EFFECTIVE INJECTIVITY OF SPECIALIZATION MAPS FOR ELLIPTIC SURFACES

A Dissertation

Submitted to the Faculty

of

Purdue University

by

Tyler R. Billingsley

In Partial Fulfillment of the

Requirements for the Degree

of

Doctor of Philosophy

August 2020

Purdue University

West Lafayette, Indiana

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF DISSERTATION APPROVAL

Dr. Edray Goins, Co-Chair
    Pomona College, Department of Mathematics
Dr. Donu Arapura, Co-Chair
    Department of Mathematics
Dr. Tong Liu
    Department of Mathematics
Dr. Kenji Matsuki
    Department of Mathematics

Approved by:

Dr. Plamen Stefanov
    Associate Head for Graduate Studies, Department of Mathematics

ACKNOWLEDGMENTS

I would like to express my appreciation for my advisor Professor Edray Goins. Without his endless patience and support this work never would have been completed. I would also like to thank Professor Donu Arapura for his insightful discussions after Edray's departure from Purdue in 2018. I additionally thank Professor Kenji Matsuki for his careful reading of an earlier draft of this document, which led to correcting numerous errors and greatly clarifying the exposition.

I would like to thank Professor Peter Turbek of Purdue University Northwest. Without his guidance I never would have made it to graduate school in the first place.

I want to additionally acknowledge my friends and fellow graduate students. The math graduate students at Purdue provided me with a truly invaluable support system, and I hope that the community flourishes for years to come.

Last but not least, I want to thank my wife Krystal, who has been endlessly supportive and encouraging throughout this whole process.

TABLE OF CONTENTS

ABSTRACT

Billingsley, Tyler R. PhD, Purdue University, August 2020. Effective Injectivity of Specialization Maps for Elliptic Surfaces. Major Professors: Edray Goins and Donu Arapura.

This dissertation concerns two questions involving the injectivity of specialization homomorphisms for elliptic surfaces. We primarily focus on elliptic surfaces over the projective line defined over $\mathbb{Q}$. The specialization theorem of Silverman proven in 1983 says that, for a fixed surface, all but finitely many specialization homomorphisms are injective. Given a subgroup of the group of rational sections with explicit generators, we thus ask the following.

1. Given some $t_0 \in \mathbb{Q}$, how can we effectively determine whether or not the specialization map at t_0 is injective?
2. What is the set Σ of $t_0 \in \mathbb{Q}$ such that the specialization map at t_0 is injective?

The classical specialization theorem of Néron proves that there is a set S which differs from a Hilbert subset of $\mathbb{Q}$ by finitely many elements such that for each $t_0 \in S$ the specialization map at t_0 is injective. We expand this into an effective procedure that determines if some $t_0 \in \mathbb{Q}$ is in S, yielding a partial answer to question 1. Computing the Hilbert set provides a partial answer to question 2, and we carry this out for some examples. We additionally expand an effective criterion of Gusić and Tadić to include elliptic surfaces with a rational 2-torsion curve.

1. INTRODUCTION

In this introduction, I give an overview of the results in the dissertation and how the dissertation is structured.

Let $K = k(C)$ be the function field of a smooth projective curve C defined over a number field k. For an elliptic surface $\mathcal{E} \to C$ defined over k and a point $t_0 \in C(k)$ such that the fiber $\mathcal{E}_{t_0}$ is smooth, the specialization map σ_{t_0} is the group homomorphism from the K-rational points of the generic fiber E/K to the k-rational points of the fiber $\mathcal{E}_{t_0}(k)$ obtained by evaluating functions in K at t_0. As shown by Silverman [15], for all but finitely many $t_0 \in C(k)$, the maps σ_{t_0} are injective. From the proof, it's not immediately clear how one might go about showing, for some specific $t_0 \in C(k)$, whether or not σ_{t_0} is injective. In Chapters 4 and 5, I discuss a variety of ways that one can check this, primarily in the case of $k = \mathbb{Q}$ and $C = \mathbb{P}^1$. The first is the following, which is based on an explicit analysis of the proof of Néron's Specialization Theorem.

Algorithm 4.9 *Let $M < E(\mathbb{Q}(t))$ be a subgroup satisfying some special properties (see Theorem 4.7). Let $t_0 \in \mathbb{Q}$. Then there is an algorithm that shows that $\sigma_{t_0}|_M$ is injective as long as t_0 lies within a specific Hilbert subset of $\mathbb{Q}$.*

The algorithm is effective as long as one can compute the Hilbert subsets in question. Using this algorithm, I compute some examples and extract the following facts.

Theorem 4.20 *Let $E/\mathbb{Q}(t)$ be the elliptic curve given by the Weierstrass equation*

$$y^2 = x^3 - t^2x + t^2.$$

Then for any positive integer $t_0 > 1$ with $t_0 \equiv 1$ mod 4 the specialization map σ_{t_0} is injective.

Theorem 4.24 *Let $E/\mathbb{Q}(t)$ be the elliptic curve given by the Weierstrass equation*

$$y^2 = x^3 - (t^2 + 27)x + 10t^2 + 48t + 90,$$

and let $M < E(\mathbb{Q}(t))$ be the subgroup generated by $P = (t + 3, 4t + 6)$ and $Q = (9, t + 24)$. Then for any $t_0 \in \mathbb{Q}$ with

$$t_0 \notin \{-26, -19, -12, -11, -5, -3, -1, 6, 9, 44\}$$

and such that the polynomial $x^3 - (t_0^2 + 27)x + 10t_0^2 + 48t_0 + 90 \in \mathbb{Q}[x]$ has no rational roots, the specialization map $\sigma_{t_0}|_M$ is injective.

Following this, after a discussion of the criteria of Gusić and Tadić [2], I conclude with a section that discusses some new ways to check that specialization maps are injective even when previous criteria fail. The first method allows us to apply the criteria of Gusić and Tadić in the case where the 2-division curve is rational. An application of this method yields the following.

Proposition 5.14 *Let $E/\mathbb{Q}(t)$ be the elliptic curve with Weierstrass equation*

$$y^2 = x^3 - t^2x + t^2.$$

Let t_0 be a rational number of the form $t_0 = 1/(\alpha_0 - \alpha_0^3)$ for some rational number α_0. Let Φ be the set of irreducible factors of

$$-\alpha^6(\alpha - 1)^6(\alpha + 1)^6(3\alpha^2 - 4)(3\alpha^2 - 1)^2$$

in $\mathbb{Z}[\alpha]$. Suppose that, for each product $h(\alpha)$ of some nonempty subset of the elements of Φ, the rational number $h(\alpha_0)$ is not a square. Then the specialization map σ_{t_0} is injective.

The second method, as detailed below, can be viewed as a generalization of the first. It allows us to partially circumvent relying on injectivity of the induced specialization map on $E(k(t))/2E(k(t))$.

Proposition 5.15 *Let k be a number field. Let $E/k(t)$ be an elliptic curve given by the Weierstrass equation*

$$y^2 = x^3 + A(t)x + B(t),$$

and fix $P = (x_P(t), y_P(t)) \in E(k(t)) \setminus E[2](k(t))$ such that P is not divisible by 2 in $E(K)$. Let $\phi(t, x)$ be an irreducible factor of $d_{2,P}(t, x)$ such that

$$C_P : \phi(t, a) = 0$$

is rational over k. Fix an isomorphism of function fields

$$\begin{aligned} k(C_P) &\cong k(\alpha) \\ t &\mapsto u(\alpha) \\ a &\mapsto v(\alpha). \end{aligned}$$

Then the elliptic curve

$$E' : y^2 = x^3 + A(u(\alpha))x + B(u(\alpha))$$

defined over $k(\alpha)$ has the following properties.

1. *$P' = (x_P(u(\alpha)), y_P(u(\alpha))) \in E'(\mathbb{Q}(\alpha))$ is divisible by 2 in $E'(\mathbb{Q}(\alpha))$.*
2. *The function field isomorphism gives an embedding $E(\mathbb{Q}(t)) \subset E'(\mathbb{Q}(\alpha))$.*
3. *Let $\alpha_0 \in \mathbb{Q}$ and set $t_0 = u(\alpha_0)$. Let $M < E(\mathbb{Q}(t))$ be a subgroup. If the specialization map σ'_{α_0} for E' is injective on the image of M via the embedding above, then the specialization map $\sigma_{t_0}|_M$ for E is injective.*

One applies the above method by taking your subgroup of interest in $E(\mathbb{Q}(t))$ and viewing it as a subgroup of $E'(\mathbb{Q}(\alpha))$, but you replace P by $R \in E'(\mathbb{Q}(\alpha))$ with $2R = P$. In this way, one can apply Algorithm 4.9 in E' for certain α_0's which correspond to t_0's where the algorithm was guaranteed to fail for E.

The layout of the dissertation is as follows.

In chapter 2, I motivate the geometric approach to the study of rational solutions to cubic equations by first addressing the same problem for quadratic equations where the situation is much simpler. I then turn our focus to elliptic curves. In this dissertation, elliptic curves are essentially identified with Weierstrass equations, supporting the concrete applications that I aim to develop. Explicit formulas for the group law and division polynomials are given, and I state the Mordell-Weil theorem.

In chapter 3, I overview the basics of the theory of elliptic surfaces. While all major results in the dissertation can (and will) be stated from the viewpoint of rational points on elliptic curves over function fields of curves, the impact of elliptic surfaces on this area cannot be understated. I establish the connection between these two subjects and state the analogs of the Mordell-Weil theorem in this case. I end by introducing specialization, the focus of the rest of the dissertation.

In chapter 4, the goal is to establish how the classical proof of Néron's Specialization Theorem can be used to address injectivity of the specialization map in an explicit manner. I use the resulting algorithm to explicitly give infinitely many injective specialization maps for two examples.

In chapter 5, I discuss the criteria of Gusić and Tadić [2] which allow you to show that a specialization map is injective without knowing generators of $E(K)$ under the assumption that $C = \mathbb{P}^1$ and that there is at least one nontrivial $k(t)$-rational 2-torsion point. Taking a slightly more general approach than their paper, the discussion centers around the idea of finding a "bounding group" of the image of $E(K)/2E(K)$ under the standard 2-descent or descent by 2-isogeny maps; this idea was first mentioned by Stoll [19]. I conclude by mentioning a new way to utilize curves defined by division polynomials to avoid the potential issues of gaining additional 2-torsion points or the failure of specialization on $E(K)/2E(K)$ to be injective, as long as the curves are rational. In this case we can prove that additional specialization maps are injective, and we illustrate this with some examples.

2. AN INTRODUCTION TO ELLIPTIC CURVES

Diophantine geometry concerns the application of geometric techniques to solve the classical number-theoretic problem of finding integer or rational solutions to equations. We begin the chapter with an overview of the simplest case of this, which is finding rational solutions to quadratic equations in two variables; geometrically, these equations determine conic sections. There are the two questions of whether or not there is a solution at all, and if there are solutions then how to find all of them. Both of these questions have nice answers for conics.

Moving up to the next simplest case, cubic equations in two variables, changes everything. Determining whether or not a given cubic equation in two variables has a rational solution is an open problem, one which we will not concern ourselves with in this dissertation. Those cubics with at least one known rational solution define the geometric objects known as elliptic curves, and how to determine the full set of rational points on such a curve is also an open problem. We will discuss the basic structure of the set of rational points on an elliptic curve, thereby setting up the required background to continue onto the study of elliptic surfaces and how they can be used to help find rational points on elliptic curves.

2.1 Rational Points on Conics

Definition 2.1 *Let* $f(x,y) = ax^2 + bxy + cy^2 + dx + ey + f$ *where* $a,b,c,d,e,f \in \mathbb{Q}$ *and at least one of* a,b,c *is nonzero. If* $f(x,y) \in \mathbb{Q}[x,y]$ *is an irreducible polynomial, then the equation*

$$f(x,y) = 0$$

defines a ***rational conic****.*

Let's begin by discussing the existence of rational points on a conic $\mathcal{C}$ defined by the equation above. After a change of variables, one arrives at one of the three classic conic cases, the parabola

$$Ax^2 + By = 0$$

or the ellipse/hyperbola

$$Ax^2 + By^2 + C = 0. \tag{2.1}$$

In the parabola case, noting that y is a function of x we may substitute any rational number for x to obtain a corresponding value of y, yielding a rational point on $\mathcal{C}$. Otherwise, suppose we are in the ellipse/hyperbola case.

Lemma 2.2 *There exist $A', B', C' \in \mathbb{Z}$ with the following properties.*

- *A', B', C' are pairwise relatively prime and squarefree.*
- *There is a bijection between the rational points on $\mathcal{C}$ and the rational points on the conic*

$$\mathcal{C}' : A'x^2 + B'y^2 + C' = 0. \tag{2.2}$$

Proof By clearing denominators and dividing through by common factors, we may assume that $A, B, C \in \mathbb{Z}$ and $\gcd(A, B, C) = 1$. Writing

$$A = \alpha^2 A_1, \qquad B = \beta^2 B_1, \qquad C = \gamma^2 C_1$$

with A_1, B_1, C_1 the squarefree parts of A, B, C, respectively, we have a bijection from rational points on $\mathcal{C}$ and those on

$$\mathcal{C}_1 : A_1x^2 + B_1y^2 + C_1 = 0$$

given by

$$(x_0, y_0) \text{ on } \mathcal{C} \iff \left(\frac{\alpha}{\gamma}x_0, \frac{\beta}{\gamma}y_0\right) \text{ on } \mathcal{C}_1.$$

Next, call

$$A_2 = A_1/\gcd(A_1, B_1), \qquad B_2 = B_1/\gcd(A_1, B_1), \qquad C_2 = \gcd(A_1, B_1)C_1.$$

In the same way as with $\mathcal{C}$ and $\mathcal{C}_1$, because these new coefficients differ from A_1, B_1, C_1 by squares, we have a bijection between the rational points of $\mathcal{C}_1$ and

$$\mathcal{C}_2 : A_2x^2 + B_2y^2 + C_2 = 0.$$

Now we have $\gcd(A_2, B_2) = 1$. For the moment, assume the following claim.

"We have $\gcd(A_2, C_2) = \gcd(A_1, C_1)$ and $\gcd(B_2, C_2) = \gcd(B_1, C_1)$. Additionally, C_2 is squarefree."

Assuming this, note that we may define

$$A_3 = A_2/\gcd(A_2, C_2), \qquad B_3 = B_2 \gcd(A_2, C_2), \qquad C_3 = C_2/\gcd(A_2, C_2),$$

and a conic $\mathcal{C}_3$ similar to above with a bijection between rational points on $\mathcal{C}_3$ and those on $\mathcal{C}$, and now

$$\gcd(A_3, B_3) = 1 \qquad \text{and} \qquad \gcd(A_3, C_3) = 1.$$

Doing this one more time to make the other remaining pair of coefficients relatively prime finishes the proof of the lemma.

Proof of the Claim: First, since $\gcd(A_1, B_1, C_1) = 1$, we have that

$$\gcd(\gcd(A_1, B_1), C_1) = 1.$$

Hence C_2 is squarefree, since it's the product of two squarefree relatively prime integers. Since A_1 is squarefree, we have that $\gcd(A_2, \gcd(A_1, B_1)) = 1$, so that $\gcd(A_2, C_2) = \gcd(A_2, C_1)$. We now show that $\gcd(A_2, C_1) = \gcd(A_1, C_1)$. Clearly $\gcd(A_2, C_1)$ divides A_1 and C_1, so

$$\gcd(A_2, C_1) \mid \gcd(A_1, C_1).$$

Conversely, say d divides A_1 and C_1. Then $\gcd(d, \gcd(A_1, B_1)) = 1$ – if not, some prime divides d and $\gcd(A_1, B_1)$, meaning the prime divides A_1, B_1 and C_1, which is impossible. Hence d and $\gcd(A_1, B_1)$ are relatively prime, so that in fact d divides $A_2 = A_1/\gcd(A_1, B_1)$. Thus

$$\gcd(A_1, C_1) \mid \gcd(A_2, C_1),$$

and so $\gcd(A_2, C_2) = \gcd(A_1, C_1)$. We can argue similarly for $\gcd(B_1, C_1)$.

■

Replace A, B, C with integers as in Lemma 2.2. Now consider the related equation

$$Ap^2 + Bq^2 + Cr^2 = 0. \tag{2.3}$$

Any solution $(p_0, q_0, r_0) \in \mathbb{Z}^3$ to Equation (2.3) with $r_0 \neq 0$ gives a corresponding solution $(p_0/r_0, q_0/r_0) \in \mathbb{Q}^2$ to Equation (2.1). Similarly, any solution $(x_1/x_2, y_1/y_2) \in \mathbb{Q}^2$ to Equation (2.1) gives rise to a corresponding solution $(x_1y_2, y_1x_2, x_2y_2) \in \mathbb{Z}^3$ to Equation (2.3) with $x_2y_2 \neq 0$. Thus to determine whether or not the conic $\mathcal{C}$ has a rational point, we need to look for integer solutions (p_0, q_0, r_0) to the equation

$$Ap^2 + Bq^2 + Cr^2 = 0$$

with $r_0 \neq 0$. The solution to this problem is characterized in terms of modular arithmetic and was originally given by Legendre.

Theorem 2.3 (Legendre's Theorem [4, Chapter 17 §3]) *The equation*

$$Ap^2 + Bq^2 + Cr^2 = 0$$

with A, B, C pairwise relatively prime squarefree integers has a nontrivial (i.e. not all zero) integer solution if and only if the following four conditions hold.

1. *A, B and C don't all have the same sign.*
2. *$-AB$ is a square mod C.*
3. *$-AC$ is a square mod B.*
4. *$-BC$ is a square mod A.*

As long as our guaranteed solution (p_0, q_0, r_0) via Legendre's Theorem has $r_0 \neq 0$ we know the conic Equation (2.1) has a rational solution. Let's check that the conditions in Legendre's Theorem yield a rational point on $\mathcal{C}$ even in the case that we find a nontrivial solution $(p_0, q_0, 0)$ to Equation (2.3). In this case, we have

$$Ap_0^2 = -Bq_0^2.$$

Since $\gcd(A, B) = 1$ and A, B are squarefree we must have that $A|q_0$ and $B|p_0$. Rewriting $p_0 = Bp_0'$ and $q_0 = Aq_0'$, we see that

$$AB^2p_0'^2 = -BA^2q_0'^2.$$

Hence

$$Bp_0'^2 = -Aq_0'^2.$$

We can now repeat the same procedure to divide p_0' by A and q_0' by B, arriving back at the original equation $Ap_0''^2 = -Bq_0''^2$. Note that

$$p_0'' = p_0/AB, \qquad q_0'' = q_0/AB,$$

so that this division cannot continue indefinitely unless $A, B \in \{\pm 1\}$. But since we're assuming that we have a nontrivial solution $(p_0, q_0, 0)$, we in fact have either $A = 1$ and $B = -1$ or $A = -1$ and $B = 1$. So, WLOG, say $A = 1$ and $B = -1$. Then Equation (2.3) becomes

$$p^2 - q^2 + Cr^2 = 0.$$

This equation always has the integer solution

$$(C - 1, C + 1, 2),$$

so that we have an integer solution with $r_0 \neq 0$ after all.

Hence, in the ellipse/hyperbola case, as long as A, B, C satisfy the conditions in Legendre's Theorem, the conic $\mathcal{C}$ has (at least one) rational point.

Example 2.4 *Consider the equation*

$$2p^2 + 3q^2 - 5r^2 = 0.$$

We clearly have the integer solution $(1,1,1)$*, and the four conditions above are satisfied.*

Example 2.5 *Consider the equation*

$$2p^2 + 3q^2 - 7r^2 = 0.$$

Since $14 \equiv 2$ *is not a square mod 3. condition 3 is not satisfied. Therefore this equation has no nontrivial integer solutions. Hence the corresponding conic*

$$\mathcal{C} : 2x^2 + 3y^2 - 7 = 0$$

has no rational points.

Now suppose $\mathcal{C}$ is a conic with a rational point (x_0, y_0). How do we find all of the rational points on $\mathcal{C}$? Take a line L with rational slope that goes through (x_0, y_0). The possibilities for the set $L \cap \mathcal{C}$ are determined by Bézout's Theorem.

Theorem 2.6 (Bézout's Theorem [12, Chapter 3 §2.2]) *Let* C_1 *and* C_2 *be curves in* $\mathbb{P}^2_{\overline{\mathbb{Q}}}$ *of degrees* d_1 *and* d_2*. Then*

$$\#(C_1 \cap C_2) = d_1 d_2,$$

accounting for multiplicity.

Thus $L \cap \mathcal{C}$ has at most two points whenever L is a line and $\mathcal{C}$ is a conic. It contains exactly one point when L is the tangent line to $\mathcal{C}$ at (x_0, y_0), and otherwise $L \cap \mathcal{C}$ has 2 distinct points, with the additional point also being rational. Of course rationality is not guaranteed by Bézout's Theorem alone, but here it amounts to the fact that if a rational quadratic equation has one rational root then it has two (up to multiplicity). On the other hand, given any rational point (x_0', y_0') on $\mathcal{C}$, we can draw the line L through this point and (x_0, y_0), choosing the tangent line in the case of $(x_0', y_0') = (x_0, y_0)$. This line will either be vertical or have rational slope. So we have a correspondence

$$\left\{\begin{array}{c}\text{lines with rational slope through } (x_0, y_0)\\ \text{and the line } x = x_0\end{array}\right\} \iff \{\text{rational points on } \mathcal{C}\}.$$

In other words, $\mathcal{C}$ is birationally equivalent to $\mathbb{P}^1$ over $\mathbb{Q}$.

Example 2.7 *We carry out this procedure explicitly for the unit circle*

$$\mathcal{C} : x^2 + y^2 = 1.$$

Set $P = (1, 0)$. *The line* L *with slope* m *going through* P *has equation*

$$y = m(x - 1).$$

Substituting this into the equation which defines $\mathcal{C}$, *we have*

$$\begin{aligned} x^2 + (m(x-1))^2 &= 1 \\ x^2 + m^2(x^2 - 2x + 1) &= 1 \\ (m^2+1)x^2 - 2m^2x + (m^2 - 1) &= 0 \\ (x-1)\left(x - \frac{m^2-1}{m^2+1}\right) &= 0. \end{aligned}$$

Thus the other intersection point of L *with* $\mathcal{C}$ *is*

$$\left(\frac{m^2-1}{m^2+1}, \frac{-2m}{1+m^2}\right).$$

Hence every rational point on $\mathcal{C}$ *(except for* $(1, 0)$, *which corresponds to a vertical line) can be written in the above form.*

2.2 Weierstrass Form

We now consider the next simplest case, rational solutions to cubic equations in 2 variables. We work over a number field K. Consider an irreducible homogeneous polynomial in 3 variables

$$\begin{aligned} f(x, y, z) = {} & a_1x^3 + a_2x^2y + a_3xy^2 + a_4y^3 + a_5x^2z \\ & + a_6xyz + a_7y^2z + a_8xz^2 + a_9yz^2 + a_{10}z^3 \end{aligned}$$

with a K-rational solution $P = (x_0, y_0, z_0)$, and call the corresponding (projective) curve E. As shorthand for saying E is defined over K, we write E/K. It is important that we require the curve to have a rational point. As with our discussion about conics, methods that we discuss for finding rational points will require there to be at least one rational point already. There are cubic curves with no rational points. A large distinction between the cubic case and the case of conics is that there is no simple "local condition" that guarantees the existence of rational points on a cubic curve.

Example 2.8 *(Cassels) Consider the curve*

$$E : 3x^3 + 4y^3 + 5z^3 = 0.$$

This curve has $\mathbb{Q}_p$-rational points for every prime p, but no $\mathbb{Q}$-rational points (except (0,0,0)).

In order to simplify our discussion, we will put our cubic in a simpler form, called Weierstrass form. First, if P happens to be a singular point, draw a line through E with K-rational slope. This is guaranteed to intersect E in another K-rational point which cannot be singular, so we may assume that P is nonsingular. We now move the point P "to infinity" using the (potentially non-linear) embedding into $\mathbb{P}^2$ given by the linear system $3P$. We then obtain a polynomial of the form

$$g(x, y, z) = y^2 z - (x^3 + Axz^2 + Bz^3).$$

Through this embedding, P maps to the only point with $z = 0$, which is $(0 : 1 : 0)$. Hence, for simplicity (and a slight abuse of notation), we dehomogenize by setting $z = 1$ and denote by E the affine curve

$$E : y^2 = x^3 + Ax + B,$$

keeping in mind the point at infinity that this form does not explicitly include. This transformation preserves rational points, reducing the problem of studying the rational points of cubics (with at least one rational point) to studying the rational points on cubic curves in Weierstrass form.

Definition 2.9 *If the polynomial $x^3 + Ax + B$ has no repeated roots (equivalently, $4A^3 + 27B^2 \neq 0$), the projective curve*

$$E : y^2 = x^3 + Ax + B$$

*is called an **elliptic curve**.*

Remark 2.10 *Technically, an elliptic curve is a nonsingular projective curve of genus 1 with a selected rational point. The Riemann-Roch theorem guarantees that all such curves can be embedded into $\mathbb{P}^2$ in Weierstrass form, where the rational point becomes the point at infinity (0:1:0); see [17, Chapter III §3] for details. The nonsingular condition is equivalent to the separability condition above. In addition, not every elliptic curve over fields of characteristic 2 or 3 can be written in the above form, but as we will not encounter fields of positive characteristic for the remainder of the dissertation using the more general form would only serve to complicate the discussion.*

When discussing K-rational points on a cubic E in Weierstrass form, we denote the set of rational points by $E(K)$. Note that this includes the point at infinity.

2.3 The Group Law

Let E be an elliptic curve over K in Weierstrass form; that is, we have an affine curve

$$E : y^2 = x^3 + Ax + B$$

with constants $A, B \in K$ such that $4A^3+27B^2 \neq 0$ and the single point $O = (0 : 1 : 0)$ in its Zariski closure in $\mathbb{P}^2$. We will develop an analog to the process described in Section 2.1 to find rational points on E.

We cannot use the same process as before because Bézout's Theorem makes any line intersect E in three points (counting multiplicity) instead of two. But this means that we can take any two points in $E(K)$ and produce a third (similar to the above reasoning, the third point will be rational because any cubic with 2 rational roots has 3). Given P_1 and P_2 in $E(K)$, we obtain the point $P_1 \oplus P_2$ by doing the following.

1. Draw the line through P_1 and P_2, taking the tangent line if $P_1 = P_2$. This line intersects $E(K)$ in a third point R.
2. Draw the line through R and O, taking the tangent line if $R = O$. This line intersects E in a third point $P_1 \oplus P_2$.

Since step 1 by itself successfully produces a third point, why is step 2 needed? Step 2 is required for the operation $\oplus$ to turn $E(K)$ into a *group*. To illustrate this, let $\uplus$ be the operation on $E(K)$ defined by only doing step 1. We examine what happens with the point at infinity O. The point O has a special property: it is a *flex* of the curve. This means that the tangent line L to E at O doesn't just intersect E at O with multiplicity 2, but it actually intersects with multiplicity 3. Hence L intersects E *only at* O, so we see that $O \uplus O = O$ (and additionally, $O \oplus O = O$). If we are to have a group, this means that O must be the identity element. But suppose we have some $P \in E(K) \setminus O$ such that the y-coordinate of P is nonzero. Then

$$P \uplus O \neq P;$$

indeed, $P \uplus O$ is the reflection of P across the x-axis. However, proceeding to step 2 above yields the point P. Therefore

$$P \oplus O = P.$$

Indeed, one can go on to check all the (abelian) group axioms for $\oplus$.

Theorem 2.11 *The operation $\oplus$ turns the set $E(K)$ into an abelian group with identity element O.*

Proof [17, Chapter III §2]. ■

We will use the following notation.

- When there is no chance of confusion, we will use + to denote the point addition operation we have just defined as $\oplus$.
- Following usual conventions for abelian groups, we denote the sum of P with itself n times by nP. We denote the inverse of P with respect to $\oplus$ as $-P$, and we set $(-n)P = -(nP)$. If we are working with specific coordinates,say $P = (x_0, y_0)$, to avoid confusion we denote $2P = [2](x_0, y_0)$.
- For any integer $n \geq 2$, we denote $E[n](K)$ as the n-torsion subgroup of $E(K)$; that is, $P \in E(K)$ is in $E[n](K)$ if and only if $nP = O$.

Using an explicit Weierstrass equation and explicit equations for lines, one can derive the following concrete formulas for the operation $\oplus$.

Proposition 2.12 *Let E be an elliptic curve over K given by the Weierstrass equation*

$$E : y^2 = x^3 + Ax + B.$$

- *Let $P = (x_0, y_0)$ be a nonidentity point of $E(K)$. Then*

  $$-P = (x_0, -y_0).$$

  In addition, if $P \neq -P$, then

  $$x(2P) = \frac{x_0^4 - 2Ax_0^2 - 8Bx_0 + A^2}{4(x_0^3 + Ax_0 + B)},$$
  $$y(2P) = \frac{(3x_0^2 + A)(x_0 - x(2P)) - 2y_0^2}{2y_0}.$$

- *Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ be nonidentity points of $E(K)$ with $P_1 \neq \pm P_2$. Let*

  $$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{and} \quad \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}.$$

  Then

  $$x(P_1 + P_2) = \lambda^2 - x_1 - x_2,$$
  $$y(P_1 + P_2) = -\lambda x(P_1 + P_2) - \nu.$$

Proof [17, Chapter III §2]. ■

2.4 Division Polynomials

The formulas above make it clear that, given a point $Q \in E(K)$, finding a point Q with $nQ = P$ requires solving polynomial equations. The polynomials which appear in this way are called **division polynomials**. Fix $A, B \in K$ with $4A^3 + 27B^2 \neq 0$ and define

$$\mathcal{O} = K[x,y]/(y^2 - (x^3 + Ax + B));$$

that is, $\mathcal{O}$ is the coordinate ring of the elliptic curve

$$E : y^2 = x^3 + Ax + B$$

defined over K. Define the following sequence of polynomials in $\mathcal{O}$.

$$\begin{aligned}
\psi_0 &= 0,\\
\psi_1 &= 1,\\
\psi_2 &= 2y,\\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2,\\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),\\
&\ \vdots\\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \text{ for } m \geq 2,\\
\psi_{2m} &= \left(\frac{\psi_m}{2y}\right) \cdot (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \text{ for } m \geq 3.
\end{aligned}$$

We have the following standard facts about the polynomials above, which we state without proof.

- The polynomials ψ_{2n+1}, ψ_{2n}/y and ψ_{2n}^2 depend only on x.
- For $n \geq 1$, the set of roots of ψ_{2n+1} is the set of x-coordinates of the nonzero $(2n+1)$-torsion points.
- For $n \geq 2$, the set of roots of ψ_{2n}/y is the set of x-coordinates of the nonzero $(2n)$-torsion points which are not 2-torsion. Additionally, the set of roots of

$x^3 + Ax + B$ is the set of x-coordinates of nonzero 2-torsion points. Since $y^2 = x^3+Ax+B$, we see that the set of roots of ψ_{2n}^2 is the set of x-coordinates of all nonzero $(2n)$-torsion points. However, it is worth noting that this polynomial is not separable.

- Combining the previous two statements, for $n \geq 2$ we have that the set of roots of ψ_n^2 is the set of x-coordinates of the nonzero n-torsion points.

- If we additionally define

$$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}, \qquad \omega_n = \frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}{4y},$$

then for any $Q = (x_Q, y_Q) \in E(K) \setminus E[n](K)$ we have that

$$nQ = \left(\frac{\phi_n(x_Q)}{\psi_n^2(x_Q)}, \frac{\omega_n(x_Q, y_Q)}{\psi_n^3(x_Q, y_Q)} \right). \tag{2.4}$$

Note that, if $Q \in E[n](K)$, by the above discussion we must have $\psi_n^2(x_Q) = 0$.

- The polynomials ψ_n^2 and ϕ_n have degrees $n^2 - 1$ and n^2, respectively.

Using Equation (2.4), the point $P \neq O$ is divisible by n in $E(K)$ if and only if there exists a point $Q = (x_Q, y_Q) \in E(K)$ such that

$$x_P = \frac{\phi_n(x_Q)}{\psi_n^2(x_Q)}, \qquad y_P = \frac{\omega_n(x_Q, y_Q)}{\psi_n^3(x_Q, y_Q)}.$$

Focusing on the equation for x_P, we must have that

$$\phi_n(x_Q) - x_P\psi_n^2(x_Q) = 0.$$

Thus x-coordinates of points Q with $nQ = P$ satisfy the polynomial

$$d_{n,P}(x) = \phi_n(x) - x_P\psi_n^2(x) = 0. \tag{2.5}$$

We call $d_{n,P}(x)$ the **n-division polynomial of the point P**.

Lemma 2.13 *Let $d_{n,P}(x)$ be the n-division polynomial of a point $P \in E(K)\backslash E[2](K)$. Then $d_{n,P}(x)$ has a root in K if and only if P is divisible by n in $E(K)$.*

Proof If P is divisible by n in $E(K)$, say $nQ = P$, use Equation (2.4) and repeat the above derivation to show that $d_{n,P}(x)$ has a root in K which is the x-coordinate of the point Q. Conversely, suppose $d_{n,P}(x_Q) = 0$ for some $x_Q \in K$. Since $d_{n,P}(x)$ is a polynomial of degree n^2 and there are n^2 n-division points of P in $\bar{K}$ all with distinct x-coordinates (since P is not 2-torsion), we have some $y_Q \in \bar{K}$ such that the point $Q = (x_Q, y_Q) \in E(\bar{K})$ has the property that $nQ = P$. Now, for any $\tau \in \mathrm{Gal}(\bar{K}/K)$, we have that

$$n \cdot \tau(Q) = P$$

with $x_{\tau(Q)} = x_Q$. Using the Weierstrass equation we then have $y_{\tau(Q)} = \pm y_Q$, so $\tau(Q) = \pm Q$. Since P is not 2-torsion we have that $P \neq -P$. Therefore we cannot have $\tau(Q) = -Q$, because otherwise $n \cdot \tau(Q) = n(-Q) = -nQ = -P \neq P$. Hence $\tau(Q) = Q$ for every $\tau \in \mathrm{Gal}(\bar{K}/K)$. Thus $y_Q \in K$.

Remark 2.14 *It is possible that $P \in E[2](K)$ and $d_{n,P}(x)$ has K-rational roots, but P is not divisible by n in $E(K)$. For example, let $n = 2$ and $K = \mathbb{Q}$. Set*

$$E : y^2 = x^3 + 503844x - 45019744.$$

Then $P = (88, 0) \in E[2](\mathbb{Q})$ with

$$d_{2,P}(x) = ((x - 814)(x + 638))^2,$$

but neither 814 nor -638 are x-coordinates of points in $E(\mathbb{Q})$ (but they are x-coordinates of points $Q \in E(\bar{\mathbb{Q}})$ with $2Q = P$).

■

2.5 The Mordell-Weil Theorem

In 1922, Mordell [7] proved the fundamental structure theorem about the group of rational points $E(\mathbb{Q})$ of an elliptic curve defined over $\mathbb{Q}$. Weil [21] generalized the theorem to abelian varieties defined over number fields, where the same statement holds.

Theorem 2.15 (Mordell, Weil) *Let K be a number field and let E/K be an elliptic curve. Then the group $E(K)$ is finitely generated; that is,*

$$E(K) \cong \mathbb{Z}^r \oplus E(K)_{tors}$$

where $E(K)_{tors}$ is the torsion subgroup. The constant r is called the ***rank*** *of $E(K)$.*

Given an elliptic curve E defined over K, how can one compute $E(K)$? Once one knows a bound on the size of the torsion subgroup using the results of Mazur [6] (for $K = \mathbb{Q}$) and Parent [8] (for a number field K), computing the torsion subgroup is simple by using the division polynomials discussed above. With far less machinery, for $K = \mathbb{Q}$ one can use the theorem of Lutz and Nagell to compute $E(\mathbb{Q})_{\mathrm{tors}}$; see [17, Chapter VIII §7]. However, there is currently no algorithm that provably terminates and computes r or free generators of the free subgroup.

3. ELLIPTIC SURFACES

Elliptic surfaces are algebraic surfaces that are built out of elliptic curves. In this way, one can use powerful tools from the theory of algebraic surfaces like the intersection pairing to study the arithmetic of elliptic curves; see Hartshorne [3, Chapter 5] for a primer on algebraic surfaces.

In this chapter, the goal is to provide enough background to rigorously understand the concept of specialization. Specialization links the "group of sections" of an elliptic surface with the groups of points on the elliptic fibers, leading us to the central questions which are addressed in this thesis; precisely when does specialization cause sections to collapse? In other words, when is the specialization map (not) injective? We will discuss effective ways to check this in chapters 4 and 5.

3.1 Definition and Basic Properties

Let k be a number field and C a smooth projective curve defined over k. We denote by $K = k(C)$ the function field of C and $C(k)$ the set of k-rational points of C.

Definition 3.1 *An* ***elliptic surface*** *is a projective algebraic surface $\mathcal{E}$ along with a morphism $\pi : \mathcal{E} \to C$ with the following properties.*

- *There exists a section $s_0 : C \to \mathcal{E}$ to π; that is, $\pi \circ s_0 = id_C$.*
- *For all but finitely many $t_0 \in C(\bar{k})$, the fiber $\mathcal{E}_{t_0} = \pi^{-1}(t_0)$ is an elliptic curve (with chosen point $s_0(t_0) = O_{t_0}$).*

If $C, \mathcal{E}, \pi$ and s_0 are defined over k, we say that $\mathcal{E} \to C$ is defined over k.

Let $\mathcal{E}(C)$ denote the set of sections of $\mathcal{E} \to C$, and if $\mathcal{E} \to C$ is defined over k we additionally define the set $\mathcal{E}(C/k)$ of sections defined over k. From this point forward, assume that all elliptic surfaces $\mathcal{E} \to C$ and projective curves C are defined over k.

Definition 3.2 *Let s_1, s_2 be two sections of the elliptic surface $\mathcal{E} \to C$. Define a section $s_1 \oplus_{\mathcal{E}} s_2$ in the following way: for any $t_0 \in C(\bar{k})$ for which the fiber $\mathcal{E}_{t_0}$ is an elliptic curve, set*

$$(s_1 \oplus_{\mathcal{E}} s_2)(t_0) = s_1(t_0) \oplus_{\mathcal{E}_{t_0}} s_2(t_0),$$

where $\oplus_{\mathcal{E}_{t_0}}$ denotes addition on the elliptic curve $(\mathcal{E}_{t_0}, O_{t_0})$.

Proposition 3.3 *The map $s_1 \oplus_{\mathcal{E}} s_2$ is a section, and the operation $\oplus_{\mathcal{E}}$ turns $\mathcal{E}(C)$ into an abelian group with identity element s_0. For sections defined over k, the same operation turns $\mathcal{E}(C/k)$ into a group.*

Proof [16, Chapter III Proposition 3.10.a, 3.10.b]. ■

Similar to the case of elliptic curves, elliptic surfaces also have a Weierstrass form. The primary difference is that elliptic surfaces are only guaranteed to be *birationally equivalent* to an elliptic surface in Weierstrass form instead of isomorphic to one.

Proposition 3.4 *Let $\mathcal{E} \to C$ be an elliptic surface defined over k.*

1. *There exist functions $A(t), B(t) \in K$ such that $\mathcal{E}$ is birationally equivalent over C to the surface in $\mathbb{P}^2 \times C$ defined by the equation*

   $$y^2 z = x^3 + A(t)xz^2 + B(t)z^3$$

   with morphism $([x : y : z], t) \mapsto t$.

2. *Let E, E' be elliptic curves over K given by*

   $$y^2 = x^3 + A(t)x + B(t),$$

   $$y^2 = x^3 + A'(t)x + B'(t).$$

Then E and E' are isomorphic over K if and only if the corresponding elliptic surfaces

$$zy^2 = x^3 + A(t)xz^2 + B(t)z^3,$$

$$zy^2 = x^3 + A'(t)xz^2 + B'(t)z^3,$$

are birationally equivalent over C.

Proof [16, Chapter III Proposition 3.8.a, 3.8.b.]. ■

Via Proposition 3.4, we see that we can associate an elliptic curve E defined over K, unique up to K-isomorphism, to each elliptic surface $\mathcal{E} \to C$. This elliptic curve is called the **generic fiber** of $\mathcal{E} \to C$. As with any elliptic curve, we can talk about the K-rational points of the curve, and they form a group. The group operation is given as follows.

Proposition 3.5 *Let $\mathcal{E} \to C$ be an elliptic surface defined over k and let E be the generic fiber given in Weierstrass form. Then there is an isomorphism of groups*

$$\begin{aligned} E(K) &\to \mathcal{E}(C/k) \\ (x_0, y_0) &\mapsto (t_0 \mapsto ([x_0(t_0) : y_0(t_0) : 1], t_0)) \\ O &\mapsto s_0. \end{aligned}$$

(The map on the right-hand side only makes sense for those t_0's which are not poles of the coefficients of the Weierstrass equation, so it makes sense on a nonempty open subset of C. Since C is smooth the map is therefore defined on all of C.) In particular, the group of sections is a birational invariant (over C).

Proof [16, Chapter III Proposition 3.10.c] ■

Thus studying the group of sections of an elliptic surface is the same as studying rational points on its generic fiber.

3.2 Mordell-Weil Theorem for Function Fields

As with elliptic curves over number fields, one can ask about the structure of the group of rational points of an elliptic curve over the function field $K = k(C)$ of a smooth projective curve C defined over a number field k. It turns out that there is a statement analogous to that of the Mordell-Weil Theorem in this case.

Theorem 3.6 *(Néron) Let K be a field that is finitely generated over $\mathbb{Q}$ and let E/K be an elliptic curve. Then the group of rational points $E(K)$ is finitely generated. The rank of this group is called the* ***Mordell-Weil rank*** *of the corresponding birational equivalence class of elliptic surfaces.*

Of course, examples of fields K satisfying the above condition are function fields of varieties defined over number fields, so this includes our case of interest with elliptic surfaces. However, some caution must be taken when dealing with stranger base fields. For instance, Theorem 3.6 is clearly false for $K = \mathbb{C}$, as E is a complex torus with uncountably many $\mathbb{C}$-rational points; see [17, Chapter 6] for details. Despite this, it will still often be true that $E(K)$ is finitely generated when K is a function field, including fields which are not finitely generated over their prime field such as $\mathbb{C}(t)$. To see what can go wrong with these fields, consider the following example.

Example 3.7 *Let E be the elliptic curve*

$$E : y^2 = x^3 + 1.$$

As with any elliptic curve defined over $\mathbb{C}$, $E(\mathbb{C})$ will be uncountable. We can also view this curve as an elliptic curve defined over $\mathbb{C}(t)$. Because $E(\mathbb{C}) \subset E(\mathbb{C}(t))$, we then have that $E(\mathbb{C}(t))$ is uncountable.

The issue here is that $E/\mathbb{C}(t)$ can be defined over $\mathbb{C}$. On the elliptic surface side, we have the following definition.

Definition 3.8 *Let $\mathcal{E} \to C$ be an elliptic surface defined over k. If there exists an elliptic curve E/k such that $\mathcal{E} \to C$ is birationally equivalent over C to the surface*

$$\begin{aligned} E \times C &\to C \\ (z_0, t_0) &\mapsto t_0, \end{aligned}$$

then $\mathcal{E} \to C$ is called a ***split*** *(or* ***isotrivial)*** ***elliptic surface****.*

Theorem 3.9 (Mordell-Weil Theorem for Function Fields) *Let k be a field, let C/k be a smooth projective curve, and let $\mathcal{E} \to C$ be a non-split elliptic surface defined over k. Then the group of sections $\mathcal{E}(C/k)$ is finitely generated.*

Proof [16, Chapter III §6]. ■

As in Section 2.5, we can ask how simple it is to actually compute the group of rational points of an elliptic curve defined over a function field. In some cases, one can determine the group algorithmically. For instance, let C be a smooth projective curve defined over $k = \mathbb{C}$. Using Shioda's theory of Mordell-Weil lattices [13], one can determine generators for the Mordell-Weil group of an elliptic curve defined over $K = k(C)$ as long as the corresponding elliptic surface is rational and non-split. In this case, one can prove that $C \cong \mathbb{P}^1$, and rationality is equivalent to being able to write the generic fiber E in Weierstrass form with $A, B \in k[t]$ where deg $A \leq 4$ and deg $B \leq 6$. If all one wants is the rank, Shioda provides an even simpler method for rational elliptic surfaces. Using the fact that the Néron-Severi rank of $\mathbb{P}^2$ is 10, the Shioda-Tate formula reduces to the remarkable formula

$$\operatorname{rank}(E(K)) = 8 - \sum_v (m_v - 1)$$

where the sum is taken over all fibers and m_v is the number of irreducible components of the fibers of the minimal model of $\mathcal{E} \to C$. The constants m_v can be computed using Tate's algorithm (see [16, Chapter IV §9]), making this computation able to be performed by computers. Tate's algorithm is implemented in Magma for elliptic curves defined over function fields, giving an easy way to check Mordell-Weil ranks of rational elliptic surfaces.

3.3 Specialization

Let $\pi : \mathcal{E} \to C$ be an elliptic surface defined over a number field k with generic fiber E/K given in Weierstrass form as

$$E : y^2 = x^3 + A(t)x + B(t).$$

As long as t_0 is not a pole of A or B, an elliptic fiber $\mathcal{E}_{t_0}$ has a Weierstrass equation

$$E_{t_0} : y^2 = x^3 + A(t_0)x + B(t_0)$$

obtained by evaluating the coefficient functions at t_0. In this way, evaluating K-rational points on E at t_0 gives k-rational points on E_{t_0}, yielding a map

$$\sigma_{t_0} : E(K) \to E_{t_0}(k).$$

For $P \in E(K)$, we use the notation P_{t_0} to denote $\sigma_{t_0}(P)$.

Definition 3.10 *The map σ_{t_0} is a group homomorphism called the* ***specialization homomorphism*** *(or* ***specialization map****) associated to $t_0 \in C(k)$.*

Using the isomorphism of Proposition 3.5, one can view σ_{t_0} with domain $\mathcal{E}(C/k)$. In this case, the map can be explicitly viewed as evaluating a section s at t_0; the fact that s is a section defined over k guarantees that the image lies in $E_{t_0}(k)$.

We will be chiefly concerned with the question of when σ_{t_0} is injective, and for which $t_0 \in C(k)$ this occurs. Let Σ be the set of all $t_0 \in C(k)$ for which σ_{t_0} is injective, and let $\bar{\Sigma}$ be the set of all $t_0 \in C(\bar{k})$ for which σ_{t_0} is injective. In the next chapter, after restricting to $k = \mathbb{Q}$ and $C = \mathbb{P}^1$, we will discuss in detail an explicit proof of Néron's specialization theorem which shows that Σ is infinite. For now, we will discuss the more powerful (and more abstract) Silverman's specialization theorem, which states that $C(k) \setminus \Sigma$ is in fact finite. More specifically, Silverman proved the following.

Theorem 3.11 (Silverman [15]) *Let $\mathcal{E} \to C$ be a non-split elliptic surface defined over a number field k with generic fiber E. Let $\delta \in Div(C)$ be a divisor of positive* *degree, and let* h_δ *be a Weil height function on* C *associated to* δ *(see [16, Chapter 3 §10]). Then there is a constant* $c > 0$ *such that*

$$\sigma_{t_0} : E(\bar{k}(C)) \to E_{t_0}(\bar{k})$$

is injective for all $t_0 \in C(\bar{k})$ *with* $h_\delta(t_0) > c$.

Proof [16, Chapter III Theorem 11.4]. ■

Corollary 3.12 *Use the same setup as Theorem 3.11. Then the set* Σ *of all* $t_0 \in C(k)$ *for which* σ_{t_0} *is injective has finite complement in* $C(k)$.

Proof We know that $(C(k) \setminus \Sigma) \subset \{t_0 \in C(k) \mid h_\delta(t_0) \leq c\}$. But since δ has positive degree, any set $T \subset C(k)$ for which $h_\delta(T)$ is bounded must be finite; see [16, Chapter 3 Theorem 10.3]. ■

The Weil height functions generalize the standard height functions on projective space. In particular, the standard height function h on $\mathbb{P}^1(\mathbb{Q})$, given by

$$h((a:b)) = \ln \max\{|a|, |b|\},$$

is a Weil height on $\mathbb{P}^1$ associated to any divisor of degree 1.

In the next chapter, without referring to the theory of heights, we will discuss a concrete way of finding an infinite subset $S \subset \Sigma$ such that, for any $t_0 \in S$, σ_{t_0} is injective. Before proceeding on to this discussion, we take note of a much simpler case.

Suppose $G < E(\mathbb{Q}(t))$ is a subgroup of rank 1 with free generator Q and torsion points $T_0 = O, T_1, ..., T_n$. Let $t_0 \in C(k)$ such that the specialized curve E_{t_0} is an elliptic curve.

Proposition 3.13 *The specialization map* $\sigma_{t_0}|_G$ *is injective if and only if* $\sigma_{t_0}(Q) = Q_{t_0}$ *is not a torsion point on the specialized curve* E_{t_0}.

Proof First, suppose that Q_{t_0} is torsion; that is, $nQ_{t_0} = O_{t_0}$ for some $n \geq 1$. Since Q has infinite order, $P = nQ \neq O$. Thus

$$\sigma_{t_0}(P) = \sigma_{t_0}(nQ) = nQ_{t_0} = O_{t_0}.$$

Hence P is a nonzero element of $\ker(\sigma_{t_0})$, so that $\sigma_{t_0}|_G$ is not injective. Conversely, assume that $\sigma_{t_0}|_G$ is not injective. Then there is some $P \in \ker(\sigma_{t_0}) \cap G$ with $P \neq O$. Hence $P = nQ + T_i$ for some nonzero $n \in \mathbb{Z}$, where $n \neq 0$ because specialization is always injective on torsion (see [17, Chapter VII §3]). If T_i has order $k \geq 1$, then

$$kP = k(nQ + T_i) = knQ,$$

so that

$$kn(\sigma_{t_0}(Q)) = O_{t_0}.$$

Thus Q_{t_0} is torsion. ■

Thus checking if a specialization map is injective for G amounts to checking if Q_{t_0} is torsion. This can be done effectively; indeed, Parent [8] offers an effective uniform bound d_k such that for any elliptic curve F/k we have $|F(k)_{\text{tors}}| < d_k$.

Corollary 3.14 *Let d_k be as above. Then the specialization map $\sigma_{t_0}|_G$ is injective if and only if $nQ_{t_0} \neq O_{t_0}$ for any integer n with $1 \leq n \leq d_k$.*

This condition is simple to check using any computer algebra system with elliptic curve packages such as Sage.

4. SPECIALIZATION AND IRREDUCIBILITY

If one follows the proof of Silverman's Specialization Theorem (Theorem 3.11), one could, in principle, find the given height bound and thus find the finitely many $t_0 \in C(k)$ for which the corresponding specialization map σ_{t_0} fails to be injective. However, as remarked by Gusić and Tadić [2], the obtained bounds are too large to be useful. In this chapter and the next, we consider other methods to find t_0's for which the specialization map is injective. More specifically, we will discuss some approaches to answering the following two questions.

1. Given some $t_0 \in \mathbb{Q}$, how can we effectively determine whether or not the specialization map at t_0 is injective?
2. What is the set Σ of $t_0 \in \mathbb{Q}$ such that the specialization map at t_0 is injective?

In this chapter, we approach these questions from the perspective of irreducibility. We review the classical Néron specialization theorem to relate the above questions to the question of irreducibility of polynomials after specialization, and we give an algorithm that can be used to find a Hilbert set which intersects Σ in an infinite set S. The algorithm is effective in certain cases, and we carry out the algorithm on some examples. The approach taken in this chapter was inspired by a mathoverflow post by Silverman [18].

4.1 Hilbert Sets

We begin by reviewing the basics on Hilbert sets that are used in the proof of Néron's specialization theorem. For the sake of concreteness, we restrict our attention to our specific case of elliptic curves over $\mathbb{Q}(t)$. For more details about Hilbert sets and Hilbert's irreducibility theorem in greater generality, see Lang [5].

Definition 4.1 *Let* $f_1(t,x), ..., f_n(t,x) \in \mathbb{Q}[t,x]$ *be irreducible polynomials over* $\mathbb{Q}$. *The* Hilbert subset of $\mathbb{Q}$ *corresponding to the* f_i*'s is the set of all* $t_0 \in \mathbb{Q}$ *such that each* $f_i(t_0, x) \in \mathbb{Q}[x]$ *is irreducible over* $\mathbb{Q}$. *That is, the Hilbert subset is the set of* t_0*'s for which all the polynomials remain irreducible upon specialization at* $t = t_0$.

Notice that the intersection of any two Hilbert sets is a Hilbert set - it corresponds to the union of the sets of polynomials defining the two Hilbert sets.

Theorem 4.2 (Hilbert's Irreducibility Theorem) *Every Hilbert subset of* $\mathbb{Q}$ *is infinite.*

Proof [5, Chapter 9 §2 Corollary 2.5]. ■

Recall that the natural density of a subset T of $\mathbb{N}$ is the limit

$$\lim_{n\to\infty} \frac{\#\{k \in T \mid k \leq n\}}{n}.$$

Proposition 4.3 *For any Hilbert subset* H *of* $\mathbb{Q}$, $H \cap \mathbb{N}$ *has natural density 1.*

Proof Lang [5, Chapter 9 §2 Corollary 2.3] states that, for n large enough,

$$n - n^{\alpha} \leq \#\{k \in H \cap \mathbb{N} \mid k \leq n\}$$

for some fixed α with $0 < \alpha < 1$ independent of n. Hence for n large enough, we have

$$1 - \frac{1}{n^{1-\alpha}} \leq \frac{\#\{k \in H \cap \mathbb{N} \mid k \leq n\}}{n} \leq 1,$$

so

$$\lim_{n\to\infty} \frac{\#\{k \in H \cap \mathbb{N} \mid k \leq n\}}{n} = 1.$$

■

4.2 Néron's Specialization Theorem

Néron's specialization theorem (for elliptic curves) is the result of applying Hilbert's irreducibility theorem to division polynomials, as discussed in chapter 2. Following Serre [11, Chapter 11], we start with a completely group-theoretic fact.

Proposition 4.4 *Let n be a positive integer and let $\phi : M \to N$ be a homomorphism of abelian groups with the following properties.*

1. *M is finitely generated.*
2. *The induced map $\bar{\phi} : M/nM \to N/nN$ is injective.*
3. *$\phi|_{M[n]}$ gives an isomorphism $M[n] \cong N[n]$.*
4. *$\phi|_{M_{tors}}$ is injective.*

Then ϕ is injective.

Proof Let $I = \ker \phi$. Since M is finitely generated, so is I. If we show that $I = nI$, Nakayama's lemma implies that $rI = 0$ for some r with $r \equiv 1 \bmod n$, so I is torsion. But condition 4 says I is torsion-free, so we must have $I = 0$.

So let $x \in I$. Since $\phi(x) = 0 \in nN$, $\bar{\phi}(x) = 0$. By injectivity of $\bar{\phi}$, $x \in nM$. Write $x = ny$ for some $y \in M$. Then $n\phi(y) = \phi(x) = 0$, so $\phi(y) \in N[n]$. By condition 3, we can find some $z \in M[n]$ with $\phi(z) = \phi(y)$. Thus $y - z \in I$, and since $nz = 0$ we have $x = ny = ny - nz = n(y - z) \in nI$. ■

Fix an elliptic curve E over $\mathbb{Q}(t)$, and set $\phi = \sigma_{t_0}$ the specialization homomorphism for a fixed $t_0 \in \mathbb{Q}$, $M = E(\mathbb{Q}(t))$, $N = E_{t_0}(\mathbb{Q})$ and a positive integer $n \geq 2$. Then conditions 1 and 4 above are always true; indeed, condition 1 is the function field version of the Mordell-Weil Theorem (Theorem 3.6), and condition 4 follows from basic results on formal groups of elliptic curves and their relationship to reduction mod p found in Silverman [17, Chapter VII §3]. It is true that conditions 2 and 3 hold inside of a Hilbert set, but instead of proving this fact directly we will replace

$E(\mathbb{Q}(t))$ with specific subgroups (which will include $E(\mathbb{Q}(t))$ itself) and prove a more general statement.

First, notice that condition 2 is equivalent to the following statement.

$$\text{For any } a \in M \text{ such that } \phi(a) \text{ is divisible by } n \text{ in } N, a \text{ is divisible by } n \text{ in } M. \tag{4.1}$$

Now suppose $M < E(\mathbb{Q}(t))$ and $\phi = \sigma_{t_0}|_M$. If we have some $a \in M$ with $\phi(a)$ divisible by n, then even if we are able to conclude that a is divisible by n in $E(\mathbb{Q}(t))$, say $a = nb$ for some $b \in E(\mathbb{Q}(t))$, in order to verify (4.1) we would be required to check that $b \in M$. Unfortunately, this is a difficult problem. To avoid this, we will restrict ourselves to subgroups M in which whenever $a \in M$ has the property that $a = nb$ for some $b \in E(\mathbb{Q}(t))$, we always know that $b \in M$. That is, condition 2 of Proposition 4.4 is satisfied for the inclusion $M \to E(\mathbb{Q}(t))$. Of course, this isn't always true; for example, if a subgroup $G < E(\mathbb{Q}(t))$ contains an element of infinite order then $M = nG$ always fails to have this property (recall that G is finitely generated). Regarding condition 3, since specialization is always injective on torsion, note that if $M[n]$ is a proper subgroup of $E[n](\mathbb{Q}(t))$, then $\phi(M[n])$ is also always a proper subgroup of $E_{t_0}[n](\mathbb{Q})$. Hence we also make the minor additional assumption that $M[n] = E[n](\mathbb{Q}(t))$. Thus we will assume all hypotheses of Proposition 4.4 for the inclusion $M \to E(\mathbb{Q}(t))$.

Now suppose that we have $M < E(\mathbb{Q}(t))$ with the inclusion satisfying the hypotheses of Proposition 4.4, $N = E_{t_0}(\mathbb{Q})$ and $\phi = \sigma_{t_0}$. In our goal of finding a Hilbert set on which conditions 2 and 3 of Proposition 4.4 hold for these very specific M, N, ϕ, one might hope that we could discard either condition 2 or 3 and still maintain the conclusion of Proposition 4.4. Unfortunately neither condition implies the other, as the following two examples illustrate.

Example 4.5 *(2 holds, but not 3) Let* $E : y^2 = x^3 - (t^2 + 27)x + (10t^2 + 48t + 90)$, $\phi = \sigma_{30}$, $M = E(\mathbb{Q}(t))$, $N = E_{30}(\mathbb{Q})$ *and* $n = 2$. *In [14], this elliptic curve is shown to have Mordell-Weil rank 4 and to have no nontrivial torsion points over* $\mathbb{Q}(t)$. *The Mordell-Weil group is generated by the four points* $P_1 = (9, t + 24), P_2 =$

$(6, 2t+12)$, $P_3 = (1, 3t+8)$ *and* $P_4 = (t+3, 4t+6)$*, so a complete set of representatives for the nonidentity cosets of* $2E(\mathbb{Q}(t))$ *in* $E(\mathbb{Q}(t))$ *is*

$$\left\{ \sum_{i \in C} P_i \mid C \subset \{1, 2, 3, 4\}, C \neq \emptyset \right\}.$$

One can check (for instance, using the `EllipticCurve` *method* `division_points(2)` *in Sage) that for* $t = 30$ *the specialization of each of these 15 points is not divisible by 2 in* E_{30}*. Thus* $\overline{\sigma_{30}} : E(\mathbb{Q}(t))/2E(\mathbb{Q}(t)) \to E_{30}(\mathbb{Q})/2E_{30}(\mathbb{Q})$ *is injective. However, the Mordell-Weil group of* E_{30} *is* $\mathbb{Z}^3 \times \mathbb{Z}/2\mathbb{Z}$*, so* σ_{30} *cannot be injective. In particular, condition 3 of Proposition 4.4 does not hold, but condition 2 does hold.*

Example 4.6 *(3 holds, but not 2) Let* $E : y^2 = x^3 - t^2x + t^2, \phi = \sigma_2$*,* $M = E(\mathbb{Q}(t))$*,* $N = E_2(\mathbb{Q})$ *and* $n = 2$*. Then, as we will show in §4.3.1,* $E(\mathbb{Q}(t)) \cong \mathbb{Z}^2$ *with generators*

$$P = (t, t), Q = (0, t).$$

Using Sage, one can check that the specialization E_2 *has* $E_2(\mathbb{Q}) \cong \mathbb{Z}$*. Hence* $\overline{\sigma_2}$ *is a map from a group of order 4 to a group of order 2, so* $\overline{\sigma_2}$ *cannot be injective.*

Thus we will need to check both of the conditions as part of the following proof of Néron's specialization theorem for subgroups. For a more general statement of Néron's specialization theorem, see [5].

Theorem 4.7 *Let* $E/\mathbb{Q}(t)$ *be a nonconstant elliptic curve given by the Weierstrass equation*

$$y^2 = x^3 + A(t)x + B(t)$$

and let $M < E(\mathbb{Q}(t))$ *be a subgroup of rank at least 1 such that the inclusion* $M \to E(\mathbb{Q}(t))$ *satisfies the hypotheses of Proposition 4.4. Then there exists a set* S_M *which differs from a Hilbert set by finitely many elements such that for each* $t_0 \in S_M$ *the specialization map* $\sigma_{t_0}|_M : M \to E_{t_0}(\mathbb{Q})$ *is injective.*

Proof By the preceding comments, it suffices to show that the set of $t_0 \in \mathbb{Q}$ for which $\phi = \sigma_{t_0}|_M$ satisfies conditions 2 and 3 of Proposition 4.4 differs from a Hilbert set by finitely many elements. Let $P_1, ..., P_k$ be a a set of representatives for the nonzero elements of M/nM. Since M has rank at least 1, by possibly changing some of the P_i's by an element of nM we may assume that no P_i is 2-torsion. Let $d_{n,P_i}(t,x)$ be the n-division polynomial of P_i (§2.4). After clearing denominators, we may assume $d_{n,P_i}(t,x) \in \mathbb{Q}[t][x]$. Because condition 2 of Proposition 4.4 holds for the inclusion $M \to E(\mathbb{Q}(t))$, no P_i is divisible by n in $E(\mathbb{Q}(t))$ and thus, by Lemma 2.13 each $d_{n,P_i}(t,x)$ has no roots in $\mathbb{Q}(t)$ as a polynomial in x - that is, the irreducible factorization of $d_{n,P_i}(t,x)$ in $\mathbb{Q}[t][x]$ has no factors with (x-)degree 1. Let H_1 be the Hilbert set corresponding to all irreducible factors of all the d_{n,P_i}'s, then remove any rational number from H_1 which appears as a zero of a coefficient in an irreducible factor; call this set S_1. Then by Hilbert's irreducibility theorem, for any $t_0 \in S_1$ each irreducible factor of each $d_{n,P_i}(t,x)$ remains irreducible upon specialization, and since none of the coefficients vanish the x-degree is preserved, and thus $d_{n,P_i}(t_0,x)$ has no roots in $\mathbb{Q}$. Since the roots of this polynomial are x-coordinates of points Q_{t_0} such that $nQ_{t_0} = P_{i,t_0}$, P_{i,t_0} is not divisible by n in $E_{t_0}(\mathbb{Q})$, and thus condition 2 is satisfied.

Next, using notation from §2.4, consider the polynomial ψ_n^2. Recall that this polynomial has the set of x-coordinates of the n-torsion points of $E(\overline{\mathbb{Q}(t)})$ as its roots. Clearing denominators, we assume that $\psi_n^2 \in \mathbb{Q}[t][x]$. Let $\{r_1, ..., r_l\}$ be the $\mathbb{Q}(t)$-rational roots of ψ_n^2 which do not correspond to $\mathbb{Q}(t)$-rational n-torsion points (by Remark 2.14 this is a possibility when n is even), and let $f_1, ..., f_l$ be the polynomials obtained by clearing the denominators in the expressions

$$x^2 - (r_i^3 + A(t)r_i + B(t)).$$

Notice that, since each r_i is not the x-coordinate of a point in $E(\mathbb{Q}(t))$, we have that each f_i is irreducible over $E(\mathbb{Q}(t))$. Let H_2 be the Hilbert set corresponding to the irreducible factors of ψ_n^2 of degree at least 2 and the polynomials f_i, and then remove any rational number from H_2 which appears as a zero of a coefficient; call this set S_2. Then, upon specialization at $t_0 \in S_2$, each irreducible factor of degree at least 2 remains irreducible of degree at least 2, and the fact that the polynomials f_i remain irreducible of x-degree 2 means that $r_i(t_0)^3 + A(t_0)r_i(t_0) + B(t_0)$ is not a square in $\mathbb{Q}$ so that $r_i(t_0)$ is not the x-coordinate of a point in $E_{t_0}(\mathbb{Q})$. Because of this, E_{t_0} gains no new $\mathbb{Q}$-rational n-torsion points, so condition 3 is satisfied. Recall that specialization is injective on torsion.

Finally, remove from $S_1 \cap S_2$ the poles of A, the poles of B and all t_0 such that E_{t_0} is not smooth; call this set S_M. Then S_M has the required property. ■

Corollary 4.8 *Let E and M be as in Theorem 4.7. Then the set Σ_M of all $k_0 \in \mathbb{N}$ such that the specialization map $\sigma_{k_0}|_M$ is injective has density 1.*

Proof Proposition 4.3. ■

We conclude the section with a summary of how the previous proof yields an algorithm that can often be used to check when a specialization map is injective.

Algorithm 4.9 *Let $E/\mathbb{Q}(t)$ be an elliptic curve given by a Weierstrass equation and let M be a subgroup as in Theorem 4.7.*

1. *Let $\{P_1, ..., P_k\}$ be a set of representatives of the nonzero cosets of nM in M, taking care not to choose a 2-torsion point.*

2. *For each P_i, compute $d_{n,P_i}(t,x)$ and clear denominators to assume that*

$$d_{n,P_i}(t,x) \in \mathbb{Q}[t][x].$$

3. *Compute the collection of polynomials f_i as in Theorem 4.7 and the non-linear irreducible factors of the division polynomial ψ_n^2.*

4. *Compute the Hilbert set corresponding to the irreducible factors of the polynomials above, then compute the set S_M as in Theorem 4.7 by removing the poles of A, the poles of B and those t_0's for which coefficients of at least one of the above polynomials vanish or E_{t_0} is not smooth.*

Remark 4.10 *In practice, one only needs that the specialized polynomials have no roots, which is weaker than asking that all irreducible factors remains irreducible.*

Remark 4.11 *Notice that step 4 requires checking that various irreducible factors remain irreducible upon specialization; for a fixed* $t_0 \in \mathbb{Q}$*, this can often be done by inspection or with computer software such as Sage.*

Remark 4.12 *Let* E *be an elliptic curve in Weierstrass form defined over the function field* K *of a curve defined over a number field* k*, and suppose the curve is given by an explicit equation. While Algorithm 4.9 was written specifically for elliptic curves over* $\mathbb{Q}(t)$*, the above algorithm can be adjusted to work for specializing at* k*-rational points of the curve. In particular, it can be used to check injectivity of a specific specialization map, as in Remark 4.11.*

4.3 Examples Using the Irreducibility Algorithm

In this section, we discuss some explicit examples of utilizing Algorithm 4.9 with the modification mentioned in Remark 4.10. We consider two examples, one with a full Mordell-Weil group of rank 2 and another with a subgroup of rank 2.

4.3.1 $y^2 = x^3 - t^2x + t^2$

Set $E : y^2 = x^3 - t^2x + t^2$. Our goal is to find an infinite set of rational numbers for which the corresponding specialization maps (on all of $E(\mathbb{Q}(t))$) are injective. First, we need generators of $E(\mathbb{Q}(t))$ in order to use Algorithm 4.9. Set $P = (t, t)$ and $Q = (0, t)$. One can check (using Magma [1]) that the determinant of the canonical height matrix of P and Q is nonzero, and thus P and Q are linearly independent in $E(\mathbb{Q}(t))$. In addition, using Magma's implementation of Tate's algorithm [16, Chapter IV §9] and combining the resulting information with the Shioda-Tate formula [13], the Mordell-Weil rank of $E/\overline{\mathbb{Q}}(t)$ is 2. Hence the rank of $E(\mathbb{Q}(t))$ is 2. In order to show that P and Q generate $E(\mathbb{Q}(t))$, we will use specialization in a way that is motivated by (but different from) the method outlined in [19]. First, we show that $E(\mathbb{Q}(t))$ has trivial torsion. Since specialization is injective on torsion, it suffices to show that a single specialization has trivial torsion. To see this, consider the following example, which (at the same time) highlights Remark 4.11 and shows how injectivity of the specialization map for an individual $t_0 \in \mathbb{Q}$ can often be checked directly using a computer algebra system such as Sage [20].

Example 4.13 *Let $t_0 = 5$ and let $M = \langle P, Q \rangle$. Consider the specialized curve*

$$E_5 : y^2 = x^3 - 25x + 25.$$

Note that

$$\begin{aligned} M/2M &= \{0, P, Q, P+Q\} \\ &= \{0, (t,t), (0,t), (-t,-t)\}. \end{aligned}$$

Run the following code in a Sage worksheet.

```
t = 5
Espec = EllipticCurve([-t^2,t^2])
Pspec = Espec(t,t)
Qspec = Espec(0,t)
print("The 2-division points of Pspec are: "
    + str(Pspec.division_points(2)))
print("The 2-division points of Qspec are: "
    + str(Qspec.division_points(2)))
print("The 2-division points of Pspec+Qspec are: "
    + str((Pspec+Qspec).division_points(2)))
print("The torsion points of Espec are: "
    + str(Espec.torsion_points()))
```

The output is the following.

```
The 2-division points of Pspec are: []
The 2-division points of Qspec are: []
The 2-division points of Pspec+Qspec are: []
The torsion points of Espec are: [(0 : 1 : 0)]
```

We interpret the output as follows. In the context of Proposition 4.4, set $\phi = \sigma_5|_M$, $N = E_5(\mathbb{Q})$, $n = 2$ *and use* M *as already defined. First, since* $E_5(\mathbb{Q})$ *has no torsion and specialization is injective on torsion, we see that* $E(\mathbb{Q}(t))$ *(and thus* M*) also has no torsion. Thus condition 3 holds. Condition 2 is equivalent to the generators of* $M/2M$ *not being divisible by 2 in* $E(\mathbb{Q})$ *upon specialization, which is shown by the above output. Hence condition 2 holds. Finally, we need to show that conditions 2 and 3 hold for the inclusion* $M \to E(\mathbb{Q}(t))$*. Clearly condition 3 holds since we've shown that* $E(\mathbb{Q}(t))$ *has no torsion, and we can show condition 2 by using Sage to show that* P, Q *and* $P+Q$ *have no 2-division points in* $E(\mathbb{Q}(t))$ *using similar commands to those above. Thus the specialization map* $\sigma_5|_M$ *is injective.*

It remains to show that P and Q generate $E(\mathbb{Q}(t))$. Consider the specialization at $t_0 = 5$ as in Example 4.13. Sage yields that E_5 has Mordell-Weil group $\mathbb{Z}^2$ over $\mathbb{Q}$ with generators $(-1, 7)$ and $(0, 5)$. Since $(-1, 7) + (0, 5) = (5, 5)$, we may instead use $(5, 5) = P_5$ and $(0, 5) = Q_5$ as generators. Fix the bases $\{P, Q\}, \{P_5, Q_5\}$ for $M, E_5(\mathbb{Q})$, respectively. After fixing some basis for $E(\mathbb{Q}(t))$ (which has 2 elements), we let the matrix A represent the inclusion $M \to E(\mathbb{Q}(t))$ and the matrix B represent the specialization map σ_5. We then have a sequence

$$M \overset{A}{\to} E(\mathbb{Q}(t)) \overset{B}{\to} E_5(\mathbb{Q}).$$

The composition BA is the specialization map $\sigma_5|_M$. Since this maps generators of M to generators of $E_5(\mathbb{Q})$, BA is the identity matrix. Hence A is invertible, so the inclusion $M \to E(\mathbb{Q}(t))$ is surjective. Hence $E(\mathbb{Q}(t)) \cong \mathbb{Z}^2$ with generators $P = (t, t)$ and $Q = (0, t)$.

Before moving forward with using Algorithm 4.9 to find injective specialization maps, it is important to notice that success of this method for a fixed n is not equivalent to injectivity of the specialization map. We can't hope for this to be true since it succeeds on (most of) a Hilbert set and Hilbert sets often have infinite complements, whereas Silverman's specialization theorem states that the specialization map fails to be injective for only finitely many rational numbers. The next example illustrates the failure of this equivalence.

Example 4.14 *Let* $t_0 = 27$*. On the elliptic curve* $E_{27} : y^2 = x^3 - 729x + 729$*, notice that*

$$[2](-9, 81) = (27, 27) = P_{27},$$

so our criterion (for $n = 2$*) cannot conclude that* σ_{27} *is injective because condition 2 of Proposition 4.4 fails. A check using Sage shows that* $E_{27}(\mathbb{Q}) \cong \mathbb{Z}^2$ *with generators* $R_1 = (-9, 81)$ *and* $R_2 = (-27, 27)$*. Now* $P_{27} = 2R_1$ *and* $Q_{27} = -(2R_1 + R_2)$*, meaning the matrix of the specialization map* σ_{27} *with respect to the ordered bases* $\{P, Q\}$ *and* $\{R_1, R_2\}$ *is*

$$\begin{bmatrix} 2 & -2 \\ 0 & -1 \end{bmatrix}.$$

The determinant of this matrix is $-2 \neq 0$*, so* σ_{27} *is injective.*

We now carry out Algorithm 4.9 for $n = 2$. As in §2.4, we find the the polynomials in steps 3 and 4 to be

$$\begin{aligned} d_{2,P}(t,x) &= x^4 + 2t^2x^2 - 8t^2x + t^4 - t(4x^3 - 4t^2x + 4t^2), \\ d_{2,Q}(t,x) &= x^4 + 2t^2x^2 - 8t^2x + t^4, \\ d_{2,P+Q}(t,x) &= x^4 + 2t^2x^2 - 8t^2x + t^4 + t(4x^3 - 4t^2x + 4t^2), \text{ and} \\ g(t,x) &= x^3 - t^2x + t^2, \end{aligned}$$

where $g(t,x) = \psi_2^2/4$. Notice that all four polynomials are irreducible over $\mathbb{Q}[t,x]$. As in Remark 4.10, we need to find t_0's for which the specialized polynomials have no roots in $\mathbb{Q}$. Equivalently, we need to find t_0's for which the curves defined by the polynomials have no rational points of the form (t_0, x_0). Set

$$\begin{aligned} C_P &: d_{2,P}(t,x) = 0, \\ C_Q &: d_{2,Q}(t,x) = 0, \\ C_{P+Q} &: d_{2,P+Q}(t,x) = 0 \\ C_2 &: g(t,x) = 0. \end{aligned}$$

Using Sage, all of the curves are rational over $\mathbb{Q}$ and have rational points, hence they have infinitely many rational points. Because of this, we will restrict to $t_0 \in \mathbb{N}$ and examine the case of specializing at natural numbers, which similarly reduces to looking at integral points on the curves (since each polynomial is monic in x). We first prove, using elementary methods, that the only obstruction to success of the method for $t_0 > 2$ comes from C_P. We begin with an algebraic lemma which will make analyzing C_{P+Q} easy.

Lemma 4.15 *[10] Consider a (depressed) quartic polynomial*

$$p(x) = x^4 + qx^2 + rx + s \in \mathbb{Q}[x]$$

with discriminant $\Delta > 0$. If $q < 0$ and $s < q^2/4$, then p has four distinct roots in $\mathbb{C} \setminus \mathbb{R}$.

Proposition 4.16 *The curves C_{P+Q}, C_Q and C_2 each have no integral points with $t_0 > 2$.*

Proof C_{P+Q}: Notice that the discriminant of $d_{2,P+Q}$ as a polynomial in x is

$$16384t^{10} - 110592t^8.$$

This is positive for $t_0 > 2$. The corresponding depressed quartic (in x) is

$$x^4 - 4t^2x^2 - 8t^2x + 4t^4 + 12t^3.$$

By Lemma 4.15, this quartic has no real roots in x for $t_0 > 2$.

C_Q: Fix $t_0 \in \mathbb{N}$ and suppose (t_0, x_0) is an integral point on C_Q. We make 3 cases based on possible values of x_0.

Case 1: If $x_0 \leq 0$, each nonzero term of $d_{2,Q}(t_0, x_0)$ is positive. Thus (t_0, x_0) is not a point on C_Q.

Case 2: Let $x_0 \geq 4$. Note that

$$d_{2,Q}(t_0, x_0) = x_0^4 + 2t_0^2x_0^2 - 8t_0^2x_0 + t_0^4 \geq 256 + 32t_0^2 - 32t_0^2 + t_0^4 = 256 + t_0^4 > 0,$$

so (t_0, x_0) is not a point on C_Q.

Case 3: Suppose $1 \leq x_0 \leq 3$. We have the following three polynomials in t:

$$d_{2,Q}(t,1) = t^4 - 6t^2 + 1,$$

$$d_{2,Q}(t,2) = t^4 - 8t^2 + 16, \text{ and}$$

$$d_{2,Q}(t,3) = t^4 - 6t^2 + 81.$$

The only one with a root is $d_{2,Q}(t,2)$ with $t_0 = 2$ as a root, yielding the integral point $(2,2)$.

C_2: Notice that (t_0, x_0) is an integral point on C_2 if and only if

$$x_0^3 = (x_0 - 1)t_0^2.$$

Noting that there are no solutions with $x_0 - 1 = 0$, we see that $x_0 - 1 | x_0^3$. Since x_0 and $x_0 - 1$ share no prime factors, we must have that $x_0 - 1$ is ± 1. So we have two possibilities for the ordered pair $(x_0, x_0 - 1)$:

$$(x_0, x_0 - 1) = (2, 1) \qquad \text{or} \qquad (x_0, x_0 - 1) = (0, -1).$$

In the first case we have $8 = t_0^2$, yielding no integral (or rational) solutions. In the second, we must have $t_0 = 0$. Hence the only integral point on C_2 is $(t_0, x_0) = (0, 0)$.

■

Note that the $t_0 > 2$ restriction is required because C_Q has the point $(2,2)$.

Corollary 4.17 *Let $t_0 > 2$ be a natural number. If the curve C_P has no integral points of the form (t_0, x_0), then the specialization map σ_{t_0} is injective.*

In order to work directly with the integral points of C_P, we will utilize the algorithm of Poulakis and Voskos [9]. This relates finding integral points on genus zero curves to solving Pell-like equations. The algorithm depends on the number of "valuations at infinity" (henceforth called points at infinity) of the curve; that is, points defined over $\overline{\mathbb{Q}}$ lying in the closure of C_P in $\mathbb{P}^2$ but not on C_P itself. Homogenizing $d_{2,P}$ then setting the new variable to zero, we obtain the equation

$$x^4 - 4tx^3 + 2t^2x^2 + 4t^3x + t^4 = 0. \tag{4.2}$$

Setting $t = 1$, we have

$$\begin{aligned} x^4 - 4x^3 + 2x^2 - 4x + 1 &= 0 \\ (x^2 - 2x - 1)^2 &= 0. \end{aligned}$$

On the other hand, setting $x = 1$ we similarly obtain

$$(t^2 + 2t - 1)^2 = 0.$$

So if σ is a root of $x^2 - 2x - 1$ and τ is a root of $t^2 + 2t - 1$, the points at infinity are

$$(1 : \sigma : 0), (1 : \bar{\sigma} : 0), (\tau : 1 : 0), (\bar{\tau} : 1 : 0).$$

However, notice that $1/\tau$ is a root of $x^2 - 2x - 1$: indeed,

$$\left(\frac{1}{\tau}\right)^2 - 2\frac{1}{\tau} - 1 = \frac{1 - 2\tau - \tau^2}{\tau^2} = -\frac{\tau^2 + 2\tau - 1}{\tau^2} = 0.$$

Hence of the four points listed above only two are distinct. Thus C_P has two points at infinity. Poulakis and Voskos now proceed as follows.

1. We first need to determine the singularities of the projective closure of C_P. Sage quickly yields $(0 : 0 : 1)$ as the only singular point.

2. Using Sage, we obtain the rational parameterization

   $$(a : b) \to (8ab^3 + 4b^4 : 8a^2b^2 + 4ab^3 : a^4 - 4a^3b + 2a^2b^2 + 4ab^3 + b^4).$$

   Notice that the third component comes from Equation (4.2); in particular,

   $$a^4 - 4a^3b + 2a^2b^2 + 4ab^3 + b^4 = (a^2 - 2ab - b^2)^2.$$

3. Set $u = 2a - 2b$ and $v = b$. Then $a = u/2 + v$ and $b = v$. After this change of variables, our birational map becomes

$$(u : v) \to \left(4uv^3 + 12v^4 : 2u^2v^2 + 10uv^3 + 12v^4 : \frac{1}{16}(u^2 - 8v^2)^2\right).$$

   Equivalently, we have

$$(u : v) \to (16(4uv^3 + 12v^4) : 16(2u^2v^2 + 10uv^3 + 12v^4) : (u^2 - 8v^2)^2).$$

   Set $p(u, v) = 16(4uv^3 + 12v^4)$ and $q(u, v) = 16(2u^2v^2 + 10uv^3 + 12v^4)$.

4. The resultant R_1 of $p(u, 1)$ and $u^2 - 8$ is 2^{12}, and the resultant R_2 of $q(u, 1)$ and $u^2 - 8$ is -2^{12}. Thus we set $D = \gcd(R_1, R_2) = 2^{12}$.

5. Every integral point (t_0, x_0) on C_P is then obtained in the following way. Let $(u_0, v_0) \in \mathbb{Z}^2$ be a solution to an equation of the form $u^2 - 8v^2 = k$ for some $k|D$ with $u_0 \geq 0$ and $\gcd(u_0, v_0) = 1$. Then we have

$$t_0 = \frac{p(u_0, v_0)}{(u_0^2 - 8v_0^2)^2}, \qquad x_0 = \frac{q(u_0, v_0)}{(u_0^2 - 8v_0^2)^2}. \tag{4.3}$$

So the specialization map σ_{t_0} is injective for any t_0 which cannot be written in the form as given in (4.3). We will now make this even more explicit by solving the Pell-like equations given above. Many of the equations $u^2 - 8v^2 = k$ have no solutions of the required form, so we identify those first.

Lemma 4.18 *Let $l \in \mathbb{Z}$ with $l \geq 4$ or $l = 2$ and let $m \in \mathbb{Z}$ with $m \geq 4$. The equations $u^2 - 8v^2 = 2^l$ and $u^2 - 8v^2 = -2^m$ have no solutions of the form (u_0, v_0) with $(u_0, v_0) \in \mathbb{Z}^2$ and gcd$(u_0, v_0) = 1$. In addition, the three equations*

$$u^2 - 8v^2 = -2$$
$$u^2 - 8v^2 = -1, \text{ and}$$
$$u^2 - 8v^2 = 2$$

have no integer solutions at all.

Proof Let $(u_0, v_0) \in \mathbb{Z}^2$. Suppose $u_0^2 - 8v_0^2 = 2^l$ with $l \geq 4$. Then $8|u_0^2$, so necessarily $4|u_0$. Write $u_0 = 4k$ for some $k \in \mathbb{Z}$. We then have

$$2k^2 - v_0^2 = 2^{l-3},$$

where $l - 3 \geq 1$. Hence $2|v_0^2$, so $2|v_0$ and thus $2|\gcd(u_0, v_0)$, so no solutions of the required form exist. Similarly, if $u_0^2 - 8v_0^2 = -2^m$ for some $m \geq 4$ we also find that $2|\gcd(u_0, v_0)$. If $l = 2$, writing $u_0 = 2k$ we have that

$$k^2 - 2v_0^2 = 1.$$

Thus $2v_0^2 = (k-1)(k+1)$, so $2|k+1$ or $2|k-1$. Thus k is odd, so $k-1$ and $k+1$ are both even. Hence $2|v_0^2$, so $2|v_0$ again. Thus the equations $u^2 - 8v^2 = 2^l$ and $u^2 - 8v^2 = -2^m$ have no solutions (u_0, v_0) with $\gcd(u_0, v_0) = 1$. For the remaining three equations, reducing mod 4 tells us that u_0^2 is congruent to either 2 or 3 mod 4, which is impossible. Thus these three equations have no integer solutions at all. ■

Next, we show that, for the remaining equations, requiring that $\gcd(u_0, v_0) = 1$ is an extraneous condition.

Lemma 4.19 *All integer solutions* (u_0, v_0) *to the equations* $u^2 - 8v^2 = k$ *for* $k \in \{-8, -4, 1, 8\}$ *have gcd*$(u_0, v_0) = 1$.

Proof Notice that $\gcd(u_0, v_0)^2|k$, so $\gcd(u_0, v_0)$ is either 1 or 2. If $\gcd(u_0, v_0) = 2$, then setting $u_0 = 2m$ and $v_0 = 2l$ we find that $m^2 - 8l^2 = k/4$. If $k = 1$ then $k/4$ isn't an integer. For $k = -4$ we have $k/4 \equiv 3 \bmod 4$ and for $k = \pm 8$ we have $k/4 \equiv 2 \bmod 4$. But $m^2 - 8l^2 \equiv 0$ or $1 \bmod 4$, so no k allows the equality to hold mod 4. So we can't have $\gcd(u_0, v_0) = 2$, and thus $\gcd(u_0, v_0) = 1$. ■

Combining what we have shown in the previous two lemmas with step 5 from the Poulakis and Voskos algorithm, we see that the t-coordinates of integral points of C_P have the form

$$t_0 = 16\frac{4u_0v_0^3 + 12v_0^4}{(u_0^2 - 8v_0^2)^2} = 64\frac{u_0v_0^3 + 3v_0^4}{(u_0^2 - 8v_0^2)^2}$$

where (u_0, v_0) is an integral solution of any of the equations $u^2 - 8v^2 = k$ where $k \in \{-8, -4, 1, 8\}$ and $u_0 \geq 0$. Before going any further, we use this formula for t_0 to extract a simple subset of $\mathbb{N}$ of density 1/4 for which the specialization map is injective.

Theorem 4.20 *Let $t_0 \in \mathbb{N}$ with $t_0 > 1$ and suppose $t_0 \equiv 1 \bmod 4$. Then the specialization map for E at t_0 is injective.*

Proof Suppose that (t_0, x_0) is an integral point on C_P so that we have

$$t_0 = 64\frac{u_0 v_0^3 + 3v_0^4}{(u_0^2 - 8v_0^2)^2}$$

where u_0, v_0 satisfies $u_0^2 - 8v_0^2 = m$ for some $m \in \{-8, -4, 1, 8\}$. Note that if $m = 1$ or $m = -4$, then t_0 is even. If t_0 is odd, we must have $m = \pm 8$, so that $t_0 = u_0 v_0^3 + 3v_0^4$ for some u_0, v_0 satisfying $u_0^2 - 8v_0^2 = \pm 8$. Hence $8|u_0^2$, so that $4|u_0$, and since we require that $\gcd(u_0, v_0) = 1$ we have that v_0 is odd. Thus

$$t_0 \equiv u_0 v_0^3 + 3v_0^4 \equiv 3 \bmod 4.$$

Now assume that we have $t_0 \in \mathbb{N}$ with $t_0 > 1$ and $t_0 \equiv 1 \bmod 4$. Then we've just shown that (t_0, x_0) is not an integral point on C_P for any $x_0 \in \mathbb{Z}$, so by Corollary 4.17 the specialization map at t_0 is injective. ■

Using some elementary algebraic number theory, we now solve the remaining four equations.

1. $u^2 - 8v^2 = 1$: The integer solutions to this equation correspond to units of $\mathbb{Z}[\sqrt{2}]$ of the form $a + 2b\sqrt{2}$ with $a, b \in \mathbb{Z}$. Recall that

   $$\mathbb{Z}[\sqrt{2}]^\times = \{\pm(1+\sqrt{2})^n \mid n \in \mathbb{Z}\}.$$

   If we write $(1+\sqrt{2})^n = c + d\sqrt{2}$, note that $2|d$ if and only if $2|n$. Hence the integer solutions of $u^2 - 8v^2 = 1$ correspond to $\pm(1+\sqrt{2})^{2m}$ for $m \in \mathbb{Z}$. The solutions with $u \geq 0$ correspond to choosing $+$.

2. $u^2 - 8v^2 = -4$: Suppose (u_0, v_0) is an integral solution. Noting that u_0 is even, set

$$x = \frac{u_0 + 4v_0}{2}, \qquad y = \frac{u_0 + 2v_0}{2}.$$

Then x, y are integers such that

$$x^2 - 2y^2 = 1;$$

that is, $x + y\sqrt{2}$ has $\mathbb{Z}[\sqrt{2}]$-norm 1. Note that every unit of $\mathbb{Z}[\sqrt{2}]$ that is an even power of $1 + \sqrt{2}$ must have norm 1 because it's either a square or minus a square (and -1 has norm 1). Additionally, every unit of $\mathbb{Z}[\sqrt{2}]$ that is an odd power of $1 + \sqrt{2}$ must have norm -1 because it's $1 + \sqrt{2}$ times (plus or minus) a square, and $1 + \sqrt{2}$ has norm -1. Hence

$$x + y\sqrt{2} = \pm(1 + \sqrt{2})^{2n}$$

for some $n \in \mathbb{Z}$.

Thus

$$u_0 + 4v_0 + (u_0 + 2v_0)\sqrt{2} = \pm 2(1 + \sqrt{2})^{2n}.$$

Multiplying both sides by $-(1 - \sqrt{2})$ gives

$$u_0 + 2v_0\sqrt{2} = \pm 2(1 + \sqrt{2})^{2n-1}.$$

Thus the solution set of $u^2 - 8v^2 = -4$ corresponds to the set

$$\{\pm 2(1 + \sqrt{2})^{2n+1} \mid n \in \mathbb{Z}\} \subset \mathbb{Z}[\sqrt{2}].$$

As before, the solutions with $u \geq 0$ correspond to choosing $+$.

3. $u^2 - 8v^2 = 8$: If (u_0, v_0) is an integral solution, notice that $4|u_0$. Writing $u_0 = 4m$, we see that

$$v_0^2 - 2m^2 = -1.$$

Hence

$$v_0 + \frac{u_0}{4}\sqrt{2} = \pm(1 + \sqrt{2})^{2n+1}.$$

Multiplying both sides by $2\sqrt{2}$, we have

$$u_0 + 2v_0\sqrt{2} = \pm 2\sqrt{2}(1+\sqrt{2})^{2n+1}.$$

So the solution set of $u^2 - 8v^2 = 8$ corresponds to the set

$$\{\pm 2\sqrt{2}(1+\sqrt{2})^{2n+1} \mid n \in \mathbb{Z}\} \subset \mathbb{Z}[\sqrt{2}].$$

The solutions with $u \geq 0$ correspond to choosing $+$.

4. $u^2 - 8v^2 = -8$: As with the $k = 8$ case, writing $u_0 = 4m$ we have

$$v_0^2 - 2m^2 = 1.$$

Using a similar argument, we find that the solution set of $u^2 - 8v^2 = -8$ corresponds to the set

$$\{\pm 2\sqrt{2}(1+\sqrt{2})^{2n} \mid n \in \mathbb{Z}\} \subset \mathbb{Z}[\sqrt{2}].$$

For $n \geq 0$ the solutions with $u \geq 0$ correspond to choosing $+$, and for $n < 0$ the solutions with $u \geq 0$ correspond to choosing $-$; notice that the choice is $\operatorname{sgn}(n)$.

We summarize the above discussion with the following formula that gives the t-coordinates of integral points on C_P.

Proposition 4.21 *If t_0 is the t-coordinate of an integral point on C_P, then t_0 is given by one of the following four formulas.*

1. $t_0 = 64(u_{1,n}v_{1,n}^3 + 3v_{1,n}^4)$ *where*

$$u_{1,n} = \frac{(1+\sqrt{2})^{2n} + (1-\sqrt{2})^{2n}}{2},$$
$$v_{1,n} = \frac{(1+\sqrt{2})^{2n} - (1-\sqrt{2})^{2n}}{4\sqrt{2}}$$

for some $n \in \mathbb{Z}$.

2. $t_0 = 4(u_{2,n}v_{2,n}^3 + 3v_{2,n}^4)$ *where*

$$\begin{aligned} u_{2,n} &= (1+\sqrt{2})^{2n+1} + (1-\sqrt{2})^{2n+1}, \\ v_{2,n} &= \frac{(1+\sqrt{2})^{2n+1} - (1-\sqrt{2})^{2n+1}}{2\sqrt{2}} \end{aligned}$$

for some $n \in \mathbb{Z}$.

3. $t_0 = u_{3,n}v_{3,n}^3 + 3v_{3,n}^4$ *where*

$$\begin{aligned} u_{3,n} &= \sqrt{2}\left((1+\sqrt{2})^{2n+1} - (1-\sqrt{2})^{2n+1}\right), \\ v_{3,n} &= \frac{(1+\sqrt{2})^{2n+1} + (1-\sqrt{2})^{2n+1}}{2} \end{aligned}$$

for some $n \in \mathbb{Z}$.

4. $t_0 = u_{4,n}v_{4,n}^3 + 3v_{4,n}^4$ *where*

$$\begin{aligned} u_{4,n} &= \sqrt{2}\left((1+\sqrt{2})^{2n} - (1-\sqrt{2})^{2n}\right), \\ v_{4,n} &= \frac{(1+\sqrt{2})^{2n} + (1-\sqrt{2})^{2n}}{2} \end{aligned}$$

for some $n \in \mathbb{Z}$.

Proof Let $k = 1$, so that for a solution (u_0, v_0) of $u^2 - 8v^2 = 1$ we have that $t_0 = 64(u_0v_0^3 + 3v_0^4)$. Let $(1+\sqrt{2})^{2n} = u_0 + 2v_0\sqrt{2}$, so that $(1-\sqrt{2})^{2n} = u_0 - 2v_0\sqrt{2}$. Adding and subtracting the equations gives

$$\begin{aligned} 2u_0 &= (1+\sqrt{2})^{2n} + (1-\sqrt{2})^{2n} \\ 4v_0\sqrt{2} &= (1+\sqrt{2})^{2n} - (1-\sqrt{2})^{2n}. \end{aligned}$$

Solving for the left hand sides gives the first formula, and the other 3 formulas are obtained in the exact same way. Finally, note that for formula 4, we do not need to include a $\operatorname{sgn}(n)$ factor as discussed when solving the corresponding equation above since it cancels out in the expression for t_0. ■

The first few integers appearing in the above list are $-1, 0, 3, 4, 7, 20, 27$; 0 is the only integer which occurs twice, corresponding to $n = -1, 0$ in the first formula. From this point forward, there are distinct groups of integers that appear, reflecting the four cases above.

343	13824	482447	16464000	559728679
384	14063	483840	16472119	559776000
459	14500	486387	16486964	559862523
500	14739	487780	16495083	559909844

For example,

$$\begin{aligned} 384 &= 64(u_{1,1}v_{1,1}^3 + 3v_{1,1}^4), & 500 &= 4(u_{2,-2}v_{2,-2}^3 + 3v_{2,-2}^4), \\ 343 &= u_{3,-2}v_{3,-2}^3 + 3v_{3,-2}^4, & 459 &= u_{4,1}v_{4,1}^3 + 3v_{4,1}^4. \end{aligned}$$

Notice that the distance between the groups is increasing, reaffirming that the complement of the set should have density one. To summarize, we have shown the following.

Theorem 4.22 *Let T be the set of integers $t_0 > 2$ which fail to satisfy the conditions of Proposition 4.21. Then $T \subset \mathbb{N}$ is a subset of density 1 and for each $t_0 \in T$ the specialization map σ_{t_0} is injective.*

Proof Let H be the Hilbert subset of $\mathbb{Q}$ corresponding to $d_{2,P}$. Proposition 4.21 shows that $H \cap \mathbb{N} \subset T$. Now use Proposition 4.3 and Corollary 4.17. ∎

Corollary 4.23 *Let T be as in Theorem 4.22. For each $t_0 \in T$, the Mordell-Weil group of the elliptic curve*

$$E_{t_0} : y^2 = x^3 - t_0^2 x + t_0^2$$

has a torsion-free subgroup of rank 2 generated by (t_0, t_0) and $(0, t_0)$. In particular,

$$\mathit{rank}(E_{t_0}(\mathbb{Q})) \geq 2.$$

4.3.2 $y^2 = x^3 - (t^2 + 27)x + 10t^2 + 48t + 90$

Set $E : y^2 = x^3 - (t^2 + 27)x + 10t^2 + 48t + 90$. This second example we consider comes from Shioda's list of rational elliptic surfaces with specified Mordell-Weil rank [14]. As indicated there, $E(\mathbb{Q}(t))$ has rank 4 with generators

$$(t+3, 4t+6), \qquad (9, t+24), \qquad (1, 3t+8), \qquad (6, 2t+12).$$

Instead of considering specialization of the entire Mordell-Weil group, we will focus on the subgroup M generated by the two points $P = (t+3, 4t+6)$ and $Q = (9, t+24)$ in order to show the utility of Algorithm 4.9 for proper subgroups.

As in the previous example, we obtain the four relevant polynomials.

$$\begin{aligned} d_{2,P}(t,x) &= x^4 - 4x^3t + 2x^2t^2 + 4xt^3 + t^4 - 12x^3 - 68xt^2 - 40t^3 \\ &\quad + 54x^2 - 276xt - 258t^2 - 396x - 936t - 351 \\ d_{2,Q}(t,x) &= x^4 + 2x^2t^2 + t^4 - 36x^3 - 44xt^2 + 54x^2 - 384xt - 306t^2 \\ &\quad + 252x - 1728t - 2511 \\ d_{2,P+Q}(t,x) &= x^4 + 4x^3t + 2x^2t^2 - 4xt^3 + t^4 + 12x^3 - 92xt^2 + 40t^3 \\ &\quad + 54x^2 - 492xt + 366t^2 - 1044x + 936t + 1809 \\ g(t,x) &= x^3 - (t^2 + 27)x + 10t^2 + 48t + 90 \end{aligned}$$

Notice that the curves C_P, C_Q, C_{P+Q} and C_2 have rational points

$$(t,x) = (9,-6), (9,36), (9,6), \text{ and } (30,15),$$

respectively. Using Sage, the curves also have genus 1, so they are elliptic curves defined over $\mathbb{Q}$ (despite the fact that these curves are defined by quartic polynomials, there is still an embedding of their normalizations into $\mathbb{P}^2$ as a cubic where we move our selected rational point to infinity), and thus the methods used for the previous examples will not work. However, using Magma and Sage, we find that the curves

C_P, C_Q and C_{P+Q} have Mordell-Weil rank zero (over $\mathbb{Q}$) and have the following finite lists of rational points.

$$\begin{aligned} C_P(\mathbb{Q}) &= \{(-11,6),(-12,9),(9,-6),(44,1)\} \\ C_Q(\mathbb{Q}) &= \{(-5,8),(-3,0),(9,36),(-1,-4)\} \\ C_{P+Q}(\mathbb{Q}) &= \{(-19,-6),(-26,1),(9,6),(6,9)\} \end{aligned}$$

Hence we obtain the following.

Theorem 4.24 *Let $t_0 \in \mathbb{Q}$ be a rational number such that*

$$t_0 \notin \{-26,-19,-12,-11,-5,-3,-1,6,9,44\}$$

and the polynomial $g(t_0,x) = x^3 - (t_0^2+27)x + 10t_0^2 + 48t_0 + 90$ has no rational roots. Then the specialization map $\sigma_{t_0}|_M$ is injective.

5. SPECIALIZATION AND 2-DESCENT

In this chapter, we utilize 2-descent to discuss another effective approach to specialization. The most notable aspect of this method, especially when contrasted with the method of Chapter 4, is the fact that one does not need to know generators of the Mordell-Weil group of an elliptic surface in order to use this criterion. In fact, the method can be used to prove that a given set of sections generates the Mordell-Weil group; see Gusić-Tadić [2] or Stoll [19] for examples.

We begin with a review of the Weak Mordell-Weil Theorem, the crucial first step in proving the Mordell-Weil Theorem (Theorem 3.9). The proof of the theorem highlights the issues facing 2-descent over non-algebraically closed ground fields. The original realization that 2-descent can be useful for specialization is due to Gusić and Tadić [2]; later, Stoll [19] formalized the results of Gusić and Tadić in terms of group cohomology. Using this language, we prove Gusić and Tadić's specialization result for elliptic curves with full $k(t)$-rational 2-torsion in section 2. We then prove Gusić's specialization result for elliptic curves with exactly one $k(t)$-rational 2-torsion point in section 3. Finally, we offer a way to apply Gusić and Tadić's criteria to certain specializations of an elliptic curve without $k(t)$-rational 2-torsion, as long as ψ_2^2 (using notation from §2.4) defines a rational curve.

In order to remain consistent with standard notation, in this chapter S will denote a set of places of a field (or, equivalently when the field is the function field of a curve, (closed) points on the curve) rather than a subset of a field where specialization is injective.

5.1 The Weak Mordell-Weil Theorem

The first step in proving the Mordell-Weil Theorem for Function Fields is to prove the Weak Mordell-Weil Theorem for Function Fields, as stated below.

Theorem 5.1 (Weak Mordell-Weil Theorem for Function Fields) *Let k be an algebraically closed field, C/k a smooth projective curve with function field $K = k(C)$ and E/K an elliptic curve. Then the group $E(K)/2E(K)$ is finite.*

Once one has justified Theorem 3.9, one knows that the statement of Theorem 5.1 remains true with k replaced by any field (when E is nonsplit). However, the proof below critically uses that k is algebraically closed, as we will see shortly. Fix a Weierstrass equation $y^2 = p(x)$ for E/K. By replacing C with the smooth projective curve corresponding to the splitting field of $p(x)$, we may assume that

$$p(x) = (x - e_1)(x - e_2)(x - e_3)$$

with $e_i \in K$ (see [17, Chapter VIII Lemma 1.1.1]). Taking $\mathrm{Gal}(\bar{K}/K)$-cohomology of the exact sequence

$$0 \longrightarrow E[2](\bar{K}) \longrightarrow E(\bar{K}) \xrightarrow{[2]} E(\bar{K}) \longrightarrow 0$$

yields the usual connecting homomorphism

$$c : E(K) \to H^1(\mathrm{Gal}(\bar{K}/K), E[2](\bar{K}))$$

with kernel $2E(K)$. Fixing a $\mathbb{Z}/2\mathbb{Z}$-basis $\{(e_1, 0), (e_2, 0)\}$ of $E[2](K)$, we obtain an isomorphism

$$H^1(\mathrm{Gal}(\bar{K}/K), E[2](\bar{K})) \cong K^*/(K^*)^2 \times K^*/(K^*)^2.$$

Composing c with this isomorphism and factoring out the kernel yields the injective homomorphism

$$\delta : E(K)/2E(K) \to K^*/(K^*)^2 \times K^*/(K^*)^2$$

where

$$\delta(P) = \begin{cases} (x(P) - e_1, x(P) - e_2) & \text{if } x(P) \neq e_1, e_2, \\ ((e_1 - e_3)(e_1 - e_2), e_1 - e_2) & \text{if } x(P) = e_1, \\ (e_2 - e_1, (e_2 - e_3)(e_2 - e_1)) & \text{if } x(P) = e_2, \\ (1, 1) & \text{if } P = O. \end{cases}$$

Let S be the set of points of $C(k)$ such that for each t_0 in S we have that either e_1, e_2 or e_3 has a pole or the discriminant of E vanishes. Then

$$\operatorname{im} \delta \subset K(S, 2) \times K(S, 2)$$

where $K(S, 2) = \{f \in K^*/(K^*)^2 \mid \operatorname{ord}_{t_0}(f) \equiv 0 \bmod 2 \text{ for every } t_0 \notin S\}$. Assuming that k is algebraically closed, one can show that $K(S, 2)$ is finite by showing that it is an extension of a finite group by a subgroup of $\operatorname{Pic}(C)[2]$ (which is also finite), completing the proof. For more details about these arguments, see [16, Chapter 3 §2].

Notice that it is certainly not always true that $K(S, 2)$ is finite when k fails to be algebraically closed. For instance, take $k = \mathbb{Q}$, $C = \mathbb{P}^1$ and $S = \emptyset$. Then

$$K(S, 2) = \{f \in \mathbb{Q}(t)^*/(\mathbb{Q}(t)^*)^2 \mid \operatorname{ord}_v(f) \equiv 0 \bmod 2 \text{ for every place } v \text{ of } \mathbb{Q}(t)\}.$$

Now $K(S, 2)$ contains the set of squarefree integers, so $K(S, 2)$ isn't even finitely generated.

5.2 The Gusić-Tadić Criterion for Full 2-Torsion

We now move back to considering specialization. Let k be a number field, C/k a smooth projective curve with function field $K = k(C)$ and E/K an elliptic curve. In this section, it is critical to (and we do) assume that

$$E[2](\bar{K}) \subset E(K).$$

Let $t_0 \in C(k)$, and let $\mathcal{O}_{t_0} \subset K$ denote the subring of functions f with $\mathrm{ord}_{t_0}(f) \geq 0$. Evaluation at t_0 induces a ring map

$$\begin{aligned} s_{t_0} : \mathcal{O}_{t_0} &\to k \\ f &\mapsto f(t_0). \end{aligned}$$

This map is precisely what the specialization map σ_{t_0} does to the coordinates of points in $E(K)$ once we've fixed a Weierstrass equation (even when a coordinate has a pole at t_0, this remains true after appropriate scaling if we view the points in $\mathbb{P}^2$). Using this map, we can view specialization of $E(K)/2E(K)$ as specialization of $\mathrm{im}(\delta)$ (as defined in the previous section). Thus, as implied by Stoll's conceptual proof [19] of the results of Gusić and Tadić [2] (for $C = \mathbb{P}^1$ and $k = \mathbb{Q}$) and motivated by the proof of the Weak Mordell-Weil Theorem, we have a different procedure for determining injectivity of a specialization map.

Algorithm 5.2 *Let δ be the 2-descent map as defined above, and let $t_0 \in C(k)$ be a k-rational point of C such that the specialization E_{t_0} is an elliptic curve.*

1. *Find a finitely generated group $G \subset \mathcal{O}_{t_0}^*/(\mathcal{O}_{t_0}^*)^2 \times \mathcal{O}_{t_0}^*/(\mathcal{O}_{t_0}^*)^2$ containing $\mathrm{im}(\delta)$.*
2. *For each of the (finitely many) nonzero $(f, g) \in G$, evaluate f and g at t_0 and determine whether or not $f(t_0)$ and $g(t_0)$ are squares in k.*
3. *If each tuple from step 2 has an entry which is not a square in k, the specialization map σ_{t_0} is injective.*

Proof First, since G is finitely generated from Step 1 and $2G = 0$, we know that G is actually finite, making Step 2 make sense. It remains to verify that Step 3 follows from Steps 1 and 2. To do this, we will show that the conditions of Proposition 4.4 hold for $n = 2$, $\phi = \sigma_{t_0}$, $M = E(K)$ and $N = E_{t_0}(k)$. We have a commutative diagram

$$\begin{tikzcd} E(K)/2E(K) \arrow[r, "\delta"] \arrow[d, "\overline{\sigma_{t_0}}"] & G \arrow[d, "\overline{s_{t_0}} \times \overline{s_{t_0}}"] \\ E_{t_0}(k)/2E_{t_0}(k) \arrow[r, "\delta_{t_0}"] & k^*/(k^*)^2 \times k^*/(k^*)^2. \end{tikzcd}$$

Recall that the vertical maps evaluate functions at t_0 (so that the evaluation in Step 2 is the same as plugging tuples into $\overline{s_{t_0}} \times \overline{s_{t_0}}$) and the horizontal maps are the 2-descent maps defined above. Thus the check in Step 3 shows that no tuple from Step 2 is in the kernel of $\overline{s_{t_0}} \times \overline{s_{t_0}}$. Hence $\overline{s_{t_0}} \times \overline{s_{t_0}}$ is injective. Since δ is always injective, following the diagram we see that $\overline{\sigma_{t_0}}$ is also injective. Thus condition 2 of Proposition 4.4 is satisfied. Since $E(K)$ has full 2-torsion and σ_{t_0} is injective on torsion, $E_{t_0}(k)$ also has full 2-torsion. Thus condition 3 is also satisfied. Hence σ_{t_0} is injective (recall that the other two conditions of Proposition 4.4 are always satisfied under our assumptions).
■

Remark 5.3 *Note that we cannot use* $G = K(S, 2) \times K(S, 2)$ *for any set of places* S*, because* $K(S, 2)$ *fails to be finitely generated. Additionally, if one tries to resolve this by replacing* k *with* $\bar{k}$*, notice that this results in* s_{t_0} *becoming the zero map.*

Remark 5.4 *If one already knows* $E(K)/2E(K)$*, such as in the situation of Algorithm 4.9 (or more generally, as indicated in Remark 4.12), this approach gives an alternative way to check that* $\overline{\sigma_{t_0}}$ *is injective. Indeed, in this case we simply take* $G = im\ \delta$*.*

Of course, the difficulty in applying Algorithm 5.2 is finding the “bounding group” G. In 2015, Gusić and Tadić [2] found an effectively computable bounding group G, independent of any points in $E(K)$, in the case of $C = \mathbb{P}^1$. Before stating and proving their result from this perspective, we recall a fact from algebraic number theory.

Lemma 5.5 *Let* k *be a number field. There exists a unique factorization domain* R *containing the ring of integers* $\mathcal{O}_k$ *with a finitely generated unit group.*

Proof Dirichlet’s Unit Theorem guarantees that $\mathcal{O}_k$ has a finitely generated unit group, so take $R = \mathcal{O}_k$ if k has class number 1. Otherwise, let $\mathfrak{a}_1, ..., \mathfrak{a}_k$ be a set of generators for $\mathrm{Cl}(\mathcal{O}_k)$, and let R be the ring of S-integers of k where S contains the prime factors of all $\mathfrak{a}_i$’s. Then R has trivial class group, and Dirichlet’s S-unit theorem says R^* is finitely generated. ■

Theorem 5.6 *[2] Let k be a number field and let R be as in the lemma. Let $E/k(t)$ be an elliptic curve given by a Weierstrass equation*

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3)$$

with $e_i \in R[t]$ for each i. Let G be the subgroup of $k(t)^*/(k(t)^*)^2 \times k(t)^*/(k(t)^*)^2$ generated by tuples with coordinates coming from the irreducible factors of

$$e_1 - e_2, \qquad e_2 - e_3, \qquad e_1 - e_3 \tag{5.1}$$

in (the UFD) $R[t]$ and the units of R. Then G is finitely generated and the connecting homomorphism δ has $im(\delta) \subset G$.

Proof Since our tuples include units of R, any choice of irreducible factors of $e_i - e_j$ works. Additionally, since R^* is finitely generated, there are only finitely many units of R^* modulo squares. Hence G is finitely generated. It remains to show that $\mathrm{im}(\delta) \subset G$. From the definition of δ given in Section 5.1, it suffices to show that, for any nonidentity $P \in E(k(t))$, if f is a prime of $R[t]$ with

$$\mathrm{ord}_f(x(P) - e_i) \equiv 1 \bmod 2$$

for $i = 1, 2$, then f divides some polynomial in (5.1). Suppose there is some f for which $\mathrm{ord}_f(x(P) - e_i)$ is odd. WLOG assume $i = 1$. Recall that

$$y(P)^2 = (x(P) - e_1)(x(P) - e_2)(x(P) - e_3).$$

By setting $X = x(P) - e_1$ and $Y = y(P)$, we have

$$Y^2 = X(X - (e_2 - e_1))(X - (e_3 - e_1)) = X(X^2 - (2e_1 - e_2 - e_3)X + (e_2 - e_1)(e_3 - e_1)).$$

Now $\mathrm{ord}_f(X)$ is odd, so $\mathrm{ord}_f(X^2 - (2e_1 - e_2 - e_3)X + (e_1 - e_2)(e_1 - e_3))$ is odd (otherwise Y^2 cannot be a square). Thus $\mathrm{ord}_f((e_1 - e_2)(e_1 - e_3))$ is nonzero, hence positive since $(e_1 - e_2)(e_1 - e_3) \in R[t]$. Since f is prime, we have that f divides $e_1 - e_2$ or $e_1 - e_3$. ■

Remark 5.7 *Note that the finite generation of R^* is critical in establishing that G is finitely generated. In particular, one cannot replace R by k and have a similar result. Even if one were willing to accept that G would not be finitely generated in this case, notice that for any t_0 such that $G \subset \mathcal{O}_{t_0}^*/(\mathcal{O}_{t_0}^*)^2 \times \mathcal{O}_{t_0}^*/(\mathcal{O}_{t_0}^*)^2$, Step 3 of Algorithm 5.2 is never satisfied. Indeed, say f is a prime factor of $e_i - e_j$. Recall that $f \in \mathcal{O}_{t_0}^*$ means that $f(t_0) \neq 0$, so that $f(t_0) \in k^*$. Then the tuple $(f(t_0)f, 1) \in G$ specializes to $(f(t_0)^2, 1)$.*

5.3 The Gusić Criterion for a Single 2-Torsion Point

In this section, we recast the criterion of Gusić [2] in terms of bounding groups. We first briefly review the basics of descent by 2-isogeny; for the full details, see [17, Chapter 10 §4] (and note that the relevant facts do not require E to be defined over a number field). Let k be a number field, C/k a smooth projective curve with function field $K = k(C)$ and E/K an elliptic curve. While one can do descent by 2-isogeny when $E(K)$ has full 2-torsion, the results we establish later will require exactly one nontrivial 2-torsion point. Hence, in this section, it is critical to (and we do) assume that

$$E(K) \text{ has exactly one nontrivial 2-torsion point.}$$

Any elliptic curve satisfying these assumptions has a Weierstrass equation of the form

$$y^2 = x^3 + ax^2 + bx$$

with 2-torsion point (0,0) and $a^2 - 4b$ not a square in K. We have a 2-isogeny ϕ with kernel $\{O, (0,0)\}$ defined by the formula

$$\begin{aligned} &\phi : E \to E', \\ &(x, y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2}\right), \end{aligned}$$

where the dual curve E' is defined by

$$E' : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X$$

with dual isogeny

$$\begin{aligned}&\hat{\phi} : E' \to E,\\ &(X, Y) \mapsto \left(\frac{Y^2}{4X^2}, \frac{Y(a^2 - 4b - X^2)}{8X^2}\right)\end{aligned}$$

that has kernel $\{O', (0, 0)\}$. We have an exact sequence

$$0 \longrightarrow E[\phi](\bar{K}) \longrightarrow E(\bar{K}) \xrightarrow{\phi} E'(\bar{K}) \longrightarrow 0,$$

and taking $\mathrm{Gal}(\bar{K}/K)$-cohomology yields the connecting homomorphism

$$c_\phi : E'(K) \to H^1(\mathrm{Gal}(\bar{K}/K), E[\phi](\bar{K})).$$

Here,

$$H^1(\mathrm{Gal}(\bar{K}/K), E[\phi](\bar{K})) \cong K^*/(K^*)^2,$$

so factoring out the kernel $E[\phi](K)$ and composing with this isomorphism gives a map

$$\delta_\phi : E'(K)/\phi(E(K)) \to K^*/(K^*)^2$$

such that

$$\delta_\phi(P) = \begin{cases} X(P) & \text{if } P \neq O', (0, 0),\\ a^2 - 4b & \text{if } P = (0, 0),\\ 1 & \text{if } P = O'. \end{cases}$$

We similarly obtain

$$\delta_{\hat{\phi}} : E(K)/\hat{\phi}(E'(K)) \to K^*/(K^*)^2$$

where

$$\delta_{\hat{\phi}}(P) = \begin{cases} x(P) & \text{if } P \neq O, (0, 0),\\ b & \text{if } P = (0, 0),\\ 1 & \text{if } P = O. \end{cases}$$

We have a specialization algorithm similar to Algorithm 5.2 in this case. The main ideas for the proof can be found in [2].

Algorithm 5.8 *Let δ_ϕ and $\delta_{\hat{\phi}}$ be the descent maps as defined above, and let $t_0 \in C(k)$ be a k-rational point of C such that the specialization E_{t_0} is an elliptic curve and $a, b \in \mathcal{O}_{t_0}$.*

1. *Find finitely generated groups $G_\phi, G_{\hat{\phi}} \subset \mathcal{O}_{t_0}^*/(\mathcal{O}_{t_0}^*)^2$ containing $im(\delta_\phi)$ and $im(\delta_{\hat{\phi}})$, respectively.*
2. *For each of the (finitely many) nonzero $f \in G_\phi$ and $g \in G_{\hat{\phi}}$, evaluate f and g at t_0 and determine whether or not $f(t_0)$ and $g(t_0)$ are squares in k.*
3. *If no values in step 2 are squares, the specialization map σ_{t_0} is injective.*

Proof As with the proof of Algorithm 5.2, we verify the conditions of Proposition 4.4 for $n = 2, \phi = \sigma_{t_0}$, $M = E(K)$ and $N = E_{t_0}(k)$ (of which conditions 1 and 4 are clearly satisfied). For condition 3, since $a^2 - 4b \in \operatorname{im}(\delta_\phi)\backslash\{1\}$ (recall our assumptions at the start of this section), we know that $a(t_0)^2 - 4b(t_0)$ is not a square in k. The specialized curve E_{t_0} has the 2-torsion point (0,0) and has additional k-rational 2-torsion points if and only if $x^2 + a(t_0)x + b(t_0)$ has roots in k; that is, if its discriminant $a^2 - 4b$ is a square in k. Hence E_{t_0} does not gain additional k-rational 2-torsion, so condition 3 holds. To see that condition 2 holds, let $P \in E(K)$ and suppose that P_{t_0} is divisible by 2 in $E_{t_0}(k)$, say

$$P_{t_0} = 2p = (\hat{\phi}_{t_0} \circ \phi_{t_0})(p)$$

where $p \in E_{t_0}(k)$. Then $P_{t_0} \in \operatorname{im}(\hat{\phi}_{t_0})$. Using the commutative diagram

$$\begin{tikzcd}
E(K)/\hat{\phi}(E'(K)) \arrow[r, "\delta_{\hat{\phi}}"] \arrow[d, "\overline{\sigma_{t_0}}"] & G_{\hat{\phi}} \arrow[d, "\overline{s_{t_0}}"] \\
E_{t_0}(k)/\hat{\phi}_{t_0}(E'_{t_0}(k)) \arrow[r, "\delta_{\hat{\phi}_{t_0}}"] & k^*/(k^*)^2,
\end{tikzcd}$$

we see that that going down then right takes P to zero. Hence going right then down also maps to zero. From Step 3, we have that $\overline{s_{t_0}}$ is injective on $G_{\hat{\phi}}$. Since $\delta_{\hat{\phi}}$

is also (always) injective, we must have that $P \in \hat{\phi}(E'(K))$. Say $P = \hat{\phi}(Q)$ where $Q \in E'(K)$. Then

$$\hat{\phi}_{t_0}(Q_{t_0}) = P_{t_0} = \hat{\phi}_{t_0}(\phi_{t_0}(p)),$$

so that $\hat{\phi}(Q_{t_0} - \phi_{t_0}(p)) = O$. So by possibly replacing Q by $Q + (0,0)$ (which still will map to P), we may assume that $Q_{t_0} = \phi_{t_0}(p)$. Repeating the same argument as above using Q instead of P and the appropriate duals, we find a point $R \in E(K)$ with $\phi(R) = Q$. Then $P = \hat{\phi}(Q) = \hat{\phi}(\phi(R)) = [2]R$, so P is divisible by 2 in $E(K)$. This means that P is zero in $E(K)/2E(K)$, so this shows that $\overline{\sigma_{t_0}}$ is injective. Hence condition 2 holds. ■

Remark 5.9 *Based on the definition of the map δ_ϕ, notice that we will not be able to show that a specialization map is injective using this algorithm if $a^2 - 4b$ is a square. Hence our assumption that $E(K)$ has exactly one nontrivial K-rational 2-torsion point is required. However, if $a^2 - 4b$ is a square then $E(K)$ has full 2-torsion, putting us back in the case of Algorithm 5.2.*

Theorem 5.10 *[2] Let k be a number field and let R be as in Lemma 5.5. Let $E/k(t)$ be an elliptic curve given by the Weierstrass equation*

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

with $a, b \in R[t]$. Let $G_\phi, G_{\hat{\phi}}$ be the subgroups of $k(t)^*/(k(t)^*)^2$ generated by the irreducible factors of

$$b \text{ and } a^2 - 4b$$

in $R[t]$, respectively, and the units of R. Then $G_\phi, G_{\hat{\phi}}$ are finitely generated with $im(\delta_\phi) \subset G_\phi$ and $im(\delta_{\hat{\phi}}) \subset G_{\hat{\phi}}$.

Proof Exactly as in the proof of 5.6, G_ϕ and $G_{\hat{\phi}}$ are finitely generated. To show the inclusion $\text{im}(\delta_{\hat{\phi}}) \subset G_{\hat{\phi}}$, let $P \in E(K)$. We need to show that, for any prime $f \in R[t]$ with $\text{ord}_f(x(P))$ odd, f must be a factor of $a^2 - 4b$. But our Weierstrass equation is of the same form as the transformed equation in the proof of Theorem 5.6, so the same argument works here. Similarly, using the Weierstrass equation for E' we obtain the corresponding statement for δ and b. ■

Remark 5.11 *In Theorem 5.6, note that the discriminant of E is*

$$16((e_3 - e_1)(e_3 - e_2)(e_2 - e_1))^2.$$

Hence the factors considered there are a subset of those of the discriminant of E.

Additionally, in Theorem 5.10, E has discriminant $-16b^2(a^2 - 4b)$ and the dual curve E' referenced above has discriminant $2^{10}b(a^2-4b)^2$. Hence the factors considered there are a subset of those of either discriminant. In particular, recall that, for an elliptic curve with a 2-torsion point that is not $(0, 0)$, moving the 2-torsion point to $(0, 0)$ does not change the discriminant. Thus we can apply Theorem 5.10 to any elliptic curve with exactly one nontrivial 2-torsion point by considering factors of the discriminant. Further, since we have demonstrated that what matters is the factors of b and $a^2 - 4b$, we may ignore the 16 in front of the discriminant of E; that is, we can take the factors of $\Delta_E/16$ and still obtain a bounding group.

5.4 Rational 2-division Curves

Notice that all methods discussed previously show that a specialization map is injective by ultimately showing that the induced map on $E(K)/2E(K)$ is injective. As Example 4.5 shows, this alone does not imply that specialization is injective. Additionally, Example 4.14 shows that specialization can be injective without this condition holding true. Provided that a polynomial appearing in Algorithm 4.9 defines a rational curve (over $\mathbb{Q}$, or, as in Remark 4.12, a number field k) in $\mathbb{A}^2$, we provide a way to get around this for certain specializations. In particular, if the 2-torsion curve is rational, this approach allows us to apply the criterion of Gusić to certain specializations of elliptic curves without rational 2-torsion points. The following Proposition provides the setup to apply Gusić's criterion in this new way.

Proposition 5.12 *Let k be a number field. Let $E/k(t)$ be an elliptic curve given by the Weierstrass equation*

$$y^2 = x^3 + A(t)x + B(t)$$

such that the 2-torsion curve

$$C_2 : a^3 + A(t)a + B(t) = 0$$

is irreducible and rational over k. Fix an isomorphism of function fields

$$\begin{aligned} k(C_2) &\cong k(\alpha) \\ t &\mapsto u(\alpha) \\ a &\mapsto v(\alpha). \end{aligned}$$

Then the elliptic curve

$$E' : y^2 = x^3 + A(u(\alpha))x + B(u(\alpha))$$

defined over $k(\alpha)$ has the following properties.

1. *$E'(k(\alpha))$ has the nontrivial 2-torsion point $(v(\alpha), 0)$.*
2. *The function field isomorphism gives an embedding $E(k(t)) \subset E'(k(\alpha))$.*
3. *Let $\alpha_0 \in k$ and set $t_0 = u(\alpha_0)$. Let $M < E(k(t))$ be a subgroup. If the specialization map σ'_{α_0} for E' is injective on the image of M via the embedding above, then the specialization map $\sigma_{t_0}|_M$ for E is injective.*

Proof

1. Note that $x^3 + A(t)x + B(t)$ vanishes at $x = a$. By applying the isomorphism of function fields above, we see that $x^3 + A(u(\alpha))x + B(u(\alpha))$ vanishes at $x = v(\alpha)$. However, $v(\alpha) \in k(\alpha)$, so E' has the $k(\alpha)$-rational 2-torsion point $(v(\alpha), 0)$.

2. The map $t \mapsto u(\alpha)$ gives an injection of function fields $k(t) \to k(\alpha)$. Now if $Q = (x_Q(t), y_Q(t)) \in E(k(t)) \setminus \{O\}$, then

$$Q' = (x_Q(u(\alpha)), y_Q(u(\alpha))) \in E'(k(\alpha)),$$

since E' was obtained from E by the same substitution. It's now clear from the injection of function fields that if $Q_1' = Q_2'$ then $Q_1 = Q_2$. Indeed if $f(t) = x_{Q_1}(t) - x_{Q_2}(t)$ evaluates to 0 under the map $t \mapsto u(\alpha)$ then $f(t)$ is identically zero; we can argue similarly for the y-coordinates.

3. From the formulas above and claim 2, we have a commutative diagram

$$\begin{tikzcd}
E(k(t)) \arrow[r] \arrow[d, "\sigma_{t_0}"] & E'(k(\alpha)) \arrow[d, "\sigma_{\alpha_0}"] \\
E_{t_0}(k) \arrow[r, "\sim"] & E'_{\alpha_0}(k)
\end{tikzcd}$$

where the top arrow is an injection and the bottom arrow is the identity map. Hence if $\sigma_{t_0}(Q) = O_{t_0}$, then Q maps to O'_{α_0} going both ways on the diagram. But going right then down is an injection, so $Q = O$.

$\blacksquare$

Remark 5.13 *You can change variables on E' (preserving Weierstrass form) and still preserve the statements above. For the commutative diagram in the proof of statement 3, instead of the bottom arrow being equality it becomes an isomorphism, and the top arrow is also changed by an isomorphism.*

The benefit of Proposition 5.12 is that one always has a 2-torsion point in $E'(\mathbb{Q}(\alpha))$. Thus one can use Theorem 5.10 (or, in the unlikely case that the polynomial defining C_2 is a cyclic cubic over $k(t)$, Theorem 5.6) on E' to make statements about the injectivity of specialization maps for E despite the fact that E has no nontrivial $\mathbb{Q}(t)$-rational 2-torsion points. In particular, in contrast with Algorithm 4.9, generators of $E(\mathbb{Q}(t))$ do not need to be known to do this. We illustrate this with the example

$$E : y^2 = x^3 - t^2x + t^2.$$

Set

$$C_2 : a^3 - t^2a + t^2 = 0.$$

Using Sage, we obtain the isomorphism of function fields

$$\begin{aligned} \mathbb{Q}(C) &\cong \mathbb{Q}(\alpha) \\ t &\mapsto \frac{1}{\alpha - \alpha^3} \\ a &\mapsto \frac{1}{1 - \alpha^2}. \end{aligned}$$

Via this isomorphism, we obtain the new elliptic curve

$$E' : y^2 = x^3 - \frac{1}{(\alpha - \alpha^3)^2} x + \frac{1}{(\alpha - \alpha^3)^2}.$$

Setting $x = (\alpha - \alpha^3)^{-2} X$ and $y = (\alpha - \alpha^3)^{-3} Y$, we obtain

$$E'' : Y^2 = X^3 - (\alpha - \alpha^3)^2 X + (\alpha - \alpha^3)^4$$

with 2-torsion point $(\alpha^4 - \alpha^2, 0)$. This elliptic curve has discriminant

$$-16\alpha^6(\alpha - 1)^6(\alpha + 1)^6(3\alpha^2 - 4)(3\alpha^2 - 1)^2.$$

Applying Theorem 5.10 to E'' now yields the following statement.

Proposition 5.14 *Let E be as above and t_0 be a rational number of the form $t_0 = 1/(\alpha_0 - \alpha_0^3)$ for some rational number α_0. Let Φ be the set of irreducible factors of*

$$-\alpha^6(\alpha - 1)^6(\alpha + 1)^6(3\alpha^2 - 4)(3\alpha^2 - 1)^2$$

in $\mathbb{Z}[\alpha]$. Suppose that, for each product $h(\alpha)$ of some nonempty subset of the elements of Φ, the rational number $h(\alpha_0)$ is not a square. Then the specialization map σ_{t_0} is injective.

Proof Theorem 5.10, Remark 5.11, Proposition 5.12. ■

For example, this can be used to show that specialization at $t_0 = 8/15$ (corresponding to $\alpha_0 = -3/2$) is injective. Indeed, the relevant factors here are

$$3/2 = -\alpha_0, 5/2 = -(\alpha_0 - 1), 1/2 = -(\alpha_0 + 1), 23/4 = 3\alpha_0^2 - 1, 11/4 = 3\alpha_0^2 - 4$$

and no product of these is a square. On the other hand, we cannot use this to decide whether or not specialization at $t_0 = 1/6$ (corresponding to $\alpha_0 = -2$) is injective because one of the factors is $1 = -(\alpha_0 + 1)$.

Next, we generalize Proposition 5.12 to give a method of introducing a $k(\alpha)$-rational 2-division point of any $P \in E(k(t)) \setminus E[2](k(t))$ which has no $k(t)$-rational 2-division points. This is a generalization in the sense that the 2-torsion points are precisely the 2-division points of O.

Proposition 5.15 *Let k be a number field. Let $E/k(t)$ be an elliptic curve given by the Weierstrass equation*

$$y^2 = x^3 + A(t)x + B(t),$$

and fix $P = (x_P(t), y_P(t)) \in E(k(t)) \setminus E[2](k(t))$ such that P is not divisible by 2 in $E(K)$. Let $\phi(t, x)$ be an irreducible factor of $d_{2,P}(t, x)$ such that

$$C_P : \phi(t, a) = 0$$

is rational over k. Fix an isomorphism of function fields

$$\begin{aligned} k(C_P) &\cong k(\alpha) \\ t &\mapsto u(\alpha) \\ a &\mapsto v(\alpha). \end{aligned}$$

Then the elliptic curve

$$E' : y^2 = x^3 + A(u(\alpha))x + B(u(\alpha))$$

defined over $k(\alpha)$ has the following properties.

1. *$P' = (x_P(u(\alpha)), y_P(u(\alpha))) \in E'(k(\alpha))$ is divisible by 2 in $E'(k(\alpha))$.*

2. *The function field isomorphism gives an embedding $E(k(t)) \subset E'(k(\alpha))$.*

3. *Let $\alpha_0 \in k$ and set $t_0 = u(\alpha_0)$. Let $M < E(k(t))$ be a subgroup. If the specialization map σ'_{α_0} for E' is injective on the image of M via the embedding above, then the specialization map $\sigma_{t_0}|_M$ for E is injective.*

Proof 1. Since $\phi(t,x) \in k(t)$ vanishes at $x = a$, we have that $\phi(u(\alpha), x)$ vanishes at $x = v(\alpha)$. Notice that $y_P(u(\alpha)) \neq 0$ since $y_P(t) \neq 0$. Hence P' is not 2-torsion, so by Lemma 2.13 we see that the roots of $\phi(u(\alpha), x)$ in $k(\alpha)$ are x-coordinates of points in $E'(k(\alpha))$ that are 2-division points of P'. Thus P' is divisible by 2 in $k(\alpha)$.

Mutatis mutandis, the proof for statements 2 and 3 follows from that of Proposition 5.12. ■

To illustrate why this can be useful, let's return to the example

$$E : y^2 = x^3 - t^2 x + t^2.$$

We reproduce the result of the calculation in Example 4.14; that is, that the specialization map for $t_0 = 27$ is injective, but this time without using generators of $E_{27}(\mathbb{Q})$. In this example, we cannot use any methods from earlier sections of this chapter due to a lack of 2-torsion. Additionally, because $P = (t,t)$ specializes to $(27, 27) = [2](-9, 81)$ (and thus $\overline{\sigma_{27}}$ is not injective), we can use neither Algorithm 4.9 nor the method just discussed above which combines Theorem 5.10 with Proposition 5.12. We use Proposition 5.15 as follows. We first find an elliptic curve E' and a point $R' \in E(\mathbb{Q}(\alpha))$ such that $2R' = P'$. Then, by essentially replacing P' by R', we examine a subgroup M of $E'(\mathbb{Q}(\alpha))$ which contains a copy of $E(\mathbb{Q}(t))$. We then hope that the inclusion $M \to E'(\mathbb{Q}(\alpha))$ satisfies the conditions of Proposition 4.4. If this is true, we may attempt to show that specialization is injective on M using the method of Example 4.13, thereby showing that σ_{27} is injective. To begin, recall that we have the curve

$$C_P : f_P(t,a) = a^4 + 2t^2a^2 - 8t^2a + t^4 - t(4a^3 - 4t^2a + 4t^2) = 0.$$

View E as an elliptic curve over the function field $\mathbb{Q}(C_P)$ of C_P (which contains $\mathbb{Q}(t)$). Now, after a bit of searching with Sage, $E(\mathbb{Q}(C_P))$ has the point

$$R = \left(a, \frac{a^3 - 3a^2t + at^2 + t^3 - 2t^2}{2t}\right)$$

such that $[2]R = P$. Sage gives the isomorphism of function fields

$$\begin{aligned} \mathbb{Q}(C_P) &\cong \mathbb{Q}(\alpha) \\ t &\mapsto \frac{4\alpha^3(\alpha+2)}{(\alpha^2+2\alpha-1)^2} = u(\alpha) \\ a &\mapsto \frac{4\alpha^2(\alpha+2)}{(\alpha^2+2\alpha-1)^2} = v(\alpha) \end{aligned}$$

from which we obtain the new elliptic curve

$$E' : y^2 = x^3 - \left(\frac{4\alpha^3(\alpha+2)}{(\alpha^2+2\alpha-1)^2}\right)^2 x + \left(\frac{4\alpha^3(\alpha+2)}{(\alpha^2+2\alpha-1)^2}\right)^2.$$

Set $Q = (0, t)$ (and recall that $E(\mathbb{Q}(t))$ is generated by P and Q; see the discussion at the start of §4.3.1.). Through this change of variables, we have

$$\begin{aligned} P' &= \left(\frac{4\alpha^3(\alpha+2)}{(\alpha^2+2\alpha-1)^2}, \frac{4\alpha^3(\alpha+2)}{(\alpha^2+2\alpha-1)^2}\right), \\ Q' &= \left(0, \frac{4\alpha^3(\alpha+2)}{(\alpha^2+2\alpha-1)^2}\right), \\ R' &= \left(\frac{4\alpha^2(\alpha+2)}{(\alpha^2+2\alpha-1)^2}, \frac{4\alpha^3(\alpha+2)(\alpha^2-3)}{(\alpha^2+2\alpha-1)^3}\right). \end{aligned}$$

In particular, in $E'(\mathbb{Q}(\alpha))$ we have $2R' = P'$, and E' is an elliptic curve defined over a rational function field over $\mathbb{Q}$.

We can now use the method of Example 4.13 on the subgroup M of $E'(\mathbb{Q}(\alpha))$ generated by R' and Q'. We omit the details (which are easily verified using Sage) of showing that the inclusion $M \to E'(\mathbb{Q}(\alpha))$ satisfies the conditions of Proposition 4.4. Since $2R' = P'$, M contains a copy of $E(\mathbb{Q}(t))$ by statement 3 of Proposition 5.15. We set $\alpha_0 = -3$, because $u(-3) = 27$. Now, using Sage, we see that the points $R'_{\alpha_0}, Q'_{\alpha_0}$, and $(R' + Q')_{\alpha_0}$ are not divisible by 2 in $E'_{\alpha_0}(\mathbb{Q})$. Additionally, the curve E'_{α_0} has no $\mathbb{Q}$-rational 2-torsion. Hence we conclude that the specialization map σ'_{α_0} is injective, so that the specialization map σ_{27} is injective.

Remark 5.16 *The specialization at $t_0 = 7$ can be shown to be injective using the same method as Example 4.14. Despite this, the method we just outlined (using* *specialization at* $\alpha_0 = -1$*) still fails to show that the map is injective. Indeed, in* $E'_{-1}(\mathbb{Q})$ *we have*

$$[2](1,1) = (R' + Q')_{-1},$$

so that $\overline{\sigma'_{-1}}$ *fails to be injective on* M*.*

REFERENCES

[1] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[2] I. Gusić and P. Tadić. Injectivity of the specialization homomorphism of elliptic curves. *arXiv:1409.7189v2*, 2014.

[3] R. Hartshorne. *Algebraic Geometry.* Springer-Verlag, 1977.

[4] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory.* Springer-Verlag, 2nd edition, 1990.

[5] S. Lang. *Diophantine Geometry.* Springer-Verlag, 2nd edition, 1983.

[6] B. Mazur. Modular curves and the Eisenstein ideal. *Publications Mathématiques de l'I.H.É.S.*, 47(2):33–186, 1977.

[7] L. J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Camb. Phil. Soc.*, 21:179–192, 1922.

[8] P. Parent. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *Journal für die reine und angewandte Mathematik*, 1999(506):85 – 116, 1999.

[9] D. Poulakis and E. Voskos. Solving genus zero diophantine equations with at most two infinite valuations. *J. Symbolic Computation.*, 33:479–491, 2002.

[10] E. L. Rees. Graphical discussion of the roots of a quartic equation. *The American Mathematical Monthly*, 29(2), 1922.

[11] J. P. Serre. *Lectures on the Mordell-Weil Theorem*, volume E 15 of *Aspects of mathematics.* Springer, Wiesbaden, 3rd edition, 1997.

[12] I. Shafarevich. *Basic Algebraic Geometry 1.* Springer-Verlag, 3rd edition, 2013.

[13] T. Shioda. On the Mordell-Weil lattices. *Comment. Math. Univ. St. Pauli*, 39, 1990.

[14] T. Shioda. Construction of elliptic curves with high rank via the invariants of the Weyl groups. *J. Math. Soc. Japan*, 43(4), 1991.

[15] J. H. Silverman. Heights and the specialization map for families of abelian varieties. *J. Reine Angew. Math.*, 342:197–211, 1983.

[16] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* Springer-Verlag, 1994.

[17] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 2nd edition, 2009.

[18] J. H. Silverman (https://mathoverflow.net/users/11926/joe-silverman). Exceptional specializations of Galois groups in the Hilbert irreducibility theorem. MathOverflow. URL:https://mathoverflow.net/q/226379 (version: 2015-12-17).

[19] M. Stoll. Diagonal genus 5 curves, elliptic curves over $\mathbb{Q}(t)$, and rational diophantine quintuples. *Acta Arithmetica*, 190(3):239–261, 2019.

[20] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.9)*, 2019. `https://www.sagemath.org`.

[21] A. Weil. L'arithmétique sur les courbes algébriques. *Acta Mathematica*, 52:281–315, 1929.