Multiplication polynomials and relative Manin-Mumford

Inauguraldissertation
zur
Erlangung der Würde eines Doktors der Philosophie

vorgelegt der
Philosophisch-Naturwissenschaftlichen Fakultät
der Universität Basel

von

Harry Schmidt
aus
Rheinfelden, Deutschland

Basel, 2015

Genehmigt von der Philosophisch-Naturwissenschaftlichen Fakultät auf Antrag von Prof. Dr. David Masser und Prof. Dr. Daniel Bertrand.

Basel, den 15. September 2015

Prof. Dr. Jörg Schibler
Dekan

Contents

1 Introduction 5

2 Resultants and discriminants of multiplication polynomials for elliptic curves 15

2.1 Introduction 15
2.2 Algebraic preparations 18
2.3 Analytic preparations 20
2.4 Proof of Theorem 1 23
2.5 Some more resultants 24
2.6 Proof of Theorem 2 26
2.7 Weierstrass and Legendre curves 29
2.8 Tate form 30

3 Relative Manin-Mumford in additive extensions 34

3.1 Introduction 34
3.2 Additive extensions 41
3.3 Reduction to G_λ 42
3.4 Rational points 44
3.5 Functions on $\mathbb{C}$ 45
3.6 Functions on C 48
3.7 Algebraic independence 49
3.8 Continuation. 51
3.9 Orders of torsion 52
3.10 Heights 53
3.11 Proof of Proposition (algebraic case) 54
3.11.1 Example of Effectivity 55
3.12 Proof of Proposition (transcendental case) 57
3.12.1 Reduction to a constant relation 58
3.12.2 Passing to a Weierstrass model defined over $\mathbb{Q}(j)$ 59
3.12.3 Galois theory 59
3.12.4 Conclusion 61
3.13 Split extensions 65
3.14 Non-split extensions again 65

4 Appendix A 67

4.1 Generalized Jacobians 67
4.1.1 Orders on a curve 67
4.1.2 Divisors 68

4.1.3 Modulus 69
4.1.4 Examples 71
4.2 Elementary integration 72
4.2.1 Definition 72
4.2.2 Proof of Theorem 4 73
4.3 Pell's equation in polynomials 75
4.3.1 Proof of Theorem 5 76
4.4 Reduction to G_λ in $\mathbb{A}^4$ 78

5 Appendix B **85**
5.1 Good reduction of flexible Lattès maps 85

1 Introduction

Since at least 300 years it is known that one can define a commutative group law, sometimes known as the chord-tangent law, on an algebraic curve defined by the equation

$$y^2 = x^3 + ax + b,\ 4a^3 + 27b^2 \neq 0.$$

The parameters a, b can lie in any field of characteristic not equal to 2 as long as the discriminant $\Delta = -(4a^3 + 27b^2)$ does not vanish. If we homogenize the equation we get a point at infinity O which is defined in any field and it is usual to fix this point as the identity. We can then speak of an elliptic curve E.

This gives means to add a point on the curve to itself. For almost all points of E (in almost all senses of the meaning) this leads to an infinite cyclic subgroup. But sometimes we get our original point back after a finite number of steps. Such a special point is then called a torsion point. These points play a central role in the study of elliptic curves.

For example it is a theorem of Mordell that if a, b lie in a number field K, the K-rational points $E(K)$ on E form a finitely generated group. More concretely $E(K)$ is isomorphic to a group of the form $T \times \mathbb{Z}^r$ for some rational integer $r \geq 0$ and some finite group T.

The number r itself has given rise to an intense field of study. It is often referred to as the rank of the elliptic curve and if $K = \mathbb{Q}$ it is generally believed that r can be arbitrarily large. But so far the biggest provable rank that occurred is 19 and the biggest lower bound for the rank of an elliptic curve is 28, both found by Elkies. In this context one should also mention the famous Birch and Swinnerton-Dyer conjecture which makes a connection between r and certain L-functions associated to E.

The finite group T of course consists of the torsion points with coordinates in K. If $K = \mathbb{Q}$ then a theorem of Mazur gives an explicit list of the groups that can occur (see for example [Si2, p.223, Theorem 7.5]). However the knowledge of the group structure does not directly provide a way to find those points and for larger fields even the structure of T is generally unknown.

In this thesis we mainly study elliptic curves defined over a field of characteristic zero. Then the complex theory with the rich theory of elliptic functions becomes central. These functions were intensely studied by 19th century mathematicians such as Weierstrass, Abel and Jacobi. Several books listing identities and relations between elliptic functions appear in the classical literature where we can name the books of Fricke [F] and Halphen [Hal] as examples.

Elliptic functions historically were often introduced as doubly periodic meromorphic functions and Weierstrass constructed the function $\wp$ named after him as

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Here Λ is a lattice $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ in $\mathbb{C}$ and the infinite sum defines a meromorphic function. The periodicity of $\wp$ with respect to ω_1 and ω_2 is then apparent from the definition.

We can define certain invariants g_2, g_3 of the lattice Λ given by infinite series

$$\begin{aligned} g_2 &= 60 \sum_{\omega \in \Lambda \setminus 0} \omega^{-4} \\ g_3 &= 140 \sum_{\omega \in \Lambda \setminus 0} \omega^{-6}. \end{aligned}$$

Even more, the pair $(g_2, g_3) \in \mathbb{C}^2$ determines the lattice Λ and always satisfies $g_2^3 - 27g_3^2 \neq 0$. The connection to elliptic curves then becomes clear with the differential equation

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3.$$

And indeed if we set $a = -g_2/4, g_3 = -g_3/4$ the map

$$\begin{aligned} \mathbb{C} &\longrightarrow E(\mathbb{C}) \\ z &\longrightarrow (\wp(z), \frac{1}{2}\wp'(z)) \end{aligned}$$

parametrizes the complex points of the curve E. The above map is often referred to as the exponential map of E and one can define such an (surjective) exponential map for each (connected) commutative group variety. The kernel of the exponential map of E is the lattice Λ and the points of order dividing n on E are the image of $\frac{1}{n}\Lambda$.

One of the many identities involving the Weierstrass $\wp$ function is

$$\wp(nz) = \frac{A_n(\wp(z))}{B_n(\wp(z))} \tag{1.0.1}$$

where A_n, B_n are polynomials with coefficients in $\mathbb{Z}[a, b]$ of degree n^2 and $n^2 - 1$ respectively and A_n is usually chosen to be monic. These polynomials can be directly defined using recursion formulae [Si2, Exercise 3.7(b)] and are itself of independent interest. One property that makes them important is that in a strong sense they encode all information about the torsion points of E.

Namely if (x, y) is of order n on E then multiplication by n sends (x, y) to the point at infinity O. From the identity (1.0.1) it follows that

$$B_n(x) = 0.$$

If $\Delta \neq 0$ then A_n, B_n are co-prime and in chapter 2 we study the relation between the resultant of these polynomials and the discriminant Δ. More precisely we obtain the following.

Theorem 1 *For natural numbers $n \geq 2$ we have*

$$\operatorname{res}(A_n, B_n) = (16\Delta)^{\frac{n^2(n^2-1)}{6}}.$$

Thus adding another identity to the long list. In the proof of Theorem 1 we make heavy use of the (20th century) theory of q-expansion of modular forms.

For each $n \geq 1$ we can define a rational map ϕ from $\mathbb{P}_1$ to $\mathbb{P}_1$ defined by homogenizing A_n, B_n. Such maps are know as flexible Lattès maps. The adjective flexible here should suggest that we can vary these maps in algebraic families. This is not the case for Lattès maps defined by complex multiplication (see for example [Mil, Lemma 5.5, p.29]) .

If the elliptic curve is defined over a field K with a non-archimedean valuation v we can define a reduction of E modulo v. If the reduced curve is an elliptic curve over the residue field we say that E has good reduction at v. Similarly we can reduce the rational map defined by A_n, B_n and we say that the reduction is good if the reduced map has the same degree as ϕ. With Canci, we investigated the connection between the reduction of E and ϕ. In Appendix B we show how to obtain the following proposition as a consequence of Theorem 1.

Proposition 2 *Let K be a field equipped with a non-archimedean valuation v and k the corresponding residue field. Let E be an elliptic curve given by an equation in Tate form defined over K. Let $\phi\colon \mathbb{P}_1(K) \to \mathbb{P}_1(K)$ be a flexible Lattès map associated to E where the corresponding π as given in (5.1.1) is also defined over K. Suppose that E has good reduction at v. Then there exists a $f \in \mathrm{PGL}_2(K)$*

such that $\phi^f = f \circ \phi \circ f^{-1}$ has good reduction at v.

Since the zeroes of B_n are the abscissa of the torsion points of order dividing n, it follows already from the fact that $\wp$ is an even function that B_n is generally not square-free. But if we take the largest square free part B_n^* of B_n it makes sense to ask for the connection between the discriminant of E and the discriminant of B_n^*. With the methods we used to prove Theorem 1 it was not a long way to obtain the following identities.

Theorem 2 *For natural numbers $n \geq 2$ we have*

$$\begin{aligned} \text{disc } B_n^* &= (-1)^{\frac{n-1}{2}} n^{\frac{n^2-3}{2}} (16\Delta)^{\frac{(n^2-1)(n^2-3)}{24}} \qquad (n \text{ odd}), \\ \text{disc } B_n^* &= (-1)^{\frac{n-2}{2}} n^{\frac{n^2}{2}} 2^{-(n^2-2)} (16\Delta)^{\frac{n^2(n^2+2)}{24}} \qquad (n \text{ even}). \end{aligned}$$

Apart from their (possible) intrinsic interest the above identities could also be useful from an algorithmic point of view. In [BuHu] the authors describe an algorithm which uses, among other things, the discriminant of B_n^* to compute the torsion points of $E(\mathbb{Q})$. In their article they already conjectured the above identity for n odd, and for n even we discuss the connection with their conjecture at the end of section 2.6.

In order to make sense of the formulae in Theorem 1 and 2 for elliptic curves in characteristic 2 and 3 we have to consider different models. In the sections 2.7 and 2.8 we translate everything to the common Weierstrass, Legendre and Tate model where we add a superscript W, L and T respectively to the multiplication polynomials.

Here the Legendre model E_λ given by

$$Y^2 = X(X-1)(X-\lambda)$$

(where we use the coordinates of chapter 3) stands out as it has only one parameter and we immediately see that the points of order 2 are always rational over the ground field (so T is never trivial).

We can view the multiplication polynomials A_n^L, B_n^L of E_λ as polynomials in two variables X, λ. (See [MZ3] where the authors studied those polynomials in more detail.)

If we fix λ to be 2, say, then the union of the solution sets of the equations

$$B_n^L(X, 2) = 0, \tag{1.0.2}$$

as n varies over the natural numbers $n \geq 2$, is the set of abscissae of the torsion points of the curve E_2. It is well known (for example from the work of Zimmer) that this set has bounded absolute height. However, already the description of the n-torsion points as $\frac{1}{n}\Lambda$ implies that its cardinality is infinite. So the union of the sets defined by the equations (1.0.2) is very sparse but still infinite.

We can then ask what happens if we specialize λ at two distinct numbers. So a natural question is whether the union of the solution sets of the simultaneous equations

$$B_n^L(X, 2) = 0, \quad B_n^L(X, 3) = 0 \tag{1.0.3}$$

is infinite.

Here it makes sense to reformulate this in more geometric terms. We do this by considering the abelian variety $E_2 \times E_3$ and the curve parameterized by

$$(X, \sqrt{X(X-1)(X-2)}, X, \sqrt{X(X-1)(X-3)})$$

in $E_2 \times E_3$. The intersection of this curve with the group of torsion points of $E_2 \times E_3$ yields the solutions to (1.0.3).

Now each variety defined by (1.0.3) has codimension 2 in $E_2 \times E_3$ and a curve has dimension 1. By the general philosophy of unlikely intersections as outlined by Zannier in the introduction of his book [Za2] we would expect finiteness. And in fact from the Manin-Mumford conjecture proven by Raynaud in the 1980's in [Ra1], [Ra2] follows finiteness for the solutions of (1.0.3).

However we could as well fix the abscissa and vary n and λ instead. In the second part of the last decade Masser asked whether analogous finiteness results for the equations

$$B_n^L(2, \lambda) = 0, \; B_n^L(3, \lambda) = 0 \tag{1.0.4}$$

hold. We can reformulate this as intersecting the curve parametrized by

$$(2, \sqrt{4 - 2\lambda}, 3, \sqrt{6 - 3\lambda})$$

in the family E_λ^2, as λ varies, with all torsion sections of the family E_λ^2. By the general philosophy of unlikely intersection we still expect finiteness since the family E_λ^2 forms a group scheme of total dimension 3 where the codimension of the torsion sections is 2 and the curve has dimension 1. And in fact in [MZ1] Masser and Zannier prove that there are at most finitely many complex λ satisfying at least one of the equations (1.0.4).

In this context it seems natural to try to formulate a relative version of the Manin-Mumford conjecture. A few years ago the following problem concerning families of semiabelian varieties came up.

Problem. *Let $\mathcal{S}$ be a semiabelian scheme (of constant toric rank) over a variety defined over $\mathbb{C}$, 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.*

Masser and Zannier went on from [MZ1] to prove the above statement for two-dimensional families of abelian varieties in a series of papers [MZ2], [MZ4], [MZ5]. In the case of a family of multiplicative extensions of an elliptic curve Bertrand [B2] found a counterexample. However he also showed that it still fits into the more general scheme of the Pink conjecture on mixed Shimura varieties (see [Pin, Conj. 1.2]) and together with Masser, Pillay and Zannier they showed in [BMPZ] that this is the only counterexample to the relative Manin-Mumford problem in the situation of two-dimensional families of semiabelian varieties.

The methods in the above mentioned work differ considerably from the methods used in [Ra1], [Ra2] to prove Manin-Mumford. Usually one part of the proof is to show that the points of finite order have bounded height and with this, one is able to deduce a lower bound for the Galois orbit of a torsion point in terms of its degree. Another part is to show that the inverse-image of a curve by the exponential map of the group varieties is generally a transcendental analytic set. Then one can use the counting theorem given in [Pil] or [PW] to give an upper bound for the Galois orbit. Comparing the two bounds then leads to finiteness.

This very broad strategy was first employed in [PZ] to give another proof of Manin-Mumford and has since then proven successful to verify various other cases of the so-called Zilber-Pink [Za1, p.78/79] conjecture.

But there is no reason to confine oneself to semiabelian varieties. As Hindry did in [Hi] for constant groups we can extend our scope to families of general two-dimensional commutative algebraic groups. With the work of Hindry, Bertrand-Masser-Pillay-Zannier and Masser-Zannier mentioned above the only remaining case for two-dimensional families are additive extensions of families of elliptic curves.

The easiest here are split such as $\mathbb{G}_a \times E_\lambda$ but if we want to treat all such extensions we also have to consider non-split extensions. Then the Weierstrass ζ function naturally comes up. This one can see for example in the letter of Serre, printed in [CMZ], where he shows how it appears in an embedding of a non-split extension.

Similarly to the Weierstrass $\wp$ function the ζ function has a multiplication formula, which is of the form

$$\zeta(nz) = n\zeta(z) + \frac{\wp'(z)B_n'(\wp(z))}{2nB_n(\wp(z))}$$

and was implicitly used in the proof of Lemma 2.5 in chapter 2. It also has an addition formula [CMZ, p.253, (3.13)] which together with the addition formula of $\wp$ transports the group structure to the embedding of the non-split extension.

In section 3.1 we introduce a Legendre model G_λ, based on an embedding of Masser (from [Mas1]), for such extensions. It is given by

$$Y^2 = X(X-1)(X-\lambda),\ V - YU = X^2$$

and in section 3.3 we show how X, Y, U, V are parametrized by the Weierstrass $\wp$ and ζ functions.

By definition $-\zeta$ is the anti-derivative of $\wp$ with respect to the complex variable z. But if we view $\zeta, \wp$ as functions of two variables z, λ, as they parametrize the family G_λ, the derivative of $\wp$ with respect to λ involves the ζ function again.

We use this fact in section 3.7 to prove, using the work of Bertrand [B1], that for a curve C in the family G_λ the inverse image of C by the exponential map is generally a transcendental analytic set. Here we could also have used the differential of the second kind on E_λ as suggested by Bertrand, and in section 3.7 we also indicate how.

As the work of Masser-Zannier on products of elliptic families [MZ2], [MZ4] the main result of chapter 3 is valid for curves over $\mathbb{C}$ while the other results in the direction of relative Manin-Mumford are only valid for curves over $\overline{\mathbb{Q}}$. The step from $\overline{\mathbb{Q}}$ to $\mathbb{C}$ is done in section 3.12 and follows the strategy of Masser-Zannier for products of elliptic families.

By reducing to the Legendre model G_λ we can summarize the result from chapter 3 in in the language of the relative Manin-Mumford problem as follows.

Theorem 3 *Let $\mathcal{G}$ be an additive extension by $\mathbb{G}_a$ of an elliptic scheme over a variety defined over $\mathbb{C}$, and denote by $\mathcal{G}^{[c]}$ the union of its flat subgroup 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 subgroup schemes of $\mathcal{G}$ of positive codimension.*

Before we proceed to the applications of Theorem 3 we want to write some words on effectivity.

In the case of a non-split additive extension the inverse image of the variety $\mathcal{V}$ by the exponential maps is a complex analytic set rather than only a real analytic one as in the abelian case. This allowed us to use the counting theorem of Masser given in [Mas2] on counting rational points on analytic curves instead of the counting results in [Pil] or [PW]. This opens the door for effective refinements of Theorem 3 for curves defined over the algebraic numbers (see also subsection 3.11.1).

The proof of the transcendental case as given in section 3.12 is already effective as are the results of Masser-Zannier in [MZ2], [MZ4] for curves not defined over $\overline{\mathbb{Q}}$. We also refer to [MZ3] here, where Masser and Zannier investigate the effectivity for the transcendental case further.

At this point one should also mention the work of Stoll [Sto] who showed, using reduction techniques, that the set defined by (1.0.4) is in fact empty. He also obtained results for curves in E_λ^2 with fixed transcendental abscissa.

Finally in Appendix A we give some examples for applications of Theorem 3. The first in section 4.2 is in the theory of elementary integration.

Here the adjective elementary refers to a certain type of function. Roughly speaking all functions known from High-School mathematics are elementary. The theory of elementary integration revolves around the question when the primitive of an elementary function is again elementary.

In this context James Davenport made an interesting claim about families of algebraic functions parametrized by a curve [Dave, p.90, Theorem 7] and we give a formulation of his claim in section 4.2. In [MZ6] Masser and Zannier prove this claim for curves defined over a finite extension of $\mathbb{Q}$ building on their previous work on the relative Manin-Mumford problem.

It seems that Theorem 3 together with [MZ2], [MZ4] makes it possible to prove the claim for curves over $\mathbb{C}$ when the functions are elements of the function field of an elliptic curve. We illustrate this in Appendix A by proving the claim for the family of functions $\frac{1}{(X-2)\sqrt{X(X-1)(X-\lambda)}}$ in section 4.2.2.

Theorem 4 *There are at most finitely many $\lambda \in \mathbb{C}$ such that*

$$\frac{1}{(X-2)\sqrt{X(X-1)(X-\lambda)}}$$

is elementary integrable.

For the proof of Theorem 4 we need the theory of generalized Jacobians which we briefly introduce in section 4.1.

Using generalized Jacobians we can also give an application of Theorem 3 to Pell's equation in polynomials. This is done in section 4.3 where we prove the following theorem.

Theorem 5 *There are at most finitely many complex t such that $D_t = X^3(X^3 + X + t)$ is Pellian.*

Here, a polynomial D is called Pellian if there exist polynomials A, B such that

$$A^2 - DB^2 = 1, B \neq 0.$$

If we replace the ring of polynomials with $\mathbb{Z}$ we are back in the classical Pell's equation which detects the units of the ring of integers of quadratic fields $\mathbb{Q}(\sqrt{D})$.

Similarly the Pellianity of D_t in Theorem 5 is equivalent to the existence of a non-trivial unit in the ring $\mathbb{C}[X, \sqrt{D_t}]$. So Theorem 5 states that there are at most finitely many specializations of t such that the specialized ring has non-trivial units.

Then in section 4.3 we show how to reduce Theorem 4 and 5 to Proposition 1 of section 3.3, which might be useful to prove explicit bounds for these problems.

Acknowledgement

First I would like to thank my research supervisor David Masser for introducing me to the vast world of the Zilber-Pink conjecture. The importance of his help and support for the development of this work can not be underestimated.

Further I want to thank Jung Kyu Canci, with whom I wrote Appendix B, for his assistance in LaTeX for chapter 2. Also I would like to thank Joseph Silverman and John Tate for valuable correspondence. We also greatly profited from a remark of Daniel Bertrand in chapter 3.

I would also like to thank the following persons for many discussions and creating a social atmosphere at the mathematical institute in Basel: Jung Kyu Canci, Jürgen Dölz, Maria and Christian Graf, Mattias Hemming, Lukas Pottmeyer, Andriy Regeta, Christian Urech and Susanna Zimmermann.

Finally I would like to thank my family and in particular my wife Tatjana and my children Leon and Evelina for their support and never ending efforts to keep me busy.

2 Resultants and discriminants of multiplication polynomials for elliptic curves

In this chapter, we prove that the resultant of the standard multiplication polynomials A_n, B_n of an elliptic curve in the form $y^2 = x^3 + ax + b$ is $(16\Delta)^{\frac{n^2(n^2-1)}{6}}$, where $\Delta = -(4a^3 + 27b^2)$ is the discriminant of the curve. We give an application to good reduction of an associated Lattès map. We also prove a similar result for the discriminant of the largest square free factor of B_n.

2.1 Introduction

If a, b are elements of a field of characteristic not 2 with

$$\Delta = -(4a^3 + 27b^2) \neq 0,$$

then the equation

$$y^2 = x^3 + ax + b \tag{2.1.1}$$

defines an elliptic curve. It is well-known, see for example [Si2], Exercise 3.7 (p.105), that for each natural number n there are polynomials $A_n, B_n \neq 0$ in x such that multiplication by n sends the point $P = (x, y)$ to a point whose x-coordinate is $\frac{A_n(x)}{B_n(x)}$. The classical literature studied such things in detail, but mainly for the Weierstrass model with an extra coefficient 4 in (2.1.1); there we see functions ϕ_n, ψ_n^2 instead of A_n, B_n. See among others Fricke [F, p.184-196], Halphen [Hal, p. 96-106] and Tannery and Molk [TM, p.100-105]. For example

$$A_1(x) = x, \quad B_1(x) = 1, \quad A_2(x) = x^4 - 2ax^2 - 8bx + a^2, \quad B_2(x) = 4(x^3 + ax + b). \tag{2.1.2}$$

In general they are usually normalized by their leading terms

$$A_n(x) = x^{n^2} + \cdots, \quad B_n(x) = n^2 x^{n^2-1} + \ldots. \tag{2.1.3}$$

(see [Si2, Exercise 3.7(b)]). More terms seem to be difficult to find in the literature, classical or otherwise, and in connexion with another investigation Masser and Zannier [MZ3] have recently found that

$$A_n(x) = x^{n^2} - \kappa_n a x^{n^2-2} - \lambda_n b x^{n^2-3} + \cdots, \quad B_n(x) = n^2 x^{n^2-1} + \mu_n a x^{n^2-3} + \cdots \tag{2.1.4}$$

where

$$\kappa_n = \frac{n^2(n^2-1)}{6}, \quad \lambda_n = \frac{2n^2(n^4-1)}{15}, \quad \mu_n = \frac{n^2(n^2-1)(n^2+6)}{30}. \tag{2.1.5}$$

With more work a few more early coefficients could be found but they get increasingly complicated, and it seems hopeless to obtain similar expressions for late coefficients like the constant terms.

A fundamental property is that A_n, B_n are coprime for any specialization of a, b to any field of charactersitic not equal to 2 as long as $\Delta \neq 0$ (see also [Si2, Exercise 3.7(c)]), which if $n \geq 2$ is equivalent to the non-vanishing of the resultant $\text{res}(A_n, B_n)$. Here we mean this in a formal sense as if B_n had degree $n^2 - 1$ (see for example [La3, p.200]). It seems that no one has ever calculated $\text{res}(A_n, B_n)$ explicitly. As the resultant is given by a complicated Sylvester determinant looking like

$$\begin{vmatrix} 1 & 0 & -\kappa_n a & -\lambda_n b & \ldots \\ 0 & 1 & 0 & -\kappa_n a & \ldots \\ \vdots & \vdots & \vdots & \vdots & \ddots \\ n^2 & 0 & \mu_n a & ? & \ldots \\ 0 & n^2 & 0 & \mu_n a & \ldots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{vmatrix} \tag{2.1.6}$$

for (2.1.4), the task would at first sight seem difficult. Nevertheless it is what we do in the present section, with a result that may initially seem surprisingly simple.

Theorem 1. *For natural numbers $n \geq 2$ we have*

$$\text{res}(A_n, B_n) = (16\Delta)^{\frac{n^2(n^2-1)}{6}}.$$

It is a natural step from resultants to discriminants, and as B_n is known to play a major role in the study of torsion points it may seem justified to ask for its discriminant. Unfortunately if $n > 1$ then B_n is not squarefree and so this discriminant vanishes. But it can be shown (see [Si2, Exercise 3.7(a)]) that we have

$$B_n = B_n^{*2} \quad (n \text{ odd}) \tag{2.1.7}$$

$$B_n = B_n^{*2}/C \quad (n \text{ even}) \tag{2.1.8}$$

for a polynomial B_n^* unique up to sign, where $C = C(x) = x^3 + ax + b$. Here B_n^* is squarefree, at least in characteristic 0. In particular C divides B_n and B_n^* when n is even. We calculate the discriminant disc B_n^* (also in the formal sense - see also [La3, p.204]).

Theorem 2. *For natural numbers $n \geq 2$ we have*

$$\text{disc } B_n^* = (-1)^{\frac{n-1}{2}} n^{\frac{n^2-3}{2}} (16\Delta)^{\frac{(n^2-1)(n^2-3)}{24}} \quad (n \text{ odd}),$$

$$\text{disc } B_n^* = (-1)^{\frac{n-2}{2}} n^{\frac{n^2}{2}} 2^{-(n^2-2)} (16\Delta)^{\frac{n^2(n^2+2)}{24}} \quad (n \text{ even}).$$

After using Fourier expansions to establish these results we came across Exercise 6.23(e) in Silverman's dynamical book [Si4, p.383], which gives the resultant in Theorem 1, at least up to an undetermined sign. During our proof we had already noted that the resultant up to undetermined powers of $-1, 2$ could be found relatively simply without Fourier. And it turns out that the prime 2 can be eliminated using the Tate form, thus supplying a similar proof of the Exercise. But this requires certain integrality assertions which are not easy to track down in the literature (see section 2.8 below).

However it seems that such purely arithmetic techniques do not extend to the discriminant in Theorem 2; at best they give in place of the displayed powers of 2 and n only some undetermined product of primes p dividing n. Even more recently we also came across Lemma 1 of Stark [Sta, p.354] which implies our Theorem 2 up to sign when n is odd (see also Exercise 1.14(b) of Silverman's second elliptic book [Si3, p.88]). His proof seems rather different using the Kronecker Limit Formula. We think it useful to publish our unified proof for general n, and it is hardly any more work to include our original proof of Theorem 1; in fact we deduce Theorem 2 from Theorem 1 rather quickly. Also in section 2.6 we comment on how Theorem 2 is related to the conjecture made in [BuHu, p.31].

Here is how the proofs are arranged. In section 2.2 we show with comparatively simple arguments that the general shape of Theorems 1 and 2 is not too surprising. In particular we get Theorem 1 up to powers of $-1, 2$. Then in section 2.3 we set the stage for the main calculations, which involve Fourier expansions of elliptic functions and modular forms. These are carried out in section 2.4 to prove Theorem 1. Here some work can be saved thanks to the transcendence of π! We could use similar calculations to prove Theorem 2 but to avoid too many complications we first give some auxiliary resultants in section 2.5. At last in section 2.6 we prove Theorem 2. Then in section 2.7 we translate our results from $x^3 + ax + b$ in (2.1.1) to the more classical Weierstrass form $4x^3 - g_2x - g_3$ and the Legendre form $x(x-1)(x-\lambda)$ investigated in [MZ3].

And finally in section 2.8 we pass to the Tate form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6; \tag{2.1.9}$$

as mentioned, this leads purely arithmetically to Theorem 1 up to sign. It also leads to a version of Proposition 6.55 of [Si4, p.362] about good reduction of the Lattès map ϕ_n of degree n^2 for a curve E in Tate form: namely if $n \geq 2$ and our ground field has a discrete ultrametric valuation with respect to which (2.1.9) is minimal, then ϕ_n has good reduction if and only if E has good reduction. This is proven in the Appendix where the arguments belong to the theory of good reduction of rational maps.

Finally a comment on the characteristic of the ground field seems to be in place. All formulae appearing are identities and Theorem 1 and 2 are valid for a, b in an arbitrary field simply by specialization. However A_n^W, B_n^W in section 2.7 are elements in $\mathbb{Z}[\frac{g_2}{4}, \frac{g_3}{4}, x]$ so it seems that it *a priori* doesn't make sense to ask for any properties in characteristic 2. In contrast $A_n^L, B_n^L, B_n^{L*} \in \mathbb{Z}[x, \lambda]$ (see [MZ3], section 2) and the formulae in section 2.7 are valid in any characteristic. The same holds for A_n^T, B_n^T in section 2.8 but B_n^{T*} can carry a denominator 2 for n even. We would need to replace B_n^{T*} by $2B_n^{T*}$ to make sense of the discriminant in characteristic 2 which is then identically zero.

At this point I thank Joseph Silverman and John Tate for valuable correspondence. I also thank my supervisor David Masser for suggesting this problem and his assistance in writing this chapter.

2.2 Algebraic preparations

The following observation gives quite quickly the general shape of the resultant.

Lemma 2.1. *For each natural number $n \geq 2$ there are integers c_n, c_n^* and $k_n \geq 0, k_n^* \geq 0$, depending only on n, such that*

$$\mathrm{res}(A_n, B_n) = c_n \Delta^{k_n}, \quad \mathrm{disc}\ B_n^* = c_n^* \Delta^{k_n^*}.$$

Further there are integers d_n and $l_n \geq 0$, depending only on n, such that

$$\mathrm{res}(C, B_n) = d_n \Delta^{l_n}, \quad (n \text{ odd})$$

$$\mathrm{res}(C, B_n/C) = d_n \Delta^{l_n}. \quad (n \text{ even})$$

Proof. It is known that $A_n(x), B_n(x)$ and even $B_n^*(x)$ lie in $\mathbb{Z}[x, a, b]$ (again see [Si2, Exercise 3.7(a)]). As $C(x)$ is monic this is also true of $B_n(x)/C(x)$ when n is even. Thus it will suffice to prove the lemma when a, b are independent variables over $\mathbb{Q}$. Now the first resultant can be denoted by $R_n(a, b)$ in $\mathbb{Q}[a, b]$. If we specialize a, b to any a_0, b_0 algebraic over $\mathbb{Q}$ then the resultant specializes too, and if it is zero then we must have $\Delta(a_0, b_0) = 0$, where $\Delta(a, b) = -(4a^3 + 27b^2)$. By the Hilbert Nullstellensatz (see for example [La3, p.380]) there is a positive integer $m = m_n$ and a Q_n in $\mathbb{Q}[a, b]$ such that $\Delta(a, b)^m = Q_n(a, b)R_n(a, b)$. Since $\Delta(a, b)$ is irreducible it follows that $R_n(a, b) = c\Delta(a, b)^k$ for some rational $c = c_n$ and some non-negative integer $k = k_n$. Finally since $R_n(a, b)$ is actually in $\mathbb{Z}[a, b]$ and $\Delta(a, b)$ is primitive in $\mathbb{Z}[a, b]$ it follows that c is in $\mathbb{Z}$, and this settles $\mathrm{res}(A_n, B_n)$. The same arguments work for disc B_n^* because we are in zero characteristic.

Similar arguments work for $\operatorname{res}(C, B_n)$ provided we can show that the two polynomials are coprime. But this is clear, because $C = \frac{1}{4}B_2$ vanishes at the x-coordinates of points $P \neq O$ with $2P = O$ and in the same way B_n with $nP = O$; as n is odd both are not simultaneously possible. And likewise for B_n/C with $nP = O$ but $2P \neq O$; this quotient is also in $\mathbb{Z}[x, a, b]$ because C is monic. That C^2 does not divide B_n can also be deduced from the fact that for the rational map $\phi_n = \frac{A_n}{B_n}$ (in affine form) satisfies $\phi_n \circ x = x \circ [n]$ where $[n]$ is the multiplication by n map and x the projection (5.1.2) as defined in the appendix. Now x is a degree 2 map ramified at O and the 2-torsion points while $[n]$ is a map of degree n^2. These arguments also deliver the shape of B_n as given in (2.1.7), (2.1.8). □

We could go a bit further and verify by homogeneity arguments (assigning x, a, b the usual weights 1,2,3 respectively in (2.1.6)) that here k_n is equal to κ_n, defined in (2.1.5), as in Theorem 1, but the details are not quite straightforward and the calculations of section 2.3 will anyway deliver this with relatively little effort. The real purpose of these calculations is to get at c_n. In fact for any prime $p \neq 2$ the equation $y^2 = x^3 - x$ over $\mathbb{F}_p$ defines an elliptic curve with $\Delta = -4$, and so if p divides c_n then $\operatorname{res}(A_n, B_n) = 0$ would contradict the coprimality (known for $p \neq 2$). Thus c_n is composed of powers of -1 and 2.

We can even deal with 2 in a similar way by passing to the curve $y^2 + y = x^3 - x$ in Tate form, and that would yield Theorem 1 up to sign; however this step is a bit more delicate and we postpone it to section 2.8. In fact all we need to know in the sequel is that c_n is a rational number depending only on n. Similar remarks apply for k_n^*, l_n. But for c_n^*, d_n we have to be more careful, because the zeroes of C and B_n can coalesce. However this happens only if the characteristic divides $2n$, so all we could conclude in general is that c_n^*, d_n are composed at most of powers of primes dividing $2n$. It may be found a little surprising that c_n^* is essentially a power of n (and we will see that $d_n = n^6$ when n is even).

Lemma 2.2. *For all natural numbers n we have*

$$4(A_n^3 + aA_nB_n^2 + bB_n^3)B_n = B_{2n}.$$

Proof. For a point $P = (x, y)$ on our elliptic curve we calculate $2nP$ as $2(nP)$. We find

$$\frac{A_{2n}}{B_{2n}} = \frac{A_2(\frac{A_n(x)}{B_n(x)})}{B_2(\frac{A_n(x)}{B_n(x)})} = \frac{A}{B}, \tag{2.2.1}$$

where by (2.1.2)

$$A = A_n^4 - 2aA_n^2B_n^2 - 8bA_nB_n^3 + a^2B_n^4, \quad B = 4(A_n^3 + aA_nB_n^2 + bB_n^3)B_n.$$

Now in (2.2.1) A_{2n}, B_{2n} are coprime, and the degree of A is at most $4n^2 = (2n)^2$ which is already the degree of A_{2n}. It follows that A_{2n}, A are equal up to constants, and by checking the leading coefficients using (2.1.3) we deduce equality. So also $B_{2n} = B$, which is what we want. □

For the sequel we record some properties of resultants. For polynomials $A = a\prod_\alpha(x-\alpha)$ of degree $r \geq 1$ and $B = b\prod_\beta(x-\beta)$ of degree $s \geq 1$ we have

$$\mathrm{res}(A,B) = a^s b^r \prod_{\alpha,\beta}(\alpha-\beta) = a^s \prod_\alpha B(\alpha) = (-1)^{rs} b^r \prod_\beta A(\beta) \qquad (2.2.2)$$

(see for example [La3, p.202]). These make clear the multiplicativity in both A and B separately; and also

$$\mathrm{res}(A,B) = \mathrm{res}(A, B+\tilde{A}) = \mathrm{res}(A+\tilde{B}, B) \qquad (2.2.3)$$

for any $\tilde{A}, \tilde{B}$ such that $B+\tilde{A}$ also has degree s, $A+\tilde{B}$ also has degree r, as well as $\tilde{A}(\alpha) = 0$ for all α and $\tilde{B}(\beta) = 0$ for all β.

2.3 Analytic preparations

From now on the coefficients a, b in (2.1.1) will be complex numbers. In fact we start with an element τ of the upper half-plane and the corresponding lattice $\Lambda(\tau) = \mathbb{Z} + \mathbb{Z}\tau$ in $\mathbb{C}$. One defines the corresponding Weierstrass function $\wp(z) = \wp(z;\tau)$ and the corresponding map P from $\mathbb{C}/\Lambda(\tau)$ to an elliptic curve $E = E(\tau)$ defined by(2.1.1), where $P(z) = (\wp(z), \frac{1}{2}\wp'(z))$ with the usual convention that $P(z)$ is the group origin for every z in the lattice. Here

$$a = a(\tau) = -\frac{1}{4}g_2(\tau), \quad b = b(\tau) = -\frac{1}{4}g_3(\tau) \qquad (2.3.1)$$

for the standard Eisenstein series g_2, g_3. This is a group isomorphism between $\mathbb{C}/\Lambda(\tau)$ and the complex points $E(\tau)(\mathbb{C})$ ([Si2, p.158]). We also define

$$e_1 = e_1(\tau) = \wp\left(\frac{\tau}{2}\right), \quad e_2 = e_2(\tau) = \wp\left(\frac{1}{2}\right), \quad e_3 = e_3(\tau) = \wp\left(\frac{\tau+1}{2}\right). \qquad (2.3.2)$$

It is well-known that

$$C(x) = x^3 + ax + b = (x-e_1)(x-e_2)(x-e_3). \qquad (2.3.3)$$

Now recall the polynomials A_n, B_n corresponding to the curve $E(\tau)$. We write $\mathcal{C}_n$ for the set

$$\mathcal{C}_n = \{(r,s) \in \mathbb{Z}^2; 0 \leq r, s < n, (r,s) \neq (0,0)\}. \qquad (2.3.4)$$

Lemma 2.3. *For all natural numbers n we have*

$$B_n(x) = n^2 \prod_{\mathcal{C}_n} \left(x - \wp\left(\frac{r\tau + s}{n}\right)\right) \tag{2.3.5}$$

and

$$\begin{aligned} A_n(x) - e_1 B_n(x) &= \prod_{\substack{\mathcal{C}_{2n} \\ r \text{ odd}, s \text{ even}}} \left(x - \wp\left(\frac{r\tau + s}{2n}\right)\right) \qquad (2.3.6) \\ A_n(x) - e_2 B_n(x) &= \prod_{\substack{\mathcal{C}_{2n} \\ r \text{ even}, s \text{ odd}}} \left(x - \wp\left(\frac{r\tau + s}{2n}\right)\right) \\ A_n(x) - e_3 B_n(x) &= \prod_{\substack{\mathcal{C}_{2n} \\ r \text{ odd}, s \text{ odd}}} \left(x - \wp\left(\frac{r\tau + s}{2n}\right)\right). \end{aligned}$$

Proof. The zeros of B_n are the x-coordinates $x(P)$ of the points $P \neq O$ on $E(\tau)$ with $nP = O$. These are the $\wp\left(\frac{r\tau+s}{n}\right)$ and we can restrict here to $\mathcal{C}_n$. Now $x(P) = x(Q)$ is equivalent to $P = \pm Q$. So each value turns up exactly twice except if n is even, when the three values (2.3.2) each turn up once. By (2.3.3) this corresponds precisely to (2.1.7) and (2.1.8) and we deduce (2.3.5).

Again using (2.3.3) on Lemma 2.2 we see that

$$4(A_n - e_1 B_n)(A_n - e_2 B_n)(A_n - e_3 B_n) B_n \;=\; B_{2n}.$$

Thus the $(2n)^2$ zeroes $\wp\left(\frac{r\tau+s}{2n}\right)$ of B_{2n} are distributed between those of $A_n - e_1 B_n$, $A_n - e_2 B_n$, $A_n - e_3 B_n$ and B_n. Clearly we get a zero of B_n if and only if r and s are both even. Also $A_n(x) - e_1 B_n(x) = 0$ for $x = x(P)$ is equivalent to $x(nP) = e_1$ and so $\wp\left(\frac{r\tau+s}{2}\right) = \wp\left(\frac{\tau}{2}\right)$ by (2.3.2). This in turn is equivalent to r odd and s even. Similarly for the remaining two factors. □

Finally we need some Fourier expansions in $q = e^{2\pi i \tau}$. We have

$$\frac{1}{(2\pi i)^{12}}(g_2^3 - 27 g_3^2) = q \prod_{l=1}^{\infty} (1 - q^l)^{24}$$

whose leading term suffices for us, in the form

$$\Delta = -(4a^3 + 27b^2) = \frac{g_2^3 - 27g_3^2}{16} = \frac{(2\pi i)^{12}}{16} q + \cdots . \tag{2.3.7}$$

Then

$$\frac{1}{(2\pi i)^2} \wp(z;\tau) \;=\; \frac{1}{12} + \sum_{m \in \mathbf{Z}} \frac{Qq^m}{(1 - Qq^m)^2} - 2 \sum_{k=1}^{\infty} \frac{kq^k}{1 - q^k},$$

where $Q = e^{2\pi iz}$ [La2, p. 46, Proposition 3]. Putting $z = \frac{r\tau+s}{n}$ for (r,s) in $\mathcal{C}_n$ we deduce not quite as in [La2, p.66]

$$\frac{1}{(2\pi i)^2}\wp\left(\frac{r\tau+s}{n};\tau\right) \;=\; \frac{1}{12}+\frac{q^{\frac{r}{n}}\zeta_n^s}{(1-q^{\frac{r}{n}}\zeta_n^s)^2}+\sum_{k=1}^{\infty}\sum_{m=1}^{\infty}kq^{mk}(q^{\frac{rk}{n}}\zeta_n^{sk}+q^{-\frac{rk}{n}}\zeta_n^{-sk}-2),$$

where $\zeta_n = e^{\frac{2\pi i}{n}}$. But here the leading term or terms are not so clear if we view the Fourier expansion as a power series in $q^{\frac{1}{n}}$.

If $r \neq 0$ then $|q^{\frac{r}{n}}\zeta_n^s| < 1$ so we can expand

$$\frac{q^{\frac{r}{n}}\zeta_n^s}{(1-q^{\frac{r}{n}}\zeta_n^s)^2} = \sum_{k=1}^{\infty} k(q^{\frac{r}{n}}\zeta_n^s)^k$$

and we get a power series in $q^{\frac{1}{n}}$ of the form

$$\frac{1}{(2\pi i)^2}\wp\left(\frac{r\tau+s}{n};\tau\right) \;=\; \frac{1}{12}+q^{\frac{r}{n}}\zeta_n^s+q^{\frac{n-r}{n}}\zeta_n^{-s}+\cdots\,, \tag{2.3.8}$$

where the remaining terms involve $q^{\frac{t}{n}}$ with $t > \min\{r, n-r\}$.

If $r = 0$ then we get

$$\frac{1}{(2\pi i)^2}\wp\left(\frac{r\tau+s}{n};\tau\right) \;=\; \frac{1}{12}+\frac{\zeta_n^s}{(1-\zeta_n^s)^2}+\cdots\,, \tag{2.3.9}$$

where the remaining terms involve $q^{\frac{t}{n}}$ with $t > 0$.

Finally we need the well-known

$$\prod_{s=1}^{n-1}(1-\zeta_n^s) = n \tag{2.3.10}$$

which is proved by evaluating $\prod_{s=1}^{n-1}(X-\zeta_n^s) = \frac{X^n-1}{X-1}$ at $X = 1$. Similarly

$$\prod_{s=1}^{n-1}(1+\zeta_n^s) = 1, \quad (n \text{ odd}) \tag{2.3.11}$$

$$\prod_{s=0,s\neq\frac{n}{2}}^{n-1}(1+\zeta_n^s) = n. \quad (n \text{ even}) \tag{2.3.12}$$

2.4 Proof of Theorem 1

In view of Lemma 2.1 and (2.3.7) it suffices to calculate the leading term of the resultant $\mathrm{res}(A_n, B_n)$ in our Fourier case (2.3.1).

In (2.2.2) we can use (2.3.5) to factorize $B = B_n$ but we have not yet factorized A_n; however by (2.2.3) the resultant is also $\mathrm{res}(A_n - \gamma B_n, B_n)$ for any complex number γ. It is most convenient here to choose $\gamma = e_1$; then we can use (2.3.6).

This leads to the basic formula

$$\mathrm{res}(A_n, B_n) \;=\; (2\pi i)^{2n^2(n^2-1)}(n^2)^{n^2} \prod_{(r,s)\in\mathcal{C}_n} \prod_{\substack{(r',s')\in\mathcal{C}_{2n} \\ r' \text{ odd, } s' \text{ even}}} f(r', s', r, s), \tag{2.4.1}$$

where

$$f(r', s', r, s) \;=\; \frac{1}{(2\pi i)^2}\left(\wp\left(\frac{r'\tau + s'}{2n}\right) - \wp\left(\frac{r\tau + s}{n}\right)\right). \tag{2.4.2}$$

Next we examine (2.4.2) using (2.3.8) and (2.3.9). The $\frac{1}{12}$ disappears; and as r' is odd the only way to get a constant term is with $r = 0$. This term is then $-\frac{\zeta_n^s}{(1-\zeta_n^s)^2}$. Taking the product over $s = 1, \ldots, n-1$ gives $(-1)^{n-1}\frac{1}{n^2}\zeta_n^{\frac{n(n-1)}{2}}$ using (2.3.10), and then the product over the n^2 pairs (r', s') in (2.4.1) gives

$$(n^2)^{-n^2}. \tag{2.4.3}$$

This cancels with one of the outside factors in (2.4.1).

It remains to consider the (2.4.2) outside $r = 0$, so that (2.3.8) holds for both parts. To ease notation we write $s' = 2t$, so that $t = 0, \ldots, n-1$. We find now

$$f(r', s', r, s) \;=\; q^{\frac{r'}{2n}}\zeta_n^t + q^{\frac{2n-r'}{2n}}\zeta_n^{-t} - q^{\frac{2r}{2n}}\zeta_n^s - q^{\frac{2n-2r}{2n}}\zeta_n^{-s} + \cdots, \tag{2.4.4}$$

where all other powers of $q^{\frac{1}{2n}}$ exceed $M = \min\{R', R\}$ for

$$R' = \min\{r', 2n - r'\}, \quad R = \min\{2r, 2n - 2r\}.$$

We claim that this minimum

$$M = \min\{r', 2n - r', 2r, 2n - 2r\} \tag{2.4.5}$$

is attained at exactly one of the four elements, so that exactly one of the four terms on the right of (2.4.4) is the leading term, then involving $q^{\frac{M}{2n}}$.

Note that R is even but R' is odd because r' is odd. In particular $R' \neq R$.

If $R' < R$ then $M = R'$ and so the above claim can be false only if $M = r' = 2n - r'$. But then $n = r'$ is odd and $M = n$, and as $R \leq n$ we must have $R < n = M = R'$, a contradiction.

Similarly if $R' > R$ then $M = R$ and the claim can be false only if $M = 2r = 2n - 2r$. But then $n = 2r$ is even and $M = n$, and as $R' \leq n$ we must have $R' < n = M = R$, another contradiction.

So the above claim regarding (2.4.5) is verified.

It follows from this discussion that if $R' < R$ then $q^{\frac{M}{2n}}\zeta_n^{\pm t}$ is the leading term in (2.4.4) while if $R' > R$ then we get $-q^{\frac{M}{2n}}\zeta_n^{\pm s}$. Furthermore the ± do not depend on t, s. These latter both range unrestrictedly from 0 to $n-1$ and so taking the product over t, s kills off the roots of unity. Taking the further product over r, r' we end up with some $(-1)^{\sigma_n}q^{k_n^*}$. Here σ_n is the number of (r, s, r', s') with $R' > R$. If n is even then σ_n is even due to the range of t (or s); while if n is odd, then σ_n is even because we may pair a given r with $n - r \neq r$.

So the product in (2.4.1) outside $r = 0$ is simply $q^{k_n^*}$. Combining this with the above result (2.4.3) for $r = 0$ we end up with $(2\pi i)^{2n^2(n^2-1)}q^{k_n^*}$ as the leading term of $\mathrm{res}(A_n, B_n)$.

On the other hand by Lemma 2.1 and (2.3.7) this leading term is $c_n\left(\frac{(2\pi i)^{12}}{16}q\right)^{k_n}$. It follows that $k_n^* = k_n$ and

$$16^{k_n}(2\pi i)^{2n^2(n^2-1)-12k_n} = c_n.$$

However c_n is rational and π is transcendental and therefore we must have $k_n = \frac{n^2(n^2-1)}{6}$ which is just κ_n from (2.1.5). Thus also $c_n = 16^{\kappa_n}$ and this completes the proof of Theorem 1.

Of course our appeal to the transcendence of π could be avoided here by directly verifying that our exponent of q, which comes out from the above as the sum of (2.4.5) over the range in (2.4.1), is κ_n. We leave this to the reader. The verification is slightly easier if one uses $A_n - e_2B_n$ rather than $A_n - e_1B_n$ in (2.3.6), when (2.4.5) becomes the more symmetric $\min\{r', n - r', r, n - r\}$.

2.5 Some more resultants

We could calculate the discriminant of B_n^* in Theorem 2 by deducing its zeros from (2.3.5) and using the standard product formula. But this leads to long and involved calculations which we prefer to avoid. Instead we first calculate the other resultants in Lemma 2.1.

Lemma 2.4. *We have*

$$\mathrm{res}(C, B_n) = \Delta^{\frac{n^2-1}{2}}, \quad (n \text{ odd})$$

$$\mathrm{res}(C, B_n/C) = n^6 \Delta^{\frac{n^2-4}{2}}. \quad (n \text{ even})$$

Proof. Of course we go back to Fourier.

We start with n odd. We have

$$\mathrm{res}(C, B_n) \;=\; (2\pi i)^{6(n^2-1)}(n^2)^3 \prod_{(r,s)\in\mathcal{C}_n} \prod_{(r',s')\in\mathcal{C}_2} f(r', s', r, s), \tag{2.5.1}$$

where now

$$f(r', s', r, s) \;=\; \frac{1}{(2\pi i)^2}\left(\wp\left(\frac{r'\tau + s'}{2}\right) - \wp\left(\frac{r\tau + s}{n}\right)\right).$$

Now the right-hand sides of (2.3.8) and (2.3.9) for $n = 2$ read simply $\frac{1}{12} + 2q^{\frac{1}{2}} + \cdots$ for $(r', s') = (1, 0)$, and $\frac{1}{12} - 2q^{\frac{1}{2}} + \cdots$ for $(r', s') = (1, 1)$, and $\frac{1}{12} - \frac{1}{4}$ for $(r', s') = (0, 1)$.

From these with $r' = 0$ we get constant terms $-\frac{1}{4}$ if $r \geq 1$ and

$$-\frac{1}{4} - \frac{\zeta_n^s}{(1-\zeta_n^s)^2} \;=\; -\frac{(1+\zeta_n^s)^2}{4(1-\zeta_n^s)^2}$$

if $r = 0$. Taking the product over (r, s) using (2.3.10) and (2.3.11) gives $n^{-2}2^{-2(n^2-1)}$.

Another constant term arises from $r' = 1$ and $r = 0$, namely $-\frac{\zeta_n^s}{(1-\zeta_n^s)^2}$, and taking the product over s', s gives an additional $(n^{-2})^2$; thus so far we have a constant term

$$(n^{-2})^3 2^{-2(n^2-1)} \tag{2.5.2}$$

which partly cancels with one of the outside factors in (2.5.1).

There remain the terms with $r' = 1$ and $r \geq 1$, which give

$$(-1)^{s'} 2q^{\frac{1}{2}} - q^{\frac{r}{n}}\zeta_n^s - q^{\frac{n-r}{n}}\zeta_n^{-s} + \cdots. \tag{2.5.3}$$

As n is odd the leading term here has coefficient $-\zeta_n^{\pm s}$ with $\pm$ independent of s. Now $\prod_{s=0}^{n-1} \zeta_n^s = 1$ so this kills the root of unity; and the minus sign is killed by the two values of s'. Thus taking the product yields just 1 for the coefficient, and together with (2.5.2) we find $\mathrm{res}(C, B_n) = (2\pi i)^{6(n^2-1)} 2^{-2(n^2-1)} q^{l_n^*} + \cdots$. Comparing with Lemma 2.1 and using again transcendence we conclude $l_n^* = l_n = \frac{n^2-1}{2}$ and $d_n = 1$ as required.

Now for n even. This time we have

$$\mathrm{res}(C, B_n/C) \;=\; (2\pi i)^{6(n^2-4)}(n^2)^3 \prod_{(r,s)\in\mathcal{C}_n^*} \prod_{(r',s')\in\mathcal{C}_2} f(r', s', r, s),$$

with f as above, where now $\mathcal{C}_n^*$ is $\mathcal{C}_n$ as in (2.3.4) but without $(r, s) = (\frac{n}{2}, 0), (0, \frac{n}{2}), (\frac{n}{2}, \frac{n}{2})$ corresponding to points of order 2.

As above with $r' = 0$ we get constant terms $-\frac{1}{4}$ if $r \geq 1$ and

$$-\frac{1}{4} - \frac{\zeta_n^s}{(1-\zeta_n^s)^2} \;=\; -\frac{(1+\zeta_n^s)^2}{4(1-\zeta_n^s)^2}$$

if $r = 0$. Taking the product over (r, s) using (2.3.10) and now (2.3.12) gives $2^{-2(n^2-4)}$.

Another constant term arises from $r' = 1$ and $r = 0$, namely $-\frac{\zeta_n^s}{(1-\zeta_n^s)^2}$, and taking the product over s', s gives an additional $16(n^{-2})^2$; thus so far we have a constant term

$$(n^{-2})^2 2^{-2(n^2-6)}. \tag{2.5.4}$$

There remain the terms with $r' = 1$ and $r \geq 1$, which give again (2.5.3). Now n is even. If $r \neq \frac{n}{2}$ then the leading term here has coefficient $-\zeta_n^{\pm s}$ with $\pm$ independent of s. Now $\prod_{s=0}^{n-1} \zeta_n^s = -1$ so this kills the root of unity; and the two minus signs are killed by the two values of s'. Thus taking the product yields just 1 for the coefficient. But if $r = \frac{n}{2}$ then we get three leading terms with a coefficient $(-1)^{s'}2 - \zeta_n^s - \zeta_n^{-s}$. This is $(1-\zeta_n^s)(1-\zeta_n^{-s})$ for $s' = 0$ and $-(1+\zeta_n^s)(1+\zeta_n^{-s})$ for $s' = 1$. Taking the product using (2.3.10) and (2.3.12) yields $(\frac{n}{2})^4$ for the coefficient.

So together with (2.5.4) we find $\mathrm{res}(C, B_n/C) = (2\pi i)^{6(n^2-4)} 2^{-2(n^2-4)} n^6 q^{l_n^*}$. Comparing with Lemma 2.1 and using again transcendence we conclude $l_n^* = l_n = \frac{n^2-4}{2}$ and $d_n = n^6$ as required. □

2.6 Proof of Theorem 2

We start by expressing $A_n = A_n(x)$ in terms of $B_n = B_n(x)$ and its derivatives.

Lemma 2.5. *For all natural numbers n we have*

$$n^2 A_n B_n \;=\; n^2 x B_n^2 - B_n B_n' C' - 2(B_n B_n'' - B_n'^2)C.$$

Proof. Again it is enough to prove this over the complex numbers; indeed in view of the coefficients n^2 it may not be so useful in positive characteristic (even though it is true there). There we have the Weierstrass σ-function $\sigma(z) = \sigma(z;\tau)$. It is well-known (see for example [F, p.184]) that

$$\frac{\sigma(nz)}{\sigma(z)^{n^2}} = \psi_n(\wp(z), \wp'(z)),$$

where the square of the right-hand side is $B_n(\wp(z))$. So squaring, then logarithmically differentiating to get the Weierstrass ζ-function, then again differentiating to involve $\wp(nz) = \frac{A_n(\wp(z))}{B_n(\wp(z))}$ we end up after a short calculation with the desired result after writing $x = \wp(z)$. □

We will now prove Theorem 2 for n odd. Substituting $B_n = B_n^{*2}$ in Lemma 2.5 we obtain $n^2A_n = A + \tilde{A}$ for $\tilde{A} = 4(B_n^*)'^2C$ and a polynomial A of degree at most n^2 and divisible by B_n^*. Also $\tilde{A}$ has the same degree n^2 as n^2A_n. So taking the resultant of both sides with B_n and using (2.2.3) we get

$$(n^2)^{n^2-1}\mathrm{res}(A_n, B_n) = \mathrm{res}(n^2A_n, B_n) = \mathrm{res}(\tilde{A}, B_n) = 4^{n^2-1}\mathrm{res}((B_n^*)'^2C, B_n)$$

because B_n^* vanishes at the zeroes of B_n. Using multiplicativity we see that the last resultant is

$$\mathrm{res}(C, B_n)\mathrm{res}((B_n^*)', B_n^*)^4 \ = \ \mathrm{res}(C, B_n)(n \text{ disc } B_n^*)^4$$

because the leading coefficient of B_n^* is ±n. Finally substituting in our values from Theorem 1 and Lemma 2.4 we end up with

$$(\text{disc } B_n^*)^4 = (n^2)^{n^2-3}(16\Delta)^{\frac{(n^2-1)(n^2-3)}{6}}.$$

The required result follows up to an unspecified sign from this by taking fourth roots and using Lemma 2.1. The sign of the discriminant will be determined below.

Now for n even, it is convenient to substitute $B_n = CB_n^{**2}$ in Lemma 2.5, where $B_n^{**} = B_n^*/C$. We obtain $n^2A_n = A + \tilde{A}$ for

$$\tilde{A} = C'^2B_n^{**2} + 4C^2(B_n^{**})'^2$$

and a polynomial A of degree at most n^2 and as before divisible by $B_n^* = CB_n^{**}$. Also $\tilde{A}$ has the same degree n^2 as n^2A_n. Taking the resultant of both sides with B_n we get as above

$$(n^2)^{n^2-1}\mathrm{res}(A_n, B_n) = \mathrm{res}(\tilde{A}, B_n) = \mathrm{res}(\tilde{A}, C)\mathrm{res}(\tilde{A}, B_n^{**2}) \qquad (2.6.1)$$

because B_n^* still vanishes at the zeroes of B_n.

Now we evaluate each resultant on the right-hand side of (2.6.1).

First $C'^2 B_n^{**2}$ also has degree n^2 and so

$$\mathrm{res}(\tilde{A}, C) = \mathrm{res}(C'^2 B_n^{**2}, C) = \mathrm{res}(C', C)^2 \mathrm{res}(B_n^{**2}, C) = n^6 \Delta^{\frac{n^2}{2}} \tag{2.6.2}$$

by Lemma 2.4.

Similarly

$$\mathrm{res}(\tilde{A}, B_n^{**2}) = \mathrm{res}(4C^2 (B_n^{**})'^2, B_n^{**2}) = 4^{n^2-4} \mathrm{res}(C, B_n^{**2})^2 (n\mathcal{D})^4 = 4^{n^2-4} n^{16} \Delta^{n^2-4} \mathcal{D}^4 \tag{2.6.3}$$

again by Lemma 2.4, where $\mathcal{D} = \mathrm{disc}\ B_n^{**}$. However we are aiming at

$$\mathrm{disc}\ B_n^* = (-1)^{\frac{n}{2}} n^{-1} \mathrm{res}(C B_n^{**}, C' B_n^{**} + C(B_n^{**})') \tag{2.6.4}$$

which by multiplicativity and (2.2.3) is

$$(-1)^{\frac{n}{2}} n^{-1} \mathrm{res}(C, C' B_n^{**}) \mathrm{res}(B_n^{**}, C(B_n^{**})') \;=\; \Delta\ \mathrm{res}(C, B_n^{**2}) \mathcal{D} \;=\; n^6 \Delta^{\frac{n^2-2}{2}} \mathcal{D} \tag{2.6.5}$$

once again by Lemma 2.4. Now combining this with Theorem 1 and (2.6.1),(2.6.2) and (2.6.3) we end up with

$$(\mathrm{disc}\ B_n^*)^4 = n^{2n^2} 2^{-4(n^2-2)} (16\Delta)^{\frac{n^2(n^2+2)}{6}}. \tag{2.6.6}$$

Again taking fourth roots we complete the proof of Theorem 2 up to an undetermined sign.
We see that from (2.6.5),(2.6.6) and (2.6.4) follows that

$$\mathcal{D} = \pm n^{\frac{n^2}{2}-6} 2^{n^2-2} (16\Delta)^{\frac{(n^2-4)(n^2-6)}{24}}.$$

We could determine the sign of the discriminant by using Fourier expansions similar as for the resultant but a referee of [Sc] pointed out the possibility for the following simpler proof.

In order to determine the sign for the discriminant we choose τ imaginary (thus 1 and τ generate a rectangular lattice) and specialize to $a(\tau), b(\tau)$. From the general theory of elliptic curves over the real numbers [KK, p.37] follows that $a, b \in \mathbb{R}$ and $\Delta(a, b) > 0$. Also for a polynomial $B = b_0 \prod_{i=1}^{d} (X - \alpha_i)$ the discriminant of B is given by $\mathrm{disc}\ B = (-1)^{\frac{d(d-1)}{2}} b_0^{2d-2} \prod_{i \neq j} (\alpha_i - \alpha_j)$. If B is defined over $\mathbb{R}$ and square free the discriminant is a non zero real number and if we denote by r the number of (distinct) real roots of B we get the following formula for its sign

$$\operatorname{sign}(\operatorname{disc} B) = (-1)^{\frac{d(d-1)+r(r-1)}{2}}. \tag{2.6.7}$$

Now from the same theory as above follows that $\wp(\frac{r\tau+s}{n}), (r,s) \in \mathcal{C}_n$, is real if and only if either of r or s is equal to 0 or $\frac{n}{2}$. We know that $\wp(\frac{r\tau+s}{n}) = \wp(\frac{r'\tau+s'}{n})$ is equivalent to $r = n - r', s = n - s'$ if (r', s') also lies in $\mathcal{C}_n$.

We deduce that B_n has exactly $n-1$ distinct real roots if n is odd and $2n-1$ if n is even. Since the degree of B_n^* is $\frac{n^2-1}{2}$ if n is odd and $\frac{n^2+2}{2}$ if n is even it follows from (2.6.7) that sign(disc B_n^*) is equal to $(-1)^{\frac{n-1}{2}}$ if n is odd and $(-1)^{\frac{n-2}{2}}$ if n is even. This then concludes the proof of Theorem 2.

We remark that we checked all results appearing in this article with Mathematica for small n. Further it seems that the conjecture as stated in [BuHu, p.31] is wrong. In order to compare the conjecture with our result we notice that the authors study the discriminant of f_n with $f_n = B_n^{**}/2$ (n even) and from (2.2.2) we deduce disc $f_n = 2^{-n^2+6}\mathcal{D}$ while by (2.6.5) $\mathcal{D}$ has the same sign as disc B_n^*. We see however that the error lies just in the determination of the sign for n even.

2.7 Weierstrass and Legendre curves

The first of these is defined by the equation $y^2 = 4x^3 - g_2x - g_3$. Now defining $A_n^W = A_n^W(x)$, $B_n^W = B_n^W(x)$ again with respect to the action of multiplication by n on the x-coordinate, so that

$$\wp(nz) = \frac{A_n^W(\wp(z))}{B_n^W(\wp(z))}$$

for the corresponding Weierstrass function, and again normalizing the numerator to be monic, we have no change except for the substitution of the form (2.3.1). Thus we find the even simpler form

$$\operatorname{res}(A_n^W, B_n^W) = (g_2^3 - 27g_3^2)^{\frac{n^2(n^2-1)}{6}}.$$

And with

$$B_n^W = B_n^{W*2} \quad (n \text{ odd})$$
$$B_n^W = 4B_n^{W*2}/(4x^3 - g_2x - g_3) \quad (n \text{ even})$$

we find

$$\begin{aligned}\text{disc } B_n^{W*} &= (-1)^{\frac{n-1}{2}} n^{\frac{n^2-3}{2}} (g_2^3 - 27g_3^2)^{\frac{(n^2-1)(n^2-3)}{24}} \quad (n \text{ odd}),\\ \text{disc } B_n^{W*} &= (-1)^{\frac{n-2}{2}} n^{\frac{n^2}{2}} 2^{-(n^2-2)} (g_2^3 - 27g_3^2)^{\frac{n^2(n^2+2)}{24}} \quad (n \text{ even}).\end{aligned}$$

The Legendre curve is defined by the equation $y^2 = x(x-1)(x-\lambda)$. Now defining $A_n^L = A_n^L(x)$, $B_n^L = B_n^L(x)$ with respect to the action of multiplication by n on the x-coordinate, and again normalizing the numerator to be monic, we have

$$A_n^L(x) = A_n(x + \frac{1}{3}(\lambda+1)), \quad B_n^L(x) = B_n(x + \frac{1}{3}(\lambda+1)) \tag{2.7.1}$$

and the substitution

$$a = -\frac{1}{3}(\lambda^2 - \lambda + 1), \quad b = -\frac{1}{27}(\lambda-2)(\lambda+1)(2\lambda-1)$$

(see [MZ3] for more about these polynomials). We find

$$\text{res}(A_n^L, B_n^L) = (4\lambda(\lambda-1))^{\frac{n^2(n^2-1)}{3}}.$$

And finally with

$$B_n^L = B_n^{L*2} \quad (n \text{ odd})$$
$$B_n^L = B_n^{L*2}/(x(x-1)(x-\lambda)) \quad (n \text{ even})$$

we find

$$\begin{aligned}\text{disc } B_n^{L*} &= (-1)^{\frac{n-1}{2}} n^{\frac{n^2-3}{2}} (4\lambda(\lambda-1))^{\frac{(n^2-1)(n^2-3)}{12}} \quad (n \text{ odd}),\\ \text{disc } B_n^{L*} &= (-1)^{\frac{n-2}{2}} n^{\frac{n^2}{2}} 2^{-(n^2-2)} (4\lambda(\lambda-1))^{\frac{n^2(n^2+2)}{12}} \quad (n \text{ even}).\end{aligned}$$

2.8 Tate form

We saw that the Tate form is given by (2.1.9). This can be reduced to $y^2 = x^3 + ax + b$ as in [Si2, p.46,48] with $a = -27c_4, b = -54c_6$ both complicated polynomials in $\mathcal{R} = \mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$; here the old variables are expressed in terms of the new as

$$36x + 3b_2, 216y + 108a_1x + 108a_3 \tag{2.8.1}$$

respectively, for some b_2 in $\mathcal{R}$. Thus multiplication by n on x is still given by polynomials $A_n^T = A_n^T(x), B_n^T = B_n^T(x)$, and again normalizing the numerator to become monic we find

$$A_n^T(x) = 36^{-n^2}(A_n(36x+3b_2) - 3b_2B_n(36x+3b_2)), \quad B_n^T(x) = 36^{-n^2+1}B_n(36x+3b_2), \tag{2.8.2}$$

the latter also looking like $n^2x^{n^2-1} + \cdots$.

Taking into account the various appearances of 36, and using another property of resultants (see for example Exercise 2.7(a) of [Si4, p.75] with $\beta = \gamma = 0, \delta = 1$) we find the nice form

$$\text{res}(A_n^T, B_n^T) = (\Delta^T)^{\kappa_n}, \tag{2.8.3}$$

where $\Delta^T = \frac{1}{1728}(c_4^3 - c_6^2)$, by definition the discriminant of (2.1.9), is an even more complicated polynomial still in $\mathcal{R}$ (with 26 terms). Similarly with

$$B_n^T = B_n^{T*2} \quad (n \text{ odd})$$

$$B_n^T = 4B_n^{T*2}/B_2^T \quad (n \text{ even})$$

for $B_2^T = 4x^3 + b_2x^2 + 2b_4x + b_6$ and the standard b_4, b_6 in $\mathcal{R}$ [Si2, p.59] we find

$$\text{disc } B_n^{T*} \;=\; (-1)^{\frac{n-1}{2}} n^{\frac{n^2-3}{2}} (\Delta^T)^{\frac{(n^2-1)(n^2-3)}{12}} \quad (n \text{ odd}),$$

$$\text{disc } B_n^{T*} \;=\; (-1)^{\frac{n-2}{2}} n^{\frac{n^2}{2}} 2^{-(n^2-2)} (\Delta^T)^{\frac{n^2(n^2+2)}{12}} \quad (n \text{ even}).$$

Now (2.8.3) has an application in good reduction, but we must first pause to prove that $A_n^T(x), B_n^T(x)$ lie in $\mathcal{R}[x]$. This seems not to be explicitly in the literature, even though it is known to the experts; indeed from (2.8.2) it looks unlikely at first sight. But Tate pointed out that it follows from Proposition 4 of his paper [MT, p.681] with Mazur. Here we supply a slightly more direct proof.

Again by [Si2, p.59] we have $A_2^T = x^4 - b_4x^2 - 2b_6x - b_8$ for the standard b_8 in $\mathcal{R}$. We can then proceed by induction using the relations in [Si2, p.216]. These imply for $n \geq 2$ that

$$x_{n-1} + x_{n+1} = S(x, x_n), \quad x_{n-1}x_{n+1} = P(x, x_n),$$

where $x_m = x(mQ)$ for the generic point $Q = (x, y)$ on $y^2 = x^3 + ax + b$ and

$$S(x,z) = \frac{2(x+z)(a+xz)+4b}{(x+z)^2 - 4xz}, \quad P(x,z) = \frac{(xz-a)^2 - 4b(x+z)}{(x+z)^2 - 4xz}.$$

We make the change of variables as in (2.8.1) to land on (2.1.9) and solve for the new x_{n-1}, x_{n+1} to find

$$x_{n-1} + x_{n+1} = S^T(x, x_n), \quad x_{n-1}x_{n+1} = P^T(x, x_n)$$

with

$$S^T(x,z) \;=\; \frac{1}{36}S(36x+3b_2,36z+3b_2)-\frac{1}{6}b_2$$

$$P^T(x,z) \;=\; \frac{1}{1296}P(36x+3b_2,36z+3b_2)-\frac{1}{432}b_2S(36x+3b_2,36z+3b_2)+\frac{1}{144}b_2^2.$$

Now setting

$$x_m=\frac{A_m^T}{B_m^T}=\frac{x^{m^2}+\cdots}{m^2x^{m^2-1}+\cdots}$$

and comparing the resulting denominator and numerator we obtain

$$B_{n-1}^TB_{n+1}^T=(A_n^T-xB_n^T)^2$$

and similarly (with mild surprise at the disappearance of the denominators) that

$$A_{n-1}^TB_{n+1}^T+A_{n+1}^TB_{n-1}^T,\quad A_{n-1}^TA_{n+1}^T$$

lie in $\mathcal{R}[x,A_n^T,B_n^T]$.

As A_{n-1}^T is monic, the second above shows that if A_{n-1}^T,A_n^T,B_n^T are over $\mathcal{R}$ then so is A_{n+1}^T; and then the first does the same for B_{n+1}^T. This suffices for the induction step.

Incidentally a similar argument shows that for the Legendre model both $A_n^L(x),B_n^L(x)$ lie in $\mathbb{Z}[x,\lambda]$ as mentioned in [MZ3]; this is not directly clear from (2.7.1) because of the denominator 3.

At this point we interrupt to indicate how to prove Theorem 1 up to sign starting only from $\mathrm{res}(A_n,B_n)=c_n\Delta^{\kappa_n}$ as in section 2.2 with $k_n=\kappa_n$ and c_n composed at most of primes 2,3. As above we deduce only

$$\mathrm{res}(A_n^T,B_n^T)=16^{-\kappa_n}c_n(\Delta^T)^{\kappa_n}, \tag{2.8.4}$$

in place of (2.8.3). Now it is a fact that Δ^T is a primitive polynomial; in fact 5 of the 26 terms have coefficient ±1. It follows that $c_n=16^{\kappa_n}c_n^T$ for c_n^T also in $\mathbb{Z}$. If 2 or 3 divides c_n^T then we look at $y^2+y=x^3-x$ over $\mathbb{F}_2$ or $\mathbb{F}_3$ with $\Delta^T=-37$, and then (2.8.4) would imply $\mathrm{res}(A_n^T,B_n^T)=0$ again contradicting coprimality.

In connection with Appendix B we make a remark about translation by a point $P=(\xi,\eta)$ of order 2. Here

$$B_2^T(\xi)=4\xi^3+b_2\xi^2+2b_4\xi+b_6=0. \tag{2.8.5}$$

From [Si2, p.59] we find that x becomes

$$\frac{A_P^T(x)}{B_P^T(x)}=\xi-\frac{\delta}{x-\xi}$$

with $\delta = a_1\eta - 3\xi^2 - 2a_2\xi - a_4$ (here $2\eta + a_1\xi + a_3 = 0$). But now there seems to be no obvious way to normalize A_P^T, B_P^T; for example ξ is probably not in the integral closure of $\mathcal{R}$. However from (2.8.5) we see that 4ξ (as well as b_6/ξ if $\xi \neq 0$) is; and if we take

$$A_P^T(x) = 4(\xi x - \xi^2 - \delta), \quad B_P^T(x) = 4(x - \xi)$$

then we also find that even $2(\xi^2 + \delta)$, which is $-4\xi^2 - b_2\xi - b_4$ or $b_4 + \frac{b_6}{\xi}$, is in the closure.

Then $\rho = \mathrm{res}(A_P^T, B_P^T)$ satisfies

$$\rho^3 + c_4\rho^2 + 256\Delta^T = 0. \tag{2.8.6}$$

This is not so nice in characteristic 2, and over $\mathbb{F}_2[a_1, a_2, a_3, a_4, a_6]$ we should normalize differently. Then $a_1 \neq 0$ otherwise we are in the supersingular case and P does not exist, and with

$$A_P^T(x) = a_1(\xi x - \xi^2 - \delta), \quad B_P^T(x) = a_1(x - \xi)$$

we get $a_1\xi = a_3$ and $a_1(\xi^2+\delta)$ the square root of $a_1(a_3^3+a_1a_2a_3^2+a_1a_4^2+a_1^2a_3a_4+a_1^3a_6)$ in the closure; and simply

$$\rho^2 = \Delta^T. \tag{2.8.7}$$

In fact, all is much nicer for Legendre when the three $\frac{A_P^L(x)}{B_P^L(x)}$ are

$$\frac{\lambda}{x}, \quad \frac{x-\lambda}{x-1}, \quad \lambda\frac{x-1}{x-\lambda}.$$

3 Relative Manin-Mumford in additive extensions

In recent papers Masser and Zannier have proved various results of “relative Manin-Mumford” type for various families of abelian varieties, some with field of definition restricted to the algebraic numbers. Typically these imply the finiteness of the set of torsion points on a curve in the family. After Bertrand discovered some counterexamples for multiplicative extensions of elliptic families, the three authors together with Pillay settled completely the situation for this case over the algebraic numbers. Here we treat the last remaining case of surfaces, that of additive extensions of elliptic families, and even over the field of all complex numbers. In particular analogous counterexamples do not exist. There are finiteness consequences for Pell’s equation over polynomial rings and integration in elementary terms. Our work can be made effective because we use counting results only for analytic curves.

3.1 Introduction

The following has motivated much recent work.

Problem. *Let $\mathcal{S}$ be a semiabelian scheme over a variety defined over $\mathbb{C}$, 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 the conjecture stated by Pink [Pin] in 2005, which generalized the Zilber conjectures [Zil] to schemes.

In [MZ1] Masser and Zannier verified the above statement in a special case where $\mathcal{S}$ 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 $\lambda \neq 0, 1$ such that the points

$$(2, \sqrt{4-2\lambda}),\ (3, \sqrt{18-6\lambda}) \tag{3.1.1}$$

both have finite order on the elliptic curve E_λ defined by

$$Y^2 = X(X-1)(X-\lambda).$$

In [MZ2] they generalized this to any pair of points defined over an algebraic closure of $\mathbb{C}(\lambda)$. It turns out that this is equivalent to the problem above with $\mathcal{S}$ isogenous to the product of two isogenous elliptic schemes and $\mathcal{V}$ a curve. In [MZ3] they obtained some more precise information when the X-coordinates (abscissae) happen to be in $\mathbb{C}$. And in [MZ4] they settled the case of two non-isogenous elliptic schemes.

Then in [MZ5] they dealt with $\mathcal{S}$ isogenous to a simple abelian surface scheme and $\mathcal{V}$ a curve; but with the restriction that $\mathcal{S}, \mathcal{V}$ are defined over an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. So with this restriction the above problem is settled for abelian surface schemes whether simple or not.

While investigating the problem for schemes that are not abelian, Bertrand [B2] discovered a surprising counterexample. This concerned schemes of multiplicative extensions of elliptic curves. The example was of a somewhat special nature involving the so-called 'Ribet curves'. In [BMPZ] Bertrand, Masser, Pillay and Zannier were able to show that there are essentially no other counterexamples for multiplicative extensions of elliptic curves, subject to the above restriction of field of definition. This settles the situation for all semiabelian surface schemes over $\overline{\mathbb{Q}}$.

Now there may be no good reason for confining all these considerations to semiabelian. For example, the finiteness of the set of complex numbers λ such that the points

$$(2\lambda, \sqrt{2\lambda(2\lambda-1)(2\lambda-4)}),\ (3\lambda, \sqrt{3\lambda(3\lambda-1)(3\lambda-4)}) \tag{3.1.2}$$

both have finite order on the elliptic curve E defined by $Y^2 = X(X-1)(X-4)$ is an easy consequence of the Manin-Mumford conjecture for $E \times E$, and this was generalized to any commutative group variety, semiabelian or not, by [Hi].

Up to isomorphism there are exactly three group schemes of relative dimension 2 $\mathcal{S}$ which are not semiabelian. These are $\mathbb{G}_a \times \mathbb{G}_a, \mathbb{G}_a \times \mathbb{G}_m$, and an additive extension $\mathcal{G}$ of an elliptic scheme $\mathcal{E}$ with

$$0 \longrightarrow \mathbb{G}_a \longrightarrow \mathcal{G} \longrightarrow \mathcal{E} \longrightarrow 0. \tag{3.1.3}$$

The first two are constant and so covered by [Hi]. In this section we treat the remaining one for curves $\mathcal{V}$. It turns out that there are no counterexamples as for multiplicative extensions. Together with the work described above, this settles the situation for all surface schemes defined over $\overline{\mathbb{Q}}$. But in fact we can handle the additive case over the full $\mathbb{C}$. Thus our main result is as follows.

Theorem 3. *Let $\mathcal{G}$ be an additive extension by $\mathbb{G}_a$ of an elliptic scheme $\mathcal{E}$ over a variety defined over $\mathbb{C}$, and denote by $\mathcal{G}^{[c]}$ the union of its flat subgroup schemes 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 subgroup schemes of $\mathcal{G}$ of positive codimension.*

We will see at the beginning of section 3.3 that the base variety can be assumed to be irreducible of dimension at most one. In case it is a point, $\mathcal{G}$ is constant and we see the classical result of Manin-Mumford type (as given in [Hi]) in the special situation under consideration. It also applies when $\mathcal{E}$ is isoconstant (isomorphic to a constant family). In fact we will appeal to the classical result to eliminate those cases.

We give a brief description of the subgroup schemes of $\mathcal{G}$ over an irreducible base curve $\mathcal{B}$. The flat subgroup schemes (see [Hab, subsection 2.4] for the abelian case) of $\mathcal{G}$ arise from algebraic subgroups of the generic fibre. So if $\mathcal{G}$ is not split the flat subgroup schemes of codimension 1 are all isogenous to $\mathbb{G}_a \times \mathcal{B}$. But if $\mathcal{G}$ is split there is in addition the subgroup scheme $0 \times \mathcal{E}$. The flat subgroup schemes of codimension 2 consist of unions of torsion sections. A typical subgroup scheme that is not flat is the union of the identity section with an algebraic subgroup of one fibre (and finite unions of those). These are either contained in a flat subgroup scheme of positive codimension, or are elliptic curves in a split fibre of a non-split $\mathcal{G}$. The latter ones occur only for finitely many fibres and for all practical purposes we may disregard the non-flat subgroup schemes in our discussion.

In the rest of this chapter as well as Appendix A all subgroup schemes that appear are assumed to be flat unless explicitly stated otherwise.

We will show in section 3.14 that if $\mathcal{G}$ is not split and the projection of $\mathcal{V}$ to the base $\mathcal{B}$ is dominant then $\mathcal{V} \cap \mathcal{G}^{[2]}$ is even contained in a finite union of subgroup schemes of codimension 2. For the image $\mathcal{V}$ of a section $s : \mathcal{B} \to \mathcal{G}$ this implies for such $\mathcal{G}$, that the intersection of $\mathcal{V}$ with the union of all torsion sections of $\mathcal{G}$ is infinite if and only if s is a torsion section. If $\mathcal{G}$ is split then we must add the possibility that $\mathcal{V}$ lies in $0 \times \mathcal{E}$ and the intersection of $\mathcal{V}$ with all torsion sections is usually infinite but sparse (see for example [MZ1, p.1677]).

We give some examples of our theorem for base curves.

As we shall see in section 3.2, a typical $\mathcal{G}$ has an affine part in $\mathbb{A}^5$, with coordinates (X, Y, U, V, λ), defined by equations

$$Y^2 = X(X-1)(X-\lambda), \ V - YU = X^2 \tag{3.1.4}$$

and with the obvious projection, call it π, to E_λ. Here we removed the kernel of π. Since the kernel does not contain any non-zero torsion points it is enough to consider the above affine part. The group law is not so easily written down, but we give an analytic description later. We may also refer to this $\mathcal{G}$ as G_λ, to indicate the fibres over the base $\mathcal{B} = \mathbb{A} \setminus \{0, 1\}$. Here one may consult the article [CMZ] of Corvaja, Masser, Zannier (in particular equation (3.6) on p.245 for the projective Weierstrass model).

Thus we get the finiteness of the set of complex numbers $\lambda \neq 0, 1$ such that the point

$$(2,\ \sqrt{4-2\lambda},\ 3,\ 3\sqrt{4-2\lambda}+4) \tag{3.1.5}$$

has finite order on G_λ (compare with (3.1.1) above). Or the complex numbers $\lambda \neq 0, 1$ such that

$$(2,\ \sqrt{4-2\lambda},\ \pi,\ \pi\sqrt{4-2\lambda}+4) \tag{3.1.6}$$

has finite order on G_λ. We also get finiteness for the set of complex $\lambda \neq 0, 1$ such that

$$(2,\ \sqrt{4-2\lambda},\ 0,\ 4) \tag{3.1.7}$$

is torsion on G_λ. We will show in Appendix A that this implies that there are at most finitely many λ such that

$$\int \frac{dX}{(X-2)\sqrt{X(X-1)(X-\lambda)}} \tag{3.1.8}$$

is integrable in elementary terms (see [MZ6] or [Ri] for the definition). This is consistent with a claim of Davenport. In [MZ6] Masser and Zannier have formulated this claim more precisely: the fundamental object is a differential on a curve defined over the function field $\mathbb{C}(C)$ of another curve C itself defined over $\mathbb{C}$. They proved the claim when the field $\mathbb{C}$ is replaced by $\overline{\mathbb{Q}}$. Our Theorem implies Davenport's Claim for any elliptic curve defined over $\mathbb{C}(C)$ but not $\mathbb{C}$. For example with

$$\int \frac{dX}{(X-2)\sqrt{X^3+X+\lambda}},\ \int \frac{dX}{(X-\pi)\sqrt{X^3+X+\lambda}}.$$

Another type of example is

$$(-1,\ \sqrt{-2-2\lambda},\ 0,\ 1); \tag{3.1.9}$$

we shall show in a future paper that this implies that there are at most finitely many λ such that there exist A and $B \neq 0$ in $\mathbb{C}[X]$ with

$$A^2 - X^3(X-1)(2X-1)((\lambda+1)X-1)B^2 = 1.$$

This property has been studied by Masser and Zannier [MZ5]; see also Zannier's article [Za2], where now the fundamental object is a polynomial D in $\mathbb{C}(C)[X]$, which is called Pellian if there exist A and $B \neq 0$ in $\overline{\mathbb{C}(C)}[X]$ with $A^2 - DB^2 = 1$. Similarly with $\mathbb{C}(C)$ replaced with $\mathbb{C}$. At the moment there is no satisfactory conjecture completely analogous to Davenport's Claim; a naive version would already be false for most quartic D such as $X(X^3 + X + \lambda)$. But our Theorem allows the full investigation of families of sextic D with a cubed factor. For example in Appendix A we prove that there are at most finitely many complex λ such that

$$X^3(X^3 + X + \lambda)$$

is Pellian and the proof translates without difficulties to

$$(X-\pi)^3(X^3 + X + \lambda).$$

It is interesting to note here that the presence of squared factors, for example as in $X^2(X^4 + X + \lambda)$ treated in [BMPZ], leads to multiplicative extensions of elliptic curves. As shown by Bertrand in [B3, p.20, Corollary 3] the counterexamples to relative Manin-Mumford given in [B2] also lead to counterexamples of a Pell analogue of Davenport's Claim. We also refer to section 4.2 of Appendix A for an exhibition of some counterexamples.

In all the examples (3.1.5), (3.1.6), (3.1.7), (3.1.9) it can be checked that $\mathcal{V}$ (the image of the corresponding sections) does not lie in $\mathcal{G}^{[1]}$; thus it has zero-dimensional intersection with any subgroup scheme of positive dimension, leading to finiteness statements. To do this checking we remark that the extension is non-split (see for example [CMZ, p.244]), and so the only such connected subgroup scheme is $\mathbb{G}_a$ inside G_λ, which is obtained by homogenizing (3.1.4) with coordinates $(Z_0, X_0, Y_0, U_0, V_0)$ and taking $(0, 0, 1, 0, v_0)$ (one of the two lines at infinity). This is the set of P with $\pi(P) = O$; and similarly any such subgroup scheme, not necessarily connected, is contained in one defined by $q\pi(P) = O$ for some positive integer q. For $P = P_\lambda$ defined by (3.1.5), (3.1.6), (3.1.7) it was already verified in [MZ1, p.1677] that $\pi(P_\lambda) = (2, \sqrt{4-2\lambda})$ is not identically torsion, for example by specializing to $\lambda = -6$; and a similar argument works for (3.1.9) at $\lambda = -9$.

Our proof follows the general strategy of Masser and Zannier, especially [MZ2] but also with elements from [MZ3]. The main case is when $\mathcal{G}$ is non-split and $\mathcal{V}$ is defined over $\overline{\mathbb{Q}}$. Then in the context of Legendre elliptic curves, this amounts to the study of the equations

$$z = xf + yg, \ w = -xk - yl \tag{3.1.10}$$

where (z, w) are group logarithms of points P_λ like (3.1.5), (3.1.6), (3.1.7) or (3.1.9), f, g are basis elements of the period lattice of E_λ, and k, l are corresponding quasi-periods. Here z, f, g are as in [MZ2], but w, k, l represent new features. Our coefficients x, y as defined in (3.8.1) are complex analytic (for example in λ) and their locus S in $\mathbb{C}^2$ is analytic, of complex dimension at most 1. When for some specific λ the point P_λ is torsion, say of order dividing some n, then we get a rational point in $\frac{1}{n}\mathbb{Z}^2$ on S. The work of Bombieri-Pila [BP] is on real analytic curves and so does not directly apply, but a variant of Masser [Mas2] provides for any $\epsilon > 0$ an upper bound for their number, of order at most n^ϵ as n tends to infinity, provided S is transcendental. This presents a new feature as it opens the door for effective refinements of our results. See also subsection 3.11.1 where we indicate how to obtain an effective result for the curve defined by (3.1.7).

Now if it happens that $q\pi(P_\lambda) = O$ for generic λ and a non-zero integer q, then we get a subgroup scheme of codimension 1 as in the Theorem, so there is nothing to prove.

Otherwise we are able to show that indeed S is transcendental; that is, the functions x, y are algebraically independent. This follows from a result of Bertrand [B1] concerning the functions z, w, f, g, l. Here we need to observe that w is closely related to a suitable derivative of z.

We conclude the proof as in [MZ2] by combining Silverman's Specialization Theorem [Si1] with David's result [Davi] on counting conjugates of torsion points, which we first have to extend from E_λ to G_λ. This implies by contrast that the number of rational points is of order at least n^δ for some $\delta > 0$. Comparison of this lower bound with the above upper bound leads to an estimate for n which suffices to prove the Theorem when $\mathcal{G}$ is non-split and $\mathcal{V}$ is defined over $\overline{\mathbb{Q}}$.

When $\mathcal{G}$ is non-split and $\mathcal{V}$ is not defined over $\overline{\mathbb{Q}}$ as in (3.1.6), we may suppose that λ is transcendental over $\mathbb{Q}$. Now the classical theory of Fricke and Weber provides so much Galois information on torsion points that we no longer need the work of [B1], [Mas2], [Si1] or [Davi]. However in the Legendre context we first have to extend also this theory from E_λ to G_λ. Then we are able to use the method of the Appendix of [MZ3] (see also the sketch in [Za1, p.81]). That involved constructing a certain curve $\check{C}$ over $\overline{\mathbb{Q}}(j)$ for the modular invariant j, representing multiplication by a suitable l as an element of some $SL_2(\mathbb{Z}/n\mathbb{Z})$, and intersecting $\check{C}$ and $l\check{C}$ using Bézout. However the details are slightly simpler here because we can use $GL_2(\mathbb{Z}/n\mathbb{Z})$ as in section 10 of [MZ2], or at least something nearly as big.

Finally when $\mathcal{G}$ is split it is $\mathbb{G}_a \times \mathcal{E}$ and the Theorem is easy to prove.

Here is a brief section-by-section account of this chapter.

We start in section 3.2 by explaining how the equations (3.1.4) arise and describing the analysis behind them. Then in section 3.3 we show how to reduce the non-split case to a Proposition over $\mathbb{C}$ involving the special case $\mathcal{G} = G_\lambda$, and in section 3.4 we record our counting result. Our own curve S is constructed from elliptic periods and quasi-periods defined in section 3.5 together with elliptic logarithms and quasi-logarithms defined in section 3.6. The relevant algebraic independence result is then proved in section 3.7, and the curve is defined in section 3.8 and shown there to be transcendental. Then in sections 3.9 and 3.10 we record the consequences of the work of David and Silverman for our purposes, and the proof of the Proposition in the "algebraic case", that is, over $\overline{\mathbb{Q}}$, is completed in section 3.11. We also indicate how to obtain an effective result for the curve given by (3.1.7) in subsection 3.11.1.

Finally, the proof for the transcendental case is done in section 3.12.

Then in section 3.13 we give the very simple proof of the Theorem in the split situation.

And in section 3.14 we return to non-split and show how the Theorem can be slightly strengthened in that situation; namely that $\mathcal{V} \cap \mathcal{G}^{[2]}$ is contained in a finite union of (not necessarily flat) subgroup schemes of $\mathcal{G}$ of codimension at least two.

All the results of this section can be made effective, thanks to the fact that our counting involves only curves, to which zero estimates of a classical form can be applied. Thus based on the arguments of section 3.11.1 we have shown that there are at most

$$\exp(\exp(\exp(\exp(\exp(5)))))$$

different values of λ such that (3.1.8) is integrable in elementary terms. With the counting on surfaces in most of the previous work, the matter is not so clear due to the implicit use of Gabrielov's Theorem (not to mention parametrizations).

We thank David Masser for introducing us into this subject and his involvement in the development of this work. Also we would like to heartily thank Daniel Bertrand for pointing out the differential relation (see section 3.7) between the differential of the first and second kind of an elliptic curve defined over a function field.

3.2 Additive extensions

As we will be using Weierstrass functions, we start with a corresponding curve E whose affine part is defined by $\tilde{Y}^2 = 4\tilde{X}^3 - g_2\tilde{X} - g_3$ and parametrized by the exponential map $\tilde{X} = \wp(z), \tilde{Y} = \wp'(z)$. Any non-split extension of E is isomorphic to the variety G whose affine part is defined in $\mathbb{A}^4$ by

$$\tilde{Y}^2 = 4\tilde{X}^3 - g_2\tilde{X} - g_3,\ \tilde{V} - \tilde{Y}\tilde{U} = 2\tilde{X}^2 \tag{3.2.1}$$

[CMZ, p.245]. The exponential map now sends (z, w) in $\mathbb{C}^2$ to

$$\tilde{X} = \wp(z),\ \tilde{Y} = \wp'(z),\ \tilde{U} = w + \zeta(z),\ \tilde{V} = (w + \zeta(z))\wp'(z) + 2\wp^2(z) \tag{3.2.2}$$

where $\zeta(z)$ is the corresponding zeta function [CMZ, p.251]. Homogenizing the equations leads to a projective variety $\overline{G}$ in $\mathbb{P}_4$, say with coordinates $(\tilde{Z}_0, \tilde{X}_0, \tilde{Y}_0, \tilde{U}_0, \tilde{V}_0)$, and analytically this amounts to multiplying (3.2.2) by the cube of the theta function (note that the last function has poles of order at most three not four). However the parametrization does not cover all of $\overline{G}$ but only that part of G with the line $\tilde{Z}_0 = \tilde{X}_0 = \tilde{Y}_0 = 0$ removed. Then

$$\tilde{\pi}(\tilde{Z}_0, \tilde{X}_0, \tilde{Y}_0, \tilde{U}_0, \tilde{V}_0) = (\tilde{Z}_0, \tilde{X}_0, \tilde{Y}_0)$$

defines a projection $\tilde{\pi}$ from G to E. And

$$\tilde{\phi}(\tilde{v}_0) = (0, 0, 1, 0, \tilde{v}_0) \tag{3.2.3}$$

defines an isomorphism $\tilde{\phi}$ of $\mathbb{G}_a$ to the kernel of $\tilde{\pi}$. So we get an exact sequence

$$0 \longrightarrow \mathbb{G}_a \longrightarrow G \longrightarrow E \longrightarrow 0$$

(compare (3.1.3) above). Finally the group law is given by addition in $\mathbb{C}^2$.

Starting instead with the Legendre form $Y^2 = X(X-1)(X-\lambda)$ we get the Weierstrass form via

$$\tilde{X} = X - \frac{1}{3}(\lambda + 1),\ \tilde{Y} = 2Y$$

and

$$g_2=\frac{4}{3}(\lambda^2-\lambda+1),\ g_3=\frac{4}{27}(\lambda-2)(\lambda+1)(2\lambda-1). \tag{3.2.4}$$

Defining also

$$\tilde{U}=U,\quad \tilde{V}=2V-\frac{4}{3}(\lambda+1)X+\frac{2}{9}(\lambda+1)^2$$

we get (3.1.4) as the analogue of (3.2.1) and

$$X=\wp_\lambda(z)+\frac{1}{3}(\lambda+1),\quad Y=\frac{1}{2}\wp'_\lambda(z), \tag{3.2.5}$$

$$U=w+\zeta_\lambda(z),\quad V=\frac{1}{2}(w+\zeta_\lambda(z))\wp'_\lambda(z)+\left(\wp_\lambda(z)+\frac{1}{3}(\lambda+1)\right)^2 \tag{3.2.6}$$

as the analogue of (3.2.2), where the subscripts denote the restriction to (3.2.4). Homogenizing the equations leads to a projective variety $\overline{G}_\lambda$ in $\mathbb{P}_4$, say with coordinates (Z_0,X_0,Y_0,U_0,V_0) as above, and its part G_λ with the line $Z_0=X_0=Y_0=0$ removed. Then

$$\pi(Z_0,X_0,Y_0,U_0,V_0)=(Z_0,X_0,Y_0) \tag{3.2.7}$$

defines a projection π from G_λ to E_λ. And

$$\phi(v_0)=(0,0,1,0,v_0) \tag{3.2.8}$$

defines an embedding ϕ of $\mathbb{G}_a$ in G_λ. With these maps we get an exact sequence

$$0\longrightarrow\mathbb{G}_a\longrightarrow G_\lambda\longrightarrow E_\lambda\longrightarrow 0. \tag{3.2.9}$$

3.3 Reduction to G_λ

It was shown in section 2 of [MZ2] that the above Problem is isogeny invariant in the following sense. Let $\mathcal{S},\mathcal{S}'$ be semiabelian schemes defined over a variety over $\mathbb{C}$ and suppose that there is an isogeny σ from $\mathcal{S}$ to $\mathcal{S}'$. Then the statement for $\mathcal{S}'$ implies the statement for $\mathcal{S}$.

In fact the same argument works for any commutative group schemes $\mathcal{S},\mathcal{S}'$ semiabelian or not.

Next, also as mentioned in section 2 of [MZ2], if $\mathcal{V}$ is a curve then we can assume that the base variety is irreducible of dimension at most one. Also if $\mathcal{E}$ is isoconstant Theroem 3 is implied by [Hi] and we will assume that this is not the case.

Now for $\mathcal{S} = \mathcal{G}$ we have an exact sequence $0 \to \mathbb{G}_a \to \mathcal{G} \to \mathcal{E} \to 0$ in our Theorem, with a (non-isoconstant) elliptic scheme $\mathcal{E}$. Under the above assumptions about the base variety for the latter, the reduction of $\mathcal{E}$ to Legendre form E_λ leads to $0 \to \mathbb{G}_a \to \mathcal{G} \to E_\lambda \to 0$ (possibly after a finite base-change). Suppose that $\mathcal{G}$ is non-split. Since all non-split extensions are isomorphic as algebraic groups (see for example [CMZ, p.243]), it follows that $\mathcal{G}$ is isomorphic to G_λ above. This provides σ as above (in fact an isomorphism), with $\mathcal{S}' = G_\lambda$ having coordinates now (X, Y, U, V). Let $\mathcal{V}$ be a curve in $\mathcal{S}$. Then $\sigma(\mathcal{V})$ in G_λ is a curve C in the affine space $\mathbb{A}^5$ with coordinates (X, Y, U, V, λ) unless it lies in the kernel of π (so is already contained in a subgroup scheme). We will regard it as being parametrized by $(\xi, \eta, \mu, \nu, \lambda)$ with $\xi, \eta, \mu, \nu, \lambda$ functions in $\mathbb{C}(C)$.

If the point $P = (\xi, \eta, \mu, \nu)$ satisfies $qP = O$ for some non-zero integer q, then the whole of $\sigma(\mathcal{V})$ lies in the corresponding subgroup scheme of codimension 2, so the Theorem is trivial for $\mathcal{S}'$. Thus we are entitled to assume $qP \neq O$ for all such integers.

If only $q\pi(P) = O$, then we will show (in section 3.14) that the Theorem is easy for $\mathcal{S}'$ (also with codimension 2).

So for the moment we will assume that $q\pi(P) \neq O$ as well.

If λ is constant on C, then the base variety can be considered as a point and the Theorem for $\mathcal{S}'$ follows from Manin-Mumford as mentioned in the Introduction.

From all these considerations, we see that our Theorem for non-split $\mathcal{G}$ is implied by the following statement (in conjunction with section 3.14).

Proposition 1. *Let C in $\mathbb{A}^5$ be an irreducible curve defined over $\mathbb{C}$ and parametrized by $(\xi, \eta, \mu, \nu, \lambda)$, with λ non-constant. Suppose that the point*

$$P = (\xi, \eta, \mu, \nu)$$

lies on G_λ and satisfies there

$$q\pi(P) \neq O \tag{3.3.1}$$

for all non-zero integers q. Then there are at most finitely many points $\boldsymbol{c}$ in $C(\mathbb{C})$ such that

$$P(\boldsymbol{c}) = (\xi(\boldsymbol{c}), \eta(\boldsymbol{c}), \mu(\boldsymbol{c}), \nu(\boldsymbol{c}))$$

is of finite order on $G_{\lambda(\boldsymbol{c})}$.

We shall prove this Proposition when C is defined over $\overline{\mathbb{Q}}$ in $\mathbb{C}$, which we refer to as the algebraic case, in the following sections 3.4 to 3.11. Due to the use of Pila's result (not to mention the work of David using transcendence techniques) this can be considered the deepest case. Then in section 3.12 we do the same when C is not defined over $\overline{\mathbb{Q}}$, which we refer to as the transcendental case. This is by comparison less deep.

3.4 Rational points

The analytic curve S in $\mathbb{C}^2$ mentioned in section 3.1 will arise as the locus of certain (f_1, f_2). In this section we record the basic counting result for such curves.

Lemma 3.4.1. *Let D be a closed disc in $\mathbb{C}$ and let $D^\#$ be the closed disc with the same centre and twice the radius. Let f_1, f_2 be algebraically independent functions analytic in a neighbourhood of $D^\#$. Then for every $\epsilon > 0$ there is $C(\epsilon)$ such that for any n in $\mathbb{N}$ there are at most $C(\epsilon)n^\epsilon$ points t in D with $(f_1(t), f_2(t))$ in $\mathbb{Z}^2/n$.*

Proof. First we observe that the closed disc of radius $R > 0$ centred at the origin can be covered by k closed discs of radius $r > 0$, where

$$k \leq 4\left(1 + \frac{\sqrt{2}}{2}\frac{R}{r}\right)^2. \tag{3.4.1}$$

By scaling it suffices to prove this with $r = \sqrt{2}/2$. We inscribe the disc of radius R in a square of side $2R$, which we then cover by unit squares with vertices in $\mathbb{Z}^2$, and finally we cover each unit square by a disc of radius $\sqrt{2}/2$. We can do this with $4l^2$ unit squares provided $l \geq R$; thus we take $l = 1 + [R] \leq 1 + R$ to get

$$k = 4l^2 \leq 4(1 + R)^2 = 4\left(1 + \frac{\sqrt{2}}{2}\frac{R}{r}\right)^2.$$

By translating it suffices to prove the lemma when the centres are at the origin; let R be the radius of D. As implicitly in [Mas2, p.2045] we define for each non-negative integer T the quantity $\gamma(T)$ as the maximum number of t in D such that

$\mathbf{f}(t) = (f_1(t), f_2(t))$ lies on an algebraic curve of degree at most T. Because f_1, f_2 are algebraically independent this is well-known to be finite. Let $M \geq 1$ be such that $\max\{|f_1(t)|, |f_2(t)|\} \leq M$ on $D^\#$. Choose $T \geq \sqrt{8}$ and define A by

$$AR = (4T)^{96/T^2}(M+1)^{16/T}(nM)^{48/T}. \tag{3.4.2}$$

We cover D by k closed discs D_0 of radius $r = (2A)^{-1}$; as $AR \geq 1$ each $D_0^\#$ of twice the radius lies in $D^\#$. Then by Proposition 2 of [Mas2, p.2039] with $d = 1, H = nM$ the number of t in any D_0 with $\mathbf{f}(t)$ in $\mathbb{Z}^2/n$ is at most $\gamma(T)$; note that $f_1(t) = a/n$ for $|a| \leq nM$ and similarly for f_2. Thus by (3.4.1) the total number of such t in D is at most

$$4\gamma(T)\left(1 + \frac{\sqrt{2}}{2}\frac{R}{r}\right)^2 \ \leq \ Cn^{96/T}$$

where C by (3.4.2) depends only on T, R and M. We conclude the proof by taking $T \geq \sqrt{8}$ minimal with $96/T \leq \epsilon$. □

This argument makes the effectivity clear provided we have an upper bound for $\gamma(T)$; but that is of course a “zero estimate”, for which many methods are available. The situation is not so clear when the analytic curve (parametrized by $\mathbf{f}(t)$ as t varies) is replaced by a surface or worse.

3.5 Functions on $\mathbb{C}$

To define the functions f, g, k, l in (3.1.10) we can work on $\mathbb{C}$ (or at least certain subsets) with classical functions. Namely let

$$F(t) \ = \ F\left(\frac{1}{2}, \frac{1}{2}, 1; t\right) \ = \ \sum_{m=0}^{\infty} \frac{(2m)!^2}{2^{4m} m!^4} t^m$$

be a hypergeometric function, convergent for $|t| < 1$. As in [MZ2] this together with $F(1-t)$ will describe the periods of E_t; but for safety we restrict for now to the set Λ defined by $|t| < 1$ and $|1-t| < 1$. Now G_t also has periods, which involve the corresponding quasi-periods of E_t, and to describe these we need also

$$K(t) \ = \ \frac{1}{3}(1-2t)F(t) + 2t(1-t)F'(t). \tag{3.5.1}$$

It is well-known that starting from any point t_0 of Λ we may continue $F(t)$ along any path not passing through 0 and 1. We can continue $F(1-t)$ along the same path, and then by (3.5.1) this gives a continuation of the vector function

$$(F(t), F(1-t), K(t), K(1-t)). \tag{3.5.2}$$

The precise connexion with periods and quasi-periods is given by the following two pairs of identities of a classical flavour; however we did not find them explicitly in the literature (which is admittedly vast). The first is not crucial for us and is included just for completeness (and possible interest).

Lemma 3.5.1. *For t in Λ we have*

$$\wp_t\left(\frac{\pi}{2}F(t)\right) = -\frac{1}{3}(t-2), \quad \wp_t\left(\frac{\pi}{2}iF(1-t)\right) = -\frac{1}{3}(t+1). \tag{3.5.3}$$

Proof. It is well-known that $\pi F(t)$ and $\pi i F(1-t)$ constitute a basis for the period lattice of E_t with respect to $\mathrm{d}X/2Y$. The abscissae of the points of order 2 are $0, 1, t$ (and the ordinates 0); and thus by (3.2.5) the two left-hand sides in (3.5.3) are among the values $-(t+1)/3, -(t-2)/3, (2t-1)/3$, which are distinct for any $t \neq 0, 1$. So we could check (3.5.3) numerically at say $t = \frac{1}{2}$ and then continue them to any point of Λ (or even $\mathbb{C}$ with $0, 1$ removed). Less computationally we could restrict to real t (so $0 < t < 1$); then it is easily seen that

$$X(r) = \wp_t(r\pi F(t)) + \frac{1}{3}(t+1), \quad Y(r) = \frac{1}{2}\wp_t'(r\pi F(t))$$

are real for $0 < r < 1$. As $r \to 0$ and $r \to 1$ we get the points at infinity of the real graph of $Y^2 = X(X-1)(X-t)$, so as r varies we get the non-compact component defined by $X \geq 1$, which cuts the X-axis at $X = 1$ with $r = \frac{1}{2}$ because there $Y(r) = 0$. The first of (3.5.3) follows, and then as above by continuation. A similar argument works for the second of (3.5.3) using real X and purely imaginary Y at $r\pi i F(1-t)$. □

To these identities we could now add the third abscissa

$$\wp_t\left(\frac{\pi}{2}F(t) + \frac{\pi}{2}iF(1-t)\right) = \frac{1}{3}(2t-1)$$

and even as mentioned above the ordinates

$$\wp_t'\left(\frac{\pi}{2}F(t)\right) = \wp_t'\left(\frac{\pi}{2}iF(1-t)\right) = \wp_t'\left(\frac{\pi}{2}F(t) + \frac{\pi}{2}iF(1-t)\right) = 0.$$

The second pair of identities is a bit more exotic.

Lemma 3.5.2. *For t in Λ we have*

$$\zeta_t\left(\frac{\pi}{2}F(t)\right) = \frac{\pi}{2}K(t), \quad \zeta_t\left(\frac{\pi}{2}iF(1-t)\right) = -\frac{\pi}{2}iK(1-t). \tag{3.5.4}$$

Proof. We will use some old-fashioned formulae from Halphen [Hal]. Probably a more modern account can be found in [Ka]. We can view a period $\tilde{\omega}$ of a curve in Weierstrass form (3.2.1) as a function of the invariants g_2, g_3, and as such it is locally analytic, provided of course that we avoid the zero locus of the discriminant $\Delta = g_2^3 - 27g_3^2$. If $\tilde{\eta} = 2\zeta(\tilde{\omega}/2)$ is the corresponding quasi-period, we have

$$\Delta\frac{\partial\tilde{\omega}}{\partial g_2} = -\frac{1}{4}g_2^2\tilde{\omega} + \frac{9}{2}g_3\tilde{\eta}, \quad \Delta\frac{\partial\tilde{\omega}}{\partial g_3} = \frac{9}{2}g_3\tilde{\omega} - 3g_2\tilde{\eta}; \tag{3.5.5}$$

see (37) of [Hal, p.307] (which actually refers to half-periods).

Now when we specialize to (3.2.4) with $\lambda = t$ to get ω, η (the reader will forgive the η both here, where it is completely traditional, and in the Proposition, where it is rather natural) we deduce for the derivatives with respect to t

$$\Delta\dot{\omega} = \left(-\frac{1}{4}\dot{g}_2g_2^2 + \frac{9}{2}\dot{g}_3g_3\right)\omega + \left(\frac{9}{2}\dot{g}_2g_3 - 3\dot{g}_3g_2\right)\eta,$$

and a simple calculation gives

$$\eta \;=\; \frac{1}{3}(1-2t)\omega + 2t(1-t)\dot{\omega}. \tag{3.5.6}$$

Taking $\omega = \pi F(t)$ and recalling (3.5.1) we get the first of (3.5.4) at once; and the second follows quickly using $\pi iF(1-t)$.

We could here add

$$\zeta_t\left(\frac{\pi}{2}F(t) + \frac{\pi}{2}iF(1-t)\right) \;=\; \frac{\pi}{2}K(t) - \frac{\pi}{2}iK(1-t).$$

Anyway $\pi K(t)$ and $-\pi iK(1-t)$ are the quasi-periods corresponding to the periods $\pi F(t)$ and $\pi iF(1-t)$ respectively, at least on Λ. The Legendre relation now looks like

$$(\pi iF(1-t))(\pi K(t)) - (\pi F(t))(-\pi iK(1-t)) = 2\pi i, \tag{3.5.7}$$

where in principle there could be a sign ambiguity on the right-hand side; this however can be removed either by computation at say $t = \frac{1}{2}$, or by noting that the period quotient $(\pi iF(1-t))/(\pi F(t))$ clearly has positive imaginary part for $0 < t < 1$. □

As for the periods of G_t, these are given by the $(\omega, -\eta)$ in (3.5.6) (note that we have $w + \zeta_t(z)$ in (3.2.6) of the exponential map).

3.6 Functions on C

To define the functions z, w in (3.1.10) we can no longer use classical functions, and we have to revert back to the curve C of the Proposition. But first we define f, g, k, l on C.

With λ in $\mathbb{C}(C)$ as in the Proposition, we write

$$f = \pi F(\lambda), \quad g = \pi i F(1-\lambda), \quad k = \pi K(\lambda), \quad l = -\pi i K(1-\lambda). \tag{3.6.1}$$

Then f, g, k, l are well-defined at all $\mathbf{c}$ in $\lambda^{-1}(\Lambda)$ in $C(\mathbb{C})$. They are analytic in $\lambda = \lambda(\mathbf{c})$. In particular, if we write $\exp_t$ for the associated exponential function from $\mathbb{C}$ to $G_t(\mathbb{C})$ as in (3.2.5),(3.2.6), then from the discussion in section 3.5 we have

$$\exp_{\lambda(\mathbf{c})}(f(\mathbf{c}), -k(\mathbf{c})) = \exp_{\lambda(\mathbf{c})}(g(\mathbf{c}), -l(\mathbf{c})) = O$$

for the origin O of $G_{\lambda(\mathbf{c})}$, which in projective form (3.2.8) is $(0,0,1,0,0)$.

Next let $P = (\xi, \eta, \mu, \nu)$ be as in the Proposition with ξ, η, μ, ν in $\mathbb{C}(C)$. We can now follow [MZ2, p.459] to define the "elliptic logarithm"

$$z(\mathbf{c}) \;=\; \int_{\xi(\mathbf{c})}^{\infty} \frac{\mathrm{d}X}{2\sqrt{X(X-1)(X-\lambda(\mathbf{c}))}}$$

locally analytic at any $\mathbf{c}$ in $C(\mathbb{C})$ with

$$\lambda(\mathbf{c}), \xi(\mathbf{c}) \neq 0, 1, \infty \;\text{ and }\; \lambda(\mathbf{c}) \neq \xi(\mathbf{c}). \tag{3.6.2}$$

Note that $\lambda \neq 0, 1$ identically as it is non-constant, and further $\xi \neq 0, 1, \lambda$ identically, otherwise $2\pi(P) = O$ contradicting (3.3.1).

For the second coordinate w we restrict further to

$$\mu(\mathbf{c}) \neq \infty. \tag{3.6.3}$$

We note from the first of (4.5) of [MZ2, p.459] and (3.2.5) above that we have

$$\wp_{\lambda(\mathbf{c})}(z(\mathbf{c})) + \frac{1}{3}(\lambda(\mathbf{c})+1) \;=\; \xi(\mathbf{c}), \quad \frac{1}{2}\wp'_{\lambda(\mathbf{c})}(z(\mathbf{c})) \;=\; \eta(\mathbf{c}). \tag{3.6.4}$$

In particular $z(\mathbf{c})$ is not a period. Now we can define the "elliptic quasi-logarithm"

$$w(\mathbf{c}) \;=\; \mu(\mathbf{c}) - \zeta_{\lambda(\mathbf{c})}(z(\mathbf{c})), \tag{3.6.5}$$

also locally analytic (for example the Weierstrass $\zeta(z)$ is locally analytic in g_2, g_3 and we specialize to (3.2.4) as above). Now consulting (3.2.5),(3.2.6) we see that

$$\exp_{\lambda(\mathbf{c})}(z(\mathbf{c}), w(\mathbf{c})) \ = \ (\xi(\mathbf{c}), \eta(\mathbf{c}), \mu(\mathbf{c}), \nu(\mathbf{c})) \ = \ P(\mathbf{c}). \tag{3.6.6}$$

Thus we have inverted the exponential map.

We could also have used integrals of the second kind instead of (3.6.5) to define w, for example

$$\int \frac{(X - \frac{1}{3}(\lambda+1))\mathrm{d}X}{2\sqrt{X(X-1)(X-\lambda)}},$$

but then we have to be careful with signs and at $X = \infty$.

3.7 Algebraic independence

The relation (3.5.6) yields on the basis elements

$$k = \frac{1}{3}(1-2t)f + 2t(1-t)\dot{f}, \tag{3.7.1}$$

$$l = \frac{1}{3}(1-2t)g + 2t(1-t)\dot{g}, \tag{3.7.2}$$

where now the derivative is taken with respect to t regarded as $\lambda(\mathbf{c})$; this at $\mathbf{c}$ makes sense provided

$$\mathrm{d}\lambda(\mathbf{c}) \neq 0. \tag{3.7.3}$$

Thus we define $\hat{C}$ as the subset of C consisting of all $\mathbf{c}$ with (3.6.2),(3.6.3),(3.7.3) (so that also $\eta(\mathbf{c}) \neq 0$). By the above discussion, it is C with at most finitely many points removed.

We now obtain an analogous relation expressing the quasi-logarithm w in terms of the logarithm z and a derivative.

Lemma 3.7.1. *For* $\mathbf{c}$ *in* $\hat{C}$ *we have*

$$w \ = \ -\frac{1}{3}(1-2t)z - 2t(1-t)\dot{z} + t(1-t)\frac{\dot{\xi}}{\eta} + \frac{\eta}{\xi - t} + \mu.$$

Proof. Note that the signs on the right-hand side of (3.5.6) get changed, because a period of G_λ is $(\omega, -\eta)$. We use some more old-fashioned formulae. Namely in the Weierstrass notation (3.5.5) we have

$$\begin{aligned} \Delta\frac{\partial\wp(z)}{\partial g_2} &= \wp'(z)\left(-\frac{9}{2}g_3\zeta(z)+\frac{1}{4}g_2^2 z\right) - 9g_3\wp(z)^2 + \frac{1}{2}g_2^2\wp(z) + \frac{3}{2}g_2g_3, \\ \Delta\frac{\partial\wp(z)}{\partial g_3} &= \wp'(z)\left(3g_2\zeta(z)-\frac{9}{2}g_3 z\right) + 6g_2\wp(z)^2 - 9g_3\wp(z) - g_2^2; \end{aligned}$$

see (14) of [Hal, p.298]. We take the total derivative as in the proof of Lemma 3.5.2 using (3.6.4) and (3.6.5) with $t = \lambda(\mathbf{c})$ and a short calculation yields the result. □

We briefly sketch an alternative proof of this lemma, as suggested by Bertrand. By standard results, there exists a linear relation over the field $\mathbb{C}(\lambda)$ between the differentials $\eta_\lambda = -(X - \frac{1}{3}(\lambda+1))dX/(2Y), \omega_\lambda = dX/(2Y)$ and $\dot{\omega}_\lambda = dX/(4(X-\lambda)Y)$ modulo the exact differentials on E_λ. And indeed one can check the following identity

$$d\left(\frac{Y}{X-\lambda}\right) = \frac{1}{3}(1-2\lambda)\omega_\lambda + 2\lambda(1-\lambda)\dot{\omega}_\lambda - \eta_\lambda$$

by dividing both sides by dX and then comparing the left with the right hand side after differentiation. The above relation would also follow from the differential equation for ω_λ in [Man, p.1397, (3)]. If we integrate both sides along a path from some suitably chosen base point $Q^*(\mathbf{c})$ on $E_{\lambda(\mathbf{c})}$ to $\pi(P(\mathbf{c}))$ we arrive at the same identity as in the statement of Lemma 3.7.1. We cannot take Q^* to be O because η has a pole there but taking one of the 2-torsion points $(0,0)$ or $(1,0)$ on E_λ works.

Thus, fixing any point $\mathbf{c}_*$ of $\lambda^{-1}(\Lambda)$ also in $\hat{C}$, we see that f, g, k, l, z, w are well-defined on a small neighbourhood N_* of $\mathbf{c}_*$. We will need the following result, where again $t = \lambda(\mathbf{c})$ is interpreted on C.

Lemma 3.7.2. *The functions z, w are algebraically independent over $\mathbb{C}(f, g, k, l)$ on N_*.*

Proof. We show the independence even over $\mathcal{K} = \mathbb{C}(t, f, g, k, l)$. From the Legendre relation (3.5.7), now in the form

$$gk - fl = 2\pi i, \tag{3.7.4}$$

together with (3.7.1), we see that $\mathcal{K}$ is $\mathcal{K}' = \mathbb{C}(t, f, g, \dot{f})$. Further by Lemma 3.7.1 it is enough to verify the algebraic independence of $z, \dot{z}$ over $\mathcal{K}'$. But this is just Théorème 5 of [B1, p.136] with $r = 1$; one can choose the parameter $x = \lambda$ there (recall that λ is not constant). Note that the condition there that z, f, g are indeed linearly independent over $\mathbb{Z}$ is satisfied because of (3.6.4) and our assumption that $\pi(P(\mathbf{c})) = (\xi(\mathbf{c}), \eta(\mathbf{c}))$ is not identically torsion. □

3.8 Continuation.

Recall that $\hat{C}$ is obtained from $C(\mathbb{C})$ by the removal of a finite set of points. Fix $\mathbf{c}_*$ in $\lambda^{-1}(\Lambda)$, choose $\mathbf{c}$ in $\hat{C}$ and then a path from $\mathbf{c}_*$ to $\mathbf{c}$ lying in $\hat{C}$. We can easily continue f, g, k, l along the path using (3.6.1) and the remark around (3.5.2), because $\lambda \neq 0, 1$ on $\hat{C}$. Then f, g remain a basis for the period lattice of E_λ, and by continuing (3.5.4) we see that $(f, -k), (g, -l)$ remain a basis for that of G_λ.

For the continuation of the functions z, w we follow section 3.6 of [MZ2]. It is convenient to remove also the singular points. Let C_0 be the finite subset which we have removed so far, and write $\widehat{C}$ for what remains. We can now speak of functions analytic on $\widehat{C}$.

To continue (z, w) from $\mathbf{c}_*$ to $\mathbf{c}$ in $\widehat{C}$ it suffices to verify that if N_1, N_2 are small open subsets in $\widehat{C}$, with $N_1 \cap N_2$ connected, such that (z, w) has an analytic definition (z_1, w_1) on N_1 and an analytic definition (z_2, w_2) on N_2, then it has an analytic definition on $N_1 \cup N_2$. But from (3.6.6) we deduce $\exp_\lambda(z_1, w_1) = \exp_\lambda(z_2, w_2)$ on $N_1 \cap N_2$. Thus there are rational integers x, y with

$$(z_2, w_2) = x(f, -k) + y(g, -l) + (z_1, w_1)$$

on this intersection, and they must be constant there. So all we have to do is for example to change (z_2, w_2) to $(z_2, w_2) - x(f, -k) - y(g, -l)$ on N_2. Using the same path it is easy to see that we can continue the function (f, g, k, l, z, w) from a small neighbourhood of $\mathbf{c}_*$ to a small neighbourhood $N_\mathbf{c}$ of $\mathbf{c}$ in $\widehat{C}$. The end result is a function $(f_\mathbf{c}, g_\mathbf{c}, k_\mathbf{c}, l_\mathbf{c}, z_\mathbf{c}, w_\mathbf{c})$ analytic on $N_\mathbf{c}$. Write Ω_t for the period lattice of G_t.

Lemma 3.8.1. *The functions $z_\mathbf{c}, w_\mathbf{c}$ are algebraically independent over the field $\mathbb{C}(f_\mathbf{c}, g_\mathbf{c}, k_\mathbf{c}, l_\mathbf{c})$ on $N_\mathbf{c}$. Further we have $\Omega_\lambda = \mathbb{Z}(f_\mathbf{c}, -k_\mathbf{c}) + \mathbb{Z}(g_\mathbf{c}, -l_\mathbf{c})$ on $N_\mathbf{c}$.*

Proof. We could continue an algebraic dependence relation backwards to get the same relation between f, g, z, w on a neighbourhood of $\mathbf{c}_*$; however this would contradict Lemma (3.7.2). The assertion about Ω_λ follows from the discussion above. □

With a view towards constructing the set S mentioned in the Introduction, we now define $x_{\mathbf{c}}, y_{\mathbf{c}}$ on $N_{\mathbf{c}}$ by

$$x_{\mathbf{c}} = -\frac{1}{2\pi i}(l_{\mathbf{c}} z_{\mathbf{c}} + g_{\mathbf{c}} w_{\mathbf{c}}), \quad y_{\mathbf{c}} = \frac{1}{2\pi i}(k_{\mathbf{c}} z_{\mathbf{c}} + f_{\mathbf{c}} w_{\mathbf{c}})$$

By (3.7.4) these satisfy

$$(z_{\mathbf{c}}, w_{\mathbf{c}}) = x_{\mathbf{c}}(f_{\mathbf{c}}, -k_{\mathbf{c}}) + y_{\mathbf{c}}(g_{\mathbf{c}}, -l_{\mathbf{c}}) \tag{3.8.1}$$

as in (3.1.10).

We use the standard maximum norm on $\mathbb{C}^5$. For small $\delta > 0$ (later to be specified) we define C^δ as the set of $\mathbf{c}$ in C satisfying $|\mathbf{c}| \leq 1/\delta$ and

$$|\mathbf{c} - \mathbf{c}_0| \ \geq \ \delta \tag{3.8.2}$$

for each $\mathbf{c}_0$ in the finite set C_0.

Shrinking $N_{\mathbf{c}}$ if necessary, we can choose for each $\mathbf{c}$ in C^δ a local analytic isomorphism $\varphi_{\mathbf{c}}$ from $N_{\mathbf{c}}$ to an open subset of $\mathbb{C}$. Choose any closed disc $D_{\mathbf{c}}$ centred at $\varphi_{\mathbf{c}}(\mathbf{c})$ such that some neighbourhood of the disc with twice the radius and the same centre is inside $\varphi_{\mathbf{c}}(N_{\mathbf{c}})$, and define

$$\theta_{\mathbf{c}} \ = \ (x_{\mathbf{c}}, y_{\mathbf{c}}) \circ \varphi_{\mathbf{c}}^{-1} \tag{3.8.3}$$

from $D_{\mathbf{c}}$ to $\mathbb{C}^2$. By compactness there is a finite set Π of $\mathbf{c}$ in C^δ such that the $\varphi_{\mathbf{c}}^{-1}(D_{\mathbf{c}})$ cover C^δ.

We are all set up for an application of Lemma 3.4.1. It will turn out that every $\mathbf{c}$ in our Proposition leads to many rational values of $x_{\mathbf{c}}, y_{\mathbf{c}}$, and of course we have to estimate their denominator. This we do in the next short section.

3.9 Orders of torsion

We first clarify the relation between torsion points of E_t and torsion points of G_t using (3.2.9) with the projection π of (3.2.7) and the embedding ϕ of (3.2.8).

Lemma 3.9.1. *For each complex $t \neq 0, 1$ and each positive integer n the map π induces a bijection from the points of order n in G_t to the points of order n on E_t.*

Proof. We first verify the analogous statement for the groups of points of order dividing n; now π is a homomorphism. It is injective because its kernel $\phi(\mathbb{G}_{\mathrm{a}})$ has no non-zero torsion. Now the group in E_t has order n^2, and this is well-known to hold also for G_t; for example they are the points $\exp_t(\mathbf{z}/n)$ for all $\mathbf{z}$ in the period group Π_t, of rank 2 over $\mathbb{Z}$, modulo $n\Pi_t$. The result follows quickly for points of order exactly n; for example by Möbius inversion or by noting that if Q has order n then $\pi(Q)$ has order d dividing n but if $d < n$ then $\pi(Q) = \pi(R)$ for R of order dividing d, which by the group isomorphism forces $Q = R$ an impossibility. □

We use the standard absolute Weil height of an algebraic number and also the standard extension to vectors. See for example [Si2, p.208].

Lemma 3.9.2. *There is a constant $c = c(C)$ with the following property. Suppose for some $\mathbf{a}$ in $\widehat{C}$ that the point $P(\mathbf{a})$ has finite order n. Then $\mathbf{a}$ is algebraic, and*

$$n \ \leq \ c[\mathbb{Q}(\mathbf{a}) : \mathbb{Q}]^2(1 + h(\mathbf{a})).$$

Proof. By Lemma 3.9.1 the point $P' = \pi(P(\mathbf{a}))$ also has order n. It is clear that $\mathbf{a}$ is algebraic, otherwise $q = n$ would contradict (3.3.1). Now we apply David's work [Davi] to $P', \ldots, nP'$, just as in the proof of Lemma 7.1 of [MZ2, p.462]. □

3.10 Heights

In view of the following result we can eliminate the height dependence in Lemma (3.9.2).

Lemma 3.10.1. *There is a constant $c = c(C)$ with the following property. Suppose for some $\mathbf{a}$ in $\widehat{C}$ 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 [Si1, p.197] for E_λ, because $\pi(P)$ is not identically of finite order. □

Another advantage of bounded height is the following easy remark concerning the sets C_0 and C^δ in section 3.8. We note that the points of C_0 are algebraic over $\mathbb{Q}$.

Lemma 3.10.2. *Given a number field K containing the coordinates of the points of C_0, and a constant c, there is a positive constant $\delta = \delta(C, K, c)$ depending only on C, K and c with the following property. Suppose $\mathbf{a}$ is algebraic on C, not in C_0, with $h(\mathbf{a}) \leq c$. Then there are at least $\frac{1}{2}[K(\mathbf{a}) : K]$ conjugates of $\mathbf{a}$ over K lying in C^δ.*

Proof. This is Lemma 8.2 of [MZ4, p.126]. □

3.11 Proof of Proposition (algebraic case)

We fix any positive $\epsilon < \frac{1}{2}$. We use $c, c_1, c_2, \ldots,$ for positive constants depending only on C. We have to show that there are at most finitely many $\mathbf{a}$ such that $P = P(\mathbf{a})$ has finite order on $G_{\lambda(\mathbf{a})}$. By Lemma 3.9.2 each such $\mathbf{a}$ is algebraic, say of degree $d = [\mathbb{Q}(\mathbf{a}) : \mathbb{Q}]$, and thanks to Lemma 3.10.1 and the Northcott property it will suffice to prove that $d \leq c$. We will actually argue with a single $\mathbf{a}$.

Next, Lemma 3.9.2 together with Lemma 3.10.1 shows that there is a positive integer

$$n \leq c_1 d^2 \tag{3.11.1}$$

such that

$$nP = O.$$

Fix a number field K containing a field of definition for the curve C and the points of C_0. By Lemma 3.10.1 and Lemma 3.10.2 the algebraic $\mathbf{a}$ has at least $\frac{1}{2}[K(\mathbf{a}) : K]$ different conjugates over K in some C^δ; here $\delta = c_2$. Now C^δ is contained in the union of at most c_3 closed sets $\varphi_{\mathbf{c}}^{-1}(D_{\mathbf{c}})$, and so there is $\mathbf{c}$ such that $\varphi_{\mathbf{c}}^{-1}(D_{\mathbf{c}})$ contains at least $\frac{1}{2}[K(\mathbf{a}) : K]/c_3 \geq d/c_4$ different conjugates $\sigma(\mathbf{a})$. And the corresponding conjugate points $\sigma(P)$ also satisfy $n\sigma(P) = O$.

We claim that each point

$$\Theta_\sigma = \theta_{\mathbf{c}}(\varphi_{\mathbf{c}}(\sigma(\mathbf{a}))) = (x_{\mathbf{c}}(\sigma(\mathbf{a})), y_{\mathbf{c}}(\sigma(\mathbf{a})))$$

lies in $\mathbb{Q}^2$ and even in $\mathbb{Z}^2/n$.

Now the function $\theta_{\mathbf{c}}$ arises from continuations $f_{\mathbf{c}}, g_{\mathbf{c}}, k_{\mathbf{c}}, l_{\mathbf{c}}, z_{\mathbf{c}}, w_{\mathbf{c}}$ of the functions in section 3.8. We deduce from (3.6.6) that

$$\exp_{\lambda}(z_{\mathbf{c}}, w_{\mathbf{c}}) = P$$

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

$$\exp_{\lambda(\sigma(\mathbf{a}))}(nz_{\mathbf{c}}(\sigma(\mathbf{a})), nw_{\mathbf{c}}(\sigma(\mathbf{a}))) = O.$$

It follows that $(nz_{\mathbf{c}}(\sigma(\mathbf{a})), nw_{\mathbf{c}}(\sigma(\mathbf{a})))$ lies in the period lattice $\Omega_{\lambda(\sigma(\mathbf{a}))}$, which by Lemma 3.8.1 is just

$$\mathbb{Z}(f_{\mathbf{c}}(\sigma(\mathbf{a})), -k_{\mathbf{c}}(\sigma(\mathbf{a})) + \mathbb{Z}(g_{\mathbf{c}}(\sigma(\mathbf{a})), -l_{\mathbf{c}}(\sigma(\mathbf{a}))).$$

Thus (3.8.1) shows that $nx_{\mathbf{c}}(\sigma(\mathbf{a})), ny_{\mathbf{c}}(\sigma(\mathbf{a}))$ lie in $\mathbb{Z}$. Thus indeed Θ_σ lies in $\mathbb{Z}^2/n$ as claimed.

We are going to apply Lemma 3.4.1 with $(f_1(t), f_2(t)) = \theta_{\mathbf{c}}(t)$ in (3.8.3). Here the algebraic independence of f_1, f_2 amounts to that of $x_{\mathbf{c}}, y_{\mathbf{c}}$ which follows at once from (3.8.1) and Lemma 3.8.1. We deduce that there are at most $c_5 n^{\epsilon}$ different possibilities for $\varphi_{\mathbf{c}}(\sigma(\mathbf{a}))$ and so for $\sigma(\mathbf{a})$. Thus by (3.11.1) at most $c_6 d^{2\epsilon}$. This contradicts the above lower bound d/c_4 provided d is sufficiently large. As observed near the beginning of this section, that suffices to prove Proposition 1 in the algebraic case.

3.11.1 Example of Effectivity

All the ingredients of the proof of Proposition 1 in the algebraic case are well-known to be effective except for the zero-estimate $\gamma(T)$ appearing in the proof of Lemma 3.4.1.

In this short subsection we indicate rapidly how to get an upper bound for $\gamma(T)$ for the curve parametrized by

$$(2, \sqrt{4-2\lambda}, 0, 4)$$

which we already presented in (3.1.7). In section 3.6 we have described how to locally invert the exponential map on a curve and for our curve the inverse is given by

$$z = \int_2^\infty \frac{dX}{2\sqrt{X(X-1)(X-t)}},$$
$$w = -\frac{1}{3}(1-2t)z - 2t(t+1)\dot{z} + \frac{\sqrt{4-2t}}{2-t}$$

for a complex parameter $\lambda = t$ in a neighbourhood of $\frac{1}{2}$. For the integral defining z we can choose the path of integration as the real line and after choosing a sign for the square-root in the definition of z, we get well-defined analytic functions z, w in a neighbourhood of $\frac{1}{2}$. Now we define the coordinates x, y by

$$\begin{aligned} x &= -\frac{1}{2\pi i}(lz + gw), \\ y &= \frac{1}{2\pi i}(kz + fw) \end{aligned}$$

where f, g, l, k are defined as in section 3.5 by hypergeometric functions. We can continue the analytic function $\mathbf{f} = (x, y)$ to any point in $\mathbb{C} \backslash \{0, 1, 2\}$ as we explained in section 3.8.

Now x, y have singularities at 0,1 and 2 coming from the hypergeometric functions f, g and the elliptic integral z. If we remove the half lines $(-\infty, 0]$ and $[1, +\infty)$ from the real line the continuation of the function (f, g, z) to the resulting simply connected domain in $\mathbb{C}$ is well-defined and we can estimate its norm as a function of the distance to 0,1 and 2. Then taking also monodromy into consideration we can compute the following bound

$$\max\{|f(t)|, |g(t)|, |z(t)|\} \leq 50 \max\{1, |2-t|^{3/2}, |\log(|1-t|)|, |\log(|t|)|\} \quad (3.11.2)$$

for a suitable continuation of (f, g, z) from $\frac{1}{2}$ to any point of $\mathbb{C} \setminus \{0, 1, 2\}$.

Now we assume that t is such that the point (3.1.7) is torsion for $\lambda = t$. The height-bound for t allows us to pick δ effectively such that at least half of the Galois conjugates of t lie in the set C_δ (analogously to C^δ in Lemma 3.10.2), which consists of all $t \in \mathbb{C}$ satisfying

$$\frac{1}{\delta} \geq |t| \geq \delta, \ |1-t| \geq \delta, \ |2-t| \geq \delta.$$

We cover C_δ by an effective number of discs of radius $\delta/8$ such that for each disc D in the cover, the disc $D^\#$ of radius $\delta/4$ and the same centre as D lies in $C_{3\delta/4}$. With our choice of the cover and the estimate in (3.11.2) we can now give an upper bound M for $\max\{|x|, |y|\}$ for a continuation of $\mathbf{f}$ from $\frac{1}{2}$ to $D^\#$ for each disc D of this cover. Now we can follow the proof of Proposition 1 with C_δ replaced by C^δ and x, y described above. What remains for an effective proof is a zero-estimate of Masser for certain functions with a logarithmic singularity. In relation to the quantity $\gamma(T)$ the following version of his estimate would be good enough for our purposes.

Masser's zero estimate: Let u, v, y be functions analytic in the open disc of radius 1 centred at 0 with $v(0) \neq 0, y'(0) \neq 0$, and let $P = P(X, Y)$ be a non-zero polynomial of degree at most d in X and of degree at most e in Y. Then for $x = u + \mathcal{L}v$, where $\mathcal{L}$ is the ordinary logarithm function, the function $\Phi = P(x, y)$ has at most

$$2^{22(d+1)^2}(e+1)^2 \log(2M)$$

zeroes in the closed disc of radius $\frac{1}{20}$ centred at $\frac{1}{2}$, where

$$\mathcal{M} = \max\{1, \frac{1}{|v(0)|}, \frac{1}{|y'(0)|}, |u|_{B(0,\frac{9}{10})}, |v|_{B(0,\frac{9}{10})}, |y|_{B(0,\frac{9}{10})}\}.$$

Here the symbol $|f|_{B(0,\frac{9}{10})}$ denotes the maximum of an analytic function f on the closed ball $B(0, \frac{9}{10})$.

In our case x has such an expansion with $v = -\frac{1}{\pi i}y$ and y is analytic on the unit disc. The method used to establish the zero-estimate is flexible enough to provide us with an estimate of $\gamma(T)$ for each disc D of the cover.

This strategy opens the door for a general effective version of Theorem 3 which will be done in future work.

3.12 Proof of Proposition (transcendental case)

Now we extend Proposition 1 to curves defined over an arbitrary subfield of $\mathbb{C}$. We have already proved it when C is defined over $\overline{\mathbb{Q}}$. We now assume that C is not defined over $\overline{\mathbb{Q}}$.

For the proof we follow the arguments in [MZ2, p.471, 472]. Given a torsion point $P(\mathbf{c})$ we construct a curve in a fixed additive extension of an elliptic curve with transcendental j-invariant containing a point of the same order. By Fricke-Weber the Galois orbit of such a point is as big as possible and this will allow us to find a bound for its order. The construction of this curve will not depend on the particular point but only on the equations defining C. Since we assumed that $q\pi(P) \neq O$ for all non-zero rational integers q this provides us with a bound on the number of torsion points on C.

If $\lambda(\mathbf{c})$ is algebraic then $G_{\lambda(\mathbf{c})}$ is defined over $\overline{\mathbb{Q}}$ and so if $P(\mathbf{c})$ is torsion it must also be defined over $\overline{\mathbb{Q}}$. But a curve not defined over $\overline{\mathbb{Q}}$ contains only finitely many points with algebraic coordinates; see for example [BMZ, Lemma 3, p.313]. So we may assume that $\lambda(\mathbf{c})$ is transcendental during the rest of this section.

3.12.1 Reduction to a constant relation

Because $\lambda(\mathbf{c})$ is transcendental it can be viewed as a generic element over $\mathbb{Q}$ which by abuse of notation we call λ. In what follows we write (ξ, η, μ, ν) for the coordinates of the point $P(\mathbf{c})$.

We start by finding a non-trivial algebraic relation between ξ and ν defined over $\mathbb{Q}(\lambda)$. For this we can follow the arguments in [MZ2, p.471] very closely. Let K be a field of definition of C and t its transcendence degree over $\mathbb{Q}$. Note that we always have $t \geq 1$ because of our assumption that C is not defined over $\overline{\mathbb{Q}}$. We can then write $K = \mathbb{Q}(\kappa_0, \kappa_1, \ldots, \kappa_t)$ where $\kappa_1, \ldots, \kappa_t$ are algebraically independent and κ_0 is algebraic over $\mathbb{Q}(\kappa_1, \ldots, \kappa_t)$. If $t = 1$ we define $K_0 = \mathbb{Q}$ and W_0 to be the algebraic variety parametrized by (ξ, ν, λ). Its dimension over $\mathbb{Q}$ is at least $t = 1$ and at most $t + 1 = 2$ since $K(\xi, \nu, \lambda)$ has transcendence degree at most 1 over K. If $t > 1$ we note that $\mathbb{Q}(\lambda, \kappa_0, \ldots, \kappa_t)$ has transcendence degree at least $t - 1$ over $\mathbb{Q}(\lambda)$. So we may and will assume that $\kappa_1, \ldots, \kappa_{t-1}$ are algebraically independent over $\mathbb{Q}(\lambda)$. In this case we define $K_0 = \mathbb{Q}(\kappa_1, \ldots, \kappa_{t-1})$ and W_0 to be the algebraic variety parametrized by $(\xi, \nu, \lambda, \kappa_1, \ldots, \kappa_{t-1})$. Again W_0 has dimension at least t and at most $t + 1$ over $\mathbb{Q}$.

If the dimension of W_0 is $t + 1$, its points lie in the zero locus of a single polynomial. So if the dimension of W_0 is $t + 1$ we get a non-trivial algebraic relation between ξ and ν of the form

$$F(\xi, \nu) = 0$$

where F has coefficients in the field $K_0(\lambda)$. If the dimension of W_0 is less than $t + 1$ it must be exactly t and we consider the projection of W_0 to the variety W_1 parametrized by $(\xi, \lambda, \kappa_1, \ldots, \kappa_{t-1})$ in $\mathbb{A}^{t+1}$. Now just as at the top of [MZ2, p.472] we again obtain a non-trivial algebraic relation between ξ and ν (but without ν) which is also defined over $K_0(\lambda)$.

We arrive at a non-trivial algebraic relation defined over $\mathbb{Q}(\lambda)$ by noting as in [MZ2, p.473] that the fields $K_0(\lambda)$ and $\overline{\mathbb{Q}(\lambda)}$ are linearly disjoint over $\mathbb{Q}(\lambda)$ by [La3, Proposition 3.3, p.363]. Since ξ and ν are coordinates of a torsion point on G_λ they are in $\overline{\mathbb{Q}(\lambda)}$ and from the linear disjointness of the fields $K_0(\lambda)$ and $\overline{\mathbb{Q}(\lambda)}$ follows that there exists a non-trivial algebraic relation between ξ and ν defined over $\mathbb{Q}(\lambda)$. By abuse of notation we denote this last algebraic relation also by F.

3.12.2 Passing to a Weierstrass model defined over $\mathbb{Q}(j)$

Before we can apply the necessary Galois theory we have to change the elliptic curve so that it is defined over $\mathbb{Q}(j)$ for its j-invariant j. We do this via g_2, g_3 defined by (3.2.4) to get $\tilde{Y}^2 = 4\tilde{X}^3 - g_2\tilde{X} - g_3$ as in (3.2.1), and then $\check{X} = u^2\tilde{X}, \check{Y} = u^3\tilde{Y}$ for any u with $u^2 = \frac{g_2}{g_3}$ (note $g_3 \neq 0$). Defining also $\check{U} = u\tilde{U}, \check{V} = u^4\tilde{V}$ we get the equations

$$\check{Y}^2 = 4\check{X}^3 - \frac{27j}{j-1728}\check{X} - \frac{27j}{j-1728}, \quad \check{V} - \check{Y}\check{U} = 2\check{X}^2 \tag{3.12.1}$$

where

$$j = 256\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(1-\lambda)^2}.$$

Here (3.12.1) defines $\check{G}_j$, an extension of $\check{E}_j$ defined by the first equation and all are defined over $\mathbb{Q}(j)$.

3.12.3 Galois theory

For a natural number $n \geq 2$ we denote by L_n the field obtained by adjoining the coordinates of all points of order dividing n of the curve $\check{E}_j$ to the field $\mathbb{Q}(j)$. Further let $\check{\wp}, \check{\zeta}$ be the Weierstrass functions associated to $\check{E}_j$ and Λ be the lattice of $\check{\wp}$.

The non-zero points of order dividing n of $\check{E}_j$ are given by

$$(\check{\wp}(\omega/n), \check{\wp}'(\omega/n)), \ \omega \in \Lambda \setminus n\Lambda.$$

The Galois group of the extension $L_n/\mathbb{Q}(j)$ is isomorphic to $GL_2(\mathbb{Z}/n\mathbb{Z})$ [La2, p.68] and we can describe its action on the points of order n as follows. If ω_1, ω_2 is a basis of the period lattice of Λ and $\omega = m_1\omega_1 + m_2\omega_2$, then $\gamma \in GL_2(\mathbb{Z}/n\mathbb{Z})$ sends $(\check{\wp}(\omega/n), \check{\wp}'(\omega/n))$ to $(\check{\wp}(\omega^\gamma/n), \check{\wp}'(\omega^\gamma/n))$ with $\omega^\gamma = m_1^\gamma\omega_1 + m_2^\gamma\omega_2$ where $\begin{pmatrix} m_1^\gamma \\ m_2^\gamma \end{pmatrix} = \gamma \begin{pmatrix} m_1 \\ m_2 \end{pmatrix}$. This is pointed out in Lemma 10.1 of [MZ2, p.464].

We denote by $\eta(\omega) = 2\check{\zeta}(\omega/2)$ the quasi-period associated to $\omega \in \Lambda$ and by exp the exponential map of $\check{G}_j$ as in (3.2.2) for the Weierstrass model. Then $\Omega = \mathbb{Z}(\omega_1, -\eta(\omega_1)) + \mathbb{Z}(\omega_2, -\eta(\omega_2))$ is the kernel of exp and the non-zero points of order dividing n on $\check{G}_j$ are

$$\exp(\omega/n, -\eta(\omega)/n), \ \omega \in \Lambda.$$

Now we describe the action of the Galois group of $L_n/\mathbb{Q}(j)$ on the torsion points of $\check{G}_j$ as follows.

Lemma 3.12.1. *Let $\check{G}_j$ and* $\exp$ *be as above. The coordinates of a point $\check{P}$ of order n are in L_n and an element $\gamma \in GL_2(\mathbb{Z}/n\mathbb{Z})$ acts on $\check{P}$ by sending $\check{P} =$* $\exp(\omega/n, -\eta(\omega)/n)$ *to $\check{P}^\gamma = \exp(\omega^\gamma/n, -\eta(\omega^\gamma)/n)$.*

Proof. We first show that the coordinates of $\check{P}$ are in L_n. It is clear from (3.2.2) that it is enough to show that $\check{\zeta}(\omega/n) - \eta(\omega)/n \in L_n$. To prove this we consider the function $\check{\zeta}((n+1)z) - (n+1)\zeta(z)$. It is an odd elliptic function with respect to the lattice Λ. By the general theory of elliptic functions there exists $Q \in \mathbb{C}(X)$ such that

$$\check{\zeta}((n+1)z) - (n+1)\check{\zeta}(z) = \check{\wp}'(z)Q(\check{\wp}(z)). \tag{3.12.2}$$

Now fairly standard arguments show that we can even take $Q \in \mathbb{Q}(j)(X)$. For example when $Q = P_1/P_2$ for $P_1, P_2 \in \mathbb{C}[X]$, we have

$$P_2(\check{\wp}(z))(\check{\zeta}((n+1)z) - (n+1)\check{\zeta}(z)) - \check{\wp}'(z)P_1(\check{\wp}(z)) = 0. \tag{3.12.3}$$

By expanding in Laurent series about $z = 0$, we can regard this as an infinite system of homogenous linear equations in the coefficients of P_1, P_2. Because it has a non-trivial solution, the rank is strictly less than the number of coefficients. Now it is well-known that the Laurent series of $\check{\wp}(z)$ and $\check{\zeta}(z)$ have coefficients in $\mathbb{Q}(j)$ (see for example [Hu, p.175] with the remark (4.6) on p.221). Thus the system is defined over $\mathbb{Q}(j)$. It follows that there is a non-trivial solution also over $\mathbb{Q}(j)$. In fact $P_2 \neq 0$ for this solution, else $P_2 = 0$ would imply also $P_1 = 0$ by (3.12.3). So indeed this $Q = P_1/P_2 \in \mathbb{Q}(j)(X)$.

We can further assume P_1, P_2 are coprime by dividing through their common factor in $\mathbb{Q}(j)[X]$.

Now we return to the relation (3.12.2) with $Q = P_1/P_2 \in \mathbb{Q}(j)(X)$. The poles of the function on the left side are contained in $\frac{1}{n+1}\Lambda$ as are the poles of $\check{\wp}, \check{\wp}'$.

We temporarily assume n is odd. Then for any $\omega \in \Lambda \backslash n\Lambda$ we have $\check{\wp}'(\omega/n) \neq 0$ and it follows that $P_2(\check{\wp}(\omega/n)) \neq 0$ otherwise $P_1(\check{\wp}(\omega/n)) \neq 0$ by coprimality and the right-hand side would become infinite. Thus $Q(\check{\wp})$ is defined at $z = \frac{\omega}{n}$.

Setting $z = \frac{\omega}{n}$ in (3.12.2) we find that

$$\check{\zeta}\left(\frac{\omega}{n}\right) - \frac{\eta(\omega)}{n} = -\frac{1}{n}\check{\wp}'\left(\frac{\omega}{n}\right)Q\left(\check{\wp}\left(\frac{\omega}{n}\right)\right) \in L_n \tag{3.12.4}$$

as claimed.

Next we take an element g of the Galois group of $L_n/\mathbb{Q}(j)$ which sends $(\check{\wp}(\omega/n), \check{\wp}'(\omega/n))$ to $(\check{\wp}(\omega^\gamma/n), \check{\wp}'(\omega^\gamma/n))$ and set $\check{\mu} = \check{\zeta}(\omega/n) - \eta(\omega)/n$. Then (3.12.4) shows that

$$\check{\mu}^g = -\frac{1}{n}\check{\wp}'\left(\frac{\omega^\gamma}{n}\right) Q\left(\check{\wp}\left(\frac{\omega^\gamma}{n}\right)\right)$$

which is equal to $\check{\zeta}(\omega^\gamma/n) - \eta(\omega^\gamma)/n$, again by (3.12.4) with ω replaced by ω^γ.

If n is even then a similar argument works provided we restrict to $\omega \in \Lambda \setminus \frac{n}{2}\Lambda$ to keep $\check{\wp}'(\omega/n) \neq 0$ (the corresponding ω^γ is then also in $\Lambda \setminus \frac{n}{2}\Lambda$ because we have avoided points of order 2). And for $\omega \in \frac{n}{2}\Lambda \setminus n\Lambda$ we have $\check{\zeta}(\omega/n) - \eta(\omega)/n = 0$ and also $\check{\zeta}(\omega^\gamma/n) - \eta(\omega^\gamma)/n = 0$ (we are now working with points of order 2), so the lemma is trivial.

□

With Lemma 3.12.1 we can refer to [MZ2, Lemma 10.1] to get the Galois bounds necessary for the proof of the Proposition in the transcendental case.

Namely for any point $P = (\xi, \eta, \mu, \nu)$ on G_λ of order $n \geq 2$ the point $\check{P} = (\check{\xi}, \check{\eta}, \check{\mu}, \check{\nu})$ on $\check{G}_j$ is of order n and from [MZ2, Lemma 10.1] follows that the cardinality of the orbit of $\check{P}$ under the action of the Galois group of $L_n/\mathbb{Q}(j)$ is bounded from below by $\frac{6}{\pi^2}n^2$.

We note for later use that this bound applies to $(\check{\xi}, \check{\eta})$, and since any $\check{\xi}$ gives rise to at most two $\check{\eta}$ we deduce that $\check{\xi}$ has degree at least $\frac{3}{\pi^2}n^2$ over $\mathbb{Q}(j)$.

3.12.4 Conclusion

We assume that $P(\mathbf{c})$ and so also $\check{P}$ is of exact order $n \geq 2$.

Note that in the formulae expressing ξ, ν in terms of $\check{\xi}, \check{\nu}$ only λ and $u^2 = \frac{g_2}{g_3} \in \mathbb{Q}(\lambda)$ turn up. So the relation F between ξ and ν from subsection 3.12.1 gives rise to a relation between $\check{\xi}$ and $\check{\nu}$ defined over $\mathbb{Q}(\lambda)$. The field $\mathbb{Q}(\lambda)$ is a finite extension of $\mathbb{Q}(j)$ so taking the norm we end up with a relation (independent of n or $\mathbf{c}$)

$$\check{F}(\check{\xi}, \check{\nu}) = 0 \tag{3.12.5}$$

defined over $\mathbb{Q}(j)$. We select a factor $\check{F}_0$ of $\check{F}$ over $\overline{\mathbb{Q}(j)}$ irreducible over $\overline{\mathbb{Q}(j)}$ also vanishing at $(\check{\xi}, \check{\nu})$. Now $\check{F}_0 = 0$ defines in $\check{G}_j$ a curve $\check{C}$ (note that by (3.2.1) $\check{X}$ and $\check{V}$ are independent on $\check{G}_j$) with $\check{P} \in \check{C}$. Now $\check{C}$ has no zero-dimensional components. This follows from [La1, Corollary, p.38] with $r = 3, s = 2, n = 4$ and V^3 there defined by $\check{F}_0 = 0$ and W^2 there defined by the equations in (3.12.1), both in the affine space $\mathbb{A}^4$. Thus there is a curve component $\check{C}_0$ over $\overline{\mathbb{Q}(j)}$ of $\check{C}$ also with $\check{P} \in \check{C}_0$ (in fact one can show that if $\check{C}$ is not itself irreducible then it has two components, of the form $\check{D}$ and $-\check{D}$).

In fact $\check{C}_0$ is defined over a finite extension K of $\mathbb{Q}(j)$. The compositum KL_n is a Galois extension of K whose group G whose index satisfies $D = [G : GL_2(\mathbb{Z}/n\mathbb{Z})] \leq [K : \mathbb{Q}(j)]$ also independent of n or $\mathbf{c}$.

Now we can apply the methods of of the Appendix of [MZ3]. We first fix a prime l not dividing n. Since $\begin{pmatrix} l & 0 \\ 0 & l \end{pmatrix}$ is in $GL_2(\mathbb{Z}/n\mathbb{Z})$ we see that $\begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix}$ is in G for $m = l^D$. So multiplication by m acts on the points of order n like an element of G. In particular $m\check{P} \in \check{C}_0$. As $m\check{P} \in m\check{C}_0$ we deduce that $m\check{P} \in \check{C}_0 \cap m\check{C}_0$ and further that for any g in G

$$m\check{P}^g \in \check{C}_0 \cap m\check{C}_0.$$

From the remarks at the end of the last subsection it follows that

$$|\check{C}_0 \cap m\check{C}_0| \geq \frac{6}{\pi^2 D} n^2. \tag{3.12.6}$$

Next we give a bound for the degree of $m\check{C}_0$ in terms of m. For this we take a new embedding of $\check{G}_j$ into projective space as described in [Hi, p.577, section 1, part (a)]. For an algebraic subvariety $\mathcal{H}$ of $\check{G}_j$ we denote by $\deg_e \mathcal{H}$ the degree of $\mathcal{H}$ with respect to that embedding and by $\deg \mathcal{H}$ the degree of $\mathcal{H}$ with respect to the original embedding of $\check{G}_j$ into $\mathbb{P}_4$ given by homogenizing (3.2.1). Since the embeddings are fixed there exist absolute constants $c_1 > 0, c_2$ such that $c_1 \deg_e \mathcal{H} \leq \deg \mathcal{H} \leq c_2 \deg_e \mathcal{H}$. For our curve $\check{C}_0$ the Corollaire in [Hi, p.589] implies that

$$\deg_e m\check{C}_0 \leq m^2 \deg_e \check{C}_0.$$

So

$$\deg m\check{C}_0 \leq c_2 \deg_e m\check{C}_0 \leq c_2 m^2 \deg_e \check{C}_0 \leq c_1^{-1} c_2 m^2 \deg \check{C}_0.$$

If $\check{C}_0$ and $m\check{C}_0$ do not have a common component then it follows by any easy version of Bézout's theorem for curves in $\mathbb{P}_4$ (see for example [BG, p.561]) that

$$|\check{C}_0 \cap m\check{C}_0| \leq cm^2(\deg \check{C}_0)^2 \tag{3.12.7}$$

for an absolute constant c. As pointed out in [MZ3, p.658] we can pick l such that $l \leq 41 + 2\log n$ with the above property. Now comparing the upper bound coming from (3.12.7) with the lower bound (3.12.6) we get

$$\frac{6}{\pi^2 D} n^2 \leq c(41 + 2\log n)^{2D}(\deg \check{C}_0)^2$$

and so a bound for n. This finishes the proof for that case.

In fact we can avoid the exponent $2D$ above by working over $\mathbb{Q}(j)$ not the closure. This may be useful in numerical examples.

It remains to consider the case that $\check{C}_0, m\check{C}_0$ do have a common component. But by irreducibility we must have

$$\check{C}_0 = m\check{C}_0. \tag{3.12.8}$$

From [Hi, Lemme 16, p.589] we deduce that $\check{C}_0$ is a translate of an algebraic subgroup of $\check{G}_j$.

The only (geometrically) connected algebraic subgroup curve of $\check{G}_j$ is $A = \tilde{\phi}(\mathbb{G}_a)$ (for $\tilde{\phi}$ as in (3.2.3)) so $\check{C}_0$ is of the form $A + S$ for some point S on $\check{G}_j$.

Now (3.12.8) implies $A + S = m(A + S)$ so $(m - 1)S \in A$. So $\pi(S) = 0$ is torsion. It follows from Lemma 3.9.1 that $\pi(S) = \pi(T)$ for T torsion. Thus $A + S = A + T$.

As $\check{C}_0$ is independent of n or $\mathbf{c}$, we can find a positive integer q independent of n such that $qT = O$.

Finally $\check{P}$ lies in $A + T$, so $q\check{P}$ lies in A and $q\pi(\check{P}) = O$ in $\check{G}_j$. Hence also $q\pi(P(\mathbf{c})) = O$ in G_λ. In view of (3.3.1) this yields as desired the finiteness of the set of $\mathbf{c}$.

This establishes the Proposition in the transcendental case, and so completes the entire proof.

We illustrate some of the arguments above by showing that there are no complex $\lambda \neq 0, 1$ such that (3.1.6) is torsion on G_λ.

Here $\xi = 2$ so $F(X, V) = X - 2$ is already defined over $\mathbb{Q}(\lambda)$ and even $\mathbb{Q}$. Then

$$\tilde{\xi} = \xi - \frac{1}{3}(\lambda + 1) = \frac{5 - \lambda}{3}$$

as well as

$$\check{\xi} = \frac{g_2}{g_3}\tilde{\xi} = \frac{g_2}{g_3}\frac{5 - \lambda}{3}$$

giving the relation between $\check{\xi}, \check{\nu}$ over $\mathbb{Q}(\lambda)$. Taking the norm to $\mathbb{Q}(j)$ we find

$$\check{F}(\check{X}, \check{V}) = A_0\check{X}^6 + A_1\check{X}^5 + \dots$$

(also independent of $\check{V}$) with

$$\begin{aligned} A_0 &= 16j^3 - 82944j^2 + 143327232j - 82556485632 \\ A_1 &= -1512j^3 + 5225472j^2 - 4514807808j. \end{aligned}$$

This is irreducible over $\mathbb{Q}(j)$. Thus $\check{\xi}$ has degree 6 over $\mathbb{Q}(j)$. But we saw that its degree is at least $\frac{3}{\pi^2}n^2$ over $\mathbb{Q}(j)$. So $n = 2, 3, 4$.

If $n = 2$ then its degree is at most 3. If $n = 3$ then its degree is at most 4. If $n = 4$ then its degree is at most 6, and we find $G(\check{\xi}) = 0$ where

$$G(\check{X}) = A_0\check{X}^6 + B\check{X}^5 + \dots$$

has the same coefficient of $\check{X}^6$ but

$$B = -540j^3 + 1866420j^2 - 1612431360j \neq A_1.$$

This gives a contradiction.

Generally the proof of Proposition 1 in the transcendental case provides an effective bound for the order of P if we have sufficient knowledge about the algebraic relations between the transcendental coefficients defining the curve C. Similarly as in [MZ2, p.471] the bound only depends on the degree of the algebraic variety W_0 defined at the beginning of subsection 3.12.1.

3.13 Split extensions

Here we prove the Theorem when $\mathcal{G} = \mathbb{G}_{\mathrm{a}} \times \mathcal{E}$ is split. Now we have a projection to $\mathbb{G}_{\mathrm{a}}$. This induces a regular function α on the curve $\mathcal{V}$. If P on $\mathcal{V}$ is torsion, then $\alpha(P)$ is torsion so zero. If α is not identically zero this gives at most finitely many P and so $\mathcal{V} \cap \mathcal{G}^{[2]}$ is contained in a finite union of subgroup schemes of $\mathcal{G}$ of codimension two. Otherwise $\mathcal{V}$ lies in $0 \times \mathcal{E}$ itself a group subgroup scheme of $\mathcal{G}$ of codimension one.

3.14 Non-split extensions again

The simple arguments of the preceding section can be combined with the Proposition to show that if $\mathcal{G}$ is non-split, and $\mathcal{V}$ is a curve in $\mathcal{G}$, then $\mathcal{V} \cap \mathcal{G}^{[2]}$ is contained in a finite union of (not necessarily flat) subgroup schemes of $\mathcal{G}$ of codimension two. We may follow the reduction in section 3.3, which allows us to assume $\mathcal{G} = G_\lambda$ and $\mathcal{V} = C$ with generic point P. If $q\pi(P) \neq O$ for every positive integer q, then the Proposition shows that $\mathcal{V} \cap \mathcal{G}^{[2]}$ is contained in a finite union of subgroup schemes of $\mathcal{G}$ of codimension two. So this time we assume $q\pi(P) = O$ for some such q. Thus $qP = \phi(\alpha)$ for some α which can also be identified with a rational function (on C). Now if $P(\mathbf{c})$ is torsion then by Lemma 3.9.1 it has order dividing q and

$$\phi(\alpha(\mathbf{c})) = O$$

forcing $\alpha(\mathbf{c}) = 0$. If α is not identically zero this gives at most finitely many $\mathbf{c}$ and so $\mathcal{V} \cap \mathcal{G}^{[2]}$ is contained in a finite union of subgroup schemes of codimension two. Otherwise $qP = O$ identically and $\mathcal{V}$ itself lies in a group subgroup scheme of $\mathcal{G}$ of codimension two.

In this situation we can write down α explicitly. Namely $P = \exp_\lambda(z_P, w_P)$ with $z_P = \omega_P/q$ for some period ω_P. Thus by (3.2.8)

$$(0,0,1,0,\alpha) = \phi(\alpha) = qP = \exp_\lambda(\omega_P, qw_P).$$

We cannot evaluate the exponential map (3.2.5),(3.2.6) directly at $z = \omega_P$, but by taking V/Y we can see that α is the limit as $z \to \omega_P$ of

$$qw_P + \zeta_\lambda(z) + 2\frac{(\wp_\lambda(z) + \frac{1}{3}(\lambda+1))^2}{\wp'_\lambda(z)}.$$

As $\zeta_\lambda(z) = \zeta_\lambda(z - \omega_P) + \eta_P$ for the quasi-period η_P corresponding to ω_P, a simple calculation shows that $\alpha = qw_P + \eta_P$. Using (3.5.6) and then $\omega_P = qz_P$ we end up thanks to Lemma 3.7.1 (which holds even if $q\pi(P) = O$ provided $q \neq 2$) with

$$\frac{\alpha}{q} \;=\; \lambda(1-\lambda)\frac{\xi'}{\eta} + \frac{\eta}{\xi - \lambda} + \mu$$

at least if $q \neq 2$. If $q = 2$ then ξ is equal to either $0, 1$ or λ and after a short calculation using $\mu = w_P + \zeta(z_P)$ we see that

$$\frac{\alpha}{2} = \mu$$

in this case.

In particular we can calculate α without having to multiply by q on the group, which may be arduous.

The example

$$P = (\sqrt{\lambda},\ i(\lambda - \sqrt{\lambda}),\ -\frac{i}{2}(\sqrt{\lambda} - 1),\ \frac{1}{2}\sqrt{\lambda}(\lambda + 1))$$

is no good because $4P = O$ identically (so all values of λ give torsion, and $\alpha = 0$). But for say

$$P = (\sqrt{\lambda},\ i(\lambda - \sqrt{\lambda}),\ -i(\lambda + \sqrt{\lambda}),\ \lambda^2)$$

with $4\pi(P) = O$ we find $\alpha = -2i(2\lambda + \sqrt{\lambda} + 1)$ and so only

$$\sqrt{\lambda} = \frac{-1 \pm \sqrt{-7}}{4}$$

gives torsion.

4 Appendix A

In this appendix we give some applications of the results from the last chapter. Beforehand we briefly introduce the theory of generalized Jacobians. This sets up the formalism to prove Theorem 4 in section 4.2 after providing some more background to the theory of elementary integration. Then in section 4.3 we prove Theorem 5 about Pell's equation in polynomials. Finally in section 4.4 we return to the context of Proposition 1 and we construct explicitly the curves C there corresponding to the theorems.

4.1 Generalized Jacobians

In this section we introduce the theory of generalized Jacobians of curves. Such a theory proved useful to treat classical problems as will be described in section 4.2 and 4.3. Additive extensions appear naturally as generalized Jacobians. This allows us to apply the main result of chapter 3 to prove Theorem 4 and 5.

For a more detailed treatment of the theory of generalized Jacobians we refer the reader to [Se].

4.1.1 Orders on a curve

Let $\mathcal{C}$ be a non-singular, projective and complete curve defined over an algebraically closed field K of characteristic 0. For each $P \in \mathcal{C}(K)$ we can define the ring $\mathcal{O}_P$ which is the ring of functions in $K(\mathcal{C})$ with no pole at P. Since $\mathcal{C}$ is non-singular this is always a local ring and the maximal ideal $\mathfrak{m}_P$ of $\mathcal{O}_P$ is principal. A function $t_P \in K(\mathcal{C})$ which generates $\mathfrak{m}_P$ is called a local uniformizer at P. For each non-zero element $f \in K(\mathcal{C})$ there is a unique integer n such that $f = t_P^n u$ where u is invertible in $\mathcal{O}_P$. This is all well-known and explained for example in [Se, p.7].

We can expand each $f \in K(\mathcal{C})$ into a Laurent series at P as follows. If $f \in \mathcal{O}_P$ we define $a_0 = f(P)$ and $a_1, \ldots, a_i, i \geq 1$ inductively by $f - \sum_{l=0}^{i} a_l t_P^l \in \mathfrak{m}_P^{i+1}$. This is well defined since $\mathfrak{m}_P^{i+1}/\mathfrak{m}_P^i$ is a vector space over K of dimension 1. We then define $l_P(f) = \sum_{l=0}^{\infty} a_l t_P^l \in K((t_p))$. If f is not in $\mathcal{O}_P$ then $1/f$ is and we can define $l_P(f) = 1/l_P(1/f)$. Thus for each $P \in \mathcal{C}(K)$ we get a well-defined map

$$l_P : K(\mathcal{C}) \longrightarrow K((t_P)) \tag{4.1.1}$$

which is in fact a field homomorphism. For non-zero f in $\mathcal{K}(\mathcal{C})$ and n as above we have

$$l_P(f) = \sum_{l=n}^{\infty} a_l t_P^l. \tag{4.1.2}$$

The integer n is called the order of f at P and we denote it by $\mathrm{ord}_P(f)$. From the discussion above it follows that ord_P defines a valuation on $K(\mathcal{C})$ equal to

$$\mathrm{ord}_P(f) = \min\{l \in \mathbb{Z}; a_l \neq 0\} \tag{4.1.3}$$

if $f \neq 0$ and for $f = 0$ we can set it formally equal to $+\infty$. The functions ord_P are related by

$$\sum_{P \in C(K)} \mathrm{ord}_P(f) = 0. \tag{4.1.4}$$

For a proof of the latter fact we refer to [Se, p.8, Proposition 1].

4.1.2 Divisors

We define the group $Div(\mathcal{C})$ to be the free abelian group generated by the points of $\mathcal{C}(K)$. Each element D of $Div(\mathcal{C})$ can be expressed as a (finite) sum

$$D = \sum_{P \in \mathcal{C}(K)} n_P(P), \quad n_p \in \mathbb{Z}$$

where $n_P = 0$ for all but finitely many P. The set of P where $n_P \neq 0$ is called the support $|D|$ of D. The degree function deg

$$\deg : Div(\mathcal{C}) \to \mathbb{Z}$$

defined by

$$\deg(D) = \sum n_P$$

is a group homomorphism between $Div(\mathcal{C})$ and $\mathbb{Z}$ and we define $Div_0(\mathcal{C})$ to be its kernel. With the valuation we defined in the last subsection we can define the divisor of a non-zero function f denoted by (f) as

$$(f) = \sum_{P \in \mathcal{C}(K)} \mathrm{ord}_P(f)(P).$$

The map from the multiplicative group $K(\mathcal{C})^*$ of $K(\mathcal{C})$ to $Div(\mathcal{C})$ sending f to (f) is a homomorphism from $K(\mathcal{C})^*$ to $Div(\mathcal{C})$ with kernel K^*. The image of $K(\mathcal{C})^*$

in $Div(\mathcal{C})$ is the group of principal divisors $\mathcal{P}(\mathcal{C})$ and by (4.1.4) it is a subgroup of $Div_0(\mathcal{C})$.

This makes it possible to consider the group $\mathcal{J}(\mathcal{C})$ defined by

$$\mathcal{J}(\mathcal{C}) = Div_0(\mathcal{C})/\mathcal{P}(\mathcal{C}).$$

This group has the fundamental property that for every curve $\mathcal{C}$ there exists a projective algebraic group $Jac(\mathcal{C})$ which is isomorphic to $\mathcal{J}(\mathcal{C})$. Moreover the isomorphism is given by extending a non-constant morphism g_0 from $\mathcal{C}$ to $Jac(\mathcal{C})$ [Se, p.2, Theorem 3] to $Div_0(\mathcal{C})$ by

$$\sum n_P(P) \longrightarrow \sum n_P g_0(P).$$

We denote the extension of g_0 to $Div_0(\mathcal{C})$ also by g_0. From the construction it follows that on $Jac(\mathcal{C})$ we have

$$\sum_{P \in \mathcal{C}(K)} \mathrm{ord}_P(f) g_0(P) = O$$

for all non-zero functions $f \in K(\mathcal{C})$.

If $\mathcal{C}$ is an elliptic curve E with identity element O, then $Jac(\mathcal{C})$ is isomorphic to E. An isomorphism is given by sending P in $E(K)$ to $(P) - (O)$ in $Div_0(E)$ and through this isomorphism we can identify E with $Jac(\mathcal{C})$. The above relation then becomes

$$\sum_{P \in E(K)} \mathrm{ord}_P(f) P = O \tag{4.1.5}$$

on E, for every non-zero $f \in K(E)$.

4.1.3 Modulus

We generalize the notion of Jacobian from the previous subsection. For this we first have to introduce the notion of a modulus $\mathcal{M}$ on $\mathcal{C}$.

This is the data of a finite (possibly empty) set of point S in $\mathcal{C}(K)$ and a postive integer s_P for every $P \in S$. It is often convenient to identify $\mathcal{M}$ with the divisor $\sum_{P \in S} s_P(P)$. We can define an equivalence relation on $K(\mathcal{C})^*$ by setting f equivalent to 1 if

$$\mathrm{ord}_P(f-1) \geq s_P, \text{ for all } P \in S$$

and write $f \equiv 1 \mod \mathcal{M}$ or that f is congruent to 1. If S is empty then the set of functions congruent to $1 \mod \mathcal{M}$ is just $K(\mathcal{C})$.

We can define the narrow class $[D]_{\mathcal{M}}$ of a divisor D in Div_0 to be the set of divisors $D' \in Div_0$ such that

$$D - D' = (f),$$
$$f \equiv 1 \mod \mathcal{M}.$$

We can restrict $Div_0(\mathcal{C})$ to the group $Div_{0,S}(\mathcal{C})$ of divisors D with support $|D|$ disjoint from S. The set of narrow classes $[D]_{\mathcal{M}}$ with $D \in Div_{0,S}(\mathcal{C})$ is a group $\mathcal{J}_{\mathcal{M}}(\mathcal{C})$.

By [Se, p.2, Theorem 3], for each modulus $\mathcal{M}$ on $\mathcal{C}$, there exists a commutative algebraic group $Jac_{\mathcal{M}}(\mathcal{C})$ and a morphism $g_{\mathcal{M}}$ from $\mathcal{C} \setminus S$ to $Jac_{\mathcal{M}}(\mathcal{C})$ such that the extension of $g_{\mathcal{M}}$ to $Div_{0,S}(\mathcal{C})$ defined by

$$Div_{0,S}(\mathcal{C}) \longrightarrow Jac_{\mathcal{M}}(\mathcal{C}) \tag{4.1.6}$$
$$g_{\mathcal{M}} : \sum n_p(P) \longrightarrow \sum n_P g_{\mathcal{M}}(P). \tag{4.1.7}$$

is surjective with kernel equal to the divisors of all functions $f \in K(\mathcal{C})$ congruent to $1 \mod \mathcal{M}$. Thus $g_{\mathcal{M}}$ induces an isomorphism from $\mathcal{J}_{\mathcal{M}}(\mathcal{C})$ to $Jac_{\mathcal{M}}(\mathcal{C})$. If S is empty then $Jac_{\mathcal{M}}(\mathcal{C})$ is just the usual Jacobian. This justifies the fact that $Jac_{\mathcal{M}}(\mathcal{C})$ is called the generalized Jacobian for general modulus $\mathcal{M}$.

There is a canonical map

$$\pi_{\mathcal{M}} : \mathcal{J}_{\mathcal{M}}(\mathcal{C}) \longrightarrow \mathcal{J}(\mathcal{C})$$

defined by sending the narrow class of a divisor D defined by $\mathcal{M}$ to the ordinary class in $Div_0(\mathcal{C})/\mathcal{P}(\mathcal{C})$. We denote the kernel of this map by $\mathcal{L}_{\mathcal{M}}$.

The map $\pi_{\mathcal{M}}$ induces a projection π of algebraic groups from $Jac_{\mathcal{M}}(\mathcal{C})$ to $Jac(\mathcal{C})$. The kernel of $\pi_{\mathcal{M}}$ is

$$\mathcal{L}_{\mathcal{M}} = \{[(f)]_{\mathcal{M}}; f \in K(\mathcal{C})^*,\ \mathrm{ord}_P(f) = 0 \text{ for all } P \in S\}$$

and it can be given the structure of a linear algebraic group $L_{\mathcal{M}} = \mathbb{G}_a^r \times \mathbb{G}_m^s$, where r, s are

$$r = \sum_P (s_P - 1),\ s = |S| - 1,$$

independent of the genus of $\mathcal{C}$ (see [Se, chapter V, §3]). This linear group $L_{\mathcal{M}}$ is isomorphic to the kernel of π as an algebraic group and we get an exact sequence of algebraic groups

$$0 \longrightarrow L_{\mathcal{M}} \longrightarrow Jac_{\mathcal{M}}(\mathcal{C}) \longrightarrow Jac(\mathcal{C}) \longrightarrow O.$$

This is again [Se, p.2, Theorem 3].

4.1.4 Examples

In order to provide the reader with some intuition for the construction of the generalized Jacobian we describe (the) two (easiest) examples. The structure of $L_{\mathcal{M}}$ is described in [Se, p.96] as a product of "local groups" and in [Se, Proposition 8] the structure of the local groups is determined. In this section we treat some specific moduli on an elliptic curve.

Let E be an elliptic curve with neutral element O. If we set $\mathcal{M} = 2O$, then $\mathcal{L}_{\mathcal{M}}$ is given by the narrow classes of the elements in the set

$$\{1 + ct_O \in K(\mathcal{C}); c \in K\}$$

where t_O as usual is a uniformizer at O.

If we multiply $f_1 = 1 + c_1 t_O, f_2 = 1 + c_2 t_O$ in $Div_{0,\mathcal{M}}$ we get the class of $1 + (c_1 + c_2)t_O$ and we see that the map sending $[1 + ct_O]_{\mathcal{M}}$ to c provides an isomorphism between $\mathcal{L}_{\mathcal{M}}$ and the additive group $\mathbb{G}_a$.

In fact $Jac_{\mathcal{M}}(E)$ is an additive extension of E. This is an algebraic group sitting inside an exact sequence

$$0 \longrightarrow \mathbb{G}_a \longrightarrow Jac_{\mathcal{M}}(E) \longrightarrow E \longrightarrow O.$$

Up to isomorphism (of algebraic groups) there are exactly two such groups. Either $Jac_{\mathcal{M}}$ is the product $\mathbb{G}_a \times E$ or it is non-split (see for example [CMZ, p.244]). In [Se, p.188, Proposition 15] it is shown that $Jac_{\mathcal{M}}$ is non-split.

We give a second example before finishing this subsection. For $\mathcal{M} = (P) + (Q)$ where $P \neq Q$, we see by normalizing at P that $\mathcal{L}_{\mathcal{M}}$ consists of the classes of functions f with expansion $l_P(f) = 1 + \dots$ at P and $l_Q(f) = c + \dots, c \neq 0$ at Q. It is easy to check as above that the map sending $[f]_{\mathcal{M}}$ to c provides an isomorphism between $\mathcal{L}_{\mathcal{M}}$ and $\mathbb{G}_m$. And in fact $Jac_{\mathcal{M}}(E)$ is a multiplicative extension of E (a semiabelian variety).

4.2 Elementary integration

In this section we give a brief introduction to the theory of elementary integration.

Intuitively “elementary functions” are the functions known from High-School mathematics such as polynomials, trigonometric functions, the log and the exp function. The theory of elementary integration can then be understood as the study of the question whether the primitive of a given elementary function is also elementary.

We give a rigorous definition of the adjective elementary and then prove some results using the theory of generalized Jacobians introduced in the previous section.

4.2.1 Definition

We start with a differential field $\mathcal{K}$ of characteristic 0. This is a field equipped with a derivation ∂. The kernel of ∂ is the field of constants of $\mathcal{K}$.

A differential field extension of $\mathcal{K}$ is a field $\mathcal{K}'$ which contains $\mathcal{K}$ with a derivation ∂' on $\mathcal{K}'$ such that the restriction of ∂' to $\mathcal{K}$ is equal to ∂. By abuse of notation we will just denote the derivation of the extension also by ∂.

We call a differential extension of $\mathcal{K}$ elementary if it is obtained as a finite tower of algebraic extensions and of extensions L/K of intermediate differential fields K, L where $L = K(y)$ with y such that either $\partial(y)/y = \partial x$ or $\partial(y) = \partial(x)/x$ for some $x \in K$. The former y can be informally thought of as $\exp(x)$ and the latter as $\log(x)$. We say that $f \in \mathcal{K}$ is elementary integrable (with respect to $\mathcal{K}$) if there exists g in an elementary extension of $\mathcal{K}$ such that $\partial g = f$.

In 1981 James Davenport made a very interesting claim about the elementary integrability of parametrized algebraic functions [Dave, p.90, Theorem 7]. This can be expressed formally in the following way.

Let $\mathcal{C}$ be an algebraic curve defined over a field k. Pick a non-constant function X in $k(\mathcal{C})$. Then $k(\mathcal{C})$ is a differential field with $\partial = \frac{d}{dX}$ (and field of constants k). Thus we can speak of the elementary integrability of any f in $k(\mathcal{C})$.

In particular this holds if $k = \mathbb{C}(\mathcal{V})$ is itself the function field of a curve $\mathcal{V}$ defined over $\mathbb{C}$.

But then we can specialize everything at a point v in $\mathcal{V}(\mathbb{C})$, at least for at most finitely many exceptions v. We get a specialized curve $\mathcal{C}_v$ over $\mathbb{C}$ and a specialized f_v in $\mathbb{C}(\mathcal{C}_v)$, which is also a differential field (now with the field of constants $\mathbb{C}$). Thus we can speak of the elementary integrability of f_v.

Davenport's Claim: *As above suppose that f is not elementary integrable in $\mathbb{C}(\mathcal{V})(\mathcal{C})$. Then there are at most finitely many $v \in \mathcal{V}(\mathbb{C})$ such that f_v is elementary integrable in $\mathbb{C}(\mathcal{C}_v)$.*

Masser and Zannier have recently proved this claim in [MZ6] "over $\overline{\mathbb{Q}}$"; that is when $\mathcal{V}$ is defined over $\overline{\mathbb{Q}}$ and f is in $\overline{\mathbb{Q}}(\mathcal{V})$.

It seems very likely that our Theorem 3 will be the key tool in proving the full Davenport's Claim "over $\mathbb{C}$" when $\mathcal{C}$ is an elliptic curve. In the next section we will illustrate this by the example $f = \frac{1}{(X-2)\sqrt{X(X-1)(X-\lambda)}}$ with $\mathcal{C}$ the Legendre elliptic curve $Y^2 = X(X-1)(X-\lambda)$ over $\mathbb{C}(\lambda) = \mathbb{C}(\mathcal{V})$ for $\mathcal{V} = \mathbb{A} \setminus \{0,1\}$. Then we obtain the following unconditional finiteness statement.

Theorem 4. *There are at most finitely many $\lambda \in \mathbb{C}$ such that*

$$\frac{1}{(X-2)\sqrt{X(X-1)(X-\lambda)}}$$

is elementary integrable.

In fact Liouville showed how to avoid the tower of extensions. He proved that if the field of constants $\mathcal{K}_0$ of $\mathcal{K}$ is algebraically closed, then f in $\mathcal{K}$ is elementary integrable if and only if there are $g_0, g_1, \ldots, g_m$ in $\mathcal{K}$ and $c_1, \ldots, c_m$ in $\mathcal{K}_0$ such that

$$f = \partial g_0 + \sum_{i=1}^{m} c_i \frac{\partial g_i}{g_i}.$$

In the situation of $\mathcal{K} = k(\mathcal{C})$ above this amounts in terms of differentials to

$$f dX = dg_0 + \sum_{i=1}^{m} c_i \frac{dg_i}{g_i}.$$

4.2.2 Proof of Theorem 4

For the proof we may assume that $\lambda \neq 0, 1$, so $f_\lambda = \frac{1}{(X-2)Y}$ is a function on the Legendre curve

$$E_\lambda : Y^2 = X(X-1)(X-\lambda).$$

We will prove that each λ such that f_λ is elementary integrable gives rise to a torsion point on a fixed curve in a non-split additive extension of E_λ. Then we can conclude with the main result of chapter 3 that there are at most finitely many such complex λ.

If f_λ is elementary integrable then by Liouville

$$f_\lambda dX = dg_0 + \sum_{i=1}^{m} c_i \frac{dg_i}{g_i} \tag{4.2.1}$$

now for $g_0, g_1, \ldots, g_m$ in $\mathbb{C}(E_\lambda)$ and $c_1, \ldots, c_m$ in $\mathbb{C}$. The differential $\xi_\lambda = f_\lambda dX = \frac{dX}{(X-2)Y}$ has a pole at $P_\lambda = (2, \sqrt{4-2\lambda})$ and $-P_\lambda$ of order 1 and a zero of order 2 at O and no other poles or zeros. If g_0 is non-constant then dg_0 has at least one pole of order at least 2 but $\sum_{i=1}^{m} c_i dg_i/g_i$ has poles of order at most 1. By comparing poles on both sides of (4.2.1) we deduce that g_0 is constant and $dg_0 = 0$.

We take m in (4.2.1) minimal. Clearly $m \geq 1$. This implies that $c_1, \ldots, c_m$ are linearly independent over $\mathbb{Q}$; for example if $c_m = c_1 + \cdots + c_{m-1}$ the sum on the right-hand side of (4.2.1) is $\sum_{i=1}^{m-1} c_i d\tilde{g}_i/\tilde{g}_i$ with $\tilde{g}_i = g_i g_m$. Now any pole or zero of g_i at some Q gives rise to a pole of dg_i/g_i of residue $\mathrm{ord}_Q(g_i)$. So we get a total residue $\sum_{i=1}^{m} c_i \mathrm{ord}_Q(g_i)$. If $Q \neq \pm P_\lambda$ this has to vanish. But then the linear independence implies $\mathrm{ord}_Q(g_i) = 0$ $(i = 1, \ldots, m)$.

Thus the only possible poles or zeros of g_i are $\pm P_\lambda$. By (4.1.4) we deduce for the divisor $(g_i) = d_i(P_\lambda) - d_i(-P_\lambda)$ $(d_i \in \mathbb{Z})$. It follows that the multiplicative rank of $g_1, \ldots, g_m$ modulo constants is at most 1, and so it is clearly 1. Adjusting by constants, we can assume for example $g_i = g_1^{a_i}$ $(i = 1, \ldots, m)$ for integers a_i and then this leads to $m = 1$ in (4.2.1). Thus we can write

$$\xi_\lambda = c\frac{dg}{g}$$

for some $g \in \mathbb{C}(E_\lambda)$ and c in $\mathbb{C}$.

We know from the above discussion that the divisor of g is of the form

$$(g) = d(P_\lambda) - d(-P_\lambda) \tag{4.2.2}$$

for some non-zero integer d. Further since ξ_λ has a zero of order 2 at O also dg has a zero of order 2 at O and there exists $a \in \mathbb{C}^*$ such that $g - a$ vanishes of order at least 3 at O. After replacing g with $(1/a)g$ we get

$$\mathrm{ord}_O(g-1) \geq 2. \tag{4.2.3}$$

Thus the narrow class of the divisor $(P_\lambda) - (-P_\lambda)$ with respect to the modulus $2O$ is a torsion point of order dividing d in $\mathcal{J}_{2O}(E_\lambda)$.

Now let us temporarily think of λ as being generic over $\mathbb{C}$ and let J_λ be the additive extension of E_λ defined by the modulus $\mathcal{M} = 2O$. Then J_λ defines a non-split additive extension of the family E_λ and together with the projection map to $\mathbb{C} \setminus \{0, 1\}$ a group scheme $\mathcal{G}$. The class $[(P_\lambda) - (-P_\lambda)]_{\mathcal{M}}$ is the generic point of a curve $\mathcal{C}_1$ in $\mathcal{G}$.

Now going back to our special λ in (4.2.1), we see that $Q_1 = [(P_\lambda) - (-P_\lambda)]_{\mathcal{M}}$ is torsion and so in $\mathcal{C}_1 \cap \mathcal{G}^{[2]}$ in the notation of Theorem 3. It follows from that result that Q_1 is contained in one of a finite number of subgroup schemes of $\mathcal{G}$ of positive codimension. As $\mathcal{G}$ is non-split the only such subschemes are torsion translates $T + \mathbb{G}_a$ of $\mathbb{G}_a$, with say $qT = O$ for some fixed positive integer q. But then we would have $q\pi(Q_1) = O$ for the projection to E_λ. Here $\pi(Q_1)$ is the ordinary class of $(P_\lambda) - (-P_\lambda)$ which is identified with $2P_\lambda$. So in E_λ we get $2qP_\lambda = O$. We remarked in section 3.1 that P_λ is not identically torsion so we get the finiteness of λ.

The reader will check without difficulty that the whole proof works also with

$$\frac{1}{(X-\pi)\sqrt{X(X-1)(X-\lambda)}}$$

analogously to the π-examples exhibited in section 3.1. This time it is obvious that the corresponding point $(\pi, \sqrt{\pi(\pi-1)(\pi-\lambda)})$ is not torsion identically.

4.3 Pell's equation in polynomials

In this section we study certain Pell's equation in polynomials. Now let $\mathcal{K}$ be a field of characteristic zero. We call a polynomial $D \in \mathcal{K}[X]$ Pellian (with respect to $\mathcal{K}$) if there exist A, B in $\overline{\mathcal{K}}[X]$ such that

$$A^2 - DB^2 = 1,\ B \neq 0.$$

This is equivalent to finding a non-trivial unit $A+YB$ in the ring $\overline{\mathcal{K}}[X, Y]/(Y^2-D)$. This problem was studied at least since the 19th century and is closely connected to certain abelian integrals. For a more precise and systematic treatment of the problem and its history we refer the reader to [Za2].

Let $\mathcal{V}$ be an algebraic curve defined over $\mathbb{C}$. Thus we can speak of the Pellianity of any $D \in \mathbb{C}(\mathcal{V})[X]$. And for any $v \in \mathbb{C}(\mathcal{V})$ (with at most finitely many exceptions) we can specialize to $D_v \in \mathbb{C}[X]$ and so speak of the Pellianity of D_v.

The natural analogue of Davenport's Claim, that if D is not Pellian over $\mathbb{C}(\mathcal{V})$ then there are at most finitely many $v \in \mathcal{V}(\mathbb{C})$ such that D_v is Pellian over $\mathbb{C}$, is false. A counterexample is $D = X^6 + X^2 + t$ [Za1, p.86] arising from elliptic factors of the Jacobian. A much more subtle counterexample comes from [B3]

$$D = X^2(X^4 + tX^3 - tX - 1) = X^2(X^2 - 1)(X^2 + tX + 1)$$

arising from Ribet curves (as described in [B2]) in multiplicative extensions of elliptic curves.

It seems likely that there are no such counterexamples when D is sextic with a triple zero. In the next section we will illustrate this with the example $D = X^3(X^3 + X + t)$ with $\mathbb{C}(t) = \mathbb{C}(\mathcal{V})$ for $\mathcal{V} = \mathbb{A}$. Then we obtain the following unconditional finiteness statement.

Theorem 5. *There are at most finitely many complex t such that*

$$D_t = X^3(X^3 + X + t)$$

is Pellian.

4.3.1 Proof of Theorem 5

Let $t \in \mathbb{C}$ be such that there exist $A, B \neq 0$ in $\mathbb{C}[X]$ such that

$$A^2 - D_t B^2 = 1. \tag{4.3.1}$$

We set $d = \deg(A)$ to be the degree of A and then necessarily $\deg(B) = d - 3$. From (4.3.1) follows that the function $f = A + XYB$ on the curve

$$Y^2 = X(X^3 + X + t) \tag{4.3.2}$$

has zeros and poles supported at the points at infinity corresponding to $X = \infty$.

The points at infinity then are P_∞^+, P_∞^- (on a suitable non-singular model) and as above we can assume that

$$(f) = d(P_\infty^+) - d(P_\infty^-).$$

From (4.3.1) we deduce that X^3 divides $(A-1)(A+1)$ and by possibly changing A to $-A$ we can assume that X^3 divides $A-1$. The function X has a zero of order 2 at $P_0 = (0,0)$ and the function Y a zero of order 1. Thus

$$\mathrm{ord}_{P_0}(f-1) \geq \min\{\mathrm{ord}_{P_0}(A-1), \mathrm{ord}_{P_0}(XYB)\} \geq 3.$$

So we could use the modulus $3P_0$. However as in the previous section (see 4.2.3) $\mathcal{M} = 2P_0$ suffices and it can be shown in both cases that considering $\mathcal{M} = 3P_0$ does not provide any new information. If we temporarily assume t to be generic over $\mathbb{C}$ then $Jac_{\mathcal{M}}(\mathcal{E})$ defines an additive extension of the Jacobian of a suitable non-singular projective model $\mathcal{E}$ of (4.3.2). The curve defined by (4.3.2) has genus 1 so $Jac_{\mathcal{M}}(\mathcal{E})$ defines a non-split additive extension of an elliptic family. Together with the projection map defined by t it is a group scheme $\mathcal{G}$ over the base curve $\mathbb{A} \setminus \{0, \pm\sqrt{-4/27}\}$ and the class $[(P_\infty^+) - (P_\infty^-)]_{\mathcal{M}}$ is the generic point of a curve $\mathcal{C}_2$ in $\mathcal{G}$.

Now going back to our special t in (4.3.1) it follows from the above discussion that $Q_2 = [(P_\infty^+) - (P_\infty^-)]_{\mathcal{M}}$ is torsion and so in $\mathcal{C}_2 \cap \mathcal{G}^{[2]}$. Thus as in subsection 4.2.2 we deduce that $q((P_\infty^+) - (P_\infty^-)) = O$ for the ordinary class.

To go further we use $\hat{X} = 1/X$ and $\hat{Y} = (1/\sqrt{t})Y/X^2$ to get a non-singular (affine) model $\hat{E}_t$ defined by

$$\hat{Y}^2 = \hat{X}^3 + t^{-1}\hat{X}^2 + t^{-1}$$

for $t(4+27t^2) \neq 0$. Then $P_\infty^\pm$ go to $\pm\hat{P}_t$ for $\hat{P}_t = (0, \sqrt{1/t})$. Thus as above it suffices to prove that $\hat{P}_t$ is not identically torsion.

However we check at $t = \frac{1}{9}$ that

$$4\hat{P}_{\frac{1}{9}} = \left(\frac{765}{4}, \frac{21651}{8}\right)$$

and so by Lutz-Nagell $\hat{P}_{\frac{1}{9}}$ is not torsion on $\hat{E}_{\frac{1}{9}}$; thus $\hat{P}_t$ is not torsion on $\hat{E}_t$ for t generic over $\mathbb{C}$. This concludes the proof of Theorem 5.

Again the reader can easily check that the whole proof works with

$$(X-\pi)^3(X^3+X+t)$$

as exhibited in section 3.1. One ends up with $\left(0, \sqrt{\frac{1+\pi^2-\pi^3 t}{t}}\right)$ on a curve more complicated than $\hat{E}_t$, and again the π prevents torsion.

4.4 Reduction to G_λ in $\mathbb{A}^4$

In this section we concentrate on the case of an additive extension of the Legendre family. For an elliptic curve over $\mathbb{C}$ the order function can be defined in terms of classical elliptic functions. We briefly outline how and then indicate how a concrete embedding of an additive extension can be obtained using the Weierstrass $\wp$ and ζ function. This then leads to an explicit description of the generalized Jacobian $Jac_{2O}(E_\lambda)$ and a map g_{2O}.

We then use this explicit description to calculate the curves in Proposition 1 corresponding to Theorems 4 and 5.

We work over an elliptic curve E defined over an algebraically closed field K of characteristic 0. Then E has a Weierstrass model of the form

$$E : \tilde{Y}^2 = 4\tilde{X}^3 - g_2\tilde{X} - g_3,\ g_2, g_3 \in K. \tag{4.4.1}$$

If $K = \mathbb{C}$ then $\tilde{X}, \tilde{Y}$ are parametrized by the Weierstrass functions $\wp, \wp'$ associated to the lattice generated by the invariant differential $\frac{d\tilde{X}}{\tilde{Y}}$. It is well-known that $\wp, \wp'$ are meromorphic functions with a Laurent expansion (at 0) of the form

$$\wp(z) = \frac{1}{z^2} + \sum_{i=0}^{\infty} s_i z^i, \tag{4.4.2}$$

$$\wp'(z) = -\frac{2}{z^3} + \sum_{i=0}^{\infty}(i+1)s_{i+1}z^i, \quad s_i \in \mathbb{Q}(g_2, g_3). \tag{4.4.3}$$

We can interpret this as formal and define a map

$$\tilde{l}_O : K(\tilde{X}, \tilde{Y}) \to K((z))$$

from the function field $K(\tilde{X}, \tilde{Y})$ of E to the field of formal Laurent series over K by setting

$$\tilde{l}_O(\tilde{X}) = \frac{1}{z^2} + \sum_{i=0}^{\infty} s_i z^i,\ \tilde{l}_O(\tilde{Y}) = -\frac{2}{z^3} + \sum_{i=0}^{\infty}(i+1)s_{i+1}z^i.$$

For an element $\phi \in K((z))$ we define $a_i(\phi)$ to be the coefficient of z^i in the Laurent series of ϕ. We can then define the order of ϕ by

$$\operatorname{ord}(\phi) = \min_{i\in\mathbb{Z}}\{a_i \neq 0\}$$

From basic properties of Laurent series follows that ord is a valuation on $K((z))$ if we formally set $\operatorname{ord}(0) = +\infty$. With the differential equation for $\wp$

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3$$

we can define the higher derivatives of $\wp$ as polynomials of $\wp, \wp'$ with coefficients in the field $\mathbb{Q}(g_2, g_3)$. Hence for any non-zero point $(x_P, y_P) \in E(K)$ we can define formal Laurent series in $K((z))$ (actually a Taylor series), by

$$\tilde{l}_P(\tilde{X}) = \sum_{i=0}^{\infty} \frac{\wp^{(i)}(x_P)}{i!} z^i,$$
$$\tilde{l}_P(\tilde{Y}) = \sum_{i=0}^{\infty} \frac{\wp^{(i+1)}(x_P)}{i!} z^i.$$

As with $\tilde{l}_O$ we can extend this to a map

$$\tilde{l}_P : K(\tilde{X}, \tilde{Y}) \to K((z)).$$

Now for each point $P \in E(K)$ (with O the point at infinity) this defines a valuation on $K(\tilde{X}, \tilde{Y})$ through

$$\mathrm{ord}_P(f) = \mathrm{ord}(\tilde{l}_P(f)).$$

It is well-known that this valuation ord_P is the same as ord_P defined in subsection 4.1.1 for $\mathcal{C} = E$. If K is a subfield of $\mathbb{C}$ then from the theory of elliptic functions it follows directly that this valuation has the property

$$\sum_{P \in E(K)} \mathrm{ord}_P(f) = 0, \quad \sum_{P \in E(K)} \mathrm{ord}_P(f) P = O \tag{4.4.4}$$

where the right sum is defined by addition on E.

If we want to pass to an additive extension of E the Weierstrass ζ function enters the picture. It is defined to be the unique odd meromorphic function such that $\zeta' = -\wp$.

It has the property that for a basis ω_1, ω_2 of the lattice Λ associated to $\wp$ we have $\zeta(z + a_1\omega_1 + a_2\omega_2) = \zeta(z) + a_1\eta_1 + a_2\eta_2$ for $a_1, a_2 \in \mathbb{Z}$, where $\eta_1 = 2\zeta(\omega_1/2), \eta_2 = 2\zeta(\omega_2/2)$ are quasi-periods of ζ. Now setting $\tilde{U} = \zeta(z) + w,\ \tilde{V} = (w + \zeta(z))\wp'(z) + 2\wp^2(z)$ we get a map from $\mathbb{C}^2 \setminus (\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) \times \mathbb{C}$ to $\mathbb{P}_4$ sending (z, w) to $(1, \tilde{X}, \tilde{Y}, \tilde{U}, \tilde{V})$ and $\tilde{U}, \tilde{V}$ satisfy

$$\tilde{V} - \tilde{Y}\tilde{U} = 2\tilde{X}^2.$$

It is easy to check that this map is invariant under translations by the group $\mathbb{Z}(\omega_1, -\eta_1) + \mathbb{Z}(\omega_2, -\eta_2)$. We can extend the above map to a map from $\mathbb{C}^2$ to $\mathbb{P}_4(\mathbb{C})$ (if necessary using the sigma function) and the image describes a quasi-projective subvariety G of $\mathbb{P}_4$. With the addition on $\mathbb{C}^2$ this map transports a group structure to G with a natural projection π down to E given by the projection from $\mathbb{C}^2$ to $\mathbb{C}$ sending (z,w) to z. So we get an exponential map exp between $\mathbb{C}^2$ and G inducing an isomorphism between $\mathbb{C}^2/(\mathbb{Z}(\omega_1,-\eta_1)+\mathbb{Z}(\omega_2,-\eta_2))$ and G.

We can further check directly that the set $0\times\mathbb{C}$ is mapped to an affine line in $\mathbb{P}_4$ and the additive group $0\times\mathbb{C}$ maps isomorphically to an additive group on this line. This line is the kernel of the projection π and G is an additive extension of E. As pointed out in [CMZ] (see (3.11) on p. 251 for the uniformization), where all of this was outlined in more detail, this extension is non-split.

We next construct the map $g = g_{\mathcal{M}}$ in (4.1.7) for $\mathcal{M} = 2O$ and $\mathcal{C} = E$. Actually it is easy to define g on $E \setminus O$ simply by

$$g(\tilde{X},\tilde{Y}) = (\tilde{X},\tilde{Y},0,2\tilde{X}^2). \tag{4.4.5}$$

This induces a map $\overline{g}$ on the tangent spaces defined by

$$\overline{g}(z) = (z,-\zeta(z)). \tag{4.4.6}$$

We see from (4.4.6) that g is odd in the sense that

$$g(P) = -g(-P)$$

for all $P \neq O$ in E.

Building on a note of Masser on elementary integration we now show that if f_0 is in $\mathbb{C}(E)$ congruent to $1 \mod 2O$ then

$$\sum_{O\neq P\in E(\mathbb{C})} \mathrm{ord}_P(f_0)g(P) = O$$

in G; this shows that the extension to $Div_{0,O}(E)$ is well-defined on narrow classes. But it is hardly any more work to establish the isomorphism property after (4.1.7).

Lemma 4.4.1. *The extension of g to $Div_{0,O}(E)$ induces an isomorphism from $\mathcal{J}_{2O}$ to G.*

Proof. Let $\mathbb{Z}\omega_1+\mathbb{Z}\omega_2$ be the lattice of E as above with $\Im(\omega_2/\omega_1)>0$ and η_1,η_2 the associated quasi-periods of ζ. Thus $\mathbb{Z}(\omega_1,-\eta_1)+\mathbb{Z}(\omega_2,-\eta_2)$ is the kernel of the exponential map of G. Now let $f\in\mathbb{C}(\tilde{X},\tilde{Y})$ be such that $f(O)=1$ and let $P_1,\ldots,P_n$ be the set of its poles and zeros with $m_1=\mathrm{ord}_{P_1}(f),\ldots,m_n=\mathrm{ord}_{P_n}(f)$. Further let $u_1,\ldots,u_n$ in $\mathbb{C}$ be such that

$$(\wp(u_i),\wp'(u_i)) = P_i,\ i=1,\ldots,n.$$

We can pick $z_0 \in \mathbb{C}$ with

$$\mathcal{F} = \{z_0 + t_1\omega_1 + t_2\omega_2;\ t_1, t_2 \in \mathbb{R}, 0 \le t_1, t_2 < 1\}$$

such that $\partial\mathcal{F} \cap \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ is empty and such that we can pick $u_1, \dots, u_n$ as above in the interior of $\mathcal{F}$ and such that 0 is the only lattice point in $\mathcal{F}$. We define the meromorphic function ϕ by

$$\phi(z) = f(\wp(z), \wp'(z)).$$

Then ϕ has zeroes and poles $u_1, \dots, u_n$ in $\mathcal{F}$ with $m_i = \mathrm{ord}_{u_i}\phi$ in the usual analytical sense.

We now repeat the standard argument from elliptic function theory to obtain an analytic version of the second equation in (4.4.4).

By the residue theorem the integral along $\partial\mathcal{F}$ (with the usual orientation) of $z\frac{\phi'}{\phi}$ is equal to

$$I_1 = \frac{1}{2\pi i}\int_{\partial F} z\frac{\phi'}{\phi}dz = \sum_{i=1}^{n} m_i u_i.$$

If we integrate along the two pairs of opposite sides of ∂F we see that $I_1 \in \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. More precisely using that ϕ is an elliptic function we get the following equalities

$$\begin{aligned}\int_{z_0+\omega_1}^{z_0+\omega_1+\omega_2} z\frac{\phi'}{\phi}dz &= \int_{z_0}^{z_0+\omega_2} z\frac{\phi'}{\phi}dz + \omega_1\int_{z_0}^{z_0+\omega_2}\frac{\phi'}{\phi}dz\\ \int_{z_0+\omega_1+\omega_2}^{z_0+\omega_2} z\frac{\phi'}{\phi}dz &= \int_{z_0+\omega_1}^{z_0} z\frac{\phi'}{\phi}dz + \omega_2\int_{z_0+\omega_1}^{z_0}\frac{\phi'}{\phi}dz.\end{aligned}$$

For the last two integrals on the right hand side we get

$$\begin{aligned}\frac{1}{2\pi i}\int_{z_0}^{z_0+\omega_2}\frac{\phi'}{\phi}dz &= \frac{1}{2\pi i}\int_{z_0}^{z_0+\omega_2}\frac{d}{dz}\log(\phi(z))dz = n_1 \in \mathbb{Z}\\ \frac{1}{2\pi i}\int_{z_0+\omega_1}^{z_0}\frac{\phi'}{\phi}dz &= \frac{1}{2\pi i}\int_{z_0+\omega_1}^{z_0}\frac{d}{dz}\log(\phi(z))dz = n_2 \in \mathbb{Z},\end{aligned}$$

where the last equalities result from the fact that the image of the lines from z_0 to $z_0 + \omega_1$ and $z_0 + \omega_2$ map to closed paths under ϕ and $n_1, -n_2$ are their winding number around 0.

In conclusion we find

$$\sum_{i=1}^{n} m_i u_i = n_1 \omega_1 + n_2 \omega_2.$$

Now following the note of Masser mentioned above and departing from standard, we consider the integral $I_2 = \frac{1}{2\pi i} \int_{\partial \mathcal{F}} \zeta \frac{\phi'}{\phi} dz$. Note that by construction ζ has exactly one pole of order 1 at 0 with residue 1 and no other poles in $\mathcal{F}$. With the residue theorem we get

$$I_2 = \sum_{i=1}^{n} m_i \zeta(u_i) + \phi'(0).$$

Next using $\zeta(z + \omega_1) = \zeta(z) + \eta_1$ and $\zeta(z + \omega_2) = \zeta(z) + \eta_2$ (the quasi-periodicity of $\zeta(z)$ instead of that of z) we get with the same arguments as for I_1 that integrating along opposite sides yields $I_2 = n_1 \eta_1 + n_2 \eta_2$. Thus

$$\sum_{i=1}^{n} m_i (u_i, -\zeta(u_i)) = (0, \phi'(0)) + n_1(\omega_1, -\eta_1) + n_2(\omega_2, -\eta_2). \tag{4.4.7}$$

Now by applying the exponential map to (4.4.7) and taking $f \equiv 1 \mod 2O$, so that $\phi'(0) = 0$, we see that $g((f)) = O$. Thus g is well-defined on the quotient $\mathcal{J}_{2O}(E)$.

To prove injectivity we first note that $\pi(g(P)) = P$ for all $P \neq O$ on E. Now take $D = \sum n_P(P)$ with $g(D) = O$. Then $\sum n_P g(P) = O$ in G, and applying π gives

$$O = \sum n_P \pi(g(P)) = \sum n_P P.$$

As $\sum n_P = 0$, it follows from well-known elliptic curve theory that $D = (f)$ is principal. Now (4.4.7) shows that $\exp(0, \phi'(0)) = O$ in G. Looking at the periods we deduce that $\phi'(0) = 0$. Thus $f \equiv 1 \mod 2O$ and D is zero in the quotient.

To prove surjectivity (which looks slightly unlikely due to the mysterious 0 in (4.4.5) above) take any Π_0 in G in the kernel of π, so that $\Pi_0 = \exp(0, c)$ for some $c \in \mathbb{C}$. Then taking $f = 1 - 2c\frac{X}{Y}$ in (4.4.7) we find from (4.4.2) and (4.4.3) that $\phi = 1 + cz + \ldots$ and so $g((f)) = \Pi_0$. So at least we have surjectivity on the kernel of π.

Now take Π in G not in the kernel of π. Then $P = \pi(\Pi) \neq O$ and we can find Q in E with $2Q = P$. For $D = (Q) - (-Q)$ in $Div_{0,O}(E)$ we compute (using that g is odd)

$$g(D) = 2g(Q) = g(P)$$

so $\pi(g(D)) = P = \pi(\Pi)$. Thus $g(D) - \Pi$ is in the kernel of π and so by the above is $g((f))$. Therefore

$$\Pi = g(D - (f))$$

and this completes the proof of surjectivity. □

It is easy to obtain the analogues of all this for the Legendre model E_λ and the associated G_λ of chapter 3. Using section 3.2 and (3.1.4) we find that the corresponding g_λ is given by

$$g_\lambda(X, Y) = (X, Y, 0, X^2) \tag{4.4.8}$$

and is again odd.

Next we return to the point P_λ from subsection 4.2.2.

If $\lambda \in \mathbb{C} \setminus \{0, 1\}$ is such that f is elementary integrable, then there exists $g \in \mathbb{C}(E_\lambda)$ congruent to $1 \mod 2O$ with divisor equal to

$$(g) = d(P_\lambda) - d(-P_\lambda)$$

for some positive integer d. This implies together with the fact that g_λ is odd that

$$2dg_\lambda(P_\lambda) = O$$

on G_λ. Thus the point

$$(2, \sqrt{4 - 2\lambda}, 0, 4)$$

is torsion. This is the point given in (3.1.7) of the introduction of chapter 3. We have already remarked there that P_λ is not identically torsion. Thus we could deduce directly from Proposition 1 that there are at most finitely many complex $\lambda \neq 0, 1$ such that $g_\lambda(P_\lambda)$ is torsion on G_λ and therefore Theorem 4.

In order to treat the point P_∞ from subsection 4.3.1 we have to pass to the Legendre family first. We have already shown how to pass from the initial curve to the point $\hat{P}_t$ on $\hat{E}_t$.

It can be checked that if we pass from $\hat{E}_t$ to E_λ, where by consideration of j-invariant we must have

$$\frac{256(\lambda^2 - \lambda + 1)^3}{\lambda^2(1 - \lambda)^2} = -\frac{256}{t^2(27t^2 + 4)},$$

then the point $\hat{P}_t$ passes to $\tilde{P}_\lambda = (\xi, \eta, \mu, \nu)$ where $3\xi^2 - 2(\lambda+1)\xi + \lambda = 0$ as well as the usual equations

$$\eta^2 = \xi(\xi-1)(\xi-\lambda),\ \mu = 0,\ \nu = \xi^2$$

arising from (4.4.8). The relation between t and λ is a bit messy.

As a matter of fact the curve C parametrized by $(\xi, \eta, \mu, \nu, \lambda)$ is of genus 0, for example with the equations

$$\xi = \frac{1-u^2}{2},\ \eta = \frac{u^4-1}{4u},\ \mu = 0,\ \nu = \frac{(1-u^2)^2}{4},\ \lambda = -\frac{(u^2-1)(3u^2+1)}{4u^2}.$$

Now each value of t gives rise to several values of u; first the roots of

$$(27t^2+4)u^{12} + (27t^2-8)u^8 + (9t^2+4)u^4 + t^2 = 0$$

and then the $u' = \sqrt{3}/u$.

Thus again we could deduce Theorem 5 from Proposition 1.

5 Appendix B

In this short appendix we give an application of Theorem 1 to the theory of good reduction of Lattès maps. After a brief introduction into the subject we give the proof of Proposition 2, which improves Proposition 6.55 in [Si4, p.362] in that it removes the condition on m there.

5.1 Good reduction of flexible Lattès maps

Recall that a rational map $\phi\colon \mathbb{P}_1 \to \mathbb{P}_1$ is called a *Lattès map* if there exists an elliptic curve E, a morphism $\Phi\colon E \to E$, and a finite separable covering $\pi\colon E \to \mathbb{P}_1$ such that the map ϕ fits in the following diagram

$$\begin{tikzcd} E \arrow[r, "\Phi"] \arrow[d, "\pi"'] & E \arrow[d, "\pi"] \\ \mathbb{P}_1 \arrow[r, "\phi"] & \mathbb{P}_1. \end{tikzcd} \tag{5.1.1}$$

The study of these type of maps has a long history. See [Mil] for an introduction to Lattès maps.

From an arithmetical point of view they are important because information about preperiodic points of a Lattès map associated to a multiplication by n-map $[n]\colon E \to E$ gives information about the torsion points of E.

From an analytic point of view they are important because they are postcritically finite maps, i.e. the set of critical points is contained in the set of preperiodic points. In other words the full forward orbit of each critical point is finite. See [Si4, Chapter 6] for more information about this. Over $\mathbb{C}$, the study of the forward orbits of the critical points is very important because it gives information about the dynamical behavior of a holomorphic map. Furthermore, the family of Lattès maps represents a very exceptional set of postcritically finite maps (see [BBLPP, Thurston's Rigidity]).

Following Milnor's definitions in [Mil], we can divide Lattès maps into two groups: the flexible Lattès maps and the rigid Lattès maps. A flexible Lattès map is characterized by the property that by varying the elliptic curve E continuously we obtain other Lattès maps which are not conformally conjugate to it. More practically, it is a map as in diagram (5.1.1) where the map Φ is of the form $\Phi(P) = [n](P) + Q$ for $n \in \mathbb{Z}$, $Q \in E$ and π is a double covering with $\pi(P) = \pi(-P)$ for all $P \in E$. A Lattès map which is not flexible is called a rigid Lattès map.

Let K be a field equipped with a discrete valuation v and k the respective residue field. Further let $\phi\colon \mathbb{P}_1 \to \mathbb{P}_1$ be a morphism defined over K. We use the usual definition (as on p.6 of the introduction) of good reduction of ϕ modulo v as given in [Si4, p.58]. Good reduction is equivalent to the existence of a morphism $\phi_v\colon \mathbb{P}_1 \to \mathbb{P}_1$ defined over k that fits in the following commutative diagram:

$$\begin{tikzcd}
\mathbb{P}_1(\overline{K}) \arrow[r, "\phi"] \arrow[d, "\sim"'] & \mathbb{P}_1(\overline{K}) \arrow[d, "\sim"] \\
\mathbb{P}_1(\bar{k}) \arrow[r, "\phi_v"] & \mathbb{P}_1(\bar{k})
\end{tikzcd}$$

where $\tilde{}$ denotes the reduction modulo v map and $\bar{k}, \bar{K}$ are suitable algebraic closures of the fields K, k respectively where we can take any extension of v to $\bar{K}$. From [Si4, Theorem 2.18] follows the existence of such a ϕ_v and if ϕ has bad reduction at v from the vanishing of the resultant follows that we can find two distinct points in $\overline{K}$ which are equal modulo v but are sent to two points which are distinct modulo v. This then clearly hurts the commutativity of the diagram.

As an application of Theorem 1 and its generalization to the Tate form in section 2.8, we prove the following proposition. It can be seen as an improvement of [Si4, Proposition 6.55] since it removes the condition on n (and the proof is valid in all characteristic).

Proposition 2. *Let K be a field equipped with a non-archimedean valuation v and k the corresponding residue field. Let E be an elliptic curve given by an equation in Tate form defined over K. Let $\phi\colon \mathbb{P}_1(K) \to \mathbb{P}_1(K)$ be a flexible Lattès map associated to E where the corresponding π is also defined over K. Suppose that E has good reduction at v. Then there exists an $f \in \mathrm{PGL}_2(K)$ such that $\phi^f = f \circ \phi \circ f^{-1}$ has good reduction at v.*

Proof of Proposition 2. In Silverman's book [Si4, Proposition 6.51] it is proven that the Q appearing in the definition of flexible Lattès maps has to be a torsion point of order dividing 2.

Since a priori π is not the projection on the x–coordinate we have to pass to a conjugate $\phi^f = f \circ \phi \circ f^{-1}$ where $f \in \mathrm{PGL}_2(K)$. Indeed, by [Si4, Proposition 6.51], there exists an automorphism $f \in \mathrm{PGL}_2(K)$ such that ϕ^f fits into a diagram of the type (5.1.1) where π now is the projection on the x–coordinate. Furthermore since E has good reduction it can be seen by standard arguments that we can conjugate with another $f \in \mathrm{PGL}_2(K)$ such that E is given by a minimal Tate equation with respect to v and π is still the projection on the x–coordinate. If Q is the identity element and n^2 the degree of the Lattès map, then $\phi^f(x) = \frac{A_n^T(x)}{B_n^T(x)}$ (where we are using the notation as in section 2.8 and the affine notation for the endomorphism ϕ). From the arguments in section 2.8 follows that the polynomials $A_n^T(x)$ and $B_n^T(x)$ have v–integer coefficients and $A_n^T(x)$ is monic of degree n^2. By [Si4, Theorem 2.15], the map $\phi^f(x)$ has good reduction if and only if the resultant $\mathrm{res}(A_n^T(x), B_n^T(x))$ is a v–unit. But this follows immediately from (2.8.3).

Suppose now that Q is not the identity element. We define the addition by Q map as $\psi(P) = P + Q$. Since $\psi(-P) = -\psi(P)$ it has a Lattès map $\phi_{_Q}$ sitting in the following commutative diagram

$$\begin{tikzcd}
E \arrow[r, "\psi"] \arrow[d, "x"'] & E \arrow[d, "x"] \\
\mathbb{P}_1 \arrow[r, "\phi_{_Q}"] & \mathbb{P}_1,
\end{tikzcd} \tag{5.1.2}$$

where x denotes the projection down to the x coordinate. We want to show that $\phi_{_Q}$ has good reduction if the chosen model for E in (5.1.2) has good reduction. To show the desired property we look at the following bigger diagram.

$$\begin{tikzcd}
E \arrow[r, "\psi"] \arrow[d, "\sim"'] & E \arrow[d, "\sim"] \\
\widetilde{E} \arrow[r, "\widetilde{\psi}"] \arrow[d, "x"'] & \widetilde{E} \arrow[d, "x"] \\
\mathbb{P}_1(\overline{k}) \arrow[r, "\widetilde{\phi_Q}"] & \mathbb{P}_1(\overline{k})
\end{tikzcd}$$

where $\widetilde{\psi}$ denotes the addition by $\widetilde{Q}$ map (by abuse of notation we use $\widetilde{}$ also for reduction on the curve). This map has an associated Lattès map $\widetilde{\phi_Q}$. The upper diagram commutes because reduction modulo v is a homomorphism of groups since E has good reduction. The lower small diagram commutes simply because of the definition of Lattès maps. Now reducing modulo v so applying $\widetilde{}$ and then projecting down to the x coordinate can be performed in the reverse order if suitably interpreted in the case of the identity element. We draw yet another diagram

$$\begin{tikzcd}
E \arrow[r, "\psi"] \arrow[d, "x"'] & E \arrow[d, "x"] \\
\mathbb{P}_1(\overline{K}) \arrow[r, "\phi_Q"] \arrow[d, "\sim"'] & \mathbb{P}_1(\overline{K}) \arrow[d, "\sim"] \\
\mathbb{P}_1(\bar{k}) \arrow[r, "\widetilde{\phi_Q}"] & \mathbb{P}_1(\bar{k})
\end{tikzcd}$$

where now the commutativity of the upper small diagram is given by definition and the commutativity of the big one by the previous remark about reversing the order of projecting and reducing. We want to verify the commutativity of the small lower diagram. We start at E in the left upper corner and go down by projecting to the x coordinate. Then we apply ϕ_Q and afterwards $^\sim$. By commutativity of the big diagram and the upper small one this is the same as applying the map x reducing modulo v and then applying $\widetilde{\phi_Q}$. Hence we get the equality $^\sim \circ \phi_Q \circ x = \widetilde{\phi_Q} \circ ^\sim \circ x$. Since x is surjective it follows that $^\sim \circ \phi_Q = \widetilde{\phi_Q} \circ ^\sim$ which is the desired commutativity of the lower small diagram. It follows that the Lattès map ϕ_Q has good reduction (a fact also consistent with (2.8.6) and (2.8.7)). This concludes the proof since good reduction is preserved under composition. □

References

[B1] D. Bertrand, *Extensions de D-modules et groupes de Galois différentiels*, Springer Lecture Notes 1454, 125–141 (1990).

[B2] D.Bertrand (with an Appendix by Bas Edixhoven), *Special points and Poincaré bi-extensions*, arXiv:1104.5178, (11 pages).

[B3] D. Bertrand, *Generalized jacobians and Pellian polynomials*, to appear in J. Th. Nombres Bordeaux.

[BMPZ] D. Bertrand, D. Masser, A. Pillay, U. Zannier, *Relative Manin-Mumford for semi-abelian surfaces*, to appear in J. Edinburgh Math. Soc. (arXiv:1307.1008).

[BG] E. Bombieri, W. Gubler, *Heights in Diophantine Geometry.* New Mathematical Monographs 4, Cambridge University Press (2006).

[BMZ] E. Bombieri, D. Masser, U. Zannier, *On unlikely intersections of complex varieties with tori.* Acta Arith. 133, 309–323 (2008).

[BP] E. Bombieri, J. Pila,*The number of integral points on arcs and ovals.* Duke Math. J. 59, 337–357 (1989).

[BBLPP] E. Brezin, R. Byrne, J. Levy, K. Pilgrim, and K. Plummer, *A census of rational maps,* Conformal Geometry and Dynamics 4 (2000), 35-74.

[BuHu] I. Burhanuddin; M. Huang, *Elliptic curve torsion points and division poynomials.*, Computational aspects of algebraic curves Lecture Notes Ser. Comput. 13 World Sci. Publ., Hackensack, NJ (2005), 13 -37.

[CMZ] P. Corvaja, D. Masser, U. Zannier, *Sharpening "Manin-Mumford" for certain algebraic groups of dimension 2.* L'Enseign. Math. 59, 225–269 (2013).

[Dave] J. Davenport, *On the integration of algebraic functions.* Lecture Notes in Computer Science, 102. Springer-Verlag, Berlin-New York (1981).

[Davi] S. David, *Points de petite hauteur sur les courbes elliptiques.* J. Number Theory 64, 104–129 (1997).

[F] R. Fricke, *Elliptische Funktionen I*, Teubner, Leipzig, Berlin, 1922.

[Hab] P. Habegger, *Special points on fibered powers of elliptic surfaces.* J. Reine Angew. Math. 685, 143–179 (2013) .

[Hal] G.-H. Halphen, *Traité des fonctions elliptiques et de leurs applications, I.* Gauthier-Villars, Paris (1886).

[Hi] M. Hindry, *Autour d'une conjecture de Serge Lang*, Inventiones Math. 94, 575–603 (1988).

[Hu] D. Husemöller (with appendices by O. Forster, R. Lawrence and S. Theisen), *Elliptic Curves*, Second edition, Graduate Texts in Mathematics 111, Springer-Verlag, New York (2004).

[Ka] N. Katz, *p-adic interpolation of real analytic Eisenstein series.* Annals of Math, 104, 459-571(1976).

[KK] M. Koecher and A. Krieg, *Elliptische Funktionen und Modulformen.* Springer-Verlag, Berlin, 1998.

[La1] S.Lang, *Introduction to algebraic geometry.* Addison-Wesley Publishing Co., Inc., Reading, MA (1973).

[La2] S. Lang (with an appendix by J. Tate), *Elliptic functions*, Second edition, Graduate Texts in Mathematics 112, Springer-Verlag, New York (1987).

[La3] S. Lang, *Algebra*, Second edition, Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA (1984).

[Li] Q. Liu, *Algebraic geometry and Arithmetic Curves*, Oxford Graduate Texts in Mathematics, 6. Oxford Science Publications, Oxford University Press, Oxford (2002).

[Man] Manin, Ju. I., *Rational points on algebraic curves over function fields*, Izv. Akad. Nauk SSSR Ser. Mat. 27 1395–1440 (1963).

[Mas1] D. Masser, *Heights, transcendence and linear independence on commutative group varieties*, In: *Diophantine Approximation (Cetraro, 2000)*, 1-51. Lecture Notes in Mathematics 1819. Springer, Berlin (2003).

[Mas2] D. Masser, *Rational values of the Riemann zeta function*, J. Number Theory 131, 2037–2046 (2011).

[MZ1] D. Masser, U. Zannier, *Torsion anomalous points and families of elliptic curves*, American J. Math. 132, 1677–1691 (2010).

[MZ2] D. Masser, U. Zannier, *Torsion points on families of squares of elliptic curves*, Math. Ann. 352, 453–484 (2012).

[MZ3] D. Masser, U. Zannier, *Bicyclotomic polynomials and impossible intersections.* J. Th. Nombres Bordeaux 25, 635–659 (2013).

[MZ4] D. Masser, U. Zannier, *Torsion points on families of products of elliptic curves*, Adv. Math. 259, 116–133 (2014).

[MZ5] D. Masser, U. Zannier, *Torsion points on families of simple abelian surfaces and Pell's equation over polynomial rings (with Appendix by V. Flynn)*, to appear in J. European Math. Soc.

[MZ6] D.Masser, U.Zannier, *Torsion points on families of abelian varieties, Pell's equation, and integration in elementary terms*, in preparation.

[MT] B. Mazur and J. Tate, *The p-adic sigma function*, Duke Math. J. 62 (1991), 663-688.

[Mil] J. Milnor. *On Lattès maps.* In Dynamics on the Riemann Sphere, A Bodil Branner Festschrift, Hjorth and Petersen, editors, pages 9-43, Eur. Math. Soc

[Pil] J. Pila, *Integer points on the dilation of a subanalytic surface.* Q. J. Math. 55, 207–223 (2004).

[PW] J. Pila, A. Wilkie, *The rational points of a definable set.* Duke Math. J. **133**, no. 3, 591–616, (2006).

[PZ] J. Pila, U. Zannier, *Rational points in periodic analytic sets and the Manin-Mumford conjecture*, arXiv:0802.4016, (12 pages).

[Pin] R. Pink, *A common generalization of the Conjectures of André-Oort, Manin-Mumford and Mordell-Lang*, manuscript (2005), homepage of R. Pink.

[Ra1] Raynaud, M. *Courbes sur une variété abélienne et points de torsion.* Invent. Math. **71** , no. 1, 207–233, (1983).

[Ra2] Raynaud, M. *Sous-variétés d'une variété abélienne et points de torsion.* Arithmetic and geometry, Vol. I, 327–352, Progr. Math., **35**, Birkhäuser Boston, Boston, MA, (1983).

[Ri] Risch, Robert H. *The solution of the problem of integration in finite terms.* Bull. Amer. Math. Soc. 76, 605–608 (1970).

[Sc] Schmidt, H. *Resultants and discriminants of multiplication polynomials for elliptic curves. Appendix A by Schmidt and Jung Kyu Canci.* J. Number Theory 149, 70–91 (2015).

[Se] J.P. Serre, *Algebraic groups and class fields.* GTM, Springer-Verlag, New York, 1988.

[Si1] J.H. Silverman, *Heights and the specialization map for families of abelian varieties.* J. Reine Angew. Math. 342, 197–211 (1983).

[Si2] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics 106, Springer-Verlag, New York (1986).

[Si3] J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer GTM 151 (1994).

[Si4] J.H. Silverman. *The Arithmetic of Dynamical Systems*, Springer-Verlag, GTM 241 (2007).

[Sta] H.M. Stark, *The Coates-Wiles Theorem revisited*, in *Number theory related to Fermat's last theorem* (Cambridge MA, 1981), Progress Math. 26, Birkhauser (p.349-362) (1982) .

[Sto] M. Stoll, *Simultaneous torsion in the Legendre family*, arXiv:1410.7070 (19 pages).

[TM] J. Tannery and J. Molk, *Fonctions elliptiques III*, Gauthier-Villars, Paris 1893.

[Za1] U. Zannier (with appendixes by David Masser), *Some Problems of Unlikely Intersections in Arithmetic and Geometry.* Annals of Mathematics Studies 181, Princeton University Press, Princeton, NJ (2012).

[Za2] U. Zannier, *Unlikely intersections and Pell's Equations in Polynomials.* Springer INDAM Series 8, Chapter 12 (2014).

[Zil] B. Zilber, *Exponential sums equations and the Schanuel conjecture.* J. London Math. Soc. 65, 27–44 (2009).