Torsion points, Pell's equation, and integration in elementary terms

David Masser, Umberto Zannier

Departement Mathematik und Informatik
Fachbereich Mathematik
Universität Basel
CH-4051 Basel

Preprint No. 2020-01
August 2020

dmi.unibas.ch

TORSION POINTS, PELL'S EQUATION, AND INTEGRATION IN ELEMENTARY TERMS

D. MASSER AND U. ZANNIER

This paper (with some devilish difficulties) is dedicated to Enrico Bombieri in celebration of his 80th birthday.

Abstract. *The main results of this paper involve general algebraic differentials ω on a general pencil of algebraic curves. We show how to determine if ω is integrable in elementary terms for infinitely many members of the pencil. In particular, this corrects an assertion of James Davenport from 1981 and provides the first proof, even in rather strengthened form. We also indicate analogies with work of André and Hrushovski and with the Grothendieck-Katz Conjecture.*

To reach this goal, we first provide proofs of independent results which extend conclusions of relative Manin-Mumford type allied to the Zilber-Pink conjectures: we characterize torsion points lying on a general curve in a general abelian scheme of arbitrary relative dimension at least 2.

In turn, we present yet another application of the latter results to a rather general pencil of Pell equations $A^2 - DB^2 = 1$ over a polynomial ring. We determine whether the Pell equation (with squarefree D) is solvable for infinitely many members of the pencil.

2010 MSC codes. 11G10, 14K15, 14K20, 11G50, 12H05.

1. Introduction.

1.1. **Preamble.** The main results of this paper involve general algebraic differentials on a general pencil of algebraic curves with a fixed function x, provided all is defined over the field $\overline{\mathbf{Q}}$ of algebraic numbers. As an example, we show that there are at most finitely many complex numbers t such that

$$\frac{\mathrm{d}x}{(x^2-1)\sqrt{x^5+tx^3+x}}$$

can be integrated in elementary terms. This is in accordance with a general conjecture of Davenport from 1981. However, we show that his conjecture is false and we prove a modified version, on the way determining all counterexamples (which are admittedly rather rare). For more details see subsection 1.3, especially Theorem 1.3.

An important element of our proofs concerns generalized Jacobians, especially products of additive extensions of elliptic curves, for which we develop some independent theory. Another key element consists of new results of relative Manin-Mumford type allied to the Zilber-Pink conjectures. Namely, we characterize torsion points lying on a general curve in a general abelian scheme of arbitrary relative dimension at least 2, again provided all is defined over $\overline{\mathbf{Q}}$. As an example, we show that there are at most finitely many complex numbers t such that a triple of points on

$$y^2 \;=\; x(x-1)(x-t)(x-t^2)(x-t^4)(x-t^5)(x-t^8)$$

with abscissae $2, 3, 5$ corresponds to a torsion point on the Jacobian. For more details see subsection 1.4, especially Theorem 1.7.

We apply the latter results also to a rather general pencil of Pell equations in a fixed variable x, once more provided all is defined over $\overline{\mathbf{Q}}$. As an example consider

$$A^2 - (x^8 + x + t)B^2 = 1, \quad B \neq 0.$$

We show in principle how one could prove that there are at most finitely many complex numbers t such that this is solvable for A, B in $\mathbf{C}[x]$ (which is practically certain to be true). For more details see subsection 1.2, especially Theorem 1.1.

1.2. **Pell's equation.** We now discuss Pell's equation. In [53] and [10] we gave some applications to

$$A^2 - DB^2 = 1, \quad B \neq 0 \tag{1.1}$$

over the polynomial ring $\mathbf{C}[x]$. There we handled only D of degree at most six, and we showed for example that there are at most finitely many complex t for which (1.1) is solvable for A, B in $\mathbf{C}[x]$ with $D = x^6 + x + t$. There are some exceptional t, as the formula

$$(2x^5 + 1)^2 - (x^6 + x)(2x^2)^2 \ = \ 1 \tag{1.2}$$

for $t = 0$ shows. We also remarked that the natural "local-to-global" assertion is generally false, with the examples $D = x^4 + x + t$ or $D = x^6 + x^2 + t$, where Pell's equation is not solvable identically in t but still solvable for infinitely many values of t.

Now we could treat $x^8 + x + t$ and so on; but we prefer to give a more general assertion as follows, replacing the parameter t by a generic point $\mathbf{c}$ on a fixed base curve.

We fix a base curve C defined over $\overline{\mathbf{Q}}$. Then we take D as a squarefree polynomial in x of even degree $2g + 2 \geq 6$ (and even $g = 1$ would do here) defined over the function field $\overline{\mathbf{Q}}(C)$. A complete smooth model (see section 10) of the hyperelliptic curve H_D defined by $y^2 = D(x)$ has genus g and two points ∞^+, ∞^- at infinity. Their difference $\infty^+ - \infty^-$ gives a point P_D on the Jacobian J_D, itself of dimension g, of this model. It is classically known that (1.1) is solvable if and only if P_D is torsion.

For all but finitely many $\mathbf{c}$ in $C(\mathbf{C})$ it is clear that we obtain a specialized polynomial $D(\mathbf{c})$ defined over $\mathbf{C}$, also of degree $2g + 2$. We will be continually using such statements in the course of this paper, sometimes in slightly less simple situations; but it is always just a matter of elementary algebraic geometry to which we will refer without further explanation as "reduction theory".

Theorem 1.1. *(a) If P_D is not torsion on J_D and there is no elliptic curve in J_D containing a positive integer multiple of P_D, then there are at most finitely many $\mathbf{c}$ in $C(\mathbf{C})$ such that Pell's equation for $D(\mathbf{c})$ is solvable.*

(b) If there is an elliptic curve E_D in J_D containing nP_D for a positive integer n, then there are infinitely many $\mathbf{c}$ in $C(\mathbf{C})$ such that Pell's equation for $D(\mathbf{c})$ is solvable; unless there is an isogeny ι from E_D to an elliptic curve E_0 defined over $\overline{\mathbf{Q}}$ with $\iota(nP_D)$ in $E_0(\overline{\mathbf{Q}})$ non-torsion, in which case there are no $\mathbf{c}$ at all.

(c) If P_D is torsion, then for all but finitely many $\mathbf{c}$ in $C(\mathbf{C})$, Pell's equation for $D(\mathbf{c})$ is solvable.

Remark. We note that if a squarefree D in $\overline{\mathbf{Q}}(C)[x]$ is given, then we may effectively determine which of $(a), (b), (c)$ holds and thereby establish whether the corresponding set of $\mathbf{c}$ is finite or not (however in case of finiteness we do not yet know how to find the set effectively - a deep problem to which the work [11] of Binyamini will certainly be relevant).

Here the cases $(a), (b), (c)$ can all occur; see just after the proof of Theorem 1.1 in section 10.

This proof uses a new generalization of Theorem 1.5 below.

It is probably possible to extend Theorem 1.1 to D which are not squarefree. One would start from Proposition 2.5 of the second author's paper [78]. Bertrand's counterexample yields among others the example

$$D = x^2(x^4 + tx^3 - tx - 1) = x^2(x^2 - 1)(x^2 + tx + 1)$$

in [9] for which Pell's equation is not identically solvable but there exist infinitely many t with solvability (yet another type of failure for "local-to-global"). This arises from a multiplicative

extension of an elliptic scheme. On the other hand there are at most finitely many t such that Pell's equation is solvable for

$$D = x^3(x^3 + x + t).$$

This arises from an additive extension of an elliptic scheme. See the second author's article [77] and Schmidt [66].

1.3. **Integration.** We proceed now to a discussion of integration. The connexion of Pell with integration of algebraic functions in elementary terms (see later for some definitions) is classically known since Abel [1] (and his functions) and Chebychev [17],[18] (for elliptic functions, with his "pseudo-elliptic integrals"). See also Halphen [32]. Thus in [53] we remarked for the above example $D = x^6+x+t$ that it follows that there are at most finitely many complex t for which there exists a non-zero E in $\mathbf{C}[x]$ of degree at most 4 such that $E/\sqrt{D}$ is integrable in elementary terms (see just below for the definition). As $D'/\sqrt{D}$ integrates to $2\sqrt{D}$ we cannot go up to degree 5 here. There are some exceptional t, as the formula

$$\int \frac{5x^2 \mathrm{d}x}{\sqrt{x^6 + x}} \;=\; \log\left(\frac{1}{2} + x^5 + x^2\sqrt{x^6 + x}\right)$$

corresponding to (1.2) for $t = 0$ shows.

For general degree we can deduce the following rather quickly from Theorem 1.1.

Corollary 1.2. *Suppose that D, P_D and J_D are as in Theorem 1.1(a), so that $g \geq 2$. Then there are at most finitely many $\mathbf{c}$ in $C(\mathbf{C})$ such that there exists $E \neq 0$ in $\mathbf{C}[x]$ of degree at most $2g$ for which $E/\sqrt{D(\mathbf{c})}$ is integrable in elementary terms.*

Again $D'/\sqrt{D}$ shows that we cannot go up to degree $2g + 1$ here.

The result for $g = 1$ would be false; for example it is classical that there are infinitely many τ in $\mathbf{C}$ such that there exists υ in $\mathbf{C}$ for which

$$\frac{x - \upsilon}{\sqrt{x^4 + x + \tau}} \tag{1.3}$$

is integrable in elementary terms.

Also in [53] we noted some similarities with an assertion in the book [21] of Davenport. His Theorem 7 (p.90) says that if an algebraic function $f(x, t)$ is not generically integrable in elementary terms, then there are at most finitely many t at which the specialised function is integrable in elementary terms. Thus there are no quantifiers about any numerator E as above, and things like

$$\int \sqrt{x^2 + t}\ \mathrm{d}x \;=\; \frac{1}{2}x\sqrt{x^2 + t} + \frac{t}{2}\log(x + \sqrt{x^2 + t}) \tag{1.4}$$

are ruled out. At that time such finiteness statements were rather rare, so this is a remarkable assertion of a "local-to-global" type (see the remarks later about results of André, Hrushovski and the Grothendieck-Katz Conjecture).

Unfortunately his proof, summarized on the same page, cannot be rescued. Already on the previous page he lists five ways in which the specialised function can become integrable in elementary terms, thus representing five possible obstacles to a proof (in fact there are many more obstacles, as will be clear from the discussion of our own arguments later). He points out that the first and second of these can be easily eliminated through what we called reduction theory above. The third obstacle he describes as "exceptionally tricky" to eliminate. It involves residues and we address this problem in section 14; if f is defined over $\overline{\mathbf{Q}}$ it naturally leads to a bound on the degree of t over $\mathbf{Q}$, but this of course does not suffice for finiteness.

The fourth obstacle presents a serious problem, and the treatment in [21] seems to be based on a misunderstanding of Picard-Fuchs operators. It is somewhat classical that integrability in elementary terms can lead to torsion properties for t (see also section 14); for example that $P_t = (2, \sqrt{2(2-t)})$ is torsion on the Legendre curve E_t defined by $y^2 = x(x-1)(x-t)$ as in (1.6) below. Now this particular property can be disproved for generic t by applying Picard-Fuchs, involving in this case the well-known hypergeometric expression

$$PF(z) \;=\; t(1-t)\frac{\mathrm{d}^2 z}{\mathrm{d}t^2} + (1-2t)\frac{\mathrm{d}z}{\mathrm{d}t} - \frac{1}{4}z,$$

to a suitable point on the tangent space for example $z_t = \int_2^\infty \mathrm{d}x/y$. We find

$$PF(z_t) = -\frac{\sqrt{2(2-t)}}{2(2-t)^2},$$

and as this is not identically zero we may conclude (keyword: Manin) that P_t is not identically torsion on E_t (that is, for generic t). But from the fact that $PF(z_t)$ is non-zero at all values $t \neq 2$ we cannot conclude that P_t is non-torsion on E_t at all values $t \neq 2$. Indeed it was first observed in [50] (p.1677) that there are infinitely many values of t such that P_t is torsion on E_t. Thus Picard-Fuchs arguments cannot be specialized. We will see that one can say something about finiteness as in (1.6) below, but that requires the full power of [50] and concerns $E_t \times E_t$ not just E_t (and more generally Theorem 1.6 and Theorem 1.7 below).

The fifth obstacle appears to be related to our section 12.

We make further references to these obstacles later in this section and also at appropriate points in our proof.

The main aim of the present paper was originally to give a proof of Davenport's Assertion provided f is defined over $\overline{\mathbf{Q}}$ (with eventual extension to $\mathbf{C}$). But right at the end of the investigation we found a counterexample, so here too "local-to-global" fails. However counterexamples seem to be extremely rare. The proof when these are excluded uses the full power of Theorems 1.6 and 1.5 below, together with our new generalization of Theorem 1.5. It occupies the main part of this paper, and several additional features, of possible interest in themselves, had to be developed.

The basic definition of integration in elementary terms involves a differential field $\mathfrak{F}$ with a derivation δ. An elementary extension $\mathfrak{F}'$ of $\mathfrak{F}$ is a differential extension obtained as a finite tower of extensions $\mathfrak{F}'_0/\mathfrak{F}_0$ of intermediate differential fields $\mathfrak{F}'_0, \mathfrak{F}_0$, where $\mathfrak{F}'_0/\mathfrak{F}_0$ is algebraic, or $\mathfrak{F}'_0 = \mathfrak{F}_0(v)$ with either $\delta v = \delta u/u$ (informally $v = \log u$) or $\delta v/v = \delta u$ (informally $v = \exp u$) for some u in $\mathfrak{F}_0$. One has by abuse of adjectives the standard

Definition. *An f in $\mathfrak{F}$ is elementary integrable if $f = \delta g$ for some g in some elementary extension of $\mathfrak{F}$.*

Abel [1] was the first to make a systematic treatment for algebraic functions, and gave the example

$$\int \frac{(5x-1)\mathrm{d}x}{\sqrt{x^4+2x^2-4x+1}} \;=\; \log\left(\frac{x^3+x-2+x\sqrt{x^4+2x^2-4x+1}}{x^3+x-2-x\sqrt{x^4+2x^2-4x+1}}\right)$$

(which Maple 18 cannot verify by integration), even though the same thing with numerator $5x - t$ is elliptic for any $t \neq 1$. This shows that exceptional t exist also for Davenport's Assertion. See also section 21 for an amazing integral of Euler, which seems to have the same spirit as one of our own counterexamples. And van der Poorten and Tran [59] (p.168) have a hyperelliptic example corresponding to genus 2. For much higher genus see some formulae, apparently due to Greenhill, in subsection 1.7.

It may have been examples like these that prompted Hardy [33] (p.11) in 1905 to write

"... no general method has been devised by which we can always tell, after a finite series of operations, whether any given integral is really elementary, or elliptic, or belongs to a higher order of transcendents."

And over a century later nothing much has changed, even for algebraic functions, although for the elementary integration of these the connexion with torsion on abelian varieties is now much better understood, and algorithms for this torsion have been developed. In particular Risch [62] gave an elegant formulation and sketched a method which should decide if a given algebraic $f(x)$ is elementary integrable. However this will not suffice for Davenport's family $f(x,t)$ with regard to the totality of its individual members.

To deal with algebraic functions we take a field $\mathbb{K}$ of characteristic zero and a curve X, for convenience assumed to be irreducible and smooth, defined over $\mathbb{K}$ together with a non-constant function x in $\mathbb{K}(X)$. Then $\mathfrak{F} = \mathbb{K}(X)$ with $\delta = \mathrm{d}/\mathrm{d}x$ is a differential field.

In connexion with counterexamples to Davenport's Assertion, we will give later in section 16 a full definition of "elusive" f in $\mathfrak{F}$; it is rather long and at first sight appears so restrictive

that it may be found surprising that any actually exist, like Higgs bosons. For the moment we remark that when X has positive genus with Jacobian J containing no elliptic curve with complex multiplication CM, then no f in $\mathfrak{F}$ is elusive. A more precise definition involves residues.

To deal with specializations we take $\mathbb{K}$ as $\overline{\mathbf{Q}}(C)$ for a base curve C as above, now defined over $\overline{\mathbf{Q}}$. We then switch from X to "calligraphic" $\mathcal{X}$; this seems better to emphasize the particular nature of $\mathbb{K}$. By reduction theory, for all but finitely many $\mathbf{c}$ in $C(\mathbf{C})$ we obtain a curve $\mathcal{X}(\mathbf{c})$, also irreducible and smooth, defined over $\mathbf{C}$ and a differential field $\mathfrak{F}(\mathbf{c}) = \overline{\mathbf{Q}}(\mathcal{X}(\mathbf{c}))$ also with $\delta = \mathrm{d}/\mathrm{d}x$. And for each f in $\mathfrak{F} = \overline{\mathbf{Q}}(C)(\mathcal{X})$ we obtain $f(\mathbf{c})$ in $\mathfrak{F}(\mathbf{c})$ (also a specialization, and not to be confused with a value of the function f).

Theorem 1.3. *(a) Suppose f in $\mathfrak{F}$ is not elusive. Then if f is not elementary integrable, there are at most finitely many $\mathbf{c}$ in $C(\mathbf{C})$ such that $f(\mathbf{c})$ in $\mathfrak{F}(\mathbf{c})$ is elementary integrable.*

(b) Suppose f in $\mathfrak{F}$ is elusive. Then f is not elementary integrable but there are infinitely many $\mathbf{c}$ in $C(\mathbf{C})$ such that $f(\mathbf{c})$ in $\mathfrak{F}(\mathbf{c})$ is elementary integrable.

Remark. It will be clear, as in the Pell discussions, that if f in $\overline{\mathbf{Q}}(C)(\mathcal{X})$ is given, then we may effectively determine which of $(a), (b)$ holds.

We will see in section 21 with several examples that both cases $(a), (b)$ actually turn up. For the moment we just quote our unexpected counterexample for (a): there are infinitely many $t = i, \sqrt{5 - 10i}/5, \ldots$ in $\mathbf{C}$ for which

$$\frac{x}{(x^2 - t^2)\sqrt{x^3 - x}} \tag{1.5}$$

is elementary integrable. It is not identically so, and thus we are now in case (b) with something elusive.

Now in Davenport's Assertion the fields $\mathbf{Q}(t)$ for the special values of t are not specified. Possibly they were intended to be contained in a fixed number field. We show here that something a bit stronger follows relatively quickly, and with no exceptions. Namely we restrict $\mathbf{c}$ to $C(\overline{\mathbf{Q}})$ (in itself harmless) and more crucially of bounded degree $[\mathbf{Q}(\mathbf{c}) : \mathbf{Q}]$. This result was one of the reasons for our believing in unconditional finiteness.

Proposition 1.4. *Suppose f in $\mathfrak{F}$ is not elementary integrable. Then for any D there are at most finitely many $\mathbf{c}$ in $C(\overline{\mathbf{Q}})$ with $[\mathbf{Q}(\mathbf{c}) : \mathbf{Q}] \leq D$ such that $f(\mathbf{c})$ in $\mathfrak{F}(\mathbf{c})$ is elementary integrable.*

1.4. **Relative Manin-Mumford.** We consider first the following conjecture to be found in our article [50], for the moment over $\mathbf{C}$.

Conjecture. *Let $\mathcal{S}$ be a semiabelian scheme over a variety defined over $\mathbf{C}$, and denote by $\mathcal{S}^{[c]}$ the union of its semiabelian subschemes of codimension at least c. Let $\mathcal{V}$ be an irreducible closed subvariety of $\mathcal{S}$. Then $\mathcal{V} \cap \mathcal{S}^{[1+\dim \mathcal{V}]}$ is contained in a finite union of semiabelian subschemes of $\mathcal{S}$ of positive codimension.*

This is a variant of that stated by Pink [58] in 2005, which generalized the Zilber Conjectures [80] of 2002 to schemes. In fact the above conjecture is false (see below), but the counterexamples do not contradict Pink's more comprehensive statement. The conjecture probably holds for abelian schemes (see for example Theorems 1.5 and 1.7 below), and possibly also for addttive extensions (see for example Theorem 1.6 below).

The first result on this conjecture (for non-constant $\mathcal{S}$) was in [50] (see also [49] for a short version). There we verified it when $\mathcal{S}$ is the fibred square of the standard Legendre elliptic family, with coordinates $(x_1, y_1), (x_2, y_2)$, and $\mathcal{V}$ is the curve defined by $x_1 = 2, x_2 = 3$. This amounted to the finiteness of the set of complex numbers $t \neq 0, 1$ such that the points

$$(2, \sqrt{2(2 - t)}), \quad (3, \sqrt{6(3 - t)}) \tag{1.6}$$

both have finite order on E_t.

The subsequent generalizations in [51], [52], [53], as well as [20] (with Corvaja), imply the following.

Theorem 1.5. (Corvaja-Masser-Zannier). *Let $\mathcal{A}$ be an abelian surface scheme over a variety defined over $\mathbf{C}$, and let $\mathcal{V}$ be an irreducible closed curve in $\mathcal{A}$. Then $\mathcal{V}\cap\mathcal{A}^{[2]}$ is contained in a finite union of abelian subschemes of $\mathcal{A}$ of positive codimension.*

This established the above Conjecture for abelian schemes of relative dimension 2 when $\mathcal{V}$ is a curve.

In all these examples we are intersecting with the set $\mathcal{S}^{[2]}$, which since $\mathcal{S}$ has relative dimension 2 is the collection of all torsion points on the fibres. This is sometimes known as the relative Manin-Mumford problem. Now the work of Hindry [34] on the original Manin-Mumford problem is not restricted to the abelian or even semiabelian situation and indeed it deals with arbitrary commutative group varieties, such as for example extensions of an elliptic curve by the additive group $\mathbf{G}_{\mathrm{a}}$ (for this example see also the paper [19] with Corvaja). And recent work [67] of Harry Schmidt treats such extensions of elliptic schemes as follows.

Theorem 1.6. (Schmidt). *Let $\mathcal{G}$ be an extension by $\mathbf{G}_{\mathrm{a}}$ of an elliptic scheme over a variety defined over $\mathbf{C}$, and denote by $\mathcal{G}^{[c]}$ the union of its flat group subschemes of codimension at least c. Let $\mathcal{V}$ be an irreducible closed curve of $\mathcal{G}$. Then $\mathcal{V}\cap\mathcal{G}^{[2]}$ is contained in a finite union of group subschemes of $\mathcal{G}$ of positive codimension.*

However Bertrand [8] discovered a counterexample when the surface scheme is an extension of an elliptic scheme by the multiplicative group $\mathbf{G}_{\mathrm{m}}$. In a work [10] with him and Pillay we have also shown that his are essentially the only counterexamples for semiabelian surfaces over $\overline{\mathbf{Q}}$. So this work completes the analysis of the above Conjecture for schemes of relative dimension 2 over $\overline{\mathbf{Q}}$. See also the second author's book [75] (pp.77-80).

Our proof of Theorem 1.3 uses Proposition 1.4 as well as Theorem 1.6 (over $\overline{\mathbf{Q}}$) together with the following generalization (also over $\overline{\mathbf{Q}}$) of Theorem 1.5.

Theorem 1.7. *Let $\mathcal{A}$ be an abelian scheme of relative dimension $g\geq 2$ over a variety defined over $\overline{\mathbf{Q}}$, and let $\mathcal{V}$ be an irreducible closed curve in $\mathcal{A}$. Then $\mathcal{V}\cap\mathcal{A}^{[g]}$ is contained in a finite union of abelian subschemes of $\mathcal{A}$ of codimension at least $g-1$.*

This is more in the style of relative Manin-Mumford because of course $\mathcal{A}^{[g]}$ is just the set of torsion points on all the fibres. It also confirms a conjecture stated in 1998 by Zhang [79].

As in our previous papers we can give simple examples of our theorem for base curves in the style of (1.6). Thus we get the finiteness of the set of complex numbers $t\neq 0$ with

$$t^5\neq 1,\ t^6\neq 1,\ t^7\neq 1,\ t^8\neq 1 \tag{1.7}$$

such that the triple of points

$$\begin{gathered}(2,\sqrt{2(2-t)(2-t^2)(2-t^4)(2-t^5)(2-t^8)})\\ (3,\sqrt{6(3-t)(3-t^2)(3-t^4)(3-t^5)(3-t^8)})\\ (5,\sqrt{20(5-t)(5-t^2)(5-t^4)(5-t^5)(5-t^8)})\end{gathered}\tag{1.8}$$

on the curve of genus 3 defined by

$$y^2 \;=\; x(x-1)(x-t)(x-t^2)(x-t^4)(x-t^5)(x-t^8) \tag{1.9}$$

give - via the unique point at infinity on (1.9) - a point of finite order on the Jacobian.

We will soon see that the base variety in Theorem 1.7 can be assumed to be irreducible of dimension at most one. In case it is a point, then $\mathcal{A}$ is constant and we see the classical result of Manin-Mumford type in the special situation under consideration. In fact we will appeal to the classical result to eliminate this case.

We have here $\mathcal{V}\cap\mathcal{A}^{[g]}$. A more difficult problem is to deal similarly with $\mathcal{V}\cap\mathcal{A}^{[2]}$, usually larger if $g\geq 3$. Barroero and Capuano [5] have proved, for example, that there are at most finitely many complex numbers $t\neq 0,1$ such that the points

$$(2,\sqrt{2(2-t)}),\quad (3,\sqrt{6(3-t)}),\quad (5,\sqrt{20(5-t)})$$

satisfy two independent linear relations on E_t (corresponding to the fibre cube). And very recently [6] they have succeeded (using among other things the techniques of our section 7) to treat $\mathcal{V}\cap\mathcal{A}^{[2]}$ in general (with $\mathcal{V}$ still a curve).

1.5. **On the proofs.** Let us now say something of our own proofs. That of our Theorem 1.7 follows the general strategy of [49],[50],[51],[52],[53] and [57] but a couple of new issues arise. We have to study equations

$$\mathbf{z} = x_1\mathbf{f}_1 + \cdots + x_{2g}\mathbf{f}_{2g} \tag{1.10}$$

where $\mathbf{f}_1, \ldots, \mathbf{f}_{2g}$ are basis elements of the period lattice of $\mathcal{A}$ and $\mathbf{z}$ is an abelian logarithm. Our coefficients $x_1, \ldots, x_{2g}$ are real and their locus S in $\mathbf{R}^{2g}$ is subanalytic, of dimension at most 2 because a complex curve has real dimension 2. When $\mathbf{z}$ corresponds to a torsion point, say of order dividing some N, then we get a rational point in $\frac{1}{N}\mathbf{Z}^{2g}$ on S. The work of Pila [56] provides for any $\epsilon > 0$ an upper bound for their number of order at most N^ϵ as N tends to infinity, provided we avoid connected semialgebraic curves inside S.

If $\mathcal{V}$ itself is contained in an abelian subscheme of $\mathcal{A}$ of positive codimension, there is nothing to prove. Otherwise we are able to show that there are no connected semialgebraic curves inside S. This follows from the algebraic independence of the g components of $\mathbf{z}$ over the field generated by the components of $\mathbf{f}_1 \ldots, \mathbf{f}_{2g}$ in (1.10). Here the remark of Bertrand mentioned in our previous papers (see for example [51] p.455) is especially essential in circumventing the question of dependence relations already holding between these components, which would presumably depend now on the Mumford-Tate group of $\mathcal{A}$. In [53] we had to appeal to more general work of André [3] (see also Bertrand's paper [7]); and this suffices here too.

We conclude the proof as in [53] by combining Silverman's Specialization Theorem [72] with a result of David [23] on degrees of torsion points of the corresponding fibre of $\mathcal{A}$. If this fibre is itself simple then we deduce by contrast that the number of rational points in $\frac{1}{N}\mathbf{Z}^{2g}$ is of order at least N^δ for some $\delta > 0$. But the fibre could well be non-simple. Perhaps this situation could be controlled with the help of conjectures (or even theorems) of André-Oort type. However we can avoid such problems as in [53] by exploiting an escape clause in [23] and using some comparatively elementary estimates from the first author's work [44] with Wüstholz. Now we have to be careful about polarizations, but by induction this leads to the desired N^δ. The resulting Proposition 7.1 should be useful in other contexts (already in [20] for example). Comparison of the lower bound with the above upper bound leads to an estimate for N which suffices to prove the Theorem.

The proof of Theorem 1.1 is then relatively short, following the arguments in [53] now in higher dimension.

To deduce Corollary 1.2 the basic first step is the classical Liouville's Theorem, which enables to dispense with the unknown extension $\mathfrak{F}'$ in the definition of elementary integrable. In general this allows one to forget about exponentials, and use logarithms in only a linear way. It implies in our situation that f is elementary integrable if and only if there are $g_0, g_1 \neq 0, \ldots, g_m \neq 0$ in $\mathfrak{F}$ and $c_1, \ldots, c_m$ in $\mathbf{C}$ with

$$f \;=\; \delta g_0 + c_1\frac{\delta g_1}{g_1} + \cdots + c_m\frac{\delta g_m}{g_m}$$

(informally $f = \delta g$ for $g = g_0 + c_1 \log g_1 + \cdots + c_m \log g_m$ a linear form in logarithms).

Then an analysis of poles (of the associated differential) gives what we want.

As for the proof of Theorem 1.3 (see also [76] for an informal exposition), this too relies heavily on Liouville. We start by reducing to the case of simple poles, which has the effect of eliminating δg_0. This appears to be related to Davenport's fifth obstacle.

Then we give the proof of Proposition 1.4. It works by bounding from above the height $h(\mathbf{c})$ using Silverman's Theorem about families of abelian varieties; however this result must be modified if there are non-zero isotrivial parts, and that causes extra technicalities. For example we have to go through estimates of the form

$$h(\mathbf{c}) \;\leq\; C(\log(h(\mathbf{c}) + 1) + 1)$$

(more commonly seen in connexion with isogeny estimates) for C independent of $\mathbf{c}$.

We proceed further by looking at residues, which have to do with Davenport's third obstacle. If these specialize in a particular degenerate way, then we come back to bounded degree as in Proposition 1.4. If not, then it is reasonably classical (through [62] for example) that this leads to torsion points on specialized abelian varieties in the sense of Theorem 1.5 or Theorem 1.7 above. Theorem 1.7 then suffices to prove Theorem 1.3(a) in case the Jacobian $\mathcal{J}$ of $\mathcal{X}$

is simple of dimension at least 2, also without exceptions. This partly overcomes Davenport's fourth and most problematic obstacle (without any Picard-Fuchs operators, which do not seem to be useful here after all - but see the proof of Lemma 5.1).

If the above dimension is 1, then we have to consider also a zero of f or rather the corresponding differential ϖ. That leads to torsion points on additive extensions in the sense of Theorem 1.6, but this step seems no longer to be classical. It is crucial that the extension is non-split. Furthermore the argument breaks down if there is complex multiplication. But if not, then again there are no exceptions.

It turns out that the main difficulties arise for non-simple $\mathcal{J}$. In that case we have to introduce an "auxiliary differential" $\varpi^\natural$ and its zeroes $\mathcal{Z}$. For each $\mathcal{Z}$ we consider a suitable additive extension $\mathcal{J}_{r\mathcal{Z}}$ of $\mathcal{J}$, and even the power $(\mathcal{J}_{r\mathcal{Z}})^m$. If we cannot use Theorem 1.5 or Theorem 1.7, then we can reduce to an additive extension $\mathcal{F}_\mathcal{Z}$ of an elliptic curve, but of much higher dimension than that in Theorem 1.6. Furthermore we no longer obtain a point which is torsion on the specialized $\mathcal{F}_\mathcal{Z}$, but only on a quotient by a certain linear subspace. It now becomes a problem to check if this quotient is non-split; such things are governed by what we call the "splitting line", for which we could find no explicit references in the literature (although its existence can be deduced from properties of the "universal vectorial extension"). Here it is necessary to take into account all the zeroes $\mathcal{Z}$, together with their full multiplicities, and then apply a primitive sort of "zero estimate" coming from Riemann-Roch. This completely overcomes Davenport's fourth obstacle.

But still the arguments break down if there is complex multiplication. In that case we cannot prove non-split, but if the thing is split then we can exploit the full additive part, which has no non-trivial torsion, to obtain finiteness. On this journey all the various parts of the definition of elusive turn up one by one, and this finally proves Theorem 1.3(a).

It is now relatively easy to reverse the arguments to prove Theorem 1.3(b); here the same sort of zero estimate is used. Actually this proof precedes that of Theorem 1.3(a), on grounds connected with the effectivity of the dichotomy between (a) and (b). Earlier we had a definition of elusive for which this effectivity was not clear, but we could change it to overcome this problem.

1.6. **Programme.** Here is a brief section-by-section account of this paper.

In section 2 we show how to reduce Theorem 1.7 to a statement, Proposition 2.1, involving the special case of a curve C in a product $\mathbf{P}_G \times \mathbf{P}_G$ of projective spaces. Here the second factor contains a certain moduli space of abelian varieties with fixed level structure, so that for each point there is an abelian variety, and this lies in the first factor. Then in section 3 we recall the main result of [56] on subanalytic sets. Our own set is constructed from abelian logarithms defined in section 4. The relevant algebraic independence result is then proved in section 5. This then leads in section 6 to the non-existence of Pila's semialgebraic curves in our set. Then in sections 7 and 8 we record the consequences of the work of David and Silverman for our purposes, and the proof of Proposition 2.1 is completed in section 9.

Then in section 10 we check the example (1.8) and prove Theorem 1.1 using the Liouville Theorem. We also say a bit more about (10.1),(10.2) and (10.3).

In a short section 11 we introduce the concept of residue divisor which will be indispensable for the effectivity considerations.

Then as preparation for the proof of Theorem 1.3(a), we show in section 12 that it suffices to consider differentials of the third kind; by this we mean that there are no poles of order at least two.

In section 13 we prove Proposition 1.4. This enables us in section 14 to reduce elementary integrability to a problem of torsion points on abelian varieties, and to prove Theorem 1.3(a) with some additional simplicity condition on the Jacobian.

Then in section 15 we pause to explain the difficulties involved in removing this condition. It is then timely in section 16 to give the definition of elusive differential together with some explanations and observations.

In section 17 we prove Theorem 1.3(b).

Then in section 18 we extend some of the considerations of section 14 to torsion points on certain quotients of products of generalized Jacobians, and in section 19 we show that

the property of being elusive is invariant under adding something elementary integrable (as it should be if Theorem 1.5 is true, but which was not obvious under our earlier definition); it is here that Theorem 1.3(b) is used, along with material from section 11.

And at last in section 20 we complete the proof of Theorem 1.3(a).

Finally in section 21 we verify the examples above and give a self-contained proof for our first counterexample (21.8), at the same time finding all exceptional values of t. We also provide some more examples of elusive differentials.

And in an appendix, so as not to interrupt too much the main exposition, we investigate the splitting line, together with a related concept of "splitting map" for additive extensions of an elliptic curve. Also we hope that these may be of independent interest in the theory of generalized Jacobians.

1.7. **Further remarks.** We now make some remarks about the broader context of our results, and we thank Michael Singer for valuable discussions around the topic of integration. As examples of recent work on elementary integration with parameters we may cite that of Caviness, Saunders and Singer [16] and also Singer [74], although these are mainly concerned with transcendental functions (but see also Davenport and Singer [22] especially the closing pages). Sometimes finiteness fails here; for example

$$(\log x)^t$$

is elementary integrable precisely for $t = 0, 1, 2, \ldots$ (not difficult from Liouville).

Also [16] extends the notion of "elementary integrability" to things like the error function, and gives a corresponding extension of Liouville's Theorem. It might be interesting also to attempt this for elliptic functions (and their inverses?) in order to address more thoroughly Hardy's quotation. It seems that Abel [2] had made a start on this. Or one could even try to treat genus 2 and so on; some of the classical literature was concerned with expressing integrals of a given genus in terms of lower genus.

In this connexion of "genus-dropping" we may extract from Greenhill [31] (pp. 156-157) the example

$$\int \frac{\mathrm{d}x}{\sqrt[6]{x^{11}+11x^6-x}} \;=\; \frac{6}{5}\int \frac{\mathrm{d}\tilde{x}}{\sqrt{4\tilde{x}^3+6912}}$$

with

$$\tilde{x} = \frac{x^{20}-228x^{15}+494x^{10}+228x^5+1}{(x^{11}+11x^6-x)^{5/3}},$$

which is elliptic even though the genus is now 25. In fact a pull-back lies behind this (not in [31] explicitly). Namely, there is a rational map ϕ from $y^6 = x^{11}+11x^6-x$ to $\tilde{y}^2 = 4\tilde{x}^3+6912$ defined by

$$\phi(x,y) = (\tilde{x},\tilde{y}) = \left(\frac{P}{y^{10}}, \frac{2Q}{y^{15}}\right),$$

where $P = P(x)$ is the polynomial of degree 20 above and $Q = Q(x)$ is the polynomial of degree 30 below. And

$$\frac{\mathrm{d}x}{y} \;=\; \frac{6}{5}\phi^*\left(\frac{\mathrm{d}\tilde{x}}{\tilde{y}}\right).$$

In particular a Jacobian of dimension 25 has an elliptic factor.

And similarly

$$\int \frac{\mathrm{d}x}{\sqrt[15]{x^{30}+522x^{25}-10005x^{20}-10005x^{10}-522x^5+1}} \;=\; \int \frac{\mathrm{d}\tilde{x}}{(1728\tilde{x}^5-1)^{2/3}}$$

(for a different $\tilde{x}$) which drops from genus 196 to genus 4 (despite Greenhill's assertion that it too is elliptic - at any rate it can be shown that the corresponding differential is not a pull-back of a differential on an elliptic curve). See also Schwarz [68] (p.253). These examples seem to be connected to the icosahedron: if $R = R(x)$ is the polynomial of degree 11 above then

$$Q^2 = P^3 + 1728R^5$$

reflects the well-known syzygy as for example in Klein's [38] (p. 62).

Of course the more modern literature has focused more on differential Galois theory, and Kaplansky [36] wrote

"There is another attractive chapter of differential algebra that is not represented in my book or in Kolchin's: the integration of functions in "elementary" terms (...).This is a kind of "pre-Galois" theory, in that only the basic properties of differential fields are involved. (In the same way, the theory of ruler and compass constructions precedes Galois theory in the study of ordinary fields)."

But despite this it seems that differential Galois theory is not sensitive enough to detect elementary integrability.

Nevertheless, replacing our $\mathrm{d}g/\mathrm{d}x = f$ by their $L(g) = 0$ leads to analogous problems, even with several parameters not just one (see Cassidy and Singer [15]). Thus André [4] and Hrushovski [35] have shown that the Galois group is unchanged under "almost all" specializations, and in particular the solvability in algebraic functions specializes similarly (the solvability of $\mathrm{d}g/\mathrm{d}x = f$ with algebraic g is essentially treated in our easy section 12). But the example

$$x\mathrm{d}g/\mathrm{d}x - tg \;=\; 0,$$

with algebraic solution $g = x^t$ when t is rational, shows that one cannot hope for finiteness statements as in our Theorem 1.3.

Finally this work of [4], [35], at least for a single parameter t, is considered as a function field analogue of the famous Grothendieck-Katz Conjecture on p-curvatures, where values of t are replaced by primes p (here too one cannot hope for finiteness); see for example Katz [37] and a general discussion in [76].

It would be interesting to know if the techniques of this paper can be applied to any of the problems above.

We thank Detmar Welz for valuable correspondence about some of the integrals in this paper, especially in section 21. We thank also the referees for their careful reading and suggestions for improvement.

2. Reduction to a fixed model.

Clearly Theorem 1.7 implies that $\mathcal{V} \cap \mathcal{A}^{[g]}$ is contained in a finite union of abelian subschemes of $\mathcal{A}$ of positive codimension. But this apparently weaker version of Theorem 1.7 actually directly implies Theorem 1.7 itself. Thus at first we see that $\mathcal{V} \cap \mathcal{A}^{[g]}$ is contained in finitely many $\mathcal{B} \neq \mathcal{A}$ in $\mathcal{A}$. But then applying to $\mathcal{V} \cap \mathcal{B}$ we get $\mathcal{V} \cap \mathcal{A}^{[g]}$ in finitely many $\mathcal{C} \neq \mathcal{B}$ in $\mathcal{B}$; and so on by induction, until we reach an ambient abelian scheme of codimension at least $g - 1$.

We noted in section 2 of [51] that the above Conjecture is isogeny invariant in the following sense. Let $\mathcal{S}, \mathcal{S}'$ be semiabelian schemes defined over varieties over $\mathbf{C}$ and suppose that there is an isogeny ι from $\mathcal{S}$ to $\mathcal{S}'$. Then the Conjecture for $\mathcal{S}'$ implies the Conjecture for $\mathcal{S}$. The same implication holds with $\mathbf{C}$ generalised to any algebraically closed field of zero characteristic, and for possible later use we maintain this generality for the present short section.

Now the argument of [51] can be repeated to prove the analogous implication for this weaker version of our Theorem 1.7 with $\mathcal{A}, A'$ (say over $\overline{\mathbf{Q}}$). We need only change $\mathcal{S}^{[1+d]}$ there to $\mathcal{A}^{[g]}$ (and it stays valid even for $\mathcal{S}^{[e]}$ with any fixed e).

If the weaker version of Theorem 1.7 holds for an abelian scheme $\mathcal{B}$ over a variety, and $\tilde{\mathcal{B}}$ is another abelian scheme over the same variety, then it also holds for their fibre product $\mathcal{A} = \mathcal{B} \times \tilde{\mathcal{B}}$. The argument is easy but we give some details, especially as it breaks down for the Conjecture. The point is that the torsion $\mathcal{A}^{[g]} = \mathcal{B}^{[h]} \times \tilde{\mathcal{B}}^{[\tilde{h}]}$ for the respective relative dimensions $g, h, \tilde{h}$. If $\mathcal{V}$ projects to $\mathcal{W}$ in $\mathcal{B}$, then $\mathcal{W} \cap \mathcal{B}^{[h]}$ is contained in a finite union of abelian subschemes $\mathcal{B}_0$ of $\mathcal{B}$ of positive codimension provided $\mathcal{W}$ is a curve (and *a fortiori* otherwise). So also $\mathcal{V} \cap \mathcal{A}^{[g]}$ is contained in a finite union of abelian subschemes $\mathcal{B}_0 \times \tilde{\mathcal{B}}$ of $\mathcal{A}$ of positive codimension.

Now every abelian scheme of relative dimension at least 2 has a factor (up to isogeny) which is either of relative dimension 2 or simple of relative dimension at least 2. Thus by Theorem 1.5 and the above remarks it suffices to prove the weaker version of Theorem 1.7 for simple $\mathcal{A}$. This will be helpful when proving the functional algebraic independence referred to in section 1.

In [53] we reduced to Jacobians (of hyperelliptic curves), where the periods could be given explicitly in terms of differentials. In fact both our applications involve only Jacobians, but the weaker version of Theorem 1.7 for these does not seem to imply directly the weaker version of Theorem 1.7 in general. Fortunately there is a very good setting where the differentials arise in a natural analytic way, that of theta functions. This has already been used by many writers, for example the first author [47], or David [23], or Wüstholz and the first author [44]. Here we follow [44] in using the $(16, 32)$ level structure, which lies between the full 16 structure and the full 32 structure. Then the moduli space is a quasi-projective variety $\mathfrak{M}$ in $\mathbf{P}_G$ for $G+1 = 16^g$, defined over $\mathbf{Q}$. For $\mathbf{m} = (m_0 : \cdots : m_G)$ in $\mathfrak{M}$ we denote by $A(\mathbf{m})$ the corresponding abelian variety, also in $\mathbf{P}_G$ with coordinates say $\mathbf{x} = (x_0 : \cdots : x_G)$ and defined over $\mathbf{Q}(\mathbf{m})$. In fact the zero of $A(\mathbf{m})$ is none other than $\mathbf{m}$. See section 4 for the explicit description by theta functions, which have the advantage that they give smooth embeddings of both the moduli space and the fibres.

Now every abelian variety is isogenous (in the usual sense) to a principally polarized one with such a level structure. Thus we have an isogeny ι from the scheme $\mathcal{A}$ (now assumed simple) of our Theorem 1.7 to some $\mathcal{A}' = A(\mathbf{m})$ as above, where now we are thinking of $A(\mathbf{m})$ as a subset of $\mathbf{P}_G \times \mathbf{P}_G$ with coordinates $(\mathbf{x}, \mathbf{m})$.

Let $\mathcal{V}$ be a curve in $\mathcal{A}$. Then $\iota(\mathcal{V})$ in $A(\mathbf{m})$ is a quasi-projective curve C in $\mathbf{P}_G \times \mathbf{P}_G$ with coordinates say

$$(\xi_0 : \cdots : \xi_G, \mu_0 : \cdots : \mu_G) \tag{2.1}$$

We will regard it as being parametrized by (2.1) with the components (projectively) functions in $\overline{\mathbf{Q}}(C)$.

If the point $P = (\xi_0 : \cdots : \xi_G)$ satisfies $NP = O$ for some positive integer N, then the whole of $\iota(\mathcal{V})$ lies in the corresponding abelian subscheme of relative dimension zero, so Theorem 1.7 is trivial for $\mathcal{A}'$. Thus we are entitled to assume $NP \neq O$ for all such N.

If $(\mu_0 : \cdots : \mu_G)$ is (projectively) constant on C, then the base variety can be considered as a point and the Theorem for $\mathcal{A}'$ follows from Manin-Mumford as mentioned in the Introduction.

From all these considerations, we see that our Theorem 1.7 for $\mathcal{A}$ is implied by the following statement (so the base variety is indeed reduced to a curve).

Proposition 2.1. *Let C in $\mathbf{P}_G \times \mathbf{P}_G$ be a curve defined over $\overline{\mathbf{Q}}$ and parametrized by the generic point*

$$\mathbf{c} \;=\; (\xi_0 : \cdots : \xi_G, \mu_0 : \cdots : \mu_G)$$

in $\mathbf{P}_G(\overline{\mathbf{Q}}(C)) \times \mathbf{P}_G(\overline{\mathbf{Q}}(C))$, such that $T = (\mu_0 : \cdots : \mu_G)$ lies in $\mathfrak{M}$, the abelian variety $A(T)$ is simple and non-isotrivial, and $P = (\xi_0 : \cdots : \xi_G)$ lies on $A(T)$. Then if P is not identically torsion, there are at most finitely many specializations $\mathbf{c}$ in $C(\mathbf{C})$ such that the point

$$P(\mathbf{c}) = (\xi_0(\mathbf{c}) : \cdots : \xi_G(\mathbf{c}))$$

is torsion on $A(T(\mathbf{c})) = A(\mu_0(\mathbf{c}) : \cdots : \mu_G(\mathbf{c}))$.

3. Rational points.

In this section we record the basic result of Pila [56] that we shall use. We recall from section 2 of [50] that a naive-m-subanalytic subset of $\mathbf{R}^s$ is a finite union of $\psi(\mathbf{D})$, where each $\mathbf{D}$ is a closed ball in $\mathbf{R}^m$ and each ψ is real analytic from an open neighbourhood of $\mathbf{D}$ to $\mathbf{R}^s$. We refer also there for the definition of S^{trans}.

Lemma 3.1. *Suppose S is a naive-2-subanalytic subset of $\mathbf{R}^s$. Then for any $\epsilon > 0$ there is a $c = c(S, \epsilon)$ with the following property. For each positive integer N there are at most cN^ϵ rational points of S^{trans} in $\frac{1}{N}\mathbf{Z}^s$.*

Proof. See Lemma 2.1 of [50] (p.1680). □

4. Functions.

We will construct our naive-2-subanalytic subset S by means of theta functions. Let $\mathcal{S}_g$ be the Siegel upper half-space of degree g. For τ in $\mathcal{S}_g$, and for row vectors $\mathbf{u}$ in $\mathbf{C}^g$ and $\mathbf{p}$ in $\mathbf{R}^g$ we use

$$\theta_{\mathbf{p}}(\tau,\mathbf{u}) \;=\; \sum_{\mathbf{h}} \exp\{\pi i(\mathbf{h}+\mathbf{p})\tau(\mathbf{h}+\mathbf{p})^t + 2\pi i(\mathbf{h}+\mathbf{p})\mathbf{u}^t\}$$

with the sum over all row vectors $\mathbf{h}$ in $\mathbf{Z}^g$, where t denotes the transpose. Here we may regard $\mathbf{p}$ in the quotient $(\mathbf{R}/\mathbf{Z})^g$. We define $\Theta(\tau,\mathbf{u})$ from $\mathcal{S}_g \times \mathbf{C}^g$ to $\mathbf{C}^{G+1}$ by arranging the elements $\mathbf{p}$ of $(\frac{1}{16}\mathbf{Z}/\mathbf{Z})^g$ in some order and taking the coordinates of $\Theta(\tau,\mathbf{u})$ to be the $\theta_{\mathbf{p}}(16\tau,16\mathbf{u})$. This parametrizes in terms of $\mathbf{u}$ an abelian variety A_τ isomorphic to $\mathbf{C}^g/U(\tau)$, where the lattice $U(\tau)$ is generated by the standard basis row vectors $\mathbf{e}_1,\dots,\mathbf{e}_g$ together with the rows $\mathbf{t}_1,\dots,\mathbf{t}_g$ of τ. See [44] p.415.

Now given any $\mathbf{c}$ in $C(\mathbf{C})$ we can find $\tau_{\mathbf{c}}$ in $\mathcal{S}_g$ with

$$\Theta(\tau_{\mathbf{c}},0) = (\mu_0(\mathbf{c}) : \cdots : \mu_G(\mathbf{c})) \tag{4.1}$$

the origin of $A_{\tau_{\mathbf{c}}}$ and then $\mathbf{u}_{\mathbf{c}}$ in $\mathbf{C}^g$ with

$$\Theta(\tau_{\mathbf{c}},\mathbf{u}_{\mathbf{c}}) = (\xi_0(\mathbf{c}) : \cdots : \xi_G(\mathbf{c})), \tag{4.2}$$

in $A_{\tau_{\mathbf{c}}}$, by smoothness both locally analytic on C.

So now we will consider these as functions $\mathbf{e}_1,\dots,\mathbf{e}_g,\mathbf{t}_1,\dots,\mathbf{t}_g$ and $\mathbf{u}$ locally analytic from C to $\mathbf{C}^g$. They generalize the $1, g/f$ and z/f of the elliptic case [50] (p.1682). To recover the generalization of f, g and z we have to modify as follows. For any $\mathbf{c}$ we can find a square submatrix $\rho = \rho_{\mathbf{c}}$ of the (affine) Jacobian matrix of $\Theta(\tau_{\mathbf{c}},\mathbf{u})$ which is non-singular at $\mathbf{u}=0$. Then we define

$$\mathbf{f}_1 = \mathbf{e}_1\rho^{-1},\dots,\mathbf{f}_g = \mathbf{e}_g\rho^{-1},\ \mathbf{f}_{g+1} = \mathbf{t}_1\rho^{-1},\dots,\mathbf{f}_{2g} = \mathbf{t}_g\rho^{-1}, \tag{4.3}$$

and

$$\mathbf{z} = \mathbf{u}\rho^{-1}. \tag{4.4}$$

This looks like an analytic construction but it is known that then the "Shimura differential" $d\mathbf{z}$ is defined over $\mathbf{C}(C)$ (see the calculations on pp. 419-422 of [44] for example, especially the differential equations in Lemmas 3.6 and 3.7). That will be crucial for the functional algebraic independence result of the next section.

5. Algebraic independence.

For this section we fix some $\mathbf{c}_*$ of C. Then $\mathbf{f}_1,\dots,\mathbf{f}_{2g}$ and $\mathbf{z}$ are well-defined on a small neighbourhood $\mathbf{N}_*$ of $\mathbf{c}_*$. In order to prove $S^{\mathrm{trans}} = S$ we will need the following result.

Lemma 5.1. *The coordinates of* $\mathbf{z}$ *are algebraically independent over* $\mathbf{C}(\mathbf{f}_1,\dots,\mathbf{f}_{2g})$ *on* $\mathbf{N}_*$.

Proof. The remark on Shimura differentials above means that the de Rham basis in Z (p.15) of [3] is over $\mathbf{C}(C)$. Thus we can use Theorem 3 (p.16) of [3] (whose proof uses among other things Picard-Fuchs), which actually specifies the transcendence degree of $\mathbf{K}(\mathbf{z},\tilde{\mathbf{z}})$ over

$$\mathbf{K} = \mathbf{C}(C)(\mathbf{f}_1,\dots,\mathbf{f}_{2g},\tilde{\mathbf{f}}_1,\dots,\tilde{\mathbf{f}}_{2g}),$$

where the extra functions are the corresponding integrals of the second kind. It is the dimension of the $\tilde{U}$ appearing in Proposition 1 (p.5) of [3], or at least its relative counterpart in the context of section 4 of [3]. The E there is $A(T)$ over C, for which our simplicity hypothesis implies that the only proper connected algebraic subgroup is O. And u there is from $\mathbf{Z}$ to $\mathbf{Z}P$ (note that $A(T)$ has no non-zero isotrivial part because it is simple and non-isotrivial). And because P is not identically torsion and $A(T)$ is simple the E' there is also E, with rational homology isomorphic to $\mathbf{Q}^{2g}$. Further because of simplicity the F there is a division algebra. So $F.u(\mathcal{X})$ is isomorphic to F. Thus we find dimension $2g$, which is the number of coordinates in $\mathbf{z},\tilde{\mathbf{z}}$; and the present lemma follows on throwing away all the extra functions. □

6. A naive-2-subanalytic set.

We describe here our naive-2-subanalytic subset S. First we construct local functions from C to $\mathbf{R}^{2g}$. Fix $\mathbf{c}_*$ in C, choose $\mathbf{c}$ in C and then a path from $\mathbf{c}_*$ to $\mathbf{c}$ lying in C. Using (4.1) and (4.2) we find no problem to continue $\mathbf{e}_1, \dots, \mathbf{e}_g, \mathbf{t}_1, \dots, \mathbf{t}_g$ (the first g of these are of course constant) and $\mathbf{u}$ to a neighborhood $\mathbf{N_c}$ of $\mathbf{c}$. And for ρ we can stick to a fixed submatrix provided we remove finitely many points from C where it becomes singular. This gives via (4.3) and (4.4) also $\mathbf{f}_1, \dots, \mathbf{f}_{2g}, \mathbf{z}$ on $\mathbf{N_c}$. They do depend on $\mathbf{c}$ but only in a mild way as this dependence is essentially locally constant, so we indicate this also with a subscript as $\mathbf{f}_{1,\mathbf{c}}, \dots, \mathbf{f}_{2g,\mathbf{c}}, \mathbf{z}_\mathbf{c}$.

Write $\Omega_\mathbf{c} = U(\tau_\mathbf{c})\rho_\mathbf{c}^{-1}$.

Lemma 6.1. *The coordinates of* $\mathbf{z_c}$ *are algebraically independent over* $\mathbf{C}(\mathbf{f}_{1,\mathbf{c}}, \dots, \mathbf{f}_{2g,\mathbf{c}})$ *on* $\mathbf{N_c}$. *Further we have* $\Omega_\mathbf{c} = \mathbf{Z}\mathbf{f}_{1,\mathbf{c}} + \dots + \mathbf{Z}\mathbf{f}_{2g,\mathbf{c}}$ *on* $\mathbf{N_c}$.

Proof. We could continue an algebraic dependence relation backwards to get the same relation between $\mathbf{f}_1, \dots, \mathbf{f}_{2g}, \mathbf{z}$ on a neighbourhood of $\mathbf{c}_*$; however this would contradict Lemma 5.1. The assertion about $\Omega_\mathbf{c}$ is clear from (4.3), and we are done. □

It follows that we can define $x_{1,\mathbf{c}}, \dots x_{2g,\mathbf{c}}$ on $\mathbf{N_c}$ by the equation

$$\mathbf{z}_\mathbf{c} = x_{1,\mathbf{c}}\mathbf{f}_{1,\mathbf{c}} + \dots + x_{2g,\mathbf{c}}\mathbf{f}_{2g,\mathbf{c}} \tag{6.1}$$

and its complex conjugate

$$\overline{\mathbf{z}_\mathbf{c}} = x_{1,\mathbf{c}}\overline{\mathbf{f}_{1,\mathbf{c}}} + \dots + x_{2g,\mathbf{c}}\overline{\mathbf{f}_{2g,\mathbf{c}}}$$

so that $x_{1,\mathbf{c}}, \dots x_{2g,\mathbf{c}}$ are real-valued.

Now we can define S. But first we make a compact set out of the quasi-projective C in $\mathbf{P}_N \times \mathbf{P}_N$. Let C_0 be the finite set of points in the Zariski closure C^0 of C but not in C. Fix any norm on $\mathbf{P}_N \times \mathbf{P}_N$. For small $\delta > 0$ (later to be specified) we define C^δ as the set of $\mathbf{c}$ in C^0 satisfying $|\mathbf{c}| \le 1/\delta$ and

$$|\mathbf{c} - \mathbf{c}_0| \ \ge \ \delta$$

for each $\mathbf{c}_0$ in C_0. Thus C^δ is a compact subset of C.

Shrinking $\mathbf{N_c}$ if necessary, we can choose a local analytic isomorphism $\varphi_\mathbf{c}$ from $\mathbf{N_c}$ to an open subset of $\mathbf{C}$ (i.e. $\mathbf{R}^2$). Choose any closed disc $\mathbf{D_c}$ inside $\varphi_\mathbf{c}(N_\mathbf{c})$ centred at $\varphi_\mathbf{c}(\mathbf{c})$, and define

$$\psi_\mathbf{c} \ = \ (x_{1,\mathbf{c}}, \dots, x_{2g,\mathbf{c}}) \circ \varphi_\mathbf{c}^{-1}$$

from $\mathbf{D_c}$ to $\mathbf{R}^{2g}$. By compactness there is a finite set $\Pi = \Pi^\delta$ of $\mathbf{c}$ such that the $\varphi_\mathbf{c}^{-1}(\mathbf{D_c})$ cover C^δ. Then our naive-2-subanalytic subset $S = S^\delta$ in $\mathbf{R}^{2g}$ is defined as the union of $\psi_\mathbf{c}(\mathbf{D_c})$ over Π.

Lemma 6.2. *We have* $S^{\mathrm{trans}} = S$.

Proof. Because every semialgebraic surface contains semialgebraic curves, it will suffice to deduce a contradiction from the existence of a semialgebraic curve B_s lying in S. Now B_s is Zariski-dense in its Zariski-closure B, a real algebraic curve. Thus we can find a subset $\hat{B}$ of B, also Zariski-dense in B, contained in some $\psi_\mathbf{c}(\mathbf{D_c})$. It will suffice to know that $\hat{B}$ is infinite. Then $\hat{B} = \psi_\mathbf{c}(E)$ for some infinite subset E of $\mathbf{D_c}$.

Now (6.1) shows that the components of $\mathbf{z_c}$ lie in $\Phi = \mathbf{C}(x_{1,\mathbf{c}}, \dots, x_{2g,\mathbf{c}}, \mathbf{f}_{1,\mathbf{c}}, \dots, \mathbf{f}_{2g,\mathbf{c}})$. But if we restrict to $\varphi_\mathbf{c}^{-1}(E)$, then Φ has transcendence degree at most 1 over $\mathbf{C}(\mathbf{f}_{1,\mathbf{c}}, \dots, \mathbf{f}_{2g,\mathbf{c}})$. It follows that the components of $\mathbf{z_c}$ are algebraically dependent over $\mathbf{C}(\mathbf{f}_{1,\mathbf{c}}, \dots, \mathbf{f}_{2g,\mathbf{c}})$ on $\varphi_\mathbf{c}^{-1}(E)$. More precisely, with independent variables $\mathbf{T}_1, \dots, \mathbf{T}_{2g}, \mathbf{T}_\mathbf{z}$, there exists a polynomial A in $\mathbf{C}[\mathbf{T}_1, \dots, \mathbf{T}_{2g}, \mathbf{T}_\mathbf{z}]$ such that the relation $A(\mathbf{f}_{1,\mathbf{c}}, \dots, \mathbf{f}_{2g,\mathbf{c}}, \mathbf{z_c}) = 0$ holds on $\varphi_\mathbf{c}^{-1}(E)$ and $A(\mathbf{f}_{1,\mathbf{c}}, \dots, \mathbf{f}_{2g,\mathbf{c}}, \mathbf{T}_\mathbf{z})$ is not identically zero in $\mathbf{C}(\mathbf{f}_{1,\mathbf{c}}, \dots, \mathbf{f}_{2g,\mathbf{c}})[\mathbf{T}_\mathbf{z}]$. By a standard principle for analytic functions ("Identity Theorem" or [42] p. 85) this relation persists on all of $\mathbf{N_c}$. And now we have a contradiction with Lemma 6.1. Thus the present lemma is proved. □

We are all set up for an efficient application of Lemma 3.1. It will turn out that every $\mathbf{c}$ in Proposition 2.1 leads to many rational points on S, and of course we have to estimate their denominator. This we do in the next section.

7. Orders of torsion.

In [53] we used a result of David [23] about orders of torsion points on a principally polarized simple abelian variety of dimension say g. While our own $A(T)$ in Proposition 2.1 is generically simple, some specializations $A(T(\mathbf{c}))$ may well not be simple. Perhaps certain conjectures of André-Oort type lead in that case to at most finitely many possibilities for $\mathbf{c}$, as required in our original Proposition 2.1. In [53] we avoided such considerations by exploiting the "obstruction subgroup" B that [23] provides. There we had $g = 2$, and so if B is an elliptic curve we can reduce to the case $g = 1$. But for general g our B may well not be principally polarized. This sort of problem was already encountered in [47] (where it was solved by doing another transcendence argument using lower bounds for Hilbert functions) and [44]. Here we use some relatively elementary lemmas in [44] to obtain the following extension of David's result to all principally polarized abelian varieties, simple or not; this should be useful in other contexts (see [20] for example). We have not troubled to obtain good dependence on g. Actually, a sharpening of Proposition 7.1, proved along similar lines, has recently been obtained by G. Rémond; see Proposition 2.9 (p.468) of [60].

Proposition 7.1. *There is a constant $c = c(g)$ with the following property. Let A be a principally polarized abelian variety of dimension g defined over a number field K and let P be a point on A with finite order N. Then*

$$N \ \leq \ c([K(P) : \mathbf{Q}] \max\{1, h(A)\})^{\tilde{G}}$$

for $\tilde{G} = 8^g g!^2$ and the semistable Faltings height $h(A)$.

Proof. This is of course by induction on g. The case $g = 1$ does follow from Théorème 1.2 (p.121) of [23]. So assume it true for dimension strictly less than some $g \geq 2$.

The arguments of [23] (p.123) show that it suffices to take $A = A(\tau)$ in the notation there. Now consulting equation (28) of [23] (p.156) we find an algebraic subgroup $B \neq A$ of A. In fact Philippon's multiplicity estimate used there (p.159) guarantees that B is connected; that is, an abelian subvariety. If $B = 0$ then the arguments around equation (29) of [23] (p.156) give the bound for N as in Théorème 2.2 [23] (p.123), namely $N \leq c(d_A^{3/2} d_P h_A^{3/2})^\kappa$ for any fixed $\kappa > g$, where $d_A = [K : \mathbf{Q}]$, $d_P = [K(P) : K]$, $h_A = \max\{1, h(A)\}$. Here as in the rest of the proof we use c indiscriminately for any constant depending only on g.

So it remains to treat the case $0 \neq B \neq A$, with B of dimension say b. We note by Lemma 2.2 of [44] (p.414) that B is defined over an extension K_B of K of degree at most c. And we get the estimate $T^{g-b} \Delta L^b \leq c(LN^2)^g$ from (28) of [23]. Here Δ is the degree of B in the embedding divided by $b!$ as in [44] (p.410), and T, L, N (not our N) are defined earlier in (17) of [23] (p.152). As T, L, N^2 are of the same order of magnitude up to logarithms, we find

$$\Delta \leq c(d_A d_P h_A)^\kappa \tag{7.1}$$

for any fixed $\kappa > g$.

We next apply Lemma 1.4 of [44] (p.413) to find another abelian subvariety B' in A (so also defined over an extension K'_B of K of degree at most c) together with an isogeny ι from $B \times B'$ to A, defined over K, of degree at most Δ^2. Further by Lemma 1.3 of [44] (p.413) B' has degree at most Δ. In the opposite direction there is an isogeny $\tilde{\iota}$ from A to $B \times B'$, defined over an extension of K of degree at most c by Lemma 2.1 of [44] (p.414), with degree at most $(\Delta^2)^{2g-1}$. Thus by standard properties of Faltings heights we have

$$\max\{h(B), h(B')\} \ \leq \ h(B \times B') + c \ \leq \ h_A + \frac{1}{2} \log(\Delta^{4g-2}) + c \ \leq \ h_A + c \log \Delta.$$

We now use Lemma 4.3 of [44] (p.425) to deal with the polarization of B. As Δ is the degree of the polarization on B induced by that of A (see for example Lemma 1.1 of [44] p.411), we find an isogeny ι_0 of degree at most Δ from B to a principally polarized B_0; further B_0 (and so ι_0 too) is defined over an extension K_0 of K_B of degree at most $c\Delta^{2b} \leq c\Delta^{2g-2}$. Similarly we get an isogeny ι'_0 of degree at most Δ from B' to a principally polarized B'_0 ; further B'_0 (and so ι'_0 too) is defined over an extension K'_0 of K'_B of degree at most $c\Delta^{2g-2}$.

Now by induction the order p of the image Q_0 in B_0 under ι_0 of the projection of $\tilde{\iota}(P)$ on B satisfies $p \leq c\mathbf{d}^{8^{g-1}(g-1)!^2}$, where

$$\mathbf{d} \ = \ [K_0 : \mathbf{Q}][K_0(Q_0) : K_0]h(B_0).$$

Here

$$[K_0 : \mathbf{Q}] = [K_0 : K_B][K_B : \mathbf{Q}] \leq c\Delta^{2g-2}d_A$$

and so $[K_0(Q_0) : K_0] \leq c\Delta^{2g-2}d_P$. Also $h(B_0) \leq h_A + c\log\Delta$. We get

$$\mathbf{d} \ \leq \ c\Delta^{4g-4}d_Ad_P(h_A + \log\Delta) \ \leq \ c(d_Ad_Ph_A)^{g(4g-2)}$$

using (7.1) with $\kappa < g + (2g-1)/(4g-4)$.

We get the same bound for the order p' of the image Q_0' in B_0' under ι_0' of the projection of $\tilde{\iota}(P)$ on B'. Thus (Q_0, Q_0') has order at most pp'. Going back to A we get $N \leq pp'q$ where q is the degree of the composite isogeny from A to $B_0 \times B_0'$. We find $q \leq c\Delta^{4g}$. Now putting everything together gives what we want, provided only $\kappa < 8^{g-1}(g-1)!^2$. This completes the proof. □

We could use more directly the factorization estimates of [45] to get B, B' and ι, but the exponents involved would be astronomical. Here things are more terrestrial (and in [60] even more so).

From now on we use the standard absolute Weil height

$$h(\alpha) \ = \ \frac{1}{[\mathbf{Q}(\alpha) : \mathbf{Q}]}\sum_v \log\max\{1, |\alpha|_v\}$$

of an algebraic number α, where v runs over a suitably normalized set of valuations; and also the standard extension to vectors using the maximum norm. See for example [73] (p. 208). For the next observation we need the notation of Proposition 2.1.

Lemma 7.2. *There is a constant $c = c(C)$ with the following property. Suppose for some $\mathbf{a}$ in C that the point $P(\mathbf{a})$ on $A(T(\mathbf{a}))$ has finite order N. Then $\mathbf{a}$ is algebraic, and*

$$N \ \leq \ c([\mathbf{Q}(\mathbf{a}) : \mathbf{Q}](1 + h(\mathbf{a}))^{\tilde{G}}.$$

Proof. It is clear that $\mathbf{a}$ is algebraic, otherwise P would be identically torsion on C contradicting a hypothesis of Proposition 2.1.

For $A = A(T(\mathbf{a}))$ we can take $K = \mathbf{Q}(T(\mathbf{a}))$ in Proposition 7.1 and so $[K : \mathbf{Q}] \leq c[\mathbf{Q}(\mathbf{a}) : \mathbf{Q}]$ with c (like the others in this proof) independent of $\mathbf{a}$. Also since $(\mu_0 : \cdots : \mu_G)$ is not constant, if for example $\lambda = \mu_1/\mu_0$, then each of the affine coordinates of P is algebraic over $\mathbf{Q}(\lambda)$. Thus we deduce $[K(P(\mathbf{a})) : K] \leq c$. And then $h(A) \leq c(1 + h(\mathbf{a}))$ by well-known properties of the Faltings height (see for example the discussion on p.123 of [23]). The required result follows. □

8. Heights.

In view of the following result we can eliminate the height dependence in Lemma 7.2, still in the notation and under the assumptions of Proposition 2.1.

Lemma 8.1. *There is a constant $c = c(C)$ with the following property. Suppose for some $\mathbf{a}$ in C that the point $P(\mathbf{a})$ has finite order. Then $h(\mathbf{a}) \leq c$.*

Proof. This is a consequence of Silverman's Specialization Theorem [72] (p.197), because P is not identically of finite order (for generic t); note that our family of abelian surfaces has no non-zero isotrivial part because it is generically simple and itself non-isotrivial. □

Another advantage of bounded height is the following easy remark, already to be found in [52], concerning the sets C_0 and C^δ in section 6.

Lemma 8.2. *Let K be a number field containing the coordinates of the points of C_0 as well as a field of definition for C. For any constant c there is a positive $\delta = \delta(C, K, c)$ depending only on C, K and c with the following property. Suppose $\mathbf{a}$ is algebraic on C, not in C_0, with $h(\mathbf{a}) \le c$. Then there are at least $\frac{1}{2}[K(\mathbf{a}) : K]$ conjugates of $\mathbf{a}$ over K lying in C^δ.*

Proof. See Lemma 8.2 of [52] (p.126); however there we mistakenly omitted to mention a field of definition for C, which is needed to ensure that the conjugates of $\mathbf{a}$ stay in C. □

9. Proof of Proposition 2.1.

We will need the following result from [51].

Lemma 9.1. *Suppose $f_0, f_1, \dots, f_s$ are analytic in an open neighbourhood N of a compact set $\mathcal{Z}$ in $\mathbf{C}$ and f_0 is linearly independent of $f_1, \dots, f_s$ over $\mathbf{C}$. Then there is $c = c(f_0, f_1, \dots, f_s)$ with the following property. For any complex numbers $a_1, \dots, a_s$ the function $F = f_0 + a_1 f_1 + \cdots + a_s f_s$ has at most c different zeroes on $\mathcal{Z}$.*

Proof. See Lemma 9.1 of [51] (p.463). □

To prove Proposition 2.1 we fix any positive $\epsilon < 1/\tilde{G}$ with $\tilde{G}$ as in Proposition 7.1. We use c for various positive constants depending only on C. We have to show that there are at most finitely many $\mathbf{a}$ such that $P(\mathbf{a})$ has finite order on $A(T(\mathbf{a}))$. By Lemma 7.2 each such $\mathbf{a}$ is algebraic, say of degree $\mathcal{D} = [\mathbf{Q}(\mathbf{a}) : \mathbf{Q}]$, and thanks to Lemma 8.1 and the Northcott property it will suffice to prove that $\mathcal{D} \le c$. We will actually argue with a single $\mathbf{a}$.

Next, Lemma 7.2 together with Lemma 8.1 shows that there is a positive integer

$$N \le c\mathcal{D}^{\tilde{G}} \tag{9.1}$$

such that

$$NP(\mathbf{a}) = O. \tag{9.2}$$

Fix a number field K containing the coordinates of the points of C_0 as well as a field of definition for the curve C. By Lemma 8.1 and Lemma 8.2 the algebraic $\mathbf{a}$ has at least $\frac{1}{2}[K(\mathbf{a}) : K]$ conjugates over K in some C^δ; here $\delta = c^{-1}$. Now C^δ is contained in the union of at most c closed sets $\varphi_{\mathbf{c}}^{-1}(\mathbf{D}_{\mathbf{c}})$, and so there is $\mathbf{c}$ such that $\varphi_{\mathbf{c}}^{-1}(\mathbf{D}_{\mathbf{c}})$ contains at least $c^{-1}[K(\mathbf{a}) : K]$ conjugates $\sigma(\mathbf{a})$, so at least $c^{-1}\mathcal{D}$. And the corresponding conjugate point $\sigma(P(\mathbf{a})) = P(\sigma(\mathbf{a}))$ also satisfies $NP(\sigma(\mathbf{a})) = O$.

We claim that each point $\Psi_\sigma = \psi_{\mathbf{c}}(\varphi_{\mathbf{c}}(\sigma(\mathbf{a})))$ in $\mathbf{R}^{2g}$ lies in $\mathbf{Q}^{2g}$ and even that $N\Psi_\sigma$ lies in $\mathbf{Z}^{2g}$.

Now the function $\psi_{\mathbf{c}}$ arises from continuations $\mathbf{f}_{1,\mathbf{c}}, \dots, \mathbf{f}_{2g,\mathbf{c}}, \mathbf{z}_{\mathbf{c}}$ of the functions in section 6. We deduce from (4.2) that

$$\Theta(\tau_{\mathbf{c}}, \mathbf{u}_{\mathbf{c}}) \;=\; P(\mathbf{c})$$

on $\mathbf{N}_{\mathbf{c}}$. At $\sigma(\mathbf{a})$ this implies

$$\Theta(\tau_{\sigma(\mathbf{a})}, N\mathbf{u}_{\sigma(\mathbf{a})}) \;=\; O.$$

It follows that $N\mathbf{u}_{\sigma(\mathbf{a})}$ lies in the period lattice

$$U(\tau_{\sigma(\mathbf{a})}) \;=\; \mathbf{Z}\mathbf{e}_1 + \cdots + \mathbf{Z}\mathbf{e}_g + \mathbf{Z}\mathbf{t}_1 + \cdots + \mathbf{Z}\mathbf{t}_g.$$

After multiplying this lattice by $\rho_{\sigma(\mathbf{a})}^{-1}$ and using (4.3) we find $\mathbf{Z}\mathbf{f}_{1,\mathbf{c}} + \cdots + \mathbf{Z}\mathbf{f}_{2g,\mathbf{c}}$ at $\sigma(\mathbf{a})$. Thus (6.1) shows that $Nx_{1,\mathbf{c}}, \dots, Nx_{2g,\mathbf{c}}$ at $\sigma(\mathbf{a})$ lie in $\mathbf{Z}$. Thus indeed $N\Psi_\sigma$ lies in $\mathbf{Z}^{2g}$ as claimed.

So each Ψ_σ in the set S of section 6 has common denominator dividing N. By Lemma 3.1 and Lemma 6.2, the number of such values Ψ_σ is at most cN^ϵ. By (9.1) this is at most $c\mathcal{D}^{\tilde{G}\epsilon}$. Let $\Psi = (x_1, \dots, x_{2g})$ be one of these values. For any σ with $\Psi_\sigma = \Psi$ the value of $\mathbf{z}_{\mathbf{c}}$ at $\sigma(\mathbf{a})$ is a linear combination with coefficients $x_1, \dots, x_{2g}$ of the values of $\mathbf{f}_{1,\mathbf{c}}, \dots, \mathbf{f}_{2g,\mathbf{c}}$ at $\sigma(\mathbf{a})$. Lemma 6.1 implies that for example the first coordinate of $\mathbf{z}_{\mathbf{c}}$ is linearly independent of the first coordinates of $\mathbf{f}_{1,\mathbf{c}}, \dots, \mathbf{f}_{2g,\mathbf{c}}$. So Lemma 9.1 shows that the number of $\sigma(\mathbf{a})$ for each Ψ is at most c.

Thus the total number of $\sigma(\mathbf{a})$ is at most $c\mathcal{D}^{\tilde{G}\epsilon}$. Now this contradicts the lower bound $c^{-1}\mathcal{D}$ noted just after (9.2), provided $\mathcal{D}$ is sufficiently large. As observed near the beginning of this section, that suffices to prove Proposition 2.1.

10. Examples and the proof of Theorem 1.1 and Corollary 1.2.

It was shown in [48] (pp.294,296) that the Jacobian of (1.9) is identically simple in the sense of generic t (and even that the endomorphism ring is $\mathbf{Z}$). It has good reduction at all the points (1.7). By the equivalence of (a),(b) in Theorem 1 of Serre-Tate [71] (p.493) any torsion point yields a field unramified outside (1.7). However the point arising from (1.8) leads to ramification for example at $t = 2$; as this is already true of the trisymmetric function defined by the product of the ordinates in (1.8). Thus the point is not identically torsion and our result applies.

To deal with the Pell equation $A^2 - DB^2 = 1$ with squarefree D of degree $2g + 2$ we choose any field $\mathbb{K}$ of characteristic zero over which D is defined, and we consider as in section 1 the hyperelliptic curve H_D defined in affine $\mathbf{A}^2$ by $y^2 = D(x)$. This is singular at infinity with two points ∞^+, ∞^- on a non-singular model; we may fix them by choosing a square root e of the leading coefficient of $D(x)$ and stipulating that the function $ex^{g+1} \pm y$ has a pole of order at most g at $\infty^{\pm}$.

We now record the following fairly well-known result, for whose formulation in slightly more sophisticated language we thank a referee, who also pointed out the irrelevance of what non-singular model we choose. As in section 1 let J_D be the Jacobian.

Lemma 10.1. *The following are equivalent:*
(i) The class of $\infty^+ - \infty^-$ in J_D is of finite order,
(ii) The group of regular functions invertible on H_D is not trivial,
(iii) There exist A and $B \neq 0$ in $\mathbb{K}[x]$ such that $A^2 - DB^2 = 1$,
(iv) There exist A and $B \neq 0$ in $\mathbb{K}[x]$ and $c \neq 0$ in $\mathbb{K}$ such that $A^2 - DB^2 = c$.

Proof. This is essentially Lemma 10.1 in [53] (p.2393) extended to arbitrary genus, together with the remark, as in [53] (pp.2393,2394), that the solvability of $A^2 - DB^2 = c, B \neq 0$ for some $c \neq 0$ is equivalent to the same for $c = 1$. In fact that lemma contains some additional information about the degree of A, which we do not need here. □

To prove Theorem 1.1 we use Theorem 1.7 for the curve $\mathcal{V} = P_D = \beta(\infty^+ - \infty^-)$ on $\mathcal{A} = J_D$. At a point $\mathbf{c}$ where the Pell equation for $D(\mathbf{c})$ is solvable we get by Lemma 10.1(i),(iii) an element $P_D(\mathbf{c})$ of $\mathcal{V} \cap \mathcal{A}^{[g]}$. So this element lies in one of a finite number of abelian subschemes of codimension at least $g-1$. If one of these has codimension g, then it is a finite group scheme and so there is a positive integer N (independent of $\mathbf{c}$) such that $NP_D(\mathbf{c}) = 0$. As $NP_D \neq 0$ generically in case (a) this gives the required finiteness. And if one of these has codimension $g - 1$ then it is an elliptic subscheme $\mathcal{E}$. Now the condition that $NP_D(\mathbf{c})$ lies in $\mathcal{E}(\mathbf{c})$ again gives the required finiteness, because NP_D is not generically in $\mathcal{E}$ in this case (a).

In case (b), if nP_D lies in an elliptic curve E_D in J_D, then E_D is defined over a finite extension of $\overline{\mathbf{Q}}(C)$ (see for example Lemma 2.2 of [44] p.414). We may find an isogeny ι from E_D to some E of the form $\tilde{y}^2 = \tilde{x}(\tilde{x} - 1)(\tilde{x} - t)$; write $Q = \iota(nP_D)$. If E is not defined over $\overline{\mathbf{Q}}$ then Q is defined over $\overline{\mathbf{Q}(t)}$. Now any of the arguments in [75] (pp.68,92) suffice to give infinitely many t in $\overline{\mathbf{Q}}$ such that Q is torsion. So there are infinitely many $\mathbf{c}$ in $C(\overline{\mathbf{Q}})$ such that $P_D(\mathbf{c})$ is torsion, and this gives the main part of case (b) again by Lemma 10.1(i),(iii).

Next suppose E is defined over $\overline{\mathbf{Q}}$. If Q is not defined over $\overline{\mathbf{Q}}$, then the infinitude of $\mathbf{c}$ is immediate. If Q is defined over $\overline{\mathbf{Q}}$, then specialization has no effect; if Q is non-torsion we get no $\mathbf{c}$ at all, also as in (b), and if Q is torsion then all but finitely many $\mathbf{c}$ will do.

Finally in case (c), if P_D is torsion then here too all but finitely many $\mathbf{c}$ will do. This completes the proof of Theorem 1.1.

We now discuss some examples, which also show that all the cases (a),(b),(c) of this theorem actually turn up.

Presumably (a) holds with affine $C = \mathbf{A}^1$ for $D = x^8 + x + t$, just as we proved in [53] for $x^6 + x + t$.

And (b) holds for

$$D = x^8 + x^2 + t; \tag{10.1}$$

in fact it is by now well-known (see for example [75] pp. 68,93) that there are infinitely many τ in $\mathbf{C}$ such that Pell's equation is solvable for $x^4 + x + \tau$, and then we need only replace x by x^2. In fact this (10.1) arises because of the map from H_D to $H_{\tilde{D}}$, with $\tilde{D}(\tilde{x}) = \tilde{x}^4 + \tilde{x} + t$, defined by sending (x, y) to (x^2, y). Extending to non-singular models and taking the pull-back, we obtain a non-zero homomorphism ϕ from $J_{\tilde{D}}$ to J_D, so $E_D = \phi(J_{\tilde{D}})$ is an elliptic curve. One checks that $2P_D = \phi(P_{\tilde{D}})$ so lies in E_D.

But for the constant

$$D = x^8 + x^2 + 1 \tag{10.2}$$

Pell for $\tilde{x}^4 + \tilde{x} + 1$ is not solvable and so we get the second possibility in (b): there are no $\mathbf{c}$ such that Pell is solvable for (10.2). This also arises in terms of maps.

And as an example of (c) we take

$$D = x^8 + x^4 + t, \tag{10.3}$$

exhibit the identity (1.1) with

$$A = \frac{8x^8 + 8x^4 + 4t + 1}{4t - 1}, \quad B = \frac{8x^4 + 4}{4t - 1}$$

and specialize to arbitrary $t \neq 1/4$. This arises analogously with $\tilde{D}(\tilde{x}) = \tilde{x}^2 + \tilde{x} + t$, for which $\tilde{A}^2 - \tilde{D}\tilde{B}^2 = c$ with $\tilde{A} = \tilde{x} + \frac{1}{2}, \tilde{B} = 1$ and $c = \frac{1}{4} - t$. We can replace c by 1 using the standard trick and then replace $\tilde{x}$ by x^4. Here $4P_D = 0$ because of the function $(x^4 + y)/(x^4 - y)$.

Finally we prove Corollary 1.2. The key here, as for Theorem 1.3, is Liouville's Theorem, which says roughly that if f is integrable in elementary terms, then it suffices to use only logarithms, and in a linear way. More precisely let $\mathfrak{F}$ be a differential field (of zero characteristic) with a derivation δ, and suppose the field F of constants c with $\delta c = 0$ is algebraically closed. Then f in $\mathfrak{F}$ is elementary integrable if and only if there are $g_0, g_1 \neq 0, \ldots, g_m \neq 0$ in $\mathfrak{F}$, and $c_1, \ldots, c_m$ in F with

$$f \;=\; \delta g_0 + c_1 \frac{\delta g_1}{g_1} + \cdots + c_m \frac{\delta g_m}{g_m}. \tag{10.4}$$

See Ritt [63], Risch [61], and for a more modern exposition also Rosenlicht [65]; also Lützen [43] for an interesting history.

As we shall stress in the sequel, it is very convenient to take m minimal in (10.4). If $m \geq 1$ this implies the linear independence over $\mathbf{Q}$ of $c_1, \ldots, c_m$. For if not, then we could find p with $1 \leq p < m$ and $b_1, \ldots, b_p$ in F such that $c_1, \ldots, c_m$ are linear combinations of $b_1, \ldots, b_p$ with integer coefficients. Then substituting into (10.4) we would obtain an expression with fewer functions $h_1, \ldots, h_p$ instead of $g_1, \ldots, g_m$.

For Corollary 1.2 we take $\mathfrak{F}$ as the function field $\mathbf{C}(H_{D(\mathbf{c})})$, again with $\delta = \mathrm{d}/\mathrm{d}x$. Let $\mathbf{c}$ be in $C(\mathbf{C})$ for which there exists $E \neq 0$ in $\mathbf{C}[x]$ of degree $e \leq 2g$ such that $f = E/\sqrt{D(\mathbf{c})}$ is elementary integrable. This means that the differential form $\omega = E\mathrm{d}x/\sqrt{D(\mathbf{c})}$ has the shape

$$\omega \;=\; \mathrm{d}g_0 + c_1 \frac{\mathrm{d}g_1}{g_1} + \cdots + c_m \frac{\mathrm{d}g_m}{g_m} \tag{10.5}$$

as in (10.4).

If $e < g$ then ω has no poles on $H_{D(\mathbf{c})}$. If g_0 is not constant then $\mathrm{d}g_0$ would have a pole of order at least 2 which would not be cancelled out by any poles of $\mathrm{d}g_i/g_i$, which have order at most 1. Thus $\mathrm{d}g_0 = 0$. However any poles of $\mathrm{d}g_i/g_i$ have rational (and even integral) residues, and so by the independence of $c_1, \ldots, c_m$ there is no cancelling here either. Thus also $\mathrm{d}g_i/g_i = 0$ $(i = 1, \ldots, m)$. But then $\omega = 0$ contradicting $E \neq 0$.

So in this case $e < g$ (which corresponds to differentials of the first kind, that is, having no poles at all) there are no $\mathbf{c}$ at all such that f is elementary integrable at $\mathbf{c}$.

If $e = g$ then ω has simple poles at ∞^+, ∞^- but no other poles. So still $\mathrm{d}g_0 = 0$. And some g_i $(i = 1, \dots, m)$ is non-constant. But now the only possible zeroes or poles of g_i are at ∞^+, ∞^-. So by Lemma 10.1(i),(iii) the Pell equation for $D(\mathbf{c})$ is solvable. Thus by Theorem 1.1(a) there are at most finitely many possibilities for $\mathbf{c}$.

Finally if $e > g$ then ω has poles of order $e - g + 1 \geq 2$ at ∞^+, ∞^- but no other poles. So the only possible poles of g_0 are at ∞^+, ∞^-, of orders $e - g$.

If some g_i $(i = 1, \dots, m)$ is non-constant then we get finiteness as above. Else $\omega = \mathrm{d}g_0$; but now $g_0 = A + yB$ for A, B in $\mathbf{C}[x]$. As $e - g \leq g$ we must have $B = 0$. But then $E/\sqrt{D(\mathbf{c})} = \mathrm{d}A/\mathrm{d}x$ is clearly impossible. This completes the proof of Corollary 1.2.

Here we see that the forbidden case $e = 2g + 1$ indeed allows $g_0 = 2y$ with $E = \mathrm{d}D(\mathbf{c})/\mathrm{d}x$ (and $m = 0$).

A referee wondered if the Corollary could be strengthened by dropping the degree condition and excluding only E of the form $\frac{1}{2}B\mathrm{d}D(\mathbf{c})/\mathrm{d}x + D(\mathbf{c})\mathrm{d}B/\mathrm{d}x$ for B in $\mathbf{C}[x]$. Then $E/\sqrt{D(\mathbf{c})} = \mathrm{d}(B\sqrt{D(\mathbf{c})}/\mathrm{d}x$ is elementary integrable. The case $B = 2$ corresponds to $e = 2g + 1$ above. And indeed the proof above gives this easily on remarking that if

$$2y\omega = 2y\mathrm{d}A + B\mathrm{d}D(\mathbf{c}) + 2D(\mathbf{c})\mathrm{d}B$$

lies in $\mathbf{C}[x]\mathrm{d}x$ then $\mathrm{d}A = 0$. See also the discussion in section 2 of [76].

11. Residue divisors.

It will be very useful later to generalize the minimality discussion around (10.4) and (10.5), at least when $g_0 = 0$.

Namely let $\mathfrak{V}, \mathfrak{W}$ be vector spaces over $\mathbf{Q}$. Any element $\mathfrak{x}$ of the tensor product $\mathfrak{V} \otimes_{\mathbf{Q}} \mathfrak{W}$ has a representation

$$\mathfrak{x} = \mathfrak{v}_1\mathfrak{w}_1 + \cdots + \mathfrak{v}_m\mathfrak{w}_m \tag{11.1}$$

where for $\mathfrak{v}$ in $\mathfrak{V}$, $\mathfrak{w}$ in $\mathfrak{W}$ we abbreviate $\mathfrak{v} \otimes \mathfrak{w}$ to $\mathfrak{v}w$.

We call (11.1) a shortest representation (sometimes known as tensor rank decomposition) if there is no representation of $\mathfrak{x}$ with fewer than m (sometimes known as tensor rank) summands.

On this topic we record a few facts, almost certainly well-known.

Lemma 11.1. *The following hold:*

(i) For a given $\mathfrak{x} \neq 0$ the representation is shortest if and only if $\mathfrak{v}_1, \dots, \mathfrak{v}_m$ are linearly independent over $\mathbf{Q}$ and $\mathfrak{w}_1, \dots, \mathfrak{w}_m$ are linearly independent over $\mathbf{Q}$.

(ii) In that case, if $\mathfrak{x} = \dot{\mathfrak{v}}_1\dot{\mathfrak{w}}_1 + \cdots + \dot{\mathfrak{v}}_{\dot{m}}\dot{\mathfrak{w}}_{\dot{m}}$ is another representation (of course with $\dot{m} \geq m$), then $\mathfrak{v}_1, \dots, \mathfrak{v}_m$ are linear combinations of $\dot{\mathfrak{v}}_1, \dots, \dot{\mathfrak{v}}_{\dot{m}}$ with coefficients in $\mathbf{Q}$ and $\mathfrak{w}_1, \dots, \mathfrak{w}_m$ are linear combinations of $\dot{\mathfrak{w}}_1, \dots, \dot{\mathfrak{w}}_{\dot{m}}$ with coefficients in $\mathbf{Q}$.

Proof. For (i) the "only if" part is easy; for example if $\mathfrak{v}_1, \dots, \mathfrak{v}_m$ are dependent then we may shorten (11.1) (as we did with (10.4) above).

For the "if" part we use the dual space $\mathfrak{V}^*$ of all homomorphisms from $\mathfrak{V}$ to $\mathbf{Q}$. An f in $\mathfrak{V}^*$ extends to $\mathfrak{V} \otimes_{\mathbf{Q}} \mathfrak{W}$ in (11.1) by

$$f(\mathfrak{x}) = f(\mathfrak{v}_1)\mathfrak{w}_1 + \cdots + f(\mathfrak{v}_m)\mathfrak{w}_m \tag{11.2}$$

in $\mathfrak{W}$ (for example by the universal property).

Suppose there is a shorter representation $\mathfrak{x} = \mathfrak{v}'_1\mathfrak{w}'_1 + \cdots + \mathfrak{v}'_n\mathfrak{w}'_n$ with $n < m$. Pick any f in $\mathfrak{V}^*$ killing $\mathfrak{v}'_1, \dots, \mathfrak{v}'_n$. Then $f(\mathfrak{x}) = 0$ in (11.2) and so by the independence of $\mathfrak{w}_1, \dots, \mathfrak{w}_m$ we see that f kills $\mathfrak{v}_1, \dots, \mathfrak{v}_m$. As f was arbitrary this implies that $\mathfrak{v}_1, \dots, \mathfrak{v}_m$ are combinations of $\mathfrak{v}'_1, \dots, \mathfrak{v}'_n$, impossible because the former are also independent.

We do (ii) similarly with f killing $\dot{\mathfrak{v}}_1, \dots, \dot{\mathfrak{v}}_{\dot{m}}$. This completes the proof. □

So far we used this only for $\mathfrak{V} = \mathbf{C}$ and $\mathfrak{W}$ as the space of differentials on a curve. When this curve X is defined over a field $\mathfrak{V} = \mathbb{K}$ of characteristic zero, and ω is a differential on X

with residues in $\mathbb{K}$, then we define the residue divisor (compare also Serre [69] p.4, for which we thank Daniel Bertrand)

$$\mathrm{Res}\ \omega = \sum_P (\mathrm{res}_P \omega) P$$

taken over all points P of X; now $\mathfrak{W}$ is the group of divisors on X itself tensored with $\mathbf{Q}$.

For example we have

$$\mathrm{Res}(\mathrm{d}g) = 0, \quad \mathrm{Res}\left(\frac{\mathrm{d}g}{g}\right) = (g)$$

for the divisor (g) of g, and as in (21.8) on the curve $y^2 = x^3 - x$

$$\mathrm{Res}\left(\frac{x\mathrm{d}x}{(x^2-t^2)\sqrt{x^3-x}}\right) \ = \ \rho_1 D_1 + \rho_2 D_2 \tag{11.3}$$

with

$$\rho_1 = \frac{1}{2s}, \ \ \rho_2 = -\frac{i}{2s}, \quad D_1 = P - R, \ \ D_2 = Q - S$$

for

$$P = (t, s), \ Q = (-t, is), \ R = (t, -s), \ S = (-t, -is)$$

and $s^2 = t^3 - t$.

In general write $R = \sum_P \mathbf{Z}(\mathrm{res}_P \omega)$ for the subgroup of $\mathbb{K}$ generated by all residues of ω. If $R \neq 0$ with rank $m \geq 1$, it is rather convenient to choose $\rho_1, \ldots, \rho_m$ in R tensored with $\mathbf{Q}$ such that R is contained in $\mathbf{Z}\rho_1 + \cdots + \mathbf{Z}\rho_m$ with finite index; this we call an *over-basis* of R (note that $\rho_1, \ldots, \rho_m$ need not themselves be residues).

Now there are integers a_{iP} with $\mathrm{res}_P \omega = \sum_{i=1}^m a_{iP}\rho_i$, and the definition of R implies that the matrix with entries a_{iP} has rank m. Also from $\sum_P \mathrm{res}_P \omega = 0$ follows $\sum_P a_{iP} = 0$, so that

$$\mathrm{Res}\ \omega \ = \ \rho_1 D_1 + \cdots + \rho_m D_m \tag{11.4}$$

for genuine divisors $D_i = \sum_P a_{iP} P$ of degree zero. Here $D_1, \ldots, D_m$ are linearly independent over $\mathbf{Q}$, and so from Lemma 11.1(i) we see that the representation (11.4) is automatically shortest.

12. Elimination of non-simple poles.

We show here that it suffices to prove Proposition 1.4 when the associated differential $\varpi = f\mathrm{d}x$ is of the third kind. We have temporarily changed from the notation ω to "calligraphic" ϖ to emphasize that we are taking $\mathbb{K}$ as $\overline{\mathbf{Q}}(C)$ at the moment. Similarly we use $\mathcal{P}$ in place of P for points, $\mathcal{D}$ in place of D for divisors, and so on.

This step seems to be related to Davenport's fifth obstacle. By taking a finite covering of C we can assume that all the poles of ϖ are defined over $\overline{\mathbf{Q}}(C)$.

Suppose that the simple poles of ϖ are among $\mathcal{P}_1, \ldots, \mathcal{P}_d$, and the non-simple poles at $\mathcal{P}'_1, \ldots, \mathcal{P}'_e$, of orders $-w_1 \geq 2, \ldots, -w_e \geq 2$ respectively. Let $\mathbf{c}$ in $C(\mathbf{C})$ be such that the specialization $\varpi(\mathbf{c})$ is integrable. Then we have an expression

$$\varpi(\mathbf{c}) \ = \ \mathrm{d}g_0^{(\mathbf{c})} + \sum_{i=1}^m c_i^{(\mathbf{c})} \frac{\mathrm{d}g_i^{(\mathbf{c})}}{g_i^{(\mathbf{c})}} \tag{12.1}$$

as in (10.5) for $c_1^{(\mathbf{c})}, \ldots, c_m^{(\mathbf{c})}$ in $\mathbf{C}$ and $g_0^{(\mathbf{c})}, g_1^{(\mathbf{c})}, \ldots, g_m^{(\mathbf{c})}$ in $\mathbf{C}(\mathcal{X}(\mathbf{c}))$. Here the superscript $(\mathbf{c})$, which unfortunately now seems necessary, indicates that the dependence on $\mathbf{c}$ is not necessarily algebraic, unlike $\mathcal{X}(\mathbf{c}), \varpi(\mathbf{c})$ - however we usually refrain from putting a superscript on $m = m^{(\mathbf{c})}$ and other similarly occurring integers or rationals, as the notation would get too cumbersome.

By reduction theory we can suppose that the only simple poles of $\varpi(\mathbf{c})$ are among the specialized $\mathcal{P}_1(\mathbf{c}), \ldots, \mathcal{P}_d(\mathbf{c})$ and the only non-simple poles at $\mathcal{P}'_1(\mathbf{c}), \ldots, \mathcal{P}'_e(\mathbf{c})$, still of orders $-w_1, \ldots, -w_e$. Then $g_0^{(\mathbf{c})}$ in (12.1) must have poles of orders $-w_1 - 1, \ldots, -w_e - 1$ at $\mathcal{P}'_1(\mathbf{c}), \ldots, \mathcal{P}'_e(\mathbf{c})$ and no other poles. Fix basis elements $f_0 = 1, f_1, \ldots, f_r$ of the linear space

$$\mathfrak{L}((-w_1 - 1)\mathcal{P}'_1 + \cdots + (-w_e - 1)\mathcal{P}'_e)$$

of elements of $\overline{\mathbf{Q}}(C)$ with poles of orders at most $-w_1-1,\dots,-w_e-1$ at $\mathcal{P}_1',\dots,\mathcal{P}_e'$ and no other poles. Then $f_0(\mathbf{c})=1, f_1(\mathbf{c}),\dots,f_r(\mathbf{c})$ are basis elements of the specialized space

$$\mathfrak{L}((-w_1-1)\mathcal{P}_1'(\mathbf{c})+\cdots+(-w_e-1)\mathcal{P}_e'(\mathbf{c})).$$

We can assume $g_0^{(\mathbf{c})}=\sum_{i=1}^r a_i^{(\mathbf{c})}f_i(\mathbf{c})$ (i.e. no f_0) for complex coefficients $a_i^{(\mathbf{c})}$; most of $g_0^{(\mathbf{c})}$ depends algebraically on $\mathbf{c}$. So $\omega(\mathbf{c})-\sum_{i=1}^r a_i^{(\mathbf{c})}\mathrm{d}f_i(\mathbf{c})$ is of the third kind.

Consider the generic condition that $\varpi-\sum_{i=1}^r a_i\mathrm{d}f_i$ is of the third kind. This amounts to a set of linear equations in the a_i over $\overline{\mathbf{Q}}(C)$. The specialized equations have a solution, and so we can assume that the generic equations also have a solution, else looking at ranks would give the finiteness of the $\mathbf{c}$ at once. In fact this latter solution is unique, otherwise we could find $b_1,\dots,b_r$ not all zero in $\overline{\mathbf{Q}}(C)$ such that $\sum_{i=1}^r b_i\mathrm{d}f_i=\mathrm{d}(\sum_{i=1}^r b_if_i)$ would be of the third kind. As it has no residues it would have to be a differential of the first kind. But the only exact differential of the first kind is zero. Thus $\sum_{i=1}^r b_if_i=b_0$ so all $b_i=0$ a contradiction.

Thus again by looking at ranks we can assume that the specialized equations also have a unique solution, and as $\varpi(\mathbf{c})-\sum_{i=1}^r a_i(\mathbf{c})\mathrm{d}f_i(\mathbf{c})$ is of the third kind, we conclude that the $a_i^{(\mathbf{c})}=a_i(\mathbf{c})$ also depend algebraically on $\mathbf{c}$. Now

$$\varpi'=\varpi-\sum_{i=1}^r a_i\mathrm{d}f_i \tag{12.2}$$

is of the third kind. Thus Proposition 1.4 for ϖ' implies Proposition 1.4 for ϖ.

As the above arguments do not mention the quantity D in Proposition 1.4, they are capable of wider application; we will see this in sections 13,14,17,19 and 20.

Remark. One may wonder about an analogue of Davenport's Assertion when "elementary integrable" is replaced by "exact". This corresponds to just $\varpi(\mathbf{c})=\mathrm{d}g_0^{(\mathbf{c})}$ in (12.1). The analogue of the above arguments goes through, showing that it suffices to treat ϖ of the third kind. But then clearly $\varpi(\mathbf{c})=0$, so that the finiteness is easy (and effective).

13. Proof of Proposition 1.4.

From section 12 we can assume that ϖ is of the third kind.

We need two preliminary observations about the relation group of elements $r_1,\dots,r_p$ of an additive group; this is defined as the set of $(m_1,\dots,m_p)$ in $\mathbf{Z}^p$ with $m_1r_1+\cdots+m_pr_p=0$.

Lemma 13.1. *Let A_0 be an abelian variety defined over a number field K, and denote by w the order of the torsion part of $A_0(K)$. Let $\hat{h}$ on $A_0(K)$ be a Néron-Tate height with respect to some polarization, and denote by $\delta>0$ the minimum of $\hat{h}$ on the non-torsion part of $A_0(K)$. Let $M_1,\dots,M_p$ be in $A_0(K)$ with $\hat{h}(M_i)\le\Delta$ $(i=1,\dots,p)$ for some $\Delta\ge\delta$. Then the relation group of $M_1,\dots,M_p$ has basis elements whose supremum norms are at most $p^{p-1}w(\Delta/\delta)^{(p-1)/2}$.*

Proof. This is Theorem A of [46] (p.257). □

Lemma 13.2. *Let $\mathcal{A}$ be an abelian variety over $\overline{\mathbf{Q}}(C)$ with no non-zero isotrivial part, and let $\mathcal{P}_1,\dots,\mathcal{P}_p$ be in $\mathcal{A}(\overline{\mathbf{Q}}(C))$. Then the $\mathbf{c}$ in $C(\overline{\mathbf{Q}})$ such that the relation group of the specialized points $\mathcal{P}_1(\mathbf{c}),\dots,\mathcal{P}_p(\mathbf{c})$ on the specialized $\mathcal{A}(\mathbf{c})$ has rank strictly larger than that of the relation group of $\mathcal{P}_1,\dots,\mathcal{P}_p$ have height bounded above.*

Proof. Let r be the rank of the relation group of $\mathcal{P}_1,\dots,\mathcal{P}_p$. Then we may suppose $r<p$ and also that $\mathcal{P}_{r+1},\dots,\mathcal{P}_p$ are independent. The relation group of $\mathcal{P}_1(\mathbf{c}),\dots,\mathcal{P}_p(\mathbf{c})$ has rank strictly larger than r, and so $\mathcal{P}_{r+1}(\mathbf{c}),\dots,\mathcal{P}_p(\mathbf{c})$ must be dependent. Now the standard form of Silverman's Theorem [72] gives what we want. □

With a view also to proving Theorem 1.3 we now take a fixed differential ϖ on our curve $\mathcal{X}$ defined over $\overline{\mathbf{Q}}(C)$.

If $\mathbf{c}$ in $C(\mathbf{C})$ is such that the specialized $\varpi(\mathbf{c})$ is elementary integrable, then we have an expression

$$\varpi(\mathbf{c}) = \sum_{i=1}^{m} c_i^{(\mathbf{c})} \frac{\mathrm{d}g_i^{(\mathbf{c})}}{g_i^{(\mathbf{c})}} \tag{13.1}$$

with $m = m^{(\mathbf{c})}$ as in (12.1) but now $\mathrm{d}g_0^{(\mathbf{c})} = 0$.

We choose (13.1) shortest as before, so that the $c_1^{(\mathbf{c})}, \dots, c_m^{(\mathbf{c})}$ (if $m \geq 1$) are linearly independent over $\mathbf{Q}$.

Now the zeroes and poles of the $g_1^{(\mathbf{c})}, \dots, g_m^{(\mathbf{c})}$ (if $m \geq 1$) give rise to poles of $\varpi(\mathbf{c})$ of order at most 1. If the poles of order at most 1 of ϖ are among $\mathcal{P}_1, \dots, \mathcal{P}_d$ (for some $d \geq 1$), then we may assume that the poles of order at most 1 of $\varpi(\mathbf{c})$ are among the specialized $\mathcal{P}_1(\mathbf{c}), \dots, \mathcal{P}_d(\mathbf{c})$. It follows that the divisors of $g_i^{(\mathbf{c})}$ have the form

$$(g_i^{(\mathbf{c})}) = \sum_{j=1}^{d} N_{ij} \mathcal{P}_j(\mathbf{c}) \quad (i = 1, \dots, m) \tag{13.2}$$

with integer coefficients N_{ij} (here we also omit the superscript) satisfying of course

$$\sum_{j=1}^{d} N_{ij} = 0 \quad (i = 1, \dots, m) \tag{13.3}$$

in $\mathbf{Z}$ (if $m \geq 1$).

We note that the matrix with rows $\mathbf{N}_i = (N_{i1}, \dots, N_{id})$ $(i = 1, \dots, m)$ has full rank m (if $m \geq 1$). Otherwise by (13.2) the $g_1^{(\mathbf{c})}, \dots, g_m^{(\mathbf{c})}$ would be multiplicatively dependent modulo constants. Then $\mathrm{d}g_1^{(\mathbf{c})}/g_1^{(\mathbf{c})}, \dots, \mathrm{d}g_m^{(\mathbf{c})}/g_m^{(\mathbf{c})}$ would be linearly dependent over $\mathbf{Q}$, and (13.1) would not be shortest.

Thus by (13.3) we have

$$m \leq d - 1 \tag{13.4}$$

(even if $m = 0$).

Now we can prove Proposition 1.4.

First we note that if $\mathcal{X}$ has genus 0 then for example by using a rational parametrization we see that ϖ itself is generically elementary integrable. So we henceforth assume that $\mathcal{X}$ has genus $g \geq 1$. The Jacobian $\mathcal{J}$ of $\mathcal{X}$ has dimension g, and by reduction theory we can assume the same for the Jacobians $\mathcal{J}(\mathbf{c})$ of the specializations $\mathcal{X}(\mathbf{c})$.

We use induction on d. If $d = 1$ the assertion is trivial by (13.4) even without bounding the degree, for then $m = 0$ and as before, any pole of $g_0^{(\mathbf{c})}$ has order at least 2 and so $\mathrm{d}g_0^{(\mathbf{c})} = 0$. Thus the integrability of $\varpi(\mathbf{c})$ implies $\varpi(\mathbf{c}) = 0$, which by $\varpi \neq 0$ would lead to finitely many $\mathbf{c}$.

So we can assume that the poles of ϖ are among $\mathcal{P}_1, \dots, \mathcal{P}_d$ for some $d \geq 2$, as before defined over $\overline{\mathbf{Q}}(C)$.

If $\mathbf{c}$ is a point as in Proposition 1.4, then we have an expression (12.1). We choose m minimal as before. As above we may assume $m \geq 1$. Thus $c_1^{(\mathbf{c})}, \dots, c_m^{(\mathbf{c})}$ are linearly independent over $\mathbf{Q}$.

We also have (13.2) and (13.3). Thus for example

$$\sum_{j=1}^{d-1} N_{ij} [\mathcal{P}_j(\mathbf{c}) - \mathcal{P}_d(\mathbf{c})] \;=\; 0 \quad (i = 1, \dots, m) \tag{13.5}$$

are m independent linear relations among the divisor classes $[\mathcal{P}_j(\mathbf{c}) - \mathcal{P}_d(\mathbf{c})]$ $(j = 1, \dots, d-1)$ considered as points on $\mathcal{J}(\mathbf{c})$.

If it happens that $\mathcal{J}$ has no non-zero isotrivial part (as in the situation of Lemma 8.1 for example) then we can finish at once. Namely the relation group of the $[\mathcal{P}_j - \mathcal{P}_d]$ $(j = 1, \dots, d-1)$ is naturally a subgroup of that of the $[\mathcal{P}_j(\mathbf{c}) - \mathcal{P}_d(\mathbf{c})]$ $(j = 1, \dots, d-1)$. There are now two possibilities.

If the two groups have the same rank, then just $m \geq 1$ shows that the $[\mathcal{P}_j - \mathcal{P}_d]$ are linearly dependent on $\mathcal{J}$. Thus there is non-constant f with divisor $\sum_{j=1}^{d-1} n_j(\mathcal{P}_j - \mathcal{P}_d)$. We may assume $n_{d-1} \neq 0$, and then we consider $\varpi' = \varpi - (\hat{\varrho}_{d-1}/n_{d-1})\mathrm{d}f/f$, where calligraphic $\hat{\varrho}_{d-1}$ is the residue $\mathrm{res}_{\mathcal{P}_{d-1}}\varpi$ of ϖ at $\mathcal{P}_{d-1}$. This has poles among $\mathcal{P}_1, \ldots, \mathcal{P}_{d-1}$; and $\varpi'(\mathbf{c})$ is elementary integrable. So by induction on d we get at most finitely many $\mathbf{c}$ unless ϖ' is elementary integrable. But then so would ϖ be, contrary to hypothesis.

If the two relation groups above do not have the same rank, then Lemma 13.2 implies that $\mathbf{c}$ has height bounded above. As by assumption its degree is also bounded above (by D), Northcott now gives the finiteness we want, at least in this special case.

In general there is an isogeny from $\mathcal{J}$ to $\mathcal{A} \times A_0$, where $\mathcal{A}$ has no non-zero isotrivial part and A_0 is isotrivial (or even "trivial", i.e. constant). Denote by $\pi_{\mathcal{A}}, \pi_0$ the corresponding maps from $\mathcal{J}$ to $\mathcal{A}, A_0$ respectively. It will cause no confusion when we write $\pi_{\mathcal{A}}, \pi_0$ also after specialization, that is, from $\mathcal{J}(\mathbf{c})$ to $\mathcal{A}(\mathbf{c}), A_0$ (indeed it might cause confusion when we didn't).

Projecting (13.5) to $\mathcal{A}(\mathbf{c})$ gives

$$\sum_{j=1}^{d-1} N_{ij}\pi_{\mathcal{A}}[\mathcal{P}_j(\mathbf{c}) - \mathcal{P}_d(\mathbf{c})] \;=\; 0 \quad (i = 1, \ldots, m).$$

Thus by Lemma 13.2 as above the height $h(\mathbf{c})$ is bounded and we can conclude, unless the

$$\sum_{j=1}^{d-1} N_{ij}\pi_{\mathcal{A}}[\mathcal{P}_j - \mathcal{P}_d] \quad (i = 1, \ldots, m). \tag{13.6}$$

themselves are torsion. So we can assume this.

Let q be the rank of the group generated by these $\pi_{\mathcal{A}}[\mathcal{P}_j - \mathcal{P}_d]$ $(j = 1, \ldots, d-1)$. Then there are basis elements $\mathbf{f}_1, \ldots, \mathbf{f}_{d-1-q}$ of their relation group F in $\mathbf{Z}^{d-1}$, with norms $\ll 1$, where the implied constant (here and subsequently) is independent of $\mathbf{c}$. We can find independent $\mathbf{f}'_1, \ldots, \mathbf{f}'_q$ in $\mathbf{Z}^{d-1}$ orthogonal to $\mathbf{f}_1, \ldots, \mathbf{f}_{d-1-q}$, also with norms $\ll 1$. We deduce from (13.6) that $\mathbf{N}_1, \ldots, \mathbf{N}_m$ are orthogonal to $\mathbf{f}'_1, \ldots, \mathbf{f}'_q$.

Write $\hat{\varrho}_1, \ldots, \hat{\varrho}_d$ for the residues of ω at $\mathcal{P}_1, \ldots, \mathcal{P}_d$ respectively. Then (12.1) and (13.2) give for the specialized residues

$$\hat{\varrho}_j(\mathbf{c}) = \sum_{i=1}^{m} c_i^{(\mathbf{c})} N_{ij} \quad (j = 1, \ldots, d). \tag{13.7}$$

It follows that $(\hat{\varrho}_1(\mathbf{c}), \ldots, \hat{\varrho}_{d-1}(\mathbf{c}))$ is orthogonal to $\mathbf{f}'_1, \ldots, \mathbf{f}'_q$.

If $(\hat{\varrho}_1, \ldots, \hat{\varrho}_{d-1})$ is not orthogonal to $\mathbf{f}'_1, \ldots, \mathbf{f}'_q$, then we get a non-trivial equation for $\mathbf{c}$ which determines it.

Thus we can suppose that $(\hat{\varrho}_1, \ldots, \hat{\varrho}_{d-1})$ is orthogonal to $\mathbf{f}'_1, \ldots, \mathbf{f}'_q$. Now we play a similar game with the relation group U in $\mathbf{Z}^{d-1}$ of $\hat{\varrho}_1, \ldots, \hat{\varrho}_{d-1}$. If the group generated by them has rank s (note that $s \geq 1$ because the $d-1 \geq 1$ residues are non-zero) then U has basis elements $\mathbf{u}_1, \ldots, \mathbf{u}_{d-1-s}$, with norms $\ll 1$. We can find independent $\mathbf{u}'_t = (u'_{t1}, \ldots, u'_{t,d-1})$ $(t = 1, \ldots, s)$ in $\mathbf{Z}^{d-1}$ orthogonal to $\mathbf{u}_1, \ldots, \mathbf{u}_{d-1-s}$, also with norms $\ll 1$. Now $\mathbf{f}'_1, \ldots, \mathbf{f}'_q$ lie in U, so are orthogonal to $\mathbf{u}'_1, \ldots, \mathbf{u}'_s$. Therefore $\mathbf{u}'_1, \ldots, \mathbf{u}'_s$ lie in $F \otimes \mathbf{Q}$. Thus their multiples by a positive integer $w_0 \ll 1$ lie in F itself. This means

$$w_0 \sum_{j=1}^{d-1} u'_{tj}\pi_{\mathcal{A}}[\mathcal{P}_j - \mathcal{P}_d] \;=\; 0 \quad (t = 1, \ldots, s). \tag{13.8}$$

We next project (13.5) to the isotrivial part A_0, giving

$$\sum_{j=1}^{d-1} N_{ij}\pi_0[\mathcal{P}_j(\mathbf{c}) - \mathcal{P}_d(\mathbf{c})] \;=\; 0 \quad (i = 1, \ldots, m). \tag{13.9}$$

Let r be the rank of the group generated by these $\pi_0[\mathcal{P}_j(\mathbf{c}) - \mathcal{P}_d(\mathbf{c})]$ $(j = 1, \ldots, d-1)$. Fix a polarization on A. By Lemma 13.1 there are basis elements $\mathbf{g}_1^{(\mathbf{c})}, \ldots, \mathbf{g}_{d-1-r}^{(\mathbf{c})}$ of their relation group G in $\mathbf{Z}^{d-1}$ with norms $\ll w(\Delta/\delta)^{(d-2)/2}$.

We are now in $A_0(K)$ for A_0 fixed and $[K:\mathbf{Q}] \le D \ll 1$. Therefore we now have $w \ll 1$ and $\delta \gg 1$ (see for example the discussion round (13),(14) of [46] pp. 255,256). It is not difficult to see also that $\Delta \ll h(\mathbf{c}) + 1$. Thus the norms are at most $\mathcal{N} \ll (h(\mathbf{c})+1)^\kappa$ for $\kappa = (d-2)/2$.

Assume for the moment $r \neq 0$. By Siegel's Lemma we can find independent $\mathbf{g}_1'^{(\mathbf{c})}, \dots, \mathbf{g}_r'^{(\mathbf{c})}$ in $\mathbf{Z}^{d-1}$ orthogonal to $\mathbf{g}_1^{(\mathbf{c})}, \dots, \mathbf{g}_{d-1-r}^{(\mathbf{c})}$, with norms at most

$$\mathcal{N}' \ \ll \ \mathcal{N}^{d-1-r} \ \ll \ (h(\mathbf{c})+1)^{\kappa'}, \tag{13.10}$$

with say $\kappa' = \kappa d$.

By (13.9) the $\mathbf{N}_1, \dots \mathbf{N}_m$ lie in G.

Now (13.7) implies that $(\hat\varrho_1(\mathbf{c}), \dots, \hat\varrho_{d-1}(\mathbf{c}))$ is orthogonal to $\mathbf{g}_1'^{(\mathbf{c})}, \dots, \mathbf{g}_r'^{(\mathbf{c})}$.

If $(\hat\varrho_1, \dots, \hat\varrho_{d-1})$ is not orthogonal to $\mathbf{g}_1'^{(\mathbf{c})}, \dots, \mathbf{g}_r'^{(\mathbf{c})}$, then we get a non-trivial equation for $\mathbf{c}$ which implies easily $h(\mathbf{c}) \ll \log \mathcal{N}' + 1$. By (13.10) this implies

$$h(\mathbf{c}) \ \ll \ \log(h(\mathbf{c})+1) + 1.$$

Thus $h(\mathbf{c}) \ll 1$ and we are after all done by Northcott.

Thus we can suppose that $(\hat\varrho_1, \dots, \hat\varrho_{d-1})$ is orthogonal to $\mathbf{g}_1'^{(\mathbf{c})}, \dots, \mathbf{g}_r'^{(\mathbf{c})}$. As above we find that $\mathbf{g}_1'^{(\mathbf{c})}, \dots, \mathbf{g}_r'^{(\mathbf{c})}$ lie in U, so are orthogonal to $\mathbf{u}_1', \dots, \mathbf{u}_s'$. Thus $\mathbf{u}_1', \dots, \mathbf{u}_s'$ lie in $G \otimes \mathbf{Q}$.

It follows that the

$$\sum_{j=1}^{d-1} u_{tj}' \pi_0[\mathcal{P}_j(\mathbf{c}) - \mathcal{P}_d(\mathbf{c})] \ \ (t = 1, \dots, s) \tag{13.11}$$

are torsion, at least if $r \neq 0$.

And if $r = 0$ this follows anyway, because then all $\pi_0[\mathcal{P}_j(\mathbf{c}) - \mathcal{P}_d(\mathbf{c})]$ $(j-1, \dots, d-1)$ are torsion.

Thus on multiplying (13.11) by the w above we get zero. The resulting equations determine $\mathbf{c}$ unless they vanish identically. That is,

$$w \sum_{j=1}^{d-1} u_{tj}' \pi_0[\mathcal{P}_j - \mathcal{P}_d] \ = \ 0 \ \ (t = 1, \dots, s).$$

In conjunction with (13.8) this shows that the $[\mathcal{P}_j - \mathcal{P}_d]$ $(j = 1, \dots, d-1)$ are linearly dependent on $\mathcal{J}$. And now we can finish by induction on d as in the case $A_0 = 0$ using ϖ'.

This completes the proof of Proposition 1.4, ready for the disposal of Davenport's third obstacle.

14. Torsion points.

14.1. **Abelian varieties.** The main argument of this section shows how the simplifications of section 12 together with Proposition 1.4 lead to torsion points. The general principle is essentially classical (see Goursat [30] for example), at least for fixed integrals; we follow the formulation due to Risch [62]. Roughly speaking this says that if ω in (11.4) is elementary integrable, then the classes $[D_1], \dots, [D_m]$ are torsion. But we carry this out in the context of families. It will lead quickly to a proof of Theorem 1.3(a) when the genus $g \ge 2$ and the Jacobian $\mathcal{J}$ of $\mathcal{X}$ is simple, again without exceptions. In that case we may apply Theorem 1.7 to deduce Theorem 1.3(a). But if $g = 1$ the proof works only if if there is no complex multiplication (again without exceptions). In that case we must use generalized Jacobians and apply Theorem 1.6 instead. This partly overcomes Davenport's fourth obstacle.

With Theorem 1.3(a) in mind, we start with ϖ (again calligraphic) not elementary integrable. The arguments of section 12 show that we can assume it to be of the third kind, with poles (if any) defined over $\overline{\mathbf{Q}}(C)$, with residues also in $\overline{\mathbf{Q}}(C)$.

If ϖ is of the first kind, then it is easy to see that (13.1) can hold for at most finitely many $\mathbf{c}$. Namely, we can assume $m = m^{(\mathbf{c})} \ge 1$, and we can also assume as above that (13.1) is

shortest and so $c_1^{(\mathbf{c})}, \dots, c_m^{(\mathbf{c})}$ are linearly independent over $\mathbf{Q}$. For any P on $\mathcal{X}(\mathbf{c})$ we have

$$0 = \mathrm{res}_P \varpi(\mathbf{c}) = \sum_{i=1}^{m} c_i^{(\mathbf{c})} \mathrm{ord}_P g_i^{(\mathbf{c})}.$$

It follows that $\mathrm{ord}_P g_i^{(\mathbf{c})} = 0$ for all P, i. Thus all $g_i^{(\mathbf{c})}$ are constants, leading to $\varpi(\mathbf{c}) = 0$. As $\varpi \neq 0$ we get at once the finiteness required in Theorem 1.3(a). Compare the arguments just after (10.5).

If ϖ is elementary integrable modulo differentials of the first kind, then again we get at most finitely many $\mathbf{c}$. For then we can suppose that ϖ is already of the first kind; and still not elementary integrable. But then the arguments just above apply.

They also apply if ϖ is of the second kind (that is, all its residues are zero).

So from now on we assume that ϖ has at least one non-zero residue, and is not elementary integrable modulo differentials of the first kind.

Now if (13.1) holds for some $\mathbf{c}$ we have as above $\mathrm{res}_P \varpi(\mathbf{c}) = \sum_{i=1}^{m} c_i^{(\mathbf{c})} \mathrm{ord}_P g_i^{(\mathbf{c})}$. Denote by $\mathcal{R}(\mathbf{c})$ the (non-zero) additive group generated by the residues of $\varpi(\mathbf{c})$. Thus $\mathcal{R}(\mathbf{c})$ lies in the group generated by $c_1^{(\mathbf{c})}, \dots, c_m^{(\mathbf{c})}$. So $\mathcal{R}(\mathbf{c})$ has rank at most m. But if $\mathcal{R}(\mathbf{c})$ had rank strictly less than m, then the matrix with entries $\mathrm{ord}_P g_i^{(\mathbf{c})}$ would have rank strictly less than m. This would imply the multiplicative dependence modulo constants of the $g_i^{(\mathbf{c})}$, so the linear dependence over $\mathbf{Q}$ of the $\mathrm{d}g_i^{(\mathbf{c})}/g_i^{(\mathbf{c})}$, contradicting shortness. Thus $\mathcal{R}(\mathbf{c})$ has rank exactly m.

At the same time we can consider the group $\mathcal{R}$ generated by the residues of ϖ. Clearly by specialization this has rank at least m. If it were strictly bigger than m, then there would be a linear dependence relation not arising from specialization. This would imply that the degree $[\mathbf{Q}(\mathbf{c}) : \mathbf{Q}]$ is bounded above independently of $\mathbf{c}$. Now Proposition 1.4 leads to the required finiteness conclusion of Theorem 1.3(a). This disposes of Davenport's third obstacle.

Thus we can suppose that $m = m^{(\mathbf{c})}$ (independently of $\mathbf{c}$) is the rank of $\mathcal{R}$, and that this coincides with the rank of $\mathcal{R}(\mathbf{c})$.

We now proceed with this preliminary approach to Theorem 1.3(a) by induction on m, the case $m = 0$ corresponding to differentials of the second kind already discussed.

Let us fix over-basis elements $\varrho_1, \dots, \varrho_m$ of $\mathcal{R}$ (recall that this means $\mathcal{R}$ is of finite index in the direct sum $\mathbf{Z}\varrho_1 + \cdots + \mathbf{Z}\varrho_m$). Then $\varrho_1(\mathbf{c}), \dots, \varrho_m(\mathbf{c})$ are over-basis elements of $\mathcal{R}(\mathbf{c})$. We have a shortest representation

$$\mathrm{Res}\ \varpi = \sum_{i=1}^{m} \varrho_i \mathcal{D}_i$$

for (calligraphic) divisors $\mathcal{D}_1, \dots, \mathcal{D}_m$. By our assumptions about poles and residues, we may specialize to

$$\mathrm{Res}\ \varpi(\mathbf{c}) = \sum_{i=1}^{m} \varrho_i(\mathbf{c}) \mathcal{D}_i(\mathbf{c})$$

and this too is shortest. The latter is also $\sum_{i=1}^{m} c_i^{(\mathbf{c})}(g_i^{(\mathbf{c})})$ by (13.1). It follows from Lemma 11.1(ii) that the vector spaces over $\mathbf{Q}$ of divisors are the same. Therefore there is $N = N^{(\mathbf{c})} \geq 1$ such that the $N\mathcal{D}_i(\mathbf{c})$ are integral linear combinations of $(g_1^{(\mathbf{c})}), \dots, (g_m^{(\mathbf{c})})$. We may use the same notation for these combinations and correspondingly $c_1^{(\mathbf{c})}, \dots, c_m^{(\mathbf{c})}$ so that (13.1) continues to hold; but now

$$(g_i^{(\mathbf{c})}) = N\mathcal{D}_i(\mathbf{c}) \quad (i = 1, \dots, m). \tag{14.1}$$

And so the classes $[\mathcal{D}_i(\mathbf{c})]$ $(i = 1, \dots, m)$ are indeed torsion on the specialized Jacobian $\mathcal{J}(\mathbf{c})$. Also

$$N\varpi(\mathbf{c}) = \sum_{i=1}^{m} \varrho_i(\mathbf{c}) \frac{\mathrm{d}g_i^{(\mathbf{c})}}{g_i^{(\mathbf{c})}}. \tag{14.2}$$

Next we show that we can assume that the generic $[\mathcal{D}_1], \dots, [\mathcal{D}_m]$ are independent over $\mathbf{Z}$. In fact an integer relation $0 = \sum_{i=1}^{m} a_i[\mathcal{D}_i] = [\sum_{i=1}^{m} a_i \mathcal{D}_i]$ would lead to f with divisor $\sum_{i=1}^{m} a_i \mathcal{D}_i$.

We may assume $a_m \neq 0$, and because

$$\operatorname{Res}\left(a_m\varpi - \varrho_m\frac{\mathrm{d}f}{f}\right) \;=\; \sum_{i=1}^{m-1}(a_m\varrho_i - \varrho_m a_i)\mathcal{D}_i \tag{14.3}$$

with fewer summands, we could finish using the induction hypothesis.

So from now on in this section we will assume that $[\mathcal{D}_1],\dots,[\mathcal{D}_m]$ are independent over $\mathbf{Z}$.

Also let us suppose for the rest of this section that $\mathcal{J}$ is simple.

If the genus $g \geq 2$ we can conclude at once, because just the torsion of $[\mathcal{D}_1(\mathbf{c})]$ on $\mathcal{J}(\mathbf{c})$ gives the finiteness using Theorem 1.7, the only abelian subschemes of codimension at least $g-1$ having codimension g.

And if $g = 1$ with $m \geq 2$ then just the torsion of $([\mathcal{D}_1(\mathbf{c})],[\mathcal{D}_2(\mathbf{c})])$ on $\mathcal{J}(\mathbf{c}) \times \mathcal{J}(\mathbf{c})$ gives the finiteness using again Theorem 1.7 (this is the main result of [51]). But as we know that $[\mathcal{D}_1],[\mathcal{D}_2]$ are independent only over $\mathbf{Z}$ this argument fails when there is complex multiplication. This gap will not be filled until section 20.

What if $g = 1$ and $m = 1$? Up to now all we know is that $[\mathcal{D}_1(\mathbf{c})]$ is torsion on the elliptic curve $\mathcal{J}(\mathbf{c})$. But we already saw in section 10 that this usually happens for infinitely many $\mathbf{c}$. So we need a new argument.

14.2. **Generalized Jacobians.** The simplest example is

$$\varpi_0 \;=\; \frac{\mathrm{d}x}{(x-2)\sqrt{x(x-1)(x-t)}}$$

over $C = \mathbf{P}_1$, because the only residues are $\pm 1/\sqrt{4-2t}$, at the poles $(2, \pm\sqrt{4-2t})$. To make progress we now have to consider the zeroes of the differential; for ϖ_0 there is a single zero (of order two) at ∞.

Return to the general case $g = 1$ and $m = 1$. As ϖ has a divisor of degree $2g-2 = 0$ it certainly has a zero at some $\mathcal{Z}$, which we can also assume defined over $\overline{\mathbf{Q}}(C)$, so also $\varpi(\mathbf{c})$ vanishes at $\mathcal{Z}(\mathbf{c})$. Thus $g_1^{(\mathbf{c})}$ satisfies $g_1^{(\mathbf{c})}(\mathcal{Z}(\mathbf{c})) \neq 0$. We can suppose this value is 1, and then by (14.2) the function $g_1^{(\mathbf{c})} - 1$ has at least a double zero at $\mathcal{Z}(\mathbf{c})$. So not only is $[\mathcal{D}_1(\mathbf{c})]$ torsion on the elliptic curve $\mathcal{J}(\mathbf{c})$ but also its "narrow" class $[\mathcal{D}_1(\mathbf{c})]_{2\mathcal{Z}(\mathbf{c})}$ is torsion on its extension $\mathcal{J}(\mathbf{c})_{2\mathcal{Z}(\mathbf{c})}$ by $\mathbf{G}_\mathrm{a}$ corresponding to the divisor $2\mathcal{Z}(\mathbf{c})$ in the sense of the Appendix (this situation seems not to be classical). Now the required finiteness follows from Theorem 1.6, for it is pointed out in the Appendix that the extension $\mathcal{J}_{2\mathcal{Z}}$ (there G_2) is non-split and so the only group subschemes of positive codimension are finite or inverse images of torsion points on $\mathcal{J}$ (finitely many copies of $\mathbf{G}_\mathrm{a}$). So we get finiteness as long as $[\mathcal{D}_1]_{2\mathcal{Z}}$ is not inside such a subscheme. But then projecting down would show that $[\mathcal{D}_1]$ is torsion, a contradiction. By the way, this argument works even when there is complex multiplication.

In fact it can be shown (when $g = m = 1$) that conversely if $[\mathcal{D}_1(\mathbf{c})]_{2\mathcal{Z}(\mathbf{c})}$ is torsion on $\mathcal{J}(\mathbf{c})_{2\mathcal{Z}(\mathbf{c})}$ for some $\mathbf{c}$, then $\varpi(\mathbf{c})$ is elementary integrable. This remark can be used to construct more unlikely integrals, for example in the constant case

$$\int \frac{x+i}{x-i}\frac{\mathrm{d}x}{\sqrt{x^3-x}} \;=\; \frac{-1+i}{4}\log\left(\frac{x^2+(2+2i)\sqrt{x^3-x}+2ix-1}{x^2-(2+2i)\sqrt{x^3-x}+2ix-1}\right) \tag{14.4}$$

comes from $D_1 = P - R$ with $P = (i, 1-i)$, $R = (i, -1+i)$ and $[D_1]_{2Z}$ of order 4 with $Z = (-i, 1+i)$; the function $-f$ in brackets having divisor $4D_1$ with $\operatorname{ord}_Z(f-1) = 2$. Detmar Welz has pointed out that this is a special case of Goursat's results in [29]. Compare also (21.11).

15. Ramification and the splitting line.

We now pause to take stock and to explain the difficulties in going further and completely overcoming Davenport's fourth obstacle. Up to now we have proved Theorem 1.3(a) when the generic Jacobian $\mathcal{J}$ is simple (but ruling out CM if $g = 1$). In some sense this is a likely situation; but already Legendre (at the age of 80) showed that it is not certain.

Namely if $g = 2$ then a Jacobian can be isogenous to a product $E_1 \times E_2$ of elliptic curves. And Jacobi himself gave the family (see also [14] p.155)

$$y^2 = ax^6 + bx^4 + cx^2 + d \tag{15.1}$$

whose Jacobians are isogenous to the product of the (palindromic pair of) elliptic curves E_1, E_2 defined by

$$y_1^2 = ax_1^3 + bx_1^2 + cx_1 + d, \quad y_2^2 = dx_2^3 + cx_2^2 + bx_2 + a \tag{15.2}$$

respectively. This is a consequence of the maps

$$\phi_1(x, y) = (x_1, y_1) = (x^2, y), \quad \phi_2(x, y) = (x_2, y_2) = (x^{-2}, x^{-3}y). \tag{15.3}$$

It is then likely that E_1, E_2 are not themselves isogenous.

If this holds in the situation of section 14, so that $g = 2$ with an isogeny ι from the parametrized $\mathcal{J}$ to a product $\mathcal{E}_1 \times \mathcal{E}_2$ of non-isogenous curves, then the considerations of the previous sections can be made to succeed provided $m \geq 2$. For example we can write

$$\iota([\mathcal{D}_1]) = ([\mathcal{D}_{11}], [\mathcal{D}_{12}]), \quad \iota([\mathcal{D}_2]) = ([\mathcal{D}_{21}], [\mathcal{D}_{22}])$$

and specialize to get two torsion points on each of $\mathcal{E}_1(\mathbf{c}), \mathcal{E}_2(\mathbf{c})$. Using [51] as above on $\mathcal{E}_1$, we get finiteness unless $[\mathcal{D}_{11}], [\mathcal{D}_{21}]$ are dependent, and so essentially the same class $[\mathcal{D}'_1]$. Similarly $[D_{12}], [D_{22}]$ are essentially the same class $[\mathcal{D}'_2]$.

Now [52] on products (also a special case of Theorem 1.7) allows us to suppose that at least one of $[\mathcal{D}'_1], [\mathcal{D}'_2]$ is essentially zero.

But this contradicts the independence of $[\mathcal{D}_1], [\mathcal{D}_2]$.

What if $m = 1$? Then we can work on a suitable additive extension as in section 14. These also arise through generalized Jacobians, even for curves X of arbitrary genus over an arbitrary field. As in Serre [70] (pp. 27,76) one chooses a modulus $\mathbf{m}$, that is, a divisor $\sum_{P \in \mathbf{P}} s_P P$ with a (possibly empty) set $\mathbf{P}$ of points of X and multiplicities $s_P \geq 1$. Then $\mathrm{Jac}_{\mathbf{m}}(X)$ is the quotient of the group of divisors D on X of degree zero prime to $\mathbf{P}$ by the group of principal divisors (f) with $\mathrm{ord}_P(f - 1) \geq s_P$ for all P in $\mathbf{P}$. We denote the class of D in this quotient by $[D]_{\mathbf{m}}$. This is slightly dangerous, because $[D] = [D']$ does not imply $[D]_{\mathbf{m}} = [D']_{\mathbf{m}}$ (rather the other way round). Such things could be avoided by using $[D]_\emptyset$ corresponding to the modulus supported on the empty set but we prefer risk over pedantry. Anyway, for empty $\mathbf{P}$ one obtains the ordinary Jacobian $\mathrm{Jac}(X)$, with classes $[D]$, and for non-empty $\mathbf{P}$ one obtains also an algebraic group, an extension of $\mathrm{Jac}(X)$ by a linear group (see [70] pp. 91-98).

We shall need only the case $\mathbf{m} = sP$ for a single point. Then $J_{sP} = \mathrm{Jac}_{\mathbf{m}}(X)$ is an extension of $J = \mathrm{Jac}(X)$ by $\mathbf{G}_{\mathrm{a}}^{s-1}$ (see [70] p. 96), so that

$$0 \longrightarrow \mathbf{G}_{\mathrm{a}}^{s-1} \longrightarrow J_{sP} \longrightarrow J \longrightarrow 0. \tag{15.4}$$

If $s \geq 2$ it is known that this is non-split in the sense that it is not isomorphic to $\mathbf{G}_{\mathrm{a}}^{s-1} \times J$ (implicit in [70] p.188 for $s = 2$ and explicit in Rosenlicht [64] p. 529 for general s).

In our calligraphic context with the Jacobian $\mathcal{J}$ of $\mathcal{X}$ we can at first try $\mathcal{J}_{2\mathcal{Z}}$ as near the end of section 14 with

$$0 \longrightarrow \mathbf{G}_{\mathrm{a}} \longrightarrow \mathcal{J}_{2\mathcal{Z}} \longrightarrow \mathcal{J} \longrightarrow 0. \tag{15.5}$$

As observed this is non-split; but Theorem 1.6 is for extensions only of elliptic curves. We can obtain these by using an isogeny from $\mathcal{J}$ to $\mathcal{E}_1 \times \mathcal{E}_2$ in (15.5), but it is not clear that they are non-split, and indeed it is not always true.

An example is for $Z = (0, 1)$ in the special case $d = 1$ in (15.1). For any $f = f(x_1, y_1)$ on E_1 having no zero or pole at $Q = \phi_1(Z) = (0, 1)$ the pull-back $f_1 = \phi_1^* f = f(x^2, y)$ on (15.1) is of course principal with $[(f_1)] = 0$ but also the narrow class $[(f_1)]_{2Z} = 0$ due to the expansion $x = \pi, y = 1 + \frac{c}{2}\pi^2 + \cdots$ with a local parameter π at Z. Thus taking $[D]$ to $[\phi_1^* D]_{2Z}$ gives a well-defined regular map from $\mathrm{Jac}(E_1)$ to J_{2Z} (at first from $(E_1)_Q$ but as in the Appendix

that is the same as the Jacobian). It is non-zero because for any $P_1 = (x_1, y_1) \neq \infty$ on E_1 with $x_1 \neq 0, y_1 \neq 0$ we have

$$\phi_1^*(P_1 - \infty) \;=\; Z_+ + Z_- - (\infty^+ + \infty^-) \tag{15.6}$$

with $Z_\pm = (\pm\sqrt{x_1}, y_1)$; but the only functions on (15.1) with polar divisor $\infty^+ + \infty^-$ are $x - \alpha$ up to constants, and these have zeroes of the shape $(x, \pm y)$. Thus even the standard class on the right of (15.6) is non-zero.

Now by restricting the analogue of (15.5) to the kernel of the projection from J to E_2 we indeed obtain an additive extension of E_1; but it splits because of ϕ_1^*. One could say that (15.5) can be "half-split".

In general the matter depends on ramification properties of ϕ_1, ϕ_2 (see subsection 16.3). In (15.5) we can resolve it by using Riemann-Roch and Hurwitz to go to a suitable $\mathcal{J}_{s\mathcal{Z}}$, possibly with $s \geq 3$, that has the effect of killing the ramification. So the case $m = 1$ can be handled.

But it can happen that E_1, E_2 in (15.2) are isogenous. The example with $a = -d = t+2, c = -b = 3t - 10$ (itself "antipalindromic") leads, after replacing x by $\frac{x+1}{x-1}$ and adjusting y, to

$$y^2 = x^5 + tx^3 + x. \tag{15.7}$$

In fact there is an isogeny ι from the Jacobian, which we could now call $\mathcal{J}$ over $\mathbf{P}_1$, to the square $\mathcal{E}^2$ of an elliptic curve, which is just

$$\tilde{y}^2 = \tilde{x}^3 - \tilde{t}\tilde{x}^2 + \tilde{t}\tilde{x} - 1 \tag{15.8}$$

with $\tilde{t} = \frac{3t-10}{t+2}$. We can take $\iota(\mathcal{D}) = (\varphi_{1*}(\mathcal{D}), \varphi_{2*}(\mathcal{D}))$ with the (calligraphic) maps

$$\varphi_1(x,y) = \left(\left(\frac{x+1}{x-1}\right)^2, \frac{8\tilde{t}y}{(x-1)^3}\right), \quad \varphi_2(x,y) = \left(\left(\frac{x-1}{x+1}\right)^2, \frac{8i\tilde{t}y}{(x+1)^3}\right) \tag{15.9}$$

from (15.7) to (15.8), where $\tilde{t}^2 = \frac{1}{t+2}$; these are easily seen to be independent, for example by considering valuations at $x = \pm 1$.

Now the above methods fail for $m = 2$ as well. In that case, assuming no problems with ramification, we have to take $m = 2$ copies of (15.5) to give

$$0 \longrightarrow \mathbf{G}_{\mathrm{a}}^2 \longrightarrow \mathcal{J}_{2\mathcal{Z}}^2 \longrightarrow \mathcal{J}^2 \longrightarrow 0.$$

However we do not obtain a torsion point on the specialized $\mathcal{J}_{2\mathcal{Z}}^2$ until we have taken the quotient by a suitable line in $\mathbf{G}_{\mathrm{a}}^2$. Using ι^2 from $\mathcal{J}^2$ to $\mathcal{E}^4$ and then [51] we can reduce to an extension of just a single $\mathcal{E}$ by $\mathbf{G}_{\mathrm{a}}^2$ (a sort of fibre product). But even here it is again not clear that we end up with something non-split after taking the quotient.

This problem has nothing to do with ramification. It turns out that we do obtain non-split with the exception of a unique bad line or "splitting line". This we explain in the Appendix.

In fact all these examples arising from (15.1) can be handled by a trick using the involution Υ sending (x, y) to $(-x, y)$; this reduces Theorem 1.3 to the case of genus 1 (which however still needs care, as (21.8) shows). For ω is elementary integrable if and only if

$$\omega_1 = \omega + \Upsilon^*(\omega), \quad \omega_2 = \omega - \Upsilon^*(\omega)$$

are, and it is easily seen that these are pull-backs of differentials on E_1, E_2 by ϕ_1, ϕ_2 respectively.

But we do not know how to use similar tricks for other examples (see also the remark in Krazer [40] p.479). Hermite found the curve

$$y^2 = (x^2 - a)(8x^3 - 6ax - b)$$

and elliptic curves

$$y_1^2 = (2ax_1 - b)(x_1^2 - a), \quad y_2^2 = x_2^3 - 3ax_2 + b,$$

with the maps

$$\phi_1(x,y) = \left(\frac{4x^3 - 3ax}{a}, \frac{4x^2 - a}{a}y\right), \quad \phi_2(x,y) = \left(\frac{2x^3 - b}{3(x^2 - a)}, \frac{\sqrt{3}}{9}\frac{x^3 - 3ax + b}{(x^2 - a)^2}y\right).$$

(see Königsberger [39] p.276 with a misprint). Consult also [40] (p. 480) for another example, and Enneper [25] (pp. 501-513) for a survey. Also Kuhn [41], Frey [27], and Frey and Kani [28] have considered general examples in genus 2. And see Cassels [13] (p.202) for an example

in genus 3. (Not to mention Mestre [54] p.196 in genus $g = 19$ or Ekedahl and Serre [24] for $g = 1297$.)

And finally when we take ramification into account, as well as the situation for general g, we have a similar problem for extensions of $\mathcal{E}$ by some $\mathbf{G}_{\mathrm{a}}^{2s-2}$; but still the splitting line controls the quotient.

16. Elusive differentials.

16.1. **Preamble.** In order to prove Theorem 1.3 we must of course say what we mean by elusive f. The reader is advised that the definition extends over the next few pages and involves two lemmas.

We work in $\mathbb{K}(X)$, where $\mathbb{K}$ is a field of characteristic zero now containing $\overline{\mathbf{Q}}$, and X (no longer calligraphic) is a smooth irreducible curve defined over $\mathbb{K}$. As in the previous sections we prefer to work with differentials ω on X defined over $\mathbb{K}$. Denote by J the Jacobian of X, the set of all classes $[D]$ of divisors D of degree zero.

For non-constant maps θ from a curve to a second curve we use the standard notations θ_*, θ^* for the action on divisors or their classes $[\ ]$, as well as θ^* on differentials (see for example [73] pp.33-35). Thus $\theta_* \circ \theta^*$ is simply multiplication by the degree of θ. But $\theta^* \circ \theta_*$ is not so easy to describe.

Soon we will take the second curve to be an elliptic curve. In that case the maps (now including constant maps) form a group, and it is easy to see that $(\theta_1 + \theta_2)_* = \theta_{1*} + \theta_{2*}$ on divisor classes of degree zero. In fact the same linearity holds with upper stars; but this is not quite so straightforward (and may be deduced from the Seesaw Principle, for example).

To begin the definition, there are no elusive ω (that is, no counterexamples to Davenport's Assertion) if the genus g of X is zero. Thus henceforth we assume $g \geq 1$, so that J has positive dimension.

Also, there are no elusive ω if J does not contain an elliptic curve.

If J does contain an elliptic curve, and θ is a non-constant map from X, then it turns out that in certain special circumstances $\theta^* \circ \theta_*$ can be described. This will be the content of the next two lemmas.

When J is as above there is an elliptic curve E and an isogeny ι from J to

$$E^n \times B \tag{16.1}$$

for some positive integer n, where B is an abelian variety containing no abelian subvariety isogenous to E.

We fix any point P_0 on X and define the embedding $\jmath$ of X in J by $\jmath(P) = [P - P_0]$. The analogous construction for E taking the origin enables us to identify E with its Jacobian. Recall that the endomorphism ring $\mathcal{O}$ of E comes with a natural Rosati involution, whose action on β we denote by $\overline{\beta}$.

We remark that if $\tilde{\phi}$ is a non-zero homomorphism from J to E then $\phi = \tilde{\phi} \circ \jmath$ is non-constant from X to E. For if not, then because $\phi(P_0) = 0$ it would be zero; but since $\jmath(X)$ generates J as a group this is absurd. We can also check that $\phi_* = \tilde{\phi}$.

Lemma 16.1. *Let X, J, E, ι, n, B be as above, and let $\pi_1, \dots, \pi_n, \pi_B$ be the projections from $\iota(J)$ to the various factors in (16.1). Write $\phi_k = \pi_k \circ \iota \circ \jmath$ $(k = 1, \dots, n)$ from X to E. Then $\iota = (\phi_{1*}, \dots, \phi_{n*}, \pi_B \circ \iota)$ provided we identify E with its Jacobian, so in particular $\phi_1, \dots, \phi_n$ must be linearly independent over $\mathcal{O}$. Let γ_{kh} be in $\mathcal{O}$ with $\gamma_{kh*} = \phi_{k*} \circ \phi_h^*$ $(k, h = 1, \dots, n)$. Then for any $\alpha_1, \dots, \alpha_n$ in $\mathcal{O}$ there are $\beta_1, \dots, \beta_n$ in $\mathcal{O}$ with*

$$\sum_{h=1}^{n} \overline{\beta_h} \gamma_{kh} = l\alpha_k \ (k = 1, \dots, n) \tag{16.2}$$

for some positive integer l.

Proof. Taking $\tilde{\phi} = \pi_k \circ \iota$ in the remark above we see the required expression for ι, and so the linear independence assertion.

Now the matrix with entries γ_{kh} is non-singular. Otherwise we could find $\alpha'_1, \dots, \alpha'_n$ in $\mathcal{O}$, not all zero, with

$$\alpha'_1\gamma_{1h} + \cdots + \alpha'_n\gamma_{nh} = 0 \quad (h = 1, \dots, n).$$

But then for $\phi = \alpha'_1\phi_1 + \cdots + \alpha'_n\phi_n$ we would have from bilinearity $\phi_* \circ \phi_h^* = 0$ $(h = 1, \dots, n)$ and then $\phi_* \circ \phi^* = 0$, leading to a contradiction through the degree.

Thus indeed $\beta_1, \dots, \beta_n$ and l exist as in (16.2). This completes the proof. □

We now make the above comment on $\theta^* \circ \theta_*$ precise.

Lemma 16.2. *Let X, J, E, ι, n, B be as above, with $\phi_1, \dots, \phi_n$ and γ_{hk} as in Lemma 16.1. Let M be a non-torsion point on J with*

$$\iota(M) = (Q_1, \dots, Q_n, H) \tag{16.3}$$

for points $Q_1, \dots, Q_n$ on E and H on B. Assume that there is a positive integer a and $\alpha_1, \dots, \alpha_n$ in the endomorphism ring $\mathcal{O}$ of E with

$$aQ_k = \alpha_k Q \ (k = 1, \dots, n), \quad aH = 0 \tag{16.4}$$

for some point Q on E. Define $\beta_1, \dots, \beta_n, l$ as in Lemma 16.1 and define $\theta = \sum_{h=1}^n \beta_h\phi_h$ from X to E. Then θ is non-constant, $c = \sum_{h=1}^n \beta_h\alpha_h \neq 0$ is in $\mathbf{Z}$ and

$$a\theta_* M = cQ; \tag{16.5}$$

further

$$ab\theta^*\theta_* M = abd_0 M$$

for the degree b of ι and the degree $d_0 = cl$ of θ.

Proof. If θ were constant, then by the remark just before Lemma 16.1, $\sum_{h=1}^n \beta_h(\pi_h \circ \iota)$ would be zero. Thus $\beta_h = 0$ $(h = 1, \dots, n)$ and also $\alpha_k = 0$ $(k = 1, \dots, n)$ by (16.2). But then (16.4) and (16.3) would show that M is torsion, against our hypothesis.

Next we define $Q_0 = \theta_* M$ on E. We calculate

$$Q_0 = \theta_* M = \sum_{h=1}^n \beta_{h*}\phi_{h*} M = \sum_{h=1}^n \beta_{h*} Q_h$$

which by hypothesis implies

$$aQ_0 = c_* Q \tag{16.6}$$

for

$$c = \sum_{h=1}^n \beta_h\alpha_h.$$

Now the degree d_0 of θ can be evaluated by working out $\theta_* \circ \theta^*$, which is

$$\left(\sum_{h=1}^n \beta_{h*}\phi_{h*}\right) \circ \left(\sum_{t=1}^n \phi_t^*\beta_t^*\right) \ = \ \sum_{h=1}^n \sum_{t=1}^n \beta_{h*}\gamma_{ht*}\beta_t^* \ = \ l\sum_{h=1}^n \beta_{h*}\alpha_{h*} \ = \ lc_*;$$

here we used (16.2) and the fact that $(\overline{\beta})_* = \beta^*$ (consider $(\beta\overline{\beta})_*$ for example) on divisor classes of degree zero. Thus $d_0 = lc$ is a rational integer and $c \neq 0$. Now c is in $\mathcal{O}$ and in $\mathbf{Q}$ so in $\mathbf{Z}$.

Define also $\xi = \theta^* Q_0 = \theta^*\theta_* M$ on J. Then

$$\iota(\xi) \ = \ (\phi_{1*}\xi, \dots, \phi_{n*}\xi, \pi_B(\iota(\xi))) \tag{16.7}$$

and here

$$\pi_B(\iota(\xi)) = \pi_B(\iota(\theta^* Q_0)) = f(Q_0)$$

for the map $f = \pi_B \circ \iota \circ \theta^*$ from E to B. However our assumptions on E and B imply that $f = 0$. Thus we can go further with (16.7) as

$$a\iota(\xi) \ = \ a(\phi_{1*}\theta^* Q_0, \dots, \phi_{n*}\theta^* Q_0, 0) \ = \ a(\sum_{h=1}^n \gamma_{1h*}\beta_h^* Q_0, \dots, \sum_{h=1}^n \gamma_{nh*}\beta_h^* Q_0, 0)$$

which is

$$al(\alpha_{1*} Q_0, \dots, \alpha_{n*} Q_0, 0) \ = \ lc(\alpha_{1*} Q, \dots, \alpha_{n*} Q, 0)$$

by (16.6). By (16.4) this is in turn $alc(Q_1, \dots, Q_n, 0)$. Thus recalling (16.3) we get

$$a\iota(\xi) = alc\iota(M).$$

Therefore $ab\xi = ablcM = abd_0M$. Thus

$$ab\theta^*\theta_*M = abd_0M$$

and this completes the proof. □

16.2. **The definition.** We now continue with the definition of elusive.

In fact there are no elusive ω if J does not contain an elliptic curve with complex multiplication.

So from now on, in this section, we suppose that this is not the case; equivalently

(E0): *There is an isogeny ι from J to $E^n \times B$ for some $n \geq 1$, where E is an elliptic curve defined over $\overline{\mathbf{Q}}$ with complex multiplication and endomorphism ring say $\mathcal{O}$, and B has no abelian subvariety isogenous to E.*

We shall need the concept of generalized Jacobian, for the moment only for $g = 1$ (but later for any g). This is recalled in the Appendix. For an elliptic curve E over $\mathbb{K}$, a point W on E and a positive integer r we denote more precisely by E_{rW} the extension called G_r there with respect to the modulus rW. The corresponding class in E_{rW} of a divisor D (prime to W) on E will be denoted more precisely, as above, by $[D]_{rW}$. The linear part of E_{rW} is isomorphic to $\mathbf{G}_{\mathrm{a}}^{r-1}$ and consists of the classes $[(k)]_{rW}$ of principal divisors (k) of functions k (with no poles or zeroes at W) on E.

Next we list certain properties (E1),(E2),(E3),(E4) about a differential ω of the third kind which is not elementary integrable modulo differentials of the first kind. As in sections 12, 13 and 14, we shall eventually prove Theorem 1.5 by reducing to such ω.

(E1): *Now ω as a differential of the third kind must have at least one non-zero residue, otherwise it would be of the first kind. Pick over-basis elements $\rho_1, \dots, \rho_m$ of the additive group generated by the residues of ω, and write*

$$\mathrm{Res}\ \omega = \rho_1 D_1 + \cdots + \rho_m D_m$$

for divisors $D_1, \dots, D_m$ in X of degree zero. Then if π_B is the projection from $E^n \times B$ to B, the $\pi_B(\iota([D_i]))$ $(i = 1, \dots, m)$ should be torsion on B.

We note that not all of $[D_1], \dots, [D_m]$ can be torsion. Otherwise there would be a positive integer $\tilde{a}$ with $\mathrm{Res}(\tilde{a}\omega) = \sum_{i=1}^m \rho_i(f_i)$. But that is Res ϵ for $\epsilon = \sum_{i=1}^m \rho_i \mathrm{d}f_i/f_i$, so $\tilde{a}\omega - \epsilon$ would have zero residue divisor. This too is already of the third kind, so would have to be of the first kind, a contradiction.

Now when the over-basis elements $\rho_1, \dots, \rho_m$ are changed by a matrix in $\mathrm{SL}_m(\mathbf{Z})$, the $D_1, \dots, D_m$ change by the inverse matrix. As $\mathrm{SL}_m(\mathbf{Z})$ is Zariski-dense in $\mathrm{SL}_m(\mathbf{R})$, it is easy to find an over-basis with $[D_1], \dots, [D_m]$ all non-torsion. It is not too natural to do this, but it will be highly convenient in what follows, especially in section 19, and we call it a *torsion-killing* over-basis. Recall the embedding $\jmath$ above from X to J.

(E2): *Let $\pi_1, \dots, \pi_n$ be the projections from $E^n \times B$ to the factors E, and put $\phi_k = \pi_k \circ \iota \circ \jmath$ $(k = 1, \dots, n)$ non-constant from X to E. Then there should be α_{ik} in $\mathcal{O}$, a divisor D of degree zero on E and a positive integer a such that*

$$a\phi_{k*}[D_i] = \alpha_{ik*}[D] \quad (i = 1, \dots, m,\ k = 1, \dots, n).$$

Further $[D]$ should not be defined over $\overline{\mathbf{Q}}$.

We note that $[D]$ above cannot be torsion. For otherwise all the $\phi_{k*}[D_i]$ would be torsion. And by (E1) the $\pi_B(\iota([D_i]))$ are torsion, so that by Lemma 16.1 the $\iota([D_i])$ would be torsion. Thus the $[D_i]$ would be torsion, which we ruled out just after (E1).

Now we can use Lemma 16.2. With non-torsion $M = [D_i]$ we can assume that the quantity a in the first equations of (16.4) is independent of i, and that $a\pi_B(\iota([D_i])) = 0$ $(i = 1, \dots, m)$. We obtain non-constant θ_i from X to E, together with non-zero functions h_i on X, such that

$$abd_iD_i - ab\theta_i^*\theta_{i*}D_i \ = \ (h_i) \quad (i = 1, \dots, m) \tag{16.8}$$

where b is the degree of ι and d_i is the degree of θ_i. Fixing these, define

$$\omega^\natural \;=\; \omega - \frac{1}{ab}\sum_{i=1}^{m}\frac{\rho_i}{d_i}\frac{\mathrm{d}h_i}{h_i} \tag{16.9}$$

which is non-zero because ω is not elementary integrable.

From (E1) and (16.8) we note for later use

$$\operatorname{Res}\omega^\natural \;=\; \sum_{i=1}^{m}\rho_i\left(D_i - \frac{1}{ab}\frac{(h_i)}{d_i}\right) \;=\; \sum_{i=1}^{m}\rho_i^\natural D_i^\natural \tag{16.10}$$

for

$$\rho_i^\natural = \frac{1}{abd}\rho_i,\quad D_i^\natural = abdD_i - e_i(h_i) = abe_i\theta_i^*\theta_{i*}D_i \qquad (i=1,\dots,m) \tag{16.11}$$

and $d_ie_i = d_1\cdots d_m$ $(i=1,\dots,m)$. However this might not be shortest as in (11.4). But in section 18 it will be. At least $\rho_1^\natural,\dots,\rho_m^\natural$ are linearly independent over $\mathbf{Q}$.

(E3): *For each zero Z of $\omega^\natural$, of order say $r-1\ge 1$, write $W_i=\theta_i(Z)$ and define F_Z as the product of the generalized Jacobians E_{rW_i} fibred over E embedded diagonally, with U_Z as the subspace of the linear part consisting of those $([(k_1)]_{rW_1},\dots,[(k_m)]_{rW_m})$ such that*

$$\operatorname{ord}_Z\left(\sum_{i=1}^{m}\rho_i\theta_i^*\frac{\mathrm{d}k_i}{k_i}\right) \;\ge\; r-1 \tag{16.12}$$

(note that if (k_i) is prime to W_i, then $\theta_i^*(k_i)$ is prime to Z, else $d_i(k_i)=\theta_{i*}\theta_i^*(k_i)$ would not be prime to $\theta_i(Z)=W_i$). Then with $G_Z=F_Z/U_Z$, of dimension say d_Z, there should be a surjective homomorphism σ_Z from G_Z to $\mathbf{G}_{\mathrm{a}}^{d_Z-1}$.

It will be clear in the sequel that there is an exact sequence

$$0\longrightarrow \mathbf{G}_{\mathrm{a}}^{d_Z-1}\longrightarrow G_Z\longrightarrow E\longrightarrow 0$$

so the above condition expresses splitting as in the Appendix (as already used in sections 14 and 15). The condition will be simplified in Lemma 16.3 below.

Next, we note that each $\theta_{i*}D_i$ is prime to W_i, else $D_i^\natural = abe_i\theta_i^*\theta_{i*}D_i$ would not be prime to anything in $\theta_i^{-1}(W_i)$ and in particular Z; but then by the linear independence of $\rho_1^\natural,\dots,\rho_m^\natural$ in (16.10) we would deduce that Z is a pole of $\omega^\natural$.

(E4): *There should be a positive integer t such that for each such Z the point*

$$T_Z \;=\; a\,(e_1[\theta_{1*}D_1]_{rW_1},\dots,e_m[\theta_{m*}D_m]_{rW_m})$$

on $E_{rW_1}\times\cdots\times E_{rW_m}$ projects to $t([D],\dots,[D])$ on E^m, and furthermore $\sigma_Z(T_Z)=0$.

At last we can state what it means for an arbitrary differential to be elusive. This we do in terms of the particular ω considered above.

Definition. *A differential on X is elusive if it differs from a differential of the third kind ω by an exact differential but is not elementary integrable modulo differentials of the first kind, and furthermore (E0) holds for J and (E1),(E2),(E3),(E4) hold for ω.*

Note that if ω exists for the original differential then it is unique. And it too is not elementary integrable modulo differentials of the first kind.

And elusiveness is invariant under adding exact differentials.

As already remarked, it may be found surprising that any elusive differentials actually exist. But

$$\omega_0 \;=\; \frac{x\mathrm{d}x}{(x^2-t^2)\sqrt{x^3-x}}$$

(with $\mathbb{K}$ as $\overline{\mathbf{Q}}(t)$ for example) in (21.8) is elusive.

It is not too hard to see that for reasonable $\mathbb{K}$, such as $\overline{\mathbf{Q}}(C)$, we can effectively decide whether a given ω is elusive. Especially for ω_0 above with $m=2$ it is fairly easy (see section 21). But it is more tedious for things like

$$\omega_0 + \frac{\mathrm{d}x}{x} \tag{16.13}$$

with $m = 3$ (and the obvious over-basis not torsion-killing), or

$$\omega_0 + \frac{1}{\sqrt{t^3 - t}} \frac{\mathrm{d}x}{x} \tag{16.14}$$

back to $m = 2$ (thanks to residues and the choice of coefficient).

The problem is that adding quite a simple elementary integrable differential (even something exact) complicates the zeroes Z in (E3) and (E4). In fact we will see in section 19, at least over $\overline{\mathbf{Q}}(C)$, that the property of elusiveness is invariant under adding arbitrary elementary integrable differentials (as it should be according to Theorem 1.5).

16.3. **More about (E3).** We will soon see how to take back control in (E3). First we need some more generalities.

Return to non-constant θ from X to another curve, say X'. The pull-back θ^* extends to generalized Jacobians. Namely there is a homomorphism $\theta^*_{\mathbf{m}}$ from $\mathrm{Jac}_{\theta_*\mathbf{m}}(X')$ to $\mathrm{Jac}_{\mathbf{m}}(X)$ defined by

$$\theta^*_{\mathbf{m}}([D']_{\theta_*\mathbf{m}}) \;=\; [\theta^* D']_{\mathbf{m}}.$$

As we could not find a reference in the literature, and especially as the push-forward θ_* seems not to extend, we give a slightly pedantic proof. It rests on

$$\mathrm{ord}_P(\theta^* h') = e_P(\theta)\mathrm{ord}_{\theta(P)} h' \tag{16.15}$$

for any function h' on X', where $e_P(\theta) \geq 1$ is the ramification index of θ at P. We have $\theta_*\mathbf{m} = \sum_{P' \in \mathbf{P}'} s'_{P'} P'$ with $\mathbf{P}' = \theta(\mathbf{P})$ and $s'_{P'} = \sum_{\theta(P)=P'} s_P$. It suffices to show that if f' is a function on X' with $\mathrm{ord}_{P'}(f' - 1) \geq s'_{P'}$ for all P' then also $\mathrm{ord}_P(\theta^* f' - 1) \geq s_P$ for all P. But $\theta^* f' - 1 = \theta^*(f' - 1)$ so (16.15) gives

$$\mathrm{ord}_P(\theta^* f' - 1) = e_P(\theta)\mathrm{ord}_{\theta(P)}(f' - 1) \geq \mathrm{ord}_{\theta(P)}(f' - 1) \geq s'_{\theta(P)} \geq s_P$$

as desired.

Later we will need the analogue of (16.15) for differentials ω' on X', namely

$$\mathrm{ord}_P(\theta^* \omega') \;=\; e_P(\theta) - 1 + e_P(\theta)\mathrm{ord}_{\theta(P)}\omega' \tag{16.16}$$

(also a standard calculation with local parameters).

Remark. By the way, when $\mathbf{m}$ has empty support the map θ^* from $\mathrm{Jac}(X')$ to $\mathrm{Jac}(X)$ is almost injective in the sense of finite kernel, because if $\theta^* D' = (f)$ then $\theta_*\theta^* D' = (\theta_* f)$ and since as remarked $\theta_*\theta^*$ is multiplication by the degree d of θ we see that $d[D'] = 0$. But for general $\mathbf{m}$ this may fail. For example with ϕ_1 around (15.6) we have

$$\mathrm{ord}_Z(y - 1) = \mathrm{ord}_Z(\phi^*(y_1 - 1)) = \mathrm{ord}_Z((y_1 - 1) \circ \phi_1) = e_Z(\phi_1)\mathrm{ord}_{\phi_1(Z)}(y_1 - 1) = 2$$

because $e_Z(\phi_1) = 2$, and so

$$\phi_1^*[(y_1)]_{2\phi_1(Z)} = [(\phi_1^* y_1)]_{2Z} = [(y)]_{2Z} = 0;$$

but $d[(y_1)]_{2\phi_1(Z)} \neq 0$ for all positive d (provided $c \neq 0$). This also explains the connexion between ramification and "half-split" around (15.5).

A later problem (see (18.3) and the discussion around it) will be the lack of surjectivity of $\phi^*_{\mathbf{m}}$; but this fails already on dimensional grounds if the genus of X exceeds that of X'.

In the case $\mathbf{m} = sP$ as in (15.4) it is known (see for example Serre [70] p.94) that the $\mathbf{G}_{\mathrm{a}}^{s-1}$ is the set of classes $[(f)]_{\mathbf{m}}$. This makes it clear that $\phi^*_{\mathbf{m}}$ acts on the linear parts $\mathbf{G}_{\mathrm{a}}^{s-1}$. It also commutes with the natural projections from $\mathrm{Jac}_{\phi_*\mathbf{m}}(X')$ to $\mathrm{Jac}(X')$ and from $\mathrm{Jac}_{\phi_*\mathbf{m}}(X)$ to $\mathrm{Jac}(X)$ via the standard ϕ^* from $\mathrm{Jac}(X')$ to $\mathrm{Jac}(X)$.

Now we can clarify (E3) by eliminating the zeroes Z. We note that there is a canonical embedding κ of $\mathcal{O}$ in $\mathbb{K}$ defined by $\alpha^*(\chi) = \kappa(\alpha)\chi$ for any differential χ of the first kind on E.

Lemma 16.3. *Suppose J is as in (E0) except possibly for the condition of complex multiplication. Suppose also that ω on X is of the third kind but is not elementary integrable modulo differentials of the first kind, and satisfies (E1),(E2). Then (E3) is equivalent to*

$$\sum_{i=1}^{m} \rho_i \kappa(\overline{\alpha_{ik}}) = 0 \quad (k = 1, \ldots, n), \tag{16.17}$$

which is in turn equivalent to

$$\sum_{i=1}^{m} \rho_i \theta_i^* \chi = 0 \tag{16.18}$$

for any differential χ of the first kind on E.

Proof. First suppose (E3) holds. We shall first deduce (16.18).

Thus define $\omega_0 = \sum_{i=1}^m \rho_i \theta_i^* \chi$ on X, also of the first kind, and assume for the moment that $\omega_0 \neq 0$. We will obtain a contradiction.

Then ω_0 has exactly $2g-2$ zeroes. Our $\omega^\natural$ has poles, because ω is not elementary integrable modulo differentials of the first kind. Thus $\omega^\natural$ has more than $2g-2$ zeroes. Thus (a primitive sort of zero estimate) there is a point Z in X with

$$r - 1 = \mathrm{ord}_Z \omega^\natural > \mathrm{ord}_Z \omega_0 \geq 0. \tag{16.19}$$

We have

$$0 \longrightarrow \mathbf{G}_{\mathrm{a}}^{r-1} \longrightarrow J_{rZ} \longrightarrow J \longrightarrow 0$$

and here the $\mathbf{G}_{\mathrm{a}}^{r-1}$ is the set of classes $[(f)]_{rZ}$ (recall that $[D]_{rZ}$ is defined only for D coprime to Z). Thus in the product

$$0 \longrightarrow (\mathbf{G}_{\mathrm{a}}^{r-1})^m \longrightarrow (J_{rZ})^m \longrightarrow J^m \longrightarrow 0$$

the $(\mathbf{G}_{\mathrm{a}}^{r-1})^m$ is the set of $([(f_1)]_{rZ}, \dots, [(f_m)]_{rZ})$. Define V_Z in $(\mathbf{G}_{\mathrm{a}}^{r-1})^m$ inside $(\mathcal{J}_{rZ})^m$ by

$$\mathrm{ord}_Z \left(\sum_{i=1}^{m} \rho_i \frac{\mathrm{d}f_i}{f_i} \right) \ \geq \ r-1. \tag{16.20}$$

By functoriality we have a map $Y = (\theta_1^*, \dots, \theta_m^*)$ from $E_{rW_1} \times \cdots \times E_{rW_m}$ to $(J_{rZ})^m$. Thus

$$U_Z = Y^{-1} V_Z$$

in $(\mathbf{G}_{\mathrm{a}}^{r-1})^m$ inside $\prod_{i=1}^m E_{rW_i}$.

From (E3) the corresponding $G_Z = F_Z/U_Z$ is split. Thus by Proposition A.3 of the Appendix and the remark immediately following, we know that U_Z contains the splitting line L_Z in F_Z.

To calculate L_Z we use Corollary A.7 of the Appendix, with τ_i translation by $-W_i$ ($i = 1, \dots, m$). Thus L_Z is the set of

$$\mathbf{l}(k) = ([(\tau_1^* k)]_{rW_1}, \dots, [(\tau_m^* k)]_{rW_m}) \tag{16.21}$$

for all k on E with

$$\mathrm{ord}_O \left(\frac{\mathrm{d}k}{k} - \lambda\chi \right) \ \geq \ r-1 \tag{16.22}$$

and some constant λ in $\overline{\mathbf{Q}}(C)$. Now L_Z inside U_Z amounts to YL_Z inside V_Z and so $Y\mathbf{l}(k)$ in V_Z for all such k. Taking any such k with $\mathrm{ord}_O(k-1) = r-1$ we have $\lambda \neq 0$ and we find that

$$(\theta_1^*([(\tau_1^* k)]_{rW_1}), \dots, \theta_m^*([(\tau_m^* k)]_{rW_m})) \ = \ ([(\theta_1^* \tau_1^* k)]_{rZ}, \dots, [(\theta_m^* \tau_m^* k)]_{rZ})$$

lies in V_Z, which is $([(f_1)]_{rZ}, \dots, [(f_m)]_{rZ})$ for

$$f_i = \theta_i^* \tau_i^* k = \theta_i^*(\tau_i^* k) \quad (i = 1, \dots, m).$$

Here

$$\frac{\mathrm{d}f_i}{f_i} \ = \ \theta_i^* \left(\frac{\mathrm{d}(\tau_i^* k)}{\tau_i^* k} \right) \ = \ \theta_i^* \tau_i^* \frac{\mathrm{d}k}{k} \ = \ \theta_i^* \tau_i^* (\lambda\chi + \eta) \ \ (i = 1, \dots, m)$$

for some η with $\mathrm{ord}_O \eta \geq r-1$ by (16.22). Now

$$\theta_i^* \tau_i^* (\lambda\chi) = \lambda \theta_i^* (\tau_i^* \chi) = \lambda \theta_i^* \chi \quad (i = 1, \dots, m)$$

by translation-invariance of χ, and

$$\mathrm{ord}_Z(\theta_i^* \tau_i^* \eta) \geq \mathrm{ord}_{W_i}(\tau_i^* \eta) \geq \mathrm{ord}_O \eta \geq r-1 \quad (i = 1, \dots, m)$$

by (16.16). It follows from the definition (16.20) of V_Z that $\mathrm{ord}_Z \omega_0 \geq r-1$. But this contradicts (16.19).

Thus indeed (16.18) holds; that is, $\omega_0 = 0$.

To get to (16.17) we write

$$\theta_i = \sum_{h=1}^{n} \beta_{ih}\phi_h \quad (i = 1, \dots, m) \tag{16.23}$$

as in Lemma 16.1 with

$$\sum_{h=1}^{n} \overline{\beta_{ih}}\gamma_{kh} = l\alpha_{ik} \quad (i = 1, \dots, m;\ k = 1, \dots, n) \tag{16.24}$$

as in (16.2). We calculate formally that ω_0 is

$$\sum_{i=1}^{m} \rho_i \sum_{h=1}^{n} \phi_h^* \beta_{ih}^* \chi = \sum_{i=1}^{m} \rho_i \sum_{h=1}^{n} \phi_h^* \kappa(\beta_{ih})\chi = \sum_{h=1}^{n} \nu_h \phi_h^* \chi. \tag{16.25}$$

for $\nu_h = \sum_{i=1}^{m} \rho_i \kappa(\beta_{ih})$ $(h = 1, \dots, n)$.

We note that the construction of $\phi_1, \dots, \phi_n$ gives $\tilde{\phi}_1, \dots, \tilde{\phi}_n$ from J to E with $\phi_h = \tilde{\phi}_h \circ \jmath$. We now use upper stars in the extended sense to indicate the pull-back action on differentials for general maps between general varieties. Thus from the above $0 = \omega_0 = \jmath^*(\sum_{h=1}^{n} \nu_h \tilde{\phi}_h^* \chi)$. Now $\jmath^*$ is well-known to be an isomorphism from differentials of the first kind on J to differentials of the first kind on X. Thus $0 = \sum_{h=1}^{n} \nu_h \tilde{\phi}_h^* \chi$ too. Also $\tilde{\Phi} = (\tilde{\phi}_1, \dots, \tilde{\phi}_n)$ would be surjective from J to E^n because $\phi_1, \dots, \phi_n$ are linearly independent over $\mathcal{O}$. And $\Psi^* \chi_h = \tilde{\phi}_h^* \chi$ for χ_h on E^n corresponding to the hth factor. From the injectivity of Ψ^* there would follow $0 = \sum_{h=1}^{n} \nu_h \chi_h$ too; an absurdity unless $\nu_h = 0$ $(h = 1, \dots, n)$.

But then using (16.24) we compute

$$0 = \sum_{h=1}^{n} \kappa(\overline{\gamma_{kh}})\nu_h = l \sum_{i=1}^{m} \rho_i \kappa(\overline{\alpha_{ik}}) \quad (k = 1, \dots, n) \tag{16.26}$$

giving (16.17) as required.

Now we can get back to (E3) as follows. Take any zero Z of $\omega^\natural$, and any $\mathbf{l}(k)$ in L_Z as in (16.21), so that by (16.22) we have $dk/k = \lambda\chi + \eta$ for η vanishing to order at least $r - 1$ at O. Then with $k_i = \tau_i^* k$ $(i = 1, \dots, m)$ we have

$$\sum_{i=1}^{m} \rho_i \theta_i^* \frac{\mathrm{d}k_i}{k_i} = \sum_{i=1}^{m} \rho_i \theta_i^* \tau_i^* (\lambda\chi + \eta) = \sum_{i=1}^{m} \rho_i \theta_i^* \tau_i^* \eta.$$

Thus this vanishes to order at least $r - 1$ at Z. So by (16.12) we are in U_Z. In other words, L_Z lies in U_Z and so G_Z is split. Therefore we are back to (E3). This completes the proof. □

To be able to handle the zeroes Z in (E4) later we need Theorem 1.3(b), which we accordingly prove next.

The following side question arose. Suppose we have verified (E0), (E1), (E2), (E3) together with (E4) except for the conditions $\sigma_Z(T_Z) = 0$. Do these then follow automatically? If not, this would provide differentials of the third kind for which Davenport's Assertion is relatively easy (compare the treatment in section 21 of (1.17) for $d = 5$, which however has a pole of order six). And indeed the answer is no, and (21.12) is such an example - we found that there are at most 138 values of t, effectively computable, for which it becomes elementary integrable.

17. Proof of Theorem 1.3(b).

Now we suppose that ϖ (once more calligraphic) is elusive. We can even suppose it is of the third kind. For it is certainly $\varpi' + \mathrm{d}f$ with ϖ' elusive of the third kind, and so Theorem 1.3(b) for ϖ' would show that ϖ' is not elementary integrable but there are infinitely many $\mathbf{c}$ with $\varpi'(\mathbf{c})$ elementary integrable. Thus ϖ itself is not elementary integrable and $\varpi(\mathbf{c})$ is elementary integrable.

So we can assume (E0) for $\mathcal{J}$ and (E1),(E2),(E3),(E4) for ϖ (with a torsion-killing over-basis) which is not elementary integrable even modulo differentials of the first kind.

Because $\mathcal{D}$ in (E2) is a divisor (of degree zero) not defined over $\overline{\mathbf{Q}}$ on the elliptic curve $\mathcal{E}$ defined over $\overline{\mathbf{Q}}$, there is an infinite (countable) set $\mathbf{S}$ of $\mathbf{c}$ such that $[\mathcal{D}(\mathbf{c})]$ is torsion.

Take any $\mathbf{c}$ in this $\mathbf{S}$, and let $\mathcal{Z}$ be any zero of $\varpi^\natural$ in (E3), of order say $r-1$. With $\mathcal{T}_\mathcal{Z}$ in (E4) we show that $\mathcal{T}_\mathcal{Z}(\mathbf{c})$ - this is short for $\mathcal{T}(\mathbf{c})_{\mathcal{Z}(\mathbf{c})}$ - is torsion on $\mathcal{G}_\mathcal{Z}(\mathbf{c})$ (similarly shortened). For the latter is an extension of $\mathcal{E}(\mathbf{c})=\mathcal{E}$ by $\mathbf{G}_{\mathrm{a}}^{d_\mathcal{Z}-1}$ and $\varsigma_\mathcal{Z}$ (this is our "calligraphic" version of σ_Z) is a surjective map from $\mathcal{G}_\mathcal{Z}(\mathbf{c})$ to $\mathbf{G}_{\mathrm{a}}^{d_\mathcal{Z}-1}$. As $\varsigma_\mathcal{Z}(\mathcal{T}_\mathcal{Z})(\mathbf{c})=0$ by (E4) we have torsion on the additive part. But also by (E4) the projection of $\mathcal{T}_\mathcal{Z}(\mathbf{c})$ to the elliptic part is $t([\mathcal{D}(\mathbf{c})],\dots,[\mathcal{D}(\mathbf{c})])$. So indeed $\mathcal{T}_\mathcal{Z}(\mathbf{c})$ is torsion on $\mathcal{G}_\mathcal{Z}(\mathbf{c})$.

With $\mathcal{Y}=(\vartheta_1^*,\dots,\vartheta_m^*)$ we deduce that $\mathcal{Y}\mathcal{T}_\mathcal{Z}(\mathbf{c})$ is torsion on $\mathcal{Y}\mathcal{G}_\mathcal{Z}(\mathbf{c})$. Now $\mathcal{Y}\mathcal{F}_\mathcal{Z}(\mathbf{c})$ lies in $\mathcal{J}^m_{r\mathcal{Z}}(\mathbf{c})$ (also shortened), and with $\mathcal{U}_\mathcal{Z}$ as in (E3), $\mathcal{Y}\mathcal{U}_\mathcal{Z}(\mathbf{c})$ lies in the subspace $\mathcal{V}_\mathcal{Z}(\mathbf{c})$ of $(\mathbf{G}_{\mathrm{a}}^{r-1})^m$ there, where now $\mathcal{V}_\mathcal{Z}$ is defined by

$$\mathrm{ord}_\mathcal{Z}\left(\sum_{i=1}^m \varrho_i\frac{\mathrm{d}f_i}{f_i}\right)\ \geq\ r-1.$$

So $\mathcal{Y}\mathcal{T}_\mathcal{Z}(\mathbf{c})$ is torsion on $\mathcal{J}^m_{r\mathcal{Z}}(\mathbf{c})/\mathcal{V}_\mathcal{Z}(\mathbf{c})$.

Now

$$b\mathcal{Y}\mathcal{T}_\mathcal{Z}(\mathbf{c})\ =\ ab\,(e_1[\vartheta_1^*\vartheta_{1*}\mathcal{D}_1]_{r\mathcal{Z}}(\mathbf{c}),\dots,e_m[\vartheta_m^*\vartheta_{m*}\mathcal{D}_m]_{r\mathcal{Z}}(\mathbf{c}))$$

which by (16.11) is

$$([\mathcal{D}_1^\natural]_{r\mathcal{Z}}(\mathbf{c}),\dots,[\mathcal{D}_m^\natural]_{r\mathcal{Z}}(\mathbf{c})).$$

So there is a positive integer $N^\natural$ with

$$N^\natural([\mathcal{D}_1^\natural]_{r\mathcal{Z}}(\mathbf{c}),\dots,[\mathcal{D}_m^\natural]_{r\mathcal{Z}}(\mathbf{c}))$$

in $\mathcal{V}_\mathcal{Z}(\mathbf{c})$. Being in $(\mathbf{G}_{\mathrm{a}}^{r-1})^m$ it has the form

$$([(g_1'^{\natural(\mathbf{c})})]_{r\mathcal{Z}(\mathbf{c})},\dots,[(g_m'^{\natural(\mathbf{c})})]_{r\mathcal{Z}(\mathbf{c})})$$

for $\mathbf{g}_1'^{\natural(\mathbf{c})},\dots,g_m'^{\natural(\mathbf{c})}$ on $\mathcal{X}(\mathbf{c})$. Thus there are $g_1''^{\natural(\mathbf{c})},\dots,g_m''^{\natural(\mathbf{c})}$ on $\mathcal{X}(\mathbf{c})$ (with suitable order conditions at $\mathcal{Z}(\mathbf{c})$ as above) so that

$$N^\natural\mathcal{D}_i^\natural(\mathbf{c})\ =\ (g_i'^{\natural(\mathbf{c})})+(g_i''^{\natural(\mathbf{c})})\ =\ (g_i^{\natural(\mathbf{c})})\quad(i=1,\dots,m)\tag{17.1}$$

for $g_i^{\natural(\mathbf{c})}=g_i'^{\natural(\mathbf{c})}g_i''^{\natural(\mathbf{c})}$ $(i=1,\dots,m)$. Then being in $\mathcal{V}_\mathcal{Z}(\mathbf{c})$ means $\mathrm{ord}_{\mathcal{Z}(\mathbf{c})}\varpi^{\natural(\mathbf{c})}\geq r-1$, where

$$\varpi^{\natural(\mathbf{c})}\ =\ \frac{1}{abdN^\natural}\sum_{i=1}^m\varrho_i(\mathbf{c})\frac{\mathrm{d}g_i^{\natural(\mathbf{c})}}{g_i^{\natural(\mathbf{c})}}.$$

Consider now $\chi^{(\mathbf{c})}=\varpi^\natural(\mathbf{c})-\varpi^{\natural(\mathbf{c})}$ on $\mathcal{X}(\mathbf{c})$. By definition $\varpi^\natural(\mathbf{c})$ vanishes to order at least $r-1$ at $\mathcal{Z}(\mathbf{c})$, and therefore so does $\chi^{(\mathbf{c})}$.

Next we show that $\chi^{(\mathbf{c})}$ is of the first kind. From (16.9) and (16.10) we get

$$\mathrm{Res}\ \varpi^\natural(\mathbf{c})\ =\ \frac{1}{abd}\sum_{i=1}^m\varrho_i(\mathbf{c})\mathcal{D}_i^\natural(\mathbf{c}).\tag{17.2}$$

On the other hand

$$\mathrm{Res}\ \varpi^{\natural(\mathbf{c})}\ =\ \frac{1}{abdN^\natural}\sum_{i=1}^m\varrho_i(\mathbf{c})(g_i^{\natural(\mathbf{c})})$$

which by (17.1) also works out as (17.2). Thus

$$\mathrm{Res}\ \chi^{(\mathbf{c})}=\mathrm{Res}\ \varpi^\natural(\mathbf{c})-\mathrm{Res}\ \varpi^{\natural(\mathbf{c})}=0.$$

As $\chi^{(\mathbf{c})}$ is already of the third kind, it must indeed be of the first kind.

Now $\varpi^\natural$ is not of the first kind, otherwise ϖ would be elementary integrable modulo differentials of the first kind, and we ruled out these right at the beginning (they obviously cannot lead to counterexamples). Thus $\varpi^\natural$ has strictly more than $2g-2$ zeroes with multiplicity. Thus so has $\chi^{(\mathbf{c})}$. This forces $\chi^{(\mathbf{c})}=0$ (the same zero estimate as before). And now $\varpi^\natural(\mathbf{c})=\varpi^{\natural(\mathbf{c})}$ is elementary integrable (for all $\mathbf{c}$ in $\mathbf{S}$). This completes the proof of Theorem 1.3(b).

18. More torsion points.

Let ϖ be a differential on $\mathcal{X}$ over $\overline{\mathbf{Q}}(C)$ of the third kind, not elementary integrable modulo differentials of the first kind. So there is at least one non-zero residue, and we have the usual (torsion-killing over-basis) Res $\varpi = \sum_{i=1}^m \varrho_i \mathcal{D}_i$ for $m \geq 1$. We saw in section 14 that if $\varpi(\mathbf{c})$ is elementary integrable and $\varrho_1(\mathbf{c}), \dots, \varrho_m(\mathbf{c})$ are linearly independent over $\mathbf{Q}$ then the broad classes $[\mathcal{D}_1(\mathbf{c})], \dots, [\mathcal{D}_m(\mathbf{c})]$ are all torsion. For the proof of Theorem 1.3(a) we will need the following refinement for narrow classes, assuming certain of the conditions of section 16.

Lemma 18.1. *Suppose ϖ on $\mathcal{X}$ over $\overline{\mathbf{Q}}(C)$ is of the third kind, not elementary integrable modulo differentials of the first kind, and that (E0) with $\mathcal{E}$ holds for $\mathcal{J}$ except possibly for the condition of complex multiplication. Suppose also that (E1) holds with $[\mathcal{D}_1], \dots, [\mathcal{D}_m]$ linearly independent over $\mathbf{Z}$, and that (E2) holds; also that there is a positive integer t such that for every zero $\mathcal{Z}$ of $\varpi^\natural$ with $\mathcal{W}_i = \vartheta_i(\mathcal{Z})$ $(i = 1, \dots, m)$ the point*

$$\mathcal{T}_\mathcal{Z} \;=\; a\,(e_1[\vartheta_{1*}\mathcal{D}_1]_{r\mathcal{W}_1}, \dots, e_m[\vartheta_{m*}\mathcal{D}_m]_{r\mathcal{W}_m})$$

on $\mathcal{E}_{r\mathcal{W}_1} \times \cdots \times \mathcal{E}_{r\mathcal{W}_m}$ projects to $t([\mathcal{D}], \dots, [\mathcal{D}])$ on $\mathcal{E}^m$. Let $\mathbf{c}$ be such that $\varpi(\mathbf{c})$ is elementary integrable and $\varrho_1(\mathbf{c}), \dots, \varrho_m(\mathbf{c})$ are linearly independent over $\mathbf{Q}$. Then the $\vartheta_{i*}\mathcal{D}_i(\mathbf{c})$ are prime to $\mathcal{W}_i(\mathbf{c})$ $(i = 1, \dots, m)$ and the point

$$\mathcal{T}_\mathcal{Z}(\mathbf{c}) \;=\; a\,(e_1[\vartheta_{1*}\mathcal{D}_1]_{r\mathcal{W}_1}(\mathbf{c}), \dots, e_m[\vartheta_{m*}\mathcal{D}_m]_{r\mathcal{W}_m}(\mathbf{c}))$$

is torsion on $\mathcal{G}_\mathcal{Z}(\mathbf{c}) = \mathcal{F}_\mathcal{Z}(\mathbf{c})/\mathcal{U}_\mathcal{Z}(\mathbf{c})$, where $\mathcal{F}_\mathcal{Z}(\mathbf{c})$ is the fibre product of the $\mathcal{E}_{r\mathcal{W}_i(\mathbf{c})}$ $(i = 1, \dots, m)$ and $\mathcal{U}_\mathcal{Z}(\mathbf{c})$ is the set of $([k_1]_{r\mathcal{W}_1(\mathbf{c})}, \dots, [k_m]_{r\mathcal{W}_m(\mathbf{c})})$ with

$$\operatorname{ord}_{\mathcal{Z}(\mathbf{c})}\left(\sum_{i=1}^m \varrho_i(\mathbf{c})\vartheta_i^*\frac{\mathrm{d}k_i}{k_i}\right) \;\geq\; r-1.$$

Proof. The assumption on the independence of $[\mathcal{D}_1], \dots, [\mathcal{D}_m]$ is not really necessary, but it seems to make certain aspects of the structure clearer.

The arguments of section 14 lead to (14.1) and (14.2), because we are assuming that $\varrho_1(\mathbf{c}), \dots, \varrho_m(\mathbf{c})$ are linearly independent.

Recall now (16.10) and (16.11). Here $\varrho_1^\natural, \dots, \varrho_m^\natural$ remain independent over $\mathbf{Q}$; but also $\mathcal{D}_1^\natural, \dots, \mathcal{D}_m^\natural$ remain independent over $\mathbf{Z}$ because we assumed $[\mathcal{D}_1], \dots, [\mathcal{D}_m]$ are independent. Thus (16.10) is shortest. It follows that the residue group $\mathcal{R}^\natural$ of $\varpi^\natural$ has rank $m^\natural \geq m$. On the other hand it is clear that $\mathcal{R}^\natural$ is contained in $\mathbf{Z}\varrho_1^\natural + \cdots + \mathbf{Z}\varrho_m^\natural$, so $m^\natural \leq m$. Hence $m^\natural = m$ and $\varrho_1^\natural, \dots, \varrho_m^\natural$ are an over-basis for $\mathcal{R}^\natural$.

For the specialization we find using (14.2) that

$$\varpi^\natural(\mathbf{c}) \;=\; \varpi(\mathbf{c}) - \frac{1}{ab}\sum_{i=1}^m \frac{\varrho_i(\mathbf{c})}{d_i}\frac{\mathrm{d}\hbar_i(\mathbf{c})}{\hbar_i(\mathbf{c})} \;=\; \frac{1}{abdN}\sum_{i=1}^m \varrho_i(\mathbf{c})\frac{\mathrm{d}g_i^{\natural(\mathbf{c})}}{g_i^{\natural(\mathbf{c})}} \tag{18.1}$$

and

$$g_i^{\natural(\mathbf{c})} \;=\; (g_i^{(\mathbf{c})})^{abd}\hbar_i(\mathbf{c})^{-Ne_i} \quad (i = 1, \dots, m). \tag{18.2}$$

Also using (14.1) we find for the divisors

$$(g_i^{\natural(\mathbf{c})}) \;=\; abd(g_i^{(\mathbf{c})}) - Ne_i(\hbar_i(\mathbf{c})) \;=\; N\mathcal{D}_i^\natural(\mathbf{c}) \;\; (i = 1, \dots, m). \tag{18.3}$$

For us the fact that these $\mathcal{D}_i^\natural$ in (16.11) are images by ϑ_i^* will be crucial; we already noted during the discussion of $\phi_\mathbf{m}^*$ in section 16 that pull-backs can be far from surjective.

Now by (18.1) we have

$$abdN\varpi^\natural(\mathbf{c}) = \sum_{i=1}^m \varrho_i(\mathbf{c})\frac{\mathrm{d}g_i^{\natural(\mathbf{c})}}{g_i^{\natural(\mathbf{c})}}$$

which has a zero of order $r-1$ at the specialized point $\mathcal{Z}(\mathbf{c})$. In particular no pole, and so $(g_1^{\natural(\mathbf{c})}), \dots, (g_m^{\natural(\mathbf{c})})$ are prime to $\mathcal{Z}(\mathbf{c})$ from the linear independence of $\varrho_1(\mathbf{c}), \dots, \varrho_m(\mathbf{c})$ over $\mathbf{Q}$. Thus by (18.3)

$$N([\mathcal{D}_1^\natural]_{r\mathcal{Z}}(\mathbf{c}), \dots, [\mathcal{D}_m^\natural]_{r\mathcal{Z}}(\mathbf{c})) \;=\; ([(g_1^{\natural(\mathbf{c})})]_{r\mathcal{Z}(\mathbf{c})}, \dots, [(g_m^{\natural(\mathbf{c})})]_{r\mathcal{Z}(\mathbf{c})})$$

lies in the subspace $\mathcal{V}_{\mathcal{Z}}(\mathbf{c})$ of $(\mathbf{G}_{\mathrm{a}}^{r-1})^m$ in $(\mathcal{J}_{r\mathcal{Z}}(\mathbf{c}))^m$, where $\mathcal{V}_{\mathcal{Z}}$ in $(\mathbf{G}_{\mathrm{a}}^{r-1})^m$ inside $(\mathcal{J}_{r\mathcal{Z}})^m$ is defined by

$$\mathrm{ord}_{\mathcal{Z}}\left(\sum_{i=1}^{m}\varrho_i\frac{\mathrm{d}f_i}{f_i}\right)\geq r-1. \tag{18.4}$$

This gives a torsion point (of order dividing N)

$$([\mathcal{D}_1^\natural]_{r\mathcal{Z}}(\mathbf{c}),\dots,[\mathcal{D}_m^\natural]_{r\mathcal{Z}}(\mathbf{c}))$$

on the quotient $(\mathcal{J}_{r\mathcal{Z}}(\mathbf{c}))^m/\mathcal{V}_{\mathcal{Z}}(\mathbf{c})$.

As before we have $\mathcal{Y}=(\vartheta_1^*,\dots,\vartheta_m^*)$ from $\mathcal{E}_{r\mathcal{W}_1}\times\cdots\times\mathcal{E}_{r\mathcal{W}_m}$ to $(\mathcal{J}_{r\mathcal{Z}})^m$. Thanks to (16.11) we have

$$ab\mathcal{Y}(e_1[\vartheta_{1*}\mathcal{D}_1]_{r\mathcal{W}_1},\dots,e_m[\vartheta_{m*}\mathcal{D}_m]_{r\mathcal{W}_m})\ =\ ([\mathcal{D}_1^\natural]_{r\mathcal{Z}},\dots,[\mathcal{D}_m^\natural]_{r\mathcal{Z}})$$

(note that $\vartheta_{i*}\mathcal{D}_i$ is prime to $\mathcal{W}_i$ else $\mathcal{D}_i^\natural$ would not be prime to $\mathcal{Z}$ and so $\mathcal{D}_i^\natural(\mathbf{c})$ not prime to $\mathcal{Z}(\mathbf{c})$ either, leading by (18.3) and (18.1) to $\mathcal{Z}(\mathbf{c})$ being a pole of $\varpi^\natural(\mathbf{c})$ rather than a zero - compare the argument in (E4) above). We thus get a torsion point

$$\mathcal{T}_{\mathcal{Z}}(\mathbf{c})\ =\ a(e_1[\vartheta_{1*}\mathcal{D}_1]_{r\mathcal{W}_1}(\mathbf{c}),\dots,e_m[\vartheta_{m*}\mathcal{D}_m]_{r\mathcal{W}_m}(\mathbf{c}))$$

on $(\prod_{i=1}^m\mathcal{E}_{r\mathcal{W}_i}(\mathbf{c}))/\mathcal{U}_{\mathcal{Z}}(\mathbf{c})$, because $\mathcal{U}_{\mathcal{Z}}=\mathcal{Y}^{-1}\mathcal{V}_{\mathcal{Z}}$ in $(\mathbf{G}_{\mathrm{a}}^{r-1})^m$, and of course $\mathcal{T}_{\mathcal{Z}}(\mathbf{c})$ is the specialization of

$$\mathcal{T}_{\mathcal{Z}}\ =\ a(e_1[\vartheta_{1*}\mathcal{D}_1]_{r\mathcal{W}_1},\dots,e_m[\vartheta_{m*}\mathcal{D}_m]_{r\mathcal{W}_m})$$

as in (E4). By hypothesis this is on the fibre product and thus so is $\mathcal{T}(\mathbf{c})$. This completes the proof. □

19. Elusive invariance.

Here we establish the result mentioned in section 16, working throughout with $\mathcal{X}$ over $\overline{\mathbf{Q}}(C)$.

Proposition 19.1. *If ϖ is elusive and ε is elementary integrable, then $\varpi+\varepsilon$ is elusive.*

Proof. By familiar arguments it suffices to do it when ϖ,ε are of the third kind. Even though the result has nothing to do with specializations, these will be used in the proof and so we take a suitable cover of C to ensure everything specializes well.

Write as usual Res $\varpi=\sum_{i=1}^m\varrho_i\mathcal{D}_i$ with an over-basis that is torsion-killing (recall that this means the classes $[\mathcal{D}_1],\dots,[\mathcal{D}_m]$ are non-torsion). We use induction on $m\geq 1$. As in section 14, this enables us to assume that $[\mathcal{D}_1],\dots,[\mathcal{D}_m]$ are linearly independent over $\mathbf{Z}$. For if not, then f exists as in (14.3) (also torsion-killing) and then we see that

$$a_m(\varpi+\varepsilon)=\left(a_m\varpi-\varrho_m\frac{\mathrm{d}f}{f}\right)+\left(\varrho_m\frac{\mathrm{d}f}{f}+a_m\varepsilon\right)$$

is elusive.

It suffices now to check the case of a single $\varepsilon=c\mathrm{d}g/g$ with g non-constant and c constant.

Write $\dot\varpi=\varpi+\varepsilon$ and as usual a shortest Res $\dot\varpi=\sum_{i=1}^{\dot m}\dot\varrho_i\dot{\mathcal{D}}_i$, where we shall soon choose $\dot\varrho_1,\dots,\dot\varrho_{\dot m}$ torsion-killing. Here $\dot m\geq 1$ otherwise $\dot\varpi$ would be of the second kind, so also of the first kind, contradicting the fact that ϖ is elusive. We have also

$$\text{Res }\dot\varpi=c(g)+\sum_{i=1}^{m}\varrho_i\mathcal{D}_i \tag{19.1}$$

for the divisor (g), but this is probably not shortest. Anyway by Lemma 11.1(ii) $\dot{\mathcal{D}}_1,\dots,\dot{\mathcal{D}}_{\dot m}$ must be linear combinations over $\mathbf{Q}$ of $(g),\mathcal{D}_1,\dots,\mathcal{D}_m$. Multiplying by a denominator and taking classes, we see that there is a positive integer $\dot N$ with $\dot N\dot{\mathfrak{D}}\subseteq\mathfrak{D}$ for the groups

$$\mathfrak{D}=\mathbf{Z}[\mathcal{D}_1]+\cdots+\mathbf{Z}[\mathcal{D}_m],\quad\dot{\mathfrak{D}}=\mathbf{Z}[\dot{\mathcal{D}}_1]+\cdots+\mathbf{Z}[\dot{\mathcal{D}}_{\dot m}].$$

(nothing to do with polynomial rings!) in $\mathcal{J}$.

From $\varpi=\dot\varpi-\varepsilon$ follows in the same way $N\mathfrak{D}\subseteq\dot{\mathfrak{D}}$ so the two groups are in a natural sense commensurable.

As $\mathfrak{D}$ has rank m, it follows that $\dot{\mathfrak{D}}$ also has rank m. Therefore $\dot{m} \geq m$.

On the other hand, for the residue spaces

$$\mathcal{S} = \mathbf{Q} \otimes \mathcal{R} = \mathbf{Q}\varrho_1 + \cdots + \mathbf{Q}\varrho_m, \quad \dot{\mathcal{S}} = \mathbf{Q} \otimes \dot{\mathcal{R}} = \mathbf{Q}\dot{\varrho}_1 + \cdots + \mathbf{Q}\dot{\varrho}_{\dot{m}}$$

we have

$$\dot{\mathcal{S}} \subseteq \mathcal{S} + \mathbf{Q}c \tag{19.2}$$

and so $\dot{m} \leq m + 1$. Also

$$\dot{\mathcal{R}} \subseteq \mathcal{R} + \mathbf{Z}c \tag{19.3}$$

for the groups.

Now there are two cases I,II according to whether c lies in $\mathcal{S}$ or not.

(I) First suppose c lies in $\mathcal{S}$, as for example in (16.14). Then by (19.2) we get $\dot{\mathcal{S}} \subseteq \mathcal{S}$ so $\dot{m} \leq m$. Thus in this case $\dot{m} = m$.

Now we replace ϱ_i by ϱ_i/q for some integer q so large that c lies in the new $\mathbf{Z}\varrho_1 + \cdots + \mathbf{Z}\varrho_m$. This new group still contains $\mathcal{R}$, so by (19.3) $\dot{\mathcal{R}}$ as well, and so we can choose

$$\dot{\varrho}_i = \varrho_i \quad (i = 1, \ldots, m), \tag{19.4}$$

indeed torsion-killing.

Writing c as an integral linear combination of $\varrho_1, \ldots, \varrho_m$, we find

$$[\dot{\mathcal{D}}_i] = [\mathcal{D}_i] \quad (i = 1, \ldots, m). \tag{19.5}$$

We now proceed to check that the conditions of elusive for ϖ carry over to $\dot{\varpi}$. In fact for (E0) there is nothing to do, as it is independent of the differentials; and for (E1),(E2) it suffices to add overhead dots everywhere. And in (E3) we can take

$$\dot{\vartheta}_i = \vartheta_i \quad (i = 1, \ldots, m). \tag{19.6}$$

We do not know how to check the rest of (E3) directly, as there is no obvious relation between the zeroes $\dot{\mathcal{Z}}$ of $\dot{\varpi}^\natural$ and the zeroes $\mathcal{Z}$ of $\varpi^\natural$. It is Lemma 16.3 which by-passes this problem with either (16.17) or (16.18). Thus the $\dot{\mathcal{G}}_{\dot{\mathcal{Z}}}$ are split for every zero $\dot{\mathcal{Z}}$ of $\dot{\varpi}^\natural$.

For (E4) we have no analogue of Lemma 16.3. But the projection of $\dot{\mathcal{T}}_{\dot{\mathcal{Z}}}$ for $\dot{\varpi}$ involves $\dot{a}\dot{e}_i[\dot{\vartheta}_{i*}\dot{\mathcal{D}}_i] = \dot{t}[\dot{\mathcal{D}}]$ for $\dot{t} = t$. Thus we are indeed on the fibre product $\dot{\mathcal{F}}_{\dot{\mathcal{Z}}}$.

For the rest of (E4) we have to argue again indirectly, this time as follows.

If the condition $\dot{\varsigma}_{\dot{\mathcal{Z}}}(\dot{\mathcal{T}}_{\dot{\mathcal{Z}}}) = 0$ (again the calligraphic σ) fails for some $\dot{\mathcal{Z}}$, take any $\mathbf{c}$ with the specialization $\dot{\varpi}(\mathbf{c})$ elementary integrable. If $\dot{\varrho}_1(\mathbf{c}), \ldots, \dot{\varrho}_m(\mathbf{c})$ are independent, then by Lemma 18.1 we get a torsion point $\dot{\mathcal{T}}_{\dot{\mathcal{Z}}}(\mathbf{c})$ on $\dot{\mathcal{G}}_{\dot{\mathcal{Z}}}(\mathbf{c})$. So $\dot{\varsigma}_{\dot{\mathcal{Z}}}(\dot{\mathcal{T}}_{\dot{\mathcal{Z}}})(\mathbf{c})$ is torsion on the additive part, that is, zero. This gives a non-trivial equation for $\mathbf{c}$, and so the number of such $\mathbf{c}$ is at most finite. The same conclusion holds if $\dot{\varrho}_1(\mathbf{c}), \ldots, \dot{\varrho}_m(\mathbf{c})$ are not independent, because then $[\mathbf{Q}(\mathbf{c}) : \mathbf{Q}]$ is bounded and we can appeal to Proposition 1.4.

Thus if some $\dot{\varsigma}_{\dot{\mathcal{Z}}}(\dot{\mathcal{T}}_{\dot{\mathcal{Z}}}) \neq 0$, there would be at most finitely many $\mathbf{c}$ with $\dot{\varpi}(\mathbf{c})$ elementary integrable. As $\dot{\varpi} = \varpi + \varepsilon$, the same would hold for $\varpi(\mathbf{c})$. But as ϖ itself is elusive this contradicts Theorem 1.3(b)!

Thus indeed we have shown that $\dot{\varpi}$ is elusive in this case that c lies in $\mathcal{S}$.

(II) Suppose that c does not lie in $\mathcal{S}$, as for example in (16.13). Then $c, \varrho_1, \ldots, \varrho_m$ are independent. Also $(g) \neq 0, \mathcal{D}_1, \ldots, \mathcal{D}_m$ are independent, otherwise clearing denominators and taking classes would contradict the independence of $[\mathcal{D}_1], \ldots, [\mathcal{D}_m]$. Thus by Lemma 11.1(i) the representation (19.1) is also shortest, so $\dot{m} = m + 1$.

Now (19.3) (without the q-trick) shows that we could assume (19.4) and also

$$\dot{\varrho}_{m+1} = c. \tag{19.7}$$

But then $\dot{\mathcal{D}}_{m+1}$ comes out as (g), so its class is zero and torsion is not killed. It suffices to make the single change

$$\dot{\varrho}_m = \varrho_m - c \tag{19.8}$$

in (19.4). Then we find even

$$\dot{\mathcal{D}}_i = \mathcal{D}_i \quad (i = 1, \ldots, m)$$

as divisors, as well as

$$[\dot{\mathcal{D}}_{m+1}] = [\dot{\mathcal{D}}_m] = [\mathcal{D}_m].$$

Thus indeed $\dot{\varrho}_1, \dots, \dot{\varrho}_{\dot{m}}$ are torsion-killing.

Again we can check that the conditions of elusive for ϖ carry over to $\dot{\varpi}$, taking into account the extra (19.7) and the change (19.8). For example we find

$$\dot{\vartheta}_{m+1} = \vartheta_m = \dot{\vartheta}_m \tag{19.9}$$

(incidentally not independent over $\mathbf{Z}$ as will be secured in the next section).

Now for example in (16.18) for $\dot{\varpi}$ we find

$$\dot{\varrho}_i \dot{\vartheta}_i^* \chi = \varrho_i \vartheta_i^* \chi \quad (i = 1, \dots, m-1)$$

as well as

$$\dot{\varrho}_m \dot{\vartheta}_m^* \chi + \dot{\varrho}_{m+1} \dot{\vartheta}_{m+1}^* \chi \;=\; \varrho_m \vartheta_m^* \chi.$$

So as before the $\dot{\mathcal{G}}_{\dot{\mathcal{Z}}}$ are split for every zero $\dot{\mathcal{Z}}$ of $\dot{\varpi}^\natural$.

Also just as before we check (E4) for $\dot{\varpi}$.

This completes the proof of Proposition 19.1. □

It would be nice here to eliminate the use of Theorem 1.3(b).

20. Proof of Theorem 1.3(a).

As above, suppose our underlying curve $\mathcal{X}$ has Jacobian $\mathcal{J}$, now not necessarily simple. There is an isogeny ι from $\mathcal{J}$ to some $\mathcal{E}_1^{n_1} \times \cdots \times \mathcal{E}_p^{n_p} \times \mathcal{A}_1 \times \cdots \times \mathcal{A}_q$, with positive powers of mutually non-isogenous elliptic curves $\mathcal{E}_1, \dots, \mathcal{E}_p$ and simple abelian varieties $\mathcal{A}_1, \dots, \mathcal{A}_q$ of dimension at least two. Here we allow $p = 0$ or $q = 0$. Further if some $\mathcal{E}$ has complex multiplication CM then we can assume that it is defined over $\overline{\mathbf{Q}}$.

If ϖ is $\varpi_0 + \varepsilon$ for ϖ_0 of the first kind (of course non-zero) and ε elementary integrable, then as in section 14 we get the required finiteness.

So we can assume ϖ is not such a $\varpi_0 + \varepsilon$, just as in the definition of elusive. As in earlier sections we take a suitable cover of C.

Of course we suppose from now on that ϖ is not elusive.

And as in section 17 it will be enough to consider differentials ϖ of the third kind.

Take $\mathbf{c}$ such that the specialization $\varpi(\mathbf{c})$ is elementary integrable as in (13.1). Then as in section 14 we get divisors $\mathcal{D}_1, \dots, \mathcal{D}_m$ on $\mathcal{X}$ with classes $[\mathcal{D}_1], \dots, [\mathcal{D}_m]$ are all non-torsion but whose specializations $[\mathcal{D}_1(\mathbf{c})], \dots, [\mathcal{D}_m(\mathbf{c})]$ are all torsion. Also as there we can assume that $\varrho_1(\mathbf{c}), \dots, \varrho_m(\mathbf{c})$ are independent over $\mathbf{Q}$.

We can still assume using induction on m that $[\mathcal{D}_1], \dots, [\mathcal{D}_m]$ are independent over $\mathbf{Z}$, because by the crucial Proposition 19.1 the $a_m \varpi - \varrho_m \mathrm{d}f/f$ in (14.3) remains not elusive.

Now in the arguments that follow, failure to prove Theorem 1.3(a) will result in the verification of the conditions (E0),(E1),(E2),(E3),(E4) one by one. This gives the contradiction that ϖ is elusive.

If some $\iota([\mathcal{D}_i])$ has a non-torsion projection to some $\mathcal{A}$ then Theorem 1.7 gives the required finiteness of the $\mathbf{c}$ straightaway (this settles the case $p = 0$).

So replacing $\mathcal{D}_1, \dots, \mathcal{D}_m$ by non-zero integer multiples of themselves (which by (14.1) amounts to replacing $g_1^{(\mathbf{c})}, \dots, g_m^{(\mathbf{c})}$ by non-zero integer powers of themselves) we can assume that their projections to $\mathcal{A}_1, \dots, \mathcal{A}_q$ are all zero.

Now $\iota([\mathcal{D}_1])$ is not torsion and so it has some non-torsion projection on some $\mathcal{E}^n$. But then by [52] we can assume that the projections on the other $\mathcal{E}^n$ are torsion. In fact the same arguments with multiples show that we can assume that the projections of all $\iota([\mathcal{D}_i])$ on the other $\mathcal{E}^n$ are zero.

Thus writing $\iota(\mathcal{J}) = \mathcal{E}^n \times \mathcal{B}$ we see that $\mathcal{B}$ contains no abelian subvariety isogenous to $\mathcal{E}$ (and if $q = 0$ we can just forget about $\mathcal{B}$ in the arguments below). Thus we have condition (E0) of the definition of elusive except for the CM part. That will follow a bit later. We can assume

$$\pi_{\mathcal{B}}(\iota([\mathcal{D}_i])) = 0 \quad (i = 1, \dots, m) \tag{20.1}$$

for the projection $\pi_{\mathcal{B}}$ from $\mathcal{E}^n \times \mathcal{B}$ to $\mathcal{B}$. Now (E1) is completely verified.

Next we go for (E2). As in section 16 we fix an embedding $\jmath$ of $\mathcal{X}$ into $\mathcal{J}$ by $\jmath(\mathcal{P}) = [\mathcal{P} - \mathcal{P}_0]$ and we identify $\mathcal{E}$ with its Jacobian. As in Lemma 16.1 we obtain maps $\varphi_1, \dots, \varphi_n$ from $\mathcal{X}$ to $\mathcal{E}$, with $\iota = (\varphi_{1*}, \dots, \varphi_{n*}, \pi_{\mathcal{B}} \circ \iota)$, which are linearly independent, even over the endomorphism ring $\mathcal{O}$ of $\mathcal{E}$.

Thanks to (20.1) we may now write

$$\iota([\mathcal{D}_i]) \;=\; ([\mathcal{D}_{i1}], \dots, [\mathcal{D}_{in}], 0) \quad (i = 1, \dots, m) \tag{20.2}$$

for divisors $\mathcal{D}_{i1}, \dots, \mathcal{D}_{in}$ of degree zero on $\mathcal{E}$.

If two from the classes $[\mathcal{D}_{ik}]$ $(i = 1, \dots, m;\ k = 1, \dots, n)$ are independent over $\mathcal{O}$ then we get finiteness from [51]. Thus we may assume that

$$a[\mathcal{D}_{ik}] = \alpha_{ik*}[\mathcal{D}] \quad (i = 1, \dots, m;\ k = 1, \dots, n) \tag{20.3}$$

for some divisor $\mathcal{D}$ on $\mathcal{E}$ (also of degree zero), some α_{ik} in $\mathcal{O}$ (with the same identification as above) and some positive integer a. We are nearly at (E2) except for the last part.

If $[\mathcal{D}]$ were defined over $\overline{\mathbf{Q}}$ then, because it is non-torsion by the remark just after (E2), the specialization $[\mathcal{D}(\mathbf{c})] = [\mathcal{D}]$ would be non-torsion for any $\mathbf{c}$. Now not all $\alpha_{ik} = 0$ in (20.3), else (20.2) would imply that all $[\mathcal{D}_i]$ are torsion, a subcontradiction. Thus again by (20.3) some $[\mathcal{D}_{ik}(\mathbf{c})]$ is non-torsion. But this again by (20.2) contradicts the fact that $[\mathcal{D}_i(\mathbf{c})]$ is torsion. Thus we have arrived at the entire condition (E2).

Now as in Lemma 16.1 the maps $\varphi_{k*} \circ \varphi_h^*$ from $\mathcal{E}$ to $\mathcal{E}$ are γ_{kh*} for γ_{kh} in $\mathcal{O}$.

We now start some calculations which will eventually lead to (E3),(E4) and the missing part of (E0). With the natural involution on $\mathcal{O}$ we get β_{ih} in $\mathcal{O}$ such that

$$\sum_{h=1}^{n} \overline{\beta_{ih}} \gamma_{kh} = l\alpha_{ik} \quad (i = 1, \dots, m;\ k = 1, \dots, n) \tag{20.4}$$

as in (16.24) (or in informal matrix notation $\overline{B}\Gamma^t = lA$) for some positive integer l. As in (16.23) we write

$$\vartheta_i = \sum_{h=1}^{n} \beta_{ih} \varphi_h \quad (i = 1, \dots, m) \tag{20.5}$$

from $\mathcal{X}$ to $\mathcal{E}$.

Soon we have to check the missing CM part of (E0). For this purpose it is convenient now to prove that

$$\vartheta_1, \dots, \vartheta_m \text{ are independent over } \mathbf{Z} \tag{20.6}$$

(which by the way failed in (19.9) for $\dot{\varpi}$). If not, then the independence (over $\mathcal{O}$) of $\varphi_1, \dots, \varphi_n$ would give $\lambda_1, \dots, \lambda_m$ in $\mathbf{Z}$, not all zero, with $\sum_{i=1}^{m} \lambda_i \beta_{ih} = 0$ $(h = 1, \dots, n)$ (informal $\lambda B = 0$). But then from (20.4)

$$\sum_{i=1}^{m} \overline{\lambda_i} \alpha_{ik} \;=\; l^{-1} \sum_{i=1}^{m} \sum_{h=1}^{n} \overline{\lambda_i \beta_{ih}} \gamma_{kh} \;=\; 0 \quad (k = 1, \dots, n)$$

(informal $\overline{\lambda} A = l^{-1} \overline{\lambda B} \Gamma^t = 0$). But now (remember that for the moment the λ_i are in $\mathbf{Z}$)

$$\iota(a \sum_{i=1}^{m} \lambda_i^* [\mathcal{D}_i]) \;=\; (\sum_{i=1}^{m} \lambda_i^* \alpha_{i1*}[\mathcal{D}], \dots, \sum_{i=1}^{m} \lambda_i^* \alpha_{in*}[\mathcal{D}], 0) \;=\; 0$$

from (20.2) and (20.3) contradicts the independence of $[\mathcal{D}_1], \dots, [\mathcal{D}_m]$ over $\mathbf{Z}$. This is what we wanted.

We now use $\varpi^\natural$ as in (16.9) with $\varpi^\natural(\mathbf{c})$ as in (18.1).

We next fix a differential $\chi \neq 0$ of the first kind on $\mathcal{E}$ and consider the pull-backs $\vartheta_i^* \chi$ $(i = 1, \dots, m)$ on $\mathcal{X}$, also of the first kind. We write

$$\varpi_0 = \sum_{i=1}^{m} \varrho_i \vartheta_i^* \chi, \tag{20.7}$$

as in Lemma 16.3, also of the first kind.

Assume for the moment that $\varpi_0 \neq 0$. In this case we will prove Theorem 1.3(a) without bothering much further about (E0), (E1), (E2), (E3), (E4). Then by Lemma 16.3 we see that (E3) cannot hold. Thus there is a zero $\mathcal{Z}$ of $\varpi^\natural$, of order say $r-1 \geq 1$, such that $\mathcal{G} = \mathcal{F}/\mathcal{U}$ is non-split, where $\mathcal{F} = \mathcal{F}_\mathcal{Z}$ is the product of the generalized Jacobians $\mathcal{E}_{r\mathcal{W}_i}$ fibred over $\mathcal{E}$ embedded diagonally with $\mathcal{W}_i = \vartheta_i(\mathcal{Z})$ $(i = 1, \dots, m)$ and $\mathcal{U} = \mathcal{U}_\mathcal{Z}$ is the subspace of the linear part consisting of those $([(k_1)]_{r\mathcal{W}_1}, \dots, [(k_m)]_{r\mathcal{W}_m})$ such that (16.12) holds.

We will eventually apply Theorem 1.6 to some projection of $\mathcal{G} = \mathcal{G}_\mathcal{Z}$.

We use the point

$$\mathcal{T} = \mathcal{T}_\mathcal{Z} \;=\; a\,(e_1[\vartheta_{1*}\mathcal{D}_1]_{r\mathcal{W}_1}, \dots, e_m[\vartheta_{m*}\mathcal{D}_m]_{r\mathcal{W}_m})$$

defined in (E4).

Then (16.5) (with $\mathcal{M} = [\mathcal{D}_i]$ and so on) shows that $\mathcal{T}$ projects down to

$$a(e_1[\vartheta_{1*}\mathcal{D}_1], \dots, e_m[\vartheta_{m*}\mathcal{D}_m]) \;=\; \frac{d}{l}([\mathcal{D}], \dots, [\mathcal{D}]) \tag{20.8}$$

on $\mathcal{E}^m$, as required in the first part of (E4). So by Lemma 18.1 the specialization $\mathcal{T}(\mathbf{c})$ is torsion on $\mathcal{G}(\mathbf{c})$.

Because $\mathcal{G}$ is non-split, it projects onto a non-split extension by a single $\mathbf{G}_\mathrm{a}$ (see Proposition A.2 of the Appendix) and as at the end of section 14 we can conclude using Theorem 1.6, as long as $\mathcal{T}$ doesn't project down to torsion on $\mathcal{E}^m$. But using (20.8) and recalling (20.2),(20.3) we see that $[\mathcal{D}]$ is not torsion.

But what if $\varpi_0 = 0$ in (20.7)? Then we show that $\mathcal{E}$ has complex multiplication, using a variation of the argument in the paragraph following (16.25).

We note that the construction of $\varphi_1, \dots, \varphi_n$ gives $\tilde\varphi_1, \dots, \tilde\varphi_n$ from $\mathcal{J}$ to $\mathcal{E}$ with $\varphi_k = \tilde\varphi_k \circ \jmath$. We obtain $\xi_1, \dots, \xi_m$ with $\vartheta_i = \xi_i \circ \jmath$. Thus $\varpi_0 = 0$ would imply $\jmath^*(\sum_{i=1}^m \varrho_i \xi_i^* \chi) = 0$. Now $\jmath^*$ is well-known to be an isomorphism from differentials of the first kind on $\mathcal{J}$ to differentials of the first kind on $\mathcal{X}$. Thus $\sum_{i=1}^m \varrho_i \xi_i^* \chi = 0$ too. Also if there is no complex multiplication then $\xi = (\xi_1, \dots, \xi_m)$ would be surjective from $\mathcal{J}$ to $\mathcal{E}^m$ because $\vartheta_1, \dots, \vartheta_m$ are linearly independent over the endomorphism ring $\mathbf{Z}$ by (20.6). And $\xi^* \chi_i = \xi_i^* \chi$ for χ_i on $\mathcal{E}^m$ corresponding to the ith factor. From the injectivity of ξ^* there would follow $\sum_{i=1}^m \varrho_i \chi_i = 0$ too; an absurdity.

Thus indeed $\mathcal{E}$ has complex multiplication. But that is the missing part of condition (E0).

Now if it happened anyway that $\mathcal{G}_\mathcal{Z}$ (as defined in (E3) of course) is non-split for some zero $\mathcal{Z}$ of $\varpi^\natural$, then we can proceed as just above.

Otherwise, if $\mathcal{G}_\mathcal{Z}$ is split for every zero $\mathcal{Z}$ of $\varpi^\natural$, then we have a surjective homomorphism $\varsigma_\mathcal{Z}$ from $\mathcal{G}_\mathcal{Z}$ to $\mathbf{G}_\mathrm{a}^{d_\mathcal{Z}-1}$ as in (E3), where $d_\mathcal{Z}$ is the dimension of $\mathcal{G}_\mathcal{Z}$ (this could be calculated explicitly in terms of ramification). This then establishes (E3).

Thus we now have all the conditions in the definition of elusive, apart from the second part $\varsigma_\mathcal{Z}(\mathcal{T}_\mathcal{Z}) = 0$ of (E4). For this we argue in the same style as in section 19. Suppose there is $\mathcal{Z}$ such that $\varsigma_\mathcal{Z}(\mathcal{T}_\mathcal{Z}) \neq 0$ in $\mathbf{G}_\mathrm{a}^{d_\mathcal{Z}-1}$. As $\mathcal{T}_\mathcal{Z}(\mathbf{c})$ is torsion on $\mathcal{G}_\mathcal{Z}(\mathbf{c})$ we deduce for the specialization $\varsigma_\mathcal{Z}(\mathcal{T}_\mathcal{Z})(\mathbf{c}) = 0$. This leads at once to the finiteness of the $\mathbf{c}$. Thus we can suppose that (E4) holds, and finally we have shown that ϖ is elusive (by the way disposing completely of Davenport's fourth obstacle).

21. Examples and further remarks.

21.1. **Examples.** The following examples are for case (a) of Theorem 1.3.

There are at most finitely many t in $\mathbf{C}$ for which

$$\frac{1}{(x^2-1)\sqrt{x^6+x+t}} \tag{21.1}$$

is elementary integrable; here $\mathcal{J}$ is simple of dimension 2. The same conclusion holds for

$$\frac{1}{(x^2-1)\sqrt{x^6+x^2+t}} \tag{21.2}$$

but now $\mathcal{J}$ is isogenous to a product of two non-isogenous elliptic curves without CM. And for

$$\frac{1}{(x^2-1)\sqrt{x^5+tx^3+x}} \tag{21.3}$$

where $\mathcal{J}$ is isogenous to the square of an elliptic curve without CM. And also for

$$\frac{1}{(x^2-t^2)\sqrt{x^6+x^4+\frac{29}{9}x^2+1}} \tag{21.4}$$

even though $\mathcal{J}$ is isogenous to a product of two elliptic curves exactly one of which has CM. And even for

$$\frac{1}{(x^2-t^2)\sqrt{x^5+\frac{14}{9}x^3+x}}, \tag{21.5}$$

$\mathcal{J}$ now being isogenous to the square of a CM elliptic curve. And more subtly for

$$\frac{1}{(x^2-t^2)\sqrt{x^6-3x^4+x^2+1}} \tag{21.6}$$

where now two non-isogenous CM elliptic curves turn up. And more simply for

$$\frac{1}{(x^2-t^2)\sqrt{x^3-x}} \tag{21.7}$$

where $\mathcal{J}$ is now itself a CM elliptic curve.

But when we make a tiny change, then there are infinitely many t in $\mathbf{C}$ for which

$$\frac{x}{(x^2-t^2)\sqrt{x^3-x}} \tag{21.8}$$

is elementary integrable. It is not identically so, and thus we are now in case (b) with something elusive.

The differentials corresponding to all the above examples are of the third kind.

It is amusing to continue the sequence (21.7),(21.8) by considering

$$\frac{x^d}{(x^2-t^2)\sqrt{x^3-x}} \qquad (d=2,3,4,5,\ldots). \tag{21.9}$$

(for which the corresponding differentials are generally not of the third kind). For example, we get finiteness for $d=2,3,4,5$; but for $d=3,5$ we can actually prove that there are no t at all (the reader is invited to tackle general d).

Now we give the details.

We start with (21.1). Here the considerations of section 14 suffice, because $g=2$ and the Jacobian of $y^2=x^6+x+t$ is simple (see [53] p. 2394). We have only to show that (21.1) is not elementary integrable. Fix s_+, s_- with $s_+^2=2+t, s_-^2=t$. The poles are at $\mathcal{P}=(1,s_+),\ \mathcal{Q}=(-1,s_-)$ together with $\mathcal{R}=(1,-s_+), \mathcal{S}=(-1,-s_-)$. The residues are $1/(2s_+), -1/(2s_-)$ together with $-1/(2s_+), 1/(2s_-)$, so $m=2$. Taking $\varrho_1=1/(2s_+), \varrho_2=-1/(2s_-)$ we find $\mathcal{D}_1=\mathcal{P}-\mathcal{R},\ \mathcal{D}_2=\mathcal{Q}-\mathcal{S}$. As in the discussion around (1.9), we see by ramification (at $t=-2,0$) that both of these are non-torsion, which does the trick.

For (21.2) the Jacobian is no longer simple, so we have to proceed to section 16. But no CM elliptic curves occur as a factor (see [53] p. 2397), so there are no elusive differentials. And ramification does the rest.

For (21.3) it is similar; that the elliptic curve in question has no CM is clear from (15.8), whose j-invariant is $64\frac{(3t-10)^3}{(t-2)(t+2)^2}$. (Actually it was examples like this that led us to the theory of the splitting line.)

For (21.4) we find that the curves $\mathcal{E}, \mathcal{E}'$ in (15.2) have invariants $1728, -\frac{778688}{729}$ respectively, so the first has CM by $\mathbf{Z}[i]$ and the second no CM. Therefore if the differential is elusive we must have $n=1$ and $\mathcal{B}=\mathcal{E}'$ in (E0). The isogeny ι can be constructed from the maps (15.3), which we denote now by φ, φ' in order to distinguish them from $\varphi_1,\ldots,\varphi_n$ in (E2). Then $\iota=(\varphi_*, \varphi'_*)$. Fix s with $s^2=t^6+t^4+\frac{29}{9}t^2+1$. The poles are at $\mathcal{P}=(t,s),\ \mathcal{Q}=(-t,s)$ together with $\mathcal{R}=(t,-s),\ \mathcal{S}=(-t,-s)$. The residues are $1/(2ts), -1/(2ts)$ together with $-1/(2ts), 1/(2ts)$ so now $m=1$ in (E1). Taking $\varrho_1=1/(2ts)$ we find $\mathcal{D}_1=\mathcal{P}-\mathcal{Q}-\mathcal{R}+\mathcal{S}$. Thus

$$\pi_{\mathcal{B}}(\iota[\mathcal{D}_1]) \ = \ \varphi'_*[\mathcal{D}_1] \ = \ \varphi'(\mathcal{P})-\varphi'(\mathcal{Q})-\varphi'(\mathcal{R})+\varphi'(\mathcal{S})$$

which works out as $4\mathcal{H}$ with $\mathcal{H} = (t^{-2}, t^{-3}s)$ on $\mathcal{E}'$. But this cannot be torsion because $\mathcal{H}$ is not. Thus the differential, call it now ϖ, is not elusive.

For (21.5) we find invariants 1728 in both, so again CM by $\mathbf{Z}[i]$. Therefore if the differential is elusive we must have $n = 2$ in (E0). Now the isogeny can be constructed from the maps (15.9), which we denote now by $\tilde\varphi_1, \tilde\varphi_2$; thus $\iota = (\tilde\varphi_{1*}, \tilde\varphi_{2*})$. Fix s with $s^2 = t^5 + \frac{14}{9}t^3 + t$. The poles are at $\mathcal{P} = (t, s)$, $\mathcal{Q} = (-t, is)$ together with $\mathcal{R} = (t, -s)$, $\mathcal{S} = (-t, -is)$. The residues are $1/(2ts), i/(2ts)$ together with $-1/(2ts), -i/(2ts)$. So $m = 2$ in (E1). Taking $\varrho_1 = 1/(2ts), \varrho_2 = i/(2ts)$ we find $\mathcal{D}_1 = \mathcal{P} - \mathcal{R}$, $\mathcal{D}_2 = \mathcal{Q} - \mathcal{S}$ in (E1); both non-torsion. For (E2) we take $\jmath(\mathcal{M}) = [\mathcal{M} - \infty]$ for the unique point at infinity. We find $\varphi_k(\mathcal{M}) = \tilde\varphi_k(\mathcal{M}) - \mathcal{W}$ $(k = 1, 2)$ for $\mathcal{W} = (0, 1)$ on $\mathcal{E}$ with $2\mathcal{W} = 0$. So for example $\varphi_{k*}(\mathcal{D}_1) = \tilde\varphi_k(\mathcal{P}) - \tilde\varphi_k(\mathcal{R})$ which on $\mathcal{E}$ is $2\tilde\varphi_k(\mathcal{P})$. Now a relation as in (E2) for $i = 1$ would imply

$$2a\alpha_{12}\tilde\varphi_1(\mathcal{P}) = 2a\alpha_{11}\tilde\varphi_2(\mathcal{P}). \tag{21.10}$$

Here $\tilde\varphi_1(\mathcal{P})$ has the abscissa $(\frac{t+1}{t-1})^2$ and $\tilde\varphi_2(\mathcal{P})$ has abscissa $(\frac{t-1}{t+1})^2$. Also α_{11}, α_{12} are not both zero, else $\varphi_{1*}[\mathcal{D}_1] = \varphi_{2*}[\mathcal{D}_1] = 0$ which would lead to $[\mathcal{D}_1]$ being torsion, which it is not. Thus (21.10) is impossible because exactly one side has a pole at $t = \epsilon$ for $\epsilon = +1$ or $\epsilon = -1$. So again the differential ϖ is not elusive.

For (21.6) we have to work a bit harder. Now we get invariants $1728, 8000$ in (15.2), so one curve has CM by $\mathbf{Z}[i]$ and the other by $\mathbf{Z}[i\sqrt{2}]$. But if the differential is elusive we do not know in advance which is the $\mathcal{E}$ in (E0). At any rate $n = 1$ and again we use $\iota = (\varphi_*, \varphi'_*)$. Fix s with $s^2 = t^6 - 3t^4 + t^2 + 1$. The poles are at $\mathcal{P} = (t, s)$, $\mathcal{Q} = (-t, s)$ together with $\mathcal{R} = (t, -s)$, $\mathcal{S} = (-t, -s)$, so as for (21.4) we get $m = 1$ in (E1), with $\mathcal{D}_1 = \mathcal{P} - \mathcal{Q} - \mathcal{R} + \mathcal{S}$ for $\varrho_1 = 1/(2ts)$.

Trying first $\mathcal{E}$ with $\mathbf{Z}[i]$, we get $\pi_{\mathcal{B}}(\iota[\mathcal{D}_1]) = 4\mathcal{H}$ as in (21.4), clearly not torsion on $\mathcal{B}$. So this $\mathcal{E}$ cannot be the source of elusiveness.

But then trying $\mathcal{E}$ with $\mathbf{Z}[i\sqrt{2}]$, we get

$$\pi_{\mathcal{B}}(\iota[\mathcal{D}_1]) \;=\; \varphi(\mathcal{P}) - \varphi(\mathcal{Q}) - \varphi(\mathcal{R}) + \varphi(\mathcal{S}) \;=\; 0$$

and so (E1) is satisfied.

As for (E2), choose $\jmath(\mathcal{M}) = [\mathcal{M} - \infty^+]$; then $\varphi_1(\mathcal{M}) = \varphi'(\mathcal{M}) - \varphi'(\infty^+)$, and (E2) holds trivially for $a = \alpha_{11} = 1$ and any $\mathcal{D}$ with

$$[\mathcal{D}] \;=\; \varphi_{1*}[\mathcal{D}_1] \;=\; [\varphi'(\mathcal{P}) - \varphi'(\mathcal{Q}) - \varphi'(\mathcal{R}) + \varphi'(\mathcal{S})];$$

for example $\mathcal{D} = 4\mathcal{H} - 4\infty$ with $\mathcal{H}$ as above.

To check (E3) we could calculate $\varpi^\natural$ and look at its zeroes. But by Lemma 16.3 it is clear immediately from (16.17) that (E3) cannot hold. Thus ϖ is not elusive.

For (21.7) we have CM again by $\mathbf{Z}[i]$, so $n = 1$ and ι is naturally the identity. Fix s with $s^2 = t^3 - t$. The poles are at $\mathcal{P} = (t, s)$, $\mathcal{Q} = (-t, is)$ together with $\mathcal{R} = (t, -s)$, $\mathcal{S} = (-t, -is)$. The residues are $1/(2ts), i/(2ts)$ together with $-1/(2ts), -i/(2ts)$ so $m = 2$, and with $\varrho_1 = 1/(2ts), \varrho_2 = i/(2ts)$ we get as usual $\mathcal{D}_1 = \mathcal{P} - \mathcal{R}$, $\mathcal{D}_2 = \mathcal{Q} - \mathcal{S}$.

For (E0) there is no $\mathcal{B}$, and so for (E1) nothing to check. In (E2) we take $\jmath$ as the identity and so φ_1 also. As $\mathcal{D}_2 = i_*\mathcal{D}_1$ for $i(x, y) = (-x, iy)$ we can take $a = 1, \mathcal{D} = \mathcal{D}_1, \alpha_{11} = 1, \alpha_{21} = i$.

To check (E3) we calculate for (16.17)

$$\frac{1}{2ts} + \frac{i}{2ts}\kappa(-i) = \frac{1}{2ts} + \frac{i}{2ts}(-i) = \frac{1}{ts}$$

and so (E3) cannot hold for ϖ, so ϖ is not elusive either.

Even though the general proof strategy in section 20 for (21.7) leads to a torsion point on a curve in an isotrivial additive extension of an isotrivial elliptic curve, which can in principle be treated by [34], it also shows that the verification of non-split is not at all straightforward.

Finally the harmless-looking change from (21.7) to (21.8) gives with now $\varrho_1 = 1/(2s), \varrho_2 = -i/(2s)$ then $\mathcal{D}_1, \mathcal{D}_2$ as before (see (11.3) above), so also ϑ_1, ϑ_2 as before, so (E0),(E1),(E2) hold. But now (16.17) is

$$\frac{1}{2s} - \frac{i}{2s}(-i) = 0$$

and so (E3) also holds. This means that $\mathcal{G}_{\mathcal{Z}}$ is split for every zero $\mathcal{Z}$ of $\varpi^\natural$.

So finally we have to examine (E4) and in particular calculate $\varpi^\natural$. We find $\beta_{11}=1, \beta_{21}=-i$ and hence $\vartheta_1=\varphi_1, \vartheta_2=-i\varphi_1$. So $\vartheta_1^*\vartheta_{1*}, \vartheta_2^*\vartheta_{2*}$ are both the identity and $\varpi^\natural=\varpi$. The zeroes are at ∞ and $O=(0,0)$, both of order $r-1=2$.

Next we need maps $\varsigma_{\mathcal{Z}}$ from $\mathcal{G}_{\mathcal{Z}}$ surjective to $\mathbf{G}_{\mathrm{a}}^r=\mathbf{G}_{\mathrm{a}}^3$. In order to check $\varsigma_{\mathcal{Z}}(\mathcal{T}_{\mathcal{Z}})=0$ it suffices by the Appendix to check the same thing with a splitting map (which we can also denote by $\varsigma_{\mathcal{Z}}$) for $\mathcal{F}_{\mathcal{Z}}$. For this we use Proposition A.8.

For $\mathcal{Z}=\infty$ we can take

$$\varsigma_\infty([\Delta_1]_{3\infty},[\Delta_2]_{3\infty}) \;=\; \left((\Delta_1,x),(\Delta_2,x),\frac{\mathrm{d}f}{f}(\infty)\right)$$

with the pairing (Δ,h) for the function $h=x$, and $(f)=\Delta_1-\Delta_2$. In $\mathcal{T}_\infty$ we find

$$\vartheta_{1*}\mathcal{D}_1=\mathcal{P}-\mathcal{R},\quad \vartheta_{2*}\mathcal{D}_2=(-i)_*(\mathcal{Q}-\mathcal{S})=\mathcal{P}-\mathcal{R}$$

and so

$$\varsigma_\infty(\mathcal{T}_\infty) \;=\; (x(\mathcal{P})-x(\mathcal{R}),x(\mathcal{P})-x(\mathcal{R}),0) \;=\; 0$$

as we wanted.

For $\mathcal{Z}=O$ we can take

$$\varsigma_O([\Delta_1]_{3O},[\Delta_2]_{3O}) \;=\; \left((\Delta_1,x^{-1}),(\Delta_2,x^{-1}),\frac{\mathrm{d}f}{f}(\infty)\right)$$

giving also $\varsigma_O(\mathcal{T}_O)=0$.

Thus indeed ϖ is elusive.

We leave (21.9) for $d=2$ as an exercise.

Also for $d=4$ - note that this is not of the third kind, so we have to find f to kill the repeated poles.

For $d=3$ it is a swindle: we note that the differential has a double pole at ∞ and no other pole. Thus if for some $t=\tau$ it is elementary integrable as in (10.5), the f would have to have a single pole at ∞ and no other pole, which is impossible. In fact the differential is not exact modulo differentials of the third kind (as in the definition of elusive), so this is a simple form of the arguments of section 12.

For $d=5$ the differential ϖ has a pole of order six at ∞ and no other poles. If there is f such that $\varpi-\mathrm{d}f$ is of the third kind, then f must have a pole of order five and no others. Thus we can take $f=ax+by+cx^2+dxy$, and it is clear that for any given value τ of t we can reduce the order of pole of $\varpi-\mathrm{d}f$ to at most two. A simple computation shows that if we can go further to order at most one, then $\tau^2=-3/5$ (here also as in section 12). This gives finiteness; but then the corresponding points (τ,σ) on $y^2=x^3-x$ must be torsion. This is not hard to disprove; for example with $x=(\tau/6)x_1,\ y=(\sigma/24)y_1$ we get $(6,24)$ on $y_1^2=x_1^3+60x_1$ with double $(1/4,-31/8)$ not integral.

21.2. **Final remarks.** Here is a direct proof that the

$$\varpi=\frac{x\mathrm{d}x}{(x^2-t^2)\sqrt{x^3-x}}$$

corresponding to (21.8) is a counterexample. In fact we show that the complex numbers τ such that

$$\varpi(\tau)=\frac{x\mathrm{d}x}{(x^2-\tau^2)\sqrt{x^3-x}}$$

is elementary integrable are precisely those τ for which the point $(\tau,\sqrt{\tau^3-\tau})$ is of finite order at least 3 on the elliptic curve $y^2=x^3-x$.

Fix s with $s^2=t^3-t$. The poles of ϖ are at $\mathcal{P}=(t,s)$ together with $\mathcal{Q}=i\mathcal{P},\mathcal{R}=-\mathcal{P},\mathcal{S}=-i\mathcal{P}$. The residues are $1/(2s)$ together with $-i/(2s),-1/(2s),i/(2s)$ respectively, so $m=2$ in (E2). Taking $\varrho_1=1/(2s),\varrho_2=-i/(2s)$ we find $\mathcal{D}_1=\mathcal{P}-\mathcal{R},\ \mathcal{D}_2=\mathcal{Q}-\mathcal{S}$. As $\mathcal{P}$ is not torsion it follows that ϖ is not elementary integrable.

Next pick $\mathcal{P}_\tau=(\tau,\sigma)$. If $\varpi(\tau)$ is elementary integrable then $\mathcal{P}_\tau$ is torsion. Let $N\geq 2$ be its order.

When $N=2$, we leave it to the reader to check that the corresponding

$$\varpi(0)=\frac{\mathrm{d}x}{x\sqrt{x^3-x}},\quad \varpi(\pm 1)=\frac{x\mathrm{d}x}{(x^2-1)\sqrt{x^3-x}}$$

(which now acquire double poles) are not elementary integrable.

When $N\geq 3$ we now show that $\varpi(\tau)$ is elementary integrable.

For the points

$$\mathcal{Q}_\tau=i\mathcal{P}_\tau=(-\tau,i\sigma),\quad \mathcal{R}_\tau=-\mathcal{P}_\tau=(\tau,-\sigma),\quad \mathcal{S}_\tau=-i\mathcal{P}_\tau=(-\tau,-i\sigma)$$

there are functions g_1,g_2 with divisors $N\mathcal{P}_\tau-N\mathcal{R}_\tau, N\mathcal{Q}_\tau-N\mathcal{S}_\tau$. We can normalize them to be 1 at infinity.

Consider

$$\chi \;=\; \varpi(\tau)-\frac{1}{2N\sigma}\left(\frac{\mathrm{d}g_1}{g_1}-i\frac{\mathrm{d}g_2}{g_2}\right).$$

We check easily that the residues at $\mathcal{P}_\tau,\mathcal{Q}_\tau,\mathcal{R}_\tau,\mathcal{S}_\tau$ are zero. Since all the poles are at worst simple, this means that $\chi=c\mathrm{d}x/y$ for some c.

Also we check again easily that $g_2=i_*g_1$.

Now let $g_1=1+a\pi+\cdots$ be the expansion at infinity, with say $\pi=x/y$. As $i_*\pi=-i\pi$ we deduce $g_2=1-ia\pi+\cdots$. It follows yet again easily that $\mathrm{d}g_1/g_1-i\mathrm{d}g_2/g_2$ vanishes at infinity.

But so does $\varpi(\tau)$! Therefore so does χ; and this implies $c=0$. Therefore

$$\varpi(\tau)=\frac{1}{2N\sigma}\left(\frac{\mathrm{d}g_1}{g_1}-i\frac{\mathrm{d}g_2}{g_2}\right)$$

is indeed elementary integrable.

An example with $N=4$ and $\mathcal{P}_i=(i,1-i)$ leads to

$$\int\frac{x\mathrm{d}x}{(x^2+1)\sqrt{x^3-x}},\tag{21.11}$$

which is

$$\frac{1+i}{16}\log\left(\frac{x^2+(2+2i)\sqrt{x^3-x}+2ix-1}{x^2-(2+2i)\sqrt{x^3-x}+2ix-1}\right)+\frac{1-i}{16}\log\left(\frac{x^2+(2-2i)\sqrt{x^3-x}-2ix-1}{x^2-(2-2i)\sqrt{x^3-x}-2ix-1}\right).$$

This was our first intimation of a counterexample to Davenport's Assertion. It can actually be deduced directly from (14.4). It (and (14.4) too) can be slightly simplified by using divisors $2\mathcal{P}_\tau-2\mathcal{R}_\tau, 2\mathcal{Q}_\tau-2\mathcal{S}_\tau$. Welz has pointed out that this too is a special case of Goursat's results in [29]. And we note Euler [26] (E539, E668) had already given something equivalent to

$$\int\frac{\sqrt{x^4+1}\;\mathrm{d}x}{x^4-1} \;=\; \frac{1}{4}\sqrt{2}\log\left(\frac{\sqrt{2}x-\sqrt{x^4+1}}{x^2-1}\right)+\frac{i}{4}\sqrt{2}\log\left(\frac{i\sqrt{2}x+\sqrt{x^4+1}}{x^2+1}\right)$$

also in which the two logarithms cannot be combined into a single one; his own solution

$$-\frac{1}{4}\sqrt{2}\log\left(\frac{\sqrt{2}x+\sqrt{x^4+1}}{x^2-1}\right)-\frac{1}{4}\sqrt{2}\,\arcsin\left(\frac{\sqrt{2}x}{x^2+1}\right)$$

does not literally involve complex logarithms and stays inside the real field (note however the intrusive $\sqrt{2}$).

We then tried other points with $N=4$ and then with $N=3$, but the clincher was with $N=5$, when

$$\int\frac{x\mathrm{d}x}{(x^2-\frac{1}{5}-\frac{2i}{5})\sqrt{x^3-x}} \;=\; c_1\log g_1+c_2\log g_2$$

with

$$c_1=\frac{1}{2b},\quad c_2=-\frac{i}{2b}$$

for

$$b \;=\; \sqrt[4]{220+40i} \;=\; (.1738\ldots)-(3.8630\ldots)i,\quad a=-\frac{2+i}{10}b^2$$

and

$$g_1=-\frac{10ax\sqrt{x^3-x}-(15-5i)bx^2-50\sqrt{x^3-x}+(2-4i)abx+(3+i)b}{10ax\sqrt{x^3-x}+(15-5i)bx^2-50\sqrt{x^3-x}-(2-4i)abx-(3+i)b},$$

$$g_2 = -\frac{10aix\sqrt{x^3-x} - (15-5i)bx^2 + 50i\sqrt{x^3-x} - (2-4i)abx + (3+i)b}{10aix\sqrt{x^3-x} + (15-5i)bx^2 + 50i\sqrt{x^3-x} + (2-4i)abx - (3+i)b}$$

which Maple 18 cannot check even by differentiation (however it can check equality up to say 1000 decimal places when we integrate between say $x = 2$ and $x = 2.1$). This probably cannot be simplified.

In this way one can construct functions "of bounded complexity" which are elementary integrable but whose integrals involve "unbounded complexity". Actually this was also possible classically using (1.3); but there the resulting (τ, υ) do not lie on a fixed parameter curve C (in fact by Theorem 1.3(a), because $y^2 = x^4+x+t$ has no CM as required for (E0) in the definition of elusive). Maybe this is related to Hrushovski's "uniform definability" in [35] (p.101).

There are also counterexamples with CM by $\mathbf{Q}(i\sqrt{3})$ instead of $\mathbf{Q}(i)$. We found

$$\frac{x\mathrm{d}x}{(x^2+tx+t^2)\sqrt{x^3-1}}$$

and Welz pointed out that it amounts to the more attractive

$$\frac{x\mathrm{d}x}{(x^3-t^3)\sqrt{x^3-1}}$$

actually integrated by Euler for $t = -2$ (according to [32] p.643 - see also [26], E695 in disguise). We originally thought we had a proof that any $\mathbf{Q}(i\sqrt{d})$ turns up, and this seemed to lead to a counterexample

$$\frac{((5t^2+40t+62)x + t^3 + 8t^2 + 70t + 144)\mathrm{d}x}{(x-t)((2t+8)x + t^2 + 4t + 18)\sqrt{x^3-30x-56}} \tag{21.12}$$

for $\mathbf{Q}(i\sqrt{2})$; but Welz was very sceptical after testing it on the computer algebra system FriCAS (see http://fricas.sf.net), and then we found a mistake in our proof. In fact we were able to show, partly computationally, that $\mathbf{Q}(i\sqrt{2})$ does not turn up, and we strongly suspect that $\mathbf{Q}(i)$ and $\mathbf{Q}(i\sqrt{3})$ are the only fields. This would make it unlikely that there are any connexions with Bertrand's counterexamples in [8], because those do exist for every $\mathbf{Q}(i\sqrt{d})$. Also they involve multiplicative extensions rather than additive extensions.

Or in higher genus one can use pull-backs φ^* to find for example

$$\frac{(3x^5 - x^4 - 2x^3 - 2x^2 - x + 3)\mathrm{d}x}{((9t-9)x^4 - (36t+12)x^3 + (54t-22)x^2 - (36t+12)x + 9t - 9)\sqrt{x^5 + \frac{14}{9}x^3 + x}},$$

which can easily shown to be not elementary integrable by using φ_* on the corresponding divisors. It would be interesting to know if all elusive differentials in higher genus come from pull-backs on elliptic curves with complex multiplication.

Probably related to this is the question of whether there are examples with "genuinely" three logarithms; that is, with $m = 3$ and $[\mathcal{D}_1], [\mathcal{D}_2], [\mathcal{D}_3]$ linearly independent.

Appendix.

We start by remarking that a referee, after seeing our presentation below, pointed out that many of the assertions are consequences of the theory of universal vectorial extensions, as for example as in Brion's Proposition 2.3 [12] (p.940). Thus given an elliptic curve E, there is an extension Γ_{univ} of E by $\mathbf{G}_{\mathrm{a}}$ such that any extension as in (A.1) below arises from a pushout from Γ_{univ} by a linear homomorphism ϕ from $\mathbf{G}_{\mathrm{a}}$ to $\mathbf{G}_{\mathrm{a}}^n$. The extension is non-trivial if and only if $\phi \neq 0$, and in that case one may define the splitting line below simply as $\phi(\mathbf{G}_{\mathrm{a}})$. Its property in Proposition A.3 below is just a consequence of composing with a second pushout. The same referee made more comments about Proposition A.2 and Theorem A.4, which we insert below at the appropriate place. But for ease of reading we have kept our original more self-contained presentation, especially as the whole paper is aimed principally at number theorists.

It will suffice here by the Lefschetz Principle to treat elliptic curves over $\mathbb{K} = \mathbf{C}$; thus we drop the calligraphy from now on. We shall consider extensions of a complex elliptic curve

E by a power of $\mathbf{G}_\mathrm{a}$, by which we mean algebraic groups Γ for which there exists an exact sequence of algebraic groups

$$0 \longrightarrow \mathbf{G}_\mathrm{a}^n \longrightarrow \Gamma \longrightarrow E \longrightarrow 0 \tag{A.1}$$

with π the projection from Γ to E.

The general theory of extensions is studied in particular in [70] and in part expanded in [19] for the present case of $\mathbf{G}_\mathrm{a}$. We shall now recall some facts, and also give short proofs of other results, apparently not easy to locate in the literature. After this, we shall prove a result, apparently new, which is important for main text.

We shall say that a (homo)morphism of such extensions ϕ from Γ to Γ' is *over* E if it commutes with the projections π, π' to E; that is, if $\pi' \circ \phi = \pi$.

We shall say that such an algebraic group is (totally) split if it is isomorphic to $E \times \mathbf{G}_\mathrm{a}^n$ over E.

Note that we intend all such isomorphisms in the sense of algebraic groups, and we do not insist that the isomorphism are in the strongest sense of extensions (as in [70] VII).

An important class of extensions is associated to the modulus rW for a positive integer r. Namely, let W be a given point in E. Following [70], we denote by G_r (or G_{rW}) the extension of E by $\mathbf{G}_\mathrm{a}^{r-1}$ obtained by the modulus rW.

We recall that, as a group, this is the factor group of divisors of degree 0 and prime to W, by the subgroup of principal divisors (f) where f is a rational function on E, regular and nonzero at W, and such that $\mathrm{d}f$ vanishes at W to order at least $r-1$.

We shall denote by $[D]_r$ (or $[D]_{rW}$) this (narrow) class of a divisor D (prime to W and of degree 0).

Let t be a local parameter at W. Then we have a map which to a principal divisor $D = (f)$ (with D prime to W, that is, f regular and nonzero at W) associates $\mathrm{d}f/f$ modulo t^{r-1}.

This target space is a vector space (over $\mathbf{C}$) of dimension $r-1$, where we can take as coordinates the first $r-1$ coefficients of $\mathrm{d}f/f$ in the t-expansion. Also, the map induces a homomorphism from the group of narrow principal divisor classes defined above, to the additive group $\mathbf{G}_\mathrm{a}^{r-1}$, injective by definition. The map is also surjective, as we may prescribe arbitrarily the first r coefficients of the expansion of f at W in terms of t, and with say $f(W) = 1$.

These definitions yield $G_1 = E$ (for example by some "approximation" result, or we may simply note that the broad classes $[D] = [\tau_* D]$ for any translation τ on E), and we have $\dim G_r = r$.

For $r \geq s$ there is a natural map π_{rs} from G_r to G_s, obtained by weakening equivalence.

The extension G_2 is especially relevant. We recall from [19] or [70] that G_2 is a non-split extension of E by $\mathbf{G}_\mathrm{a}$. Also, it is proved in [19] that G_2 does not contain properly any connected algebraic subgroups other than the identity and $\mathbf{G}_\mathrm{a}$. In particular, this itself implies that G_2 is not split (otherwise it would contain a copy of E) and that it admits no non-constant homomorphisms to $\mathbf{G}_\mathrm{a}$. (Actually, it admits no non-constant morphisms to $\mathbf{G}_\mathrm{a}$, as is proved in Remark 3.7 of [19] for example.)

We shall soon recall how G_2 in fact suffices to classify all extensions in question.

An issue is what happens if we start with another point W' in place of W and consider the extension G'_r defined by the modulus rW'. Let as above $[.]_r, [.]'_r$ denote classes with respect to W, W'. We shall prove the following

Proposition A.1 *The extensions G_r, G'_r are isomorphic over E, with an explicit isomorphism induced by translation on classes of points; and in particular $[(f)]_r$ goes to $[(\tau^* f)]'_r$ where τ is translation by $W - W'$.*

Proof. Translation by $W' - W$ induces an isomorphism of pointed curves from (E, W) to (E, W') inducing the identity on $\mathrm{Pic}^0(E)$, so it induces an isomorphism from G_r to G'_r over E. Note that translations on E induce the identity on $\mathrm{Pic}^0(E)$ because they preserve the value of the σ of Proposition III.3.4 of [73] (p.66).

□

We now denote by t a local parameter at a point W in E.

Let us consider again the extension G_r, defined above, where $r \geq 2$ and W in E is a given point. We have mentioned the map π_{r2} from G_r to G_2 obtained by weakening equivalence; it

is a homomorphism over E. Since G_2 is not split, G_r cannot be split as well (for otherwise we would have a non constant map E to G_2, contrary to the fact that G_2 does not contain other 1-dimensional subgroups other than $\mathbf{G}_\mathrm{a}$, as shown in [19] for example).

Recall that we may map the group of narrow divisor classes prime to W and principal, to G_r by associating a narrow class $[(f)]_r$ to $\mathrm{d}f/f \pmod{t^{r-1}}$. This is a group homomorphism, sending the narrow divisor classes of functions onto $\mathbf{G}_\mathrm{a}^{r-1}$.

Definition. We define $V = V_r \subset G_r$ as the vector subspace of G_r consisting of divisor classes $[(f)]_r$, where $f-1$ vanishes to order at least 2 at W.

Note that this is indeed a vector subspace, because these functions form a multiplicative group, and we may prescribe the truncated expansion in t of f modulo t^r arbitrarily.

From the above definitions, it also immediately follows that V is precisely the kernel of π_{r2}.

Note that, for an integer $m \geq 1$, the space $\mathfrak{L}_m = \mathfrak{L}(-mW)$ of functions in $\mathbf{C}(E)$ with at most a pole of order m at W has dimension m (for $m = 1$ it is just $\mathbf{C}$ of course).

For $r \geq 3$, we now construct a pairing from $G_r \times \mathfrak{L}_{r-1}$ to $\mathbf{G}_\mathrm{a}$ as follows.

For a divisor $D = \sum_P m_P P$ of degree 0, prime to W (so that $m_W = 0$), and for a function h in $\mathfrak{L}_{r-1}$, we define

$$(D, h) = \sum_P m_P h(P). \tag{A.2}$$

Note this is well-defined, and a pairing to $\mathbf{G}_\mathrm{a}$ from the product of the group of divisors of degree 0 prime to W with $\mathfrak{L}_{r-1}/\mathfrak{L}_1$. (It is naturally suggested for example by Theorem 1 (p.1) in [70]; see also p.33 therein.)

We prove

Proposition A.2 *The above pairing induces a pairing from $G_r \times (\mathfrak{L}_{r-1}/\mathfrak{L}_1)$ to $\mathbf{G}_\mathrm{a}$ of algebraic groups, which is perfect when restricted to V on the left. This also induces an isomorphism of algebraic groups $G_r \cong_E G_2 \times \mathbf{G}_\mathrm{a}^{r-2}$ (over E).*

Proof. We start by observing that the pairing (A.2), with divisors on the left, induces indeed a pairing of additive groups on $G_r \times (\mathfrak{L}_{r-1}/\mathfrak{L}_1)$, which is $\mathbf{C}$-linear on the right. For this it suffices to check that a divisor D of degree 0, coprime to W and equivalent to 0 in the narrow sense associated to G_r, lies inside the kernel on the left.

Indeed, if such a D is equivalent to 0 in the narrow sense, there exists a function f in $\mathbf{C}(E)$ with divisor D and such that $\mathrm{d}f$ vanishes at W of order at least $r-1$. Consider now the differential $h\mathrm{d}f/f$ on E; it has no residue at W (since it has no pole there), and hence the sum of its residues is just (D, h). But the sum of the residues of a differential is zero ([70], II, Proposition 6), whence the assertion.

Now, from the construction of generalised Jacobians given in [70], we see that the induced pairing is algebraic also on the left, and it follows that it is $\mathbf{C}$-linear when restricted to $\mathbf{G}_\mathrm{a}^{r-1} \subset G_r$ on the left. (Or one may also argue by continuity here.)

Let us now consider such induced pairing, and let K be its kernel on the left.

To restrict it on the left to $\mathbf{G}_\mathrm{a}^{r-1} \subset G_r$ is just like restricting to narrow divisor classes $[(f)]_r$ for functions f in $\mathbf{C}(E)$, regular and nonzero at W. By the same argument as above we see that $-([(f)]_r, h)$ equals the residue at W of $h\mathrm{d}f/f$.

Let now f be a non-constant function with $f \equiv 1 \pmod{t}$, and such that $[(f)]_r$ is in $V \cap K$.

Then, by the definition of V, for some $m \geq 2$, we can write expansions at W as

$$f = 1 + c_m t^m + \cdots, \quad \frac{\mathrm{d}f}{f} = (m c_m t^{m-1} + \cdots)\mathrm{d}t,$$

where $c_m \neq 0$. If $[(f)]_r \neq 0$, we have $m \leq r-1$. Also, let h_m in $\mathfrak{L}_m$ be a function with a pole of exact order m at W (which exists since $m \geq 2$). Then the residue at W of $h_m \mathrm{d}f/f$ is nonzero, whence the above remark entails $([(f)]_r, h_m) \neq 0$, against the assumption.

Hence $V \cap K = \{0\}$, so the pairing yields an isomorphism between V and the dual of $\mathfrak{L}_{r-1}/\mathfrak{L}_1$, which is isomorphic to $\mathbf{G}_\mathrm{a}^{r-2}$.

Take now g in G_r; then the map taking x to (g, x) is a linear map from $\mathfrak{L}_{r-1}$ to $\mathbf{G}_\mathrm{a}$ vanishing on $\mathfrak{L}_1$, whence there is v in V with $(g, x) = (v, x)$ for all x. Then $g - v$ is in K, hence $G_r \cong_E K \times V$.

As noted above, the natural map from G_r to G_2 has kernel V and is surjective, so $K \cong_E G_2$. This completes the proof. □

Remark. It also follows that $G_r \cong_E G_2 \times \mathbf{G}_{\mathrm{a}}^{r-2}$, where the first projection is π_{r2}, and we have a section λ_{2r} from G_2 to G_r, which is unique (e.g. because any homomorphism from G_2 to $\mathbf{G}_{\mathrm{a}}$ must be zero). And $K = \lambda_{2r}(G_2)$.

We now come to the main objects of our study.

Definition. For the extension G_r as above, we define the *splitting line* in G_r as $L = K \cap \mathbf{G}_{\mathrm{a}}^{r-1}$, where K is the kernel on the left of the pairing of Proposition A.2.

Note that, by the isomorphism $G_r \cong_E G_2 \times \mathbf{G}_{\mathrm{a}}^{r-2}$, this line is the image of the unique $\mathbf{G}_{\mathrm{a}}$ inside G_2, through the natural section from G_2 to G_r.

Proposition A.3 *The splitting line is the unique line Λ in $\mathbf{G}_{\mathrm{a}}^{r-1} \subset G_r$ with the property that, for a vector subspace U of $\mathbf{G}_{\mathrm{a}}^{r-1} \subset G_r$, the extension G_r/U of E is split if and only if $\Lambda \subset U$.*

Proof. Clearly, in view of Proposition A.2, the splitting line has the stated property. In particular, G_r/L is split. Conversely, let Λ have this property. By the previous remark, Λ contains L, proving what is stated. □

We now come to the main result of this appendix, which characterizes the splitting line in G_r in terms of classes of principal divisors.

Theorem A.4 *The splitting line in G_r consists of divisor classes $[(f)]_r$ of functions f regular and nonzero at W and such that $\mathrm{d}f/f$ coincides with some nonzero invariant differential $\chi = \chi_f$ up to order $r-1$, that is, such that*

$$\frac{\mathrm{d}f}{f} - \chi$$

has a zero of order at least $r-1$ at W.

Proof. We start by observing that, since χ has no zeros, these divisor classes form indeed a line in $\mathbf{G}_{\mathrm{a}}^{r-1} \subset G_r$.

Then, it suffices to show that this line is inside K. For this, let f in $\mathbf{C}(E)$ have the property stated in the theorem. Then, for any h in $\mathfrak{L}_{r-1}$, we have (as in Proposition A.2)

$$([(f)]_r, h) \;=\; -\mathrm{res}_W\left(h\frac{\mathrm{d}f}{f}\right) \;=\; \mathrm{res}_W(h\chi) - \mathrm{res}_W\left(h\left(\frac{\mathrm{d}f}{f} - \chi\right)\right).$$

The term on the right is zero, because the differential $h(\mathrm{d}f/f - \chi)$ has no pole at W (since h is in $\mathfrak{L}_{r-1}$). The same holds for the first term, since the differential $h\chi$ has a pole only at W, and therefore, since the sum of all of its residues vanishes, its only residue at W must also vanish. This completes the proof. □

As remarked above, a referee outlined another proof of Theorem A.4. One restricts the pairing of Proposition A.2 to the kernel V' rather of π_{r1} and notes that as above V' is isomorphic to the space Ω_{r-1} of differentials regular at W modulo those vanishing to order at least $r-1$. The resulting pairing from $\Omega_{r-1} \times (\mathfrak{L}_{r-1}/\mathfrak{L}_1)$ to $\mathbf{G}_{\mathrm{a}}$ has left kernal which is the image of the one-dimensional space H^0 of invariant differential forms on E, and trivial right kernel - this follows for example from Theorem VIII.1.3 of Mumford and Oda [55]. Finally if L is the image of H^0 in Ω_{r-1} in G_r via V', we get an isomorphism between G_r/L and $\mathbf{G}_{\mathrm{a}}^{r-2}$; thus L is the splitting line.

We next consider the splitting line in a fibre product $\Gamma = \Gamma_1 \times_E \cdots \times_E \Gamma_s$ (over E), where the Γ_j are non-split extensions of E by powers of $\mathbf{G}_{\mathrm{a}}$, with injections λ_j from G_2 into Γ_j over E (namely, these maps commute with the projections to E).

Proposition A.5 *We have $\Gamma \cong_E G_2 \oplus \mathbf{G}_{\mathrm{a}}^{s-1}$, again over E, where the embedding of G_2 into Γ sends z to $(\lambda_1(z), \ldots, \lambda_s(z))$.*

Proof. Indeed, let $x = (x_1, \dots, x_s)$ be in Γ. We have $x = (\lambda_1(y_1), \dots, \lambda_s(y_s))$, where y_j is in G_2 and $\pi_2(y_j) = u$ in E is independent of j. Then $y_j = y_1 + a_j$ for suitable $a_1 = 0, a_2, \dots, a_s$ in $\mathbf{G}_\mathrm{a}$, hence $x = (\lambda_1, \dots, \lambda_s)(y_1) + v$ where v is in $\mathbf{G}_\mathrm{a}^{s-1}$; this shows what we want, identifying G_2 with its image in Γ through the map $(\lambda_1, \dots, \lambda_s)$. □

Similarly, a fibre product $\Gamma \times_E (E \times \mathbf{G}_\mathrm{a})^r_E \cong_E \Gamma \times_E (E \times \mathbf{G}_\mathrm{a}^r)$, where Γ is as above, and $s \geq 1$, is isomorphic to $G_2 \oplus \mathbf{G}_\mathrm{a}^{r+s-1}$, as is immediately checked on using the previous result.

Finally, suppose that ι from Γ to Γ' is an isomorphism over E between extensions of E by $\mathbf{G}_\mathrm{a}^r$. Then $\Gamma \times_E \Gamma' \cong_E \Gamma \times \mathbf{G}_\mathrm{a}^r$, where the last isomorphism sends (x, x') to $(x, x' - \iota(x))$. (Observe that indeed, since $\pi(x) = \pi'(x')$ and $\pi = \pi' \circ \iota$, we have that $\pi'(x' - \iota(x)) = 0$, that is, $x' - \iota(x)$ is in $\ker \pi' = \mathbf{G}_\mathrm{a}^r$.)

A similar fact holds of course for products of several isomorphic extensions, generalising the previous situations.

The previous results allow us to describe the splitting line in a fibre product.

Corollary A.6 *Let $\Gamma_1, \dots, \Gamma_s$ be non-split extensions of E by $\mathbf{G}_\mathrm{a}^{r_1}, \dots, \mathbf{G}_\mathrm{a}^{r_s}$ respectively, with injections λ_j from G_2 into Γ_j over E. Also, let $\Gamma = \Gamma_1 \times_E \cdots \times_E \Gamma_s$. Then the splitting line in Γ is the set of $(\lambda_1(x), \dots, \lambda_s(x))$ for x in L, where L is the splitting line in G_2.*

Proof. Immediate from Proposition A.5 above. □

Corollary A.7 *For $r \geq 2$ the splitting line in $E_{rW_1} \times_E \cdots \times_E E_{rW_m}$ consists of elements*

$$([(\tau_1^* f)]_{rW_1}, \dots, [(\tau_m^* f)]_{rW_m})$$

with functions f regular and nonzero at W and such that $\mathrm{d}f/f$ coincides with some nonzero invariant differential $\chi = \chi_f$ up to order $r-1$, where τ_i is translation by $W - W_i$ $(i = 1, \dots, m)$.

Proof. We apply Corollary A.6 with $\Gamma_i = E_{rW_i}$ $(i = 1, \dots, m)$. By Proposition A.1 there are isomorphisms T_i from E_{rW} to E_{rW_i} taking $[(f)]_{rW}$ to $[(\tau_i^* f)]_{rW_i}$ $(i = 1, \dots, m)$. With λ from G_2 into E_{rW} the standard section, we obtain sections $\lambda_i = T_i \circ \lambda$ from G_2 into E_{rW_i} $(i = 1, \dots, m)$. So the splitting line consists of all $(\lambda_1(x), \dots, \lambda_m(x))$ as x runs over the splitting line in G_2. As already noted, the $\lambda(x)$ describe the splitting line in E_{rW}, which consists of all $[(f)]_{rW}$ as in Theorem A.4, and what we want follows at once. □

We shall need also the following

Definition. Suppose Γ in (A.1) is non-split with splitting line L. Then Γ/L is split, and we shall say that any surjective σ to $\mathbf{G}_\mathrm{a}^{n-1}$ is a *splitting map* for Γ.

Note that σ is unique up to automorphisms of $\mathbf{G}_\mathrm{a}^{n-1}$ (because there are no non-zero maps from G_2 to $\mathbf{G}_\mathrm{a}$).

A similar argument shows that for any linear subspace U of Γ, say of dimension p, containing L there is an essentially unique surjective map from Γ/U to $\mathbf{G}_\mathrm{a}^{n-p}$, obtained by identifying $\mathbf{G}_\mathrm{a}^{n-1}/\sigma(U)$ with $\mathbf{G}_\mathrm{a}^{n-p}$.

If $r = 2$ then $\sigma_2 = 0$ is trivially a splitting map for G_r. If $r \geq 3$ we can easily obtain a splitting map for G_r from the pairing. Pick a basis $(h_0, h_1, \dots, h_{r-2})$ of $\mathfrak{L}_{r-1}$ with $h_0 = 1$. Thanks to Proposition A.2 we can define σ_r from G_r to $\mathbf{G}_\mathrm{a}^{r-2}$ by

$$\sigma_r([D]_r) = ((D, h_1), \dots, (D, h_{r-2})).$$

As $(D, h_0) = 0$ the kernel is K, of dimension 2 containing L; thus σ_r induces a map on G_r/L with kernel of dimension 1, and so we get surjectivity.

Here is a generalization to fibre products.

Proposition A.8 *For $r \geq 3, m \geq 2$ and $\Gamma_i = G_r$ $(i = 1, \dots, m)$, a splitting map on $\Gamma = \Gamma_1 \times_E \cdots \times_E \Gamma_m$ is induced by the map from Γ to $\mathbf{G}_\mathrm{a}^{m(r-1)-1}$ sending $([D_1]_r, \dots, [D_m]_r)$ to*

$$\left(\sigma_r(D_1), \dots, \sigma_r(D_m), \frac{\mathrm{d}f_1}{f_1}(W), \dots, \frac{\mathrm{d}f_{m-1}}{f_{m-1}}(W)\right)$$

for any functions $f_1, \dots, f_{m-1}$ on E with $(f_i) = D_i - D_m$ $(i = 1, \dots, m-1)$.

Proof. Again we look at the kernel. First we see that $[D_1]_r, \dots, [D_m]_r$ lie in $K = \lambda(G_2)$ with λ the standard section. So $[D_i]_r = \lambda(x_i)$ for x_i in G_2 $(i = 1, \dots, m)$. Second the vanishing of the $(\mathrm{d}f_i/f_i)(W)$ means that the $[D_i]_2$ $(i = 1, \dots, m)$ are all equal. These are just the $\pi([D_i]_r)$ for $\pi = \pi_{r2}$, and so the $x_i = \pi(\lambda(x_i))$ $(i = 1, \dots, m)$ are all equal in G_2. Thus the kernel has dimension at most 2. As Γ has dimension $m(r-1)+1$ this implies surjectivity. □

References

1. N.H. Abel, *Über die Integration der Differential-Formel $\rho dx/\sqrt{R}$, wenn R und ρ ganze Funktionen sind*, J. für Math. (Crelle) **1** (1826), 185-221 – see also Oeuvres Complètes, Cambridge 2012 (pp.104–144).
2. N.H. Abel, *Précis d'une théorie des fonctions elliptiques*, J. für Math. (Crelle) **4** (1829), 236–277 and 309–348 – see also Oeuvres Complètes, Cambridge 2012 (pp.508–617).
3. Y. André, *Mumford-Tate groups of mixed Hodge structures and the theorem of the fixed part*, Compositio Math. **82** (1992), 1-24.
4. Y. André, *Sur la conjecture des p-courbures de Grothendieck-Katz et un problème de Dwork*, in Geometric Aspects of Dwork Theory (eds. A. Adolphson, F. Baldassarri, P. Berthelot, N. Katz, F. Loeser), de Gruyter 2004 (pp.55-112).
5. F. Barroero, L. Capuano, *Linear relations in families of powers of elliptic curves*, Algebra and Number Theory **10** (2016), 195-214.
6. F. Barroero, L. Capuano, *Unlikely intersections in families of abelian varieties and the polynomial Pell equation*, arXiv:1801.02885v1 (January 2018, 27 pages).
7. D. Bertrand, *Théories de Galois différentielles et transcendance*, Ann. Inst. Fourier **59** (2009), 2773-2803.
8. D. Bertrand, *Special points and Poincaré bi-extensions; with an Appendix by Bas Edixhoven*, arXiv: 1104.5178v1 (April 2011, 11 pages).
9. D. Bertrand, *Generalized jacobians and Pellian polynomials*, J. Théorie des Nombres de Bordeaux **27** (2015), 439-461.
10. D. Bertrand, D. Masser, A. Pillay, U. Zannier, *Relative Manin-Mumford for semi-abelian surfaces*, J. Edinburgh Math. Soc. **59** (2016), 837-875.
11. G. Binyamini, *Density of algebraic points on Noetherian varieties*, arXiv: 1704.00442v1 (April 2017, 40 pages).
12. M. Brion, *Anti-affine algebraic groups*, J. Algebra **321** (2009), 934–952.
13. J.W.S. Cassels, *The arithmetic of certain quartic curves*, Proc. Royal Soc. Edinburgh **100A** (1985), 201-218.
14. J.W.S. Cassels, E.V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, London Math. Soc. Lecture Notes **230**, Cambridge 1996.
15. P.J. Cassidy, M.F. Singer, *Galois theory of parameterized differential equations and linear differential algebraic groups*, in Differential Equations and Quantum Groups, IRMA Lectures in Mathematics and Theoretical Physics **9** (eds. D. Bertrand, B. Enriquez, C. Mitschi, C. Sabbah, R. Schaefke), EMS Publishing house 2006 (pp.113-157).
16. B.F. Caviness, B.D. Saunders, M.F. Singer, *An extension of Liouville's Theorem on integration in finite terms*, SIAM Journal of Computing **14** (1985), 966-990.
17. P. Chebychev, *Sur l'intégration des différentielles qui contiennent une racine carée d'un polynome du troisième ou du quatrième degré*, J. Math. Pures Appl. **2** (1857), 168-192.
18. P. Chebychev, *Sur l'intégration de la différentielle* $\frac{x+A}{\sqrt{x^4+\alpha x^3+\beta x^2+\gamma x+\delta}}$, J. Math. Pures Appl. **9** (1864), 225-246.
19. P. Corvaja, D. Masser, U. Zannier, *Sharpening 'Manin-Mumford' for certain algebraic groups of dimension* 2, L'Enseignement Math. **59** (2013), 225-269.
20. P. Corvaja, D. Masser, U. Zannier, *Torsion curves on abelian schemes and Betti coordinates*, Math. Annalen **371** (2018), 1013–1045.
21. J.H. Davenport, *On the integration of algebraic functions*, Lecture Notes in Computer Science **102**, Springer 1981.
22. J.H. Davenport and M.F. Singer, *Elementary and Liouvillian solutions of linear differential equations*, J. Symbolic Comp. **2** (1986), 237-260.
23. S. David, *Fonctions thêta et points de torsion des variétés abéliennes*, Compositio Math. **78** (1991), 121-160.
24. T. Ekedahl and J-P. Serre, *Exemples de courbes algébriques à jacobienne complètement décomposable*, C. R. Acad. Sci. Paris, Ser. I **317** (1993), 509-513.
25. A. Enneper, *Elliptische Functionen*, Nebert, Halle 1890.
26. L. Euler, papers E539 (p.25), E668 (p.39) and E695 (p.22) in The Euler Archive (eulerarchive.maa.org).

27. G. Frey, *On elliptic curves with isomorphic torsion structures and corresponding curves of genus 2*, in Elliptic curves, modular forms, and Fermat's Last Theorem (eds. J. Coates, S.T. Yau), International Press 1995 (pp. 79-98).
28. G. Frey, E Kani, *Curves of genus 2 covering elliptic curves and an arithmetical application*, in Arithmetic Algebraic Geometry (eds. G. van der Geer, F. Oort, J. Steenbrink), Progress in Math. **89**, Birkhäuser 1991 (pp. 153-176).
29. E. Goursat, *Note sur quelques intégrales pseudo-elliptiques*, Bull. Soc. Math. France **15** (1887), 106–120.
30. E. Goursat, *Sur les intégrales abéliennes qui s'expriment par des logarithmes*, C. R. Acad. Sci. Paris, Ser. I **118** (1894), 515-517.
31. A.G. Greenhill, *The applications of elliptic functions*, London 1892.
32. G.-H. Halphen, *Fonctions elliptiques II*, Gauthier-Villars, Paris 1888.
33. G.H. Hardy, *The integration of functions of a single variable*, Tracts in Mathematics and Mathematical Physics **2**, Cambridge 1928.
34. M. Hindry, *Autour d'une conjecture de Serge Lang*, Inventiones Math. **94** (1988), 575-603.
35. E. Hrushovski, *Computing the Galois group of a linear differential equation*, Banach Center Publ. **58**, Polish Acad. Sci., Warszawa 2002 (pp. 97-138).
36. I. Kaplansky, *An introduction to differential algebra* (2nd edition), Hermann, Paris 1957.
37. N.M. Katz, *Algebraic solutions of differential equations (p-curvature and the Hodge filtration)*, Inventiones Math. **18** (1972), 1-118.
38. F. Klein, *Lectures on the icosahedron and the solution of equations of the fifth degree*, Dover 1956.
39. L. Königsberger, *Ueber die Reduction hyperelliptischer Integrale auf elliptische*, J. reine angew. Math. **85** (1878), 273-294.
40. A. Krazer, *Lehrbuch der Thetafunktionen*, Teubner, Leipzig 1903.
41. R.M. Kuhn, *Curves of genus 2 with split Jacobian*, Trans. Amer. Math. Soc. **307** (1988), 41-49.
42. S. Lang, *Complex analysis*, Addison-Wesley 1977.
43. J. Lützen, *Joseph Liouville 1809-1882: master of pure and applied mathematics I*, Studies in the History of Mathematics and Physical Sciences **15**, Springer 1990.
44. D. Masser, G. Wüstholz, *Periods and minimal abelian subvarieties*, Ann. of Math. **137** (1993), 407-458.
45. D. Masser, G. Wüstholz, *Factorization estimates for abelian varieties*, Publ. Math. IHES **81** (1995), 5-24.
46. D. Masser, *Linear relations on algebraic groups*, in New Advances in Transcendence Theory (ed. A. Baker), Cambridge University Press 1988 (pp. 248-262).
47. D. Masser, *Small values of heights on families of abelian varieties*, in: Diophantine approximation and transcendence theory (ed. G. Wüstholz), Lecture Notes in Math. **1290**, Springer 1988 (pp.109-148).
48. D. Masser, *Specializations of some hyperelliptic Jacobians*, in: Number Theory in Progress (eds. K. Győry, H. Iwaniec, J. Urbanowicz), Walter de Gruyter, Berlin New York 1999 (pp.293-307).
49. D. Masser. U. Zannier, *Torsion anomalous points and families of elliptic curves*, C. R. Acad. Sci. Paris, Ser. I **346** (2008), 491-494.
50. D. Masser, U. Zannier, *Torsion anomalous points and families of elliptic curves*, Amer. J. Math. **132** (2010), 1677-1691.
51. D. Masser, U. Zannier, *Torsion points on families of squares of elliptic curves*, Math. Annalen **352** (2012), 453-484.
52. D. Masser, U. Zannier, *Torsion points on families of products of elliptic curves*, Advances in Math. **259** (2014), 116-133.
53. D. Masser, U. Zannier, *Torsion points on families of abelian surfaces and Pell's equation over polynomial rings* (with Appendix by V. Flynn), J. European Math. Soc. **17** (2015), 2379-2416.
54. J.-F. Mestre, *Familles de courbes hyperelliptiques à multiplications réelles*, in Arithmetic Algebraic Geometry (eds. G. van der Geer, F. Oort, J. Steenbrink), Progress in Math. **89**, Birkhäuser 1991 (pp.193-208).
55. D. Mumford, T. Oda, *Algebraic Geometry II*, Hindustan Book Agency 2015.
56. J. Pila, *Integer points on the dilation of a subanalytic surface*, Quart. J. Math. **55** (2004), 207-223.
57. J. Pila, U. Zannier, *Rational points in periodic analytic sets and the Manin-Mumford conjecture*, Rendiconti Lincei Mat. Appl. **19** (2008), 149-162.
58. R. Pink, *A combination of the conjectures of Mordell-Lang and André-Oort*, in: Bogomolov F., Tschinkel Y. (eds) Geometric Methods in Algebra and Number Theory. Progress in Mathematics **235**, Birkhäuser Boston 2005.
59. A.J. van der Poorten, X.C. Tran, *Quasi-elliptic integrals and periodic continued fractions*, Monatsh. Math. **131** (2000), 155-169.
60. G. Rémond, *Conjectures uniformes sur les variétés abéliennes*, Quart. J. Math. **69** (2018), 459–486.
61. R.H. Risch, *The problem of integration in finite terms*, Trans. Amer. Math. Soc. **139** (1969), 167-189.
62. R.H. Risch, *The solution of the problem of integration in finite terms*, Bull. Amer. Math. Soc. **76** (1970), 605-608.
63. J.F. Ritt, *Integration in finite terms*, Columbia 1948.
64. M. Rosenlicht, *Generalized Jacobian varieties*, Annals of Math. **59** (1954), 505-530.
65. M. Rosenlicht, *Liouville's Theorem on functions with elementary integrals*, Pacific J. Math. **24** (1968), 153-161.
66. H. Schmidt, *Pell's equation in polynomials and additive extensions*, Quarterly J. Math. **68** (2017), 1335–1355.

67. H. Schmidt, *Relative Manin-Mumford in additive extensions*, Trans. Amer. Math. Soc. **371** (2019), 6463–6486.
68. H.A. Schwarz, *Gesammelte Math. Abh. II*, Springer-Verlag 1890.
69. J-P. Serre, *Morphismes universels et différentielles de troisième espèce*, Séminaire Claude Chevalley **4** (1958-1959), exposé 11, 1-8.
70. J-P. Serre, *Algebraic groups and class fields*, Graduate Texts in Math. **117**, Springer-Verlag 1988.
71. J-P. Serre, J. Tate, *Good reduction of abelian varieties*, Annals of Math. **88** (1968), 492-517.
72. J.H. Silverman, *Heights and the specialization map for families of abelian varieties*, J. reine Angew. Math. **342** (1983), 197-211.
73. J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math. **106**, Springer-Verlag 1986.
74. M.F. Singer, *Liouvillian solutions of linear differential equations with Liouvillian coefficients*, J. of Symbolic Computation **11** (1991), 251-274.
75. U. Zannier, *Some problems of unlikely intersections in arithmetic and geometry*, Annals of Math. Studies **181**, Princeton 2012.
76. U. Zannier, *Elementary integration of differentials in families and conjectures of Pink*, Proceedings ICM II (2014), 531-555.
77. U. Zannier, *Unlikely intersections and Pell's equations in polynomials*, Ch. 12 in Trends in Contemporary Mathematics (eds. V. Ancona and E. Strickland), Springer Indam Series 8, vol. **151**, DOI 10.1007/978-3-319-05254-0_12, Springer International Publishing Switzerland 2014.
78. U. Zannier, *Hyperelliptic continued fractions and generalized Jacobians*, to appear in Amer. J. Math.
79. S. Zhang, *Small points and Arakelov theory*, Documenta Math. (Extra Volume II of ICM 1998), 217–225.
80. B. Zilber, *Exponential sums equations and the Schanuel conjecture*, J. London Math. Soc. **65** (2002), 27-44.

D. Masser: Departement Mathematik und Informatik, Universität Basel, Spiegelgasse 1, 4051 Basel, Switzerland (*David.Masser@unibas.ch*).
U. Zannier: Scuola Normale Superiore, Piazza dei Cavalieri 7, 56126 Pisa, Italy (*u.zannier@sns.it*).

26th June 2020.