TORSION POINTS ON ELLIPTIC CURVES OVER FUNCTION FIELDS AND A THEOREM OF IGUSA

ANDREA BANDINI, IGNAZIO LONGHI AND STEFANO VIGNI

ABSTRACT. If F is a global function field of characteristic $p > 3$, we employ Tate's theory of analytic uniformization to give an alternative proof of a theorem of Igusa describing the image of the natural Galois representation on torsion points of non-isotrivial elliptic curves defined over F. Along the way, using basic properties of Faltings heights of elliptic curves, we offer a detailed proof of the function field analogue of a classical theorem of Shafarevich according to which there are only finitely many F-isomorphism classes of admissible elliptic curves defined over F with good reduction outside a fixed finite set of places of F. We end the paper with an application to torsion points rational over abelian extensions of F.

1. INTRODUCTION

In any modern treatment of the theory of elliptic curves over arithmetically interesting fields a central role is played by the structure of the subgroup of torsion points viewed as a Galois module. Indeed, if E is an elliptic curve defined over a global field F (by which we mean, as usual, a finite extension of the field $\mathbb{Q}$ of rational numbers or the function field of a smooth, projective algebraic curve over a finite field) then the absolute Galois group $\mathrm{Gal}(F^s/F)$ of F (with F^s being the separable closure of F in a fixed algebraic closure $\bar{F}$) acts on the n-torsion subgroup $E[n]$ of E for all integers $n \geq 1$ not divisible by the characteristic of F. (We remark that $E[n] \subset E(F^s)$ if $\mathrm{char}(F) \nmid n$; this is due to the fact that $E[n]$, viewed as a group scheme, is étale over F, cf. [16, Ch. 7, Theorem 4.38]. An alternative proof of this rationality result is given in Proposition 3.8 below.) This basic property, an immediate consequence of the fact that the group law on E is given by rational functions with coefficients in F (which says that, in a fancier language, E is an algebraic group over F), naturally leads to the study of one of the most important objects that can be attached to an elliptic curve: its ℓ-adic representation.

Explicitly, let ℓ be a rational prime number such that $\ell \neq \mathrm{char}(F)$. The natural action of $\mathrm{Gal}(F^s/F)$ on the subgroups $E[\ell^n]$ gives rise to (continuous) Galois representations

$$\bar{\rho}_{E,\ell^n} : \mathrm{Gal}(F^s/F) \longrightarrow \mathrm{Aut}(E[\ell^n]) \cong GL_2(\mathbb{Z}/\ell^n\mathbb{Z}), \tag{1}$$

the non-canonical isomorphism on the right depending on the choice of a basis of the free module $E[\ell^n]$ over $\mathbb{Z}/\ell^n\mathbb{Z}$. Let now

$$T_\ell(E) := \varprojlim_n E[\ell^n] \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$$

be the *ℓ-adic Tate module* of E, where the projective limit is taken with respect to the multiplication-by-ℓ maps. By considering the action of $\mathrm{Gal}(F^s/F)$ on $T_\ell(E)$ we obtain a continuous Galois representation

$$\rho_{E,\ell} : \mathrm{Gal}(F^s/F) \longrightarrow \mathrm{Aut}(T_\ell(E)) \cong GL_2(\mathbb{Z}_\ell) \tag{2}$$

which is called the *ℓ-adic representation* of $E_{/F}$. Moreover:

$$\rho_{E,\ell} \bmod \ell^n = \bar{\rho}_{E,\ell^n}$$

2000 *Mathematics Subject Classification.* 11G05, 11F80.

Key words and phrases. elliptic curves, function fields, Galois representations.

for all $n \geq 1$. Observe that composing $\rho_{E,\ell}$ with the natural inclusion $\mathbb{Z}_\ell \subset \mathbb{Q}_\ell$ gives a representation of $\mathrm{Gal}(F^s/F)$ over a field of characteristic zero. In the following we will regard the representations defined in (1) and (2) as matrix-valued; in other words, for all ℓ we fix a $\mathbb{Z}_\ell$-basis of $T_\ell(E)$. Put $p := \mathrm{char}(F) > 0$; since

$$\varprojlim_{(n,p)=1} E[n] = \prod_{\ell \neq p} T_\ell(E), \tag{3}$$

we have a single large, continuous Galois representation

$$\rho_E : \mathrm{Gal}(F^s/F) \longrightarrow \prod_{\ell \neq p} GL_2(\mathbb{Z}_\ell) \tag{4}$$

whose ℓth component is the ℓ-adic representation $\rho_{E,\ell}$. Now denote by $E_{(p)\text{-tors}}$ the subgroup of torsion points of E whose order is prime to p. Our choice of bases for the groups $E[n]$ gives an identification

$$\mathrm{Aut}(E_{(p)\text{-tors}}) = \varprojlim_{(n,p)=1} GL_2(\mathbb{Z}/n\mathbb{Z}) = \prod_{\ell \neq p} GL_2(\mathbb{Z}_\ell). \tag{5}$$

If F has characteristic zero then $E_{(p)\text{-tors}}$ is the whole torsion subgroup E_{tors} of E, and the inverse limits and the products in (3), (4) and (5) are taken over all positive integers and over all prime numbers, respectively.

Given an elliptic curve $E_{/F}$ as above, at least two natural, closely related questions arise:

(∗) *Can we describe the image of $\rho_{E,\ell}$ (resp. ρ_E) in $GL_2(\mathbb{Z}_\ell)$ (resp. in the product)?*

And, somewhat less ambitiously:

(∗∗) *How "large" is the image of $\rho_{E,\ell}$ (resp. ρ_E)?*

Seeking an answer to questions (∗) and (∗∗) has been the fuel for much investigation in arithmetic algebraic geometry over the past few decades. In particular, we have come to realize that the zero and positive characteristic settings lead to different phenomena. When F is a number field (i.e., a finite extension of $\mathbb{Q}$), a celebrated theorem of Serre gives a very satisfying answer for a large class of elliptic curves $E_{/F}$. Namely,

Theorem 1.1 (Serre)**.** *Let F be a number field and let $E_{/F}$ be an elliptic curve without complex multiplication*[1]*. The closed subgroup $\rho_E(\mathrm{Gal}(\bar{F}/F))$ is open (i.e., has finite index) in $\mathrm{Aut}(E_{\mathrm{tors}})$. Equivalently:*

i) $\rho_{E,\ell}(\mathrm{Gal}(\bar{F}/F))$ is open (i.e., has finite index) in $GL_2(\mathbb{Z}_\ell)$ for all primes ℓ;

ii) $\rho_{E,\ell}(\mathrm{Gal}(\bar{F}/F)) = GL_2(\mathbb{Z}_\ell)$ for all but finitely many primes ℓ.

A complete proof of this result, often cited in the literature as "the open image theorem", can be found in [21] (see also [22], where part *i)* was first proved).

Remark 1.2. Theorem 1.1 is false for CM elliptic curves. In fact, if $E_{/F}$ has complex multiplication *over* F then it can be shown that the action of $\mathrm{Gal}(\bar{F}/F)$ on $T_\ell(E)$ is abelian, hence $\rho_{E,\ell}$ falls short from being surjective. For details, see the proof of [25, Ch. II, Theorem 2.3].

In the positive characteristic case (i.e., when F is a global function field) things have a similar but slightly more involved description. To explain what happens, we need to introduce some notation. Let $\mathcal{C}_{/\mathbb{F}_r}$ be a geometrically irreducible, smooth, projective algebraic curve over a finite field of characteristic $p > 0$, and denote $F := \mathbb{F}_r(\mathcal{C})$ and $\mathcal{O}_\mathcal{C}$ the function field and the structure sheaf of $\mathcal{C}$, respectively. (In particular, the irreducibility condition implies that $\mathbb{F}_r$ is algebraically closed in F, i.e., $\mathbb{F}_r$ is the field of constants of F; see, e.g., [16, Ch. 3,

[1]Recall that, by definition, this means that $\mathrm{End}(E) = \mathbb{Z}$. We remark that throughout our paper we write $\mathrm{End}(E)$ for $\mathrm{End}_{\bar{F}}(E)$.

Corollary 2.14 (d)].) Fix a closed point ∞ of $\mathcal{C}$ and denote $A := \mathcal{O}_{\mathcal{C}}(\mathcal{C} - \{\infty\})$ the Dedekind domain of the elements of F that are regular outside ∞. The choices of the prime ∞ and of the ring A, which is essentially the analogue of the ring of integers in an algebraic number field and whose role in our arguments will become apparent only later, are immaterial for the statement of Igusa's results. However, for the sake of clarity, we deem it convenient to introduce our setup once and for all at the beginning of the paper.

The basic example to keep in mind is the following:

- $\mathcal{C} = \mathbb{P}^1_{/\mathbb{F}_r}$,
- $\infty = [1:0]$ (the usual point at infinity),
- $A = \mathbb{F}_r[T]$,
- $F = \mathbb{F}_r(T)$.

If they find it preferable, in all that follows the readers can interpret our notation according to the dictionary above without impairing their understanding in any significant way. In the sequel we adopt the notation of [4, §7.2].

Let n be an integer prime to $p = \mathrm{char}(F)$; composing the Galois representation

$$\bar{\rho}_{E,n} : G_F := \mathrm{Gal}(F^s/F) \longrightarrow \mathrm{Aut}(E[n]) \cong GL_2(\mathbb{Z}/n\mathbb{Z})$$

with the determinant

$$\det : \mathrm{Aut}(E[n]) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

induces a homomorphism $G_F \to (\mathbb{Z}/n\mathbb{Z})^\times$. Set $H_n := \langle r \rangle \subset (\mathbb{Z}/n\mathbb{Z})^\times$ for the cyclic subgroup generated by r. The natural identification of $r \in (\mathbb{Z}/n\mathbb{Z})^\times$ with the rth-power Frobenius shows that $H_n \cong \mathrm{Gal}(\mathbb{F}_r(\boldsymbol{\mu}_n)/\mathbb{F}_r)$, where $\boldsymbol{\mu}_n$ denotes the nth roots of unity in F^s. As in [4, §7.2], define the subgroup Γ_n of $GL_2(\mathbb{Z}/n\mathbb{Z})$ via the short exact sequence

$$0 \longrightarrow SL_2(\mathbb{Z}/n\mathbb{Z}) \longrightarrow \Gamma_n \xrightarrow{\det} H_n \longrightarrow 0. \tag{6}$$

In other words, Γ_n is the inverse image of H_n in $GL_2(\mathbb{Z}/n\mathbb{Z})$ via the determinant. Passing to the inverse limit over all integers n not divisible by p we get an exact sequence of profinite groups

$$0 \longrightarrow SL_2(\hat{\mathbb{Z}}_{(p)}) \longrightarrow \hat{\Gamma} \longrightarrow \hat{H} \longrightarrow 0. \tag{7}$$

Here $\hat{\mathbb{Z}}_{(p)} := \prod_{\ell \neq p} \mathbb{Z}_\ell$ is the prime-to-p profinite completion of $\mathbb{Z}$, the group $\hat{\Gamma}$ is closed in $GL_2(\hat{\mathbb{Z}}_{(p)})$ and $\hat{H}$ is the subgroup of $\hat{\mathbb{Z}}^\times_{(p)}$ which is topologically generated by r. If we perform the same procedure restricting instead to the powers of a prime $\ell \neq p$, the sequence (6) yields a sequence

$$0 \longrightarrow SL_2(\mathbb{Z}_\ell) \longrightarrow \hat{\Gamma}_\ell \longrightarrow \hat{H}_\ell \longrightarrow 0.$$

Equivalently:

$$\hat{\Gamma} = \prod_{\ell \neq p} \hat{\Gamma}_\ell \subset \prod_{\ell \neq p} GL_2(\mathbb{Z}_\ell).$$

Finally, assume that $E_{/F}$ is not isotrivial, i.e. that we cannot find a finite extension F' of F such that $E_{/F'}$ is isomorphic to a constant curve (i.e., a curve defined over the field of constants of F'). This is easily seen to be equivalent to the condition $j(E) \notin \bar{\mathbb{F}}_r$.

Theorem 1.3 (Igusa)**.** *The profinite group $\rho_E(G_F)$ is an open subgroup of $\hat{\Gamma}$.*

If $E[\ell^\infty]$ is the ℓ-primary part of the torsion of E (for ℓ a prime number), Theorem 1.3 can be equivalently formulated as

Theorem 1.4. *The profinite group $\mathrm{Gal}(F(E[\ell^\infty])/F)$ is an open subgroup of $\hat{\Gamma}_\ell$ for all prime numbers $\ell \neq p$, and is equal to $\hat{\Gamma}_\ell$ for almost all such ℓ.*

Theorem 1.3, which is the counterpart in the function field setting of Theorem 1.1, was first proved by Igusa in [13], where Galois-theoretic techniques are combined with an explicit (but somewhat involved) case-by-case analysis of degenerations of elliptic curves and ramification of fields of modular functions. The language adopted by Igusa is that of pre-Grothendieck algebraic geometry, and this old-fashioned style could probably make his paper hard to appreciate for the "modern" reader, typically acquainted (at least at an introductory level) with scheme theory but perhaps less familiar with the geometric formalism of Weil's school.

The main goal of our article is to provide an alternative proof of Theorem 1.3. Our strategy is based on the following simple fact: at the cost of passing to a finite separable extension of F, we can choose ∞ to be a prime of split multiplicative reduction for E [2]. This implies that E is a *Tate curve* locally at ∞, that is, if F_∞ is the completion of F at ∞ then the ∞-adic Lie group $E(\bar{F}_\infty)$ is Galois-equivariantly isomorphic over F_∞ to the quotient $\bar{F}_\infty^\times/\langle q\rangle$ for a certain "period" $q \in F_\infty^\times$. Following ideas of Serre in characteristic zero, this analytic property allows us to replace the algebro-geometric arguments of Igusa with local ∞-adic considerations. Although our strategy follows that of Serre closely, it is important to stress a remarkable difference between the characteristic zero and the positive characteristic settings: while our proof is valid for all non-isotrivial elliptic curves over a function field F as above, Tate's theory over number fields yields a proof only of a part of Serre's theorem. In fact, not every elliptic curve without complex multiplication has a non-integral j-invariant, so only a proper subclass of non-CM elliptic curves can be dealt with by means of these "analytic" arguments (actually, a full proof of Theorem 1.1 is achieved in [21] using different and, in many respects, more sophisticated techniques).

In any case, the fact that this approach to questions $(*)$ and $(**)$ is fruitful both in characteristic zero and in positive characteristic should come as no surprise. In fact, broadly speaking, this is just another manifestation of the strong parallel between the arithmetic over number fields and the arithmetic over function fields: from this perspective, our work is no exception to this familiar principle. In this direction, the reader is referred to the survey articles [2] by Böckle and [27] by Ulmer for further number fields/function fields analogies on more advanced and abstract topics.

Our paper is organized as follows. **Section 2** begins with a review of the basic properties of Faltings heights of elliptic curves over global function fields. These heights, originally defined by Faltings on suitable moduli spaces of abelian varieties of arbitrary dimension, play a key role in the proof of the function field analogue (Theorem 2.17) of the well-known theorem of Shafarevich asserting that there are only finitely many K-isomorphism classes of elliptic curves defined over a number field K with good reduction outside a fixed finite set of places of K. Remarkably enough, the need to use the theory of heights of elliptic curves seems to be peculiar of our characteristic p setting, since in this case the classical diophantine arguments given over number fields (see [22, Ch. IV, §1.4]) do not apply (cf. Remark 2.20). Although the validity of Shafarevich's theorem for admissible elliptic curves over global function fields is certainly well known (cf., e.g., [11], [26]), to the best of our knowledge this is the first time that the proof is written in a detailed and essentially self-contained way; in this sense, §2.1 and §2.3 may be of independent interest and apparently fill a gap in the literature. A crucial role in the proof of Shafarevich's theorem is played by a remarkable property of admissible elliptic curves over global function fields: their Faltings height is bounded in terms of the degree of their conductor and the genus of F. A complete proof of this result, which is expected to be valid for elliptic curves over all global fields and is commonly known as the "height

[2] I.e., the reduced curve E mod ∞ has a node as its only singularity, and the slopes of the two tangent lines at the curve in the node belong to the (finite) residue field of F at ∞ (and not just to its quadratic extension).

conjecture", is given in §2.2 (Proposition 2.15). The section closes with irreducibility results for Tate modules (§2.4) that are applied in the proof of Theorem 1.3.

In **Section 3** we conclude the proof of Igusa's theorem. After showing (in §3.1 and §3.2) that we can actually reduce to the case where E has (split) multiplicative reduction at the prime ∞ of F, we review basic facts on Tate curves in §3.3, and then give in §3.4 and §3.5 crucial results on the "horizontal" and "vertical" variation of the Galois groups (this suggestive terminology is borrowed from Lang's book [14]). In particular, in Proposition 3.12 we prove that $\mathrm{Gal}(F(E[\ell])/F) = \Gamma_\ell$ for almost all primes $\ell \neq p$, and this result can be usefully applied to gain control on the Galois cohomology of elliptic curves (cf., e.g., [4], [28]). Finally, with all the "geometric" results at our disposal, in §3.6 we finish the proof of Theorem 1.3. It should be noted that, as in [14, Ch. 17, §5] and [22, Ch. IV, §3.4], the final steps in the proof are of a purely algebraic nature: they are just a formal "juggling" in abstract group theory and have really nothing to do with elliptic curves.

The subsequent part, **Section 4**, is devoted to an interesting arithmetic consequence of Igusa's theorem: we show (Theorem 4.2) that on a non-isotrivial elliptic curve $E_{/F}$ there are only finitely many torsion points rational over abelian extensions of F. Results in the same spirit have been applied in various arithmetic contexts (see, e.g., [1], [3], [4], [28]), but it seems that the statement above was never explicitly proved in this form.

The article is closed by **Appendix A**, which deals with isotrivial elliptic curves over F. These are precisely the elliptic curves over F having a ring of endomorphisms which is larger than $\mathbb{Z}$, and we show that in this situation Theorem 1.4 is always false. In this case the image of Galois is not open in $\hat{\Gamma}$, hence in particular it cannot be "as large as possible" (in analogy to what happens with CM elliptic curves over number fields).

To conclude this introduction, we would like to spend a few words on the background required of the reader. In order to make this note reasonably self-contained, we have tried to keep the prerequisites to a minimum. In fact, apart from basic results in Galois theory and algebraic number theory, we only assume a knowledge of the first definitions and properties in the arithmetic of elliptic curves over local and global fields as treated, for example, in Chapters VII and VIII of Silverman's book [23]. In particular, we have made an effort not to rely on results in the theory of Lie algebras and Lie groups, contrary to what done in [22] over number fields. As a consequence, we think that our exposition is more elementary and down-to-earth than those in [14] and [22]. Moreover, when we introduce more specific notions (e.g., Faltings heights of elliptic curves, Tate's theory of analytic uniformization) we always give complete definitions and suggest references where the interested reader can find details and proofs we have to omit.

Convention. Throughout the paper we assume (unless otherwise stated) that $p > 3$. This condition is crucially exploited in the proof of Theorem 2.17 (Shafarevich's theorem) to get a uniform upper bound on the degree of the conductor of certain elliptic curves. We remark, however, that Igusa's results are valid in any positive characteristic.

Acknowledgements. We would like to thank Matthias Schütt for useful comments on an earlier version of the paper and Bert Van Geemen for helpful conversations on some of the topics of this work. We are also grateful to Matthew Baker for pointing us the article [30] and to Chris Hall for interesting remarks and for showing us alternative proofs of some of the results in this paper. Finally, we thank the anonymous referee for several valuable remarks and suggestions which led to significant improvements in the exposition.

2. Faltings heights and a theorem of Shafarevich

In this section we want to prove two auxiliary results (Theorem 2.17 and Theorem 2.22) that will be crucially employed in the course of our main arguments.

2.1. **Review of Faltings heights of elliptic curves.** Before giving precise definitions in the situation we are interested in, let us briefly describe the idea of "heights" over global fields in its most basic form. Intuitively speaking, in all its various manifestations the notion of height captures the "size" or "complexity" of objects of an arithmetic nature. In the simplest case, take a point P in the projective space $\mathbb{P}^n(\mathbb{Q})$. Since $\mathbb{Z}$ is a PID, we can find homogeneous coordinates for P of the form

$$P = [x_0 : \cdots : x_n]$$

with $x_0, \dots, x_n \in \mathbb{Z}$ and the greatest common divisor of the x_i equal to 1. Then the *height* of P is naturally defined as

$$h(P) := \max\big\{|x_0|, \dots, |x_n|\big\}.$$

Notice that the set

$$\big\{P \in \mathbb{P}^n(\mathbb{Q}) \mid h(P) \leq C\big\}$$

is finite for any constant C (in fact, it has fewer than $(2C+1)^{n+1}$ elements). This sort of finiteness property is one of the most useful features of a well-defined height function (cf. Propositions 2.9 and 2.11 below). A similar definition can be given over any global field, and this can be usefully applied (at least in principle) to obtain finiteness results for much more complex arithmetic objects. For example, one can embed the (compactified) moduli space of (isomorphism classes of) elliptic curves into a suitable projective space, and then compute the height of an elliptic curve over a global field by means of the chosen embedding. As a consequence, for every C there will be only finitely many (isomorphism classes of) elliptic curves whose height is bounded by C. Actually, this idea can be effectively exploited without going through all the geometry which underlies the above considerations. This is achieved by making *a posteriori* all the definitions explicit and then proving that one has a height function on the objects of interest which enjoys the desired formal properties. As will become apparent below, this will be the course taken in our article.

After this brief panoramic detour, let us return to our characteristic p setting. Retain the previous notation; in particular, F is the function field of $\mathcal{C}_{/\mathbb{F}_r}$ and A is the subring of functions in F that are regular outside the closed point ∞. Finally, let Σ_F be the set of places of the global field F, and if $\mathfrak{p} \in \Sigma_F$ denote by $v_\mathfrak{p}$ the discrete valuation associated with $\mathfrak{p}$. Note that the elements of Σ_F correspond to the (closed) points of $\mathcal{C}$.

For any $x \in F^\times$ define the principal divisor of x as

$$(x) := \sum_{\mathfrak{p} \in \Sigma_F} v_\mathfrak{p}(x) \cdot \mathfrak{p}.$$

Recall that the degree of a prime $\mathfrak{p} \in \Sigma_F$ is by definition the degree over $\mathbb{F}_r$ of the residue field of $\mathfrak{p}$, and by linearity the degree of any divisor of F can be introduced; it can be checked that the degree of (x) is 0 (see, e.g., [19, Proposition 5.1]). The zero divisor of x is

$$(x)_0 := \sum_{\mathfrak{p} \in \Sigma_F} \max\{0, v_\mathfrak{p}(x)\} \cdot \mathfrak{p}$$

and its pole divisor is

$$(x)_\infty := (x^{-1})_0,$$

so we can write $(x) = (x)_0 - (x)_\infty$. We define the *F-height* of x to be

$$h_F(x) := \deg\big((x)_0\big) = \deg\big((x)_\infty\big) \in \mathbb{N}.$$

Remark 2.1. It turns out that $h_F(x) \neq 0$ if and only if $x \notin \mathbb{F}_r$ (i.e., if and only if x is not constant), and then

$$h_F(x) = [F : \mathbb{F}_r(x)].$$

For a proof of this fact, see [19, Proposition 5.1]. Observe also that, in the language of algebraic geometry, the integer $h_F(x)$ is the degree of the rational map $\mathcal{C}_{/\mathbb{F}_r} \to \mathbb{P}^1_{/\mathbb{F}_r}$ induced by x.

Let now $E_{/F}$ be an elliptic curve and let $\mathscr{D}_E$ be its minimal discriminant divisor; it is the effective divisor of F defined as

$$\mathscr{D}_E := \sum_{\mathfrak{p} \in \Sigma_F} v_{\mathfrak{p}}(\Delta_{\mathfrak{p}}) \cdot \mathfrak{p} \tag{8}$$

where $\Delta_{\mathfrak{p}}$ is the discriminant of a minimal Weierstrass equation for E at $\mathfrak{p}$ in the sense of [23, Ch. VII, §1] (see also [9, §2] and [23, Ch. VIII, §8]). For the purposes of the present paper, we give

Definition 2.2. The *Faltings height* (over F) of $E_{/F}$ is the rational number

$$h_F(E) := \frac{1}{12} \deg(\mathscr{D}_E) \geq 0.$$

Remark 2.3. Although the notation adopted is the same, the height on $F^\times$ and the Faltings height over F are calculated on objects of a different nature, so no confusion is likely to arise.

The height $h_F(E)$ is an invariant of the class of F-isomorphism of $E_{/F}$. There is another natural notion of height of an elliptic curve $E_{/F}$, essentially equal to the F-height of its j-invariant $j(E)$, that we recall below.

Definition 2.4. The *geometric Faltings height* (over F) of $E_{/F}$ is the rational number

$$h_{F,g}(E) := \frac{1}{12} h_F\big(j(E)\big) \geq 0.$$

The height $h_{F,g}(E)$ is evidently an invariant of the $\bar{F}$-isomorphism class of $E_{/F}$; moreover, by Remark 2.1:

$$h_{F,g}(E) > 0 \quad \Longleftrightarrow \quad E \text{ is not isotrivial.}$$

The following proposition establishes a fundamental relation between h_F and $h_{F,g}$.

Proposition 2.5. *The inequality*

$$h_{F,g}(E) \leq h_F(E)$$

holds for every elliptic curve $E_{/F}$.

Proof. Let $E_{/F}$ be an elliptic curve, and set

$$T := \big\{\mathfrak{p} \in \Sigma_F \mid v_{\mathfrak{p}}(\Delta_{\mathfrak{p}}) > 0\big\}, \qquad T' := \big\{\mathfrak{p} \in \Sigma_F \mid v_{\mathfrak{p}}(j(E)) < 0\big\}$$

where $\Delta_{\mathfrak{p}}$ is the discriminant for E at $\mathfrak{p}$ introduced in (8). Note that T' consists of the places at which E does not have potential good reduction (cf. [23, Ch. VII, Proposition 5.5]). Locally at $\mathfrak{p}$ we can write $j(E) = c_{4,\mathfrak{p}}^3/\Delta_{\mathfrak{p}}$ where $c_{4,\mathfrak{p}}$ is a polynomial expression in the coefficients of a minimal Weierstrass equation for E at $\mathfrak{p}$ (see [23, Ch. III, §1] for a precise formula). In particular, $c_{4,\mathfrak{p}}$ is an integer in the completion $F_{\mathfrak{p}}$ of F at $\mathfrak{p}$. Thus we obtain:

$$v_{\mathfrak{p}}(j(E)) = 3v_{\mathfrak{p}}(c_{4,\mathfrak{p}}) - v_{\mathfrak{p}}(\Delta_{\mathfrak{p}}) \geq -v_{\mathfrak{p}}(\Delta_{\mathfrak{p}}).$$

We immediately deduce that

- $T' \subset T$;
- $-v_{\mathfrak{p}}(j(E)) \leq v_{\mathfrak{p}}(\Delta_{\mathfrak{p}})$.

Now, by equation (8) we can write

$$\mathscr{D}_E = \sum_{\mathfrak{p}\in T} v_{\mathfrak{p}}(\Delta_{\mathfrak{p}}) \cdot \mathfrak{p}.$$

Hence:

$$\begin{aligned} h_F\big(j(E)\big) &= \sum_{\mathfrak{p}\in T'} \big(-v_{\mathfrak{p}}(j(E))\big) \deg(\mathfrak{p}) \\ &\leq \sum_{\mathfrak{p}\in T'} v_{\mathfrak{p}}(\Delta_{\mathfrak{p}}) \deg(\mathfrak{p}) \\ &\leq \sum_{\mathfrak{p}\in T} v_{\mathfrak{p}}(\Delta_{\mathfrak{p}}) \deg(\mathfrak{p}) = \deg(\mathscr{D}_E), \end{aligned}$$

and this proves the proposition by definition of the two Faltings heights. □

Remark 2.6. The heights h_F and $h_{F,g}$, introduced for abelian varieties of arbitrary dimension by Faltings in his landmark paper [8] in which he proved (among others) the Mordell conjecture, admit the simple expressions given in Definitions 2.2 and 2.4 because we are working with elliptic curves (i.e., in dimension one) and our base fields are function fields. In particular, in our setting there are no archimedean valuations, so no logarithmic error terms appear in the expression of $h_F(E)$ (cf. [24, Proposition 1.1] for a formula in the number field case). The reader may wish to consult [12] for details and for results related to Lang's conjecture on lower bounds for the Néron-Tate canonical height of non-torsion points on an elliptic curve E in terms of the Faltings height $h_F(E)$ (see, in particular, [12, Theorem 6.1]).

For a general discussion of the theory of heights of abelian varieties over global fields (albeit with a slant towards the number field setting) we refer the reader to the papers [6] by Deligne and [26] by Szpiro. In any case, the notion of height of an elliptic curve will play in the sequel only an auxiliary (and limited) role, so in order to keep things as plain as possible we decided to adopt the somewhat *ad hoc* definitions given above.

Remark 2.7. By normalizing by the so-called "degree" of F (which is defined as the smallest value of $h_F(x)$ with x varying in the non-constant elements of F, cf. [10, §1]), it would be possible to modify Definitions 2.2 and 2.4 and introduce "absolute" versions of the heights of E which do not depend on the field taken as field of definition of E. However, since the properties of the functions h_F and $h_{F,g}$ will suffice for our goals, in this note we are content with the "relative" (and more common) notions explained above.

Lemma 2.8. *If $\mathfrak{d}$ is a divisor of F then the number of the $x \in F^\times$ such that $(x) = \mathfrak{d}$ is either* 0 *or the cardinality of $\mathbb{F}_r^\times$.*

Proof. If the set of such x is not empty, let $x, y \in F^\times$ be such that $(x) = (y)$. Then $(xy^{-1}) = 0$, and we conclude that $xy^{-1} \in \mathbb{F}_r^\times$ by [19, Proposition 5.1]. □

Proposition 2.9. *The set $\{x \in F^\times \mid h_F(x) \leq C\}$ is finite for all $C \geq 0$.*

Proof. Since the function h_F is $\mathbb{N}$-valued on $F^\times$, the claim of the proposition is equivalent to the assertion that the set

$$\mathscr{B}_n := \{x \in F^\times \mid h_F(x) = n\}$$

is finite for all integers $n \geq 0$. To begin with, note that if $h_F(x) = n$ then both $(x)_0$ and $(x)_\infty$ are effective divisors of degree n. Since F has a finite field of constants, by [19, Lemma 5.5] the set $\mathtt{Div}_n^+$ of effective divisors of degree n is finite. We immediately conclude from Lemma 2.8 that every fibre of the natural map

$$\begin{array}{ccc} \mathscr{B}_n & \longrightarrow & \mathtt{Div}_n^+ \times \mathtt{Div}_n^+ \\ x & \longmapsto & \big((x)_0, (x)_\infty\big) \end{array}$$

is finite, and the proposition is proved. □

As a straightforward consequence of the above proposition, we get

Corollary 2.10. *For all $C \geq 0$ there are only finitely many $\bar{F}$-isomorphism classes of elliptic curves $E_{/F}$ with $h_{F,g}(E) \leq C$.*

Proof. Immediate from Proposition 2.9 by definition of $h_{F,g}(E)$. □

We end this § with a finiteness property of the Faltings height h_F that will be needed in §2.3 for the proof of Shafarevich's theorem. Before stating this result, we introduce one more piece of notation: if $S \subset \Sigma_F$ is a finite set we let A_S be the ring of S-integers of F. In other words:

$$A_S := \big\{x \in F \mid v_{\mathfrak{p}}(x) \geq 0 \text{ for all } \mathfrak{p} \notin S\big\}.$$

Proposition 2.11. *For all $C \geq 0$ there are only finitely many F-isomorphism classes of non-isotrivial elliptic curves $E_{/F}$ satisfying $h_F(E) \leq C$.*

See [24, Corollary 2.5] for the corresponding statement over number fields.

Proof. Since $h_{F,g}(E) \leq h_F(E)$ by Proposition 2.5, Corollary 2.10 implies that there are only finitely many $\bar{F}$-isomorphism classes of (non-isotrivial) elliptic curves $E_{/F}$ with $h_F(E) \leq C$. Thus we are reduced to the following problem: given a non-isotrivial elliptic curve $E_{/F}$, up to F-isomorphism there are only finitely many elliptic curves $E'_{/F}$ satisfying

$$j(E') = j(E), \qquad h_F(E') \leq C.$$

So fix E as above, and note that (by the very definition of the Faltings height!) bounding $h_F(E')$ is equivalent to bounding $\deg(\mathscr{D}_{E'})$.

Now choose a finite set of places $T \subset \Sigma_F$ such that

- T contains all places of bad reduction for E;
- the ring A_T of T-integers is a PID.

Recall that $p = \mathrm{char}(F) > 3$; then by [23, Ch. VIII, Proposition 8.7] we can find an affine Weierstrass equation

$$E : y^2 = x^3 + ax + b$$

for $E_{/F}$ with $a, b \in A_T$ and discriminant $\Delta(E) := -16(4a^3 + 27b^2) \in A_T^{\times}$ (this result is proved in *loc. cit.* for elliptic curves over number fields, but the arguments work over global function fields too). The elliptic curves over F which are isomorphic over $\bar{F}$ to E are the twists of E given by the equations

$$E_d : y^2 = x^3 + ad^2x + bd^3, \qquad d \in F^{\times}.$$

Furthermore, $E_d \cong E_{d'}$ *over* F if and only if $(d/d') \in (F^{\times})^2$. For a proof of these facts, see [23, Ch. X, Proposition 5.4 and Corollary 5.4.1]. Our goal is to bound the set of such d (mod $(F^{\times})^2$). First of all, without loss of generality we can assume that $d \in A_T$. Moreover, a direct computation shows that

$$\Delta(E_d) = d^6\Delta(E). \tag{9}$$

Since E_d is isomorphic to E over a finite extension of F and E has good reduction outside T, it follows from [23, Ch. VII, Proposition 5.4 (b)] that E_d has either good or additive reduction at primes outside T. From (9), if E_d has additive reduction at $\mathfrak{p} \notin T$ then $v_{\mathfrak{p}}(d) > 0$. More precisely, if $\mathfrak{p} \notin T$ then E_d has additive reduction at $\mathfrak{p}$ if and only if $v_{\mathfrak{p}}(d) \equiv 1 \pmod 2$.[3]

[3]In fact, if $v_{\mathfrak{p}}(d) \equiv 0 \pmod 2$ then E_d is isomorphic over F to the curve $E_{d'}$ with $d' := d\pi_{\mathfrak{p}}^{-v_{\mathfrak{p}}(d)}$, where $\pi_{\mathfrak{p}} \in A_T$ is such that $v_{\mathfrak{p}}(\pi_{\mathfrak{p}}) = 1$ and $v_{\mathfrak{p}'}(\pi_{\mathfrak{p}}) = 0$ for all primes $\mathfrak{p}' \notin T$, $\mathfrak{p}' \neq \mathfrak{p}$. This shows that E_d has good reduction at $\mathfrak{p}$.

Hence:

$$\deg(\mathscr{D}_{E_d}) \geq \sum_{\substack{\mathfrak{p}\notin T \\ v_{\mathfrak{p}}(d)\equiv 1\,(2)}} \deg(\mathfrak{p}),$$

so a bound on $\deg(\mathscr{D}_{E_d})$ also bounds the degree of those $\mathfrak{p} \notin T$ with $v_{\mathfrak{p}}(d) \equiv 1 \pmod 2$. Put $C' := 12C$ and define

$$S := T \cup \big\{\mathfrak{p} \in \Sigma_F \mid \deg(\mathfrak{p}) \leq C'\big\}.$$

Since there are only finitely many primes of F of a given degree, the set S is finite. Now observe that the proposition is proved if we show that the set

$$\big\{d \in F^\times \mid E_d \text{ has good reduction outside } S\big\}/(F^\times)^2 \tag{10}$$

is finite. By the S-unit theorem for function fields (see [19, Proposition 14.2]) we know that the abelian group $A_S^\times/\mathbb{F}_r^\times$ is free of finite rank (equal to $|S| - 1$), hence $A_S^\times/(A_S^\times)^2$ is finite. But A_S is a unique factorization domain and E_d has good reduction outside S if and only if $v_{\mathfrak{p}}(d) \equiv 0 \pmod 2$ for all $\mathfrak{p} \notin S$, so we can assume that $d \in A_S^\times$. Thus the set (10) injects into $A_S^\times/(A_S^\times)^2$, and we are done. □

2.2. **Admissible elliptic curves and the height conjecture.** First of all, we introduce a large class of elliptic curves over global function fields of characteristic $p > 3$, the so-called "admissible" curves: these will be precisely the elliptic curves for which Shafarevich's theorem (Theorem 2.17) holds. Following [10, Definition 1.2], we give

Definition 2.12. An elliptic curve $E_{/F}$ is called *admissible* if the extension $F/\mathbb{F}_r(j(E))$ is finite and separable.

Thus an admissible elliptic curve is non-isotrivial. Definition 2.12 is equivalent to requiring that $j(E)$ is not a pth power in F.

The next proposition shows that admissibility is preserved under prime-to-p isogenies. This property will be used in the proof of Theorem 2.22.

Proposition 2.13. *Let $E_{/F}$, $E'_{/F}$ be elliptic curves and let $f : E \to E'$ be an isogeny whose degree is not divisible by p. If E is admissible then E' is admissible.*

Proof. For simplicity, write $j := j(E)$ and $j' := j(E')$. We know that j and j' are linked by an isogeny of degree d not divisible by p. Choose an elliptic curve $E_{j'}$ defined over $\mathbb{F}_r(j')$ whose j-invariant is equal to j'. Then $\mathbb{F}_r(j', E_{j'}[d])$ is separable over $\mathbb{F}_r(j')$ (cf. the references given in the introduction, or adapt the proof of Proposition 3.8 below), and so is $\mathbb{F}_r(j', \Lambda)$ for any subgroup Λ of $E_{j'}[d]$. Now j lies in $\mathbb{F}_r(j', \Lambda)$ for some Λ as above (take Λ equal to the kernel of the corresponding dual isogeny), hence the extension $\mathbb{F}_r(j, j')/\mathbb{F}_r(j')$ is finite and separable. But the extension $F/\mathbb{F}_r(j)$ is finite and separable because E is admissible, hence $F/\mathbb{F}_r(j, j')$ is finite and separable as well. Thus we conclude that $F/\mathbb{F}_r(j')$ is finite and separable, and the proposition is proved. □

Remark 2.14. From a highbrow point of view, the separability of the extension $\mathbb{F}_r(j, j')/\mathbb{F}_r(j')$ could also be proved as follows. By decomposing the isogeny f into cyclic (i.e., with cyclic kernel) isogenies we are reduced to the case where f is cyclic of degree d. Let $\Phi_d(X, Y) \in \mathbb{Z}[X, Y]$ be the modular polynomial of order d, whose definition and main properties can be found, e.g., in [14, Ch. 5, §2]. Then the separability of the above extension can be obtained by exploiting the fact that $\Phi_d(j, j') = 0$ and by applying the moduli interpretation explained by Deligne and Rapoport in [7, Ch. VI, §6]. This separability result is also pointed out by Igusa in the concluding remarks of [13].

Now we come to the main result of this §, the so-called "height conjecture" for admissible elliptic curves. This conjecture predicts that the Faltings height of an elliptic curve $E_{/F}$ is bounded in terms of the degree of the *conductor* of E and the genus of F (i.e., the genus of the curve $\mathcal{C}$). The canonical name for this statement is "height *conjecture*" because the corresponding assertion in the number field case (and, more generally, for abelian varieties) is still unproved.

Recall that the conductor of an elliptic curve E is the conductor of the Galois representation $T_\ell(E)\otimes\mathbb{Q}_\ell$ (for $\ell\neq p$) as defined in [25, Ch. IV, §10]. We also refer the reader to [20, §2.1] for a more conceptual approach to conductors of general ℓ-adic representations.

Proposition 2.15 (Height conjecture)**.** *Let $E_{/F}$ be an admissible elliptic curve. Then*

$$h_F(E)\leq \frac{1}{2}\deg(\mathfrak{n}_E)+g-1 \tag{11}$$

where $\mathfrak{n}_E$ is the conductor of E over F and g is the genus of F.

Proof. We follow the proof of [12, Theorem 5.1] closely. For any prime $\mathfrak{p}$ of F we denote $j(E)_\mathfrak{p}$ the reduction of $j(E)$ modulo $\mathfrak{p}$ (with $j(E)_\mathfrak{p}=\infty$ if $v_\mathfrak{p}(j(E))<0$) and $e(\mathfrak{p})$ the ramification index of $\mathfrak{p}$ over $\mathbb{F}_r(j(E))$.

To begin with, by [19, Proposition 5.1] there are equalities

$$\begin{aligned}\big[F:\mathbb{F}_r(j(E))\big] &= \sum_{j(E)_\mathfrak{p}=0} v_\mathfrak{p}(j(E))\deg(\mathfrak{p}) = \sum_{j(E)_\mathfrak{p}=\infty} -v_\mathfrak{p}(j(E))\deg(\mathfrak{p})\\ &= \sum_{j(E)_\mathfrak{p}=1728} v_\mathfrak{p}\big(j(E)-1728\big)\deg(\mathfrak{p})\end{aligned} \tag{12}$$

(for the last term note that $\mathbb{F}_r(j(E))=\mathbb{F}_r(j(E)-1728)$). Furthermore, since $j(E)$ and $j(E)-1728$ are primes of $\mathbb{F}_r(j(E))$, the following relations hold:

$$\begin{aligned} j(E)_\mathfrak{p}=0 &\quad\Longrightarrow\quad e(\mathfrak{p})=v_\mathfrak{p}(j(E)),\\ j(E)_\mathfrak{p}=\infty &\quad\Longrightarrow\quad e(\mathfrak{p})=-v_\mathfrak{p}(j(E)),\\ j(E)_\mathfrak{p}=1728 &\quad\Longrightarrow\quad e(\mathfrak{p})=v_\mathfrak{p}\big(j(E)-1728\big).\end{aligned} \tag{13}$$

Now E is admissible by assumption, so we can apply the Riemann-Hurwitz formula ([19, Theorem 7.16]) to the finite separable extension $F/\mathbb{F}_r(j(E))$, and since the genus of $\mathbb{F}_r(j(E))$ is 0 we get the inequality

$$2g-2\geq -2\big[F:\mathbb{F}_r(j(E))\big]+\sum_{\mathfrak{p}\in\Sigma_F}\big(e(\mathfrak{p})-1\big)\deg(\mathfrak{p}). \tag{14}$$

Our strategy is to estimate the integers $e(\mathfrak{p})$ and then apply (14) to get the desired inequality (11). More precisely, the $e(\mathfrak{p})$ for the primes $\mathfrak{p}$ with $j(E)_\mathfrak{p}\in\{0,\infty,1728\}$ are computed by means of (13), while for the other primes we simply use the inequality $e(\mathfrak{p})\geq 1$. Keeping (12) and (13) in mind, we can write

$$\begin{aligned}2\big[F:\mathbb{F}_r(j(E))\big] &= \frac{5}{6}\sum_{j(E)_\mathfrak{p}=\infty} e(\mathfrak{p})\deg(\mathfrak{p}) + \frac{2}{3}\sum_{j(E)_\mathfrak{p}=0} e(\mathfrak{p})\deg(\mathfrak{p})\\ &\quad + \frac{1}{2}\sum_{j(E)_\mathfrak{p}=1728} e(\mathfrak{p})\deg(\mathfrak{p}).\end{aligned} \tag{15}$$

Let Σ'_F be the set of primes of F such that $j(E)_\mathfrak{p}\notin\{0,\infty,1728\}$ and recall the definition (8) of the minimal discriminant divisor $\mathscr{D}_E$. Then, after some easy manipulations, formulas (14)

and (15) yield

$$\begin{aligned}\frac{1}{6}\deg(\mathscr{D}_E) - 2g + 2 \leq & \sum_{j(E)_\mathfrak{p}=\infty} \left(\frac{1}{6}v_\mathfrak{p}(\Delta_\mathfrak{p}) - \frac{1}{6}e(\mathfrak{p}) + 1\right)\deg(\mathfrak{p}) \\ & + \sum_{j(E)_\mathfrak{p}=0} \left(\frac{1}{6}v_\mathfrak{p}(\Delta_\mathfrak{p}) - \frac{1}{3}e(\mathfrak{p}) + 1\right)\deg(\mathfrak{p}) \\ & + \sum_{j(E)_\mathfrak{p}=1728} \left(\frac{1}{6}v_\mathfrak{p}(\Delta_\mathfrak{p}) - \frac{1}{2}e(\mathfrak{p}) + 1\right)\deg(\mathfrak{p}) \\ & + \sum_{\mathfrak{p}\in\Sigma'_F} \left(\frac{1}{6}v_\mathfrak{p}(\Delta_\mathfrak{p}) - e(\mathfrak{p}) + 1\right)\deg(\mathfrak{p}).\end{aligned} \tag{16}$$

At this point, we examine all coefficients according to the different reduction types of E. These coefficients can be calculated using [25, Table 4.1], and the results are identical to the ones in [12, Table 1]: here we give the details in two of the possible cases just to illustrate the methods. As customary, to denote the reduction type of E at a prime $\mathfrak{p}$ of F we use Kodaira symbols, as in the two references given above.

1) $j(E)_\mathfrak{p} = \infty$ (i.e., $v_\mathfrak{p}(j(E)) < 0$), reduction type I_n^*.

Here $v_\mathfrak{p}(\Delta_\mathfrak{p}) = n + 6$, $e(\mathfrak{p}) = -v_\mathfrak{p}(j(E)) = n$ and $v_\mathfrak{p}(\mathfrak{n}_E) = 2$. One then has

$$\frac{1}{6}v_\mathfrak{p}(\Delta_\mathfrak{p}) - \frac{1}{6}e(\mathfrak{p}) + 1 = 2 = v_\mathfrak{p}(\mathfrak{n}_E).$$

2) $j(E)_\mathfrak{p} = 1728$ (i.e., $v_\mathfrak{p}(j(E) - 1728) > 0$), reduction type III.

For an equation $y^2 = x^3 + ax + b$ of E minimal at $\mathfrak{p}$ one has

$$j(E) - 1728 = -1728\left(\frac{(4^3a^3)}{\Delta} + 1\right) = \frac{-1728}{\Delta}(-16\cdot 27b^2),$$

so $e(\mathfrak{p}) = v_\mathfrak{p}(j(E) - 1728) = 2v_\mathfrak{p}(b) - v_\mathfrak{p}(\Delta_\mathfrak{p})$. Under our assumption on the reduction, $v_\mathfrak{p}(\Delta_\mathfrak{p}) = 3$, $e(\mathfrak{p}) = v_\mathfrak{p}(j(E) - 1728) = 2v_\mathfrak{p}(b) - 3 \geq 1$ and $v_\mathfrak{p}(\mathfrak{n}_E) = 2$. One then has

$$\frac{1}{6}v_\mathfrak{p}(\Delta_\mathfrak{p}) - \frac{1}{2}e(\mathfrak{p}) + 1 \leq 1 < v_\mathfrak{p}(\mathfrak{n}_E).$$

All other cases can be dealt with in an analogous manner. The crucial point is that the coefficients of $\deg(\mathfrak{p})$ in the right hand side of (16) are always bounded from above by $v_\mathfrak{p}(\mathfrak{n}_E)$. Hence inequality (16) gives

$$\frac{1}{6}\deg(\mathscr{D}_E) - 2g + 2 \leq \sum_{\mathfrak{p}\in\Sigma_F} v_\mathfrak{p}(\mathfrak{n}_E)\deg(\mathfrak{p}),$$

and finally

$$h_F(E) \leq \frac{1}{2}\deg(\mathfrak{n}_E) + g - 1$$

by definition of the Faltings height of E. □

This proposition is clearly interesting in its own right, and we refer the reader to [9, §2] and [10, §1 (b)] for comments, consequences and a slightly different proof. For the purposes of this paper its importance lies in the central role it will play in the proof of Shafarevich's

theorem: in fact, inequality (11) is the ingredient that allows us to deduce Theorem 2.17 from the finiteness property of the Faltings height h_F that was established in Proposition 2.11.

2.3. **Shafarevich's theorem.** A well-known theorem due to Shafarevich ([23, Ch. IX, Theorem 6.1]) asserts that if K is a number field there are only a finite number of K-isomorphism classes of elliptic curves defined over K having good reduction at all primes of K outside a fixed finite subset. We now show that an analogous result holds for elliptic curves over a global function field F of characteristic $p > 3$ which are admissible in the sense of Definition 2.12. This seems to be well known to experts and is essentially a consequence of the basic properties of Faltings heights recalled in §2.1; however, we were not able to track down a reasonably self-contained reference in the literature, so for the convenience of the reader we give a detailed proof of this result.

Before turning to Shafarevich's theorem, let us state the following result, which will be used to prove Corollary 2.18 below.

Proposition 2.16. *Let $E_{/F}$, $E'_{/F}$ be elliptic curves and let $f : E \to E'$ be an isogeny defined over F. Then E and E' have the same conductor over F.*

Proof. It is easy to see that the Tate modules $T_\ell(E)$ and $T_\ell(E')$ are isomorphic as G_F-modules for $\ell \neq p$, and the claim follows. □

Now we prove

Theorem 2.17 (Shafarevich)**.** *Let S be a finite set of primes of F. There are only finitely many F-isomorphism classes of admissible elliptic curves $E_{/F}$ having good reduction at all primes of F outside S.*

Proof. Let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. If an elliptic curve $E_{/F}$ has good reduction outside S then the support of its conductor $\mathfrak{n}_E$ is contained in S. Since we are assuming that $p > 3$, it follows that[4]

$$\deg(\mathfrak{n}_E) \leq C(S) := 2\sum_{j=1}^{n} \deg(\mathfrak{p}_j). \tag{17}$$

Note that the constant $C(S)$ is independent of E. Now, by Proposition 2.15 we know that if $E_{/F}$ is admissible then

$$h_F(E) \leq \frac{1}{2}\deg(\mathfrak{n}_E) + g - 1. \tag{18}$$

Combining (18) and (17) yields the inequality

$$h_F(E) \leq \frac{1}{2}C(S) + g - 1,$$

and the claim of the theorem follows from Proposition 2.11. □

It seems worthwhile to point out a straightforward consequence of Shafarevich's theorem.

Corollary 2.18. *Every F-isogeny class of elliptic curves defined over F contains only finitely many F-isomorphism classes of admissible elliptic curves.*

Proof. By Proposition 2.16, two elliptic curves defined over F which are F-isogenous have the same conductor over F, and so they have the same set of primes of bad reduction. □

[4]The uniform bound (17) does not hold in characteristic $p = 2, 3$ due to the possible high divisibility of $\mathfrak{n}_E$ by places of additive reduction for E.

The reader is referred to [23, Ch. IX, Corollary 6.2 and Remark 6.5] for the counterpart of this result over number fields and for interesting arithmetic consequences of a (still-to-be-found) proof of Shafarevich's theorem over number fields which did not use Siegel's theorem or diophantine approximation techniques.

Remark 2.19. If the word "admissible" in Theorem 2.17 is replaced by "non-isotrivial", the resulting statement is false. For example, let $E_{/F}$ be a non-isotrivial elliptic curve and let S be the set of places of bad reduction for E. Moreover, for all $i \geq 0$ let E_i be the elliptic curve obtained by applying to E the ith iteration of the rth-power (relative) Frobenius. Then the family $\{E_i\}_{i\geq 0}$ together with the finite set S gives a counterexample to this stronger assertion (cf. Proposition 2.16).

Remark 2.20. The reader might wonder why we did not mimic, in the proof of Theorem 2.17, the arguments originally given by Tate for elliptic curves over number fields and reproduced, for example, in [22, Ch. IV, §1.4] and [23, Ch. IX, Theorem 6.1]. The reason is simply that they do not work in our function field setting. In fact, the proof by Tate is based on applying Siegel's finiteness theorem for S-integral points to a certain auxiliary elliptic curve with $j = 0$. Unfortunately, the analogue over global function fields of Siegel's result is valid in full strength only for non-isotrivial elliptic curves (cf. [29, Lemma 5.1 and Theorem 5.3]).

2.4. **Irreducibility results.** As in [14, Ch. 17], the first step towards Igusa's theorem is an irreducibility property for the Tate modules of a non-isotrivial elliptic curve E, which we show in Theorem 2.22 below. As we shall see, its proof rests upon Shafarevich's theorem.

Lemma 2.21. *Let $E_{/K}$ be an elliptic curve over a field K of positive characteristic p. Then* $\mathrm{End}(E) = \mathbb{Z}$ *if and only if* $j(E) \notin \bar{\mathbb{F}}_p \cap K$.

Here $\mathbb{F}_p$ is the finite field with p elements.

Proof. This is part of a classical result of Deuring, a complete statement and a proof of which can be found in [17, p. 217]. □

As before, let F be our global function field of characteristic $p > 3$. In the following let $E_{/F}$ be a non-isotrivial elliptic curve. Write $V_\ell(E) := T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ for all prime numbers $\ell \neq p$.

Theorem 2.22. *Retain the above notation. Then:*

i) the G_F-module $E[\ell]$ is irreducible for almost all primes $\ell \neq p$;
ii) the G_F-module $V_\ell(E)$ is irreducible for all primes $\ell \neq p$.

Proof. Since E is non-isotrivial, there exists an integer $m \geq 0$ such that

$$j(E) \in F^{p^m}, \qquad j(E) \notin F^{p^{m+1}}.$$

In particular, E is isomorphic over a finite, separable extension L of F to (the base change to F of) an elliptic curve E' which is defined and admissible over $F_m := F^{p^m}$. Now notice that it clearly suffices to show that *i)* and *ii)* hold when G_F is replaced by the smaller absolute Galois group G_L of L. On the other hand, the group of automorphisms of a purely inseparable extension is trivial, hence there are natural identifications

$$\mathrm{Gal}(F^s/F) = \mathrm{Aut}(\bar{F}/F) = \mathrm{Aut}(\bar{F}/F_m) = \mathrm{Gal}(F_m^s/F_m).$$

Thus, up to replacing F by F_m and E by E', in order to prove the theorem it is not restrictive to assume that $E_{/F}$ is admissible, which we do.

i) Suppose that $E[\ell]$ is reducible for infinitely many primes $\ell \neq p$, and for any such prime let $H_\ell \subset E[\ell]$ be a nonzero G_F-invariant proper subspace. It follows that the elliptic curve $E_\ell := E/H_\ell$ can be defined over F; moreover, the natural (cyclic) isogeny $\pi_\ell : E \twoheadrightarrow E_\ell$ is defined over F and has degree ℓ. Now we claim that E_ℓ and $E_{\ell'}$ are not isomorphic (over $\bar{F}$)

if ℓ and ℓ' are distinct primes (which is equivalent to saying that $j(E_\ell) \neq j(E_{\ell'})$ if $\ell \neq \ell'$). In fact, suppose that

$$\delta : E_\ell \xrightarrow{\cong} E_{\ell'}$$

is an isomorphism, and consider the map $\psi := \hat{\pi}_{\ell'} \circ \delta \circ \pi_\ell$ where $\hat{\pi}_{\ell'}$ is the dual isogeny to $\pi_{\ell'}$. Since $\mathrm{End}(E) = \mathbb{Z}$ by Lemma 2.21, there exists an integer n such that

$$\psi = [n] \tag{19}$$

as endomorphisms of E. Hence, passing to the degrees on both sides of (19), we get the equality $\ell\ell' = n^2$, which is impossible because $\ell \neq \ell'$. It follows that the set

$$\mathscr{E} := \{E_\ell \mid \ell \neq p \text{ a prime such that } E[\ell] \text{ is } G_F\text{-reducible}\}$$

consists of infinitely many elliptic curves which are defined over F, are isogenous to E and are pairwise not F-isomorphic. Furthermore, since E is admissible and for every $\ell \neq p$ as above the isogeny π_ℓ has degree ℓ, Proposition 2.13 ensures that all of them are admissible. But every curve in $\mathscr{E}$, being isogenous *over* F to E, has good reduction outside the support of the conductor of E (which consists of finitely many primes of F), and this contradicts Theorem 2.17.

ii) If $X \subset V_\ell(E)$ is a G_F-invariant, one-dimensional $\mathbb{Q}_\ell$-vector subspace then $X \cap T_\ell(E)$ is a G_F-invariant submodule of $T_\ell(E)$ which is free of rank one over $\mathbb{Z}_\ell$, so the irreducibility result for $V_\ell(E)$ is proved once we show that $T_\ell(E)$ is simple as a G_F-module. Thus suppose that this is not the case, and let $W \subset T_\ell(E)$ be a nonzero proper $\mathbb{Z}_\ell$-submodule which is G_F-invariant. Then W is free of rank one over $\mathbb{Z}_\ell$, and by the linearity of the G_F-action we can assume that it is a direct summand of $T_\ell(E)$. For every $n \geq 1$ let $\lambda_n : T_\ell(E) \twoheadrightarrow E[\ell^n]$ be the canonical projection, and set $W_n := \lambda_n(W)$. It follows that W_n is cyclic of order ℓ^n and G_F-invariant, and the elliptic curve $E_n := E/W_n$ is defined over F and isogenous to E over F. Moreover, the natural (cyclic) isogeny $E \twoheadrightarrow E_n$ has degree ℓ^n. We contend that E_n and E_m are non-isomorphic if $n < m$, which can be seen as follows. There is an obvious isogeny $\pi_{n,m} : E_n \twoheadrightarrow E_m$ which is defined over F, is separable and has a cyclic kernel (of order ℓ^{m-n}). Suppose now that

$$\delta : E_m \xrightarrow{\cong} E_n$$

is an isomorphism, and consider the separable map $\psi := \delta \circ \pi_{n,m}$. Since E is admissible, the curve E_n is admissibile (so, in particular, non-isotrivial) as well by Proposition 2.13. Now we know by Lemma 2.21 that $\mathrm{End}(E_n) = \mathbb{Z}$, hence

$$\psi = [t]$$

for a certain integer t not divisible by p. But ψ has a cyclic kernel (equal to the kernel of $\pi_{n,m}$), while the kernel of $[t]$, being isomorphic to $(\mathbb{Z}/t\mathbb{Z})^2$, is not cyclic. This proves our claim, and we conclude as before that the set

$$\mathscr{E} := \{E_n \mid n \geq 1\}$$

consists of infinitely many admissible elliptic curves defined over F and belonging to different F-isomorphism classes. Since all the curves in $\mathscr{E}$ have good reduction outside the support of the conductor of E, this contradicts once again Theorem 2.17. □

3. Proof of Theorem 1.3

Now that we have collected some of the algebraic results that will be used (most notably Theorem 2.22), we can prove Igusa's theorem. This will be done in §3.6, and before that we need to gather a handful of geometric features that will pave our way towards Theorem 1.3.

3.1. **Consequences of the Weil pairing.** In this § the curve $E_{/F}$ is an arbitrary elliptic curve, possibly isotrivial. Let $n \geq 2$ be an integer not divisible by p; recall from [23, Ch. III, §8] that there is a bilinear, alternating, non-degenerate pairing (called the *Weil pairing*)

$$e_n : E[n] \times E[n] \longrightarrow \boldsymbol{\mu}_n$$

such that

$$e_n(P^\sigma, Q^\sigma) = e_n(P, Q)^\sigma \tag{20}$$

for all $P, Q \in E[n]$ and $\sigma \in \mathrm{Gal}(\bar{F}/F)$. As a consequence of the properties of e_n, it turns out ([23, Ch. III, Corollary 8.1.1]) that $\boldsymbol{\mu}_n \subset F(E[n])$.

In the rest of the paper we will regard elements of $\mathrm{Gal}(F(E[n])/F)$ *as* 2×2 *invertible matrices via the map* $\bar{\rho}_{E,n}$.

Lemma 3.1. *The equality*

$$e_n(Q_1, Q_2)^\sigma = e_n(Q_1, Q_2)^{\det(\sigma)}$$

holds for all $Q_1, Q_2 \in E[n]$ *and all* $\sigma \in \mathrm{Gal}(F(E[n])/F)$.

Proof. Let P_1, P_2 be a $\mathbb{Z}/n\mathbb{Z}$-basis for $E[n]$ and let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be the matrix of σ for this basis. Then, by the properties of the Weil pairing (in particular, the Galois equivariance of e_n expressed by (20)), one gets:

$$\begin{aligned} e_n(P_1, P_2)^\sigma &= e_n(P_1^\sigma, P_2^\sigma) \\ &= e_n(aP_1 + cP_2, bP_1 + dP_2) \\ &= e_n(P_1, P_2)^{ad-bc} \\ &= e_n(P_1, P_2)^{\det(\sigma)}, \end{aligned}$$

and the equality for arbitrary points Q_1, Q_2 in $E[n]$ follows by bilinearity. □

The following important results are consequences of the above lemma.

Proposition 3.2. *For all* $n \geq 1$ *prime to* p *there is an inclusion* $\mathrm{Gal}(F(E[n])/F) \subset \Gamma_n$.

Proof. The case $n = 1$ being trivial, we assume $n \geq 2$. Let $\sigma \in \mathrm{Gal}(F(E[n])/F)$; by definition of Γ_n, we have to show that $\det(\sigma)$ belongs to the subgroup H_n of $(\mathbb{Z}/n\mathbb{Z})^\times$ generated by r.

Choose $P, Q \in E[n]$ such that $\zeta_n := e_n(P, Q)$ is a primitive nth root of unity: this can be done by the non-degeneracy of the Weil pairing. Then

$$\zeta_n^\sigma = \zeta_n^{\det(\sigma)} \tag{21}$$

by Lemma 3.1. On the other hand, there is a natural identification $\mathrm{Gal}(\mathbb{F}_r(\boldsymbol{\mu}_n)/\mathbb{F}_r) = H_n$, so there exists a positive integer s such that

$$\zeta_n^\sigma = \zeta_n^{r^s}. \tag{22}$$

The claim follows immediately by comparing (21) and (22). □

As in the introduction, denote

$$\rho_E : G_F \longrightarrow \prod_{\ell \neq p} GL_2(\mathbb{Z}_\ell)$$

the Galois representation attached to E and write $\hat{\Gamma}$ for the profinite group defined in (7).

Corollary 3.3. *There is an inclusion* $\rho_E(G_F) \subset \hat{\Gamma}$.

Proof. Pass to the projective limit in the inclusions of Proposition 3.2. □

3.2. **Reduction to the split multiplicative case.** From here on $E_{/F}$ is non-isotrivial. We explain why it is not restrictive, for the purposes of our paper, to assume that $E_{/F}$ has split multiplicative reduction at ∞.

Proposition 3.4. *There exist a finite separable extension F' of F and a prime ∞' of F' such that the base-changed elliptic curve $E_{/F'} := E \times_F F'$ has split multiplicative reduction at ∞'.*

Proof. By assumption, $j(E) \notin \mathbb{F}_r$. In other words, $j(E)$ is a non-constant function on the smooth projective curve $\mathcal{C}$, hence there exists a closed point ∞ of $\mathcal{C}$ at which $j(E)$ has a pole. This means that $v_\infty(j(E)) < 0$, so E has potential multiplicative reduction at ∞ (cf. [23, Ch. VII, Propositions 5.4 and 5.5]). Thus we can find a finite extension $\tilde{F}$ of F and a prime $\tilde{\infty}$ of $\tilde{F}$ above ∞ such that $E_{/\tilde{F}}$ has multiplicative reduction at $\tilde{\infty}$. At the cost of passing to a quadratic extension F' of $\tilde{F}$ in which $\tilde{\infty}$ is inert (equal to a prime ∞'), E acquires *split* reduction. Finally, note (see *loc. cit.*) that we are making an extension $\tilde{F}/F$ of degree dividing 24 followed by an extension $F'/\tilde{F}$ of degree at most two: the separability of F'/F is granted by our assumption that $p > 3$. □

Now let L be a (not necessarily finite) separable extension of F and let $G_L \subset G_F$ be the corresponding absolute Galois group. In the sequel, Proposition 3.4 will be applied in conjunction with the following result.

Proposition 3.5. *If $\rho_E(G_L)$ is an open subgroup of $\hat{\Gamma}$ such is $\rho_E(G_F)$, hence Theorem 1.3 holds for $E_{/F}$ if it holds for $E_{/L}$.*

Proof. This is a simple argument about topological groups. Suppose that G is a topological group and let $H \subset H'$ be subgroups of G with H open in G. Then

$$H' = \bigcup_{h' \in H'} h'H$$

is open in G as well because it is the union of the open subsets $h'H$. To prove the proposition, observe that by Corollary 3.3 we already know that $\rho_E(G_F)$ is a subgroup of $\hat{\Gamma}$, and then apply the above result to the subgroups $\rho_E(G_L) \subset \rho_E(G_F)$ of $\hat{\Gamma}$. □

3.3. **Tate curves: an overview.** General references for the theory of Tate's analytic uniformization of elliptic curves are [14, Ch. 15], [22, Ch. IV, Appendix A.1] and [25, Ch. V], and we refer to them for more details and for proofs of the cited results.

Quite generally, in this § we let K denote a field which is complete with respect to a discrete valuation v; we assume that the residue field of K is perfect of characteristic $p > 0$. Let $q \in K^\times$ be such that $v(q) > 0$, and let $\langle q \rangle$ be the discrete subgroup of $K^\times$ generated by q. The *Tate elliptic curve* (relative to q) is the curve with Weierstrass equation

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)$$

whose coefficients are given by the power series

$$a_4(q) := -5 \sum_{n \geq 1} \frac{n^3 q^n}{1 - q^n}, \qquad a_6(q) := -\frac{1}{12} \sum_{n \geq 1} \frac{(7n^5 + 5n^3) q^n}{1 - q^n}.$$

Since $v(q) > 0$, these series converge in the v-adic metric. The discriminant and the j-invariant of E_q are given by the formulas

$$\Delta(q) = q \prod_{n \geq 1} (1 - q^n)^{24}, \qquad j(q) = \frac{1}{q} + 744 + 196884q + \dots,$$

which are clearly reminiscent of the corresponding ones from the complex case. If we define the series

$$x(u,q) := \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2\sum_{n\geq 1}\frac{nq^n}{1-q^n},$$

$$y(u,q) := \sum_{n\in\mathbb{Z}} \frac{q^{2n}u^2}{(1-q^n u)^3} + \sum_{n\geq 1}\frac{nq^n}{1-q^n}$$

we obtain a v-adic analytic uniformization

$$\begin{array}{rccc} \phi: & \bar{K}^\times/\langle q\rangle & \xrightarrow{\cong} & E_q(\bar{K}) \\ & u & \longmapsto & \big(x(u,q), y(u,q)\big). \end{array} \tag{23}$$

Since the action of $G_K := \mathrm{Gal}(\bar{K}/K)$ on $\bar{K}$ is v-adically continuous, the map ϕ defined in (23) is G_K-equivariant, i.e. ϕ is not only an isomorphism of v-adic Lie groups but also an isomorphism of G_K-modules. Of course, this property is of the utmost importance for arithmetic applications.

Because the j-invariant $j(q)$ of E_q is not integral (i.e., $v(j(q)) < 0$), it is clear that, unlike what happens for elliptic curves over the complex numbers, *not* every elliptic curve over K is analytically isomorphic to a quotient $\bar{K}^\times/\langle q\rangle$ for some $q \in K^\times$ with $v(q) > 0$. More precisely, the reduction $\tilde{E}_q$ of E_q modulo v has the equation

$$\tilde{E}_q : y^2 + xy = x^3,$$

so E_q has split multiplicative reduction over K. The crucial point in Tate's theory is that the non-integrality of the j-invariant is a necessary and sufficient condition for an elliptic curve E over K to be analytically uniformized as above. Indeed, the following fundamental result holds.

Theorem 3.6 (Tate)**.** *Let K be as before.*

i) For every $q \in K^\times$ with $v(q) > 0$ the map

$$\phi : \bar{K}^\times/\langle q\rangle \longrightarrow E_q(\bar{K})$$

described in (23) *is an isomorphism of G_K-modules.*

ii) For every $j_0 \in K^\times$ with $v(j_0) < 0$ there is a unique $q \in K^\times$ with $v(q) > 0$ such that the Tate elliptic curve $E_{q/K}$ has j-invariant j_0. The curve E_q is characterized by the equality $j(E_q) = j_0$ and the fact that it has split multiplicative reduction over K.

iii) Let $E_{/K}$ be an elliptic curve with non-integral j-invariant $j_0 \in K^\times$, and let E_q be the Tate curve with j-invariant j_0 as in ii). If E has split multiplicative reduction then E is isomorphic to E_q over K, while if E does not have split multiplicative reduction then there is a unique quadratic extension L of K such that E is isomorphic to E_q over L.

A complete proof of this theorem can be found in [25, Ch. V]. If $E_{/K}$ is an elliptic curve with non-integral j-invariant, the element $q \in K^\times$ whose existence is established in Theorem 3.6 is called "Tate period" for E.

Corollary 3.7. *Let $E_{/K}$ be an elliptic curve with non-integral j-invariant and split multiplicative reduction, and retain the notation of Theorem 3.6.*

i) Let $n \geq 0$ be an integer not divisible by p, let ζ_n be a primitive nth root of unity in $\bar{K}$ and fix an nth root $q^{1/n}$ of q in $\bar{K}$. There is an isomorphism

$$E[n] \cong \big\langle q^{1/n}, \zeta_n\big\rangle/\langle q\rangle$$

of G_K-modules.

ii) Let π be a uniformizer of K, write $q = \pi^e u$ with $e := v(q) > 0$ and denote v_ℓ the ℓ-adic valuation on $\mathbb{Q}$ for a prime ℓ. For all primes $\ell \neq p$ and integers $m > v_\ell(e)$ the field $K\big(q^{1/\ell^m}, \zeta_{\ell^m}\big)$ admits an automorphism σ over K leaving ζ_{ℓ^m} fixed and such that $\sigma(q^{1/\ell^m}) = (\zeta_{\ell^m})^{\ell^{v_\ell(e)}} \cdot q^{1/\ell^m}$. Thus there exists an element

$$\sigma \in \mathrm{Gal}(K(E[\ell^m])/K)$$

which is represented by $\left(\begin{smallmatrix} 1 & \ell^{v_\ell(e)} \\ 0 & 1 \end{smallmatrix}\right)$ with respect to the basis of $E[\ell^m]$ corresponding to the basis $\big\{\zeta_{\ell^m}, q^{1/\ell^m}\big\}$ of $E_q[\ell^m]$.

iii) With notation and conventions as before, the group $\mathrm{Gal}(K(E[\ell^\infty])/K)$ contains the subgroup

$$\begin{pmatrix} 1 & \ell^{v_\ell(e)}\mathbb{Z}_\ell \\ 0 & 1 \end{pmatrix}$$

of $GL_2(\mathbb{Z}_\ell)$ for all primes $\ell \neq p$.

Proof. Part *i)* is an immediate consequence of part *i)* of Theorem 3.6, while *ii)* follows from Kummer theory. Finally, *iii)* is implied by *ii)*. □

We shall use these results in the following situation. By Proposition 3.5, in order to prove Theorem 1.3 we can extend the ground field F to any separable extension; on the other hand, Proposition 3.4 guarantees the existence of a prime of split multiplicative reduction for E in a suitable finite separable extension of F. When combined together, these two results say that it is not restrictive for us to assume that the prime ∞ of F that we chose at the outset is of split multiplicative reduction for E, which from here on we do without any further comment. In particular, there are a Tate period $q \in F_\infty^\times$ and a $\mathrm{Gal}(\bar{F}_\infty/F_\infty)$-equivariant short exact sequence

$$0 \longrightarrow \langle q \rangle \longrightarrow \bar{F}_\infty^\times \longrightarrow E(\bar{F}_\infty) \longrightarrow 0$$

which expresses the geometric points of $E_{/F_\infty}$ as a quotient of a one-dimensional ∞-adic torus by an infinite cyclic subgroup.

As an application of Tate's uniformization, we conclude this § by showing that the prime-to-p torsion of E is rational over F^s.

Proposition 3.8. *With notation as above, let k be the smallest positive integer such that $q \notin (F_\infty^\times)^{p^k}$ and let $P \in E_{\mathrm{tors}}(\bar{F})$. Then $P \in E_{\mathrm{tors}}(F^s)$ if and only if p^k does not divide the order of P.*

Proof. Let n be the order of P and let $q^{1/n}$ be an nth root of q in $\bar{F}_\infty$. The geometric points in $E[n]$ are rational over $F_\infty(\boldsymbol{\mu}_n, q^{1/n}) \cap \bar{F}$, and the proposition follows from the next lemma. □

Lemma 3.9. $F^s = \bar{F} \cap F_\infty^s$.

Proof. It is enough to observe that the purely inseparable extensions of F are totally ramified at all places (as can be deduced, e.g., from [19, Proposition 7.5]). □

3.4. **Galois groups: horizontal control.** In this § we prove two results describing (in a strong way) the asymptotic behaviour of the Galois groups of $F(E[\ell])$ and of $F(E[\ell^\infty])$ over F when ℓ varies. As we shall see, the fact that E admits, locally at ∞, an analytic uniformization will be crucially exploited.

As a notational convention, if R is a domain denote $Q(R)$ the quotient field of R. We begin with two algebraic lemmas.

Lemma 3.10. *Let R be either a discrete valuation ring or a (topological) field. Let H be a subgroup of $GL_2(R)$ that acts irreducibly on $Q(R)^2$ and suppose that H contains the subgroup $\left(\begin{smallmatrix} 1 & I \\ 0 & 1 \end{smallmatrix}\right)$ where I is a nonzero ideal of R. Then H contains an open subgroup of $SL_2(R)$.*

In particular, if R is a field then $I = R$ and $H = SL_2(R)$.

Sketch of proof. By adapting the proof of [15, Ch. XIII, Lemma 8.1] it can be shown that

$$\left\langle \begin{pmatrix} 1 & 0 \\ I & 1 \end{pmatrix}, \begin{pmatrix} 1 & I \\ 0 & 1 \end{pmatrix} \right\rangle \supset \ker\Big(SL_2(R) \longrightarrow SL_2\big(R/I^2\big)\Big).$$

The kernel on the right is understood to be the whole $SL_2(R)$ if $I = R$. Observe that this kernel is open in $SL_2(R)$ because all nonzero ideals in R are open, hence the quotient R/I^2 is discrete. Finally, from the irreducibility condition and the fact that $\left(\begin{smallmatrix} 1 & I \\ 0 & 1 \end{smallmatrix}\right)$ is contained in H one can deduce the existence of a suitable basis of $Q(R)^2$ such that H contains $\left(\begin{smallmatrix} 1 & 0 \\ I & 1 \end{smallmatrix}\right)$ as well (see [22, Ch. IV, §3.2, Lemma 2] for details), and this completes the proof of the lemma. □

Lemma 3.11. *If $p \nmid n$ then* $\mathrm{Gal}(F(\boldsymbol{\mu}_n)/F) = H_n$.

Proof. Since $\mathbb{F}_r$ is algebraically closed in F it follows that

$$F \cap \mathbb{F}_r(\boldsymbol{\mu}_n) = \mathbb{F}_r,$$

i.e. F and $\mathbb{F}_r(\boldsymbol{\mu}_n)$ are linearly disjoint over $\mathbb{F}_r$. Thus

$$\mathrm{Gal}(F(\boldsymbol{\mu}_n)/F) = \mathrm{Gal}(\mathbb{F}_r(\boldsymbol{\mu}_n)/\mathbb{F}_r),$$

whence the claim. □

In the sequel let $\mathbb{F}_\ell$ be the field with ℓ elements. Now we can prove

Proposition 3.12. *The equality* $\mathrm{Gal}(F(E[\ell])/F) = \Gamma_\ell$ *holds for almost all primes $\ell \neq p$.*

Proof. First we show that $\mathrm{Gal}(F(E[\ell])/F)$ contains $SL_2(\mathbb{F}_\ell)$ for almost all primes $\ell \neq p$. To begin with, there is a natural embedding

$$\mathrm{Gal}(F_\infty(E[\ell])/F_\infty) \hookrightarrow \mathrm{Gal}(F(E[\ell])/F)$$

which we interpret as an inclusion, so that we view the former group as a subgroup of the latter. As in §3.3, write q for the Tate period of E at ∞, so $E(\bar{F}_\infty) \cong \bar{F}_\infty^\times/\langle q \rangle$ as Galois modules. Now let ℓ be a prime different from p not dividing $e = v_\infty(q)$. By part *ii)* of Corollary 3.7, there exists $\sigma \in \mathrm{Gal}(F_\infty(E[\ell])/F_\infty)$ which is represented by the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ with respect to a suitable $\mathbb{F}_\ell$-basis of $E[\ell]$. But part *i)* of Theorem 2.22 says that $E[\ell]$ is an irreducible $\mathrm{Gal}(F(E[\ell])/F)$-module for almost all primes $\ell \neq p$, so our claim follows from Lemma 3.10.

Now let $\ell \neq p$ be a prime such that $\mathrm{Gal}(F(E[\ell])/F)$ contains $SL_2(\mathbb{F}_\ell)$. As noticed before, one knows that $\boldsymbol{\mu}_\ell \subset F(E[\ell])$ and that the Galois action on the roots of unity is given by the determinant (Lemma 3.1), so Lemma 3.11 ensures that $\mathrm{Gal}(F(E[\ell])/F)$ fits into a short exact sequence

$$0 \longrightarrow SL_2(\mathbb{F}_\ell) \longrightarrow \mathrm{Gal}(F(E[\ell])/F) \xrightarrow{\det} H_\ell \longrightarrow 0.$$

By definition of Γ_ℓ, the proposition is proved. □

Remark 3.13. In their paper [5], Cojocaru and Hall give a uniform version of Proposition 3.12. More precisely, they show that there exists a positive constant $c(F)$, depending at most on the genus of $\mathcal{C}$, such that $\mathrm{Gal}(F(E[\ell])/F) = \Gamma_\ell$ for any non-isotrivial elliptic curve $E_{/F}$ and any prime number $\ell \geq c(F)$, $\ell \neq p$. Moreover, they determine an explicit expression for $c(F)$: see [5, Theorem 1].

Now we state an auxiliary result that will be applied in various occasions later on. By defining it componentwise in the obvious manner, consider the determinant map

$$\det : \hat{\Gamma} \longrightarrow \hat{H}.$$

This map is the one that appears in (7). By a slight abuse of notation, we denote in the same way both the determinant map on $\hat{\Gamma}$ and the analogous maps on the $\hat{\Gamma}_\ell$.

Lemma 3.14. *The following hold:*

i) $\det(\rho_{E,\ell}(G_F)) = \hat{H}_\ell$ *for all primes* $\ell \neq p$*;*

ii) $\det(\rho_E(G_F)) = \hat{H}$*.*

Proof. i) If ℓ is a prime different from p, it is an immediate consequence of Lemma 3.1 (cf. also [22, Ch. I, §1.2]) that

$$\det(\rho_{E,\ell}) : G_F \longrightarrow \mathbb{Z}_\ell^\times$$

coincides with the cyclotomic character giving the action of G_F on the ℓ^∞th roots of unity. It follows that $\det(\rho_{E,\ell}(G_F))$ identifies with the Galois group $\mathrm{Gal}(F(\boldsymbol{\mu}_{\ell^\infty})/F)$ where $F(\boldsymbol{\mu}_{\ell^\infty})$ is the extension of F generated by all roots of unity of order a power of ℓ. On the other hand, by setting $n = \ell^m$ and passing to the projective limit over m in Lemma 3.11 we get that

$$\mathrm{Gal}(F(\boldsymbol{\mu}_{\ell^\infty})/F) = \hat{H}_\ell,$$

whence our claim.

Part *ii)* can be proved in exactly the same way, this time working with all roots of unity of prime-to-p order. □

Remark 3.15. Lemma 3.14 is valid for all elliptic curves $E_{/F}$, including isotrivial ones.

Proposition 3.16. *For all primes* $\ell \neq p$ *the group* $\mathrm{Gal}(F(E[\ell^\infty])/F)$ *is open in* $\hat{\Gamma}_\ell$*.*

Proof. Let $\ell \neq p$ be a prime. From the theory of Tate's uniformization (see part *iii)* of Corollary 3.7) we know that

$$\begin{pmatrix} 1 & \ell^n\mathbb{Z}_\ell \\ 0 & 1 \end{pmatrix} \subset \rho_{E,\ell}(G_F) = \mathrm{Gal}(F(E[\ell^\infty])/F) \subset GL_2(\mathbb{Z}_\ell)$$

for $n = v_\ell(e)$ and $e = -v_\infty(j(E))$. But $V_\ell(E)$ is an irreducible $\rho_{E,\ell}(G_F)$-module by part *ii)* of Theorem 2.22, hence $\rho_{E,\ell}(G_F)$ contains an open subgroup of $SL_2(\mathbb{Z}_\ell)$ by Lemma 3.10. To prove the proposition one can proceed as follows. As a consequence of part *i)* of Lemma 3.14, there is a commutative diagram of short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & W & \longrightarrow & \rho_{E,\ell}(G_F) & \xrightarrow{\det} & \hat{H}_\ell & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & SL_2(\mathbb{Z}_\ell) & \longrightarrow & \hat{\Gamma}_\ell & \xrightarrow{\det} & \hat{H}_\ell & \longrightarrow & 0 \end{array} \tag{24}$$

where $W := \rho_{E,\ell}(G_F) \cap \ker(\det)$ and the vertical maps are inclusions. Since $\ker(\det) = SL_2(\mathbb{Z}_\ell)$ and W is an open subgroup of $SL_2(\mathbb{Z}_\ell)$, it follows that W is of finite index in $SL_2(\mathbb{Z}_\ell)$ because this matrix group is compact. But then the exact sequence between the cokernels of the vertical maps in (24) shows that $\rho_{E,\ell}(G_F)$ has finite index in $\hat{\Gamma}_\ell$, and this suffices to prove our claim because $\rho_{E,\ell}(G_F)$ is closed in $\hat{\Gamma}_\ell$. □

We conclude this § with the following

Proposition 3.17. *Let* S *be a finite set of primes not containing* p *and let*

$$\hat{\Gamma}_S := \prod_{\ell \in S} \hat{\Gamma}_\ell.$$

Moreover, denote $E[S^\infty]$ *the group of points of* E *of order divisible only by primes in* S*. Then* $\mathrm{Gal}(F(E[S^\infty])/F)$ *is open in* $\hat{\Gamma}_S$*.*

Proof. If L/F is a finite (separable) extension then $\mathrm{Gal}(L(E[S^\infty])/L)$ canonically identifies with the Galois group of $F(E[S^\infty])$ over $F(E[S^\infty]) \cap L$, so it can naturally be viewed as an open subgroup of $\mathrm{Gal}(F(E[S^\infty])/F)$. Let m be the product of the primes in S and set

$L := F(E[m])$. Then, as ℓ varies in S, the extensions $L(E[\ell^\infty])/L$ are pro-ℓ, thus the fields $L(E[\ell^\infty])$ are pairwise linearly disjoint over L. It follows that

$$\mathrm{Gal}(L(E[S^\infty])/L) = \prod_{\ell\in S} \mathrm{Gal}(L(E[\ell^\infty])/L). \tag{25}$$

But the same reasoning as above shows that, for all ℓ, $\mathrm{Gal}(L(E[\ell^\infty])/L)$ is an open subgroup of $\mathrm{Gal}(F(E[\ell^\infty])/F)$, and then Proposition 3.16 implies that $\mathrm{Gal}(L(E[\ell^\infty])/L)$ is open in $\hat{\Gamma}_\ell$. We readily deduce from (25) that $\mathrm{Gal}(L(E[S^\infty])/L)$ is open in $\hat{\Gamma}_S$, hence $\mathrm{Gal}(F(E[S^\infty])/F)$ is open in $\hat{\Gamma}_S$ as well. □

3.5. **Galois groups: vertical control.** In this short § we take a closer look at the Galois group of $F(E[\ell^\infty])$ over F for a prime number $\ell \neq p$. In order to do this, we need to introduce an algebraic notion that will prove extremely useful.

Let X be a profinite group and let Σ be a finite simple group. Following [22, Ch. IV, §3.4], we say that Σ *occurs* in X if there exist closed subgroups X_1, X_2 of X such that X_2 is normal in X_1 and $X_1/X_2 \cong \Sigma$.

Lemma 3.18. *With X and Σ as above, the following hold:*

i) let Y be a closed normal subgroup of X; if Σ occurs in X then Σ occurs in either Y or X/Y;

ii) if $X = \varprojlim X/\Omega_\alpha$ with Ω_α open in X for all α then Σ occurs in X if and only if Σ occurs in X/Ω_α for some α.

Proof. i) Let X_1, X_2 be closed subgroups of X with X_2 normal in X_1 and $X_1/X_2 \cong \Sigma$. Consider the composite map

$$X_1 \cap Y \hookrightarrow X_1 \twoheadrightarrow X_1/X_2,$$

which has $X_2 \cap Y$ as its kernel. Then it is easy to see that $(X_1 \cap Y)/(X_2 \cap Y)$ is a normal subgroup of X_1/X_2, which is simple by assumption. Hence there are two possibilities:

1. $(X_1 \cap Y)\big/(X_2 \cap Y) \cong X_1/X_2 \cong \Sigma$: in this case Σ occurs in Y;

2. $(X_1 \cap Y)\big/(X_2 \cap Y) = 0$, i.e. $X_1 \cap Y = X_2 \cap Y$: then Σ occurs in X/Y because

$$\Sigma \cong X_1/X_2 \cong (X_1/X_1 \cap Y)\big/(X_2/X_2 \cap Y) \cong (X_1Y/Y)\big/(X_2Y/Y).$$

ii) The "if" part is easy. For the other implication, observe that the family $\{\Omega_\alpha\}_\alpha$ is a basis of neighbourhoods of the identity in X. Let $X_1, X_2 \subset X$ be closed subgroups with X_2 normal in X_1 and $X_1/X_2 \cong \Sigma$. Since Σ is finite, X_2 is open in X_1, hence there exists an index α such that $X_1 \cap \Omega_\alpha \subset X_2$ and, in particular, $X_1 \cap \Omega_\alpha = X_2 \cap \Omega_\alpha$. There are closed injections

$$X_2/(X_2 \cap \Omega_\alpha) \hookrightarrow X_1/(X_1 \cap \Omega_\alpha) \hookrightarrow X/\Omega_\alpha$$

with $X_2/(X_2 \cap \Omega_\alpha)$ normal in $X_1/(X_1 \cap \Omega_\alpha)$, hence Σ occurs in X/Ω_α. □

As usual, set $PSL_2(\mathbb{F}_\ell) := SL_2(\mathbb{F}_\ell)/\{\pm 1\}$ for all primes ℓ. It is well known that these groups are simple for $\ell \geq 5$ (see, e.g., [15, Ch. XIII, Theorem 8.4]), and it is easy to see that they are pairwise non-isomorphic; a common theme of the next proposition and of the proof of Proposition 3.21 below will be the study of their occurrences in suitable profinite groups.

Proposition 3.19. *The group $PSL_2(\mathbb{F}_\ell)$ occurs in $\mathrm{Gal}(F(E[\ell^\infty])/F)$ for almost all $\ell \neq p$.*

Proof. We know that

$$\mathrm{Gal}(F(E[\ell^\infty])/F) = \varprojlim_n \mathrm{Gal}(F(E[\ell^n])/F).$$

Moreover, by Proposition 3.12 the group $\mathrm{Gal}(F(E[\ell])/F)$ contains $SL_2(\mathbb{F}_\ell)$ for almost all primes $\ell \neq p$. Hence $PSL_2(\mathbb{F}_\ell)$ occurs in $\mathrm{Gal}(F(E[\ell])/F)$ for almost all $\ell \neq p$, and the claim follows from part *ii)* of Lemma 3.18. □

3.6. **Conclusion of the proof.** As remarked in the introduction, this is really an exercise in abstract group theory; in particular, elliptic curves will play no role. We follow *mutatis mutandis* the exposition in [14, Ch. 17, §5] and [22, Ch. IV, §3.4]. We begin by stating a very useful lemma, a proof of which is given in [22, Ch. IV, §3.4, Lemmas 2 and 3].

Lemma 3.20. *Let $\ell \geq 5$ be a prime number and let H be a closed subgroup of $SL_2(\mathbb{Z}_\ell)$ whose reduction* mod ℓ *surjects onto $PSL_2(\mathbb{F}_\ell)$. Then $H = SL_2(\mathbb{Z}_\ell)$.*

With this result at our disposal, we can prove

Proposition 3.21. *With self-explaining notation, the group $\rho_E(G_F)$ contains*

$$S_\ell := \big(\dots, 1, 1, SL_2(\mathbb{Z}_\ell), 1, 1, \dots\big)$$

for almost all primes $\ell \neq p$.

Proof. By Proposition 3.19, we know that $PSL_2(\mathbb{F}_\ell)$ occurs in the component of $\rho_E(G_F)$ corresponding to ℓ for almost all primes $\ell \neq p$. To prove the proposition, we first show that $PSL_2(\mathbb{F}_\ell)$ occurs in $\rho_E(G_F) \cap S_\ell$ for almost all $\ell \neq p$. Let

$$U_\ell := \big(\dots, 1, 1, \hat{\Gamma}_\ell, 1, 1, \dots\big)$$

for all primes $\ell \neq p$. Clearly, for every prime $\ell \neq p$ there is an injection

$$\rho_E(G_F)\big/\big(\rho_E(G_F) \cap U_\ell\big) \hookrightarrow \hat{\Gamma}/U_\ell. \tag{26}$$

By part *ii)* of Lemma 3.18, $PSL_2(\mathbb{F}_\ell)$ does not occur in $\hat{\Gamma}_q$ for any prime $q \neq \ell$ if $\ell > 5$. Hence, by (26), $PSL_2(\mathbb{F}_\ell)$ does not occur in the quotient $\rho_E(G_F)/(\rho_E(G_F) \cap U_\ell)$, so part *i)* of Lemma 3.18 ensures that it occurs in $\rho_E(G_F) \cap U_\ell$ for almost all $\ell \neq p$. It follows from part *i)* of Lemma 3.18 that for any such ℓ the group $PSL_2(\mathbb{F}_\ell)$ occurs in $\rho_E(G_F) \cap S_\ell$, which is closed in S_ℓ and maps to $PSL_2(\mathbb{F}_\ell)$ by reducing mod ℓ and projecting. Denote M_ℓ the image of $\rho_E(G_F) \cap S_\ell$ in $PSL_2(\mathbb{F}_\ell)$: we claim that $M_\ell = PSL_2(\mathbb{F}_\ell)$. If not, M_ℓ is a proper subgroup, so $PSL_2(\mathbb{F}_\ell)$ occurs in the kernel of this map, hence in

$$\big\{u \in SL_2(\mathbb{Z}_\ell) \mid u \equiv 1 \pmod{\ell}\big\}. \tag{27}$$

But this is impossible if $\ell \geq 5$ because the group in (27) is prosolvable[5] while $PSL_2(\mathbb{F}_\ell)$ is nonabelian and simple, hence nonsolvable.

Therefore $\rho_E(G_F) \cap S_\ell$ maps onto $PSL_2(\mathbb{F}_\ell)$, hence $\rho_E(G_F) \cap S_\ell \cong SL_2(\mathbb{Z}_\ell)$ by Lemma 3.20. □

Corollary 3.22. *There exists a finite set S of prime numbers such that $p \in S$ and $\rho_E(G_F)$ contains $\prod_{\ell \notin S} SL_2(\mathbb{Z}_\ell)$.*

In the statement of this corollary, the partial product is understood as a subgroup of $\hat{\Gamma}$ in the natural way.

---

[5]This can be seen as follows. For all $n \geq 1$ and $j \in \{1, \dots, n\}$ define the groups

$$K_j^{(n)} := \ker\Big(SL_2(\mathbb{Z}/\ell^n\mathbb{Z}) \twoheadrightarrow SL_2(\mathbb{Z}/\ell^j\mathbb{Z})\Big).$$

Then for all n there is a chain

$$K_n^{(n)} = \{1\} \subset K_{n-1}^{(n)} \subset \cdots \subset K_1^{(n)}$$

with $K_{j+1}^{(n)}$ normal in $K_j^{(n)}$ and $K_j^{(n)}/K_{2j}^{(n)}$ abelian (for example, it injects in the additive group $M_2(\mathbb{Z}/\ell^n\mathbb{Z})$). This shows that $K_1^{(n)}$ is solvable for all $n \geq 1$, and since

$$\big\{u \in SL_2(\mathbb{Z}_\ell) \mid u \equiv 1 \pmod{\ell}\big\} = \varprojlim_n K_1^{(n)}$$

the claim follows.

Proof. With identifications as before, by Proposition 3.21 there exists a finite set S of primes such that $p \in S$ and $\rho_E(G_F)$ contains $SL_2(\mathbb{Z}_\ell)$ for all $\ell \notin S$. It follows that $\rho_E(G_F)$ contains

$$\mathscr{S} := \bigcup_{\substack{|T|<\infty \\ T\cap S=\emptyset}} \prod_{\ell\in T} SL_2(\mathbb{Z}_\ell),$$

where T runs through the finite sets of primes that are disjoint from S. But $\rho_E(G_F)$ is closed in $\hat{\Gamma}$, hence it contains the closure of $\mathscr{S}$, which is the product appearing in the statement of the corollary. □

Now we are in a position to prove Igusa's theorem. For the reader's convenience we restate Theorem 1.3, and then proceed to its proof.

Theorem 3.23 (Igusa)**.** *The group $\rho_E(G_F)$ is open in $\hat{\Gamma}$.*

Proof. Let S be as in Corollary 3.22, let $S' := S - \{p\}$ and let S'' be the (infinite) set of primes not in S. As before, write

$$\hat{\Gamma}_{S'} := \prod_{\ell\in S'} \hat{\Gamma}_\ell, \qquad \hat{\Gamma}_{S''} := \prod_{\ell\in S''} \hat{\Gamma}_\ell.$$

Denote $\rho_{E,S'}(G_F)$ and $\rho_{E,S''}(G_F)$ the projections of $\rho_E(G_F)$ to $\hat{\Gamma}_{S'}$ and $\hat{\Gamma}_{S''}$, respectively. A combination of Corollary 3.22 and part *i)* of Lemma 3.14 shows that $\rho_{E,S''}(G_F) = \hat{\Gamma}_{S''}$. On the other hand, $\rho_{E,S'}(G_F)$ is open in $\hat{\Gamma}_{S'}$ by Proposition 3.17. It follows that

$$\rho_E(G_F) \supset \rho_{E,S'}(G_F) \times \hat{\Gamma}_{S''},$$

which is an open subgroup of $\hat{\Gamma}$. The theorem is proved. □

Remark 3.24. To prove Igusa's theorem one could also proceed as follows. By an argument with Lie algebras exactly as in [22, Ch. IV, §3.4, Lemma 6], it can be deduced from Proposition 3.17 and Corollary 3.22 that $\rho_E(G_F)$ contains an open subgroup of $\prod_{\ell\neq p} SL_2(\mathbb{Z}_\ell)$. But then part *ii)* of Lemma 3.14 allows one to conclude the proof as in Proposition 3.16.

4. An arithmetic application

In this final section we collect an arithmetic consequence of Theorem 1.3. We retain throughout our previous notation; in particular, $F = \mathbb{F}_r(\mathcal{C})$ is a function field of characteristic $p > 0$ and F^s is the separable closure of F contained in an algebraic closure $\bar{F}$. We remark that Theorem 1.3 is valid in any positive characteristic, though in the present paper we have proved it only for $p > 3$.

4.1. **Main application.** The result we want to prove in this § says that a non-isotrivial elliptic curve $E_{/F}$ has only finitely many torsion points rational over abelian extensions of F. Although properties in the same spirit have been exploited, at least implicitly, in various recent works on the arithmetic of elliptic curves in positive characteristic (cf., e.g., [1], [3], [4], [28]), it seems that (quite surprisingly) the result below has never been written down in detail.

We begin with a lemma in linear algebra.

Lemma 4.1. *Let ℓ be a prime and let S_n be the kernel of the reduction-modulo-ℓ^n map*

$$SL_2(\mathbb{Z}_\ell) \longrightarrow SL_2(\mathbb{Z}/\ell^n\mathbb{Z}).$$

The commutator subgroup $[S_n, S_n]$ contains S_{2n+2} for all $n \geq 2$.

Sketch of proof. One just adapts the arguments of [15, Ch. XIII, Lemma 8.1] (as in Lemma 3.10). □

Now we can prove the result we alluded to before.

Theorem 4.2. *Let $E_{/F}$ be a non-isotrivial elliptic curve and let $H := F^{ab}$ be the maximal abelian extension of F. The group $E_{\mathrm{tors}}(H)$ is finite.*

Proof. Define an *Igusa prime* to be a prime number satisfying the second part of Theorem 1.4. To prove our result we show that

i) $E[\ell^\infty](H)$ is finite for all primes ℓ;
ii) $E[\ell](H) = \{0\}$ if ℓ is an Igusa prime.

Since by Theorem 1.4 almost all primes are Igusa, the theorem will follow.

i) We need to distinguish between two cases according as whether ℓ is equal to the characteristic of F or not.

If $\ell = p$ the claim is immediate from Proposition 3.8 (see also [3, Lemma 2.2] for a proof using a different argument).

If $\ell \neq p$ define the groups S_n as in Lemma 4.1. By Theorem 1.4, $S_n \subset \rho_{E,\ell}(G_F)$ for some $n \geq 2$. Since $\mathrm{Gal}(F^s/H)$ is the topological closure of the commutator subgroup $[G_F, G_F]$, its image under $\rho_{E,\ell}$ contains the commutator subgroup $[S_n, S_n]$ of $GL_2(\mathbb{Z}_\ell)$, and hence, by Lemma 4.1, S_{2n+2}. Therefore $E[\ell^\infty](H)$ is contained in the fixed subgroup of $E[\ell^\infty]$ under the action of S_{2n+2}, which is the finite group $E[\ell^{2n+2}]$.

ii) Let ℓ be an Igusa prime and set $F_\ell := F(E[\ell])$; then $\mathrm{Gal}(F_\ell/F)$ contains a subgroup isomorphic to $SL_2(\mathbb{F}_\ell)$, hence the Galois orbit of a nonzero point $P \in E[\ell]$ is the whole $E[\ell] - \{0\}$. In particular, since the extension H/F is normal, if $P \in E[\ell](H)$ and $P \neq 0$ then $F_\ell \subset H$, which is impossible because H/F is abelian. Thus $E[\ell](H) = \{0\}$, and the theorem is completely proved. □

Remark 4.3. Replacing Igusa's theorem with Serre's theorem (Theorem 1.1) and disregarding, of course, the "$\ell = p$" part, the proof of Theorem 4.2 carries over *verbatim* to the case of an elliptic curve without complex multiplication defined over a number field. More precisely, one shows that if K is a number field and $E_{/K}$ is a non-CM elliptic curve then there are only finitely many torsion points on E that are rational over abelian extensions of K. Note that this is the one-dimensional case of a theorem of Zarhin ([30, Theorem 1]) for non-CM abelian varieties (see also [18, Theorem 1] for a weaker result which is valid for all abelian varieties).

Remark 4.4. If $\mathbb{Z} \subsetneq \mathrm{End}(E)$, i.e., if $E_{/F}$ is isotrivial (resp., has complex multiplication) in the function field (resp., in the number field) case, then Theorem 4.2 is false. Indeed, with notation as in the introduction, it can be shown that there exists a finite extension K/F such that

$$E_{(p)\text{-tors}} \subset E(K^{ab}).$$

This fact is a consequence of the results described in Appendix A in the function field case and of the theory of complex multiplication in the number field case.

Appendix A. The isotrivial case

For the sake of completeness, in this appendix we treat the case of isotrivial elliptic curves. We remark that we only give a "qualitative" description of the image of Galois; actually, something more precise can presumably be proved, but we shall not pursue this issue here.

So let $E_{/F}$ be our elliptic curve over the function field $F = \mathbb{F}_r(\mathcal{C})$ and suppose that E is isotrivial. Recall that this means that after a finite extension L/F the curve E becomes isomorphic to an elliptic curve E' defined over $\mathbb{F}_r$; equivalently, $j(E) \in \mathbb{F}_r$. By Lemma 2.21, we can also equivalently define the elliptic curve $E_{/F}$ to be isotrivial if its ring of endomorphisms is larger than $\mathbb{Z}$.

First of all, note that there is an inclusion $\rho_E(G_F) \subset \hat{\Gamma}$ (in fact, the arguments in §3.1 do not rely on E being non-isotrivial, but just on general properties of the Weil pairing). Our

present goal is to show that $\rho_E(G_F)$ is not open in $\hat{\Gamma}$ (in particular, the above inclusion is proper), so that Theorem 1.4 is always false in the isotrivial case.

Let L/F be an extension as above, so that the base-changed curve $E_{/L}$ is isomorphic to an elliptic curve E' defined over $\mathbb{F}_r$. Since we are assuming that $p > 3$, the extension L/F may be taken to be separable, and we denote $G_L \subset G_F$ the absolute Galois group of L. Observe that there are isomorphisms

$$E_{(p)\text{-tors}}(F^s) = E_{(p)\text{-tors}}(L^s) \cong E'_{(p)\text{-tors}}(\bar{\mathbb{F}}_r)$$

of G_L-modules, and if we set $\mathbb{F}_s := L \cap \bar{\mathbb{F}}_r$ (that is, $\mathbb{F}_s$ is the field of constants of L) then the action of G_L on $E'_{(p)\text{-tors}}$ factors through the absolute Galois group $G_{\mathbb{F}_s} := \mathrm{Gal}(\bar{\mathbb{F}}_r/\mathbb{F}_s)$. This last group is procyclic, isomorphic to the profinite completion $\hat{\mathbb{Z}}$ of $\mathbb{Z}$. It follows that $\rho_E(G_L)$ is a procyclic (hence abelian) group, so it cannot be open in $\hat{\Gamma}$. Since $\rho_E(G_L)$ has finite index in $\rho_E(G_F)$, we can state the following

Proposition A.1. *If $E_{/F}$ is isotrivial then $\rho_E(G_F)$ is not open in $\hat{\Gamma}$.*

In fact, we can say something more. To this end, define the profinite groups $\hat{H}'$ and $\hat{\Gamma}'$ as in (7) by replacing r with s. Clearly, $\hat{H}' \subset \hat{H}$ and $\hat{\Gamma}' \subset \hat{\Gamma}$. Now recall that $\hat{\mathbb{Z}}_{(p)}$ is a shorthand for $\prod_{\ell \neq p} \mathbb{Z}_\ell$ and let

$$\rho_{E'} : G_{\mathbb{F}_r} \longrightarrow GL_2(\hat{\mathbb{Z}}_{(p)})$$

be the Galois representation attached to E'. The cyclotomic character χ induces an isomorphism

$$\chi : G_{\mathbb{F}_s} \xrightarrow{\cong} \hat{H}'$$

with the property that $\det \circ \rho_{E'} = \chi$, thus the diagram

$$\begin{array}{ccc} G_L & \xrightarrow{\rho_E} & \rho_E(G_L) \\ \downarrow & \overset{\rho_{E'}}{\nearrow} & \downarrow \det \\ G_{\mathbb{F}_s} & \xrightarrow{\chi} & \hat{H}' \end{array}$$

is commutative. It follows that the determinant gives an isomorphism

$$\det : \rho_E(G_L) \xrightarrow{\cong} \hat{H}',$$

hence the short exact sequence defining $\hat{\Gamma}'$ admits a (topological) splitting as follows:

$$\begin{array}{ccccccccc} & & & & \rho_E(G_L) & & & & \\ & & & & \downarrow & \searrow^{\det} & & & \\ 0 & \longrightarrow & SL_2(\hat{\mathbb{Z}}_{(p)}) & \longrightarrow & \hat{\Gamma}' & \longrightarrow & \hat{H}' & \longrightarrow & 0. \end{array}$$

In other words, we have proved the following

Theorem A.2. *With notation as above, if $E_{/F}$ is isotrivial then there are isomorphisms*

$$\hat{\Gamma}' \cong SL_2(\hat{\mathbb{Z}}_{(p)}) \rtimes \hat{H}' \cong SL_2(\hat{\mathbb{Z}}_{(p)}) \rtimes \rho_E(G_L)$$

of topological groups. In particular, $\rho_E(G_L)$ is not open in $\hat{\Gamma}'$.

Actually, by working componentwise it can be shown (as above) that $\rho_{E,\ell}(G_F) \subsetneq \hat{\Gamma}_\ell$ for all primes $\ell \neq p$.

Remark A.3. The goal of this appendix was to highlight the following "principle": as long as one is interested in the "asymptotic size" of the images of the Galois representations on Tate modules of elliptic curves, *isotriviality* is the counterpart in characteristic p of *complex multiplication* over number fields. In fact, when the ring of endomorphisms is "as small as possible" (i.e., equal to $\mathbb{Z}$) the image of Galois is definitively "as large as possible" (i.e., equal to $GL_2(\mathbb{Z}_\ell)$ in characteristic zero and to $\hat{\Gamma}_\ell$ in positive characteristic), while this never happens (both in positive characteristic and in characteristic zero, cf. Remark 1.2) when the elliptic curve has an endomorphism ring of rank greater than one.

References

[1] A. Bandini, I. Longhi, Control theorems for elliptic curves over function fields, *Int. J. Number Theory*, to appear.

[2] G. Böckle, Arithmetic over function fields: a cohomological approach. In *Number fields and function fields – two parallel worlds*, G. van der Geer, B. Moonen and R. Schoof (eds.), Progress in Mathematics **239**, Birkhäuser, Boston, 2005, 1-38.

[3] F. Breuer, Higher Heegner points on elliptic curves over function fields, *J. Number Theory* **104** (2004), 315-326.

[4] M. L. Brown, *Heegner modules and elliptic curves*, Lecture Notes in Mathematics **1849**, Springer, Berlin, 2004.

[5] A. C. Cojocaru, C. Hall, Uniform results for Serre's theorem for elliptic curves, *Int. Math. Res. Not.* **50** (2005), 3065-3080.

[6] P. Deligne, Preuve des conjectures de Tate et de Shafarevitch (d'après G. Faltings). In "Séminaire Bourbaki" 36e année, 1983/84, no. 619, *Astérisque* **121-122** (1985), 25-41.

[7] P. Deligne, M. Rapoport, Les schémas de modules de courbes elliptiques. In *Modular functions II*, P. Deligne and W. Kuyk (eds.), Lecture Notes in Mathematics **349**, Springer-Verlag, Berlin, 1973, 143-316.

[8] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), 349-366.

[9] G. Frey, Links between solutions of $A - B = C$ and elliptic curves. In *Number theory*, H. P. Schlickewei and E. Wirsing (eds.), Lecture Notes in Mathematics **1380**, Springer-Verlag, New York, 1989, 31-62.

[10] ———, On ternary equations of Fermat type and relations with elliptic curves. In *Modular forms and Fermat's last theorem*, G. Cornell, J. H. Silverman and G. Stevens (eds.), Springer-Verlag, New York, 1997, 527-548.

[11] ———, Galois representations attached to elliptic curves and Diophantine problems. In *Number theory*, M. Jutila and T. Metsänkylä (eds.), Walter de Gruyter & Co., Berlin, 2001, 71-104.

[12] M. Hindry, J. H. Silverman, The canonical height and integral points on elliptic curves, *Invent. Math.* **93** (1988), 419-450.

[13] J.-I. Igusa, Fibre systems of jacobian varieties (III. Fibre systems of elliptic curves), *Amer. J. Math.* **81** (1959), 453-476.

[14] S. Lang, *Elliptic functions*, second edition, Graduate Texts in Mathematics **112**, Springer-Verlag, New York, 1987.

[15] ———, *Algebra*, revised third edition, Graduate Texts in Mathematics **211**, Springer-Verlag, New York, 2002.

[16] Q. Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics **6**, Oxford University Press, Oxford, 2002.

[17] D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research studies in mathematics **5**, Oxford University Press, Oxford, 1970.

[18] K. A. Ribet, Torsion points on abelian varieties in cyclotomic extensions (appendix to an article by N. Katz and S. Lang), *Enseign. Math. (2)* **27** (1981), 315-319.

[19] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics **210**, Springer-Verlag, New York, 2002.

[20] J.-P. Serre, Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures). In *Séminaire Delange-Pisot-Poitou. Théorie des nombres*, tome **11**, n. 2 (1969-1970), exp. n. 19, 1-15 (Œuvres n. **87**). Available at `http://www.numdam.org`.

[21] ———, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259-331.

[22] ———, *Abelian l-adic representations and elliptic curves*, revised second edition, Research Notes in Mathematics **7**, A K Peters, Wellesley, MA, 1998.

[23] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 1986.
[24] ———, Heights and elliptic curves. In *Arithmetic Geometry*, G. Cornell and J. H. Silverman (eds.), revised second printing, Springer-Verlag, New York, 1998, 253-265.
[25] ———, *Advanced topics in the arithmetic of elliptic curves*, corrected second printing, Graduate Texts in Mathematics **151**, Springer-Verlag, New York, 1999.
[26] L. Szpiro, La conjecture de Mordell (d'après G. Faltings). In "Séminaire Bourbaki" 36e année, 1983/84, no. 619, *Astérisque* **121-122** (1985), 83-103.
[27] D. Ulmer, Elliptic curves and analogies between number fields and function fields. In *Heegner points and Rankin L-series*, H. Darmon and S.-W. Zhang (eds.), MSRI Publications **49**, Cambridge University Press, Cambridge, 2004, 285-315.
[28] S. Vigni, On ring class eigenspaces of Mordell-Weil groups of elliptic curves over global function fields, *J. Number Theory*, to appear.
[29] F. Voloch, Explicit p-descent for elliptic curves in characteristic p, *Compos. Math.* **74** (1990), 247-258.
[30] Yu. G. Zarhin, Endomorphisms and torsion of abelian varieties, *Duke Math. J.* **54** (1987), 131-145.

A. B.: Dipartimento di Matematica, Università della Calabria, Via P. Bucci – Cubo 30B, 87036 Arcavacata di Rende (CS), Italy
E-mail address: bandini@mat.unical.it

I. L.: Dipartimento di Matematica, Università di Milano, Via C. Saldini 50, 20133 Milano, Italy
E-mail address: longhi@mat.unimi.it

S. V.: Dipartimento di Matematica, Università di Milano, Via C. Saldini 50, 20133 Milano, Italy
E-mail address: stevigni@mat.unimi.it