPIKIAN

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 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.

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements. Let $A = \mathbb{F}_q[T]$ be the ring of polynomials in indeterminate T with coefficients in $\mathbb{F}_q$, and let $F = \mathbb{F}_q(T)$ be the fraction field of A. Given a nonzero prime ideal $\mathfrak{p}$ 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

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

(Note that ϕ is uniquely determined by ϕ_T.) 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 $a \in A$ (or equivalently such that $u\phi_T = \psi_T u$).

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 free 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 $\mathcal{E}$.

2010 *Mathematics Subject Classification.* 11G09, 11R58.

Key words and phrases. Drinfeld modules; endomorphism rings; isogeny classes; Gorenstein rings.

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. [16, Theorem 4.3.2]. 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. [14, 10]. Our approach is inspired by the work of Waterhouse [17] 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 6 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 divison algorithm, we have $k\{\tau\}I = k\{\tau\}u_I$ for some $u_I \in k\{\tau\}$. This element defines an isogeny $u_I \colon \phi \to \psi$, where ψ is the Drinfeld module determined by $\psi_T = u_I \phi_T u_I^{-1}$ and is also denoted by $I * \phi$. 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 [17] 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 [18]. 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 published literature.

In general, we have that $\mathrm{End}_k(I * \phi) \supseteq u_I \mathcal{O}_I u_I^{-1} \cong \mathcal{O}_I$, 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 [15], an algorithm is presented for computing the ideal class monoid of an order in a number field. In an ongoing project, we are working on adapting that algorithm to orders in function fields. Since for a given ideal $I \trianglelefteq \mathcal{E}$ computing $I * \phi$ is fairly straightforward, Theorem B combined with this algorithm will provide an efficient method for computing explicit representatives of isomorphism classes of all Drinfeld modules isogenous to ϕ such that $\mathrm{End}_k(\phi) \cong A[\pi]$. Let us mention that Assong [2] has recently 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 2.6) 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 contain 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 5.3), and prove when $A[\pi]$ occurs as an endomorphism ring (Corollary 5.2), to obtain Theorem B (cf. Corollary 5.4). Finally, Section 6 contains a comparison between the results obtained in this paper and results from the literature ([17, 6, 5]) on abelian varieties over finite fields.

2. Local maximality at π of the Frobenius order

As in the introduction, let $A = \mathbb{F}_q[T]$ and $F = \mathbb{F}_q(T)$, and let $k = \mathbb{F}_{q^n}$ be a finite A-field, i.e., a field equipped with a homomorphism $\gamma\colon A \to k$. We denote $t = \gamma(T)$. Let $\mathfrak{p} \trianglelefteq A$ be the kernel of A. Then $\mathfrak{p}$ is a maximal ideal such that $\mathbb{F}_{\mathfrak{p}} := A/\mathfrak{p} = \mathbb{F}_{q^d}$ is a subfield of $\mathbb{F}_{q^n}$. We call d the degree of $\mathfrak{p}$; note that d divides n. By slight abuse of notation, we denote the monic generator of $\mathfrak{p}$ in A by the same symbol.

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 [9, 14, 18], but for the convenience of a single reference and consistency of notation, we will refer to [16].

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; see [16, Proposition 4.1.1]. 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

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

Let B be the integral closure of A in $\tilde{F}$. There is a unique place $\widetilde{\mathfrak{p}}$ in $\widetilde{F}$ over the place (π) of K; see [16, Theorem 4.1.5]. 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. Suppose $\mathcal{E}$ is commutative. Then $\mathcal{E}$ can be considered as an A'-order in $\widetilde{F}$. It is observed in [18, 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.

Let $m(x)$ be the minimal polynomial of π over F, so that $\widetilde{F} \cong F[x]/(m(x))$. Note that $\pi \in \mathcal{E}$ is integral over A, so the polynomial $m(x)$ is monic with coefficients in A and $A[\pi] \cong A[x]/(m(x))$. To analyze the local maximality of $A[\pi]$, it will be convenient to change the perspective and express $A[\pi]$ as a quotient of $A'[x]$. To do so, consider T and π as two independent indeterminates over $\mathbb{F}_q$. Then consider $m(\pi) \in \mathbb{F}_q[T, \pi] = A'[T]$ as a polynomial $\widetilde{m}(T)$ in indeterminate T with coefficients in A'.

Lemma 2.3. *We have:*

(1) $\widetilde{m}(T)$ is irreducible in $K[T]$ and has degree $[\widetilde{F} : K]$ in T.
(2) The leading coefficient of $\widetilde{m}(T)$ is in $\mathbb{F}_q^\times$.
(3) Let $\bar{m}(T) \in \mathbb{F}_q[T]$ be the polynomial obtained by reducing the coefficients of $\widetilde{m}(T)$ modulo π. Then, up to an $\mathbb{F}_q^\times$-multiple, $\bar{m}(T)$ is equal to $\mathfrak{p}^{[\widetilde{F}:K]/d}$.

Proof. By [16, Theorem 4.2.7], the degree in T of $m(0)$ is strictly larger than the degrees of the other coefficients of $m(x)$. Hence, the leading term of $\widetilde{m}(T)$ is the leading term of $m(0) \in A$, so its leading coefficient is in $\mathbb{F}_q^\times$. Moreover, by [16,

Theorem 4.2.2 and Theorem 4.2.7], up to an $\mathbb{F}_q^\times$-multiple, $m(0)$ is equal to $\mathfrak{p}^{\frac{[\widetilde{F}:F]\cdot n}{r\cdot d}}$. Using [16, (4.1.3)], we get

$$(m(0)) = \mathfrak{p}^{\frac{[\widetilde{F}:K]}{d}}.$$

Thus, $\deg_T \widetilde{m}(T) = [\widetilde{F} : K]$. Since $\widetilde{F}$ is obtained by adjoining a root of $\widetilde{m}(T)$, the equality $\deg_T \widetilde{m}(T) = [\widetilde{F} : K]$ implies that $\widetilde{m}(T)$ is irreducible over K. Finally, note that $\bar{m}(T) = m(0)$, which completes the proof of the lemma. □

Lemma 2.4. *The following hold:*

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

Proof. We have

$$\begin{aligned} A[\pi]_{\widetilde{\mathfrak{p}}} &= A[\pi] \otimes_{\mathbb{F}_q[\pi]} \mathbb{F}_q[\![\pi]\!] \\ &\cong \mathbb{F}_q[\pi][T]/(\widetilde{m}(T)) \otimes_{\mathbb{F}_q[\pi]} \mathbb{F}_q[\![\pi]\!] && \text{(by Lemma 2.3)} \\ &\cong \mathbb{F}_q[\![\pi]\!]\,[T]/(\widetilde{m}(T)). \end{aligned}$$

(Note that $\widetilde{F} \cong K[T]/(\widetilde{m}(T))$ and, because there is a unique place in $\widetilde{F}$ over π, [16, proof of Theorem 2.8.5] implies that $\widetilde{m}(T)$ remains irreducible over $\mathbb{F}_q(\!(\pi)\!)$.)

The element π of $A[\pi]_{\widetilde{\mathfrak{p}}}$ is not a unit. Now

$$A[\pi]_{\widetilde{\mathfrak{p}}}/(\pi) \cong \mathbb{F}_q[T]/(\bar{m}(T)) \cong A/\mathfrak{p}^{[\widetilde{F}:K]/d}.$$

This shows that $\mathfrak{p}$ is also not invertible in $A[\pi]_{\widetilde{\mathfrak{p}}}$ and

$$A[\pi]_{\widetilde{\mathfrak{p}}}/(\pi, \mathfrak{p}) \cong A/\mathfrak{p}.$$

This proves (1) and (2).

Next, 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 (3). □

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 2.5. *$A[\pi]$ 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 2.4, we have $\mathcal{M} = \widetilde{\mathfrak{p}}$ 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 $f_K = 1$.

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 $B_{\widetilde{\mathfrak{p}}}$. By the structure theorem of local fields of positive characteristic, we have $B_{\widetilde{\mathfrak{p}}} = \mathbb{F}_{\mathfrak{p}}[\![\mathfrak{p}]\!]$ or $B_{\widetilde{\mathfrak{p}}} = \mathbb{F}_{\mathfrak{p}}[\![\pi]\!]$. On the other hand, by Lemma 2.4,

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

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

Theorem 2.6. *Let H be the height of ϕ (see* [16, Lemma 3.2.11] *for the definition). 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. We have the following equalities:

$$\frac{[\widetilde{F} : F]}{[\widetilde{F} : K]} = \frac{r}{n} \qquad \text{(see [16, (4.1.3)])},$$
$$[\widetilde{F} : K] = e_K \cdot f_K \qquad \text{(see [16, (4.1.4)])},$$
$$f_K = f_F \cdot d \qquad \text{(see [16, (4.1.6)])}.$$

On the other hand, by [16, Proposition 4.1.10],

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

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 2.5. □

Remark 2.7. The advantage of having the inequality of Theorem 2.6, rather than the statement of Proposition 2.5, 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 2.8. *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 2.6 holds. □

Corollary 2.9. *If $k = \mathbb{F}_{\mathfrak{p}}$, i.e., $d = n$, then $A[\pi]$ is locally maximal at π.*

Proof. If $k = \mathbb{F}_{\mathfrak{p}}$, then $[\widetilde{F} : F] = r$; see [7, Proposition 2.1]. But $[\widetilde{F} : F] = r$ is equivalent to $[\widetilde{F} : K] = n$, so $[\widetilde{F} : K] = d$. Therefore, the inequality of Theorem 2.6 becomes

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

so it is an equality. □

Corollary 2.10. *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 [16, Theorem 4.1.5], $\mathrm{End}_k(\phi)$ is commutative if and only if $[\widetilde{F} : F] = r$. Now, as in the previous proof, $[\widetilde{F} : K] = n$. The inequality of Theorem 2.6 becomes

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

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

Example 2.11. 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 $x^2 - T^3$ (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 2.6 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 $A[\pi]_{\widetilde{\mathfrak{p}}}$. Indeed, $A[\pi] = A[T\sqrt{T}]$ and $B = A[\sqrt{T}]$. Since $\sqrt{T}$ is the unique prime over T, $A[\pi]_{\widetilde{\mathfrak{p}}} = A_T[T\sqrt{T}] \neq A_T[\sqrt{T}] = B_{\widetilde{\mathfrak{p}}}$. Also, note that $\mathrm{End}_k(\phi) = \mathbb{F}_q[\tau] \cong A[\sqrt{T}]$ is the maximal A-order in $\widetilde{F}$.

Example 2.12. 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 $\widetilde{m}(x) = x^6 + (\pi^2 + 1)x^3 + (\pi^4 - \pi^2 + 2)$. Hence, $[\widetilde{F} : K] = 6$, so $A[\pi]$ is not locally maximal at π.

Example 2.13. 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 $\widetilde{m}(x) = x^4 + 2x^3 + 2x^2 + (2\pi + 1)x + \pi^2 + \pi + 1$, so $[\widetilde{F} : K] = 4$. Thus,

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

so equality in Theorem 2.6 holds. In this case, $A[\pi]$ is maximal at π.

The next four examples show that the quantities in Proposition 2.5 are essentially independent of each other.

Example 2.14 (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 2.15 (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 2.16 (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 2.17 (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 is $x^2 + c\mathfrak{p} + c'\mathfrak{p}^2$, where $c, c' \in \mathbb{F}_q^\times$ are such that $c^2 - 4c'$ is not a square in $\mathbb{F}_q^\times$; see [16, 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 $e_K = 1$.

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.

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 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 $\psi_T = u_I \phi_T u_I^{-1}$, then ψ is a Drinfeld module over k of rank r and $u_I \colon \phi \to \psi$ is an isogeny. We denote $\psi = I * \phi$.

Let $D = \mathcal{E} \otimes_A F$ be the division 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

$$k\{\tau\}\, I \cap D = (k\{\tau\}\, I \cap D) \cap \mathcal{E} = k\{\tau\}\, I \cap (D \cap \mathcal{E}) = k\{\tau\}\, I \cap \mathcal{E}. \tag{1}$$

Definition 3.1. We say that I is a *kernel ideal* if $(k\{\tau\}\, I) \cap D = I$. This definition is the one in [18, 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 $\ker(u_I) \subseteq \ker(\alpha)$, and consequently $\ker(u_I) \subseteq \phi[I]$. 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 $\phi[I] \subseteq \ker(u_I)$. □

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 [17, 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 by Lemma 2.1.1 in [14] we have $u = wu_I$ for some $w \in k\{\tau\}$. 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

$$0 \longrightarrow T_{\mathfrak{l}}(\phi) \longrightarrow u_{\mathfrak{l}}^{-1}T_{\mathfrak{l}}(\psi) \longrightarrow \ker(u)_{\mathfrak{l}} \longrightarrow 0. \tag{2}$$

Following [14, (2.3.6)], we denote

$$H_{\mathfrak{l}}(\phi) = \mathrm{Hom}_{A_{\mathfrak{l}}}(T_{\mathfrak{l}}(\phi), A_{\mathfrak{l}}). \tag{3}$$

Taking the $A_{\mathfrak{l}}$-duals of (2), 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 $\{e_1, \ldots, e_n\}$ 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 omitted since it is fairly straightforward. □

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 $IH_{\mathfrak{l}}(\phi)$ and we have proved:

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

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 [14, 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 [14, 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

$$\begin{cases} \mathfrak{p}M_{\mathfrak{p}} \subseteq f_{\phi,\mathfrak{p}}(M_{\mathfrak{p}}) \subseteq M_{\mathfrak{p}}, \\ \dim_k(M_{\mathfrak{p}}/f_{\phi,\mathfrak{p}}(M_{\mathfrak{p}})) = 1. \end{cases} \tag{4}$$

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 $u_I(H_{\mathfrak{p}}(I*\phi)) = IH_{\mathfrak{p}}(\phi)$. □

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 have $I \subseteq J$, 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 $J \subseteq I$. □

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

Example 3.10. 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

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

We algorithmically compute, cf. [8], 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 [8, Example 4.12] implies that $\mathcal{E}_{\mathfrak{l}}$ is not Gorenstein.

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 $(T + 1)^2 \notin I$. This proves that 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 [17, 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, $(I * \phi)_T = u_I \phi_T u_I^{-1}$ and $(J * \phi)_T = u_J \phi_T u_J^{-1}$. We have

$$\begin{aligned} I * \phi \cong J * \phi \quad &\iff \quad c u_I \phi_T u_I^{-1} c^{-1} = u_J \phi_T u_J^{-1} && \text{for some } c \in k^\times \\ &\iff u_J^{-1} c u_I \in D \\ &\iff c u_I = u_J u && \text{for some } u \in D. \end{aligned}$$

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

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

□

Let

$$\mathcal{O}_I := \{g \in D \mid Ig \subseteq I\} \tag{5}$$

be the (right) order of I in D. The next lemma is the analogue of [17, 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_T in $k(\tau)$. Therefore,

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

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

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

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 $w(u_I \phi_T u_I^{-1})w^{-1} = u_I \phi_T u_I^{-1}$. This implies that $u_I^{-1} w u_I \in D$. We have

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

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 $\mathrm{End}_k(I * \phi) = u_I \mathcal{O}_I u_I^{-1}$. □

The next lemma is the analogue of [17, 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 $\alpha\mathcal{E}$. We have $k\{\tau\}\, \alpha\mathcal{E} = k\{\tau\}\, \alpha$. Suppose $u = g\alpha \in k\{\tau\}\, \alpha$ 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. We have

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

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 we have $I'J \subseteq IJ$. Multiplying both sides by $J^{-1} \subseteq D$, we get $I' \subseteq I$. Since $I \subseteq I'$, we have $I' = I$, so I is a kernel ideal. □

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 $A_{\mathfrak{l}}$-module of rank 1; cf. [4].

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. [8, 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. [8, 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

$$H_{\mathfrak{p}}(\phi) = H^c_{\mathfrak{p}}(\phi) \oplus H^{\text{ét}}_{\mathfrak{p}}(\phi) \tag{6}$$

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

$$D_{\mathfrak{p}} := D \otimes_F F_{\mathfrak{p}} = \bigoplus_{\nu|\mathfrak{p}} D_\nu, \tag{7}$$

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. [14, 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 [14, Corollary 2.5.8], the splitting (7) induces a compatible splitting $\mathcal{E}_{\mathfrak{p}} = \mathcal{E}_{\tilde{\mathfrak{p}}} \oplus \mathcal{E}'_{\mathfrak{p}}$ such that

$$\mathcal{E}_{\tilde{\mathfrak{p}}} \simeq \mathrm{End}(H^c_{\mathfrak{p}}(\phi)), \tag{8}$$

$$\mathcal{E}'_{\mathfrak{p}} \simeq \mathrm{End}(H^{\text{ét}}_{\mathfrak{p}}(\phi)) \simeq \mathrm{End}_{A_{\mathfrak{p}}[G_k]}(T_{\mathfrak{p}}(\phi)). \tag{9}$$

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 [18, Corollary, p. 164] we have 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 [8, Theorem 4.9] to (9) 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 place $\mathfrak{l}$ 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. □

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 [17, 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 [3, 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 [18, 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. (5)), 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 (3), 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 index $\chi := \chi(R^*_{\mathfrak{l}_1}/(H_{\mathfrak{l}_1}(\phi_0) \cap R^*_{\mathfrak{l}_1}))$, which is a product of non-zero A-ideals. We have

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

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 $D_{\mathfrak{p}} = \oplus_{\nu|\mathfrak{p}} D_\nu = D_{\tilde{\mathfrak{p}}} \oplus (\oplus_{\nu \neq \tilde{\mathfrak{p}}} D_\nu) =: D_{\tilde{\mathfrak{p}}} \oplus D'_{\mathfrak{p}}$, cf. (7). In this case, we have that 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. [14, 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 [18, Corollary, p. 164], $\mathrm{End}_k(\psi)$ is locally maximal at π, so we also have $\mathrm{End}_k(\psi)_{\tilde{\mathfrak{p}}} = R_{\tilde{\mathfrak{p}}}$. □

Corollary 5.2. *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 2.10 states that $A[\pi]$ is locally maximal at π if and only if either ϕ is ordinary or $k = \mathbb{F}_{\mathfrak{p}}$. □

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 $\psi_T = u_I \phi_T u_I^{-1}$ 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 5.3. *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 [17, 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 (4) 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 (6) and their compatibility in (8) and (9), 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 [18, 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 5.4. *Suppose that $\mathcal{E} = A[\pi]$ (so that either ϕ is ordinary or $k = \mathbb{F}_{\mathfrak{p}}$, by Lemma 5.2). 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. Since $A[\pi]$ is Gorenstein (cf. [8, Proposition 4.10]), every $A[\pi]$-ideal is a kernel ideal by Proposition 4.5. The statement now follows from Theorem 5.3 since every endomorphism ring is an overorder of $A[\pi]$; note that all such overorders occur as endomorphism rings by Proposition 5.1. □

Remark 5.5.
(1) The ideal action already appears in [11, 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 5.3 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 [10, §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.

(3) The problem of describing endomorphism rings of Drinfeld modules has been considered by several authors, see e.g. [1, 9, 18]. Explicit algorithms to compute endomorphism rings were developed in [7] for Drinfeld modules of rank 2 over $\mathbb{F}_{\mathfrak{p}}$ and in [8] for any Drinfeld module with commutative endomorphism algebra; in [12], the existence of an effective general algorithm is shown.

6. 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 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 [6], 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 a analytic uniformization by a lattice $\Lambda \subseteq \mathbb{C}_\infty$ (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 Picard group 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 $\chi(\Lambda/\mathcal{E})\Lambda \trianglelefteq \mathcal{E}$. One can

show that if $u_I : \phi \to I * \phi$ 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, like 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 [5], 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 2.9 and Lemma 5.2. 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 [5, Theorem 25]. Essential surjectivity follows from the main result in [13], 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 $\phi_T = u_I(\phi_w)_T u_I^{-1}$ for $u_I \in k\{\tau\}$ with $k\{\tau\}I = k\{\tau\}u_I$. Then, using that $A[\pi] = \mathrm{End}_k(\phi_w) = \{v \in k\{\tau\} : v(\phi_w)_T = (\phi_w)_T v\}$, we see that

$$\begin{aligned}
\mathrm{Hom}_k(\phi, \phi_w) &= \{u \in k\{\tau\} : u\phi_T = (\phi_w)_T u\} \\
&= \{u \in k\{\tau\} : uu_I(\phi_w)_T = (\phi_w)_T uu_I\} \\
&= \{u \in k\{\tau\} : uu_I \in A[\pi]\} \\
&= k\{\tau\}u_I \cap A[\pi] = I,
\end{aligned}$$

where the last equality follows from the definition of a kernel ideal, see Definition 3.1 above and cf. Equation (1). This shows that the two constructions are in fact equivalent for Drinfeld modules.

References

[1] Bruno Angles, *On some subrings of Ore polynomials connected with finite Drinfeld modules*, J. Algebra **181** (1996), no. 2, 507–522.

[2] Sedric Nkotto Nkung Assong, *Explicit description of isogeny and isomorphism classes of Drinfeld modules over finite field*, arXiv e-prints (2020), arXiv:2009.02533.

[3] ———, *Orders occurring as endomorphism ring of a Drinfeld module in some isogeny classes of Drinfeld modules of higher ranks*, arXiv e-prints (2020), arXiv:2009.11578.

[4] Hyman Bass, *On the ubiquity of Gorenstein rings*, Math. Z. **82** (1963), 8–28.

[5] Tommaso Giorgio Centeleghe and Jakob Stix, *Categories of abelian varieties over finite fields, I: Abelian varieties over* $\mathbb{F}_p$, Algebra Number Theory **9** (2015), no. 1, 225–265.

[6] Pierre Deligne, *Variétés abéliennes ordinaires sur un corps fini*, Invent. Math. **8** (1969), 238–243.

[7] Sumita Garai and Mihran Papikian, *Endomorphism rings of reductions of Drinfeld modules*, J. Number Theory **212** (2020), 18–39.

[8] ———, *Computing endomorphism rings and Frobenius matrices of Drinfeld modules*, J. Number Theory **237** (2022), 145–164.

[9] Ernst-Ulrich Gekeler, *On finite Drinfeld modules*, J. Algebra **141** (1991), no. 1, 187–203.

[10] ———, *Frobenius distributions of Drinfeld modules over finite fields*, Trans. Amer. Math. Soc. **360** (2008), no. 4, 1695–1721.

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

[12] Nikolas Kuhn and Richard Pink, *Finding endomorphisms of Drinfeld modules*, J. Number Theory **232** (2022), 118–154.

[13] Claiborne G. Latimer and Cyrus C. MacDuffee, *A correspondence between classes of ideals and classes of matrices*, Ann. of Math. (2) **34** (1933), 313–316.

[14] Gérard Laumon, *Cohomology of Drinfeld modular varieties. Part I*, Cambridge Studies in Advanced Mathematics, vol. 41, Cambridge University Press, Cambridge, 1996.

[15] Stefano Marseglia, *Computing the ideal class monoid of an order*, J. Lond. Math. Soc. (2) **101** (2020), no. 3, 984–1007.

[16] Mihran Papikian, *Drinfeld modules*, Graduate Texts in Mathematics, vol. 296, Springer-Verlag, New York, 2023, to appear.

[17] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560.

[18] Jiu-Kang Yu, *Isogenies of Drinfeld modules over finite fields*, J. Number Theory **54** (1995), no. 1, 161–171.

Mathematical Institute, Utrecht University, Utrecht, The Netherlands
Email address: V.Z.Karemaker@uu.nl

Department of Mathematics, Pennsylvania State University, University Park, Pennsylvania, United States of America
Email address: jmk1097@psu.edu

Department of Mathematics, Pennsylvania State University, University Park, Pennsylvania, United States of America
Email address: papikian@psu.edu