Isogenies of elliptic curves over function fields

Richard GRIFFON Fabien PAZUKI

Abstract – We prove two theorems concerning isogenies of elliptic curves over function fields. The first one describes the variation of the height of the j-invariant in an isogeny class. The second one is an "isogeny estimate", providing an explicit bound on the degree of a minimal isogeny between two isogenous elliptic curves. We also give several corollaries of these two results.

Keywords: Elliptic curves over function fields, Heights, Isogenies.

2010 Math. Subj. Classification: 11G05, 11G35, 11G50, 11R58, 14G17, 14G25, 14G40, 14H52, 14K02.

Introduction

Let k be a perfect field, and C be a smooth projective and geometrically irreducible curve over k. We write $K := k(C)$ for the function field of C, and fix an algebraic closure $\overline{K}$ of K.

It is well-known that two elliptic curves defined over K become isomorphic over $\overline{K}$ if and only if they have the same j-invariant. One may wonder, more generally, about the effect of an isogeny of arbitrary degree between two elliptic curves on their j-invariants. There is no *a priori* reason why their j-invariants should be related. Denoting the Weil height on K by $h(.)$, we nonetheless prove that:

Theorem A. *Let E_1, E_2 be two non-isotrivial elliptic curves defined over K with respective j-invariants $j(E_1)$, $j(E_2)$. Let $\varphi : E_1 \to E_2$ be a $\overline{K}$-isogeny and $\widehat{\varphi} : E_2 \to E_1$ be its dual. We have*

$$h(j(E_2)) = \frac{\deg_{\mathrm{ins}}(\varphi)}{\deg_{\mathrm{ins}}(\widehat{\varphi})} \cdot h(j(E_1)). \tag{1}$$

Here $\deg_{\mathrm{ins}}(\varphi)$ and $\deg_{\mathrm{ins}}(\widehat{\varphi})$ denote the inseparability degrees of φ and $\widehat{\varphi}$ (see §4.1 for the definition); if K has characteristic 0, they should be interpreted as 1.

In the particular case where the field K has characteristic 0, the above result states that isogenies preserve the height of the j-invariant! This statement should be compared to its analogue for elliptic curves over number fields: Theorem 1.1 in [Paz19] asserts that the j-invariants of two elliptic curves E_1, E_2 defined over $\overline{\mathbb{Q}}$ which are linked by an isogeny φ satisfy:

$$|ht(j(E_1)) - ht(j(E_2))| \leq 9.204 + 12 \log \deg \varphi, \tag{2}$$

where $ht(.)$ is the logarithmic Weil height on $\overline{\mathbb{Q}}$. Results of Szpiro–Ullmo [SU99] imply that the displayed upper bound is almost optimal – in the sense that the Weil heights of j-invariants of elliptic curves related by isogeny can actually differ by a quantity of the same order of magnitude as a multiple of $\log \deg \varphi$. This latter statement in turn implies that, given an elliptic curve $E/\overline{\mathbb{Q}}$ without CM, the set

$$\mathscr{E}(E, B) := \left\{ j(E') \in \overline{\mathbb{Q}} : E'/\overline{\mathbb{Q}} \text{ is isogenous to } E, \text{ and } ht(j(E')) \leq B \right\}$$

is finite for all $B \geq 1$.

In the function field setting, Theorem A provides a much tighter control on the variation of the Weil height of the j-invariant in isogeny classes of elliptic curves than what can be proved in the number field setting (compare (2) with Theorem A). It leads to the surprising consequence that the sets which are natural analogues for $\mathscr{E}(E, B)$ are infinite in the function field setting (see Proposition 5.9)! We prove Theorem A in section 5.

We refer to the recent [BPR20] for a version of Theorem A for isogenous Drinfeld modules.

Let us now turn to the second main theorem of this article, which is an isogeny estimate for elliptic curves over function fields. The result (Theorem 6.1) may be stated as follows:

Theorem B. *Let E_1 and E_2 be two elliptic curves defined over a function field K of genus g, with respective j-invariants $j(E_1)$, $j(E_2)$. Assume that E_1 and E_2 are isogenous. Then there exists a $\overline{K}$-isogeny $\varphi_0 : E_1 \to E_2$ with*

$$\deg \varphi_0 \leq 49 \max\{1, g\} \cdot \max\left\{ \frac{\deg_{\mathrm{ins}} j(E_1)}{\deg_{\mathrm{ins}} j(E_2)}, \frac{\deg_{\mathrm{ins}} j(E_2)}{\deg_{\mathrm{ins}} j(E_1)} \right\},$$

where $\deg_{\mathrm{ins}} j(E_1), \deg_{\mathrm{ins}} j(E_2)$ are the inseparability degrees of $j(E_1), j(E_2)$ (see §1.4 for the definition); if K has characteristic 0, they should be interpreted as 1.

This result has the same flavour as theorems of Masser and Wüstholz [MW90, MW93], Pellarin [Pel01], and Gaudron and Rémond [GR14] concerning Abelian varieties over number fields (typically called "isogeny estimate"). These authors indeed prove the existence of a "small" isogeny between a pair of isogenous elliptic curves. Here "small" means that the degree of the isogeny is bounded (at worst) in terms of the height of the elliptic curves and simple invariants of the base field.

The proofs in [MW90, MW93, Pel01, GR14] heavily rely on transcendence methods, and uniformisation at an Archimedean place. In the context of function fields, all places are non-Archimedean and, as far as the authors know, only few transcendence results are available in positive characteristic. Therefore, our proof follows a different strategy as the above mentioned works. We also note that David and Denis have proved an analogous statement for isogenies between Drinfeld modules (see [DD99, Théorème 1.3]).

In Theorem B too, the case where K has characteristic 0 offers the most striking result: in this situation, the degree of φ_0 can be bounded independently of E_1, E_2. In other words, Theorem B provides a *uniform* isogeny estimate. In positive characteristic p, one can easily see that such an isogeny estimate cannot be uniform: the smallest isogeny between a non-isotrivial elliptic curve E and its p-th Frobenius twist $E^{(p)}$ is indeed the p-th power Frobenius isogeny $\mathrm{Fr}_p : E \to E^{(p)}$, which has degree p. In positive characteristic, the dependency of Theorem B on the elliptic curves E_1, E_2 is optimal. Theorem B is proved in Section 6 of the paper, where we also establish a few corollaries of this isogeny estimate.

1. Preliminaries about function fields

Let k be a perfect field of characteristic $p \geq 0$, and let C be a smooth projective and geometrically irreducible curve over k. We let $K := k(C)$ denote the function field of C over k. The field k is then algebraically closed in K, and we call it the *constant field of* K. It is well-known that the (isomorphism class of the) field K characterises C up to birational equivalence over $\overline{k}$ (see [Sil09] Chapter II, Remark 2.5 for instance). Any smooth projective curve over k whose function field is K will be called a *model* for K.

Any finite extension L of K is also a function field in the above sense. Precisely, there is a finite extension k'/k and a smooth projective and geometrically irreducible curve C'/k' such that $L = k'(C')$. The inclusion $K \subset L$ induces a morphism $C' \to C$ between the underlying curves.

We refer to [Ros02] for more details about function fields, in particular, Chapter V there.

1.1. Absolute values on K. – Let K be the function field of a curve C/k as above. We let M_K denote the set of *places* of K *i.e.*, equivalence classes of discrete valuations on K. Once a model C of K has been chosen, there is a bijection between M_K and the set of closed points on C. Given a place $v \in M_K$, the residue field k_v of K at v is a finite extension of k: the degree $\deg v := [k_v : k]$ of this extension will be called the degree of v.

If k is finite, we put $c := |k|^{-1}$; if not, we let $c := \mathrm{e}^{-1}$. To each place $v \in M_K$, one associates an absolute value $|.|_v$ on K, defined by $|x|_v := c^{\deg v \cdot v(x)}$ for all $x \in K$, where $v(x)$ is the order of x at v. It is classical that we then have a *product formula*:

$$\forall x \in K^*, \qquad \prod_{v \in M_K} |x|_v = 1, \quad \text{i.e.,} \quad \sum_{v \in M_K} v(x) \cdot \deg v = 0;$$

(see [Lan83, Chap. I, §1]). In terms of a model C for K, this identity is a reformulation of the fact that a rational function on C has as many poles as zeros (counted with multiplicities).

1.2. Absolute values on finite extensions of K. – Let K be as in the previous subsection, and let L/K be a finite field extension. The constant field k' of L is then a finite extension of k. We let M_L denote the set of equivalence classes of discrete valuations on L. Consider a place $w \in M_L$, and write v for the place of K lying under w (*i.e.*, v is the restriction of w to $K \subset L$). The residue field k'_w of L at w is then a finite extension of k', itself a finite extension of k; and we let $\deg w := [k'_w : k]$. (This choice might not be the most common one, but will avoid some notational complications later on).

We associate to $w \in M_L$ a normalised absolute value $|.|_w$ on L: the normalisation is the one such that $|x|_w = |x|_v$ for all $x \in K$. The image of L under $|.|_w$ is then a subgroup of $\mathbb{R}_{>0}$ which contains as a subgroup of finite index the image of K under $|.|_v$. That index is the ramification index of w, we denote it by $e_w := \big(|L|_w : |K|_v\big)$. We denote by $f_w := [k'_w : k_v]$ the residual degree at w. With our normalisations, note that $\deg w = [k'_w : k] = [k'_w : k_v] \cdot [k_v : k] = f_w \cdot \deg v$. Finally, write L_w and K_v for the completions of L at w and of K and v, respectively, and let $n_w := [L_w : K_v]$ denote the local index.

By [Lan83, Chap. I, Prop. 2.4], we have $n_w = e_w \cdot f_w$. With these definitions at hand, one shows that

$$\forall x \in L^*, \qquad n_w \cdot \log_c |x|_w = \deg w \cdot w(x),$$

where $\log_c$ denotes the logarithm to the base c.

Thus endowed with these absolute values, one can prove that L satisfies a product formula:

$$\forall x \in L^*, \qquad \prod_{w \in M_L} |x|_w^{n_w} = 1, \quad \text{i.e.,} \quad \sum_{w \in M_L} w(x) \cdot \deg w = 0.$$

The key part of the proof is to show that, for any $x \in L$ and any $v \in M_K$, we have $|\mathbf{N}_{L/K}(x)|_v = \prod_{w|v} |x|_w$. The latter identity is usually proved under the assumption that L/K be separable but, as noted in [Lan83], it remains true without this assumption, provided that v is "well-behaved" in the terminology of Lang. A general proof may be found in [DGS94, Chap. I, Thm. 5.3].

1.3. Weil height on $\overline{K}$. – We use the notation introduced above. Let $P = [x_0 : x_1] \in \mathbb{P}^1(\overline{K})$ be a point, and pick a finite extension L/K over which P is rational. We define the relative height of P by

$$h_L(P) = \sum_{w \in M_L} n_w \cdot \log_c \max\{|x_0|_w, |x_1|_w\},$$

and the *absolute logarithmic Weil height* of P by the formula:

$$h(P) := \frac{h_L(P)}{[L:K]} = \frac{1}{[L:K]} \sum_{w \in M_L} n_w \cdot \log_c \max\{|x_0|_w, |x_1|_w\}. \tag{1.1}$$

One may check that this last definition does not depend on the choice of an extension L containing P, nor on the choice of homogeneous coordinates for P (see [Lan83, Chap. III, §1]). This construction thus defines a height function on $\mathbb{P}^1(\overline{K})$, which takes values in $\mathbb{Q}_{\geq 0}$.

For any $f \in \overline{K}$, we write $h(f) = h([1 : f])$ for the absolute logarithmic Weil height of the point $[f : 1] \in \mathbb{P}^1(\overline{K})$. Explicitly, for any $f \in \overline{K}$, we have

$$h(f) = \frac{1}{[L:K]} \sum_{w \in M_L} n_w \cdot \max\{0, \log_c |f|_w\} = \frac{1}{[L:K]} \sum_{w \in M_L} \deg w \cdot \max\{0, -w(f)\},$$

where L is any finite extension of K containing f. Choosing a model C' for L, one may view an element $f \in L^*$ as a rational map $f : C' \to \mathbb{P}^1$. Write $\operatorname{div}_\infty(f) \in \operatorname{Div}(C')$ for the divisor of poles of that function. By the right-most expression of the previous display, we have

$$h(f) = \frac{1}{[L:K]} \deg\big(\operatorname{div}_\infty(f)\big),$$

which means that $h_L([f : 1]) = [L : K]h(f)$ equals the degree of f, viewed as a rational map $C' \to \mathbb{P}^1$.

For a given $f \in \overline{K}$, note that $h(f) = 0$ if and only if f is constant (*i.e.*, f belongs to an algebraic extension of the constant field of K). Indeed, a non-constant rational map $C' \to \mathbb{P}^1$ is surjective. In particular, its divisor of poles is a non-zero effective divisor. Hence the height of this map must be positive. In particular, note that the height $h : \overline{K} \to \mathbb{Q}_{\geq 0}$ does not necessarily satisfy the Northcott property: when the constant field k is infinite, the set $\{f \in K : h(f) = 0\}$ (which equals k) is not finite.

1.4. Inseparability degree. – Let K be a function field with constant field k. We assume in this subsection that K has *positive* characteristic p. Recall that the inseparability degree of an element $f \in K^*$ is defined by

$$\deg_{\text{ins}}(f) := \begin{cases} 1 & \text{if } f \in k, \\ \left[K : k(f)\right]_i & \text{if } f \notin k, \end{cases}$$

where $\left[K : k(f)\right]_i$ denotes the inseparability degree of the extension $K/k(f)$ (which is finite under the assumption that f be non-constant). The inseparability degree of f is a non-negative power of p. If f is non-constant, one can prove that $\deg_{\text{ins}}(f) = p^e$ where $e \geq 0$ is the maximal integer such that $f \in K^{p^e}$.

Fixing a model C of K, we view f as a rational map $f : C \to \mathbb{P}^1$. We can then factor f as the composition $f_s \circ F_q$ of a (purely inseparable) Frobenius map $F_q : C \to C^{(q)}$ for some power q of p, with a separable map $f_s : C^{(q)} \to \mathbb{P}^1$. The inseparability degree of f then equals $q = \deg F_q$. We refer to [Sil09, Chap. II, Cor. 2.12] for a proof.

For completeness, we also note the following easily proved fact. Given a finite extension K'/K with inseparability degree $[K' : K]_i$, the inseparability degree of an element $f \in K$ viewed as an element of K' is equal to

$$\deg_{\text{ins}}(f \in K') = \deg_{\text{ins}}(f \in K) \cdot [K' : K]_i.$$

2. Preliminaries on reduction of elliptic curves

Let K be a function field (in the sense of section 1) with constant field k. An elliptic curve over K is called *isotrivial* if its j-invariant is constant (*i.e.* is an element of k). After a finite extension of K, an isotrivial elliptic curve becomes isomorphic to (the base change of) an elliptic curve defined over a finite extension of k. We will be mostly interested in elliptic curves which are *not* isotrivial.

For a more complete overview of the arithmetic of elliptic curves over function fields, the reader is referred to [Ulm11] and [Sil94, Chap. III].

2.1. Minimal discriminant and conductor. – Let E be an elliptic curve over K. Let $v \in M_K$ be a place of K. After a suitable change of coordinates, the curve E admits Weierstrass models

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.1}$$

where the coefficients $a_1, \ldots, a_6 \in K$ are integral at v *i.e.*, models for which $v(a_i) \geq 0$ for $i \in \{1, 2, 3, 4, 6\}$. Each of these models has a discriminant $\Delta(a_1, \ldots, a_6) \in K$ which, being a polynomial in the a_i's, is also integral at v. We write $\delta_v \in \mathbb{Z}_{\geq 0}$ for the minimal value of $v(\Delta(a_1, \ldots, a_6))$ among all models of E which are integral at v. A Weierstrass model (2.1) of E is called *minimal integral at* v if the valuation at v of its discriminant equals δ_v.

Given this collection of local data, we define a global invariant of E: the *minimal discriminant* of E/K is the divisor on K defined by $\Delta_{\min}(E/K) = \sum_{v \in M_K} \delta_v \cdot v$.

We also recall that the *conductor* of E/K is the divisor given by $\mathcal{N}(E/K) = \sum_{v \in M_K} f_v \cdot v$, where $f_v \in \mathbb{Z}_{\geq 0}$ is the *local conductor of* E *at* v. We refer the reader to [Sil94, Chap. IV, §10] for a detailed definition of f_v.

2.2. Good and semi-stable primes. – Let E/K be an elliptic curve and $v \in M_K$ be a place of K. We say that E has *good reduction at* v if and only if the reduction modulo v of one/any integral minimal model of E at v is a smooth curve over the residue field k_v.

More generally, we say that E has *semi-stable reduction at* v if there exists a model of the type (2.1) whose reduction modulo v has at most one double point. This is equivalent to requiring that the reduction of E at v is either good or multiplicative. An elliptic curve over K is said to be *semi-stable* if it has semi-stable reduction at every place of K.

For any elliptic curve E over K, there exists a finite extension K'/K such that $E \times_K K'/K'$ is semi-stable. This statement is the famous Semi-stable Reduction Theorem (see [MB85, Chap. XI]).

The theorem of Kodaira-Néron (see for instance [Sil09, Thm. 6.1, p. 200]) implies that for any semi-stable elliptic curve E/K and any place $v \in M_K$, one has $v(\Delta_v) = -v(j)$, where j denotes the j-invariant of E, and Δ_v the discriminant of a minimal integral model of E at v.

2.3. Tate's uniformisation of elliptic curves with non-integral j-invariants. – In this subsection, we work in the following setting. Consider a field F which is complete for a non-trivial non-Archimedean valuation $|\cdot|$. We review some aspects of Tate's uniformisation of elliptic curves over F: the reader is referred to Tate's beautiful survey [Tat93] for a more in-depth presentation, or to [Sil94, Chap. V, §3-§5] for an overview in the case where F is a finite extension of $\mathbb{Q}_p$.

Let $t \in F$ be such that $|t| < 1$. Consider the curve defined over F by

$$\mathbb{E}_t : \qquad Y^2 + XY = X^3 + c_4(t) \cdot X + c_6(t),$$

where $c_4, c_6 : \overline{F}^\times \to \overline{F}$ are certain power series which converge on the disc $\{z \in \overline{F} : |z| < 1\}$. Tate proved that $\mathbb{E}_t$ is an elliptic curve, whose j-invariant $j(\mathbb{E}_t) \in F$ is given by a convergent power series in t and satisfies $|j(\mathbb{E}_t)| = |t|^{-1} > 1$. Furthermore, he has shown that there is an analytic group isomorphism $\mathbb{E}_t \to \mathbb{G}_m/t^{\mathbb{Z}}$ (the uniformisation map) which is Galois equivariant. In other words, for any algebraic extension F' of F, there is a group isomorphism $\mathbb{E}_t(F') \simeq (F')^\times/t^{\mathbb{Z}}$. Note that $\mathbb{E}_t$ has split multiplicative reduction at the maximal ideal of $|\cdot|$.

Conversely, let E be an elliptic curve over F whose j-invariant satisfies $|j(E)| > 1$. Then, there exists a unique $t \in F$ with $|t| < 1$ such that E is isomorphic to $\mathbb{E}_t$, the isomorphism being defined over an at most quadratic extension of F. See [Sil94, Chap. V, Thm. 5.3].

For $t_1, t_2 \in F$ such that $|t_1| < 1$ and $|t_2| < 1$, let $\mathrm{Hom}_{\overline{F}}(\mathbb{E}_{t_1}, \mathbb{E}_{t_2})$ denote the $\mathbb{Z}$-module consisting of isogenies $\mathbb{E}_{t_1} \to \mathbb{E}_{t_2}$ (defined over $\overline{F}$) together with the constant morphism equal to $0_{\mathbb{E}_{t_2}}$. The theorem p. 16 of [Tat93] states that $\mathrm{Hom}_{\overline{F}}(\mathbb{E}_{t_1}, \mathbb{E}_{t_2})$ is in bijection with the set $\{(n_1, n_2) \in \mathbb{Z}^2 : t_1^{n_1} = t_2^{n_2}\}$.

In particular, for any $t \in F$ with $|t| < 1$, the ring of $\overline{F}$-endomorphisms of $\mathbb{E}_t$ viewed as an elliptic curve over F is isomorphic to $\mathbb{Z}$. Indeed, the above paragraph implies that we have

$$\mathrm{Hom}_{\overline{F}}(\mathbb{E}_t, \mathbb{E}_t) \simeq \{(n, n),\ n \in \mathbb{Z}\}, \tag{2.2}$$

where the correspondence associates the multiplication-by-n map $\mathbb{E}_t \to \mathbb{E}_t$ to the pair $(n, n) \in \mathbb{Z}^2$.

2.4. CM and isotriviality. – Over a number field, it is well known that an elliptic curve with non-integral j-invariant does not have CM (see [Sil94, Chap. 5, §6, Thm. 6.3]).

By the work of Serre–Tate, we know that an elliptic curve defined over a local field and with complex multiplication has integral j-invariant, hence has potentially good reduction. From this we infer that an elliptic curve defined over a function field K, with complex multiplication and with potentially good reduction everywhere must have integral j-invariant at all places of K. In particular its j-invariant, having no poles, must be a constant rational map, which means that the curve E is isotrivial. In positive characteristic, the isotriviality is also implied by Deuring's Theorem (see [Hus04, Thm. 6.4, p. 268]).

Lemma 2.1. *Let K be a function field as above, and let E be an elliptic curve over K whose j-invariant is not constant. Then, the ring* End(E) *of $\overline{K}$-endomorphisms of E is isomorphic to $\mathbb{Z}$. In other words, the curve E has "no complex multiplication".*

Let us give an *ad hoc* proof of this lemma, which is independent of the characteristic of K.

Proof. Because $\mathrm{End}(E)$ contains all the multiplication-by-n maps $[n] : E \to E$, this ring always contains an isomorphic copy of $\mathbb{Z}$. Conversely, let $\psi : E \to E$ be an endomorphism of E. The j-invariant $j(E)$ being non-constant, there exists a place v of K at which $j(E)$ has a pole (*i.e.*, for which $v(j(E)) < 0$).

Let K_v denote the completion of K at v; the field K_v is of the type considered in subsection §2.3. Now, since $v(j(E)) < 0$, we know from the results recalled there that there exists an element $t \in K_v$ with $v(t) > 0$ such that E/K_v becomes isomorphic to the Tate curve $\mathbb{E}_t$ over a finite extension of K_v. Through this isomorphism, the endomorphism ψ becomes an endomorphism $\Psi : \mathbb{E}_t \to \mathbb{E}_t$. By (2.2), there exists an integer n such that Ψ is the multiplication-by-n map of $\mathbb{E}_t$. The original endomorphism $\psi : E \to E$ is thus nothing else but the multiplication map $[n] : E \to E$. Hence the result. □

3. Heights of elliptic curves

Let k be a perfect field and C be a smooth projective and geometrically irreducible curve over k. We let $K := k(C)$ be its function field. We let $p \geq 0$ denote the characteristic of K (p is then either 0 or a prime). We also fix an algebraic closure $\overline{K}$ of K. Algebraic extension of K will be viewed as sub-extensions of $\overline{K}$.

3.1. Differential and stable heights. – Let L be a finite field extension of K; we choose a model C' of L and write k' for the field of constants of L.

Let E be an elliptic curve over L. The minimal regular model $\mathcal{E}$ of E is the unique (up to isomorphism) smooth projective and geometrically irreducible surface over k', equipped with a minimal surjective morphism $\pi : \mathcal{E} \to C'$ whose generic fiber is E. We denote by $\pi : \mathcal{E} \to C'$ the minimal regular model of E and $s_0 : C' \to \mathcal{E}$ its zero section. We refer to [Ulm11, Lecture 3, §1-§2] for more details about the construction of this model. Let $\Omega^1_{\mathcal{E}/C'}$ be the sheaf of relative differential 1-forms on $\mathcal{E}$. Pulling-back $\Omega^1_{\mathcal{E}/C'}$ along the zero section s_0 results in a line bundle on C', which will be denoted by $\omega_{E/L} := s_0^*\Omega^1_{\mathcal{E}/C'}$. One can then define the *differential height of* E/L by:

$$\mathrm{h}_{\mathsf{diff}}(E/L) := \frac{1}{[L:K]}\deg \omega_{E/L},$$

where deg here means degree of a line bundle. The following identity is well-known:

Lemma 3.1. *In the above setting, denote by* $\Delta_{\min}(E/L) \in \mathrm{Div}(C')$ *the minimal discriminant divisor of* E*. Then one has*

$$12 \cdot \mathrm{h}_{\mathsf{diff}}(E/L) = \frac{\deg \Delta_{\min}(E/L)}{[L:K]}.$$

See [Sil86, Prop. 1.1] for a proof: the main point is that $\Delta_{\min}(E/L)$ provides a section of $\omega_{E/L}^{\otimes 12}$. In contrast to the number field setting (treated in [Sil86]), no "Archimedean terms" come into play in the computation of the degree of the line bundle $\omega_{E/L}$. This Lemma provides a simple way to compute and estimate the differential height.

One checks that the differential height does not increase in finite extensions, by which we mean that, if L'/L is a further finite extension, one has $\mathrm{h}_{\mathsf{diff}}(E \times L'/L') \leq \mathrm{h}_{\mathsf{diff}}(E/L)$. We refer the reader to [MB85, Prop. 2.3, p. 228] for a proof of this fact for general Abelian varieties.

Given an elliptic curve E over a finite extension L of K, pick an extension L'/L such that the base-changed curve $E_{L'}/L'$ is semi-stable (as was recalled above, such an extension exists). We then define the *stable height of* E to be

$$\mathrm{h}_{\mathsf{st}}(E/L) := \frac{\mathrm{h}_{\mathsf{diff}}(E_{L'}/L')}{[L':L]} = \frac{\deg(\omega_{E_{L'}/L'})}{[L':L]}.$$

This definition makes sense: it is indeed shown in [MB85, Prop. 2.3, p. 228] that the quantity $\mathrm{h}_{\mathsf{st}}(E/L)$ does not depend on the choice of a particular extension L'/L over which E attains semi-stable reduction.

3.2. Modular height. – Let E be an elliptic curve defined over $\overline{K}$. Its j-invariant $j(E)$ lies in $\overline{K}$: we can then define the *modular height of* E to be

$$\mathrm{h}_{\mathsf{mod}}(E) := h\big(j(E)\big) \in \mathbb{Q}_{\geq 0},$$

where h is the Weil height on $\overline{K}$ defined in §1.3. This modular height is closely related to the height called *hauteur modulaire numérique* defined by Moret-Bailly in [MB85, p. 226].

If we fix a finite extension L of K containing $j(E)$, and write $L = k'(C')$ (where k'/k is a finite extension and C' is a smooth projective geometrically integral curve over k'), we may view $j(E)$ as a rational map $j : C' \to \mathbb{P}^1$. Denoting by $\mathrm{div}_\infty(j) \in \mathrm{Div}(C')$ the divisor of poles of this map, we then have

$$\mathrm{h}_{\mathsf{mod}}(E) = \frac{1}{[L:K]}\deg(\mathrm{div}_\infty(j)).$$

(See the discussion in §1.3). It follows that the modular height $\mathrm{h}_{\mathsf{mod}}(E)$ vanishes if and only if $j(E)$ is a constant element of $\overline{K}$, *i.e.*, if and only if E is isotrivial.

3.3. Comparison of heights. – We now compare the various notions of heights of an elliptic curve over $\overline{K}$ that were just introduced. Let L/K be a finite extension, and let E be an elliptic curve over L.

Proposition 3.2. *With the above notation, one has*

$$0 \leq \mathrm{h}_{\mathsf{diff}}(E/L) - \frac{1}{12}\mathrm{h}_{\mathsf{mod}}(E) \leq \frac{1}{[L:K]} \cdot \sum_{w \text{ not s.s.}} \deg w, \tag{3.1}$$

where the sum is over the (finite) set of places of L *where* E *does not have semi-stable reduction.*

The reader might want to compare this estimate with the one in [Sil86, Prop. 2.1] where a similar comparison is carried out between differential and modular heights of an elliptic curve over a number field. The proof in our setting is simplified by the absence of Archimedean places.

Proof. For any place w of L, we let δ_w denote the valuation at w of the discriminant of a minimal integral model of E at w, and we let $\theta_w = w(j(E))$ denote the order of the pole/zero of $j(E)$ at w.

By construction of the modular and differential heights, we have

$$[L:K] \cdot \mathrm{h}_{\mathsf{diff}}(E/L) = \frac{\deg \Delta_{\min}(E/L)}{12} = \frac{1}{12} \sum_{w \in M_L} \delta_w \cdot \deg w,$$

$$[L:K] \cdot \mathrm{h}_{\mathsf{mod}}(E) = \sum_{w \in M_L} n_w \cdot \max\{0, \log_c |j(E)|_w\} = \sum_{w \in M_L} \max\{0, -\theta_w\} \cdot \deg w,$$

where the sums are supported on the places of bad reduction of E. Note indeed that the j-invariant has no poles outside places of bad reduction. (Actually, as the table p. 365 of [Sil94] shows, poles of j only occur at places of potentially multiplicative reduction.) Hence we have

$$12[L:K] \cdot \mathrm{h}_{\mathsf{diff}}(E/L) - [L:K] \cdot \mathrm{h}_{\mathsf{mod}}(E) = \sum_{w \in M_L} (\delta_w - \max\{0, -\theta_w\}) \cdot \deg w.$$

For any place $w \in M_L$, by the discussion in [Sil94, Chap. IV, §9], the minimality of δ_w implies that, either $0 \leq \delta_w < 12$ or $0 \leq \delta_w + \theta_w \leq 12$. Therefore, for any place w of bad reduction, the integer $\delta_w - \max\{0, -\theta_w\} = \min\{\delta_w, \theta_w + \delta_w\}$ lies in $[0, 12]$. If, moreover, w is a place of multiplicative reduction for E, the above mentioned table in [Sil94] yields that $\delta_w + \iota_w = 0$. We have thus proved that

$$\begin{aligned} 0 \leq 12[L:K] \cdot \mathrm{h}_{\mathsf{diff}}(E/L) - [L:K] \cdot \mathrm{h}_{\mathsf{mod}}(E) &= \sum_{w \text{ add. red.}} \min\{\delta_w, \iota_w + \delta_w\} \cdot \deg w \\ &\leq 12 \cdot \sum_{w \text{ not s.s.}} \deg w. \end{aligned}$$

This entails the desired bounds. □

It is clear that an elliptic curve E/L is semi-stable if and only if the sum on the right-hand side of (3.1) vanishes. Hence, the above proposition directly implies:

Corollary 3.3. *Let E be an elliptic curve defined over a finite extension L of K. Then E/L is semi-stable if and only if $\mathrm{h}_{\mathsf{mod}}(E) = 12 \cdot \mathrm{h}_{\mathsf{diff}}(E/L)$. In particular, we have $\mathrm{h}_{\mathsf{mod}}(E) = 12 \cdot \mathrm{h}_{\mathsf{st}}(E/L)$.*

3.4. Heights and conductor. – Let L/K be a finite field extension. We fix a model C' of L. The genus of C' will be denoted by $g(L)$.

For any elliptic curve E over L, Ogg's formula (see formula (11.1) in [Sil94, Chap. IV, §11]), implies that $v(\mathcal{N}(E/L)) \leq v(\Delta_{\min}(E/L))$ for all places $v \in M_K$. Hence we have $\deg \mathcal{N}(E/L) \leq \deg \Delta_{\min}(E/L)$, and it follows that

$$\frac{\deg \mathcal{N}(E/L)}{[L:K]} \leq 12 \cdot \mathrm{h}_{\mathsf{diff}}(E/L).$$

Obtaining an inequality in the other direction is much harder. The result is as follows:

Theorem 3.4 (Szpiro's inequality)**.** *Let E be an elliptic curve defined over L. We have*

$$\deg \Delta_{\min}(E/L) \leq 6 \cdot \deg_{\mathrm{ins}} j(E) \cdot \big(2g(L) - 2 + \deg \mathcal{N}(E/L)\big). \tag{3.2}$$

where $\mathcal{N}(E/L)$ denotes the conductor of E, and $\deg_{\mathrm{ins}} j(E)$ the inseparability degree of its j-invariant.

The proof in the semi-stable case can be found in [Szp90], and the general case is treated in [PS00]. Rewriting this inequality in terms of $\mathrm{h}_{\mathsf{diff}}$ yields that, for any elliptic curve over K, we have

$$\frac{1}{12} \cdot \deg \mathcal{N}(E/K) \leq \mathrm{h}_{\mathsf{diff}}(E/K) \leq \deg_{\mathrm{ins}} j(E) \cdot (g(K) - 1 + \deg \mathcal{N}(E/K)).$$

In particular, for an elliptic curve E/K whose j-invariant is separable, Szpiro's inequality reads:

$$\frac{1}{12} \cdot \deg \mathcal{N}(E/K) \leq \mathrm{h}_{\mathsf{diff}}(E/K) \leq (g(K) - 1) + \deg \mathcal{N}(E/K).$$

Hence, for these elliptic curves, the conductor $\deg \mathcal{N}(E/K)$ and the differential height $\mathrm{h}_{\mathsf{diff}}(E/K)$ have the same order of magnitude (up to constants depending at most on the genus of K).

4. Isogenies between elliptic curves

In this section, we work in the same setting as before. Precisely, we let k be a perfect field, C be a smooth projective and geometrically irreducible curve over k, and K be the function field $k(C)$. We denote the characteristic of K by p (which is either a prime or 0).

The goal of this section is to recall a few standard facts about isogenies between elliptic curves, as well as prove a decomposition result for them. The reader is referred to [Sil09, Chap. III, §4] for further details about isogenies.

4.1. Preliminaries on isogenies. – Let E_1 and E_2 be two elliptic curves defined over K. We denote by $0_{E_1} \in E_1(K)$ and $0_{E_2} \in E_2(K)$ the respective neutral elements of the groups E_1 and E_2.

An *isogeny* $\varphi : E_1 \to E_2$ is a surjective morphism of varieties satisfying $\varphi(0_{E_1}) = 0_{E_2}$. It can then be shown that φ is a group morphism $E_1 \to E_2$. Unless otherwise specified, we do not assume that isogenies are defined over K.

As a morphism between algebraic varieties, φ induces a finite embedding of function fields

$$\varphi^* : \overline{K}(E_2) \hookrightarrow \overline{K}(E_1).$$

The *degree of* φ, denoted by $\deg\varphi$, is defined to be the degree of the finite field extension $\overline{K}(E_1)/\varphi^*(\overline{K}(E_2))$.

If the characteristic of K is positive, the extension $\overline{K}(E_1)/\varphi^*\overline{K}(E_2)$ may be split into two subextensions, as follows. We let L_φ be the maximal subextension of $\overline{K}(E_1)/\varphi^*(\overline{K}(E_2))$ which is separable on $\varphi^*(\overline{K}(E_2))$ (*i.e.*, L_φ is the separable closure of $\varphi^*\overline{K}(E_2)$ in $\overline{K}(E_1)$). Then $L_\varphi/\varphi^*\overline{K}(E_2)$ is a finite separable extension, whose degree is denoted by $\deg_{\mathrm{sep}}\varphi$ and called the *separable degree of* φ. The degree of the extension $\overline{K}(E_1)/L_\varphi$ is denoted by $\deg_{\mathrm{ins}}\varphi$ and is called the *inseparable degree of* φ. It is clear that $\deg_{\mathrm{ins}}\varphi$ is a power of the characteristic of K, and that we have $\deg\varphi = \deg_{\mathrm{sep}}\varphi \cdot \deg_{\mathrm{ins}}\varphi$.

Coming back to the general case, and viewing $\varphi : E_1 \to E_2$ as a homomorphism of group varieties, we may define its kernel $\ker\varphi = \varphi^{-1}(\{0\}) \subset E_1$ as a a finite group variety over K. (If φ is separable, its kernel is a reduced group scheme; hence we do not lose much by identifying the kernel with its set of closed points). In general, one can check that the finite Abelian group $(\ker\varphi)(\overline{K})$ has order $\deg_{\mathrm{sep}}\varphi$. A separable isogeny is called *cyclic* if its kernel is a cyclic Abelian group.

If $\varphi : E_1 \to E_2$ is an isogeny, recall that there is a *dual isogeny* $E_2 \to E_1$, which we denote by $\widehat{\varphi}$. The compositions $\varphi \circ \widehat{\varphi}$ and $\widehat{\varphi} \circ \varphi$ are equal to the multiplication by $\deg\varphi$ on E_2, resp. E_1. The degrees of φ and $\widehat{\varphi}$ are equal.

Let us now assume that K has positive characteristic p, and let E be an elliptic curve over K. For any power q of p, we we write $E^{(q)}$ for the q-th power Frobenius twist of E (if E is defined by a Weierstrass model with coefficients $a_1, \dots, a_6 \in K$, then $E^{(q)}$ is the elliptic curve given by the Weierstrass model with coefficients $a_1^q, \dots, a_6^q$). Recall that there is a *q-th power Frobenius morphism* $\mathrm{Fr}_q : E \to E^{(q)}$ which is defined over K, and that this morphism is an isogeny of degree q. As such, it admits a dual isogeny $\mathrm{V}_q : E^{(q)} \to E$ which is called the *q-th power Verschiebung isogeny*, and is also defined over K. The multiplication-by-q map $[q] : E \to E$ then decomposes as $[q] = \mathrm{V}_q \circ \mathrm{Fr}_q$. If E is non-isotrivial, it is known that $\mathrm{Fr}_q : E \to E^{(q)}$ is purely inseparable of degree q (that is, we have $\deg_{\mathrm{sep}}\mathrm{Fr}_q = 1$ and $\deg_{\mathrm{ins}}\mathrm{Fr}_q = q$) and that its dual $\mathrm{V}_q : E^{(q)} \to E$ is separable of degree q. These facts follow from [Sil09, Chap. V, §3].

Finally, we recall three results concerning isogenies between elliptic curves.

Proposition 4.1. *Let E_1, E_2 be two elliptic curves defined over a field K, whose characteristic is p, and let $\varphi : E_1 \to E_2$ be an isogeny between them. The isogeny φ factors as $\varphi = \psi \circ \mathrm{Fr}_{p^e}$ where $\mathrm{Fr}_{p^e} : E_1 \to E_1^{(p^e)}$ is the p^e-th power Frobenius isogeny and $\psi : E_1^{(p^e)} \to E_2$ is a separable isogeny. (Note that $p^e = \deg_{\mathrm{ins}}\varphi$).*

Proposition 4.2. *Let E_1, E_2, E_3 be elliptic curves defined over a field K. Let $\varphi : E_1 \to E_2$ be a separable isogeny, and $\psi : E_1 \to E_3$ be an isogeny. If $\ker\varphi \subseteq \ker\psi$, then ψ factors uniquely through φ i.e., there is a unique isogeny $\lambda : E_2 \to E_3$ such that $\psi = \lambda \circ \varphi$.*

Proposition 4.3. *Let E be an elliptic curve defined over a field K, and let G be a finite subgroup of E. Then there exist a unique elliptic curve E' defined over $\overline{K}$ and a separable isogeny $\pi : E \to E'$ such that $\ker\pi = G$. The curve E' is usually denoted by E/G.*

These three statements and their proofs can be found in [Sil09]: see Corollary 2.12 in Chapter II, Corollary 4.11 in Chapter III, and Proposition 4.12 in Chapter III, respectively.

4.2. A useful decomposition of isogenies. – Let K be a function field in the above sense. In this subsection, we assume that the characteristic p of K is positive.

Let E_1, E_2 be two non-isotrivial elliptic curves defined over K, and let $\varphi : E_1 \to E_2$ be an isogeny between them. By Proposition 4.1, one can decompose φ as

$$E_1 \xrightarrow{\mathrm{Fr}_{p^e}} E_1^{(p^e)} \xrightarrow{\psi} E_2,$$

where Fr_{p^e} denotes the p^e-th power Frobenius isogeny, and ψ is a separable isogeny. Since ψ is separable, we see that $\deg_{\mathrm{ins}}\varphi = \deg_{\mathrm{ins}}\mathrm{Fr}_{p^e} = p^e$. Let us now consider the dual isogeny $\widehat{\psi} : E_2 \to E_1^{(p^e)}$ to ψ. Using the same Proposition 4.1 as in the previous paragraph, we obtain that $\widehat{\psi}$ factors as

$$E_2 \xrightarrow{\mathrm{Fr}_{p^f}} E_2^{(p^f)} \xrightarrow{\psi'} E_1^{(p^e)},$$

where ψ' is a separable isogeny, and where $p^f = \deg_{\mathrm{ins}}\widehat{\varphi}$. We thus have $\widehat{\psi} = \psi' \circ \mathrm{Fr}_{p^f}$. By contravariance of taking duals, we deduce that $\psi = \widehat{\widehat{\psi}} = \widehat{\mathrm{Fr}_{p^f}} \circ \widehat{\psi'}$. By definition, the dual of Fr_{p^f} is the Verschiebung isogeny $\mathrm{V}_{p^f} : E_2^{(p^f)} \to E_2$. Since E_2 is non-isotrivial, V_{p^f} is a separable isogeny of degree p^f. The isogeny $\varphi_s := \widehat{\psi'}$ is separable, because both $\psi = \mathrm{V}_{p^f} \circ \varphi_s$ and V_{p^f} are (by multiplicativity of the inseparability degree in compositions). In particular, φ_s is a separable isogeny whose dual $\widehat{\varphi_s} = \psi'$ is also separable.

We have therefore decomposed our original isogeny $\varphi : E_1 \to E_2$ as a composition

$$E_1 \xrightarrow{\mathrm{Fr}_{p^e}} E_1^{(p^e)} \xrightarrow{\varphi_s} E_2^{(p^f)} \xrightarrow{\mathrm{V}_{p^f}} E_2,$$

where φ_s is separable with separable dual. We also know that $p^e = \deg_{\mathrm{ins}}\varphi$ and $p^f = \deg_{\mathrm{ins}}\widehat{\varphi}$. This should motivate the following definition:

Definition 4.4. Let $\varphi : E \to E'$ be an isogeny between two elliptic curves E, E' over K. If both φ and its dual $\widehat{\varphi}$ are separable, we will say that φ is *biseparable.*

Such isogenies may be characterised as follows:

Lemma 4.5. *Let E and E' be two elliptic curves over K and let $\varphi : E \to E'$ be an isogeny. Then φ is biseparable if and only if $\deg\varphi$ is coprime to the characteristic of K.*

Proof. Let $p > 0$ denote the characteristic of K. We factor the degree $d := \deg\varphi$ as $d = p^r \cdot d'$, with $r \geq 0$ and $d' \in \mathbb{Z}$ is coprime to p. By construction of the dual isogeny, we have $\widehat{\varphi} \circ \varphi = [d] = [d'] \circ [p^r]$, where $[n] : E \to E$ denotes the multiplication-by-n map on E. Now, the multiplication-by-p^r map $[p^r]$ on E is inseparable of degree p^{2r} (with inseparability degree with $p^r \leq \deg_{\mathrm{ins}}[p^r] \leq p^{2r}$); and, since d' is coprime to p, the map $[d'] : E \to E$ is separable. All in all, the inseparability degree of the map $\widehat{\varphi} \circ \varphi = [d] : E \to E$ satisfies $p^r \leq \deg_{\mathrm{ins}}[d] \leq p^{2r}$.

Now assume that φ is biseparable of degree $d = d'p^r$. Since both φ and $\widehat{\varphi}$ are separable, their composition is separable. Hence the multiplication-by-d map on E is separable. By the previous paragraph, we must have $r = 0$. Therefore, the degree of φ is coprime to p.

Conversely, assume that the degree d of φ is coprime to p. Then φ must be separable because the map $[d] : E \to E$ is separable and factors through φ. Since the dual of φ has degree $\deg\widehat{\varphi} = d$, the very same argument shows that $\widehat{\varphi}$ is also separable. □

The discussion preceding Definition 4.4 proves the following decomposition result:

Proposition 4.6. *Let E_1, E_2 be two non-isotrivial elliptic curves over K, and let $\varphi : E_1 \to E_2$ be an isogeny between them. The isogeny φ factors as*

$$E_1 \xrightarrow{\mathrm{Fr}_{p^e}} E_1^{(p^e)} \xrightarrow{\psi} E_2^{(p^f)} \xrightarrow{\mathrm{V}_{p^f}} E_2,$$

where ψ is a biseparable isogeny. We have $p^e = \deg_{\mathrm{ins}}\varphi$ and $p^f = \deg_{\mathrm{ins}}\widehat{\varphi}$.

This decomposition will be used repeatedly in the remainder of the article. We conclude this section by the following lemma:

Lemma 4.7. *Let K be a function field as above. Let $\varphi : E_1 \to E_2$ be a biseparable isogeny between non-isotrivial elliptic curves over K. Then the kernel $H = \ker\varphi$ of φ is defined over a finite separable extension of K, that is, the extension $K(H)/K$ is separable.*

Proof. Let d be the degree of φ, $[d] : E_1 \to E_1$ denote the multiplication-by-$[d]$ map on E_1, and $E_1[d]$ be the d-torsion subgroup of E_1. We have $H = \ker\varphi \subset \ker[d] = E_1[d]$, so that $K(H)$ is a subfield of $K(E_1[d])$. It therefore suffices to prove that the extension $K(E_1[d])/K$ is separable. We know by Lemma 4.5 that d is coprime to the characteristic of K. Then it is well-known (see [ST68, §1] for instance) that $E_1[d]$ is contained in $E_1(K^{\mathrm{sep}})$, where K^{sep} denotes the separable closure of K. The extension $K(E_1[d])/K$ is therefore separable, and the Lemma is proved. □

5. Isogenies and heights

Let k be a perfect field of characteristic $p \geq 0$. Let C be a smooth projective geometrically irreducible curve over k, and $K = k(C)$ denote its function field. The goal of this section is to describe the effect of an isogeny between elliptic curves over K on the height of their j-invariants: we prove Theorem A, as well as state a few consequences thereof.

The general idea is that "biseparable isogenies preserve the height". If K has characteristic 0, this will directly lead to the desired result. In positive characteristic p, more work is required.

5.1. Biseparable isogenies preserve the differential height. – We begin by recalling the following result (see [Par70, Par73] for instance) and its proof. The reader is referred to [BLR90] (especially §7.3 there) and [Ray85] for more details about Néron models and isogenies.

Theorem 5.1. *Let E_1, E_2 be non-isotrivial elliptic curves over K. Assume that there exists a biseparable isogeny $\varphi : E_1 \to E_2$. Then, we have*

$$\mathrm{h}_{\mathsf{diff}}(E_1/K) = \mathrm{h}_{\mathsf{diff}}(E_2/K).$$

Proof. For $i = 1, 2$, we denote the Néron model of E_i/K by $\pi_i : \mathcal{E}_i \to C$, and we write $s_i : C \to \mathcal{E}_i$ for its zero-section. The surface $\mathcal{E}_i$ is smooth over C: let $\Omega^1_{\mathcal{E}_i/C}$ denote the sheaf of relative differential 1-forms on $\mathcal{E}_i/C$, and consider the line bundle $\omega_i := s_i^*\Omega^1_{\mathcal{E}_i/C}$ on C. Recall from §3.1 that the differential height of E_i equals $\deg\omega_i$. To prove the Theorem, it is (more than) sufficient to show that $\omega_1 \simeq \omega_2$ as line bundles on C. The given isogeny $\varphi : E_1 \to E_2$ extends into a group morphism $\Phi : \mathcal{E}_1 \to \mathcal{E}_2$ which is still an isogeny, which means that Φ is, fiber by fiber, finite and surjective on the identity components. The morphism Φ induces a map $\Phi^*\Omega^1_{\mathcal{E}_2/C} \to \Omega^1_{\mathcal{E}_1/C}$, which we may restrict to the zero-section. Using that Φ satisfies $\Phi \circ s_1 = s_2$, we obtain a map of $\mathcal{O}_C$-modules

$$F : \omega_2 = s_2^*\Omega^1_{\mathcal{E}_2/C} \simeq s_1^*\Phi^*\Omega^1_{\mathcal{E}_2/C} \longrightarrow s_1^*\Omega^1_{\mathcal{E}_1/C} = \omega_1.$$

Is suffices to show that F is an isomorphism: to so so, we may argue locally on C. We thus set out to show that, for any closed point v of C, the restriction of F to the fibers $\omega_{1,v}$ and $\omega_{2,v}$ of ω_1 and ω_2 above v is an isomorphism.

Let v be a closed point of C. Write $\mathcal{O}_v$ for the local ring of C at v and $S := \operatorname{Spec}\mathcal{O}_v$. We also let k_v denote the residue field at v (note that k_v is a finite extension of k, and thus has the same characteristic as k). Denoting the fiber of $\mathcal{E}_i$ at v by $\mathcal{E}_{i,v} := \mathcal{E}_i \times_C \operatorname{Spec}\mathcal{O}_v$, the restriction $\varphi_v : \mathcal{E}_{1,v} \to \mathcal{E}_{2,v}$ of Φ is an isogeny. It is then known (see [BLR90, §7.3, Lem. 5]) that there exists a dual isogeny $\widehat{\varphi}_v : \mathcal{E}_{2,v} \to \mathcal{E}_{1,v}$, such that $\widehat{\varphi}_v \circ \varphi_v = [d]$ with $d = \deg\varphi$. Since d is coprime to the characteristic of k_v, all three of φ_v, $\widehat{\varphi}_v$ and $[d]$ are étale by [Ray85, 1.1.2], or [BLR90, §7.3, Lem. 2].

The isogeny φ_v induces a canonical map $\varphi_v^*\Omega^1_{\mathcal{E}_{2,v}/S} \to \Omega^1_{\mathcal{E}_{1,v}/S}$ which, since φ_v is étale on $\mathcal{E}_{1,v/S}$, is actually an isomorphism (see [BLR90, §2.2, Coro. 10]). Moreover, φ_v being a group morphism, we have $\varphi_v \circ s_1|_{\mathcal{E}_{1,v}} = s_2|_{\mathcal{E}_{2,v}}$. Pulling back the above isomorphism along (the restriction of) s_1, we obtain an isomorphism of $\mathcal{O}_v$-modules

$$\omega_{2,v} = s_2^*\Omega^1_{\mathcal{E}_{2,v}/S} \simeq s_1^*\varphi_v^*\Omega^1_{\mathcal{E}_{2,v}/S} \longrightarrow s_1^*\Omega^1_{\mathcal{E}_{1,v}/S} = \omega_{1,v},$$

which is the restriction of F to the fibers above v. This concludes the proof. □

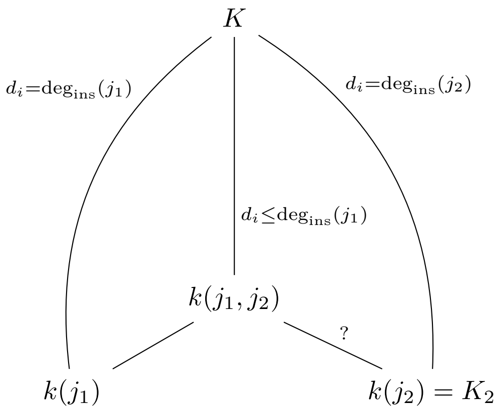
5.2. Biseparable isogenies preserve the inseparability degree of the j-invariants. – In this subsection, we assume that the function field K has positive characteristic p. We describe the effect of a biseparable isogeny on the inseparability degree of the j-invariants.

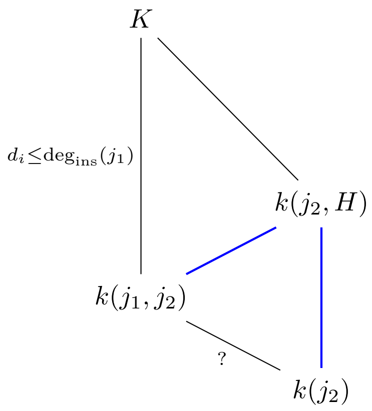
Proposition 5.2. *Let E_1, E_2 be two* non-isotrivial *elliptic curves over K. Assume that there exists a biseparable isogeny $E_1 \to E_2$. Then, the inseparability degrees of $j(E_1)$ and $j(E_2)$ are equal.*

The proof below is adapted from [BLV09, 2.2] where it is proven that, if $E_1 \to E_2$ is a biseparable isogeny and if $j(E_1) \in K$ is separable, then $j(E_2)$ is separable too.

Proof. We write j_1, j_2 to denote the j-invariants of E_1 and E_2 respectively. Let $\varphi : E_1 \to E_2$ be a biseparable isogeny, whose degree is denoted by d (by assumption, d is thus coprime to p). Choose an elliptic curve E_2' defined over $k(j_2)$ whose j-invariant is j_2: by construction, E_2 and E_2' are isomorphic over $\overline{K}$. Actually, E_2 and E_2' become isomorphic over a finite separable extension K'/K of degree ≤ 24, see [Sil09, Chap. III, Prop. 1.4]. Moreover one can assume that the field of constants of K' is k. We may and do base change the situation to K', so that $E_2 \simeq E_2'$ over $K' = K$.

For the convenience of the reader, here are diagrams of the field extensions we are going to consider: all these extensions are finite, we have indicated some of the inseparability degrees, and the thicker lines denote extensions which are separable (see below).


K
$d_i{=}\deg_{\mathrm{ins}}(j_1)$
$d_i{=}\deg_{\mathrm{ins}}(j_2)$
$d_i{\leq}\deg_{\mathrm{ins}}(j_1)$
$k(j_1, j_2)$
?
$k(j_1)$
$k(j_2) = K_2$



Let $K_2 = k(j_2) \subset K$. Since d is coprime to p, the extension $K_2(E_2'[d])/K_2$, obtained by adjoining to K_2 the coordinates of points of d-torsion on E_2', is finite and separable (see [BLV09, Prop. 3.8] for a proof). We view φ as an isogeny $\varphi : E_1 \to E_2 \simeq E_2'$. Let $\widehat{\varphi} : E_2' \to E_1$ be its dual isogeny: the kernel $H := (\ker \widehat{\varphi})(\overline{K})$ of $\widehat{\varphi}$ is then a subgroup of $E_2'[d]$. Therefore the finite extension $K_2(H)/K_2$ obtained by adjoining to K_2 the coordinates of points of H, being a subextension of $K_2(E_2'[d])/K_2$ is separable.

The curves E_1 and E_2' are linked by the isogeny $\widehat{\varphi}$, and thus $E_1 \simeq E_2'/H$. In particular, E_1 is isomorphic to an elliptic curve defined over $K_2(H)$, so that $j_1 \in K_2(H)$. This implies that $K_2(j_1) = k(j_1, j_2)$ is a finite separable extension of $K_2 = k(j_2)$. Indeed, $k(j_1, j_2)/K_2$ is a sub-extension of $K_2(H)/K_2$, which is finite separable (see Lemma 4.7). Hence the extension K/K_2 has the same inseparability degree as the finite extension $K/k(j_1, j_2)$:

$$\deg_{\mathrm{ins}}(j_2) = [K : K_2]_i = [K : k(j_1, j_2)]_i.$$

On the other hand, we have a chain of finite extensions $k(j_1) \subset k(j_1, j_2) \subset K$. Therefore, we have the divisibility relation:

$$[K : k(j_1, j_2)]_i \text{ divides } [K : k(j_1)]_i = \deg_{\mathrm{ins}}(j_1).$$

We thus conclude that $[K : k(j_2)]_i = \deg_{\mathrm{ins}}(j_2)$ divides $\deg_{\mathrm{ins}}(j_1)$.

Applying the same argument to the dual isogeny $\widehat{\varphi} : E_2 \to E_1$ (which is also biseparable), we conclude that $\deg_{\mathrm{ins}}(j_1)$ divides $\deg_{\mathrm{ins}}(j_2)$. These two quantities are therefore equal. □

Making use of Proposition 4.6, we now describe the effect of an arbitrary isogeny on the inseparability degrees of the j-invariants.

Corollary 5.3. *Let E_1, E_2 be two non-isotrivial elliptic curves over K. Assume that there exists an isogeny $\varphi : E_1 \to E_2$. Then we have*

$$\deg_{\mathrm{ins}}(\widehat{\varphi}) \cdot \deg_{\mathrm{ins}} j(E_2) = \deg_{\mathrm{ins}}(\varphi) \cdot \deg_{\mathrm{ins}} j(E_1).$$

Proof. By Proposition 4.6, one may decompose $\varphi : E_1 \to E_2$ as a composition

$$E_1 \xrightarrow{\mathrm{Fr}_{p^e}} E_1^{(p^e)} \xrightarrow{\psi} E_2^{(p^f)} \xrightarrow{\mathrm{V}_{p^f}} E_2,$$

where ψ is biseparable, $p^e = \deg_{\mathrm{ins}}(\varphi)$, and $p^f = \deg_{\mathrm{ins}}(\widehat{\varphi})$. By the previous proposition, the inseparability degrees of $j(E_1^{(p^e)})$ and $j(E_2^{(p^f)})$ are equal. For $i \in \{1, 2\}$ and any $k \in \mathbb{Z}_{\geq 0}$, since $j(E_i^{(p^k)}) = j(E_i)^{p^k}$, we have $\deg_{\mathrm{ins}} j(E_i^{(p^k)}) = p^k \deg_{\mathrm{ins}}(j(E_i))$. The claimed identity is then clear. □

5.3. Isogenies and modular heights. – We can now conclude our study of the effect of isogenies between elliptic curves on their modular height. We fix a function field K as above. In case K has characteristic 0, all the inseparability degrees should be interpreted as being 1. The following result was announced in the introduction as Theorem A:

Theorem 5.4. *Let E_1 and E_2 be two non-isotrivial elliptic curves over $\overline{K}$. Assume that there is an isogeny $\varphi : E_1 \to E_2$ between them. Then one has*

$$\mathrm{h}_{\mathsf{mod}}(E_2) = \frac{\deg_{\mathrm{ins}}(\varphi)}{\deg_{\mathrm{ins}}(\widehat{\varphi})} \cdot \mathrm{h}_{\mathsf{mod}}(E_1).$$

In particular, biseparable isogenies preserve the modular height.

Proof. Fix a finite extension L/K over which both E_1, E_2 are defined. We may and will also assume that L is chosen so that E_1 and E_2 are semi-stable over L. As above (see Proposition 4.6), we decompose the isogeny $\varphi : E_1 \to E_2$ as a composition of $\mathrm{Fr}_{p^e} : E_1 \to E_1^{(p^e)}$, $\psi : E_1^{(p^e)} \to E_2^{(p^f)}$ and $\mathrm{V}_{p^f} : E_2^{(p^f)} \to E_2$ where ψ is biseparable and $p^e = \deg_{\mathrm{ins}}(\varphi)$, $p^f = \deg_{\mathrm{ins}}(\widehat{\varphi})$. We denote $E_1^{(p^e)}$ by E_1' and $E_2^{(p^f)}$ by E_2', for simplicity. We write that

$$\frac{\mathrm{h}_{\mathsf{mod}}(E_2)}{\mathrm{h}_{\mathsf{mod}}(E_1)} = \frac{\mathrm{h}_{\mathsf{mod}}(E_2)}{\mathrm{h}_{\mathsf{mod}}(E_2')} \cdot \frac{\mathrm{h}_{\mathsf{mod}}(E_2')}{\mathrm{h}_{\mathsf{mod}}(E_1')} \cdot \frac{\mathrm{h}_{\mathsf{mod}}(E_1')}{\mathrm{h}_{\mathsf{mod}}(E_1)}.$$

By definition, we have $j(E_1') = j(E_1^{(p^e)}) = j(E_1)^{p^e}$, so that $\mathrm{h}_{\mathsf{mod}}(E_1') = p^e \cdot \mathrm{h}_{\mathsf{mod}}(E_1)$ and, similarly, we have $\mathrm{h}_{\mathsf{mod}}(E_2') = p^f \cdot \mathrm{h}_{\mathsf{mod}}(E_2)$.

We now make use of the "semi-stable case" of Proposition 3.2 and obtain that

$$\mathrm{h}_{\mathsf{mod}}(E_2') - \mathrm{h}_{\mathsf{mod}}(E_1') \overset{(i)}{=} 12 \cdot (\mathrm{h}_{\mathsf{diff}}(E_2'/L) - \mathrm{h}_{\mathsf{diff}}(E_1'/L)) + 0 \overset{(ii)}{=} 0.$$

Here, equality (i) follows from Proposition 3.2: the 'error term' in the comparison of heights vanishes because the curves are semi-stable over L (hence $\mathrm{h}_{\mathsf{diff}}(E_i'/L)$ is really $\mathrm{h}_{\mathsf{st}}(E_i')$). Equality (ii) comes from the fact that $\psi : E_1' \to E_2'$, being biseparable, preserves the differential height (see Theorem 5.1).

Therefore $\mathrm{h}_{\mathsf{mod}}(E_1') = \mathrm{h}_{\mathsf{mod}}(E_2')$, and the result is proved. □

5.4. Isogenies and differential heights. – As we saw in §5.1, biseparable isogenies preserve the differential height (Theorem 5.1). If K has characteristic 0, all isogenies are biseparable so that Theorem 5.4 completely solves the problem of describing the effect of isogenies on the differential height. In this subsection, we thus assume that the function field K has positive characteristic p and attempt to describe this effect. In view of the decomposition given by Proposition 4.6, it is enough to focus on the effect of the Frobenius isogeny on $\mathrm{h}_{\mathsf{diff}}$: this is what we elucidate now.

Lemma 5.5. *Let K be a function field of characteristic $p > 0$. For any non-isotrivial elliptic curve E over K, there exists $\alpha(E/K) \geq 1$ such that, for any power q of p, we have*

$$\alpha(E/K)^{-1} \cdot q \cdot \mathrm{h}_{\mathsf{diff}}(E/K) \leq \mathrm{h}_{\mathsf{diff}}(E^{(q)}/K) \leq q \cdot \mathrm{h}_{\mathsf{diff}}(E/K). \tag{5.1}$$

If, moreover, E is semi-stable over K, we have $\alpha(E/K) = 1$ and $\mathrm{h}_{\mathsf{diff}}(E^{(q)}) = q \cdot \mathrm{h}_{\mathsf{diff}}(E/K)$.

Proof. To lighten notation, we write $E' := E^{(q)}$. For any place v of K, denote the ring of integers at v by $\mathcal{O}_v \subset K$. We may pick a minimal v-integral Weierstrass model for E of the form:

$$E: \quad y^2 + a_{1,v}xy + a_{3,v}y = x^3 + a_{2,v}x^2 + a_{4,v}x + a_{6,v},$$

with $a_{1,v}, \ldots, a_{6,v} \in \mathcal{O}_v$. By definition, the discriminant $\Delta_{E,v} = \Delta(a_{1,v}, \ldots, a_{6,v}) \in \mathcal{O}_v$ of this model has minimal valuation $v(\Delta_{E,v})$ among all choices of Weierstrass coefficients $a_{1,v}, \ldots, a_{6,v} \in \mathcal{O}_v$ for E.

A Weierstrass model for the Frobenius twist $E' = E^{(q)}$ is then given by:

$$E': \quad y^2 + a_{1,v}^q xy + a_{3,v}^q y = x^3 + a_{2,v}^q x^2 + a_{4,v}^q x + a_{6,v}^q. \tag{5.2}$$

We note that $a_{1,v}^q, \ldots, a_{6,v}^q$ all lie in $\mathcal{O}_v$, so that (5.2) is a v-integral model for E'. The discriminant Δ_v' of this model is clearly equal to $\Delta_{E,v}^q$. Let $\Delta_{E',v}$ be the discriminant of a minimal v-integral Weierstrass model of E'. Since Δ_v' and $\Delta_{E',v}$ differ by the 12-th power of an element of $\mathcal{O}_v$, the difference $v(\Delta_v') - v(\Delta_{E',v})$ is a non-negative integral multiple of 12. In particular, we obtain that $q \cdot v(\Delta_{E,v}) \geq v(\Delta_{E',v})$. Multiplying this inequality by $\deg v$, and summing over all places v of K yields that

$$q \cdot \deg \Delta_{\min}(E/K) \geq \deg \Delta_{\min}(E'/K).$$

The right-most inequality in (5.1) ensues immediately. To prove the other inequality in (5.1), we argue as follows. The proof of Proposition 3.2 implies the bounds:

$$0 \leq \deg \Delta_{\min}(E/K) - \deg \mathrm{div}_\infty(j(E)) \leq 12 \deg \mathcal{A}(E/K), \tag{5.3}$$

where $\mathcal{A}(E/K) = \sum_{v \text{ not s.s.}} v$ is the divisor whose support consists in the places v of K where E does not have semi-stable reduction. In particular, we have

$$\deg \Delta_{\min}(E'/K) \geq \deg \mathrm{div}_\infty(j(E')) \qquad \text{and} \qquad \deg \Delta_{\min}(E/K) \leq \deg \mathrm{div}_\infty(j(E)) + 12 \deg \mathcal{A}(E/K).$$

Therefore, since $j(E') = j(E)^q$, we deduce that

$$\begin{aligned} \frac{q \cdot \deg \Delta_{\min}(E/K)}{\deg \Delta_{\min}(E'/K)} &\leq \frac{q \cdot \deg \Delta_{\min}(E/K)}{\deg \mathrm{div}_\infty(j(E'))} = \frac{q \cdot \deg \Delta_{\min}(E/K)}{q \cdot \deg \mathrm{div}_\infty(j(E))} \\ &\leq \frac{\deg \mathrm{div}_\infty(j(E)) + 12 \deg \mathcal{A}(E/K)}{\deg \mathrm{div}_\infty(j(E))} = \alpha(E/K), \end{aligned}$$

where we have set $\alpha(E/K) := 1 + 12 \deg \mathcal{A}(E/K)/(\deg \mathrm{div}_\infty j(E))$. From which we obtain that

$$q \cdot \mathrm{h}_{\mathsf{diff}}(E/K) \leq \alpha(E/K) \cdot \mathrm{h}_{\mathsf{diff}}(E'/K).$$

It is clear that $\alpha(E/K) \geq 1$, and that $\alpha(E/K) = 1$ if and only if E/K is semi-stable. The above proves both the left-most inequality in (5.1) and the last assertion of the Lemma. □

Remark 5.6. We assume here that K has characteristic $p \neq 2, 3$. Let E be a non-isotrivial elliptic curve over K, and $E' := E^{(q)}$ be its q-th power Frobenius twist. Since E and E' are K-isogenous, they have the same reduction behaviour at all places of K.

If v is a place where E has multiplicative reduction of type $\mathbf{I}_n$, for some $n \geq 1$, then E' also has multiplicative reduction at v, and its fiber at v is of type $\mathbf{I}_{n \cdot q}$. Therefore we have $v(\Delta_{\min}(E/K)) \leq qv(\Delta_{\min}(E/K)) = v(\Delta_{\min}(E'/K))$. If v is a place where E has additive reduction, then by inspection of the possible Kodaira–Néron reduction types of E' at v (see the table p. 365 of [Sil94], which is only valid in characteristic $p \neq 2, 3$), we find that $v(\Delta_{\min}(E/K)) \leq 12 v(\Delta_{\min}(E'/K))$. Therefore, for any place v where either of E and E' have bad reduction, we have

$$v(\Delta_{\min}(E/K)) \leq 12 v(\Delta_{\min}(E'/K)).$$

Multiplying this inequality by $\deg v$ and summing over all places v of K, we obtain that

$$\frac{1}{12} \cdot \mathrm{h}_{\mathsf{diff}}(E/K) \leq \mathrm{h}_{\mathsf{diff}}(E^{(q)}/K).$$

This may be viewed as a weak (but uniform) version of the lower bound in (5.1).

We can now give the final estimate of this subsection.

Proposition 5.7. *Let E_1, E_2 be a pair of* non-isotrivial *elliptic curves over a function field K. Assume that there exists an isogeny $\varphi : E_1 \to E_2$. If both E_1 and E_2 are semi-stable over K, we have*

$$\mathrm{h}_{\mathsf{diff}}(E_2/K) = \frac{\deg_{\mathrm{ins}} \varphi}{\deg_{\mathrm{ins}} \widehat{\varphi}} \cdot \mathrm{h}_{\mathsf{diff}}(E_1/K).$$

In general, we have

$$\alpha(E_2/K)^{-1} \leq \frac{\deg_{\mathrm{ins}} \varphi \cdot \mathrm{h}_{\mathsf{diff}}(E_1/K)}{\deg_{\mathrm{ins}} \widehat{\varphi} \cdot \mathrm{h}_{\mathsf{diff}}(E_2/K)} \leq \alpha(E_1/K),$$

where $\alpha(E_1/K), \alpha(E_2/K) \geq 1$ are the same as in Lemma 5.5.

Proof. The semi-stable case is a direct consequence of Theorem 5.4 and Corollary 3.3. In the general case, by Proposition 4.1, the isogeny $\varphi : E_1 \to E_2$ decomposes as

$$\varphi : E_1 \xrightarrow{\mathrm{Fr}_{p^e}} E_1^{(p^e)} \xrightarrow{\psi} E_2^{(p^f)} \xrightarrow{\mathrm{V}_{p^f}} E_2,$$

where ψ is a biseparable isogeny, $p^e = \deg_{\mathrm{ins}}(\varphi)$, and $p^f = \deg_{\mathrm{ins}}(\widehat{\varphi})$. We then write that

$$\frac{\mathrm{h}_{\mathsf{diff}}(E_1)}{\mathrm{h}_{\mathsf{diff}}(E_2)} = \frac{\mathrm{h}_{\mathsf{diff}}(E_1)}{\mathrm{h}_{\mathsf{diff}}(E_1^{(p^e)})} \cdot \frac{\mathrm{h}_{\mathsf{diff}}(E_1^{(p^e)})}{\mathrm{h}_{\mathsf{diff}}(E_2^{(p^f)})} \cdot \frac{\mathrm{h}_{\mathsf{diff}}(E_2^{(p^f)})}{\mathrm{h}_{\mathsf{diff}}(E_2)}.$$

Since the isogeny $\psi : E_1^{(p^e)} \to E_2^{(p^f)}$ is biseparable, Theorem 5.1 yields that the ratio $\mathrm{h}_{\mathsf{diff}}(E_1^{(p^e)})/\mathrm{h}_{\mathsf{diff}}(E_2^{(p^f)})$ is 1. To conclude, one then applies inequality (5.1) in Lemma 5.5 to the other two ratios. □

Remark 5.8. If K has characteristic $p \neq 2, 3$, we may carry out the same argument using the bound in Remark 5.6 instead of inequality (5.1). We would then obtain the following bound. If $\varphi : E_1 \to E_2$ is an isogeny between two non-isotrivial elliptic curves over K, we have

$$(12 \deg_{\mathrm{ins}}(\varphi))^{-1} \leq \frac{\mathrm{h}_{\mathsf{diff}}(E_1/K)}{\mathrm{h}_{\mathsf{diff}}(E_2/K)} \leq 12 \deg_{\mathrm{ins}}(\widehat{\varphi}).$$

5.5. A surprising consequence on isogeny classes. – Let E be a non CM elliptic curve over $\mathbb{Q}$. For any $B \geq 0$, consider the set

$$\mathscr{E}_{\mathbb{Q}}(E, B) = \left\{E'/\overline{\mathbb{Q}} : E' \text{ is isogenous to } E \text{ and } ht(j(E')) \leq B\right\} / \,\overline{\mathbb{Q}}\text{-isomorphism},$$

where $ht : \overline{\mathbb{Q}} \to \mathbb{R}$ is the standard logarithmic absolute Weil height on $\overline{\mathbb{Q}}$. It is known that $\mathscr{E}_{\mathbb{Q}}(B)$ is a finite set (see Lemma 5.9 in [Hab13]). The main input in the proof is an estimate from [SU99] (see Théorème 1.1 there) which states that

$$ht(j(E')) \geq ht(j(E)) + \frac{1}{2} \log \deg \varphi - o(\log \deg \varphi)$$

if there is a cyclic isogeny $\varphi : E \to E'$ (where the implicit constants in the error term depend on E). Using our results in §5.3, we study a set analogous to $\mathscr{E}_{\mathbb{Q}}(E, B)$ in the context of function fields.

Let K be a function field as in section 1, with characteristic $p \geq 0$. Let E be a fixed non-isotrivial elliptic curve over K, and write $\mathscr{E}_{\mathrm{bs}}(E)$ for the set of elliptic curves over $\overline{K}$ which are biseparably isogenous to E (*i.e.* such that there is a biseparable isogeny $E \to E'$). For any real number $B \geq 1$, consider the set

$$\mathscr{E}_K(E, B) = \left\{E' \in \mathscr{E}_{\mathrm{bs}}(E) : \mathrm{h}_{\mathsf{mod}}(E') \leq B\right\} / \,\overline{K}\text{-isomorphism}.$$

When the characteristic of K is 0, all isogenies are biseparable, so that $\mathscr{E}_{\mathrm{bs}}(E)$ is the whole isogeny class of E. The biseparable condition was added in order to avoid trivial situations in positive characteristic: without this condition, if K has characteristic p, we would indeed directly obtain infinitely many (isomorphism classes of) elliptic curves over $\overline{K}$ which are isogenous to E and have bounded modular height by considering the sequence

$$\ldots \xrightarrow{\mathrm{V}_p} E^{(1/p^n)} \xrightarrow{\mathrm{V}_p} E^{(1/p^{n-1})} \xrightarrow{\mathrm{V}_p} \ldots \xrightarrow{\mathrm{V}_p} E^{(1/p^2)} \xrightarrow{\mathrm{V}_p} E^{(1/p)} \xrightarrow{\mathrm{V}_p} E.$$

In stark contrast to the above mentioned result of Habegger, we prove:

Proposition 5.9. *If $B \geq \mathrm{h}_{\mathsf{mod}}(E)$, the set $\mathscr{E}_K(E, B)$ is infinite.*

Proof. Given an integer $n \geq 1$ which is coprime to the characteristic p of K, we may pick a point $P_n \in E(\overline{K})$ of exact order n. We then let π_n denote the quotient isogeny $\pi_n : E \to E/\langle P_n \rangle$ from E to its quotient E_n by the subgroup generated by P_n. The isogeny π_n has degree n (see Proposition 4.3), and is therefore biseparable (see Lemma 4.5).

This construction provides a sequence $(E_n)_n$ of elliptic curves over $\overline{K}$ indexed by prime-to-p integers. Let us prove that (the isomorphism class of) E_n lies in $\mathscr{E}_K(E, B)$ if the requirement on B is met. It is clear that the curve $E_n/\overline{K}$ is biseparably isogenous to E. Applying Theorem 5.4 to the isogeny $\pi_n : E \to E_n$ yields that $\mathrm{h}_{\mathsf{mod}}(E_n) = \mathrm{h}_{\mathsf{mod}}(E)$. Therefore, the isomorphism class of E_n does belong to $\mathscr{E}_K(E, B)$, thanks to our assumption that $\mathrm{h}_{\mathsf{mod}}(E) \leq B$.

In order to conclude the proof, it now suffices to show that the above-constructed sequence $(E_n)_n$ provides infinitely many isomorphism classes. Let ℓ_1, ℓ_2 be two prime numbers, both coprime to p, and assume that $E_{\ell_1} \simeq E_{\ell_2}$. Let us denote the isomorphism by $\iota : E_{\ell_1} \to E_{\ell_2}$. The composition $\lambda := \iota \circ \pi_{\ell_1}$ is an isogeny $E \to E_{\ell_2}$ of degree ℓ_1. Hence, the isogeny $\psi : E \to E$ defined by $\psi = \widehat{\pi_{\ell_2}} \circ \lambda$ is a biseparable endomorphism of E of degree $\ell_1 \ell_2$. Since E is non-isotrivial, its endomorphism ring is trivial; hence, there is an integer d such that $\psi = [d]$. Taking degrees, we obtain in particular that $d^2 = \ell_1 \ell_2$. Since ℓ_1 and ℓ_2 are primes, we deduce that $\ell_1 = \ell_2 = d$. Thereby we conclude that the sequence $(E_\ell)_\ell$ indexed by prime numbers $\ell \neq p$ provides infinitely many elements in $\mathscr{E}_K(E, B)$. □

The main difference between the number field and the function field cases lies in how much the modular height varies along an isogeny class. Over number fields, the above-mentioned Théorème 1.1 in [SU99] shows that $ht(j(E'))$ does vary as $E'/\overline{\mathbb{Q}}$ runs through the isogeny class of $E/\overline{\mathbb{Q}}$, provided that E has no CM. Therefore, bounding $ht(j(E'))$ sufficiently constrains the degree of possible isogenies $E \to E'$ that the set $\mathscr{E}_{\mathbb{Q}}(E, B)$ is finite. Over a function field K, on the contrary, our Theorem 5.4 shows that $\mathrm{h}_{\mathsf{mod}}(E')$ remains constant as E' runs through $\mathscr{E}_{\mathrm{bs}}(E)$, provided that E is non-isotrivial. The absence of constraints on the degree of isogenies $E \to E'$ other than coprimality with the characteristic, allows the set $\mathscr{E}_K(E, B)$ to be infinite.

6. An isogeny estimate

The goal in this last section is to prove the second main result of the paper (Theorem B), which is the following isogeny estimate:

Theorem 6.1. *Let K be a function field of genus g. For any pair of non-isotrivial isogenous elliptic curves E_1, E_2 defined over K, there exists an isogeny $\varphi_0 : E_1 \to E_2$ with*

$$\deg \varphi_0 \leq 49 \max\{1, g\} \cdot \max \left\{ \frac{\deg_{\mathrm{ins}} j(E_1)}{\deg_{\mathrm{ins}} j(E_2)}, \frac{\deg_{\mathrm{ins}} j(E_2)}{\deg_{\mathrm{ins}} j(E_1)} \right\},$$

where $\deg_{\mathrm{ins}} j(E_1), \deg_{\mathrm{ins}} j(E_2)$ *are the inseparability degrees of* $j(E_1), j(E_2)$.

If K has characteristic 0, the inseparability degrees appearing on the right-hand side of the inequality should be interpreted as 1. Specifically, in that situation, the statement above yields that there is an effective constant $c_1 > 0$ (depending only on the genus of K) such that: for all pairs E_1, E_2 of non-isotrivial $\overline{K}$-isogenous elliptic curves, there exists a ($\overline{K}$-)isogeny $\varphi_0 : E_1 \to E_2$ with $\deg \varphi_0 \leq c_1$. This isogeny estimate is thus *uniform* for a fixed K. This should be compared to the number field case (treated in [MW90, Pel01, GR14]) where the right-hand side of such isogeny estimates depend on the heights of the involved elliptic curves.

Let us remark that, in positive characteristic p, the appearance of the inseparability degrees on the right-hand side is unavoidable, because of Theorem 5.4 and the existence of the Frobenius isogeny. Given a non-isotrivial elliptic curve E/K, the smallest isogeny between E and its Frobenius twist $E^{(p)}$ is indeed the p-th power Frobenius, which has degree p. Similar considerations with the Verschiebung show, more generally, that the dependency in $\deg_{\mathrm{ins}} j(E_1)$ and $\deg_{\mathrm{ins}} j(E_2)$ on the right-hand side of the bound in Theorem 6.1 is optimal.

Remark 6.2. If one assumes that E_1, E_2 are linked by an isogeny φ which is defined over K, then the isogeny $\varphi_0 : E_1 \to E_2$ whose existence is asserted in Theorem 6.1 is also defined over K. More generally, all isogenies $E_1 \to E_2$ are then defined over K. See Lemma 6.10 below.

6.1. Preliminaries about modular curves.

– Let us briefly recall some facts about modular curves. Given an integer $N \geq 1$, there is a smooth scheme $\mathcal{Y}_0(N)$ of relative dimension 1 over $\operatorname{Spec} \mathbb{Z}[1/N]$ which is a coarse moduli scheme for elliptic curves endowed with a cyclic subgroup of order N. In other words, the curve $\mathcal{Y}_0(N)$ enjoys the following property: For any field F whose characteristic is coprime to N, there is a bijection (which is functorial in F) between the set $\mathcal{Y}_0(N)(F)$ and the set of equivalence classes of pairs (E, H) where E is an elliptic curve over F, and H is a cyclic subgroup of E of order N which is stable under the action of the absolute Galois group of F. Two such pairs are called equivalent if they are isomorphic over the algebraic closure $\overline{F}$ of F. These properties of $\mathcal{Y}_0(N)$ are explained in more details in [DI95, §8], and the construction is carried out comprehensively in [KM85] (in particular, Chapters III, VI and VIII there). Adding a finite number of points (called cusps) to $\mathcal{Y}_0(N)$, one obtains the usual compactification, denoted by $\mathcal{X}_0(N)$, of $\mathcal{Y}_0(N)$. The smooth projective curve $\mathcal{X}_0(N)$ is also defined over $\operatorname{Spec} \mathbb{Z}[1/N]$ (and, further, has an interpretation as a moduli space, in terms of generalized elliptic curves, see [DI95, §9]).

In particular, the curve $\mathcal{X}_0(1)$ is nothing but the "j-line" over $\operatorname{Spec} \mathbb{Z}$ *i.e.*, $\mathcal{X}_0(1) \simeq \mathbb{P}^1_{/\mathbb{Z}}$, where the isomorphism is given on isomorphism classes of elliptic curves by $E \mapsto j(E)$.

For any divisor n of N, there is a "degeneration" morphism $\mathcal{X}_0(N) \to \mathcal{X}_0(n)$, which extends the map on pairs (E, H) as above, defined by $(E, H) \mapsto (E, \frac{N}{n} H)$. In the special case $n = 1$, we obtain a map $f_N : \mathcal{X}_0(N) \to \mathcal{X}_0(1) = \mathbb{P}^1$, which extends the map $(E, H) \mapsto E \mapsto j(E)$.

Let $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$ be the subgroup formed by 2×2 integral matrices of determinant 1 whose reduction modulo N is upper triangular. The fiber $X_0(N) := \mathcal{X}_0(N) \times \mathbb{C}$ is isomorphic (as a Riemann surface) to the compactification of the quotient $\{\tau \in \mathbb{C} : \operatorname{Im} \tau > 0\}/\Gamma_0(N)$. One can show (see [Shi94, Chap. I] for instance) that the degree of the degeneration morphism $f_N : X_0(N) \to X_0(1) = \mathbb{P}^1_{/\mathbb{C}}$ is equal to the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]$. Propositions 1.40 and 1.43 in [Shi94] then show that

$$\deg f_N = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \cdot \prod_{\ell | N} \left(1 + \frac{1}{\ell}\right) := \psi(N). \tag{6.1}$$

A detailed study of the ramification behaviour of f_N, combined with the Riemann–Hurwitz formula then allows to compute the genus of $X_0(N)$. Specifically, Propositions 1.40 and 1.43 in [Shi94] yield that the modular curve $X_0(N)$ has genus

$$g(X_0(N)) = 1 + \frac{\psi(N)}{12} - \frac{\nu_2(N)}{4} - \frac{\nu_3(N)}{3} - \frac{\nu_\infty(N)}{2}, \tag{6.2}$$

where $\psi(N)$ is as above, $\nu_\infty(N) = \sum_{d|N} \varphi(\gcd(d, N/d))$, and

$$\nu_2(N) = \begin{cases} 0 & \text{if } 4 \mid N, \\ \prod_{\ell|N} \left(1 + \left(\frac{-1}{\ell}\right)\right) & \text{if } 4 \nmid N, \end{cases} \quad \text{and} \quad \nu_3(N) = \begin{cases} 0 & \text{if } 9 \mid N, \\ \prod_{\ell|N} \left(1 + \left(\frac{-3}{\ell}\right)\right) & \text{if } 9 \nmid N. \end{cases}$$

Here φ denotes Euler's totient function, and $(\cdot/\ell)$ is the Legendre symbol.

We end this brief summary by estimating the growth of the genus $g(X_0(N))$ of $X_0(N)$ as N grows. We thank Gaël Rémond for the following argument, which yields better bounds than our original proof.

Lemma 6.3. *For any integer $N \geq 300$, we have $g(X_0(N)) \geq N/49$. Moreover, for all $N \geq 1$, we have*

$$N \leq 49 \max\{1, g(X_0(N))\}.$$

Proof. We estimate separately the terms on the right-hand side of equation (6.2). We start by noticing that ν_∞, ν_2 and ν_3 are all multiplicative functions. For any prime ℓ, and any integer $e \geq 1$, one has

$$\nu_\infty(\ell^e) = \begin{cases} \sqrt{\ell^e}\left(1 + \ell^{-1}\right) & \text{if } 2 \mid e, \\ \sqrt{\ell^e} \cdot 2\ell^{-1/2} & \text{if } 2 \nmid e. \end{cases}$$

Since, for all ℓ, we have $1 + \ell^{-1} \geq 2\ell^{-1/2}$, the multiplicativity of ν_∞ implies that, for all $N \geq 1$,

$$\frac{\nu_\infty(N)}{\sqrt{N}} \leq \prod_{\ell|N} \left(1 + \frac{1}{\ell}\right) = \frac{\psi(N)}{N}.$$

Hence we deduce that $\nu_\infty(N) \leq \psi(N)/\sqrt{N}$.

Similarly, we notice that $\max\{\nu_2(\ell^e), \nu_3(\ell^e)\} \leq \nu_\infty(\ell^e)$ for all primes ℓ and integers $e \geq 1$. We directly infer that, for any integer $N \geq 1$, one has $\max\{\nu_2(N), \nu_3(N)\} \leq \nu_\infty(N)$.

Plugging these bounds into equation (6.2) yields that

$$\begin{aligned} g(X_0(N)) &\geq 1 + \frac{\psi(N)}{12} - \frac{7}{12}\max\{\nu_2(N), \nu_3(N)\} - \frac{1}{2}\nu_\infty(N) \\ &\geq 1 + \frac{\psi(N)}{12} - \frac{13}{12}\nu_\infty(N) \geq 1 + \frac{\psi(N)}{12}\left(1 - \frac{13}{\sqrt{N}}\right). \end{aligned}$$

By definition of ψ, we have $\psi(N) \geq N$. Therefore, $g(X_0(N)) > \frac{N}{12}\left(1 - \frac{13}{\sqrt{N}}\right)$ for $N \geq 13^2$. Furthermore, as a quick computation shows, for any $N \geq 297$, we have

$$g(X_0(N)) > \frac{N}{12}\left(1 - \frac{13}{\sqrt{N}}\right) \geq \frac{N}{49}.$$

This proves the first assertion of the lemma.

Direct calculations with formula (6.2) using a computer show that the bound $N \leq 49 \max\{1, g(X_0(N))\}$ also holds for all $N \in \{1, \ldots, 299\}$. (The worst case is $N = 49$ for which $g(X_0(N)) = 1$.) □

Remark 6.4. Depending on the situation at hand, the bounds of Lemma 6.3 can be somewhat optimized. For instance, one can deduce from $12g(X_0(N)) > \sqrt{N}(\sqrt{N} - 13)$ that $N \leq 25g(X_0(N))$ for all $N \geq 625$. Explicit computations for $N \in \{1, \ldots, 624\}$ then show that

$$N \leq \max\{49, 25g(X_0(N))\} \leq 49 \max\{1, 0.5 \cdot g(X_0(N))\},$$

for all $N \geq 1$. In a similar vein, one can show that $N \leq 13g(X_0(N))$ for all $N \geq 28561$, and check with the help of a computer that, for all $N \geq 1$,

$$N \leq \max\{3721, 13g(X_0(N))\} \leq 3721 \max\{1, 0.004 \cdot g(X_0(N))\}.$$

The worst case happens for $N = 3721$ when $g(X_0(N)) = 284$. These inequalities are more precise than Lemma 6.3 for larger genera.

In the other direction, explicit computation using formula (6.2) show that the modular curve $X_0(N)$ has genus zero if and only if $N \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}$.

6.2. Bounding biseparable isogenies. – Let K be a function field with field of constants k, and fix a model C of K (see §1). We write $g(C)$ for the genus of C (which we also call the genus of K), and we let G_K denote the absolute Galois group of K.

Let $d \geq 1$ be an integer which is coprime to the characteristic of K. Assume that we are given a non-isotrivial elliptic curve E over K, equipped with a cyclic, G_K-stable subgroup $H \subset E$ of order d. Consider the modular curve $\mathcal{X}_0(d)$, defined over $\operatorname{Spec}\mathbb{Z}[1/d]$, and write $X_0(d)_{/F}$ for its base change to a field F whose characteristic is prime to d. By the coarse moduli space interpretation of $\mathcal{X}_0(d)$, there is a canonical map sending the K-isomorphism class of the pair (E, H) to a non-cuspidal K-rational point P on $\mathcal{X}_0(d)$. From the given data, we thus deduce a non-cuspidal K-rational point $P \in \mathcal{X}_0(d)$.

By definition, the point P is given by a morphism $\operatorname{Spec} K \to \mathcal{X}_0(d)$ over $\operatorname{Spec}\mathbb{Z}[1/d]$, which factors as a morphism $\operatorname{Spec} K \to X_0(d)_{/k}$ over $\operatorname{Spec} k$. Since $\operatorname{Spec} K$ is the generic point of C, the latter induces a rational map $C \dashrightarrow X_0(d)_{/k}$. Since both C and $X_0(d)_{/k}$ are smooth projective curves over k, this rational map extends to a morphism $s_P : C \to X_0(d)_{/k}$ over k.

Let $f_d : X_0(d)_{/k} \to X_0(1)_{/k} = \mathbb{P}^1_{/k}$ denote the degeneration morphism, which extends the map sending a pair (E', H') to $j(E')$. By construction, the morphism $j_E : C \to \mathbb{P}^1_{/k}$ deduced from the j-invariant of E factors through s_P and f_d. In other words, the diagram

$$\begin{tikzcd} C \arrow[rr, "s_P"] \arrow[dr, "j_E"'] & & X_0(d)_{/k} \arrow[dl, "f_d"] \\ & \mathbb{P}^1_{/k} & \end{tikzcd} \tag{6.3}$$

is commutative. We may now prove the following:

Proposition 6.5. *Let E be a non-isotrivial elliptic curve over K. Let $H \subset E$ be a cyclic, G_K-stable subgroup of order d. If d is coprime to the characteristic of K, we have*

$$d \leq 49 \max\{1, g(C)\}.$$

Proof. By the discussion above, the data (E, H) of the proposition yields a morphism $s_P : C \to X_0(d)_{/k}$ such that the diagram (6.3) commutes. The fact that E is non-isotrivial implies that $j_E : C \to \mathbb{P}^1_{/k}$ is not constant which, in particular, ensures that the morphism $s_P : C \to X_0(d)_{/k}$ is non-constant.

A weak version of the Riemann–Hurwitz formula then entails that the genus of $X_0(d)_{/k}$ is no greater than that of C. Since $\mathcal{X}_0(d)$ is a smooth curve other $\operatorname{Spec}\mathbb{Z}[1/d]$, the genus of $X_0(d)_{/k}$ is equal to the genus of the complex Riemann surface $X_0(d)_{/\mathbb{C}}$. This means that $g(C) \geq g(X_0(d)_{/\mathbb{C}})$. We then appeal to the lower bound of Lemma 6.3, which shows that $d \leq 49 \max\{1, g(X_0(d)_{/\mathbb{C}})\}$.

We obtain that $d \leq 49 \max\{1, g(X_0(d)_{/\mathbb{C}})\} \leq 49 \max\{1, g(C)\}$. □

We now state and prove a variant of the previous proposition, which is significantly weaker (it is not uniform in the elliptic curve) but which might prove more flexible. This version may indeed be of interest for applications where one studies elliptic curves defined over a varying field L whose degree over K is bounded (in which case a bound depending on the genus of L may be too crude). We provide an instance of such an application in §6.5.

Proposition 6.6. *Let K be a function field and let L/K be a finite extension. Let E be a non-isotrivial elliptic curve over L, and $H \subset E$ be a cyclic, G_L-stable subgroup of order d. Assuming that d is coprime to the characteristic of K, we have*

$$d \leq [L : K] \cdot \mathrm{h}_{\mathsf{mod}}(E).$$

Proof. We fix a model C' of L, and denote the constant field of L by k'. Carrying out the argument preceding the previous proposition with L instead of K, we deduce from the input (E, H) an L-rational point Q on the modular curve $\mathcal{X}_0(d)$, and a morphism $s_Q : C' \to X_0(d)_{/k'}$. As in (6.3), the j-invariant $j_E : C' \to \mathbb{P}^1_{/k'}$ factors through s_Q; we thus have $j_E = f_d \circ s_Q$, where $f_d : X_0(d)_{/k'} \to \mathbb{P}^1_{/k'}$ is the degeneration map. Since $j_E = f_d \circ s_Q$, it is clear that $\deg(j_E) \geq \deg(f_d)$.

As was recalled in the previous subsection, the degree of f_d is nothing but $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(d)] = \psi(d)$. It is clear that $\psi(d) \geq d$, so that

$$\deg(j_E) \geq \deg(f_d) = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(d)] = \psi(d) \geq d.$$

Now, the degree of $j_E : C' \to \mathbb{P}^1$ is the degree of its divisor of poles $\operatorname{div}_\infty(j_E) \in \operatorname{Div}(C')$. As was remarked in §3.2, the modular height of E satisfies $\mathrm{h}_{\mathsf{mod}}(E) = [L : K]^{-1} \cdot \deg(\operatorname{div}_\infty(j_E))$. Rearranging the terms in the inequality above then yields that $d \leq [L : K] \cdot \mathrm{h}_{\mathsf{mod}}(E)$, which concludes the proof. □

We now have enough tools to treat a special case of Theorem 6.1:

Proposition 6.7. *Let E_1, E_2 be two non-isotrivial elliptic curves over K. Assume that there exists a biseparable isogeny $\varphi : E_1 \to E_2$. Then there exists a biseparable isogeny $\varphi_0 : E_1 \to E_2$ with*

$$\deg \varphi_0 \leq 49 \max\{1, g(K)\}.$$

Note that, when K has characteristic 0, the proof of this statement will conclude that of Theorem 6.1. Since K is then perfect, all isogenies are indeed biseparable in that case. The following proof uses arguments inspired by the ones of [Ulm11, Lect. I, Prop. 7.1], which proves a uniform upper bound for the order of the prime-to-p K-rational torsion on an elliptic curve over K.

Proof. Fix a biseparable isogeny $\varphi : E_1 \to E_2$, and consider the set of positive integers:

$$\mathscr{D} := \{\deg \phi,\ \phi : E_1 \to E_2 \text{ biseparable isogeny}\} \subset \mathbb{Z}_{\geq 1}.$$

By assumption, $\mathscr{D}$ contains $\deg \varphi$ and is thus not empty. Hence $\mathscr{D}$ contains a minimal element d_0, and there exists a biseparable isogeny $\varphi_0 : E_1 \to E_2$ with $\deg \varphi_0 = d_0$. Note that the degree d_0 of φ_0 is coprime to p, for φ_0 is biseparable (see Lemma 4.5).

Let us now prove that φ_0 is cyclic *i.e.*, that the group $H_0 := (\ker \varphi_0)(\overline{K})$ is cyclic. By the structure theorem for finite Abelian groups, and by the description of finite subgroups of E_1, we know that H_0 is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ for some integers $m, n \geq 1$ with $m \mid n$ and $mn = \deg_{\text{sep}}(\varphi_0) = d_0$. In particular, the kernel of the multiplication-by-m map $[m] : E_1 \to E_1$ is a subgroup of H_0 which is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^2$. Proposition 4.2 then implies that the isogeny φ_0 can be factored as $\varphi_0 = \varphi_1 \circ [m]$ for a unique isogeny $\varphi_1 : E_1 \to E_2$. Taking degrees yields that $\deg \varphi_0 = d_0 = \deg \varphi_1 \cdot m^2$. This shows that φ_1 is biseparable: indeed, being a divisor of d_0, $\deg \varphi_1$ must be coprime to p (Lemma 4.5). On the other hand, the degree of φ_0 is minimal among all degrees of biseparable isogenies $E_1 \to E_2$. We thus have $m = 1$, and the kernel of φ_0 is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Hence H_0 is cyclic, as claimed.

Since the degree of φ_0 is coprime to the characteristic of K, Lemma 4.7 shows that the kernel H_0 of φ_0 is defined over a separable extension of K, *i.e.* that the extension $K(H_0)/K$ is separable. Let G_K denote the absolute Galois group of K. We now prove that H_0 is stable under the action of G_K on E_1 (in other words, we show that H_0 is "defined over K").

To do so, we first prove that ${}^\sigma\varphi_0 = \pm\varphi_0$ for all $\sigma \in G_K$. Let $\sigma \in G_K$ be an arbitrary automorphism. Since both E_1 and E_2 are defined over K, we get an isogeny ${}^\sigma\varphi_0 : E_1 \to E_2$ of degree d_0. The composition of the dual $\widehat{\varphi_0} : E_2 \to E_1$ with ${}^\sigma\varphi_0 : E_1 \to E_2$ yields an endomorphism $\widehat{\varphi_0} \circ {}^\sigma\varphi_0$ of E_1. The curve E_1 being non-isotrivial, it has no non-trivial endomorphisms (see §2.4), so that there exists an integer n such that $\widehat{\varphi_0} \circ {}^\sigma\varphi_0 = [n]$ is the multiplication-by-n. Comparing degrees, we get that $n = \pm d_0$, whence $\widehat{\varphi_0} \circ {}^\sigma\varphi_0 = [\pm d_0] = [\pm 1] \circ \widehat{\varphi_0} \circ \varphi_0$. Therefore $\widehat{\varphi_0} \circ ({}^\sigma\varphi_0 - [\pm 1] \circ \varphi_0) = 0$, and we deduce that the image of ${}^\sigma\varphi_0 - [\pm 1] \circ \varphi_0$ is contained in the kernel of $\widehat{\varphi_0}$. Since the latter is finite, ${}^\sigma\varphi_0 - [\pm 1] \circ \varphi_0$ must be constant equal to 0. Thus ${}^\sigma\varphi_0 = \pm\varphi_0$, as claimed.

It then formally follows from the previous paragraph that H_0 is stable under the action of G_K. We may now apply Proposition 6.5 to the pair (E_1, H_0), and we infer that $d_0 = \deg \varphi_0 \leq 49 \max\{1, g(K)\}$. □

6.3. Proof of Theorem 6.1. – We can now conclude the proof of the main theorem of this section. Let E_1 and E_2 be non-isotrivial isogenous elliptic curves over K: we fix a $\overline{K}$-isogeny $\varphi : E_1 \to E_2$ between them. If φ is biseparable, Proposition 6.7 in the previous subsection already allows us to conclude. To treat the general case, we require the following lemma:

Lemma 6.8. *Let E_1, E_2 be two non-isotrivial elliptic curves over K. We assume that $j(E_1)$ and $j(E_2)$ have the same inseparability degree, and that there exists an isogeny $\varphi : E_1 \to E_2$. Then there exists a biseparable isogeny $\psi : E_1 \to E_2$ with $\deg \psi \mid \deg \varphi$.*

Since E_1, E_2 are non-isotrivial isogenous elliptic curves, it can be shown that the $\mathbb{Z}$-module $\operatorname{Hom}(E_1, E_2)$, consisting of isogenies $E_1 \to E_2$ together with the constant trivial morphism, is free of rank 1. We may thus fix an isogeny $\varphi_0 : E_1 \to E_2$ which generates $\operatorname{Hom}(E_1, E_2)$. This generator φ_0 has minimal degree among all non-zero elements in $\operatorname{Hom}(E_1, E_2)$. Assuming that $\deg_{\text{ins}} j(E_1) = \deg_{\text{ins}} j(E_2)$, the above result shows that φ_0 must be biseparable.

Proof. We begin by decomposing φ as in Proposition 4.6: there is a biseparable isogeny $\phi_s : E_1^{(p^a)} \to E_2^{(p^b)}$ such that

$$\varphi = \mathrm{V}_{p^b} \circ \phi_s \circ \mathrm{Fr}_{p^a},$$

where $\deg_{\mathrm{ins}}\varphi = p^a$ and $\deg_{\mathrm{ins}}\widehat{\varphi} = p^b$. Moreover the degree m of ϕ_s is coprime to p. By assumption we have $\deg_{\mathrm{ins}} j(E_2) = \deg_{\mathrm{ins}} j(E_1)$, hence Theorem 5.4 implies that $p^a = \deg_{\mathrm{ins}}\varphi = \deg_{\mathrm{ins}}\widehat{\varphi} = p^b$, so that $a = b$. In particular, we have $\deg\varphi = p^a m p^b = p^{2a} m$ and $\deg_{\mathrm{sep}}\varphi = mp^a$. If $a = 0$ there is nothing to prove, for φ is then already biseparable. We thus assume that $a \geq 1$ in the rest of the proof.

The set of $\overline{K}$-rational points in the kernel $G := (\ker\varphi)(\overline{K})$ of φ is a finite Abelian group of order $\deg_{\mathrm{sep}}\varphi = mp^a$. (Even if the kernel is not reduced, we identify it with its set of closed points.) Since p^a divides $|G|$ and since m is coprime to p, G contains a unique subgroup H of order p^a (consisting of elements of order a power of p). By Proposition 4.3, there exist a unique elliptic curve E_1' over $\overline{K}$ and a separable isogeny $\pi : E_1 \to E_1'$ with kernel H. The isogeny π is separable of degree $\deg\pi = \deg_{\mathrm{sep}}\pi = p^a$.

By construction, $H = (\ker\pi)(\overline{K})$ is a subgroup of G and, π being separable, we deduce from Proposition 4.2 that $\varphi : E_1 \to E_2$ factors through π: there exists an isogeny $\lambda : E_1' \to E_2$ such that $\varphi = \lambda\circ\pi$. It follows from the multiplicativity of degrees that

$$\deg\lambda = \deg\varphi/\deg\pi = mp^a, \qquad \deg_{\mathrm{sep}}\lambda = \deg_{\mathrm{sep}}\varphi/\deg_{\mathrm{sep}}\pi = m, \qquad \deg_{\mathrm{ins}}\lambda = \deg_{\mathrm{ins}}\varphi/\deg_{\mathrm{ins}}\pi = p^a.$$

Again, we make use of the decomposition provided by Proposition 4.6 to factor π. Since π is separable of degree a power of p, we obtain that the diagram

$$\begin{tikzcd}
E_1 \arrow[r, "\pi"] \arrow[d, "\iota"'] & E_1' \\
(E_1')^{(p^a)} \arrow[ur, "\mathrm{V}_{p^a}"'] &
\end{tikzcd}$$

is commutative, where ι is a biseparable isogeny. Comparing degrees, we observe that ι has degree 1 and therefore must be an isomorphism $E_1 \simeq (E_1')^{(p^a)}$.

Let us apply Proposition 4.6 once more, this time to factor λ. Since the separability degree of λ is coprime to p, we deduce that $\widehat{\lambda}$ is separable. Therefore, there is a biseparable isogeny $\gamma : (E_1')^{(p^a)} \to E_2$ such that $\lambda = \gamma\circ\mathrm{Fr}_{p^a}$. Here is a diagram summarising the various isogenies considered in this proof:

$$\begin{tikzcd}
 & E_1 \arrow[r, "\varphi"] \arrow[d, "\pi"] \arrow[dl, "\sim"', "\iota"] & E_2 \arrow[d, equal] \\
(E_1')^{(p^a)} \arrow[r, "\mathrm{V}_{p^a}"'] & E_1' \arrow[r, "\lambda"] \arrow[d, "\mathrm{Fr}_{p^a}"] & E_2 \arrow[d, equal] \\
 & (E_1')^{(p^a)} \arrow[r, "\gamma"] & E_2 \\
 & E_1 \arrow[u, "\iota", "\wr"'] \arrow[ur, "\psi"'] &
\end{tikzcd}$$

We now set $\psi := \gamma\circ\iota$. The composition $\psi : E_1 \to E_2$ is an isogeny between E_1 and E_2 of degree m, which is coprime to p. Hence ψ is biseparable by Lemma 4.5, and it is clear that $\deg\psi$ divides $\deg\varphi$. □

End of the proof of Theorem 6.1. If K has characteristic 0, Proposition 6.7 proves an assertion which is equivalent to Theorem 6.1. We may therefore assume that the characteristic p of K is positive. Let $\varphi : E_1 \to E_2$ be a $\overline{K}$-isogeny. We distinguish several cases:

- If $\deg_{\mathrm{ins}} j(E_1) = \deg_{\mathrm{ins}} j(E_2)$, Lemma 6.8 implies the existence of a biseparable isogeny $\psi : E_1 \to E_2$. We can now use Proposition 6.7 and conclude that there exists an isogeny $\varphi_0 : E_1 \to E_2$ with $\deg\varphi_0 \leq 49\max\{1, g(K)\}$.

- If $\deg_{\mathrm{ins}} j(E_1) > \deg_{\mathrm{ins}} j(E_2)$, we let $p^f := \deg_{\mathrm{ins}} j(E_1)/\deg_{\mathrm{ins}} j(E_2)$. Composing $\varphi : E_1 \to E_2$ with $\mathrm{Fr}_{p^f} : E_2 \to E_2^{(p^f)}$, we obtain an isogeny $E_1 \to E_2^{(p^f)}$. By construction, $\deg_{\mathrm{ins}} j(E_1) = \deg_{\mathrm{ins}} j(E_2^{(p^f)})$. Lemma 6.8 then ensures that there exists a biseparable isogeny $\psi : E_1 \to E_2^{(p^f)}$. By Proposition 6.7, there exists an isogeny $\psi_0 : E_1 \to E_2^{(p^f)}$ with $\deg\psi_0 \leq 49\max\{1, g(K)\}$.

  Composing $\psi_0 : E_1 \to E_2^{(p^f)}$ with $\mathrm{V}_{p^f} : E_2^{(p^f)} \to E_2$, we obtain an isogeny $\varphi_0 : E_1 \to E_2$ of degree

$$\deg\varphi_0 = p^f\cdot\deg\psi_0 \leq 49\max\{1, g(K)\}\cdot\frac{\deg_{\mathrm{ins}} j(E_1)}{\deg_{\mathrm{ins}} j(E_2)}.$$

- If $\deg_{\mathrm{ins}} j(E_1) < \deg_{\mathrm{ins}} j(E_2)$, we let $p^e := \deg_{\mathrm{ins}} j(E_1)/\deg_{\mathrm{ins}} j(E_2)$. Composing $\varphi : E_1 \to E_2$ with $\mathrm{V}_{p^e} : E_1^{(p^e)} \to E_2$, we get an isogeny $E_1^{(p^e)} \to E_2$. Since $\deg_{\mathrm{ins}} j(E_2) = \deg_{\mathrm{ins}} j(E_1^{(p^e)})$, Lemma 6.8 entails the existence of a biseparable isogeny $\psi : E_1^{(p^e)} \to E_2$. Applying Proposition 6.7 then yields an isogeny $\psi_0 : E_1^{(p^e)} \to E_2$ with $\deg \psi_0 \leq 49 \max\{1, g(K)\}$.

  The composition of $\psi_0 : E_1^{(p^e)} \to E_2$ with $\mathrm{Fr}_{p^e} : E_1 \to E_1^{(p^e)}$ provides an isogeny $\varphi_0 : E_1 \to E_2$ of degree
  $$\deg \varphi_0 = p^e \cdot \deg \psi_0 \leq 49 \max\{1, g(K)\} \cdot \frac{\deg_{\mathrm{ins}} j(E_2)}{\deg_{\mathrm{ins}} j(E_1)}.$$

In all cases, we have found an isogeny $\varphi_0 : E_1 \to E_2$ with
$$\deg \varphi_0 \leq 49 \max\{1, g(K)\} \cdot \max\left\{\frac{\deg_{\mathrm{ins}} j(E_1)}{\deg_{\mathrm{ins}} j(E_2)}, \frac{\deg_{\mathrm{ins}} j(E_2)}{\deg_{\mathrm{ins}} j(E_1)}\right\},$$
which concludes the proof of Theorem 6.1. □

6.4. Number of K-isomorphism classes in a K-isogeny class.

– Let K be a function field as above, and E be a non-isotrivial elliptic curve over K. For any $M \geq 1$, let us introduce the set
$$\mathscr{I}_K(E, M) := \{E'/K : E' \text{ is } K\text{-isogenous to } E, \text{ and } \deg_{\mathrm{ins}}(j(E')) \leq M\} / K\text{-isomorphism}.$$

(As before, if K has characteristic 0, one may ignore the condition on $\deg_{\mathrm{ins}} j(E')$.)

By construction, the elliptic curves E'/K (whose isomorphism classes are) in $\mathscr{I}_K(E, M)$ have the same conductor as E. In particular, they all have good reduction outside the set S of places of K where E has bad reduction. By a version of Shafarevich's theorem, there are finitely many K-isomorphism classes of elliptic curves over K with good reduction outside S, and with bounded inseparability degree of j-invariant. The set $\mathscr{I}_K(E, M)$ is thus finite. The goal of this section is to prove an effective form of that statement:

Proposition 6.9. *In the above setting, we have*
$$\left|\mathscr{I}_K(E, M)\right| \leq {C_{E,M}}^2,$$
where $C_{E,M} = 49 \max\{1, g(K)\} \cdot \max\left\{\deg_{\mathrm{ins}} j(E), M \cdot (\deg_{\mathrm{ins}} j(E))^{-1}\right\}$.

If K has characteristic 0, the above yields the uniform (*i.e.* independent of the chosen E/K) bound
$$\left|\{E'/K : E' \text{ is } K\text{-isogenous to } E\} / K\text{-isomorphism}\right| \leq C_K^2,$$
on the number of K-isomorphism classes of elliptic curves within the K-isogeny class of E, with $C_K = 49 \max\{1, g(K)\}$. To prove the proposition, we take inspiration from section 2 of [MW89], which proves the analogue of Proposition 6.9 for elliptic curves over number fields. We also need the following:

Lemma 6.10. *Let E_1, E_2 be two non-isotrivial elliptic curves over K. We assume that there exists an isogeny $\varphi : E_1 \to E_2$ which is defined over K. Then all isogenies $E_1 \to E_2$ are defined over K.*

Proof. Let $\mathrm{Hom}(E_1, E_2)$ denote the $\mathbb{Z}$-module of $\overline{K}$-isogenies $E_1 \to E_2$ together with the constant trivial morphism. Since E_1 is non-isotrivial, $\mathrm{Hom}(E_1, E_2)$ is free of rank 1; we choose an isogeny $\psi_0 : E_1 \to E_2$ such that $\mathrm{Hom}(E_1, E_2) = \mathbb{Z} \cdot \psi_0$. We may then write φ as $\varphi = [m] \circ \psi_0 = \psi_0 \circ [m]$ for some integer $m \neq 0$.

Let us first treat the case where φ is *biseparable* (*i.e.* the case where E_1 and E_2 are linked by a biseparable isogeny defined over K). Since φ is biseparable, both $\deg \varphi$ and m are coprime to the characteristic of K (Lemma 4.5). Then the kernel $\ker \varphi$ of φ contains $\ker[m]$. Hence, by Proposition 4.2, φ factors uniquely through $[m] : E_1 \to E_1$ as $\varphi = \psi' \circ [m]$, where $\psi' : E_1 \to E_2$ must be defined over K since both $[m]$ and φ are. By uniqueness, we have $\psi_0 = \psi'$, which is thus defined over K. Since ψ_0 generates $\mathrm{Hom}(E_1, E_2)$, all isogenies $E_1 \to E_2$ are defined over K.

For general φ, we argue in essentially the same way, working with group schemes over K instead. Since $\varphi = \psi_0 \circ [m]$, the schematic kernel $\mathcal{H} := \ker \varphi$ contains the subgroup scheme $\mathcal{E}_{1,m} := \ker[m]$. Here, we view, as we may, both $\mathcal{H}$ and $\mathcal{E}_{1,m}$ as (non-necessarily reduced) group schemes over K. We then use Theorem 1 in [Mum08, §12], which is a group-scheme theoretic version of Proposition 4.2, and deduce that the isogeny φ factors uniquely (up to K-isomorphism) through $[m]$ as $\varphi = \psi' \circ [m]$, where $\psi' : E_1 \to E_2$ is a K-isogeny. As above, the uniqueness of ψ' implies that ψ_0 is defined over K. □

Proof of Proposition 6.9. Let E' be an elliptic curve over K which is K-isogenous to E and whose j-invariant satisfies $\deg_{\mathrm{ins}} j(E') \leq M$. By the isogeny estimate (Theorem 6.1) combined with Lemma 6.10, there exists an isogeny $\varphi_0 : E \to E'$ which is defined over K, with

$$\deg \varphi_0 \leq 49 \max\{1, g(K)\} \cdot \max\left\{ \frac{\deg_{\mathrm{ins}} j(E)}{\deg_{\mathrm{ins}} j(E')}, \frac{\deg_{\mathrm{ins}} j(E')}{\deg_{\mathrm{ins}} j(E)} \right\}.$$

Hence, we have $\deg \varphi_0 \leq C_{E,M}$, where

$$C_{E,M} := 49 \max\{1, g(K)\} \cdot \max\left\{\deg_{\mathrm{ins}} j(E), M \cdot (\deg_{\mathrm{ins}} j(E))^{-1}\right\}.$$

By the proof of Theorem 6.1, we may assume that φ_0 is cyclic. In this situation, E' is then K-isomorphic to the quotient $E/\ker \varphi_0$. This entails that the cardinality of $\mathscr{I}_K(E, M)$ is no greater than the number of cyclic subgroups of E with order at most $C_{E,M}$.

Given the structure of the n-torsion subgroup of E, for any integer $n \geq 1$, the number of cyclic subgroups of E of order n is $\psi(n)$ (see §6.1 for the definition of $\psi(n)$). An elementary computation shows that $\psi(n) \leq \sigma(n)$, where $\sigma(n)$ denotes the sum of divisors of n (both functions are multiplicative, and the inequality holds for prime powers). On the other hand, one easily sees that, for all $C \geq 1$,

$$\sum_{1 \leq n \leq C} \sigma(n) \leq \sum_{1 \leq n \leq C} \sum_{d | n} d \leq \sum_{1 \leq d \leq C} \sum_{\substack{1 \leq n \leq C \\ \text{s.t. } nd \leq C}} d = \sum_{1 \leq d \leq C} d \cdot \left\lfloor \frac{C}{d} \right\rfloor \leq C^2.$$

We therefore obtain the desired upped bound on $|\mathscr{I}_K(E, M)|$:

$$\left|\mathscr{I}_K(E, M)\right| \leq \sum_{1 \leq n \leq C_{E,M}} \psi(n) \leq \sum_{1 \leq n \leq C_{E,M}} \sigma(n) \leq {C_{E,M}}^2.$$

□

6.5. Back to isogeny classes. – We close this paper by going back to the situation studied in §5.5, and recover a finiteness result. Let K be a function field as above, and fix a non-isotrivial elliptic curve E over K. Recall that $\mathscr{E}_{\mathrm{bs}}(E)$ denotes the set of elliptic curves $E'/\overline{K}$ which are biseparably isogenous to E. For any $B \geq 1$ and $D \geq 1$, consider the set

$$\mathscr{E}'_K(E, B, D) = \left\{E' \in \mathscr{E}_{\mathrm{bs}}(E) : \mathrm{h}_{\mathsf{mod}}(E') \leq B \text{ and } [K(j(E')) : K] \leq D\right\} / \overline{K}\text{-isomorphism}.$$

Note that the set $\mathscr{E}_K(E, B)$ studied in §5.5 is the union $\bigcup_{D \geq 1} \mathscr{E}'_K(E, B, D)$ and, further, that

$$\forall B \geq \mathrm{h}_{\mathsf{mod}}(E), \quad \mathscr{E}'_K(E, B, D) = \left\{E' \in \mathscr{E}_{\mathrm{bs}}(E) : [K(j(E')) : K] \leq D\right\} / \overline{K}\text{-isomorphism}.$$

Indeed, all elliptic curves $E' \in \mathscr{E}_{\mathrm{bs}}(E)$ satisfy $\mathrm{h}_{\mathsf{mod}}(E') = \mathrm{h}_{\mathsf{mod}}(E) \leq B$ (see Theorem 5.4).

We prove the following bound:

Proposition 6.11. *In this setting, for any $B \geq \mathrm{h}_{\mathsf{mod}}(E)$, and any $D \geq 1$, the set $\mathscr{E}'_K(E, B, D)$ is finite. Moreover, we have*

$$|\mathscr{E}'_K(E, B, D)| \leq D^2 \cdot \mathrm{h}_{\mathsf{mod}}(E)^2.$$

Proof. Let $E' \in \mathscr{E}_{\mathrm{bs}}(E)$ be an elliptic curve which is biseparably isogenous to E. Let $j(E') \in \overline{K}$ denote its j-invariant and $K' := K(j(E'))$. If necessary, we replace E' by a $\overline{K}$-isomorphic elliptic curve E_2 defined over K'. We write E_1 for the base-change $E_1 := E \times_K K'$.

By assumption, there exists a biseparable isogeny $\varphi : E_1 \to E_2$. We may assume (see the proof of Proposition 6.7) that $\varphi = \varphi_0$ has minimal degree among all biseparable isogenies $E_1 \to E_2$. By the same arguments as in the proof of Proposition 6.7, the kernel $H_0 := \ker \varphi_0$ is then cyclic and stable under the action of $G_{K'}$. Proposition 6.6 then yields the bound

$$|H_0| = \deg \varphi_0 \leq [K' : K] \cdot \mathrm{h}_{\mathsf{mod}}(E_1) \leq D \cdot \mathrm{h}_{\mathsf{mod}}(E) =: C'(E_1, D).$$

It is also clear that E_2 is then $\overline{K}$-isomorphic to the quotient E_1/H_0.

Therefore, the cardinality $|\mathscr{E}'_K(E, B, D)|$ does not exceed the number of cyclic subgroups of E_1 with order at most $C'(E_1, D)$. By the computation carried out in the proof of Proposition 6.9, we have

$$|\mathscr{E}'_K(E, B, D)| \leq C'(E_1, D)^2 = D^2 \cdot \mathrm{h}_{\mathsf{mod}}(E)^2.$$

This proves the finiteness of $\mathscr{E}'_K(E, B, D)$ and the asserted upper bound on its cardinality. □

Acknowledgements RG is supported by the Swiss National Science Foundation, through the SNSF Professorship #170565 awarded to Pierre Le Boudec, and received additional funding from ANR project ANR-17-CE40-0012 (FLAIR). He wishes to thank Universität Basel for providing excellent working conditions. FP thanks the ANR project ANR-17-CE40-0012 (FLAIR) and the IRN GANDA (CNRS).

Both authors would like to thank Gabriel Dill, Marc Hindry, Pierre Le Boudec, Samuel Le Fourn, and Douglas Ulmer for stimulating conversations about the topic of this work. The authors also warmly thank Gaël Rémond for his valuable comments and suggestions on an earlier version of the article.

References

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990. ↑ 10

[BLV09] Andrea Bandini, Ignazio Longhi, and Stefano Vigni. Torsion points on elliptic curves over function fields and a theorem of Igusa. *Expo. Math.*, 27(3):175–209, 2009. ↑ 11

[BPR20] Florian Breuer, Fabien Pazuki, and Mahefason H. Razafinjatovo. Heights and isogenies of Drinfeld modules. *Acta Arithmetica*, 2020. ↑ 1

[DD99] Sinnou David and Laurent Denis. Isogénie minimale entre modules de Drinfel′d. *Math. Ann.*, 315(1):97–140, 1999. ↑ 2

[DGS94] Bernard Dwork, Giovanni Gerotto, and Francis J. Sullivan. *An introduction to G-functions*, volume 133 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1994. ↑ 3

[DI95] Fred Diamond and John Im. Modular forms and modular curves. In *Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994)*, volume 17 of *CMS Conf. Proc.*, pages 39–133. Amer. Math. Soc., Providence, RI, 1995. ↑ 15

[GR14] Éric Gaudron and Gaël Rémond. Théorème des périodes et degrés minimaux d'isogénies. *Comment. Math. Helv.*, 89(2):343–403, 2014. ↑ 2, 15

[Hab13] Philipp Habegger. Special points on fibered powers of elliptic surfaces. *J. Reine Angew. Math.*, 685:143–179, 2013. ↑ 14

[Hus04] Dale Husemöller. *Elliptic curves*, volume 111 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2004. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen. ↑ 5

[KM85] Nicholas M. Katz and Barry Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985. ↑ 15

[Lan83] Serge Lang. *Fundamentals of Diophantine geometry*. Springer-Verlag, New York, 1983. ↑ 2, 3

[MB85] Laurent Moret-Bailly. Pinceaux de variétés abéliennes. *Astérisque*, (129):266, 1985. ↑ 4, 6

[Mum08] David Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition. ↑ 20

[MW89] David W. Masser and Gisbert Wüstholz. Some effective estimates for elliptic curves. In *Arithmetic of complex manifolds (Erlangen, 1988)*, volume 1399 of *Lecture Notes in Math.*, pages 103–109. Springer, Berlin, 1989. ↑ 20

[MW90] David W. Masser and Gisbert Wüstholz. Estimating isogenies on elliptic curves. *Invent. Math.*, 100(1):1–24, 1990. ↑ 2, 15

[MW93] David Masser and Gisbert Wüstholz. Isogeny estimates for abelian varieties, and finiteness theorems. *Ann. of Math. (2)*, 137(3):459–472, 1993. ↑ 2

[Par70] Aleksei N. Paršin. Isogenies and torsion of elliptic curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 34:409–424, 1970. ↑ 10

[Par73] Aleksei N. Paršin. Modular correspondences, heights and isogenies of abelian varieties. *Trudy Mat. Inst. Steklov.*, 132:211–236, 266, 1973. ↑ 10

[Paz19] Fabien Pazuki. Modular invariants and isogenies. *Int. J. Number Theory*, 15(3):569–584, 2019. ↑ 1

[Pel01] Federico Pellarin. Sur une majoration explicite pour un degré d'isogénie liant deux courbes elliptiques. *Acta Arith.*, 100(3):203–243, 2001. ↑ 2, 15

[PS00] Jérôme Pesenti and Lucien Szpiro. Inégalité du discriminant pour les pinceaux elliptiques à réductions quelconques. *Compositio Math.*, 120(1):83–117, 2000. ↑ 7

[Ray85] Michel Raynaud. Hauteurs et isogénies. Number 127, pages 199–234. 1985. Seminar on arithmetic bundles: the Mordell conjecture (Paris, 1983/84). ↑ 10

[Ros02] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002. ↑ 2

[Shi94] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. ↑ 15

[Sil86] Joseph H. Silverman. Heights and elliptic curves. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 253–265. Springer, New York, 1986. ↑ 6, 7

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. ↑ 4, 5, 7, 13

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, 2nd edition, 2009. ↑ 2, 4, 8, 11

[ST68] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968. ↑ 10

[SU99] Lucien Szpiro and Emmanuel Ullmo. Variation de la hauteur de Faltings dans une classe de $\overline{\mathbf{Q}}$-isogénie de courbe elliptique. *Duke Math. J.*, 97(1):81–97, 1999. ↑ 1, 14

[Szp90] Lucien Szpiro. Discriminant et conducteur des courbes elliptiques. *Astérisque*, (183):7–18, 1990. Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988). ↑ 7

[Tat93] John Tate. A review of non-Archimedean elliptic functions. In Int. Press, editor, *Elliptic curves, modular forms, and Fermat's last theorem (Hong Kong, 1993)*, pages 162–184, 1993. ↑ 5

[Ulm11] Douglas Ulmer. Elliptic curves over function fields. In *Arithmetic of L-functions*, volume 18 of *IAS/Park City Math. Ser.*, pages 211–280. Amer. Math. Soc., Providence, RI, 2011. ↑ 4, 6, 18

Richard Griffon (*richard.griffon@unibas.ch*) – Departement Mathematik, Universität Basel, Spiegelgasse 1, 4051 Basel, Switzerland.

Fabien Pazuki (*fpazuki@math.ku.dk*) – Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, 2100 Copenhagen ø, Denmark.