Journal
de Théorie des Nombres
de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Alina Carmen COJOCARU et Nathan JONES

Degree bounds for projective division fields associated to elliptic modules with a trivial endomorphism ring

Tome 33, n^{o} 1 (2021), p. 95-106.

<http://jtnb.centre-mersenne.org/item?id=JTNB_2021__33_1_95_0>

Journal de Théorie des Nombres de Bordeaux **33** (2021), 95–106

Degree bounds for projective division fields associated to elliptic modules with a trivial endomorphism ring

par Alina Carmen COJOCARU et Nathan JONES

Résumé. Soient k un corps global, A un anneau de Dedekind avec $\mathrm{Quot}(A) = k$ et K un corps de type fini. Pour les courbes elliptiques et les modules de Drinfeld M définis sur K et ayant un anneau d'endomorphismes trivial (où $k = \mathbb{Q}$ et $A = \mathbb{Z}$ dans le premier cas et k est un corps de fonctions global et A son anneau des fonctions régulières en dehors d'un idéal premier fixé dans le second cas), nous nous intéressons au sous-corps engendré par les points de $\mathfrak{a}$-torsion associé à un idéal non nul $\mathfrak{a} \lhd A$ et à son sous-corps maximal fixé par les automorphismes scalaires. En utilisant une approche unifiée, nous prouvons les meilleures estimations possibles pour le degré de ce dernier corps sur K en termes de la norme $|\mathfrak{a}|$.

Abstract. Let k be a global field, let A be a Dedekind domain with $\mathrm{Quot}(A) = k$, and let K be a finitely generated field. Using a unified approach for both elliptic curves and Drinfeld modules M that are defined over K and that have a trivial endomorphism ring, with $k = \mathbb{Q}$, $A = \mathbb{Z}$ in the former case and with k a global function field, A its ring of functions regular away from a fixed prime in the latter case, we prove, for any nonzero ideal $\mathfrak{a} \lhd A$, best possible estimates in the norm $|\mathfrak{a}|$ for the degree over K of the subfield of the $\mathfrak{a}$-division field of M fixed by the scalars.

1. Introduction

In the theory of elliptic modules (elliptic curves and Drinfeld modules) division fields play a fundamental role; their algebraic properties (e.g., ramification, degree, and Galois group structure) are intimately related to properties of Galois representations and are essential to global and local questions about elliptic modules themselves. Among the subfields of

Manuscrit reçu le 24 février 2020, révisé le 17 octobre 2020, accepté le 12 décembre 2020.

2010 *Mathematics Subject Classification.* 11G05, 11G09, 11F80.

Mots-clefs. Elliptic curves, Drinfeld modules, division fields, Galois representations.

A.C.C. was partially supported by a Collaboration Grant for Mathematicians from the Simons Foundation under Award No. 318454.

the division fields of an elliptic module, those fixed by the scalars are of special significance. For example, as highlighted in [1, Chapter 5] and [5, Section 3], in the case of an elliptic curve E defined over $\mathbb{Q}$ and a positive integer a, the subfield J_a of the a-division field $\mathbb{Q}(E[a])$ fixed by the scalars of $\mathrm{Gal}(\mathbb{Q}(E[a]/\mathbb{Q})) \leq \mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z})$ is closely related to the modular curve $X_0(a)$ which parametrizes cyclic isogenies of degree a between elliptic curves; indeed, J_a may be interpreted as the splitting field of the modular polynomial $\Phi_a(X, j(E))$ (see [16, Section 69] and [9, Section 11.C] for the properties of the modular polynomials $\Phi_a(X, Y)$). The arithmetic properties of the family of fields $(J_a)_{a\geq 1}$ are closely related to properties of the reductions $E(\mathrm{mod}\, p)$ of E modulo primes p, including the growth of the order of the Tate–Shafarevich group of the curve $E(\mathrm{mod}\, p)$ when viewed as constant over its own function field (see [5]) and the growth of the absolute discriminant of the endomorphism ring of the curve $E(\mathrm{mod}\, p)$ when viewed over the finite field $\mathbb{F}_p$ (see [6]). An essential ingredient when deriving properties about $E(\mathrm{mod}\, p)$ from the fields J_a is the growth of the degrees $[J_a : \mathbb{Q}]$. The goal of this article is to prove best possible estimates in a for the degrees of such fields in the unified setting of elliptic curves and Drinfeld modules with a trivial endomorphism ring.

To state our main result, we proceed as in [2, pp. 1–2] and fix: k a global field, A a Dedekind domain with $\mathrm{Quot}(A) = k$, K a finitely generated field (i.e. K is finitely generated over its prime field), and M a (G_K, A)-module of rank $r \geq 2$, where $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ denotes the absolute Galois group of K. Specifically, by definition, a (G_K, A)-module of rank $r \geq 2$ is an A-module M endowed with a continuous G_K-action that commutes with the A-action and having the property that, for any ideal $0 \neq \mathfrak{a} \lhd A$, the $\mathfrak{a}$-division submodule $M[\mathfrak{a}] := \{x \in M : \alpha x = 0 \ \ \forall\, \alpha \in \mathfrak{a}\}$ has A-module structure $M[\mathfrak{a}] \simeq_A (A/\mathfrak{a})^r$.

The (G_K, A)-module structure on M gives rise to a compatible system of Galois representations $\rho_{\mathfrak{a}} : G_K \to \mathrm{GL}_r(A/\mathfrak{a})$ and to a continuous representation $\rho : G_K \to \mathrm{GL}_r(\widehat{A})$, where $\widehat{A} := \varprojlim_{\mathfrak{a}\lhd A} A/\mathfrak{a}$. Associated to these representations we have the $\mathfrak{a}$-division fields $K_{\mathfrak{a}} := (K^{\mathrm{sep}})^{\mathrm{Ker}\,\rho_{\mathfrak{a}}}$, for which we distinguish the subfields $J_{\mathfrak{a}}$ fixed by the scalars $\{\lambda I_r : \lambda \in (A/\mathfrak{a})^\times\} \cap \mathrm{Gal}(K_{\mathfrak{a}}/K)\}$ (with $\mathrm{Gal}(K_{\mathfrak{a}}/K)$ viewed as a subgroup of $\mathrm{GL}_r(A/\mathfrak{a})$).

Denoting by $\widehat{\rho}_{\mathfrak{a}} : G_K \to \mathrm{PGL}_r(A/\mathfrak{a})$ the composition of the representation $\rho_{\mathfrak{a}}$ with the canonical projection $\mathrm{GL}_r(A/\mathfrak{a}) \to \mathrm{PGL}_r(A/\mathfrak{a})$, we observe that $J_{\mathfrak{a}} = (K^{\mathrm{sep}})^{\mathrm{Ker}\,\hat{\rho}_{\mathfrak{a}}}$ and we deduce that

$$[J_{\mathfrak{a}} : K] \leq |\mathrm{PGL}_r(A/\mathfrak{a})|\,.$$

Our main result provides a lower bound for $[J_{\mathfrak{a}} : K]$ of the same order of growth as $|\mathrm{PGL}_r(A/\mathfrak{a})|$, as follows:

Theorem 1.1. *We keep the above setting and assume that*

$$|\mathrm{GL}_r(\widehat{A}) : \rho(G_K)| < \infty. \tag{1.1}$$

Then, for any ideal $0 \neq \mathfrak{a} \lhd A$,

$$|\mathfrak{a}|^{r^2-1} \ll_{M,K} [J_{\mathfrak{a}} : K] \leq |\mathfrak{a}|^{r^2-1}, \tag{1.2}$$

where $|\mathfrak{a}| := |A/\mathfrak{a}|$.

By specializing the above general setting to elliptic curves and to Drinfeld modules, we obtain:

Corollary 1.2. *Let K be a finitely generated field with* $\mathrm{char}\, K = 0$ *and let E/K be an elliptic curve over K with* $\mathrm{End}_{\overline{K}}(E) \simeq \mathbb{Z}$. *Then, for any integer $a \geq 1$, the degree $[J_a : K]$ of the subfield J_a of the a-division field $K_a := K(E[a])$ fixed by the scalars of* $\mathrm{Gal}(K(E[a])/K)$ *satisfies*

$$a^3 \ll_{E,K} [J_a : K] \leq a^3. \tag{1.3}$$

Corollary 1.3. *Let k be a global function field, let ∞ be a fixed place of k, let A be the ring of elements of k regular away from ∞, let K be a finitely generated field which is also an A-field with A-*$\mathrm{char}\, K = 0$ *(i.e. $k \subseteq K$), and let $\psi : A \to K\{\tau\}$ be a (generic) Drinfeld A-module over K of rank $r \geq 2$ with* $\mathrm{End}_{\overline{K}}(\psi) \simeq A$. *Then, for any ideal* $0 \neq \mathfrak{a} \lhd A$, *the degree* $[J_{\mathfrak{a}} : K]$ *of the subfield $J_{\mathfrak{a}}$ of the $\mathfrak{a}$-division field $K_{\mathfrak{a}} := K(\psi[\mathfrak{a}])$ fixed by the scalars of* $\mathrm{Gal}(K(\psi[\mathfrak{a}])/K)$ *satisfies*

$$|\mathfrak{a}|^{r^2-1} \ll_{\psi,K} [J_{\mathfrak{a}} : K] \leq |\mathfrak{a}|^{r^2-1}. \tag{1.4}$$

The proof of Theorem 1.1 relies on consequences of assumption (1.1), on applications of Goursat's Lemma, as well as on vertical growth estimates for open subgroups of GL_r. Specializing to elliptic curves and to Drinfeld modules, assumption (1.1) is essentially Serre's Open Image Theorem [15] and, respectively, Pink–Rütsche's Open Image Theorem [13]. Variations of these open image theorems also hold for elliptic curves and Drinfeld modules with nontrivial endomorphism rings. While these complementary cases are treated unitarily in [2] when investigating the growth of torsion, when investigating the growth of $[J_{\mathfrak{a}} : K]$ they face particularities whose treatment we relegate to future work.

We emphasize that the upper bound in Theorem 1.1 always holds and does not necessitate assumption (1.1). In contrast, the lower bound in Theorem 1.1 is intimately related to assumption (1.1). Indeed, one consequence of (1.1) is that there exists an ideal $\mathfrak{a}(M, K) \unlhd A$, which (a priori) depends on M and K and which has the property that, for any prime ideal $\mathfrak{l} \nmid \mathfrak{a}(M, K)$, $\mathrm{Gal}(J_{\mathfrak{l}}/K) \simeq \mathrm{PGL}_r(A/\mathfrak{l})$. Then, for such an ideal $\mathfrak{l}$, the lower bound in (1.2) follows immediately. The purpose of Theorem 1.1 is to prove similar lower bounds for *all* ideals $\mathfrak{a} \lhd A$.

The dependence of the lower bound in (1.2) on M (which also includes dependence on r) and on K is an important topic related to the uniform boundedness of the torsion of M; while we do not address it in the present paper, we refer the reader to [2] and [12] for related discussions and for additional references.

The fields $J_{\mathfrak{a}}$ play a prominent role in a multitude of problems, such as in deriving non-trivial upper bounds for the number of non-isomorphic Frobenius fields associated to an elliptic curve and, respectively, to a Drinfeld module (see [3] and [4]); in investigating the discriminants of the endomorphism rings of the reduction of an elliptic curve and, respectively, of a Drinfeld module (see [6] and [8]); and in proving non-abelian reciprocity laws for primes and, respectively, for irreducible polynomials (see [7], [10], and [11]). For such applications, an essential piece of information is the growth of the degree $[J_{\mathfrak{a}} : K]$ as a function of the norm $|\mathfrak{a}|$. For example, Corollary 1.2 is a key ingredient in proving that, for any elliptic curve $E/\mathbb{Q}$ with $\operatorname{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$, provided the Generalized Riemann Hypothesis holds for the division fields of E, there exists a set of primes p of natural density 1 with the property that the absolute discriminant of the imaginary quadratic order $\operatorname{End}_{\mathbb{F}_p}(E)$ is as close as possible to its natural upper bound; see [6, Theorem 1]. Similarly, Corollary 1.3 is a key ingredient in proving that, denoting by $\mathbb{F}_q$ the finite field with q elements and assuming that q is odd, for any generic Drinfeld module $\psi : \mathbb{F}_q[T] \to \mathbb{F}_q(T)\{\tau\}$ of rank 2 and with $\operatorname{End}_{\overline{\mathbb{F}_q(T)}}(\psi) \simeq \mathbb{F}_q[T]$, there exists a set of prime ideals $\mathfrak{p} \lhd \mathbb{F}_q[T]$ of Dirichlet density 1 with the property that the norm of the discriminant of the imaginary quadratic order $\operatorname{End}_{\mathbb{F}_{\mathfrak{p}}}(\psi)$ is as close as possible to its natural upper bound; see [8, Theorem 6]. We expect that Theorem 1.1 will be of use to other arithmetic studies of elliptic modules.

Notation. In what follows, we use the standard $\ll$, $\gg$, and $\asymp$ notation: given suitably defined real functions h_1, h_2, we say that $h_1 \ll h_2$ or $h_2 \gg h_1$ if h_2 is positive valued and there exists a positive constant C such that $|h_1(x)| \leq Ch_2(x)$ for all x in the domain of h_1; we say that $h_1 \asymp h_2$ if h_1, h_2 are positive valued and $h_1 \ll h_2 \ll h_1$; we say that $h_1 \ll_D h_2$ or $h_2 \gg_D h_1$ if $h_1 \ll h_2$ and the implied $\ll$-constant C depends on priorly given data D; similarly, we say that $h_1 \asymp_D h_2$ if the implied constant in either one of the $\ll$-bounds $h_1 \ll h_2 \ll h_1$ depends on priorly given data D. We also use the standard divisibility notation for ideals in a Dedekind domain. In particular, given two ideals $\mathfrak{a}$, $\mathfrak{b}$, we write $\mathfrak{a} \mid \mathfrak{b}^{\infty}$ if all the prime ideal factors of $\mathfrak{a}$ are among the prime ideal factors of $\mathfrak{b}$ (with possibly different exponents). Further notation will be introduced over the course of the paper as needed.

2. Goursat's Lemma and variations

In this section we recall Goursat's Lemma on fibered products of groups (whose definition we also recall shortly) and detail the behavior of such fibered products under intersection.

Lemma 2.1 (Goursat's Lemma)**.** *Let G_1, G_2 be groups and for $i \in \{1,2\}$ denote by $\pi_i : G_1 \times G_2 \to G_i$ the projection map onto the i-th factor. Let $G \le G_1 \times G_2$ be a subgroup and assume that $\pi_1(G) = G_1$, $\pi_2(G) = G_2$. Then there exist a group Γ and a pair of surjective group homomorphisms $\psi_1 : G_1 \to \Gamma$, $\psi_2 : G_2 \to \Gamma$ such that*

$$G = G_1 \times_\psi G_2 := \{(g_1, g_2) \in G_1 \times G_2 : \psi_1(g_1) = \psi_2(g_2)\}.$$

Proof. See [14, Lemma 5.2.1]. □

We call $G_1 \times_\psi G_2$ the *fibered product of* G_1 *and* G_2 *over* $\psi := (\psi_1, \psi_2)$. The next lemma details what happens when we intersect such a fibered product with a subgroup of the form $H_1 \times H_2$ defined by subgroups $H_1 \le G_1$ and $H_2 \le G_2$.

It is clear that

$$\begin{aligned}&(H_1 \times H_2) \cap (G_1 \times_\psi G_2)\\ &\qquad\qquad = H_1 \times_\psi H_2 := \{(h_1, h_2) \in H_1 \times H_2 : \psi_1(h_1) = \psi_2(h_2)\}.\end{aligned}$$

However, this representation does not specify the restricted common quotient inside Γ. In particular, it can be the case that the fibered product $H := H_1 \times_\psi H_2$ does *not* satisfy $\pi_i(H) = H_i$ for each $i \in \{1,2\}$. The following lemma clarifies this situation.

Lemma 2.2. *Let G_1, G_2 be groups, let $\psi_1 : G_1 \to \Gamma$, $\psi_2 : G_2 \to \Gamma$ be surjective group homomorphisms onto a group Γ, and let $G_1 \times_\psi G_2$ be the associated fibered product. Furthermore, let $H_1 \le G_1$, $H_2 \le G_2$ be subgroups. Define the subgroup*

$$\Gamma_H := \psi_1(H_1) \cap \psi_2(H_2) \le \Gamma.$$

Then

$$(H_1 \times H_2) \cap (G_1 \times_\psi G_2) = \big(H_1 \cap \psi_1^{-1}(\Gamma_H)\big) \times_\psi \big(H_2 \cap \psi_2^{-1}(\Gamma_H)\big) \tag{2.1}$$

and the canonical projection maps

$$\begin{aligned}\pi_1 &: (H_1 \cap \psi_1^{-1}(\Gamma_H)) \times_\psi (H_2 \cap \psi_2^{-1}(\Gamma_H)) \longrightarrow H_1 \cap \psi_1^{-1}(\Gamma_H),\\ \pi_2 &: (H_1 \cap \psi_1^{-1}(\Gamma_H)) \times_\psi (H_2 \cap \psi_2^{-1}(\Gamma_H)) \longrightarrow H_2 \cap \psi_2^{-1}(\Gamma_H)\end{aligned}$$

are surjective.

Proof. We first establish (2.1). Since the containment "$\supseteq$" is immediate, we only need to establish "$\subseteq$." Let $(h_1, h_2) \in (H_1 \times H_2) \cap (G_1 \times_\psi G_2)$, i.e. $h_1 \in H_1$, $h_2 \in H_2$, and $\psi_1(h_1) = \psi_2(h_2)$. From the definition of Γ_H, it follows that

$\psi_1(h_1) = \psi_2(h_2) \in \Gamma_H$. Thus $(h_1, h_2) \in (H_1 \cap \psi_1^{-1}(\Gamma_H)) \times_\psi (H_2 \cap \psi_2^{-1}(\Gamma_H))$, establishing (2.1).

To see why the projection map

$$\pi_1 : H_1 \cap \psi_i^{-1}(\Gamma_H) \longrightarrow H_1 \cap \psi_1^{-1}(\Gamma_H) \tag{2.2}$$

is surjective, fix $h_1 \in H_1 \cap \psi_1^{-1}(\Gamma_H)$ and set $\gamma := \psi_1(h_1) \in \Gamma_H$. By the definition of Γ_H, we find $h_2 \in H_2$ with $\psi_2(h_2) = \gamma$. Thus $(h_1, h_2) \in (H_1 \cap \psi_1^{-1}(\Gamma_H)) \times_\psi (H_2 \cap \psi_2^{-1}(\Gamma_H))$ and $\pi_1(h_1, h_2) = h_1$, proving the surjectivity of π_1 in (2.2). The surjectivity of π_2 is proved similarly. □

3. Proof of Theorem 1.1

In this section we prove Theorem 1.1. We will make use of the following notation:

$$G := \rho(G_K) \leq \mathrm{GL}_r(\widehat{A});$$

for any ideal $0 \neq \mathfrak{a} \lhd A$, we write

$$G(\mathfrak{a}) := \rho_{\mathfrak{a}}(G_K) \leq \mathrm{GL}_r(A/\mathfrak{a});$$

for any subgroup $H \leq \mathrm{GL}_r(A/\mathfrak{a})$, we write

$$\mathrm{Scal}_H := H \cap \{\alpha I_r : \alpha \in (A/\mathfrak{a})^\times\}.$$

With this notation, we see that $J_{\mathfrak{a}} = K(E[\mathfrak{a}])^{\mathrm{Scal}_{G(\mathfrak{a})}}$.

To prove the theorem, let $0 \neq \mathfrak{a} \lhd A$ be a fixed arbitrary ideal. The proof of the upper bound is an immediate consequence to the injection $\mathrm{Gal}(J_{\mathfrak{a}}/K) \hookrightarrow \mathrm{PGL}_r(A/\mathfrak{a})$ defined by $\widehat{\rho}_{\mathfrak{a}}$. Indeed, using that

$$|\mathrm{PGL}_r(A/\mathfrak{a})| = \frac{1}{|(A/\mathfrak{a})^\times|} |\mathrm{GL}_r(A/\mathfrak{a})|,$$

$$|(A/\mathfrak{a})^\times| = |\mathfrak{a}| \prod_{\mathfrak{p}|\mathfrak{a}} \left(1 - \frac{1}{|\mathfrak{p}|}\right),$$

and

$$|\mathrm{GL}_r(A/\mathfrak{a})| = |\mathfrak{a}|^{r^2} \prod_{\substack{\mathfrak{p}|\mathfrak{a} \\ \mathfrak{p} \text{ prime}}} \left(1 - \frac{1}{|\mathfrak{p}|}\right)\left(1 - \frac{1}{|\mathfrak{p}|^2}\right) \dots \left(1 - \frac{1}{|\mathfrak{p}|^r}\right)$$

(see [2, Lemma 2.3, p. 1244] for the latter), we obtain that

$$[J_{\mathfrak{a}} : K] \leq |\mathrm{PGL}_r(A/\mathfrak{a})| = |\mathfrak{a}|^{r^2-1} \prod_{\substack{\mathfrak{p}|\mathfrak{a} \\ \mathfrak{p} \text{ prime}}} \left(1 - \frac{1}{|\mathfrak{p}|^2}\right) \dots \left(1 - \frac{1}{|\mathfrak{p}|^r}\right) \leq |\mathfrak{a}|^{r^2-1}.$$

The proof of the lower bound relies on several consequences to assumption (1.1), as well as on applications of Goursat's Lemma 2.1 and its variation Lemma 2.2, as detailed below.

Thanks to (1.1), there exists an ideal $\mathfrak{m} = \mathfrak{m}_{M,K} \trianglelefteq A$ such that

$$G = \pi^{-1}(G(\mathfrak{m})), \tag{3.1}$$

where $\pi : \mathrm{GL}_r(\widehat{A}) \to \mathrm{GL}_r(A/\mathfrak{m})$ is the canonical projection. We take $\mathfrak{m}$ to be the smallest such ideal with respect to divisibility and we write its unique prime ideal factorization as $\mathfrak{m} = \prod_{\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})} \| \mathfrak{m}} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})}$, where each exponent satisfies $v_\mathfrak{p}(\mathfrak{m}) \geq 1$.

With the ideal $\mathfrak{m}$ in mind, we write the arbitrary ideal $\mathfrak{a}$ uniquely as

$$\mathfrak{a} = \mathfrak{a}_1 \mathfrak{a}_2, \tag{3.2}$$

where

$$\mathfrak{a}_1 \mid \mathfrak{m}^\infty, \tag{3.3}$$

$$\gcd(\mathfrak{a}_2, \mathfrak{m}) = 1. \tag{3.4}$$

For future use, we record that

$$\gcd(\mathfrak{a}_1, \mathfrak{a}_2) = 1. \tag{3.5}$$

We also write the ideal $\mathfrak{a}_1$ uniquely as

$$\mathfrak{a}_1 = \mathfrak{a}_{1,1}\ \mathfrak{a}_{1,2},$$

where $\mathfrak{a}_{1,1} = \prod_{\substack{\mathfrak{p}^{e_\mathfrak{p}} \| \mathfrak{a}_1 \\ e_\mathfrak{p} > v_\mathfrak{p}(\mathfrak{m})}} \mathfrak{p}^{e_\mathfrak{p}}$ and $\mathfrak{a}_{1,2} = \prod_{\substack{\mathfrak{p}^{f_\mathfrak{p}} \| \mathfrak{a}_1 \\ f_\mathfrak{p} \leq v_\mathfrak{p}(\mathfrak{m})}} \mathfrak{p}^{f_\mathfrak{p}}$. Note that

$$\gcd(\mathfrak{a}_{1,1}, \mathfrak{a}_{1,2}) = 1, \tag{3.6}$$

$$\mathfrak{a}_{1,1} \mid \mathfrak{m}^\infty \tag{3.7}$$

and

$$\mathfrak{a}_{1,2} \mid \mathfrak{m}. \tag{3.8}$$

Under the isomorphism of the Chinese Remainder Theorem, we deduce from (3.1) that

$$G(\mathfrak{a}) \simeq G(\mathfrak{a}_1) \times \mathrm{GL}_r(A/\mathfrak{a}_2) \tag{3.9}$$

and, consequently, that there exist group isomorphisms

$$\mathrm{Scal}_{G(\mathfrak{a})} \simeq \mathrm{Scal}_{G(\mathfrak{a}_1)} \times \mathrm{Scal}_{\mathrm{GL}_r(A/\mathfrak{a}_2)}, \tag{3.10}$$

$$G(\mathfrak{a})/\,\mathrm{Scal}_{G(\mathfrak{a})} \simeq (G(\mathfrak{a}_1)/\,\mathrm{Scal}_{G(\mathfrak{a}_1)}) \times \mathrm{PGL}_r(A/\mathfrak{a}_2). \tag{3.11}$$

Next, applying Lemma 2.1 to the groups $G = G(\mathfrak{a}_1)$, $G_1 = G(\mathfrak{a}_{1,1})$, and $G_2 = G(\mathfrak{a}_{1,2})$, we deduce that there exist a group Γ and surjective group homomorphisms $\psi_1 : G(\mathfrak{a}_{1,1}) \to \Gamma$, $\psi_2 : G(\mathfrak{a}_{1,2}) \to \Gamma$, which give rise to a group isomorphism

$$G(\mathfrak{a}_1) \simeq G(\mathfrak{a}_{1,1}) \times_\psi G(\mathfrak{a}_{1,2}). \tag{3.12}$$

Furthermore, applying Lemma 2.2 to the subgroups $H_1 = \operatorname{Scal}_{G(\mathfrak{a}_{1,1})}$ and $H_2 = \operatorname{Scal}_{G(\mathfrak{a}_{1,2})}$, we deduce that there exists a group isomorphism

$$\begin{aligned}(3.13)\quad &(\operatorname{Scal}_{G(\mathfrak{a}_{1,1})} \times \operatorname{Scal}_{G(\mathfrak{a}_{1,2})}) \cap (G(\mathfrak{a}_{1,1}) \times_\psi G(\mathfrak{a}_{1,2})) \\ &\qquad \simeq (\operatorname{Scal}_{G(\mathfrak{a}_{1,1})} \cap \psi_1^{-1}(\Gamma_{\mathrm{Scal}})) \times_\psi (\operatorname{Scal}_{G(\mathfrak{a}_{1,2})} \cap \psi_2^{-1}(\Gamma_{\mathrm{Scal}})),\end{aligned}$$

where

$$\Gamma_{\mathrm{Scal}} := \psi_1(\operatorname{Scal}_{G(\mathfrak{a}_{1,1})}) \cap \psi_1(\operatorname{Scal}_{G(\mathfrak{a}_{1,2})}) \leq \Gamma.$$

From (3.11) we derive that

$$(3.14)\quad [J_{\mathfrak{a}} : K] = \left|G(\mathfrak{a})/\operatorname{Scal}_{G(\mathfrak{a})}\right| = \left|G(\mathfrak{a}_1)/\operatorname{Scal}_{G(\mathfrak{a}_1)}\right| \cdot \left|\mathrm{PGL}_r(A/\mathfrak{a}_2)\right|.$$

Then, using (3.12) and (3.13), we derive that

$$\begin{aligned}&\left|G(\mathfrak{a}_1)/\operatorname{Scal}_{G(\mathfrak{a}_1)}\right| \\ &\quad = \frac{\left|G(\mathfrak{a}_{1,1}) \times_\psi G(\mathfrak{a}_{1,2})\right|}{\left|(\operatorname{Scal}_{G(\mathfrak{a}_{1,1})} \times \operatorname{Scal}_{G(\mathfrak{a}_{1,2})}) \cap G(\mathfrak{a}_1)\right|} \\ &\quad = \frac{\left|G(\mathfrak{a}_{1,1}) \times_\psi G(\mathfrak{a}_{1,2})\right|}{\left|(\operatorname{Scal}_{G(\mathfrak{a}_{1,1})} \cap \psi_1^{-1}(\Gamma_{\mathrm{Scal}})) \times_\psi (\operatorname{Scal}_{G(\mathfrak{a}_{1,2})} \cap \psi_2^{-1}(\Gamma_{\mathrm{Scal}}))\right|} \\ &\quad = \frac{\left|G(\mathfrak{a}_{1,1})\right|}{\left|\operatorname{Scal}_{G(\mathfrak{a}_{1,1})} \cap \psi_1^{-1}(\Gamma_{\mathrm{Scal}})\right|} \cdot \frac{\left|\Gamma_{\mathrm{Scal}}\right|}{|\Gamma|} \cdot \frac{\left|G(\mathfrak{a}_{1,2})\right|}{\left|\operatorname{Scal}_{G(\mathfrak{a}_{1,2})} \cap \psi_2^{-1}(\Gamma_{\mathrm{Scal}})\right|} \\ (3.15)\quad &\quad = \frac{\left|G(\mathfrak{a}_{1,1})\right|}{\left|\operatorname{Scal}_{G(\mathfrak{a}_{1,1})} \cap \psi_1^{-1}(\Gamma_{\mathrm{Scal}})\right|} \cdot \frac{\left|\psi_1(\operatorname{Scal}_{G(\mathfrak{a}_{1,1})}) \cap \psi_2(\operatorname{Scal}_{G(\mathfrak{a}_{1,2})})\right|}{|\Gamma|} \\ &\qquad\qquad \cdot \frac{\left|G(\mathfrak{a}_{1,2})\right|}{\left|\operatorname{Scal}_{G(\mathfrak{a}_{1,2})} \cap \psi_2^{-1}(\Gamma_{\mathrm{Scal}})\right|}.\end{aligned}$$

Recalling (3.8), we deduce that the last two factors above are bounded, from above and below, by constants depending on $\mathfrak{m}$, hence on M and K:

$$(3.16)\quad \frac{\left|\psi_1(\operatorname{Scal}_{G(\mathfrak{a}_{1,1})}) \cap \psi_2(\operatorname{Scal}_{G(\mathfrak{a}_{1,2})})\right|}{|\Gamma|} \cdot \frac{\left|G(\mathfrak{a}_{1,2})\right|}{\left|\operatorname{Scal}_{G(\mathfrak{a}_{1,2})} \cap \psi_2^{-1}(\Gamma_{\mathrm{Scal}})\right|} \asymp_{M,K} 1.$$

It remains to analyze the first factor in (3.15). For this, consider the canonical projection

$$\pi_{1,1} : \mathrm{GL}_r(A/\mathfrak{a}_{1,1}) \longrightarrow \mathrm{GL}_r(A/\gcd(\mathfrak{a}_{1,1}, \mathfrak{m}))$$

and, upon recalling (3.1), observe that

$$(3.17)\qquad G(\mathfrak{a}_{1,1}) = \pi_{1,1}^{-1}(G(\gcd(\mathfrak{a}_{1,1}, \mathfrak{m})))$$

and

$$(3.18)\qquad \operatorname{Ker} \pi_{1,1} \subseteq \operatorname{Ker} \psi_1.$$

Thus the subgroups $G(\mathfrak{a}_{1,1}) \leq \mathrm{GL}_r(A/\mathfrak{a}_{1,1})$ and $G(\gcd(\mathfrak{a}_{1,1}, \mathfrak{m})) \leq \mathrm{GL}_r(A/\gcd(\mathfrak{a}_{1,1}, \mathfrak{m}))$, together with the group Γ, fit into a commutative diagram

$$\begin{tikzcd}
G(\mathfrak{a}_{1,1}) \arrow[r, two heads, "\pi_{1,1}"] \arrow[dr, two heads, "\psi_1"'] & G(\gcd(\mathfrak{a}_{1,1}, \mathfrak{m})) \arrow[d, two heads, dashed, "\rho"] \\
 & \Gamma
\end{tikzcd}$$

in which the vertical map ρ is some surjective group homomorphism and the horizontal map $\pi_{1,1}|_{G(\mathfrak{a}_{1,1})}$ is $\left(\frac{|\mathfrak{a}_{1,1}|}{|\gcd(\mathfrak{a}_{1,1},\mathfrak{m})|}\right)^{r^2}$ to 1. Furthermore, the subgroups $\psi_1^{-1}(\Gamma_{\mathrm{Scal}}) \cap \mathrm{Scal}_{G(\mathfrak{a}_{1,1})} \leq \mathrm{Scal}_{\mathrm{GL}_r(A/\mathfrak{a}_{1,1})} \simeq (A/\mathfrak{a}_{1,1})^\times$ and $\rho^{-1}(\Gamma_{\mathrm{Scal}}) \cap \mathrm{Scal}_{G(\gcd(\mathfrak{a}_{1,1},\mathfrak{m}))} \leq \mathrm{Scal}_{\mathrm{GL}_r(A/\gcd(\mathfrak{a}_{1,1},\mathfrak{m}))} \simeq (A/\gcd(\mathfrak{a}_{1,1}, \mathfrak{m}))^\times$, together with the group Γ_{Scal}, fit into the commutative diagram

$$\begin{tikzcd}
\psi_1^{-1}(\Gamma_{\mathrm{Scal}}) \cap \mathrm{Scal}_{G(\mathfrak{a}_{1,1})} \arrow[r, two heads, "\pi_{1,1}"] \arrow[dr, two heads, "\psi_1"'] & \rho^{-1}(\Gamma_{\mathrm{Scal}}) \cap \mathrm{Scal}_{G(\gcd(\mathfrak{a}_{1,1},\mathfrak{m}))} \arrow[d, two heads, "\rho"] \\
 & \Gamma_{\mathrm{Scal}}
\end{tikzcd}$$

in which the horizontal map $\pi_{1,1}|_{\psi_1^{-1}(\Gamma_{\mathrm{Scal}})\cap\mathrm{Scal}_{G(\mathfrak{a}_{1,1})}}$ is $\frac{|\mathfrak{a}_{1,1}|}{|\gcd(\mathfrak{a}_{1,1},\mathfrak{m})|}$ to 1. We deduce that

$$(3.19) \qquad |G(\mathfrak{a}_{1,1})| = \left(\frac{|\mathfrak{a}_{1,1}|}{|\gcd(\mathfrak{a}_{1,1}, \mathfrak{m})|}\right)^{r^2} |G(\gcd(\mathfrak{a}_{1,1}, \mathfrak{m}))| \asymp_{M,K} |\mathfrak{a}_{1,1}|^{r^2}$$

and

$$(3.20) \quad \left|\psi_1^{-1}(\Gamma_{\mathrm{Scal}}) \cap \mathrm{Scal}_{G(\mathfrak{a}_{1,1})}\right| = \frac{|\mathfrak{a}_{1,1}|}{|\gcd(\mathfrak{a}_{1,1}, \mathfrak{m})|}\left|\rho^{-1}(\Gamma_{\mathrm{Scal}}) \cap \mathrm{Scal}_{G(\gcd(\mathfrak{a}_{1,1},\mathfrak{m}))}\right| \asymp_{M,K} |\mathfrak{a}_{1,1}|.$$

Putting together (3.14), (3.15), (3.16), (3.19), and (3.20), we obtain that

$$(3.21) \qquad [J_{\mathfrak{a}} : K] \asymp_K |\mathfrak{a}_{1,1}|^{r^2-1} \left|\mathrm{PGL}_r(A/\mathfrak{a}_2)\right|.$$

To conclude the proof, observe that

$$\begin{aligned}
\left|\mathrm{PGL}_r(A/\mathfrak{a}_2)\right| &= |\mathfrak{a}_2|^{r^2-1} \prod_{\substack{\mathfrak{p}|\mathfrak{a}_2 \\ \mathfrak{p} \text{ prime}}} \left(1 - \frac{1}{|\mathfrak{p}|^2}\right) \cdots \left(1 - \frac{1}{|\mathfrak{p}|^r}\right) \\
&\geq |\mathfrak{a}_2|^{r^2-1} \prod_{\substack{\mathfrak{p} \\ \mathfrak{p} \text{ prime}}} \left(1 - \frac{1}{|\mathfrak{p}|^2}\right) \cdots \left(1 - \frac{1}{|\mathfrak{p}|^r}\right) \\
&\gg_{r,K} |\mathfrak{a}_2|^{r^2-1},
\end{aligned}$$

which, combined with (3.21), (3.2) and (3.8), gives

$$[J_{\mathfrak{a}} : K] \asymp_K \frac{|\mathfrak{a}_1|^{r^2-1}}{|\mathfrak{a}_{1,2}|^{r^2-1}} |\mathrm{PGL}_r(A/\mathfrak{a}_2)| \gg_{r,K} \frac{|\mathfrak{a}_1\mathfrak{a}_2|^{r^2-1}}{|\mathfrak{a}_{1,2}|^{r^2-1}} \gg_{M,K} |\mathfrak{a}|^{r^2-1}.$$

4. Proof of Corollaries 1.2 and 1.3

First, consider the setting of Corollary 1.2: K is a finitely generated field with $\operatorname{char} K = 0$ and E/K is an elliptic curve over K with $\operatorname{End}_{\overline{K}}(E) \simeq \mathbb{Z}$. This is the specialization of the setting of Theorem 1.1 to $k = \mathbb{Q}$, $A = \mathbb{Z}$, K as above, and $M = E(\overline{K})$, as we now explain.

We recall that an elliptic curve E/K is a smooth, projective curve over K, of genus 1, and with a given K-rational point that we call $\mathcal{O}$. From the theory of elliptic curves, we know that the set $E(\overline{K})$ of $\overline{K}$-rational points on E has a $\mathbb{Z}$-module structure and is endowed with a continuous G_K-action that commutes with the $\mathbb{Z}$-action. We also know that, for any non-zero integer a, the set of a-division points on E, $E[a] := \{P \in E(\overline{K}) : aP = \mathcal{O}\}$, is a $\mathbb{Z}$-module satisfying the $\mathbb{Z}$-module isomorphism $E[a] \simeq_{\mathbb{Z}} (\mathbb{Z}/a\mathbb{Z})^2$. Thus, the elliptic curve E/K gives rise to a $(G_K, \mathbb{Z})$-module $E(\overline{K})$ of rank 2, in the sense of Breuer's definition given in [2, pp. 1–2]. In this setting, assumption (1.1) of Theorem 1.1 holds thanks to an extension of Serre's Open Image Theorem for non-CM elliptic curves over number fields [15, Théorème 3, p. 299] to non-CM elliptic curves over finitely generated fields of characteristic zero, as explained in [2, Theorem 3.2, p. 1248]. Corollary 1.2 follows.

Next, consider the setting of Corollary 1.3: k is a global function field with field of constants $\mathbb{F}_q$, ∞ is a fixed place of k, A is the ring of elements of k regular away from ∞, K is a finitely generated A-field with $\operatorname{char} K = \operatorname{char} k$ and $A\text{-}\operatorname{char} K = 0$, and $\psi : A \to K\{\tau\}$ is a (generic) Drinfeld A-module over K of rank $r \geq 2$ with $\operatorname{End}_{\overline{K}}(\psi) \simeq A$. This is the specialization of the setting of Theorem 1.1 to k, A, K as above, and to $M = \psi(\overline{K})$, as we now explain.

We recall that an A-field is a pair (K, δ), where K is a field that contains $\mathbb{F}_q$ and $\delta : A \to K$ is an $\mathbb{F}_q$-algebra homomorphism. The kernel of δ is called the A-characteristic of K; it is either (0), in which case we say that K has generic A-characteristic and write that $A\text{-}\operatorname{char} K = 0$, or is a non-zero prime ideal $\mathfrak{p}$ of A, in which case we say that K has finite A-characteristic and write that $A\text{-}\operatorname{char} K = \mathfrak{p}$. Thus, in our setting, K is a field that contains A. We recall that $K\{\tau\}$ denotes the skew-symmetric polynomial ring in τ over K, that is, $K\{\tau\} := \{\sum_{0 \leq i \leq n} c_i \tau^i : n \geq 0, c_0, \ldots, c_n \in K\}$, with the multiplication rule $\tau c = c^q \tau$ for all $c \in K$. We recall that a Drinfeld A-module over K of rank $r \geq 2$ is an $\mathbb{F}_q$-algebra homomorphism $\psi : A \to K\{\tau\}$, $a \mapsto \psi_a$, where $\Im\psi \not\subseteq K$ and the differentiation map $D : K\{\tau\} \to K$,

$D(\sum_{0\leq i\leq n} c_i\tau^i) = c_0$, satisfies $D(\psi_a) = \delta(a)$ for all $a \in A$. The rank of ψ is the unique positive integer r for which $\deg_\tau(\psi_a) = r \deg a$ for all $a \in A$.

For our given generic Drinfeld A-module over K of rank r, $\psi : A \to K\{\tau\}$, the field $\overline{K}$ acquires an A-module structure defined by ψ, which we denote by $\psi(\overline{K})$. From the theory of Drinfeld modules, we know that G_K acts continuously on $\psi(\overline{K})$ and that this action commutes with the A-action. Furthermore, we know that for any non-zero ideal $0 \neq \mathfrak{a} \lhd A$, the set of $\mathfrak{a}$-division elements on $\psi(\overline{K})$, $\psi[\mathfrak{a}] := \{\lambda \in \overline{K} : \psi_a(\lambda) = 0 \ \ \forall\ a \in \mathfrak{a}\}$, is an A-module satisfying the A-module isomorphism $\psi[\mathfrak{a}] \simeq_A (A/\mathfrak{a})^r$. Thus, the A-Drinfeld module ψ gives rise to the (G_K, A)-module $\psi(\overline{K})$ of rank r, in the sense of Breuer's definition given in [2, pp. 1–2]. In this setting, assumption (1.1) of Theorem 1.1 holds thanks to Pink–Rütsche's Open Image Theorem for Drinfeld modules [13, Theorem 0.1, p. 883]; see also [2, Section 3.1, p. 1247] for a related application of this theorem in a setting like ours. Corollary 1.3 follows.

References

[1] C. Adelmann, *The decomposition of primes in torsion point fields*, Lecture Notes in Mathematics, vol. 1761, Springer, 2001.

[2] F. Breuer, "Torsion bounds for elliptic curves and Drinfeld modules", *J. Number Theory* **130** (2010), no. 5, p. 1241-1250.

[3] A. C. Cojocaru & C. David, "Frobenius fields for Drinfeld modules of rank 2", *Compos. Math.* **144** (2008), no. 4, p. 827-848.

[4] ———, "Frobenius fields for elliptic curves", *Am. J. Math.* **130** (2008), no. 6, p. 1535-1560.

[5] A. C. Cojocaru & W. Duke, "Reductions of an elliptic curve and their Tate-Shafarevich groups", *Math. Ann.* **329** (2004), no. 3, p. 513-534.

[6] A. C. Cojocaru & M. Fitzpatrick, "The absolute discriminant of the endomorphism ring of most reductions of a non-CM elliptic curve is close to maximal", `https://arxiv.org/abs/2003.01253`, to appear in *Contemporary Mathematics*, 2020.

[7] A. C. Cojocaru & M. Papikian, "Drinfeld modules, Frobenius endomorphisms, and CM-liftings", *Int. Math. Res. Not.* **2015** (2015), no. 17, p. 7787-7825.

[8] ———, "The growth of the discriminant of the endomorphism ring of the reduction of a rank 2 generic Drinfeld module", `https://arxiv.org/abs/2002.09582`, to appear in *J. Number Theory* (Pisa Conference volume), 2020.

[9] D. A. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication*, John Wiley & Sons, 1989.

[10] W. Duke & A. Tóth, "The splitting of primes in division fields of elliptic curves", *Exp. Math.* **11** (2002), no. 4, p. 555-565.

[11] S. Garai & M. Papikian, "Endomorphism rings of reductions of Drinfeld modules", *J. Number Theory* **212** (2020), p. 18-39.

[12] N. Jones, "A bound for the conductor of an open subgroup of GL_2 associated to an elliptic curve", *Pac. J. Math.* **308** (2020), no. 2, p. 307-331.

[13] R. Pink & E. Rütsche, "Adelic openness for Drinfeld modules in generic characteristic", *J. Number Theory* **129** (2009), no. 4, p. 882-907.

[14] K. Ribet, "Galois action on division points of Abelian varieties with real multiplications", *Am. J. Math.* **98** (1976), no. 3, p. 751-804.

[15] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15** (1972), p. 259-331.

[16] H. Weber, *Lehrbuch der Algebra, Band III*, 1908 (reprint AMS Chelsea, New York, 2001).

Alina Carmen Cojocaru
Department of Mathematics, Statistics and Computer Science
University of Illinois at Chicago,
851 S Morgan St, 322 SEO,
Chicago, 60607, IL, USA
Institute of Mathematics “Simion Stoilow” of the Romanian Academy
21 Calea Grivitei St
Bucharest, 010702
Sector 1, Romania
E-mail: cojocaru@uic.edu

Nathan Jones
Department of Mathematics, Statistics and Computer Science
University of Illinois at Chicago
851 S Morgan St, 322 SEO
Chicago, IL 60607, USA
E-mail: ncjones@uic.edu