Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 59 (2013)

Artikel: Sharpening "Manin-Mumford" for certain algebraic groups of dimension 2
Autor: Corvaia, Pietro / Masser, David / Zannier, Umberto
DOI: https://doi.org/10.5169/seals-515835

L'Enseignement Mathématique (2) 59 (2013), 225–269

SHARPENING 'MANIN-MUMFORD' FOR CERTAIN ALGEBRAIC GROUPS OF DIMENSION 2

by Pietro CORVAJA, David MASSER and Umberto ZANNIER

ABSTRACT. The present paper arises from the extensions of the Manin-Mumford conjecture, where we shall focus on the case of (complex connected) commutative algebraic groups G of dimension 2. This context predicts finiteness for the set of torsion points in an algebraic curve inside G, unless the curve is 'special', i.e. a translate of an algebraic subgroup of G.

Here we shall consider not merely the set of torsion points, but its topological closure in G (which equals the maximal compact subgroup). In the case of abelian varieties this closure is the whole space, but this is not so for other groups G; actually, we shall prove that in certain cases (where a natural dimensional condition is fulfilled) the intersection of this larger set with a non-special curve must still be a finite set.

Beyond this, in the paper we shall briefly review some of the basic theory of group extensions of an elliptic curve by the additive group $\mathbf{G}_a$, especially relevant in the said result.

We shall conclude by stating some general questions in the same direction and discussing some simple examples.

The paper concludes with the reproduction of a letter of Serre (whom we thank for his permission) to the second author, explaining how to obtain explicit projective embeddings of the said group extensions.

1. INTRODUCTION

The celebrated Manin-Mumford conjecture stated that *a complex curve of genus ≥ 2, embedded in its Jacobian variety J, contains only finitely many torsion points of J*. (See for instance [22] for a discussion.) The conjecture was proved by Raynaud [11], actually in extended form, considering a general (complex) abelian variety A and an irreducible subvariety X; he proved that

the set of torsion points[1]) of A contained in X is Zariski-dense in X only in the 'obvious' case when X is a translate (by a torsion point) of an abelian subvariety of A.

After Raynaud's, several proofs of this and related statements appeared. A quantitative proof of Raynaud's theorem was given by Hindry [6]; his paper in fact contains a complete treatment of the case of arbitrary commutative algebraic groups, and so also includes the case of extensions of abelian varieties by commutative linear groups, these last being known to be of the shape[2]) $\mathbf{G}_{\mathrm{m}}^{r} \times \mathbf{G}_{\mathrm{a}}^{s}$.

HINDRY'S THEOREM. *Let G be a commutative complex connected algebraic group and let $X \subset G$ be an irreducible algebraic subvariety. If X contains a Zariski-dense set of torsion points of G, then X is a translate of an algebraic subgroup by a torsion point.*

This general viewpoint shall be especially relevant for our issues here, which concern any commutative algebraic group.

This result is almost tautological when $\dim G = 1$, i.e. when G is either the multiplicative group $\mathbf{G}_{\mathrm{m}}$, or the additive group $\mathbf{G}_{\mathrm{a}}$, or an elliptic curve, but it is already far from obvious when G has dimension 2. Taking the case of dimension 2 for the sake of example, a related question had been posed by Lang (almost simultaneously with Mumford's question on Jacobians) for the special case of a multiplicative torus[3]); Lang expected that:

An irreducible curve X in $\mathbf{G}_{\mathrm{m}}^{2}$ contains infinitely many torsion points of $\mathbf{G}_{\mathrm{m}}^{2}$ only if it is a translate (by a torsion point) of an algebraic subgroup.

A 'concrete' view of this statement is gotten on noting that torsion points of $\mathbf{G}_{\mathrm{m}}^{2}$ are those whose coordinates are roots of unity; so, if X is defined by $F(x,y) = 0$, we are concerned with the algebraic equation $F(\theta,\eta) = 0$ in roots of unity θ,η. Also, that X is such a translate (commonly called

[1]) Here and in the sequel we shall tacitly restrict to fields of characteristic 0, typically $\overline{\mathbf{Q}}$ or $\mathbf{C}$. Note that if for instance A is defined over a finite field, then every algebraic point is torsion, so the conclusion of the Manin-Mumford statement is clearly false, and the same happens for related statements we shall meet.

[2]) This holds if the ground field is algebraically closed, which we shall assume here, being immaterial for the present purposes.

[3]) By this we mean a power of $\mathbf{G}_{\mathrm{m}}$, which in turn may be defined as the affine line $\mathbf{A}^{1}$ deprived of the origin, equipped with the multiplicative group law. We shall briefly recall below some standard definitions, also for other notions appearing in this Introduction.

torsion-coset) amounts[4]) to $F(x,y)$ being, up to a monomial factor, of the shape $x^a y^b - \zeta$ for integers a,b and a root of unity ζ. This 'exceptional' shape clearly leads indeed to infinitely many torsion points on X and is the analogue of the exceptional varieties appearing in Raynaud's theorem above.

Elementary proofs of Lang's expectation were soon found by Ihara, Serre and Tate, and subsequently by other authors. (See again [22] for references and for a discussion of such issues and their origins, also in connection with the Manin-Mumford conjecture.)

A particularly simple special case of Lang's above statement is obtained for instance when X is a polynomial graph: $X : \{(t,f(t))\}$ for an $f \in \mathbf{C}[x]$, so X is defined by $y - f(x) = 0$. Now we are considering the roots of unity θ such that $f(\theta)$ is also a root of unity. There are several easy ways to prove that *this can occur for infinitely many* θ *only if* $f(x) = \zeta x^d$, *for some root of unity* ζ (which is the shape predicted for this case by the above general statement). One of the many possible proofs actually shows more, namely:

If there are infinitely many $\xi \in \mathbf{C}$ *with* $|\xi| = |f(\xi)| = 1$ *then* $f(x) = \eta x^d$ *for some* $\eta \in \mathbf{C}$.

This conclusion, which indeed immediately leads to the previously sought one, is easily proved as follows. Let $S_1 = \{z \in \mathbf{C} : |z| = 1\}$ denote the unit circle in $\mathbf{C}$ and let $\bar{f}$ denote the polynomial obtained by conjugating coefficients. Then the function $\phi(z) := f(z)\bar{f}(z^{-1})$ is holomorphic in $\mathbf{C} - \{0\}$, actually a Laurent polynomial, and such that $\phi(z) = |f(z)|^2$ for $z \in S_1$. Then, under our assumptions $\phi(z)$ takes a same value (i.e. 1) infinitely many times in the compact set S_1 and thus must be a constant c (necessarily $= 1$). Then, if $d = \deg f$, the equation $f(z)(z^d \bar{f}(z^{-1})) = cz^d$ exhibits a factorization of cz^d into a product of two polynomials, which therefore must themselves be monomials, proving the claim.

This shows that, excluding the said special (monomial) shape, it is not merely true that the curve X of this example contains only finitely many torsion points, but actually X *meets their full topological closure* $S_1^2 \subset \mathbf{G}_m^2$ *only in a finite set*[5]). Note that indeed S_1 is the topological closure of the set of roots of unity in $\mathbf{C}$. We further note that this set is relevant also in

[4]) Actually, such explicit phrasing was already pointed out by Lang in his original problem.

[5]) An especially simple and illustrative instance occurs when X is the line $x + y = 1$; now the points in $X \cap S_1^2$ are obtained by intersecting the unit circles in $\mathbf{C}$ centered at 0 and 1.

being the *maximal compact subgroup* of the complex torus $\mathbf{G}_{\mathrm{m}}(\mathbf{C}) = \mathbf{C}^*$, in the complex topology.

One may ask whether this sharper conclusion holds in place of Lang's statement, i.e. for every irreducible algebraic curve $X \subset \mathbf{G}_{\mathrm{m}}^2$ that $X \cap S_1^2$ *is finite provided* $X \subset \mathbf{G}_{\mathrm{m}}^2$ *is not a translate of an algebraic subgroup*, which we abbreviate by *coset*. It turns out that this is not generally true, indeed already for curves which are rational graphs: for instance, any Möbius transformation $z \mapsto \frac{z-\alpha}{1-\overline{\alpha}z}$, $\alpha \in \mathbf{C} - S_1$, is a holomorphic automorphism of the Riemann sphere $\mathbf{P}_1(\mathbf{C}) = \mathbf{C} \cup \{\infty\}$ sending S_1 into itself; hence the algebraic curve X defined in $\mathbf{G}_{\mathrm{m}}^2$ by $y(1-\overline{\alpha}x) = x - \alpha$ meets S_1^2 in an infinite set, although for $\alpha \neq 0$ the curve is not a translate of an algebraic subgroup, and hence contains only finitely many torsion points. A similar fact holds if we take any finite ("Blaschke") product of such Möbius transformations [6]).

More generally, suppose that the curve $X \subset \mathbf{G}_{\mathrm{m}}^2$ meets S_1^2 in an infinite set Ω. Then, since complex conjugation $\overline{\cdot}$ acts as the map $[-1]$ on S_1^2 (here $[m]$ denotes multiplication by m in the relevant algebraic group), we must have $\overline{\Omega} \subset \overline{(X \cap S_1^2)} \subset \overline{X} \cap [-1]X$ and hence, given that X is an irreducible curve, we must have [7])

$$\overline{X} = [-1]X\,.$$

The above argument shows that for a polynomial graph this cannot happen unless X is a torsion coset, but on the other hand, this condition itself does not imply, for a general algebraic curve X, that X is a coset, not even assuming that Ω is infinite; this is shown as above, by the 'Möbius graphs', but much more general examples may be constructed, starting from polynomials $F(x,y)$ which are 'self-reciprocal', i.e. such that $\overline{F}(x,y) = \mu F(x^{-1}, y^{-1})$, for a suitable monomial μ. (Note that the above arguments work more generally under the mere assumption that X is *analytic* rather than *algebraic*. On the other hand, we shall point out — see the comments after Theorem 1 — that this weaker assumption is not sufficient for our conclusions below.)

EXAMPLE 1.1. We note that the said (necessary) condition $\overline{X} = [-1]X$ is not sufficient to ensure that $\Omega = X \cap S_1^2$ is infinite (or merely nonempty). Here is an example: X: $x^2y + xy^2 + 5xy + x + y = 0$. This is absolutely irreducible,

---

[6]) It will be seen in the last section that if the curve inside $\mathbf{G}_{\mathrm{m}}^2$ is only supposed to be analytic, then even the "strong" assumption that it contains infinitely many torsion points is not sufficient to imply Lang's conclusion.

[7]) Here $\overline{X}$ denotes the curve obtained by conjugating the coefficients of defining equations, a notation which shall be adopted throughout, for any algebraic variety; note that this operation indeed sends any algebraic variety in an algebraic one, whose complex points are the conjugates of the complex points of the original variety.

defined over $\mathbf{R}$ and invariant by $[-1]$. To find its points in S_1^2 set $x = e^{i\theta}$, $y = e^{i\phi}$ with real θ, ϕ. We obtain $2\cos\theta + 2\cos\phi + 5 = 0$, which has no solutions. (Or else: the quadratic equation $y^2 + (x + 5 + x^{-1})y + 1 = 0$ shows that y must be real for $x \in S_1$.)

The condition becomes sufficient for the infinitude of Ω under supplementary assumptions, such as e.g. that some nonconstant map $x^a y^b : X \to \mathbf{G}_m$, $a, b \in \mathbf{Z}$, has odd degree. (This is easy to see. We can reduce to the case when the said map is x. Then, for general $\xi \in S_1$, if $\{\eta_1, \ldots, \eta_d\}$ is the fiber in X above $x = \xi$, the fiber in $\overline{X}$ above $\overline{\xi} = \xi^{-1}$ is both $\{\overline{\eta_1}, \ldots, \overline{\eta_d}\}$ and $\{\eta_1^{-1}, \ldots, \eta_d^{-1}\}$, because $\overline{X} = [-1]X$. Hence the map $\eta \mapsto \overline{\eta^{-1}}$ induces a permutation of $\{\eta_1, \ldots, \eta_d\}$, and has clearly order 2. Then, if d is odd this permutation necessarily has a fixed point η, which means that $\eta \in S_1$. On varying ξ we get the claim.)

In view of these examples it may be not without interest to investigate, especially in connection with issues of Manin-Mumford type, what happens for other (connected) complex commutative algebraic groups G; namely, to study the intersections $\Omega = X \cap \Gamma$, where X is an algebraic subvariety of G and where $\Gamma = \Gamma_G$ is the *closure* in the complex topology of the set of torsion points of G.

The set Γ is significant also because it turns out to be always the *maximal compact subgroup* of G (as follows from Lie-group theory, see for instance the examples below, especially Section 3).

Let us display such notation, to be used throughout:

DEFINITION 1. For an algebraic group G as above, we shall use additive notation and denote by $\Gamma = \Gamma_G$ the closure of the set of torsion points of G (for the complex topology), or equivalently the maximal compact subgroup of G for the complex topology.

For an algebraic subvariety X of G, we put $\Omega = \Omega_X = \Omega_{X,G} := X \cap \Gamma$.

If $X = \gamma + H$ is a translate of the algebraic subgroup H of G by a point $\gamma \in G$, then either Ω is empty or γ may be taken in Γ, in which case Ω_X is easily described as $\Omega_X = \gamma + \Gamma_H$. Then we shall usually omit from our analysis such subvarieties, which we call '*special*'.

DEFINITION 2. For an irreducible algebraic subvariety X of G, we say that it is '*special*', or a '*coset*' if it is a translate of an algebraic subgroup of G.

As above, we shall concentrate here on the possible finiteness of Ω. (We note in passing that if Ω is infinite then it must contain an arc of a real-analytic curve, because Γ is compact and X, Γ are real-analytic.) Taking into account natural dimensional reasons, is sensible to expect finiteness only if the following inequality holds:

$$2\dim X + \dim_{\mathbf{R}} \Gamma \leq 2\dim G, \tag{1.1}$$

where $\dim_{\mathbf{R}}$ denotes dimension as a real manifold, and dim is the usual complex dimension. So, our basic question is (where we suppose that G is given):

QUESTION A. *Is it true that for any irreducible algebraic subvariety X of G, not a translate of an algebraic subgroup, but satisfying* (1.1), *the set $X \cap \Gamma$ is finite?*

In this article we shall focus on the case $\dim G = 2$, when the question is sensible only for X a curve in G. We have already seen that if $G = \mathbf{G}_{\mathrm{m}}^2$ the question has a negative answer, but that it may have a positive answer under simple supplementary assumptions on X (such as $\overline{X} \neq [-1]X$). In the next section we shall analyze the various possibilities for G, and answer the question. It will turn out that the restriction (1.1) really leaves us with a single significant case: an extension of an elliptic curve by the additive group. Our main result is then represented by the following

THEOREM 1. *If G is an extension of a complex elliptic curve by $\mathbf{G}_{\mathrm{a}}$, and if X is a non special algebraic curve in G, then G meets Γ only in a finite set.*

This result, which answers positively Question A for this class of groups G, may be rephrased with additional precision in the following way: *The intersection $X \cap \Gamma$ is finite unless G is a product $\mathbf{G}_{\mathrm{a}} \times E$ with an elliptic curve E and $X = \Gamma = \{0\} \times E$.*

We shall see in Section 3 that the non-product extensions G of this type are analytically isomorphic to $\mathbf{G}_{\mathrm{m}}^2$. However the result shows that for our question the behaviour is different from the case of $\mathbf{G}_{\mathrm{m}}^2$, so there is no 'analogue of Möbius transformations' for such extensions. Also, this isomorphism shows that the assumption that X is an analytic curve in G is no more sufficient for the conclusion. Actually, in the last section we shall show that there are transcendental analytic curves in G which contain infinitely many torsion points.

EXAMPLE 1.2 (An application to integration). An attractive motivation for considering the 'Manin-Mumford issue' for such group extensions comes from the classical problem of 'integration in finite terms' which was widely studied in the nineteenth century by Abel, Liouville, Chebyshev and others. We give just a simple example. Consider the elliptic differential $\omega = \frac{dt}{u}$, where $u^2 = p(t)$, and $p(t) \in \mathbf{C}[t]$ is a cubic polynomial with distinct roots; the integral of ω arises for instance in the calculation of the length of the lemniscate. The differential ω is regular on the elliptic curve E corresponding to the above equation and then a well-known criterion of Liouville [13] implies that $\int \omega$ cannot be expressed in 'finite terms' in a certain well-defined sense. Let us now slightly modify the differential by changing it into $\tilde{\omega}_a = \frac{\omega}{t-a}$, where $a \in \mathbf{C}$. This has a double zero at infinity on E and two poles at the two points $P_a, Q_a \in E$ where $t = a$. It may be checked that Liouville's criterion in this case easily implies that $\tilde{\omega}_a$ is integrable in finite terms if and only if for some non-zero integer m and a rational function g on E, we have $m\tilde{\omega}_a = \frac{dg}{g}$. In turn, this means that the divisor $m(P_a - Q_a)$ has class zero in the generalized Jacobian G in the sense of Sub-section 3.5; this G turns out to be a non-trivial extension of E by $\mathbf{G}_a$. Now, to conclude observe that, as a varies, the set of these divisors yields a (non-special) curve on G. And now Hindry's theorem or our Theorem 1 implies that $\tilde{\omega}_a$ is integrable in finite terms only for finitely many $a \in \mathbf{C}$.

Note that this conclusion sharpens the corresponding one in the 'Manin-Mumford spirit', which would predict finiteness merely for the set of torsion points in X. (For the groups G of the theorem, this last fact is proved in [6].)

As anticipated, our discussion will in fact go slightly beyond this result, in that we shall analyze all other cases when $\dim G = 2$. Of course when $\dim_{\mathbf{R}} \Gamma > 2$ the Question A concerns an empty set of curves; however it may still be of interest to study those for which Ω is infinite, and we shall do that in the final section, after the proof of Theorem 1 (see Theorem 7). It will turn out that in the other cases when the question makes sense, either we fall into the previously discussed case of $\mathbf{G}_{\mathrm{m}}^2$ or the answer follows trivially.

Of course it may be also of interest to know what happens in higher dimensions. Here at the moment we have no definite results or conjectures to suggest. In the final section we shall offer some other natural generalizations[8]).

[8]) It might be also asked what happens on considering the closure of the torsion in a p-adic setting, for instance over a field $\mathbf{C}_p$; however in this case there are no accumulation points for the torsion, so nothing new emerges.

The rest of the paper is organized as follows. In the next short Section 2 we shall recall the possible structures for commutative complex algebraic groups of dimension 2 and observe some trivial cases of the above Question A. In Section 3 we shall review the theory of extensions of an elliptic curve by the additive group, which are the very basis of Theorem 1. We shall take this opportunity to go beyond the mere preliminaries necessary for the subsequent proof of Theorem 1, and shall illustrate the general setting for such algebraic groups, both from the algebraic and the analytic viewpoint. We thought that this may be convenient for the reader, since it is seemingly not easy to locate a complete account in the existing literature. In this direction, we shall point out the references [16] and [15], and moreover we shall also reproduce in an appendix at the end a letter of Serre to the second author, explaining in particular how to obtain projective embeddings for the said algebraic group extensions. This letter was indeed discussed in a paper of Hindry [7] which did not reproduce the letter, but reported on its content in detail. We also recommend this paper of Hindry for a general discussion of commutative algebraic groups.

We shall rely on elementary facts of algebraic geometry and algebraic groups, for which we refer e.g. to [4].

ACKNOWLEDGEMENTS. It is a pleasure to express our thanks to Daniel Bertrand for his attention and for several important remarks and references; for other references we thank Michel Waldschmidt. We owe other interesting remarks to Anand Pillay and Angelo Vistoli. Also, we heartily thank Jean-Pierre Serre for his attention in suggesting further comments on a version of the paper and for his kind permission to reproduce below his letter to the second author.

The present work was partially supported by the ERC 2011 project "Diophantine problems".

2. COMMUTATIVE COMPLEX ALGEBRAIC GROUPS OF DIMENSION 2

In this short section we shall review the various possibilities for a commutative complex connected algebraic group G of dimension 2, and in the simplest cases we shall pause to see how the above Question A has an easy answer. This short discussion together with Theorem 1 will show that

Question A *has a positive answer for all commutative algebraic groups of dimension two, except for the group* $\mathbf{G}_{\mathrm{m}}^2$, *in which case the answer is negative.*

We shall often tacitly identify an algebraic group with the set of its complex points.

By a theorem of Barsotti, Rosenlicht and Chevalley (recalled as Thm. 11, Ch. III of [16], but see also [15] for references), we have that G contains a connected linear algebraic group R such that G/R is an abelian variety. In turn, linear commutative algebraic groups are known to be of the type $G = \mathbf{G}_{\mathrm{m}}^r \times \mathbf{G}_{\mathrm{a}}^s$, as is not too difficult to prove (see [4]).

REMARK 2.1. We recall that $\mathbf{G}_{\mathrm{m}}$ is the *multiplicative algebraic group*, defined as being $\mathbf{A}^1 - \{0\}$ as a variety, equipped with the multiplicative operation $(x, y) \mapsto xy$; powers of $\mathbf{G}_{\mathrm{m}}$ are often called *algebraic tori*. Also, $\mathbf{G}_{\mathrm{a}}$ is the *additive* algebraic group, defined as $\mathbf{A}^1$ as a variety, with the additive operation $(x, y) \mapsto x + y$. As to abelian varieties, for a rather self-contained vast introduction see e.g. [3]. Here we shall meet only abelian varieties of dimension 1, i.e. *elliptic curves*, for which we refer e.g. to [18].

So, (given that G is connected and commutative) we fall into the following cases:

1. *G is an abelian variety*. Note that now G is compact, analytically isomorphic to a complex torus $\mathbf{C}^2/\Lambda$, where Λ is a lattice of rank 4. Hence the torsion points are dense for the complex topology, so $\Gamma = G$ and the situation concerning the above question and theorem is of trivial type.

2. *G is a linear algebraic group*. As recalled above, any such commutative group is of the shape $\mathbf{G}_{\mathrm{m}}^r \times \mathbf{G}_{\mathrm{a}}^s$, where now $r + s = 2$. From our viewpoint, we have already seen the full picture when $r = 2$, whereas the situation is trivial when $s = 2$, since the only torsion point is then the origin. For $\mathbf{G}_{\mathrm{m}} \times \mathbf{G}_{\mathrm{a}}$ we also fall in a trivial case: now we have $\Gamma = S_1 \times \{0\}$ and if X is an irreducible curve in G, condition (1.1) is true and the intersection $X \cap (\mathbf{G}_{\mathrm{m}} \times \{0\})$ of curves is infinite if and only if $X = \mathbf{G}_{\mathrm{m}} \times \{0\}$. Hence this is the only case when $X \cap \Gamma$ is infinite; note that this X is an algebraic subgroup, hence special[9]), and so Question A has a positive answer.

We are left with the cases where neither R nor G/R are trivial, i.e.

---

[9]) It may be easily seen that the algebraic subgroups of dimension 1 are either $\mathbf{G}_{\mathrm{m}} \times \{0\}$ or products $\Phi \times \mathbf{G}_{\mathrm{a}}$, where Φ is a finite subgroup of $\mathbf{G}_{\mathrm{m}}$.

3. $\dim R = 1$, so $R = \mathbf{G}_m$ or $R = \mathbf{G}_a$, and we have an exact sequence of algebraic groups

$$0 \to R \to G \to E \to 0, \tag{2.1}$$

where E is an abelian variety, necessarily of dimension 1, so an elliptic curve.

One also says that G *is an extension of* E *by* R. Such extensions are studied and classified algebraically in [16] (see especially Ch. VII). Below we shall recall some of the corresponding results and also other ones from the analytic theory.

In turn, the simplest types now are the so-called *split* extensions, i.e. those for which the map $\pi\colon G \to E$ has a regular homomorphical section, i.e. a regular (algebraic) homomorphism $s\colon E \to G$ such that $\pi \circ s$ is the identity on E. If this is the case, of course $G \cong E \times R$ as an algebraic group.

Let us pause on this split case, which is very easy for our Question A.

If $R = \mathbf{G}_m$, we have $\Gamma = E \times S_1$, so $\dim_{\mathbf{R}} \Gamma = 3$ and the basic condition (1.1) is not verified and hence one would expect $X \cap \Gamma$ to be infinite. Still, one may ask for what non-special curves $X \subset G$ this actually happens. If X is non-special, then the second projection induces a regular map $X \to \mathbf{G}_m$ which is generically surjective (otherwise X would be of the shape $E \times \{c\}$). Hence the inverse image of S_1, which is Ω is infinite. (See Theorem 7 below for the non-split case.)

If $R = \mathbf{G}_a$, then $\Gamma = E \times \{0\}$ is an algebraic curve, actually a special one. Hence the intersection $X \cap \Gamma$ may be infinite only if $X = \Gamma$, so X is special. So, the answer to Question A is obviously positive in this case. Note that this is a first evidence for the validity of our Theorem 1.

The case when the extension is not split however seems not that obvious; our proof requires more involved analysis, and some known facts on Lie theory and the structure of such general group-extensions. So, before going ahead with the proof of Theorem 1 in general, we shall now review in brief a few of these facts; actually, for completeness we shall go beyond what is strictly necessary for our subsequent proofs.

3. Extensions of an elliptic curve by the additive group

3.1 Generalities

In this section we let E be a complex elliptic curve and G be an extension of E by $\mathbf{G}_a$, so G is a commutative complex connected algebraic group such

that there is an exact sequence of algebraic groups

$$0 \to \mathbf{G}_a \to G \to E \to 0\,, \tag{3.1}$$

where we shall denote by π the third map. Note that since E has genus 1 any copy of the rational curve $\mathbf{G}_a$ contained in G has to project to a constant in E, so this copy is contained in a fiber of π, which is itself a translate of $\mathbf{G}_a$. But any embedding $\mathbf{G}_a \to \mathbf{G}_a$ is an automorphism, so the said copy is a whole fiber. Hence there is a unique such copy containing the origin. This uniqueness also shows that E is uniquely determined by G up to isomorphism, as the quotient $G/\mathbf{G}_a$. (Of course the maps in the exact sequence are not uniquely determined by G and can be changed by composing with automorphisms of the corresponding groups.)

We shall suppose that E is given by a Weierstrass equation

$$E: \qquad \xi^2 = 4\eta^3 - g_2\eta - g_3\,, \tag{3.2}$$

with the point at infinity being the origin; we shall denote by the same letters ξ, η the corresponding functions in $\mathbf{C}(E)$.

We shall review some basic facts, referring mainly to [16]; other references for some analytic theory are [9], [20, p. 64] and [15]. We shall however in part give a different description. We shall try to keep the treatment (partly) self-contained, but of course we shall have occasionally to refer to certain fundamental results.

REMARK 3.1 (Commutativity). Throughout this paper we are considering only commutative algebraic groups. However we observe that the exact sequence (3.1) itself implies that G is commutative. In fact, conjugacy by $g \in G$ induces an automorphism $\phi_g\colon x \mapsto g^{-1}xg$ of G. Since $\mathbf{G}_a$ is normal in G, by restriction we obtain an automorphism of $\mathbf{G}_a$. The map $g \mapsto \phi_g|_{\mathbf{G}_a}$ is then a homomorphism of G to $\mathrm{Aut}(\mathbf{G}_a) = \mathbf{G}_m$ (the action of an element of $\mathbf{G}_m$ being through multiplication), and since $\mathbf{G}_a$ is commutative, this induces a homomorphism $G/\mathbf{G}_a = E \to \mathbf{G}_m$. However it is clear that there are no non-constant such homomorphisms (and even merely regular maps). So $g \mapsto \phi_g|_{\mathbf{G}_a}$ is constant, necessarily the identity of $\mathrm{Aut}(\mathbf{G}_a)$, proving that $\mathbf{G}_a$ is in the center of G. Take then an element $u \in G$ whose image in E is not torsion and note that the group generated by $u, \mathbf{G}_a$ in G is clearly commutative. But this is Zariski-dense in G (the Zariski closure projects generically surjectively to E), so G itself must be commutative, as wanted. (Given that $\mathbf{G}_a$ is central, another argument is as follows: for $g \in G$, the map $x \mapsto g^{-1}xgx^{-1}$, taking values in $\mathbf{G}_a$ because E is commutative, depends only

on x modulo $\mathbf{G}_a$ and thus induces a regular map from E to $\mathbf{G}_a$. This must be constant, so equal to the value at the identity, which is the identity. Or else, for $x \in G$, $\phi_g(x)$ equals x modulo $\mathbf{G}_a$, so we can write $\phi_g(x) = l_g(x)x$ with $l_g(x) \in \mathbf{G}_a$. Since $\mathbf{G}_a$ is central, the map $l_g\colon G \to \mathbf{G}_a$ is a homomorphism, and it is trivial on $\mathbf{G}_a$, so it is a homomorphism from E to $\mathbf{G}_a$, necessarily constant.)

We note in passing that already in dimension 2 there exist extensions of linear groups which are noncommutative; for instance, the group $\mathrm{Aut}(\mathbf{A}^1)$ of affine maps, i.e. those of the shape $t \mapsto at + b$, corresponds to an extension $0 \to \mathbf{G}_a \to \mathrm{Aut}(\mathbf{A}^1) \to \mathbf{G}_m \to 0$ (where the right map is $at + b \mapsto a$) which is a non-commutative semi-direct product.

We recall from [16, Prop. 6 of VII.6] that (in particular) the extension (3.1) has a rational section s, i.e. there is a rational map $s\colon E \to G$ such that if $\pi\colon G \to E$ is the homomorphism in (3.1), then $\pi \circ s : E \to E$ is the identity of E. Using the section s we can establish a birational isomorphism between G and $E \times \mathbf{G}_a$ by $g \mapsto (\pi(g), g - s(\pi(g)))$, with inverse $(x, t) \mapsto s(x) + t$.

REMARK 3.2 (Existence of rational sections). We sketch the existence proof in this case, which boils down to Hilbert Theorem 90: by taking a curve in G projecting generically surjectively to E, we see that there is certainly a 'multisection', i.e. a finite (ramified) cover $\theta\colon Z \to E$ of E and a rational map $s\colon Z \to G$ such that $\pi \circ s = \theta$; also, going to a Galois closure of $Z \to E$, we may suppose $Z \to E$ to be Galois with group Σ. For $\sigma \in \Sigma$ we have $\pi \circ s \circ \sigma = \theta \circ \sigma = \theta = \pi \circ s$, whence $\phi_\sigma := s \circ \sigma - s\colon Z \to G$ is a rational map taking values actually in $\mathbf{G}_a$, so it is a rational function on Z. Then $\sigma \mapsto \phi_\sigma$ is an (additive) 1-cocycle of Σ in $\mathbf{C}(Z)$, so by (the additive form of) Hilbert 90 there is a rational function $\xi\colon Z \to \mathbf{G}_a$ such that $\phi_\sigma = \xi \circ \sigma - \xi$. Then $\delta := s - \xi$ is a map from Z to G invariant by Σ; hence it induces a map $s^*\colon E \to G$, i.e. $\delta = s^* \circ \theta$. Also, $\pi \circ s^* \circ \theta = \pi \circ \delta = \pi \circ (s - \xi) = \pi \circ s = \theta$ (where the penultimate equality holds because ξ takes values in $\mathbf{G}_a$). So finally, since θ is generically surjective, $\pi \circ s^*$ must be the identity of E, as required.

3.2 PRINCIPAL FIBER SPACES

As explained in [16, VII.5] the section s allows us to view G as a *principal fiber space* with base E and structure group $\mathbf{G}_a$, i.e. a fiber bundle over E with fibers $\mathbf{G}_a$ and such that the transition functions are given by

translation-automorphisms[10]) of $\mathbf{G}_a$. Let us see how. The section s shall be regular on some (Zariski) open set $U \subset E$. We may cover E by (finitely many) translates $U_\alpha := U + \alpha$, and define regular section $s_\alpha : U_\alpha \to G$ as $s_\alpha(x+\alpha) := s(x) + s(\alpha)$: note that indeed this s_α is a section because $\pi \circ s_\alpha(x+\alpha) = \pi \circ s(x) + \pi \circ s(\alpha) = x + \alpha$. These sections make G a bundle since, through s_α, G is clearly isomorphic to $U_\alpha \times \mathbf{G}_a$ above U_α: if $g \in G$ is such that $\pi(g) = z \in U_\alpha$, then g corresponds to $z \times (g - s_\alpha(z))$ and $g - s_\alpha(z)$ lies in $\mathbf{G}_a$ because $\pi(g) = z = \pi(s_\alpha(z))$.

The transition functions are obtained as follows: if $g \in G$ and $z := \pi(g) \in U_\alpha \cap U_\beta$, then g corresponds to $z \times (g - s_\alpha(z))$ as an element above U_α and similarly to $z \times (g - s_\beta(z))$ as an element above U_β. The transition from the first fiber to the second one is done by translation by $s_\alpha(z) - s_\beta(z)$; this lies in $\mathbf{G}_a$ and equals $s(z-\alpha) + s(\alpha) - s(z-\beta) - s(\beta)$.

Hence we may associate to such a section also an element of $H^1(E, \mathbf{G}_a)$, which is by definition the group of isomorphism classes of fiber spaces as above. It may be easily checked that the class of a fiber space yields a *cocycle* of the open covering $E = \bigcup_\alpha U_\alpha$ with values in $\mathbf{G}_a$, i.e. a collection of regular maps $u_{\alpha\beta} : U_\alpha \cap U_\beta \to \mathbf{G}_a$ such that $u_{\alpha\beta} + u_{\beta\gamma} = u_{\alpha\gamma}$ on $U_\alpha \cap U_\beta \cap U_\gamma$. Two cocycles $(u_{\alpha\beta}), (u'_{\alpha\beta})$ give the same class if there are regular maps $v_\alpha : U_\alpha \to \mathbf{G}_a$ with $u_{\alpha\beta} - u'_{\alpha\beta} = v_\alpha - v_\beta$.

A cocycle corresponding to the section s is given precisely by the above transition function $s(z-\alpha) + s(\alpha) - s(z-\beta) - s(\beta)$ (the cocycle condition being trivially checked).

Of course the trivial class is the one of the space $E \times \mathbf{G}_a$; it corresponds to the zero element of $H^1(E, \mathbf{G}_a)$ and it occurs if and only if there exists some regular section. Given a rational section $s : E \to \mathbf{G}_a$, the above calculations show that we fall in the trivial class if and only if $s(z-\beta)+s(\beta)-s(z-\alpha)-s(\alpha) = v_\alpha(z) - v_\beta(z)$ for some regular functions to $\mathbf{G}_a$ as above and $z \in U_\alpha \cap U_\beta$. Indeed, this would say that $s(z-\alpha)+s(\alpha)+v_\alpha(z)$ does not depend on α such that $z \in U_\alpha$. Hence it defines a regular section from E to G.

In the case we are considering, this actually yields the same isomorphism also as *algebraic groups*; in fact, given a regular section $s : E \to G$, for each $\alpha \in E$ the regular map $s(x+\alpha) - s(x) - s(\alpha) : E \to G$ would take values in $\mathbf{G}_a$. But then it would have to be a constant, say $c = c_\alpha \in \mathbf{G}_a$. But

[10]) We note that such a notion is different from the one of *vector bundle*: for this last structure it is assumed to have a regular section and that the transition functions are given by multiplications (rather than additive translations). Also, we shall note in a moment that for a principal fiber space the existence of a regular section itself implies that the structure is the trivial one.

then, setting $s^* := s + c$ we have $s^*(x + \alpha) = s^*(x) + s^*(\alpha)$, so s^* defines a section which is a homomorphism, proving the claim. (Another argument comes from [3, Cor. 8.2.9]. See also [16, VII.15, Theorem 5].)

One can reverse the construction and, starting from a cocycle, obtain a fiber space. In the present case all cocycles lead to an algebraic group structure; see [16, VII.17, Theorem 7]. In that book it is also proved in particular that the present group of cocycle-classes is isomorphic to $\mathbf{C}$, which leads to an essentially unique algebraic group structure apart from the product one. Here we shall present part of this by following a somewhat different path, less general but more explicit for the case in question here.

From the topological or even differentiable viewpoint, it may be seen that any principal fiber space with respect to $\mathbf{G}_a$ is trivial. This can be proved by showing, via partitions of unity, that every cocycle with values in $\mathbf{G}_a$ is a coboundary. We recall the argument. Let $(U_\alpha)_\alpha$ be an open covering of E and choose a partition of unity $(\rho_\alpha)_\alpha$ related to it. Let now $(\varphi_{\alpha,\beta})_{\alpha\beta}$ be a differentiable 1-cocycle, so $\varphi_{\alpha,\beta}\colon U_\alpha \cap U_\beta \to \mathbf{C}$ are C^∞ functions satisfying $\varphi_{\alpha,\beta} + \varphi_{\beta,\gamma} = \varphi_{\alpha,\gamma}$ in $U_\alpha \cap U_\beta \cap U_\gamma$. For each index α, the function $\varphi_\alpha := \sum_{\beta\neq\alpha} \rho_\beta \varphi_{\alpha,\beta}$ can be continued to a smooth function on U_α. Now, it is easily checked that $\varphi_\alpha - \varphi_\beta = \varphi_{\alpha,\beta}$, proving that the 1-cocycle is indeed a coboundary.

The triviality of principal fiber spaces on E with structure group $\mathbf{G}_a$ is also a consequence of the universal covering provided by the exponential map, as explained in the sequel.

3.3 Factor systems

Suppose that G is given and let $s\colon E \to G$ be a rational section (delivered by Remark 3.2). Let us consider the rational map $f\colon E \times E \to G$ given by $f(x,y) = s(x+y) - s(x) - s(y)$. We have $\pi \circ f = 0$, so f takes values in $\mathbf{G}_a$ (as embedded in G). It is clearly symmetric and it satisfies the familiar (cocycle) identity

$$f(y,z) - f(x+y,z) + f(x,y+z) - f(x,y) = 0\,, \qquad x,y,z \in E\,. \tag{3.3}$$

Such functions are called *(symmetric) factor systems* and they arise also in abstract group theory, to classify group extensions. Observe that they form a vector space over $\mathbf{C}$ containing the constant functions and more generally those of the shape $g(x+y) - g(x) - g(y)$ (as in Remark 3.4 below). Recalling the birational isomorphism between $E \times \mathbf{G}_a$ and G given by $(x,t) \mapsto s(x) + t$,

we may then express the group law on $E \times \mathbf{G}_a$ by

$$(x,a) * (y,b) := (x+y, a+b+f(x,y)) . \tag{3.4}$$

Reversing the arguments, we note (as in [16, VII.4]) that given such a map f on $E \times E$ we can define a *rational* composition law on $E \times \mathbf{G}_a$ by (3.4). The identity (3.3) shows that this defines an associative law, which is also commutative since f is symmetric. But of course this law is not defined for all x, y since f is merely a rational map[11]). Concerning this issue, let us pause for a remark which will be useful.

REMARK 3.3 (Domain of definition of a factor system). Let D be an effective (reduced) divisor on $E \times E$ with support at the poles of f. We may write $D = D_0 + E \times H + V \times E$ where H, V are finite subsets of E and D_0 does not contain horizontal or vertical components. By symmetry we have $H = V$. The identity (3.3) helps to determine the structure of D. In fact, suppose that $(x,y) \in D_0$ but that $x, y \notin V$. Then on choosing z suitably in E we deduce that $x + y \in V$. This shows that $D_0 = \{(x,y) : x + y \in V\}$.

The identity (3.3) actually shows more; namely, for each $v \in V$ there is a rational function g_v on E such that the pole divisor of $f(x,y) - g_v(x+y)$ does not have the 'line' $x + y = v$ on $E \times E$ as a component, and such that the pole divisor of $f(x,y) + g_v(x)$ does not have $y = v$ as a component. (In view of (3.3), it suffices to take $g_v(x) := -f(x, z_0)$ for a sufficiently 'general' $z_0 \in E$.) Then, by the symmetry of f, this implies that $f(x,y) - g_v(x+y) + g_v(x) + g_v(y)$ is regular on an open dense subset of the support of $\{x+y=v\} + \{x=v\} + \{y=v\}$ in $E \times E$, i.e. no component of this divisor is a pole.

CONSTRUCTING AN ALGEBRAIC GROUP FROM A FACTOR SYSTEM. Even if a factor system does not define a group law on the whole $E \times \mathbf{G}_a$, it is a general result of Weil that this is sufficient to define an algebraic group G, birationally isomorphic to $E \times \mathbf{G}_a$ as a variety, whose composition law is expressed by (3.4) on an open subset of $G \times G$. Even if we shall give more explicit constructions later, we think it is worthwhile to see, very briefly, how this can be done in our case.

The factor system defines a principal fiber space (as above) and a group structure as follows. Let $U := E - V$ where V is as in the last remark. Then f is defined at all pairs (x,y) such that none among $x, y, x+y$ lies in V.

---

[11]) Actually, if f were regular, it would be constant and G would be isomorphic to $E \times \mathbf{G}_a$ as an algebraic group.

We define G to be $U \times \mathbf{G}_a$ above U (as a fiber space, not as a group!), and for $x, y, x+y \in U$ we define the group law[12]) as in (3.4). Now, we cover E with translates $U_\alpha := U + \alpha$ of U, chosen so that no sum or difference of two α's (including $\alpha = 0$) is in V; we define transition functions $u_{\alpha\beta}\colon U_\alpha \cap U_\beta \to \mathbf{G}_a$ by $u_{\alpha\beta} = f(x-\alpha, \alpha-\beta) - f(\beta, \alpha-\beta)$. The identity (3.3) shows this is indeed a cocycle.

We define the group law for $x, y, x+y \in U_\alpha$ by[13]) $(x,a)_\alpha * (y,b)_\alpha = (x+y, a+b+f_\alpha(x,y))_\alpha$ where $f_\alpha(x,y) := f(x-\alpha, y) + f(y-\alpha, \alpha)$. Using (3.3) once more, one can check that these charts and group laws are compatible and then they define an algebraic group structure on the principal fiber space G obtained from the charts $U_\alpha \times \mathbf{G}_a$. Such a G is merely an 'abstract variety', i.e. obtained by gluing affine charts, however it may also be seen that it may be embedded in projective space. This shall implicitly follow from the sequel.

REMARK 3.4 (Coboundaries). For a rational function g on E we can modify a given factor system $f(x,y)$ by subtracting the 'coboundary' $(\delta g)(x,y) := g(x+y) - g(x) - g(y)$, i.e. changing it into $f(x,y) - g(x+y) + g(x) + g(y)$. Such a coboundary defines itself a factor system, called trivial. The classes of factor systems modulo trivial ones form a group, denoted $H^2(E, \mathbf{G}_a)_s$ (see [16, VII.4]).

If G is given and the factor system originates from a section $s\colon E \to G$, this would correspond to changing the section $s(x)$ to $s(x) - g(x)$, on viewing the values $g(x)$ as elements of $\mathbf{G}_a \subset G$. Conversely, if the group G is instead constructed out from the factor system (as we have just illustrated), then addition of a coboundary yields an isomorphic group extension[14]). (A special case, already mentioned above, is to add a constant to f.) In particular, a trivial factor system defines the product group extension $E \times \mathbf{G}_a$.

CLASSIFICATION OF FACTOR SYSTEMS. We want to describe explicitly the factor systems $f\colon E \times E \to \mathbf{G}_a$, actually their classes modulo coboundaries, in a different way compared to [16]. We shall denote by $[f]$ the class of f.

---

[12]) Suppose for simplicity that $f(x,0)$ is regular, whence constant by (3.3). Then, on choosing the section $x \mapsto (x,0)$, and adding a constant to $f(x,y)$, we find back the factor system f as $(0, f(x,y)) = s(x+y) - s(x) - s(y)$, similarly to the opening construction of it.

[13]) Here $(\cdot,\cdot)_\alpha$ refers to the 'chart' $U_\alpha \times \mathbf{G}_a$.

[14]) There is an obvious natural notion of isomorphism between two group extensions as in (3.1), say with the same E but possibly different algebraic groups G, G'; this results in a notion which strictly implies the isomorphism of G, G', but is not equivalent with this. We shall not dwell further in this paper on this precision.

Let f be a factor system. We have seen in Remark 3.3 that for each v in the finite set $V = V_f \subset E$ there is a rational function $g_v \in \mathbf{C}(E)$ on E such that $f(x,y) - g_v(x+y) + g_v(x) + g_v(y)$ is regular on an open dense subset of the (support of the) divisor $\Delta_v := \{x+y=v\} + \{x=v\} + \{y=v\}$. Also, f is regular outside the support of $\sum_{v\in V} \Delta_v$. Without loss of generality we may include in V the origin $0 \in E$.

Let m_v be the order of pole of g_v at v. By the Riemann-Roch Theorem for E (see e.g. [18] or [5]) the vector space $\mathcal{R}$ of rational functions $\psi \in \mathbf{C}(E)$, regular outside V and such that $\mathrm{ord}_v \psi \geq -m_v$ for all $v \in V$ has dimension $\sum_{v\in V} m_v$.

To a $\psi \in \mathcal{R}$ we associate the polar parts of the Laurent expansion of ψ at v, for all[15]) $v \in V$. In this way we obtain a linear map from $\mathcal{R}$ to a vector space of dimension $\sum_{v\in V} m_v$. The kernel of this map clearly consists only of the constant functions and thus the image has dimension $(\sum_{v\in V} m_v) - 1$. Since there are no functions on E with a simple pole at 0 and no other pole, we deduce that each possible polar part is represented by a $\psi \in \mathcal{R}$ plus a multiple of a simple polar part at 0; we can represent this polar part as α/t where $\alpha \in \mathbf{C}$ and $t \in \mathbf{C}(E)$ is a given local parameter at 0.

In particular, we may choose a function $\psi \in \mathcal{R}$ such that $\psi - g_v$ is regular at each $v \in V - \{0\}$ and of the shape ω/t for $v = 0$, where $\omega = \omega_f \in \mathbf{C}$. We associate to the class of the factor system f the number $\omega_f \in \mathbf{C}$. Note that this number indeed depends only on the class of f: if we change $f(x,y)$ with $f(x,y) - g(x+y) + g(x) + g(y)$ then g_v is changed into $g + g_v$ and ψ into $\psi + g$. So $\psi - g_0$ is unchanged and the same holds for ω. Also, the map $f \mapsto \omega_f$ is clearly linear.

Note that if we have two factor systems f_1, f_2 then we may form a nontrivial linear combination $h := \alpha f + \beta g$, $\alpha, \beta \in \mathbf{C}$ not both 0, so that $\omega_h = 0$. Then by definition there exists a function ψ on E such that $h(x,y) - \psi(x+y) + \psi(x) + \psi(y)$ is regular on $E \times E$. But this means that it is constant, and changing ψ by a constant we may assume it is 0. Hence $[h] = 0$.

So, we have that $[f] \mapsto \omega_f$ is a well-defined injective linear map; thus the vector space of classes of factor systems has dimension at most 1.

We now show[16]) that it has dimension 1 by exhibiting an explicit non-trivial factor system. We refer to the Weierstrass equation (3.2) and set, for

---

[15]) Of course we are repeating here the well-known arguments of 'Principal parts' or so-called 'Mittag-Leffler' distributions, in the special case of elliptic curves. See [5], 2.18.

[16]) This is implicitly deduced in a somewhat different way in [16].

independent generic points $x = (u_1, u_2),\ y = (v_1, v_2) \in E$,

$$f(x,y) := \frac{\xi(y) - \xi(x)}{\eta(y) - \eta(x)} = \frac{v_2 - v_1}{u_2 - u_1}\,. \tag{3.5}$$

Note that this f is defined at all points $(x,y) \in E \times E$ such that $x, y, x+y \neq 0$, so out of Δ_0 in the previous notation. Given (3.3), this also shows that this is not in the trivial class, for otherwise 0 would be the unique simple pole of a function on E. We can directly verify (3.3) but it is much simpler to argue indirectly. Suppose we fix $y = y_0, z = z_0$ in (3.3), so as to obtain functions of $x \in E$. For y_0, z_0 sufficiently general, only the terms $f(x, y_0 + z_0)$ and $-f(x, y_0)$ may have a pole at $x = 0$. For $u_0 \neq 0$, the expansion at 0 of $f(x, u_0)$ is given by $t^{-1}(1 + O(t^2))$ where $t = \eta/\xi$ is a local parameter at 0. This immediately shows that $f(x, y_0+z_0) - f(x, y_0)$ is regular and vanishing at 0. Then the function $f(x, y_0+z_0) - f(x, y_0) + f(y_0, z_0) - f(x+y_0, z_0)$ is regular outside $-y_0, -y_0 - z_0$, and vanishes both at $x = 0$ and at $x = z_0$. Since the poles are at most simple, and since $0 + z_0 + y_0 + (y_0 + z_0) \neq 0$ for general y_0, z_0, it must vanish identically on E. Since this holds for (y_0, z_0) in a dense open set in $E \times E$, (3.3) is proved.

REMARK 3.5. Formula (3.5) may seem to come from good luck. However, there are good *a priori* motivations for it: on the one hand, it is the simplest choice of function on $E \times E$ with pole divisor a linear combination of divisors of type Δ_v ; on the other hand, we shall soon see that it comes from complex analysis, as a constant multiple of $\zeta(z_1 + z_2) - \zeta(z_1) - \zeta(z_2)$ where ζ is the *Weierstrass zeta function*.

We conclude this discussion by reading these conclusions on factor systems in terms of the group law (3.4). If the class of f is 0, then G is isomorphic to $E \times \mathbf{G}_a$ as an algebraic group. Conversely, this group-structure yields a factor system in the trivial class. Suppose now that G_1, G_2 are two extensions (3.1) such that the corresponding factor systems f_1, f_2 have both nontrivial class. Then we have $[f_2] = c[f_1]$ for some $c \in \mathbf{C}^*$, and we may thus assume that $f_2 = cf_1$. We contend that $G_1 \cong G_2$ as algebraic groups. For this it suffices to show that there is a birational isomorphism $\phi\colon G_1 \to G_2$ which is a group-homomorphism. (In fact, one then sees by translation that ϕ is everywhere defined, and is therefore a group-isomorphism.) For this, we use that G_1, G_2 are both birationally isomorphic to $E \times \mathbf{G}_a$, with law expressed by (3.4). We define $\phi(x,t) := (x, ct)$. We check $\phi((x,a) *_1 (y,b)) = \phi(x+y, a+b+f_1(x,y)) = (x+y, ca+cb+cf_1(x,y)) = (x+y, ca+cb+f_2(x,y)) = \phi(x,a) *_2 \phi(x,b)$, where $*_i$ denotes (3.4) read in G_i. This proves the claim.

We can summarize some of the previous considerations in the following

PROPOSITION 2. *The group of classes of factor systems is a* $\mathbf{C}$*-vector space of dimension* 1. *The trivial class corresponds to the product (i.e. split) group structure* $E \times \mathbf{G}_a$. *Any other two classes give rise to isomorphic algebraic groups, which are not isomorphic to* $E \times \mathbf{G}_a$.

REMARK 3.6 (Complete curves in G). Since we are dealing here with algebraic curves $X \subset G$, it may be worthwhile to pause and note that such an X can be complete only if G is split. In fact, if X is complete the projection $\pi|_X : X \to E$ is either constant or surjective; the first case yields that X is a translate of $\mathbf{G}_a$, which is impossible. In the second case, for a point $x \in E$, consider the sum $\sigma(x) := \sum_{z \in X, \pi(z)=x} z \in G$ (where distinct z projecting to the same x are counted with multiplicity). If $\deg \pi|_X = d$, we have $\pi(\sigma(x)) = dx$, so in particular σ is nonconstant. By [3, Cor. 8.2.9] the map $x \mapsto \sigma(x) - \sigma(0)$ of E in G is necessarily a homomorphism. So we obtain a homomorphism $\psi : E \times \mathbf{G}_a \to G$ such that $\psi(x, y) = \sigma(x) - \sigma(0) + y$. We have that $\pi \circ \psi$ is surjective, so ψ is also surjective. (If $z \in G$ take $u \in E \times \mathbf{G}_a$ with $\pi(\psi(u)) = \pi(z)$; then $\psi(u) = z + v$ with $v \in \mathbf{G}_a$ and $\psi(u - v) = z$.) But then G is the quotient of $E \times \mathbf{G}_a$ by $\ker \psi$, which is finite (its order is the degree of ψ). On the other hand, this kernel is identified with a finite subgroup F of E, since $\mathbf{G}_a$ has no torsion, and $G \cong (E/F) \times \mathbf{G}_a$ is split, as asserted. (Another argument consists in using the fact, observed later in Remark 3.10, that a nonsplit G is analytically isomorphic to $\mathbf{G}_m^2$, hence cannot contain compact Riemann surfaces.)

REMARK 3.7 (Regular functions on G). We also note that another way to distinguish between split and nonsplit case comes from regular functions. Of course $E \times \mathbf{G}_a$ admits nonconstant regular functions. On the other hand, every regular function on a nonsplit G is constant; for this we offer the following argument suggested by A. Vistoli: any such function f, restricted to a fiber of π would have a leading term at infinity of the shape at^n, where t is a coordinate on the fiber. Note that since locally G is a product and since transition functions are given by translations, we may define a, n so that they only depend on the fiber. Now pick a fiber with maximal n; then the coefficient a of t^n is again well-defined and it becomes a function on E with no poles (a priori with zeros); but it is then (a nonzero) constant. Let now $X = f^{-1}(0)$. This is a curve on G which is complete, because it intersects each fiber n times (counting multiplicities). Then the previous remark applies.

REMARK 3.8 (Uniqueness of the group law on G). We prove that given an algebraic group $(G,+)$, a homomorphism $\pi\colon G \to E$ to an elliptic curve E with kernel isomorphic to $\mathbf{G}_a$, and given another algebraic group law $(G,*)$ with the same origin, this in fact coincides with the previous one.

First we observe that π is a homomorphism with respect to $*$ too. Indeed, $t \mapsto \pi(x*t)$ is a constant map for $t \in \mathbf{G}_a$, since it sends $\mathbf{G}_a$ to E. Hence $\pi(x*t) = \pi(x)$ for all $t \in \mathbf{G}_a$. Since a regular map $\mathbf{G}_a \to \mathbf{G}_a$ is either surjective or constant, we also deduce that $\pi(y) = \pi(x)$ if and only if $y = x*t$ for some $t \in \mathbf{G}_a$. Let u and v be in E and $x \in \pi^{-1}(u), y \in \pi^{-1}(v)$, then it follows that $\psi\colon (u,v) \mapsto \pi(x*y)$ is a well-defined regular map $E^2 \to E$. For fixed u the map $\psi_u\colon v \mapsto \psi(u,v) - \psi(u,0)$ must be an endomorphism of E. Its kernel is by definition the set of v such that $\pi(x*y) = \pi(x)$, whence by the above is reduced to 0. So $\psi_u \in \mathrm{Aut}(E)$, and we have an algebraic map $u \mapsto \psi_u$, which must be constant, so $\pi(x*y) = \pi(x) + \pi(y)$.

Pick a point $p \in G$ and let us define $\phi_p\colon x \mapsto (x*p) - p$. We have $\phi_p(0) = 0$ and $\pi \circ \phi = \pi$. So ϕ preserves the fibers of π, which yields that $\phi_p(x) - x$ is a regular map from G to $\mathbf{G}_a$.

If we are in the non-split case, by what we have seen in the previous remark we must have that $\phi_p(x) - x$ is constant; since it vanishes at 0, we have $\phi_p(x) = x$ for all x, hence $x*p = x+p$ as wanted.

If G is split, similar arguments show that $x*p - x - p$ depends only on the $\mathbf{G}_a$ component of x and p and we are reduced to the fact that the only group law on $\mathbf{G}_a$ is the usual one (which is easy to establish).

3.4 PROJECTIVE EMBEDDING

To obtain a projective embedding of an extension of type (3.1), not isomorphic to a product, one can follow for instance a procedure outlined in a letter of Serre to the second author; this letter is reproduced below in the Appendix, after kind permission of the author, but we briefly describe also here some of the principles. (See also the paper [7] by Hindry for a very careful and detailed discussion of Serre's letter.)

One first compactifies the fiber space corresponding to G; as explained also in [15], if G is defined by charts $E_\alpha \times \mathbf{G}_a$ (E_α open subsets of E) one can add to $\mathbf{G}_a$ a point at infinity, obtaining a $\mathbf{P}_1$, and then define a new fiber space, denoted $\overline{G}$, with charts $E_\alpha \times \mathbf{P}_1$ and transition functions as before [17]).

[17]) See [1, Ch. 3] for a description of $\overline{G}$ in terms of the theory of minimal models of surfaces. It appears as $\mathbf{P}(\mathcal{F})$, where $\mathcal{F}$ is a rank 2 vector bundle on E, with an exact sequence $0 \to \mathcal{O}_E \to \mathcal{F} \to \mathcal{O}_E \to 0$, which splits if and only if this holds for G.

Once we have a compactification, it suffices to find a very ample divisor of the surface so obtained. One may check that, if F is a fiber of π and G_∞ is the divisor obtained by gluing the $E_\alpha \times \infty$, the divisor $D := 3F + G_\infty$ is very ample. This may be done e.g. by working on the charts. More explicitly, as remarked below, it turns out that removing from G a fiber F, above a point $P \in E$, one obtains a trivial fiber space, i.e. $G - F$ is isomorphic (as an algebraic variety) to $(E - P) \times \mathbf{G}_a$. This already shows that $\overline{G} - (G_\infty \cup F)$ is affine, so $F + G_\infty$ is big, and so also ample since the self-intersections of its components are non-negative. But since $3P$ is well-known to be very ample on E and since any point is very ample on $\mathbf{P}_1$, we see that $3F + G_\infty$ is actually very ample, as asserted.

Actually, the said Serre's letter provides an explicit basis of functions in $L(D)$ and a corresponding embedding in $\mathbf{P}_5$ (the closure is the complement of a plane in a complete intersection of three quadrics).

Subsequently Masser projected down to $\mathbf{P}_4$; as in his article [9] we embed G as $V - L$ where V is the surface defined by

$$X_0X_2^2 = 4X_1^3 - g_2X_0^2X_1 - g_3X_0^3\,, \qquad X_0X_4 - X_2X_3 = 2X_1^2\,, \tag{3.6}$$

and where L is the line defined by $X_0 = X_1 = X_2 = 0$; so X_0, X_2 cannot be both 0 on G.

We identify $\mathbf{G}_a$ as the subset $X_2 \neq 0$ of $\mathbf{P}_1$ with coordinates X_2, X_4, and we embed this in G by $(X_2 : X_4) \mapsto (0 : 0 : X_2 : 0 : X_4)$. We send G to E by the obvious projection map, denoted π, on the first three coordinates (note this is well-defined because $L \cap G = \varnothing$).

This embedding may look surprising but note that a fiber $\pi^{-1}(x)$ is indeed an affine line, depending on x, given by the equation on the right (where $X_0, -X_2, 2X_1^2$ are viewed as the coefficients and X_3, X_4 the variables); this at least makes this G a bundle over E. Also, we shall soon point out how this embedding comes more naturally from analysis, with a group law related to addition formulae for the $\wp$ and ζ functions of Weierstrass.

A rational section $s\colon E \to G$ is given for instance by

$$s(X_0 : X_1 : X_2) = (X_0^2 : X_0X_1 : X_0X_2 : 0 : 2X_1^2)\,, \qquad \text{for} \quad X_0 \neq 0\,, \tag{3.7}$$

and another one is e.g. $(X_0^2 : X_0X_1 : X_0X_2 : -2X_1^2 : 0)$, defined[18]) on $X_2 \neq 0$.

[18]) We observe that such a section is regular except at a single point of E; in particular, this proves the above claim that (as observed in the letter of Serre reproduced below) G − fiber is isomorphic (as an algebraic variety) to $(E - \text{point}) \times \mathbf{G}_a$.

THE GROUP LAW. We have seen that the group law is unique, once the identity is fixed. Here we use the identity $(0:0:1)$ on E and $(0:0:1:0:0)$ on G.

To write down the group law, we start with the simple case of translation by a point $t \in \mathbf{G}_a$; this is necessarily given by

$$(X_0 : X_1 : X_2 : X_3 : X_4) + (0:0:1:0:t) := (X_0 : X_1 : X_2 : X_3 + tX_0 : X_4 + tX_2),$$

(which is an action of $\mathbf{G}_a$ which actually extends to $\mathbf{P}_4$). Note that indeed this action is an automorphism of each fiber, which characterizes it up to replacing t by a non-zero constant multiple. The constant must be 1, by taking the first point to be the identity of G.

The general case is more complicated. We begin by writing down what turns out to be a factor system relative to the section (3.7). Note that this section is regular outside $O \in E$. The factor system $\phi(x,y) := s(x+y) - s(x) - s(y)$ must be such that $\phi(x,y) - s(x+y)$ is regular for $x, y \neq O$. The advantage comes from the fact that we know how to add $\phi(x,y)$, which takes values in $\mathbf{G}_a$. Also, we have established that a priori $\phi(x,y) = c \cdot f(x,y) + \delta(x,y)$, where $f(x,y)$ is given by (3.5), c is a constant and δ is a coboundary. To proceed, note that the section may be also written as $s(X_0 : X_1 : X_2) = (X_0/X_2 : X_1/X_2 : 1 : 0 : 2X_1^2/X_0X_2)$; the entries are functions on the elliptic curve, which are regular at the origin, apart from the last one which has a simple pole. Then the argument used to classify factor systems shows that δ must be zero. On the other hand, $s(x+y) - cf(x,y)$ must be regular for $x, y \neq O$; this condition together with small calculations shows that $c = 1/2$. In particular, this extension is not split [19]).

For points $g := (\mu_0 : \ldots : \mu_4)$, $h := (\nu_0 : \ldots : \nu_4)$ of G we set $x = \pi(g), y = \pi(h) \in E$ and

$$\phi(x,y) := \frac{1}{2} \cdot \frac{\mu_2\nu_0 - \nu_2\mu_0}{\mu_1\nu_0 - \nu_1\mu_0} = \frac{\mu_1^2\nu_0^2 + \mu_1\nu_1\mu_0\nu_0 + \nu_1^2\mu_0^2 - (g_2/4)\mu_0^2\nu_0^2}{\mu_0\nu_0(\mu_2\nu_0 + \nu_2\mu_0)}, \tag{3.8}$$

where the formula on the right may be used when $\pi(g) = \pi(h) \neq O$, whereas, as in (3.5), we do not define this when some of $\pi(g), \pi(h), \pi(g) + \pi(h)$ is the origin of E.

---

[19]) Indeed this follows immediately from the last representation of s: if G were split, it would have a regular section, which would differ from s by a function on E, which would have at least two poles.

Now, let $g, h \in G$ be as above, and set $\rho := \frac{\mu_3}{\mu_0} + \frac{\nu_3}{\nu_0} - \phi(x,y)$, if $\phi(x,y)$ is defined. Then set $(\gamma_0 : \gamma_1 : \gamma_2) = \pi(g) + \pi(h) = x + y$ and [20])

$$g + h = (\gamma_0^2 : \gamma_0\gamma_1 : \gamma_0\gamma_2 : \gamma_0^2\rho : 2\gamma_1^2 + \gamma_0\gamma_2\rho)\,. \tag{3.9}$$

This is not defined when e.g. $\phi(x,y)$ is not defined. However it may be checked that the above formulae lead to a compatible definition on the whole $G \times G$; alternatively, and more naturally, one may use the analytic formulae to be written down in the next subsection.

REMARK 3.9 (Embeddings in $\mathbf{P}_3$). We have seen that a nonsplit extension of E by $\mathbf{G}_a$ may be embedded in $\mathbf{P}_4$, and the same holds for the split extension $E \times \mathbf{G}_a$: it suffices to compose the usual embeddings $E \to \mathbf{P}_2$, $\mathbf{G}_a \to \mathbf{P}_1$ with the Segre embedding $\mathbf{P}_2 \times \mathbf{P}_1 \to \mathbf{P}_5$, and then to project down to $\mathbf{P}_4$. Explicit formulae are for instance $(x_0 : x_1 : x_2) \times (1 : t) \mapsto (x_0 : x_1 : x_2 : x_1 t : x_2 t)$, where $x_0 x_2^2 = 4x_1^3 - g_2 x_0^2 x_1 - g_3 x_0^3$ is a Weierstrass equation for E.

The question arises whether any of these extensions of E by $\mathbf{G}_a$ may be embedded in $\mathbf{P}_3$. We note that the compactification denoted $\overline{G}$ above in this section cannot, because it is not simply connected (as follows e.g. from the analytic picture given below) whereas any smooth surface in $\mathbf{P}_3$ is known to be simply connected. However, for the extension itself the question seems more difficult and we do not know the answer, even for the split case. We limit ourselves to a few remarks on the failure of some attempts.

A first attempt could be to embed E as a plane curve in $\mathbf{P}_3$ and to consider the cone (in $\mathbf{P}_3$) over it, obtaining for instance the variety H defined in $\mathbf{P}_3$ (with homogeneous coordinates x_0, x_1, x_2, x_3) by $x_0 x_2^2 = 4x_1^3 - g_2 x_0^2 x_1 - g_3 x_0^3$. Removing from H the vertex $(0 : 0 : 0 : 1)$, we obtain a fiber space H' over E with fibers isomorphic, in the algebraic sense, to $\mathbf{G}_a$. However, while this is a vector bundle over E of rank 1, it is isomorphic neither to $E \times \mathbf{G}_a$ nor to a nonsplit extension. In fact, H' contains the complete curve E, so Remark 3.6 applies and shows that the second case is impossible. As to the first case, it is easy to see that there are no nonconstant regular functions on H' (H is a normal variety and then any nonconstant function must have poles along a whole divisor), which is not true for $E \times \mathbf{G}_a$.

A further attempt to embed $E \times \mathbf{G}_a$ into $\mathbf{P}_3$ consists in starting with a $\mathbf{G}_a$-action on $\mathbf{P}_3$, given by a 1-parameter matrix group in GL_4; taking a plane cubic curve in $\mathbf{P}_3$ on which no two points are in the same orbit, the

[20]) This formula is derived on using $s(x+y)$ and adding to it the point of $\mathbf{G}_a$ corresponding to $\phi(x,y)$.

image of this curve under the group will be in bijection with $E \times \mathbf{G}_a$. For instance, consider the 1-parameter group

$$\mathbf{G}_a \ni t \mapsto A^t := \begin{pmatrix} 1 & t & \frac{t(t+1)}{2} & \frac{t(t+1)(t+2)}{6} \\ 0 & 1 & t & \frac{t(t+1)}{2} \\ 0 & 0 & 1 & t \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

which fixes the point $(1:0:0:0)$ (and acts freely on its complement). Using coordinates $(x_0 : x_1 : x_2 : x_3)$ for $\mathbf{P}_3$, it leaves invariant the plane $x_3 = 0$ and the line $x_2 = x_3 = 0$, which contains the fixed point. Take now a plane curve E on the plane $x_2 = x_3$, meeting the invariant line at only one point Q, distinct from the fixed point. Then the map $E \times \mathbf{G}_a \ni (P, t) \to A^t(P)$ is an injective morphism. However, its differential will not be injective at the points of $\{Q\} \times \mathbf{G}_a$, so we obtain an injective regular map but not an embedding.

3.5 Generalized Jacobians

A further viewpoint on these group varieties comes from the theory of generalized Jacobians. This is treated in detail in [16], and here we only recall briefly the case of our interest.

One may define an equivalence relation $\approx$ on divisors of degree zero on E, with support disjoint from the origin, as follows: $D_1 \approx D_2$ if $D_1 - D_2 = (f)$ is principal, where the function f on E (which is regular at the origin O by assumption) has vanishing differential at the origin. This relation is well defined and of course more strict then the usual linear equivalence between divisors. We shall denote by $[D]$ the $\approx$-class of D.

The set of classes forms naturally a group, and it may be shown that it can be given a structure of algebraic group variety G; in the present case it is called the *generalized Jacobian* with respect to the modulus $2 \cdot O$ (see [16, Ch. V]). Note that this G is indeed an extension of E by $\mathbf{G}_a$: the map $\pi\colon G \to E$ simply associates to a divisor class $[D]$ (in the strict sense) the corresponding class in the usual sense, which defines a point $x = x_D$ of E (which is such that D is linearly equivalent to $[x] - [O]$). To describe the fiber over O, let us first choose a local parameter t at the origin of E. Let D be a divisor of degree zero, with $\pi([D]) = O$; this means that $D = (f)$ is principal, where f is defined up to a non-zero constant and is regular at O. Now, the value of $df/(fdt)$ is well defined at the origin, and provides an isomorphism $\pi^{-1}(O) \cong \mathbf{G}_a$.

It turns out that this is not a split extension; for a proof see Proposition 15, p. 188 of [16]; a simple argument being also as follows. For a given point

$x_0 \neq O$ on E, consider the map

$$\sigma\colon E \to G\,, \qquad \sigma(x) := [(x + x_0) - (x_0)]\,. \tag{3.10}$$

This is clearly a section; its factor system is given as follows: $\sigma(x+y) - \sigma(x) - \sigma(y) = [(x+y+x_0) - (x+x_0) - (y+y_0) + (x_0)]$. The divisor in brackets is indeed principal, equal to (F) for a rational function F of degree two on E, depending on x, y, x_0, which can be written down (it is the ratio of two linear functions in the Weierstrass coordinates). The factor system, as a function to $\mathbf{G}_a$, is simply the value of dF/Fdt at the origin. This value depends on x, y, x_0 and an easy local calculation proves that for fixed x_0, y, it has a simple pole at $x = -x_0$. As observed previously, this pole structure proves that this cannot be a trivial factor system.

It is not without interest to see how to identify these strict divisor classes with points of the variety explicitly given by (3.6). We again consider the above section (3.10). To "compute" it, it suffices to compute the difference $\delta(x) = \sigma(x) - s(x)$, where s is our previous section σ given by (3.7). Note that this difference indeed lies in $\mathbf{G}_a$ when σ and s are defined and therefore is represented by a rational function g on E. This rational function is regular except at the origin and $-x_0$. Now fix a point $y_0 \in E$ different from O and $-x_0$. Observe that $\delta(x + y_0) - \delta(x) - \delta(y_0)$ is the difference of the factor systems associated to σ and s, evaluated at the point (x, y_0). Directly from the definition, we see that the first factor system is regular at (O, y_0) and vanishes therein. Therefore, the expansions at O of $\delta(x)$ and $\phi(x, y_0)$ coincide up to the constant term. An analogous calculation ensures that δ has at most a simple pole at $-x_0$. This completely determines the rational function δ concluding the identification, because s is known.

3.6 Analytic theory

The complex points of the algebraic group G defined by (3.1) form a complex Lie group, and hence there is an analytic exponential map $\exp_G\colon T \to G$ from the tangent space $T \cong \mathbf{C}^2$ to G at the origin (see for instance [17]). In this commutative case this is especially useful because $\exp_G$ then turns out to be a surjective analytic homomorphism; let us see some important consequences of this.

This $\exp_G\colon T \to G$ is the universal covering map of G. The kernel $\Lambda := \ker \exp_G$ is discrete because $\exp_G$ is a local homeomorphism.

Let T' denote the tangent space to $\mathbf{G}_a \subset G$, so $T' \cong \mathbf{C}$ and $\exp_G|_{T'}$ sends T' onto $\mathbf{G}_a$. The quotient $T'/\Lambda \cap T' \cong \mathbf{G}_a = \mathbf{C}$ is simply connected; hence $\Lambda \cap T' = \{0\}$ and $\exp_G|_{T'}$ is an analytic isomorphism.

Now, the quotient $T'' := T/T' \cong \mathbf{C}$ is identified as the tangent space to $E = G/\mathbf{G}_a$ and the map $\pi \circ \exp_G : T \to E$ factors through T'', producing the exponential map $\exp_E : T'' \to E$. It is classical that the kernel of $\exp_E$ is a lattice (of rank 2) $\Lambda'' \subset T''$. Let $\widetilde{\Lambda} \subset T$ be a lattice of rank 2 such that $\widetilde{\Lambda} \bmod T' = \Lambda''$; then $\pi \circ \exp_G(\widetilde{\Lambda}) = \exp_E(\Lambda'') = 0$, whence $\exp_G$ sends $\widetilde{\Lambda}$ in $\mathbf{G}_a$. Thus, since $\exp_G(T') = \mathbf{G}_a$, we may modify a basis for $\widetilde{\Lambda}$ with vectors in T' to suppose that $\widetilde{\Lambda} \subset \Lambda$.

Now, note that $\Lambda \subset \widetilde{\Lambda} + T'$; however since $\Lambda \cap T' = \varnothing$ we have that actually $\Lambda = \widetilde{\Lambda}$ and Λ has rank 2. On counting real dimensions, we have $T = \mathbf{R}\Lambda \oplus T'$.

Note now that G as a real-analytic group is isomorphic to $\mathbf{R}^4/\Lambda$, thus a product $\mathbf{R}^2 \times (\mathbf{R}^2/\Lambda')$, for a lattice $\Lambda' \subset \mathbf{R}^2$ of rank two.

TORSION POINTS AND THE GROUP Γ. It is clear that the torsion points of G constitute precisely the set $\exp_G(\mathbf{Q}\Lambda)$. Hence the set Γ (defined above as the topological closure of the set of torsion points of G) is precisely $\Gamma = \exp(\mathbf{R}\Lambda)$. It is also clear that Γ is the maximal compact subgroup: in the first place it is compact; also, any element $\exp_G u \in G - \Gamma$ has $u = u_0 + u'$, with $u_0 \in \exp(\mathbf{R}\Lambda)$, $u' \in T'$. But the multiples of u' have no convergent subsequence unless $u' = 0$.

Coming back to the kernel Λ, there are now two possibilities:

CASE I: $\dim_{\mathbf{C}} \mathbf{C}\Lambda = 1$. Then $\mathbf{C}^2 = \mathbf{C}\Lambda \oplus T'$, so $\exp(\mathbf{C}\Lambda)$ is analytically isomorphic to an elliptic curve inside G, projecting isomorphically to E. But this image must be algebraic: in fact, it is an analytic compact, hence closed subset of some projective space, and we may apply Chow's theorem (see [10, Ch. IV]). These isomorphisms also hold in the group-theoretical sense, so we are in the product case $G \cong E \times \mathbf{G}_a$ and $\Gamma = E \times \{0\}$.

CASE II: $\dim_{\mathbf{C}} \mathbf{C}\Lambda = 2$. Now a $\mathbf{Z}$-basis for Λ is still linearly independent over $\mathbf{C}$. The image $\Gamma = \exp(\mathbf{R}\Lambda)$ is a real-analytic subset of G projecting isomorphically onto E. Note that Γ is not complex-analytic, e.g. because its tangent space $\mathbf{R}\Lambda$ is not a $\mathbf{C}$-vector subspace of T. In particular, Γ is not an algebraic variety[21]). It also follows that Γ is Zariski-dense in G (as for instance its Zariski closure is also a subgroup of G, or else, since the tangent space at 0 of the Zariski closure is a complex space containing $\mathbf{R}\Lambda$ and is therefore the whole T).

[21]) This also follows on noting that, since $\mathbf{R}\Lambda \cap T' = \{0\}$, Γ is a subgroup of G with $\Gamma \cap \mathbf{G}_a = \{0\}$; then Γ would be an elliptic curve in G; since it is isomorphic to E through π, G would be a direct product.

REMARK 3.10. Note that G, as a real-analytic group, is isomorphic to $\mathbf{R}^4/\Lambda$, thus to a product $\mathbf{R}^2 \times (\mathbf{R}^2/\Lambda')$, where Λ' is a lattice of rank 2.

In particular this implies that, even in Case II, G is isomorphic to $E \times \mathbf{G}_a$ as a *real*-analytic variety. This may also be directly seen from the description involving fiber spaces: as mentioned above, by partition of unity one can construct a real-analytic section $\theta\colon E \to G$ of the projection $G \to E$, so identifying G with $E \times \mathbf{G}_a$. Still alternatively, note that the restriction π_Γ of the projection $\pi\colon G \to E$ is a real Lie group isomorphism $\pi_\Gamma\colon \Gamma \to E$; its inverse $\theta\colon E \to \Gamma$ will be a section of π and a Lie group homomorphism.

Note also that in Case II, G is complex-analytically isomorphic to $\mathbf{G}_m^2$ under a group isomorphism. (In fact, $G \cong \mathbf{C}^2/\Lambda \cong (\mathbf{C}\lambda_1/\mathbf{Z}\lambda_1) \times (\mathbf{C}\lambda_2/\mathbf{Z}\lambda_2)$, where $\Lambda = \mathbf{Z}\lambda_1 + \mathbf{Z}\lambda_2$.) This is somewhat striking, taking into account that the conclusion of Theorem 1 does not hold for $\mathbf{G}_m^2$, as we have seen in the introduction. Also, this shows that the analytic structure is independent of the curve E, contrary to the algebraic structure.

This description also shows that any lattice Λ of rank two gives rise at least to one extension of an ellipltic curve by $\mathbf{G}_a$, the elliptic curve being determined only if $\mathbf{C}\Lambda$ has dimension one. So the situation is quite different to that of abelian varieties of dimension two.

We summarize some of these conclusions in the following statement, used in our later proofs.

PROPOSITION 3. *Let G be a non-product extension of E by $\mathbf{G}_a$ and let Γ be the topological closure of the torsion in G. Then Γ is a real-analytic surface in G of the shape $\exp_G(\mathbf{R}\Lambda)$, where Λ is a lattice of rank 2 with basis linearly independent over $\mathbf{C}$. In particular, Γ is neither analytic nor algebraic, but is Zariski-dense in G. In all cases Γ is the maximal compact subgroup of G.*

Let us now produce some formulae which make $\exp_G$ explicit. Referring to the embedding of G in $\mathbf{P}_4$ corresponding to (3.6), and letting z, w be complex coordinates in $T \cong \mathbf{C}^2$, we have

$$\exp_G(z,w) = (1 : \wp(z) : \wp'(z) : w + \zeta(z) : (w + \zeta(z))\wp'(z) + 2\wp(z)^2)\,. \tag{3.11}$$

Here $\wp(z)$ is the *Weierstrass elliptic function* associated to (3.2), so $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$ (see [8] or [18]). Of course $\wp(z)$ has double poles at the points in Λ'' and an expansion at the origin of the shape $\wp(z) = z^{-2} + O(z^2)$; this also yields $\wp'(z) = -2z^{-3} + O(z)$. The function $\zeta(z)$ is the '*Weierstrass*

zeta-function', defined so that $\zeta'(z) = -\wp(z)$ and $\zeta(z) = z^{-1} + O(z^3)$ at the origin. Of course the functions $\wp, \wp'$ are periodic under translations by Λ'', whereas ζ verifies the '*quasi-periodic*' condition

$$\zeta(z+\lambda) = \zeta(z) + \eta(\lambda)\,, \qquad \lambda \in \Lambda'', \tag{3.12}$$

where $\eta\colon \Lambda'' \to \mathbf{C}$ is $\mathbf{Z}$-linear.

Of course (3.11) is not defined as it stands for $z \in \Lambda''$; however we are using homogeneous coordinates, hence we may divide out all coordinates by $\wp'(z)$ when z is near to Λ''. For instance, if $z \approx 0$, the said expansions show that $\zeta(z)\wp'(z) + 2\wp(z)^2$ is regular near 0, hence for fixed w the right side of (3.11) becomes $(O(z^3) : O(z) : 1 : O(z^2) : w + O(z^3))$, which tends to the element $(0 : 0 : 1 : 0 : w)$ of $\mathbf{G}_a$ as $z \to 0$. (Similarly if $z \approx \lambda \in \Lambda''$, on replacing w by $w + \eta(\lambda)$ and $\zeta(z)$ with $\zeta(z) - \eta(\lambda)$.)

The functional equation (3.12) also shows that, setting $\Lambda = \{(\lambda, -\eta(\lambda)) \in \mathbf{C}^2 \,:\, \lambda \in \Lambda''\}$ we have indeed $\exp_G((z,w)+\omega)) = \exp_G(z,w)$ for $\omega \in \Lambda$ and the Λ so defined is indeed the kernel of $\exp_G$, as in the opening discussion. (A basis of Λ is linearly independent over $\mathbf{C}$, as we have deduced above, and as follows from the celebrated *Legendre relation* — see [8, p. 241].)

REMARK 3.11 (Periods). The lattice Λ may also be seen as generated by *periods*. For elliptic curves, this is done as usual, on taking a nonzero holomorphic 1-form μ and integrating $\int_Q^P \mu$, where Q is a fixed point on E and $P \in E$ varies. This yields a map $E \to \mathbf{C}$ which is well-defined only modulo the lattice spanned by the integrals $\int_{\gamma_i} \mu$, where γ_1, γ_2 are closed paths at Q generating the homology of E. The resulting map is inverse to $\exp_E$.

Things here are similar. Let us remove e.g. the origin O from E; we obtain a space whose fundamental group is the free group on two generators, so the 1-homology is again $\mathbf{Z}^2$. We can take the form μ and another form ν regular except at O (e.g. $\eta \cdot \mu$) and consider a map, this time to $\mathbf{C}^2$, $P \mapsto (\int_Q^P \mu, \int_Q^P \nu)$, for a path joining Q, P and not passing through O. Again this is well-defined up to the lattice generated by $(\int_{\gamma_i} \mu, \int_{\gamma_i} \nu)$, where γ_1, γ_2 generate the homology of $E - \{0\}$. This map is inverse to $\pi \circ \exp_G$. (See also [14, pp. 16–18].)

An analogue of the Abel-Jacobi theorem would show that this construction provides an equivalent description of the generalized Jacobian defined in the previous sub-section.

The group law may be derived from that of $\mathbf{C}^2$ on using the addition formulae for the $\wp$, $\wp'$ and ζ functions. The first ones come of course from

the *chord and tangent process* on (3.2); let us recall these formulae (see e.g. [8]):

$$\wp(z_1+z_2) = -\wp(z_1) - \wp(z_2) + \frac{1}{4}\left(\frac{\wp'(z_2)-\wp'(z_1)}{\wp(z_2)-\wp(z_1)}\right)^2, \tag{3.13}$$

$$\wp'(z_1+z_2) = \wp'(z_1) + \left(\frac{\wp'(z_2)-\wp'(z_1)}{\wp(z_2)-\wp(z_1)}\right)(\wp(z_1+z_2)-\wp(z_1)). \tag{3.14}$$

For the ζ function, the addition theorem seems to be less easy to locate in the literature. One can find it e.g. as Ex. 2, 20.53 of [21]. Here it is[22]):

$$\zeta(z_1+z_2) - \zeta(z_1) - \zeta(z_2) = \frac{1}{2}\left(\frac{\wp'(z_2)-\wp'(z_1)}{\wp(z_2)-\wp(z_1)}\right). \tag{3.15}$$

These formulae lead to the group law on G as previously illustrated. Through (3.11), the ζ function also leads to an analytic (non-algebraic) section $E \to G$, which may be used to derive the factor system written above. (This was anticipated in Remark 3.5; in fact, (3.5) corresponds to (3.15).)

4. Proof of Theorem 1

Let us suppose throughout that G is a non-product extension of E by $\mathbf{G}_a$ (the product case being trivial). We have developed above some properties of such extensions, for instance Proposition 3, which will be used below.

Remark 4.1 (Algebraic subgroups). We shall use the important remark that $\mathbf{G}_a$ *is the unique connected algebraic subgroup of* G *of dimension* 1 : in fact, if H were such a subgroup such that $\pi|_H$ is nonconstant, then $\pi(H)$ would be the whole E ; the kernel of $\pi|_H$ would be a finite subgroup of $\mathbf{G}_a$ and therefore $\{0\}$. Then $\pi\colon H \to E$ would be an isomorphism and it immediately follows that G would be a product. (See also Remark 3.6 above.) Therefore $\pi|_H$ is constant, necessarily 0, and we have the claim.

On the contrary, there are several *analytic* subgroups of G. As we already remarked, G is isomorphic as complex Lie group to the product $\mathbf{C}^* \times \mathbf{C}^*$, so in particular it contains the algebraic subgroups of $\mathbf{G}_m^2$ as one-dimensional analytic subgroups. (One may actually show that there are even other ones.)

---

[22]) Note that $\zeta(z)$ is not an algebraic function of $\wp(z)$, but $\zeta(z+u)-\zeta(z)$ is one, for each $u \in \mathbf{C}$.

REMARK 4.2 (Automorphisms). Since G is analytically isomorphic to $\mathbf{G}_{\mathrm{m}}^2$, the automorphisms of $\mathbf{G}$ as a complex Lie group form a discrete group isomorphic to $\mathrm{GL}_2(\mathbf{Z})$ (this can be viewed by considering their differentials, which are the linear automorphisms of the tangent space leaving the period lattice invariant). On the contrary, the group of algebraic automorphisms of G (as algebraic group) is finite. To see this, let $\Phi\colon G \to G$ be an algebraic automorphism. By uniqueness, the subgroup $\mathbf{G}_{\mathrm{a}}$ must be invariant, hence Φ acts on $E = G/\mathbf{G}_{\mathrm{a}}$. If E has no complex multiplication, then this action on E should be ± 1; then $1 \pm \Phi$ sends homomorphically $G \to \mathbf{G}_{\mathrm{a}}$, and since the only connected one-dimensional algebraic subgroup of G is $\mathbf{G}_{\mathrm{a}}$, such homomorphism must be the zero constant (otherwise the kernel would be $\mathbf{G}_{\mathrm{a}}$ and $E \cong \mathbf{G}_{\mathrm{a}}$). Hence $\Phi = \pm 1$. If E admits complex multiplication automorphisms, the above argument proves that any such automorphism of E is induced by at most one automorphism of G: if Φ_1, Φ_2 are such automorphisms, then $\Phi_1 \circ \Phi_2^{-1}$ would induce the identity on E, whence by the above would be the identity. This proves the finiteness claim.

Suppose finally that E has a CM automorphism θ (which must be a unit in an imaginary quadratic order, thus a root of unity of order dividing 4 or 6). Then there are two isomorphism classes for E, with Weierstrass equation with either $g_2 = 0$ or $g_3 = 0$, and the automorphisms can easily be written down explicitly as linear automorphisms of the variables. From the equation (3.6) it may be checked that there exists an algebraic automorphism Θ of G acting on $\mathbf{G}_{\mathrm{a}}$ by multiplication by θ^{-1} (if we read the action on the tangent space, the determinant must be ± 1).

In particular, the differential at the origin of any algebraic automorphism of G has determinant 1 (whereas the analytic ones may also have determinant -1).

As to the split group $E \times \mathbf{G}_{\mathrm{a}}$, this admits a one-dimensional algebraic group of automorphisms (as an algebraic group), whose connected component is $\mathbf{G}_{\mathrm{m}}$.

We start by proving a general fact, which shall repeatedly be useful below:

LEMMA 4. *Let X, Y be complex algebraic curves and let $f\colon X \to Y$ be an analytic map with finite fibers. Then f is a morphism of algebraic curves.*

Proof. By considering coordinate functions on Y, we can assume $Y = \mathbf{P}_1$. Let us embed X in some projective space, denoting by $\bar{X}$ its closure therein. By going to a normalization $\nu\colon \widetilde{X} \to \bar{X}$ (in some other projective embedding)

and composing with f to produce an analytic map from a dense open subset of $\widetilde{X}$ to $\mathbf{P}_1$, we may assume that $\overline{X}$ is smooth. It suffices to show that f extends to an analytic map $\overline{X} \to \mathbf{P}_1$: in fact, e.g. by Chow's theorem, such a map would automatically be algebraic[23]).

Now, by assumption f is defined outside a finite subset S of $\widetilde{X}$, and it suffices to show that it may be extended analytically to each point of S. Let $x_0 \in S$. There is a small neighborhood $U \subset \widetilde{X}$ of x_0, analytically isomorphic to an open disk Δ in $\mathbf{C}$ around the origin, through a local parameter $t\colon U \to \Delta$, so that $t(x_0) = 0$; and there is an analytic function $g\colon \Delta - \{0\} \to \mathbf{P}_1(\mathbf{C})$ such that $f(x) = g(t(x))$ for $x \in U - \{x_0\}$. We may write $g = (g_0 : g_1)$, where $g_0, g_1\colon \Delta - \{0\} \to \mathbf{C}$ are analytic functions. If g_0/g_1 does not have an essential singularity at 0, then it is either regular or has a pole; in either case, using $g = (1 : g_1/g_0) = (g_0/g_1 : 1)$ on $\Delta - \{0\}$, f may be extended as required. On the other hand, if g_0/g_1 has an essential singularity at 0, by the 'Big Picard Theorem' (see e.g. [19]) it assumes each value, with at most two exceptions, in each neighborhood of 0. However this contradicts the fact that f has finite fibers.

So f may indeed be extended to x_0 and repeating the argument for each point of S we obtain the sought conclusion. □

In the proof we have used the Big Picard Theorem; for our purposes, the present lemma could be replaced by a weaker one, relying only on the easier theorem of Weierstrass on the density of values of a function near an essential singularity. We omit the (easy) details.

To prove Theorem 1 we assume from now on that X is an irreducible closed algebraic curve in G such that $X \cap \Gamma$ is infinite. On translating X by a point in Γ, we may assume that the identity 0 of G lies in X. Note that $\pi|_X$ is generically surjective, because $\pi|_\Gamma$ is injective and so the image $\pi(X)$ contains infinitely many points of E. In particular, since $\mathbf{G}_a$ is the unique connected algebraic subgroup of G of dimension 1, X cannot be a translate of an algebraic subgroup.

We go ahead with the following reduction step, whose proof contains several elements used again in the sequel:

LEMMA 5. *Under the above assumptions, G is isomorphic (as an algebraic group) to the central element in an extension* (2.1) *where all the involved groups and maps are defined over* $\mathbf{R}$.

[23]) See [10, Ch. IV] for a proof of Chow's theorem. However for curves more elementary results suffice: see e.g. [14, Theorem 4].

Proof. Let G^* be the complex-conjugate group: its complex points are by definition the complex-conjugates of the points of G. Here we suppose that G is embedded in some projective space, in which case G^* is defined by equations conjugate to those defining G. (This may of course depend on the embedding.) This G^* turns out to be automatically an algebraic variety and actually an extension of E^* by $\mathbf{G}_a$, where E^* is similarly defined as being conjugate to E in an embedding corresponding to the relevant exact sequence. (And the maps in the two exact sequences are also related by conjugation in an obvious way.)

The conjugation map $\tau\colon G \to G^*$, $\tau(g) = \overline{g}$, is an isomorphism of real Lie groups. We consider its differential $\mathrm{d}\tau\colon T \to T^*$, where T^* is the tangent space to G^* at the origin[24]). We may similarly define X^*, Γ^* and their intersection is still infinite. Note that clearly, in the notation of the introduction, $(\Gamma_G)^* = \Gamma_{G^*} = \Gamma^*$.

We also have an exponential map $\exp^*\colon T^* \to G^*$ and, by general theory, $\mathrm{d}\tau$ is an isomorphism such that $\exp^* \circ \mathrm{d}\tau = \tau \circ \exp$, whence in particular $\mathrm{d}\tau$ sends isomorphically Λ to the kernel[25]) Λ^* of $\exp^*$.

We may now uniquely extend the linear map $\mathrm{d}\tau|_\Lambda$ (i.e. the restriction of $\mathrm{d}\tau$ to Λ) to a $\mathbf{C}$-linear map $\phi\colon T \to T^*$: this is because a $\mathbf{Z}$-basis of Λ (resp. Λ^*) is a $\mathbf{C}$-basis of T (resp. T^*). Note that $\phi(\Lambda) = \Lambda^*$. In turn, since ϕ is complex-linear, by general theory, this induces a complex-analytic isomorphism $\Phi\colon G \to G^*$, such that $\mathrm{d}\Phi = \phi$. (Note that this satisfies $\exp^* \circ \phi = \Phi \circ \exp$.)

Note that the restrictions of τ and Φ to Γ have the same differential (because the points of Γ expressed in a basis of Λ have real coordinates); since they are isomorphisms of connected Lie groups, they coincide on Γ: $\tau|_\Gamma = \Phi|_\Gamma$. (Of course $\tau \neq \Phi$ as isomorphisms on G: for instance only the second one is complex-analytic.)

We have $\Phi(X \cap \Gamma) = \tau(X \cap \Gamma) = X^* \cap \Gamma^*$. Hence $\Phi(X) \cap X^*$ contains an infinite set lying in the compact set Γ^*. However $\Phi(X)$ is a closed analytic curve in G^* (since Φ is an analytic isomorphism), and X^* is algebraic, and hence is closed analytic as well. Therefore, by analytic continuation we deduce that $\Phi(X) = X^*$. (For instance, it suffices to note that every analytic relation holding on $\Phi(X)$ must hold as well on X^* and conversely; in turn, this follows by analytic continuation, on restricting to X^* the functions expressing the relation.)

---

[24]) If G is embedded in some projective space and we view geometrically T as being likewise embedded, then the space T^* consists of the complex conjugates of the points in T. However, as for G, complex conjugation is not intrinsically defined on T.

[25]) This Λ^* of course consists of the vectors complex conjugates to those in Λ.

In particular, by Lemma 4, the *a priori* analytic map $\Phi_X := \Phi|_X$ must then be algebraic. We then want to show that this property extends to Φ.

Let $\sigma\colon G \times G \to G$ and $\sigma^*\colon G^* \times G^*$ be the addition maps. The map $\sigma|_{X\times X}\colon X \times X \to G$ is dominant (and hence $\sigma|_{X\times X}$ has generically finite nonempty fibers). In fact, otherwise its image $X+X$ would be contained and dense in a curve in G; the image is irreducible (like $X \times X$) so this curve would equal $X + 0 = X$. But then X would be closed under addition. Now, for $\xi \in X$, the curve $X+\xi$ is closed in G and contained in X, so equals X. All of this proves that X would be an algebraic subgroup, which has been shown impossible[26]).

Consider now the regular algebraic map $\sigma^* \circ (\Phi_X \times \Phi_X)\colon X \times X \to G^*$. This is constant on the fibers of $\sigma|_{X\times X}$, because Φ is a homomorphism. (In fact, if $x + x' = g$, then $\Phi_X(x) + \Phi_X(x') = \Phi(g)$ depends only on g.) Therefore, by a known fact this means that this map may be written as $\varphi \circ (\sigma|_{X\times X})$, for a suitable rational[27]) map $\varphi\colon G \to G^*$.

We have $\varphi(x + x') = \Phi_X(x) + \Phi_X(x') = \Phi(x + x')$. Hence φ coincides with Φ, which is therefore a rational map (not merely analytic). But then $\Phi\colon G \to G^*$ is an algebraic isomorphism: it is rational and, since it is a homomorphism, we see by translation that it is everywhere regular.

The image $\Phi(\mathbf{G}_a)$ is an algebraic subgroup of G^* of dimension 1, which is unique (as remarked above) and thus must be $\mathbf{G}_a$. Therefore Φ induces an isomorphism between $E = G/\mathbf{G}_a$ and $E^* = G^*/\mathbf{G}_a$.

Note now that the invariant $j(E^*)$ is the complex conjugate of the invariant $j_0 := j(E)$ of E, and therefore these invariants must be equal, i.e. they lie in $\mathbf{R}$. But it is easy to write down a Weierstrass equation of an elliptic curve E_0 with invariant j_0 and defined over $\mathbf{Q}(j_0)$ (see e.g. [8, p. 18]). This E_0 is isomorphic to E. But we have seen in Section 3 that we may construct a non-product extension G_0 of E_0 by $\mathbf{G}_a$, and this extension shall be defined over $\mathbf{R}$. Also, by Proposition 2, the algebraic group G_0 is determined uniquely by E_0 up to algebraic isomorphism. Hence G is isomorphic to G_0 as an algebraic group, as asserted[28]). □

---

[26]) We do not need here the assumption that X is non-special.

[27]) A way to see this is to observe that the assumption implies that the finite function-field extension $\mathbf{C}(X \times X)/\mathbf{C}(G^*)$ corresponding to the map must contain the finite extension $\mathbf{C}(X \times X)/\mathbf{C}(G)$ (induced by $\Phi_X \times \Phi_X$) as an intermediate extension: if not, some element of $\mathbf{C}(G^*)$ would have degree > 1 over $\mathbf{C}(G)$, and therefore the corresponding function could not be constant on the said fibers. See also e.g. [4, p. 43, first Proposition].

[28]) Note that we may conjugate Φ to obtain an isomorphism $\Phi^*\colon G^* \to G$, such that for $x \in G$, $\Phi^*(\tau(x)) = \tau(\Phi(x))$. Then $\Phi^* \circ \Phi\colon G \to G$ is an automorphism of G. Actually, if $x \in \Gamma$, we have that $\Phi(x) = \tau(x)$, so $\Phi^*(\Phi x) = x$. Then, since Γ is Zariski-dense in G, we have that $\Phi^* \circ \Phi$ is the identity. In particular, this allows us to use Weil's descent theory as an alternative

We can now complete the proof of Theorem 1, where by the last lemma we can and shall assume that all varieties and maps in (2.1) are defined over $\mathbf{R}$. We shall use arguments similar in part to the proof of such lemma. With reference to such proof, we note that now $G^* = G$, $T^* = T$, $\Gamma = \Gamma^*$ (but of course in general X shall not necessarily be equal to X^*).

The conjugation map τ of the proof of Lemma 5 sends G to itself and is an automorphism of G as a real Lie group. As before we obtain a $\mathbf{C}$-linear map $\phi\colon T \to T$ such that $\phi(\Lambda) = \Lambda$ and extending τ on $\mathbf{R}\Lambda$, so we obtain a complex-analytic automorphism $\Phi\colon G \to G$ whose differential at the origin is ϕ. Exactly as before, we may prove, using the curves X, X^*, that Φ is an algebraic automorphism[29]).

We go on by showing that both maps $\tau \pm 1$ have infinite kernel on Γ.

Observe that not all the torsion points of G can be defined over $\mathbf{R}$, for otherwise the same would be true of E (whereas they are dense in E for the complex topology). Therefore $\tau - 1$ is not identically zero on Γ.

On the other hand, E being defined over $\mathbf{R}$, the group $E(\mathbf{R})$ is isomorphic to S_1 and thus has torsion points of any order, dense in it[30]). Let then $\xi \in E(\mathbf{R})$ be a torsion point of order n and let $x \in G$ with $\pi(x) = \xi$. Then $\pi(nx) = 0$, hence $y := nx \in \mathbf{G}_a$. If now we set $z := x - (y/n)$, we have $\pi(z) = \xi$ and $nz = 0$. (Alternatively, one may pick z as the unique point of Γ projecting to x.) Since both ξ, π are defined over $\mathbf{R}$, we have $\pi(z - \bar{z}) = 0$ and $nz = n\bar{z} = 0$. But then $z - \bar{z}$ is a torsion point on $\mathbf{G}_a$ and thus must vanish, proving that z is defined over $\mathbf{R}$. Naturally, z lies in Γ.

Therefore, since $\tau^2 = 1$, both maps $\tau \pm 1$ must have infinite kernel on Γ.

Since τ and Φ coincide on Γ (as already remarked), the same is true of the maps $\Phi \pm 1$, i.e. both kernels of $\Phi \pm 1$ are infinite; however they are both algebraic curves, and then both of these curves have infinite intersection with Γ. However they are both algebraic subgroups of dimension 1, which contradicts the opening remarks of this section. This concludes the proof of Theorem 1.

Note that the same argument fails if G is replaced by $\mathbf{G}_m^2$ because $\tau = -1$ on the whole Γ!

---

argument to conclude. See [16, V.20] for an account of Weil's descent and for references.

[29]) Here we also could conclude the proof by appealing to Remark 4.2: since $\det \varphi = -1$, Φ cannot be algebraic, unless G is split.

[30]) Alternatively, if $\xi \in E$ is a torsion point, then $\xi + \bar{\xi}$ is a real torsion point on E. Thus, if e.g. $E(\mathbf{R})$ contained only finitely many torsion points, the map $\xi \mapsto \xi + \bar{\xi}$ would have finite image on the torsion, whence by continuity would have finite image on all $E(\mathbf{C})$, which is plainly false.

REMARK 4.3 (Uniformity of bounds). Note that in the split case $G = E \times \mathbf{G}_a$ we have that, for a non-special curve $X \subset G$, the cardinality $|X \cap \Gamma|$ is not only finite, but is bounded in terms only of $\deg X$ (where the degree refers to a fixed embedding of G). This is due to the fact that $\Gamma = E \times \{0\}$ is also an algebraic curve. This last fact is not true in the non-split case; however it still makes sense to ask whether the said cardinality (again finite by Theorem 1) may be bounded only in terms of $\deg X$. We give a simple proof that this indeed holds, using a well-known (rather delicate) result by Gabrielov. Namely, we prove

THEOREM 6. *With notations as in Theorem* 1, *there is a function* $c\colon \mathbf{N} \to \mathbf{N}$ *(depending on a projective embedding of* G*) such that for a non-special curve* $X \subset G$ *of degree* d *we have* $|X \cap \Gamma| \leq c(d)$.

Proof. Note first that a curve $X \subset G$ of degree d (in a projective space $\mathbf{P}_n$ in which G is embedded) may be defined by the vanishing of homogeneous (complex) polynomials of degree d. (Consider the cones over X with vertex a general linear subspace of dimension $n-3$.)

We now consider the space of such (nonzero) polynomials f of degree d in $n+1$ projective coordinates, up to a nonzero constant factor, which may be viewed as a certain projective space $\mathbf{P}_m(\mathbf{C})$. We define Z as the subvariety of $\Gamma \times \mathbf{P}_m(\mathbf{C})$ made up of the pairs (x, f) such that $f(x) = 0$; then Z may be considered a real-analytic variety. We now apply Theorem 3.14 of [2] (i.e. Gabrielov's theorem) with $M = \Gamma \times \mathbf{P}_m(\mathbf{C})$, $X = Z$, $N = \mathbf{P}_m(\mathbf{C})$ and $\varphi\colon Z \to N$ defined as the second projection. Note that M is compact, and Z is closed in M, so Z is compact; also, φ is subanalytic, and thus it is legitimate to apply the said theorem. Its conclusion says that the number of connected components of a fiber $\varphi^{-1}(y)$ is locally bounded on N. However $\varphi(Z)$ is compact, hence this number is uniformly bounded on the whole N; let then $c(d)$ be such a uniform bound.

To conclude, just observe that if $X \subset G$ is a non-special curve, then the points in the intersection $X \cap \Gamma$ make up a finite set by Theorem 1 and are connected components of any fiber $\varphi^{-1}(f_X)$ where f_X is a polynomial of degree d vanishing on X but not on any special curve in G (and hence defining a curve in G containing X as a component and no special components). □

We do not know a specific shape for a suitable function $c(d)$, or whether this may be given in principle, in terms of an explicit presentation of G; it is possible that this could be done on carrying out the steps of a proof of Gabrielov's theorem for the case relevant here.

5. Concluding remarks

1. We have already remarked that in the case when G is an extension of E by $\mathbf{G}_m$ the fundamental dimensional condition (1.1) is not verified, since Γ has real dimension 3; hence we expect infinitely many intersections with a curve inside G. Indeed, in the split case $G \cong \mathbf{G}_m \times E$ (as algebraic groups), we have checked that any non-special curve has infinite intersection with Γ. We now briefly prove that this holds even for non-split extensions.

THEOREM 7. *Let G be an extension of an elliptic curve E by the multiplicative group $\mathbf{G}_m$, $\Gamma \subset G(\mathbf{C})$ its maximal compact subgroup. Let $X \subset G$ be an irreducible non-special curve. Then $\Gamma \cap X$ is infinite.*

Also, we could add that finiteness can arise only if $G = \mathbf{G}_m \times E$ and $X = \{\lambda\} \times E$, where $\lambda \in \mathbf{G}_m - S_1$; now the intersection is empty.

We shall use the following two lemmas (for which we have not found explicit reference):

LEMMA 8. *Let X be an irreducible algebraic curve (affine or projective, possibly singular). Let $f: X \to \mathbf{R}$ be a non-constant harmonic function*[31]*; then f has infinitely many zeros.*

Proof. By going to a normalization, we may assume that X is smooth. Suppose $f: X \to \mathbf{R}$ is harmonic with only finitely many zeros; replacing X by the complement in X of the finite set of zeros of f, we obtain a new affine curve with a never vanishing harmonic function. Then, let us suppose that f is harmonic never vanishing on X; we shall prove that it is constant. The curve X can be viewed as $\widetilde{X} - S$, where $\widetilde{X}$ is smooth and projective and $S \subset \widetilde{X}$ is a finite set. Fix a point $p \in S$. Taking a holomorphic local parameter z at p, we can write locally in a unique way

$$f = a \log |z| + \Re(g(z)),$$

where a is a real number and g a holomorphic function in a punctured disk[32] around the origin of $\mathbf{C}$. We now distinguish two cases, according to g having

---

[31] Whenever X is singular, by harmonic function on X we mean the following: let $\varphi: X' \to X$ be the normalization of X; we say that $f: X \to \mathbf{R}$ is harmonic if so is the function $f \circ \varphi$, which is now defined on a Riemann surface.

[32] Let Δ^* be a punctured disk around the origin in $\mathbf{C}$ and $h: \Delta^* \to \mathbf{R}$ a harmonic function. Locally in disks U_j, we can write $h_{U_i} = \Re(h_i)$ for holomorphic h_i, and in the intersections $U_j \cap U_k$ the function $(h_j - h_k)/\sqrt{-1}$ is locally constant and real. Since $H^1(\Delta^*, \mathbf{R})$ is one-

a singularity at 0 or not.

FIRST CASE. Suppose that for at least one point p in S, g has a singularity at 0. We show that f takes the value zero in every neighborhood of p.

Consider the Fourier development of $\Re(g(z))$; writing $z = re^{i\theta}$, we obtain

$$\Re(g(z)) = \Re(g(re^{i\theta})) = \sum_{n\in\mathbf{Z}} (a_n \cos(n\theta) + b_n \sin(n\theta))r^n ,$$

$a_n, b_n \in \mathbf{R}$, where at least one coefficient a_n or b_n is non-zero for at least one negative integer n. Let $n_0 < 0$ be one such integer and suppose for instance that $a_{n_0} \neq 0$ (the case when $b_{n_0} \neq 0$ is symmetrical). Multiplying the function $\Re(g(z))$ by the non-negative functions $1 \pm \cos(n_0\theta)$ and integrating we obtain that

$$\int_0^{2\pi} \Re(g(re^{i\theta}))(1 \pm \cos(n_0\theta))\frac{d\theta}{2\pi} = a_0 \pm a_{n_0} r^{n_0} , \qquad a_n, b_n \in \mathbf{R} .$$

Since $0 < (1 \pm \cos(n_0\theta)) < 2$, we have that for sufficiently small r, $\max_\theta \Re(g(re^{i\theta})) \geq \frac{|a_{n_0}|r^{n_0}}{3}$ and $\min_\theta \Re(g(re^{i\theta})) \leq \frac{-|a_{n_0}|r^{n_0}}{3}$. Then $f = a\log|z| + \Re(g(z))$ takes both positive and negative values on sufficiently small circles around p. In particular, it must vanish somewhere.

SECOND CASE. Suppose now that for every point $p \in S$, the corresponding holomorphic function g is regular at 0. Then f can be continued to S defining a continuous function $\widetilde{X} \to \mathbf{R} \cup \{\pm\infty\}$. If it takes both the value $-\infty$ and the value $+\infty$ (at distinct points of S), then by connectedness of X it takes the value zero at some point of X. On the other hand, if it omits the value $+\infty$, then by compactness of $\widetilde{X}$ it must take a finite maximum value, and so is constant by the maximum principle for harmonic functions. Of course, if it omits $-\infty$ then it has a finite minimum, and again it is constant, concluding the proof. □

LEMMA 9. *Let V be a complex vector space of finite dimension. Then every real-linear form on V can be written as $\Re(\varphi)$, where $\varphi: V \to \mathbf{C}$ is a complex-linear form.*

Proof. Let $d = \dim_{\mathbf{C}} V$ be the complex dimension of V; then $\dim_{\mathbf{R}} V = 2d$. Also the complex dual $\widehat{V}$ of V has dimension d, while

---

dimensional, we obtain that the quotient of the vector space of harmonic functions modulo the subspace of real parts of holomorphic functions has dimension ≤ 1. Since $\log|z|$ is one of these functions, the result follows.

the real-dual $\widehat{V}_{\mathbf{R}}$ of V, i.e. the space of $\mathbf{R}$-linear functions $V \to \mathbf{R}$, has dimension $2d$. The map $\widehat{V} \to \widehat{V}_{\mathbf{R}}$ sending $\varphi \mapsto \Re(\varphi)$ is $\mathbf{R}$-linear and injective. By the above considerations on dimensions, it must also be surjective. □

We can now prove Theorem 7. Let $X \subset G$ be a non-special curve. Consider, as before, the exponential map $\exp: T \to G$; its kernel now is a rank three lattice $\Lambda \subset T$, and $\Gamma = \exp(\mathbf{R}\Lambda)$. The real vector space $\mathbf{R}\Lambda$ is a real-hyperplane in T, so by Lemma 9 it is defined in T by an equation of the form $\Re(\varphi)(z) = 0$, for a complex linear form φ on $T \cong \mathbf{C}^2$. The linear function $\Re(\varphi)$ is invariant under translations by vectors of $\mathbf{R}\Lambda$, so *a fortiori* under the translations by the lattice Λ. Then it can be written in terms of a function on G, i.e.

$$\Re(\varphi) = f \circ \exp, \tag{5.1}$$

for a function f on G. Let us again denote by f its restriction to X. It is a harmonic function on X, because exp is locally a biholomorphism. By Lemma 8, f is either constant or has infinitely many zeros on X. In the first case φ is constant on $\exp^{-1}(X)$, so X would be a translate of a subgroup, which we have excluded. Then we can suppose that f has infinitely many zeros on X, which means that $X \cap \Gamma$ is infinite, as wanted.

2. We have seen that in $\mathbf{G}_{\mathrm{m}}^2$ the Moebius transformations provide examples of non-special algebraic curves meeting Γ in an infinite set; since a non-split extension of E by $\mathbf{G}_{\mathrm{a}}$ is analytically isomorphic to $\mathbf{G}_{\mathrm{m}}^2$, this also shows that in Theorem 1 the curve X cannot be merely supposed analytic. In this section we add further precision to this picture by showing that there are transcendental (thus non-special) analytic curves in $\mathbf{G}_{\mathrm{m}}^2$ (and so in every non-split extension of E by $\mathbf{G}_{\mathrm{a}}$) which contain an infinity of torsion points.

We start by constructing an entire function $g(z)$ such that the real part of $g(\zeta)$ is rational for all roots of unity ζ, which we enumerate as a sequence of distinct elements $\zeta_1, \zeta_2, \ldots$. We also want that the rational numbers $\Re(g(\zeta_i))$ are not all equal. We write $g(z)$ in the form

$$g(z) = g_0 + g_1(z-\zeta_1) + \frac{g_2}{2!}(z-\zeta_1)(z-\zeta_2) + \ldots + \frac{g_k}{k!}(z-\zeta_1)\cdots(z-\zeta_k) + \ldots,$$

where the g_i shall be chosen as complex numbers with $0 < |g_i| < 1$,so that indeed the series converges absolutely for all complex z, and defines an entire function. We choose the g_i inductively in the following way. We choose $g_0 = 1/2$ and, supposing to have chosen $g_0, \ldots, g_{k-1}$ for a $k \geq 1$,

we choose g_k in the punctured unit disk so that the real part of

$$g_0+g_1(\zeta_{k+1}-\zeta_1)+\frac{g_2}{2!}(\zeta_{k+1}-\zeta_1)(\zeta_{k+1}-\zeta_2)+\ldots+\frac{g_k}{k!}(\zeta_{k+1}-\zeta_1)\cdots(\zeta_{k+1}-\zeta_k)$$

is rational and distinct from $1/2$; this is clearly possible by continuity. Now observe that for $k\geq 0$ we have

$$g(\zeta_{k+1})=g_0+g_1(\zeta_{k+1}-\zeta_1)+\frac{g_2}{2!}(z-\zeta_1)(z-\zeta_2)+\ldots+\frac{g_k}{k!}(\zeta_{k+1}-\zeta_1)\cdots(\zeta_{k+1}-\zeta_k).$$

This completes the construction, obeying all the above requirements.

Now put $h(z):=g(z)+\bar{g}(z^{-1})$, where $\bar{g}$ is the entire function defined by conjugating the Taylor coefficients of $g(z)$; it coincides with the function defined by $\bar{g}(z)=\overline{g(\bar{z})}$.

Observe that $h(z)$ is holomorphic in the punctured complex plane and that for z in the unit circle we have $h(z)=2\Re(g(z))$ and in particular h takes rational values at all roots of unity and is non constant.

Finally, put $f(z):=\exp(2\pi i h(z))$. This is also holomorphic in the punctured plane and non constant, so f is transcendental: if it were algebraic, being holomorphic it would be rational, but then $f'(z)/f(z)=2\pi i h'(z)$ would have no residues, a contradiction. Also, $f(z)$ takes values which are roots of unity at every root of unity, as wanted.

3. In the whole paper, motivated by the Manin-Mumford question on torsion points, we have considered intersections with the maximal compact subgroup of a commutative algebraic group G, and one can consider generalizations of Theorem 1. For instance, it seems to us that the above argument works also in the case of the universal vector extension of an arbitrary complex abelian variety. Namely, take an abelian variety A of dimension g and consider the *universal extension* G of A by $\mathbf{G}_{\mathrm{a}}^{g}$, which is such that: (1) it is not of the form $\mathbf{G}_{\mathrm{a}}\times G'$ for any extension G' of A by $\mathbf{G}_{\mathrm{a}}^{g-1}$ and (2) every extension of A by $\mathbf{G}_{\mathrm{a}}^{d}$ is a product of a quotient of G by a power of $\mathbf{G}_{\mathrm{a}}$. Such a G exists and is essentially unique in view of a theorem of Rosenlicht [12]. Then our proof should extend to give the following conclusion: *If $X\subset G$ is an algebraic curve, then $X\cap\Gamma$ is finite*. (This issue has been suggested to us by A. Pillay.)

However one can consider, more generally, intersections of algebraic subvarieties of G with smaller compact subgroups, or even closed Lie-subgroups.

For instance, in the case of an extension G of an elliptic curve by $\mathbf{G}_{\mathrm{m}}$, one can consider intersections of an algebraic curve $X\subset G$ with $\exp(\mathbf{R}\Lambda')$,

where Λ' is a sublattice of rank 2 of the lattice Λ of the proof of Theorem 7 (i.e. $\Lambda = \ker\exp$). *Does an analogue of Theorem* 1 *hold in this case ?*

One can also generalize the dimensional condition (1.1) to the cases when the intersection $X \cap \Gamma$ has 'unlikely' dimension, i.e. $\dim_{\mathbf{R}}(X \cap \Gamma) > 2\dim X + \dim_{\mathbf{R}} \Gamma - \dim G$. A general (vague) question is: *What does this imply for* X *?*

And one can similarly consider intersections of an algebraic curve (or variety) X in an abelian variety G, with $\exp(T')$ where T' is a vector subspace whose projection modulo Λ is a real subtorus of the underlying complex torus. For example, when G is the Jacobian of a real algebraic curve X of genus 2, $G(\mathbf{R})$ has real-dimension 2 and the intersection $G(\mathbf{R}) \cap X$ can sometimes be infinite (when X has a smooth real point) or even empty (when X has no real point).

We have not studied these more general forms of our original question, and it also seems that they have not been considered in the existing literature, at any rate systematically. We believe it may not be without of interest to investigate the cases when some natural dimensional assumptions do indeed imply finiteness or infiniteness, as the case may be, of the relevant intersections.

Appendix: A letter of Jean-Pierre Serre

As promised above, we reproduce (in LaTeX style) a (typewritten) letter of Jean-Pierre Serre to David Masser. (The "Appendice à Waldschmidt" mentioned in the letter is [15].)

Paris, le 19 juin 1980

cher Masser,

Vous m'avez demandé l'autre jour un plongement explicite dans un espace projectif du groupe commutatif de dimension 2 correspondant aux formes de deuxième espèce sur une courbe elliptique. Voici un tel plongement:

Je note A la courbe elliptique, définie par

$$y^2 = 4x^3 - g_2x - g_3 \qquad \omega = dx/y$$

à la façon habituelle, et paramétrée par $\omega = du$, $x = \wp(u)$, $y = \wp'(u)$ comme il se doit.

Le groupe qui nous intéresse est une extension E de A par $\mathbf{G}_a$ (groupe additif); cette extension est non triviale; elle est unique, à automorphisme de $\mathbf{G}_a$ près. (La normalisation de E correspond au choix d'une forme de 2ème espèce; je ferai choix ici de $x\omega = xdx/y$; c'est ce qu'il y a de plus standard.)

Comme je l'ai expliqué dans mon Appendice à Waldschmidt, on peut obtenir des compactifications projectives lisses de E de la façon suivante: on compactifie d'abord E en $\bar{E}$ de la manière évidente, i.e. en ajoutant un point à l'infini à chacune des fibres de la projection $E \to A$, fibres qui sont isomorphes à une droite affine. Ceci fait, on obtient un fibré $\bar{E}$ de base A, à fibres des droites projectives, chaque fibre ayant un point marqué, le point " à l'infini " que l'on a ajouté. Appelons E^∞ le lieu de ces points, de sorte que $E = \bar{E} - E^\infty$. Appelons d'autre part F une fibre quelconque de la projection $\bar{E} \to A$. On peut voir F et E^∞ comme des diviseurs irréductibles sur la surface lisse $\bar{E}$. Leurs relations d'intersection sont: $F.F = 0$, $F.E^\infty = 1$, $E^\infty.E^\infty = 0$. Si l'on prend alors pour diviseur la combinaison linéaire

$$\Delta = 3F + E^\infty \qquad \text{(c'est ce que j'appelle } D_{3,1} \ \ldots\text{)}$$

on voit facilement que Δ est *très ample*, et donne un plongement projectif de $\bar{E}$ dans *l'espace projectif* $\mathbf{P}_5$ *de dimension* 5. Comme $\Delta.\Delta = (3F + E^\infty)^2 = 6F.E^\infty = 6$, on voit que $\bar{E}$ est réalisée comme une *variété de degré* 6 dans $\mathbf{P}_5$.

En principe, ceci devrait vous suffire. Mais il peut être intéressant d'expliciter en termes classiques les fonctions qui donnent le plongement de $\bar{E}$ dans $\mathbf{P}_5$. C'est ce que je vais faire. Je choisirai pour F la fibre F_0 de l'origine O dans la courbe elliptique A. On doit alors regarder l'espace $L(\Delta)$ des fonctions rationnelles f sur $\bar{E}$ telles que $(f) \geq -3F_0 - E^\infty$; ces fonctions ont donc un pôle simple sur la fibre générique, et un pôle triple (au plus) sur la fibre particulière F_0, image réciproque de O. L'espace $L(\Delta)$ est de dimension 6. Il contient tout d'abord les fonctions

$$1,\ x,\ y \qquad \text{provenant de } A$$

qui sont constantes sur les fibres de $\bar{E} \to A$. Il contient également des fonctions linéaires (affines) sur les fibres:

$$t_1,\ t_x,\ t_y$$

telles que

$$t_f(g+t) = t_f(g) + f(g)t,$$

pour tout $g \in E$ et $t \in \mathbf{G}_a$. (Par exemple $t_1(g+t) = t_1(g)+t$.) On peut en outre demander que t_1, t_x, t_y aient des pôles simple, double et triple (respectivement) sur la fibre F_0 ; et on peut demander que t_1 et t_x soient impaires et t_y paire. Cela fixe t_1 et t_x. On a

(1) $xt_1 - t_x = \lambda y$ (λ scalaire $\neq 0$)

et

(2) $yt_1 - t_y = \mu x^2$ si t_y est bien choisi ($\mu \neq 0$).

On peut montrer que $\mu = 4\lambda$. Quitte à faire une homothétie sur $\mathbf{G}_a$, on peut se ramener au cas où $\lambda = -1/2$, $\mu = -2$, et c'est ce que je ferai dans la suite. Enfin, on a

(3) $yt_x - xt_y = -\frac{1}{2}(g_2 x + g_3)$.

Les 6 fonctions $1, x, y, t_1, t_x, t_y$ donnent un plongement de $\bar{E}$ dans $\mathbf{P}_5$, qui est le plongement cherché. Je me permetterai de noter (z, x, y, a, b, c) les coordonnées projectives correspondantes. Les équations ci-dessus s'écrivent alors sous forme homogène

(1') $bz - xa = \frac{1}{2}yz$

(2') $zc - ya = 2x^2$

(3') $xc - yb = \frac{1}{2}(g_2 xz + g_3 z^2)$.

Noter que la variété $\bar{E}$ *n'est pas* égale à l'intersection des trois quadriques définies par ces équations ! Cette intersection se compose en fait de $\bar{E}$ et du plan $x = y = z = 0$ compté 2 fois (ce qui redonne le fait que $\bar{E}$ est de degré $2 \cdot 2 \cdot 2 - 2 = 6$).

On peut d'ailleurs exhiber des équations satisfaites par $\bar{E}$ qui ne sont pas conséquences de (1'), (2'), (3'), par exemple :

(4) $ac^2 - 4b^3 + g_2 ba^2 + g_3 a^3 = \frac{1}{2}g_2 ya^2 + y^2 b - 4yb^2 - xyc + 2xbc$.

Je n'ai pas essayé de déterminer un système de générateurs de l'idéal des polynômes nuls sur $\bar{E}$; j'espère que vous n'en aurez pas besoin ...

Autres remarques sur ce modèle :

a) l'origine est le point $(0, 0, 1, 0, 0, 0)$;

b) l'addition à un point $g = (z, x, y, a, b, c)$ d'un élément t de $\mathbf{G}_a$ se traduit par les formules :

$$g + t = (z, x, y, a + tz, b + tx, c + ty);$$

c) les points à l'infini (i.e. E^∞) sont les points $(0, 0, 0, z, x, y)$ avec

(5) $zy^2 = 4x^3 - g_2 xz^2 - g_3 x^3$

(équation qui est d'ailleurs conséquence de (1'), (2'), (3') comme on le voit facilement);

d) les fibres de $\bar{E} \to A$ sont réalisées dans $\mathbf{P}_5$ comme des droites projectives; cela résulte de b), ou bien du fait qu'on a choisi 1 comme coefficient de E^∞ dans le diviseur Δ.

Exercice (que je n'ai pas fait): écrire explicitement la loi de composition de E.

Exercice (que j'ai fait): écrire x, y, t_1, t_x, t_y en fonction de la paramétrisation analytique naturelle (sur $\mathbf{C}$) de E. Pour cela, on remarque que les formes invariantes sont

$$\omega = \mathrm{d}x/y \qquad \text{et} \qquad \eta = \mathrm{d}t_1 + x\mathrm{d}x/y\,.$$

Si l'on intègre ces formes, i.e. si l'on pose $\omega = \mathrm{d}u$ et $\eta = \mathrm{d}t$, on est conduit aux développements suivants:

$(x/z) = x = \wp(u) = u^{-2} + c_2u^2 + c_4u^4 + \ldots \quad (c_2 = g_2/20,\ c_4 = g_3/28)$

$(y/z) = y = \wp'(u) = -2u^{-3} + 2c_2u + 4c_4u^3 + \ldots$

$(a/z) = t_1 = t + \zeta(u) = t + u^{-1} - c_2u^3/3 + \ldots \qquad (\zeta' = -\wp)$

$(b/z) = t_x = t\wp(u) + \wp(u)\zeta(u) + \frac{1}{2}\wp'(u) = t(u^{-2} + c_2u^2 + \ldots) + \frac{5}{3}c_2u + \ldots$

$(c/z) = t_y = t\wp'(u) + \wp'(u)\zeta(u) + 2\wp^2(u) = t(-2u^{-3} + 2c_2u + \ldots) + \frac{20}{3}c_2 + \ldots$

J'espère que mes coefficients numériques sont justes! Mais je ne le garantis pas complètement...

Voilà ce que je peux faire de mieux comme plongement de la variété $\bar{E}$ elle-même. Si vous êtes moins exigeant, et si vous désirez seulement un plongement d'un *ouvert* U de E contenant un sous-groupe de type fini Γ *donné*, on peut s'en tirer bien plus trivialement. En effet, il suffit de choisir un point Q de E non situé dans la projection de Γ dans A, et de remarquer:

a) la courbe elliptique A privée du point Q peut se réaliser comme cubique affine dans un plan affine;

b) la restriction du fibré $E \to A$ à $A - \{Q\}$ est un produit direct.

Il s'ensuit que l'on peut identifier E privé de la fibre F_Q de Q comme le *produit direct* de $A - \{Q\}$ et du groupe additif $\mathbf{G}_a$. Ceci permet de réaliser l'ouvert $U = E - F_Q$ comme une *surface cubique* (et même un "cylindre cubique" $y^2 = 4x^3 - g_2x - g_3$) dans *l'espace affine de dimension* 3, de coordonnées x, y, t. C'est là un procédé un peu brutal; je suis un peu sceptique sur son utilité: à vous de juger.

Bien à vous

J-P. Serre

PS — Merci pour votre lettre sur les points de torsion des var. abéliennes.

REFERENCES

[1] BEAUVILLE, A. *Surfaces algébriques complexes.* Astérisque *54*. Soc. Math. de France, Paris, 1978.

[2] BIERSTONE, E. and P. D. MILMAN. Semianalytic and subanalytic sets. *Publ. Math. Inst. Hautes Études Sci. 67* (1988), 5–42.

[3] BOMBIERI, E. and W. GUBLER. *Heights in Diophantine Geometry.* New Mathematical Monographs *4*. Cambridge University Press, Cambridge, 2006.

[4] BOREL, A. *Linear Algebraic Groups.* Second edition. Graduate Texts in Mathematics *126*. Springer-Verlag, New York, 1991.

[5] FORSTER, O. *Lectures on Riemann Surfaces.* Graduate Texts in Mathematics *81*. Springer-Verlag, New York-Berlin, 1981. (Original German edition, Berlin, 1977.)

[6] HINDRY, M. Autour d'une conjecture de Serge Lang. *Invent. Math. 94* (1988), 575–603.

[7] —— *Groupes algébriques commutatifs, exemples explicites.* Séminaire d'arithmétique, Saint-Étienne (1988-89).

[8] LANG, S. *Elliptic Functions.* Addison-Wesley Publishing Co., Inc., Reading, Mass.-London-Amsterdam, 1973.

[9] MASSER, D. W. Heights, transcendence, and linear independence on commutative group varieties. In: *Diophantine Approximation (Cetraro, 2000)* (F. Amoroso and U. Zannier, eds.), 1–51. Lecture Notes in Mathematics *1819*. Springer, Berlin, 2003.

[10] MUMFORD, D. *Algebraic Geometry I, Complex Projective Varieties.* Reprint of the 1976 edition. Classics in Mathematics, Springer-Verlag, Berlin, 1995.

[11] RAYNAUD, M. Courbes sur une variété abélienne et points de torsion. *Invent. Math. 71* (1983), 207–233.

[12] ROSENLICHT, M. Extensions of vector groups by abelian varieties. *Amer. J. Math. 80* (1958), 685–714.

[13] —— Liouville's theorem on functions with elementary integrals. *Pacific J. Math. 24* (1968), 153–161.

[14] SWINNERTON-DYER, H. P. F. *Analytic Theory of Abelian Varieties.* London Mathematical Society Lecture Note Series *14*. Cambridge University Press, London-New York, 1974.

[15] SERRE, J-P. Quelques propriétés des groupes algébriques commutatifs, appendice ii. In: *Nombres transcendants et groupes algébriques*, by M. Waldschmidt, 191–202. Astérisque *69–70*, Soc. Math. de France, 1987.

[16] —— *Algebraic Groups and Class Fields.* Graduate Texts in Mathematics *117*. Springer-Verlag, New York, 1988.

[17] —— *Lie Algebras and Lie Groups.* Lecture Notes in Mathematics *1500*. Springer-Verlag, Berlin, 1992.

[18] SILVERMAN, J. H. *The Arithmetic of Elliptic Curves.* Corrected reprint of the 1986 original. Graduate Texts in Mathematics *106*. Springer-Verlag, New York, 1992.

[19] TITCHMARSH, E. C. *The Theory of Functions.* Second edition. Oxford University Press, 1978.

[20] WALDSCHMIDT, M. *Nombres transcendants et groupes algébriques*. Astérisque *69–70*, Soc. Math. de France, 1987.

[21] WHITTAKER, E. T. and G. N. WATSON. *A Course of Modern Analysis*. An introduction to the general theory of infinite processes and of analytic functions: with an account of the principal transcendental functions. Fourth edition. Reprinted Cambridge University Press, New York, 1962.

[22] ZANNIER, U. *Some Problems of Unlikely Intersections in Arithmetic and Geometry*. With appendixes by D. Masser. Annals of Mathematics Studies *181*. Princeton University Press, Princeton, NJ, 2012.

(Reçu le 9 février 2012)

Pietro Corvaja

Dipartimento di Matematica e Informatica
Università degli studi di Udine
Via delle Scienze 206
I-33100 Udine
Italia
e-mail : pietro.corvaja@uniud.it

David Masser

Mathematisches Institut
Universität Basel
Rheinsprung 21
CH-4051 Basel
Switzerland
e-mail : David.Masser@unibas.ch

Umberto Zannier

Scuola Normale Superiore
Piazza dei Cavalieri, 7
I-56126 Pisa
Italia
e-mail : u.zannier@sns.it