

Ranks of Elliptic Curves via the Shioda-Tate Theorem

A thesis submitted by
Fengning (David) Ding

advised by
Noam Elkies

to the Department of Mathematics at Harvard University

on March 21, 2016

in partial fulfillment of the requirements
for the degree of Bachelor of Arts with Honors.

Acknowledgments

I would like to thank my family for their love and encouragement. From an early age, they have encouraged my passion for mathematics and helped me in my academic endeavors. I am grateful for their support, without which this thesis would not have been possible.

I would also like to thank my advisor, Noam Elkies. He has helped me discover an area of mathematics about which I am genuinely interested, and his explanations have helped me clarify both my own lines of inquiry as well as the bigger picture.

As well, I would like to thank the Harvard mathematics department for the wonderful learning environment and courses it has afforded me. In particular, I thank all my professors, especially Joe Harris, who has taught me in two exceptional courses on the representation theory of Lie algebras and intersection theory, which both shaped the direction of this thesis; Junecue Suh (now at U.C. Santa Cruz), for teaching my first math course at Harvard and for stimulating my interest in elliptic curves at freshman faculty dinner; and my advisor Yum-Tong Siu, for offering advice on courses and lending structure to my undergraduate course of study.

I would also like to acknowledge the Harvard computer science department, from which I am receiving an S.M. in Computer Science. I especially thank Professor Margo Seltzer, for her teaching of two wonderful courses on operating systems and for inviting me to work as a teaching fellow for her courses. Finally, I thank Professor Seltzer for her advice, from coursework to my future career.

Finally, I would like to thank all of my friends for making Harvard a great place in which to live and study. I especially thank Aaron Landesman for his partnership in several math classes and for stimulating discussions on mathematics and Sitan Chen for being a sounding board for my mathematical questions and for his careful reading of and suggestions on this thesis.

Contents

1	Introduction	3
2	Elliptic Curves	6
2.1	The Mordell–Weil Theorem	8
3	Elliptic Surfaces	12
3.1	Singular fibers	14
3.2	Elliptic surfaces over \mathbb{P}^1	16
4	Intersection Theory on Elliptic Surfaces	18
4.1	The height pairing	24
5	The Shioda-Tate Theorem	27
6	Lattice Structures on Elliptic Surfaces	31
6.1	The Mordell–Weil lattice	33
6.2	Mordell–Weil lattices of rational elliptic surfaces	35
7	Construction of elliptic curves of rank 8	37
7.1	Proof of Theorem	39
7.2	Remarks on high rank elliptic curves over \mathbb{Q}	44

Chapter 1

Introduction

Elliptic curves are rich mathematical objects appearing in many different contexts. For instance, in number theory, one important class of problems is the solution of Diophantine equations. Suppose we want to find rational solutions for the equation

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

where $F \in \mathbb{Q}[x, y]$ is a polynomial in x and y . If F has degree 1 (i.e. F defines a line), the solution is very simple: for any rational number q , substituting $x = q$ will give a rational number y that solves the equation. The case when F has degree 2 (i.e. F defines a conic section) is also simple if we can find one rational solution $q = (q_0, q_1)$ for F . Let L be a line defined by a linear equation with rational coefficients that does not contain q . Then, it is easy to show that for every point $p \in L$, the second point of intersection of the line \overline{pq} with the curve defined by F has rational coefficients [17]. Moreover, all rational points satisfying F arise in this manner. Geometrically, conic sections with a k -rational point are isomorphic to the projective line, so finding rational points on conic sections is just as easy as finding points on projective lines.

The case when F has degree 3 is much more difficult. Suppose F has at least one rational solution. Then, via various algebraic transforms, we can always write the defining equation of the curve as

$$y^2 = x^3 + c_4x + c_6$$

for rational numbers c_4 and c_6 , and if the resulting curve is smooth, we say that it is an elliptic curve. An elliptic curve could contain finitely many rational points or infinitely many rational points. Moreover, unlike the case of conic sections, it is difficult to parametrize all the rational points on the elliptic curve. Because of this, elliptic curves are interesting number theoretically, as the first “difficult” case of polynomial Diophantine equations.

It turns out that the points on an elliptic curve form an abelian group. First, we choose an arbitrary point $O \in E$ to be the identity element. The group law is then defined geometrically as follows: if P and Q are points on an elliptic curve E , then let R be the third point of intersection of the line \overline{PQ} with the elliptic curve E . We define $P + Q$ to be the third point of intersection of \overline{OR} with E . The group structure provides a method to construct rational points on the curve E : if P and Q are rational points, then $P + Q$ is also a rational point on E . In fact, an elliptic curve defined over a global field is a finitely generated abelian group (the Mordell–Weil Theorem). Hence, it is possible to give a finite description of all rational points on E . Unfortunately, determining the generators is a difficult problem; in fact, even the rank of elliptic curves is not well-understood. For instance, it is not known whether there exist elliptic curves of arbitrarily large rank, and it is difficult to construct elliptic curves of high rank.

One way of approaching this problem is to work with elliptic curves over function fields $K = k(C)$. An elliptic curve $E(K)$ over the function field K can be regarded as a curve over

K , for which we can leverage the extensive theory of elliptic curves, or as a smooth surface S in the (x, y, t) space with a fibration $f : S \rightarrow C$ such that almost all fibers are elliptic curves over k . We call such surfaces *elliptic surfaces*. The Shioda-Tate theorem connects the group structure of $E(K)$ (which we refer to as the Mordell–Weil group of the elliptic surface S) with that of the Neron-Severi group $\text{NS}(S)$, defined to be the group of dimension 1 divisors on S up to algebraic equivalence.

Theorem (Shioda-Tate theorem). *There is an isomorphism $E(K) \cong \text{NS}(S)/T$, where T , the trivial sublattice of $\text{NS}(S)$, is defined to be*

$$T = \langle O, F, \{\Theta_{v,i}\} \rangle.$$

Here, O refer to the divisor corresponding to $O \in E(K)$, F refers to any fiber (since all fibers are algebraically equivalent), and $\Theta_{v,i}$ is the i -th irreducible component of a singular fiber over $v \in C$.

Using techniques of intersection theory, we can show that $\text{NS}(S)$ has finite rank, and compute the rank in certain cases (for example, when S is birationally equivalent to \mathbb{P}^2 , $\text{rank } \text{NS}(S) = 10$). The Shioda-Tate theorem then tells us that $E(K)$ is finite rank and gives an explicit formula for $\text{rank } E(K)$ in terms of $\text{rank } \text{NS}(S)$.

The intersection pairing on the elliptic surface S induces a lattice structure on $\text{NS}(S)$ and allows us to define a height pairing on $E(K)$, turning $E(K)$ into a positive-definite lattice (known as the Mordell–Weil lattice). The lattice structure of $\text{NS}(S)$ is well understood: if W is the *frame* of the elliptic surface (i.e. W is the orthogonal complement of $\langle O, F \rangle$), then W^- , the opposite lattice, is a positive-definite even integral lattice of rank $\rho - 2$, where $\rho = \text{rank } \text{NS}(S)$. If we assume that the elliptic surface is birationally equivalent to \mathbb{P}^2 (i.e. S is a rational elliptic surface) so that $\rho = 10$, then $\text{rank } W^- = 8$. Since E_8 is the unique (up to isomorphism) rank 8 positive-definite even lattice, we conclude that $W^- \cong E_8$. Comparing the definition of W with the isomorphism given in the Shioda-Tate theorem, we see that $E(K) \otimes \mathbb{Q}$ is a sublattice of $W^- \otimes \mathbb{Q}$. If the elliptic surface only has irreducible fibers, $E(K)$ is isomorphic to W^- . Hence, by constructing curves with no reducible singular fibers, we get an infinite family of elliptic curves over $\mathbb{Q}(t)$ that are isomorphic to E_8 as a lattice under the height-pairing (we need to choose E carefully so that all sections of $E(K)$ are actually defined over \mathbb{Q}). The Silverman specialization theorem then assures us that under almost all specializations of t to a rational number, the rank of the fiber $f^{-1}(v)$ is at least 8.

Moreover, the construction of elliptic curves over $\mathbb{Q}(t)$ with Mordell–Weil lattice isomorphic to E_8 yields a beautiful connection with the invariant theory of reflection groups. Recall that if G is a reflection group acting on a k -vector space V , the sub-algebra of G -invariants in $k(V)$ is a polynomial algebra generated by $\dim V$ elements (the celebrated Chevalley-Shephard-Todd theorem [2]). The Weyl group of E_8 , denoted $W(E_8)$, is a reflection group acting on the lattice E_8 , and quite remarkably, the $W(E_8)$ -invariants in the polynomial algebra generated by elements of the Mordell–Weil lattice are simply the coefficients appearing in the defining equation of the elliptic curve. This beautiful picture will also be further explained in this thesis.

The rest of this thesis is organized as follows. In Chapter 2, we give a technical introduction to elliptic curves, including a sketch of the proof that elliptic curves over global fields are finitely generated (the Mordell–Weil theorem). In Chapter 3, we define elliptic surfaces and study their basic geometric properties. In Chapter 4, we study the intersection theory of elliptic surfaces and present various properties of the Neron-Severi group. In Chapter 5 we prove the Shioda-Tate theorem, which implies the Mordell–Weil theorem for elliptic surfaces and provides an explicit formula for the rank of the elliptic surface (more correctly, the Mordell–Weil group of the elliptic surface) in terms of the rank of the Neron-Severi group. In Chapter 6, we define a

lattice structure on the Mordell–Weil group of the elliptic surface and relate these structures to the root lattice E_8 . Finally, in Chapter 7, we construct a family of elliptic surfaces whose Mordell–Weil groups are isomorphic to the lattice E_8 and showcase the beautiful connection between the structure of rational elliptic surfaces and the invariant theory of reflection groups.

Chapter 2

Elliptic Curves

Let C be a smooth irreducible projective curve defined over a field k , let $k(C)$ be the field of meromorphic functions on C (i.e. $k(C)$ is the field of fractions of the coordinate ring $\mathcal{O}_C(C)$), and let Ω_C be the k -vector space of holomorphic differential forms on C . We define the geometric genus of C to be $\dim \Omega_C$. Generally, if we have an irreducible variety V , we define the cycles of V to be formal sums of irreducible subvarieties of V , and we define a divisor to be a cycle where all components have codimension 1 in V . We use $\mathcal{D}(V)$ to denote the group of all divisors of V . If D is a divisor, we define $\deg D$ to be the sum of the coefficients appearing in D .

For a regular function $f \in k(V)$, we define $\operatorname{div}(f)$ to be

$$\operatorname{div}(f) = \sum_{Z \subseteq V} \operatorname{ord}_Z(f)[Z],$$

where the sum runs over all codimension one subvarieties of V , and $\operatorname{ord}_Z(f)$, the order of vanishing of f on Z , is defined to be the length of $\mathcal{O}_V(Z)/f\mathcal{O}_V(Z)$; this sum is finite since the length is 0 unless f vanishes on the generic point of Z . More generally, if $f = g/h \in k(V)$ where g and h are regular functions, we define $\operatorname{div}(f) = \operatorname{div}(g) - \operatorname{div}(h)$. We say two divisors D_1 and D_2 are linearly equivalent if $D_1 = D_2 + \operatorname{div} f$ for some $f \in k(V)$, and we write $D_1 \sim D_2$. Finally, we define $\mathcal{D}_l(V)$ to be the group of divisors linearly equivalent to 0, and $\operatorname{Pic}^0 V$ to be the degree 0 component of $\mathcal{D}(V)/\mathcal{D}_l(V)$.

Using this vocabulary, we can state the Riemann-Roch theorem for curves:

Theorem (Riemann-Roch). *Let C be a smooth curve, K_C a canonical divisor on C , and $g \in \mathbb{Z}_{\geq 0}$ the geometric genus of C . For a divisor D , define the vector space*

$$L(D) = \{f \in \bar{k}(C)^* : \operatorname{div}(f) \geq -D\} \cup \{0\},$$

and let $l(D) = \dim L(D)$. Then,

$$l(D) - l(K_C - D) = \deg D - g + 1.$$

Because the Riemann-Roch theorem relates the size of $\bar{k}(C)^*$ to the genus of C , it makes sense to study curves based on their genus.

Because genus 0 smooth curves are isomorphic to \mathbb{P}^1 if they contain a k -rational point, their geometry is already well understood, so we turn our attention to genus 1 smooth curves, which we call *elliptic curves*.

Definition 2.1. Let k be any field. An elliptic curve E/k is a smooth genus 1 projective curve over k with a specified point $O \in E(k)$.¹

¹ The nomenclature arises from the connection between elliptic curves and elliptic integrals, which represent the perimeter of an ellipse. If $\wp(t)$ denotes the Weierstrass elliptic function, $(\wp(t), \wp'(t))$ gives a parametrization of an elliptic curve $E(\mathbb{C})$.

The constraint of genus 1 gives remarkable structure to these objects: we can write down explicit formulas for elliptic curves and prove that they in fact form a group.

Proposition 2.2 (see [15] for proof). *Let $E(k)$ be an elliptic curve with chosen point O .*

1. *$E(k)$ is isomorphic to a curve in \mathbb{P}^2 given by the inhomogeneous equation*

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

for some $a_1, a_2, a_3, a_4, a_6 \in k$. We call this a Weierstrass form for E .

2. *There is a bijection between $E(k)$ and $\text{Pic}^0(E)$ given by $P \mapsto (P) - (O)$, which turns $E(k)$ into an abelian group with identity element O . Moreover, if $E(k)$ is given by the Weierstrass equation, and $P, Q \in E(k)$, then $P + Q$ is derived geometrically from P and Q in the following fashion: let R be the third intersection point of the line \overline{PQ} with $E(k)$ (since $E(k)$ is of degree 3, lines intersect $E(k)$ at 3 points with multiplicity). Then, $P + Q$ is the third point of intersection of \overline{RO} with $E(k)$.*

Because of Proposition 2.2, we can assume without loss of generality that we are working with an elliptic curve in Weierstrass form:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

If we assume $\text{char}(k) \neq 2$, then the substitution $y \mapsto \frac{1}{2}(y - a_1x - a_3)$ transforms the equation into

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

where

$$\begin{aligned} b_2 &= a_1^2 + 4a_4 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6. \end{aligned}$$

If we further assume that $\text{char}(k) \neq 3$ then the substitution

$$(x, y) \mapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108} \right)$$

transforms the curve into the simpler form

$$y^2 = x^3 - 27c_4x - 54c_6,$$

where $c_4 = b_2^2 - 24b_4$ and $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$. The only changes of variables preserving this form of the equation are of the form $x = u^2x'$ and $y = u^3y'$. Then, x' and y' satisfy the transformed Weierstrass equation

$$y'^2 = x'^3 - 27c'_4x' - 54c'_6,$$

where $c'_4 = u^4c_4$ and $c'_6 = u^6c_6$ (which, of course, is why we labeled the coefficients in this specific way).

More generally, any cubic polynomial in x and y of the form

$$s_1x^3 + s_2x^2y + s_3xy^2 + s_4y^3 + s_5x^2 + s_6xy + s_7y^2 + s_8x + s_9y = 0$$

defines an elliptic curve, and Nagell's algorithm gives the change of variables necessary to transform a general cubic to the Weierstrass form [8]. We can choose O to be the point $(0, 0)$.

From here on, we assume that $\text{char}(k) = 0$. A curve C described by the Weierstrass equation

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

is nonsingular if and only if the discriminant

$$\Delta = -16(4A^3 + 27B^2)$$

is nonzero. If $\Delta = 0$, then C has a singular point, which is a cusp if $A = B = 0$ and a node otherwise.

We also define the invariant differential for an elliptic curve E to be

$$\omega = \frac{dx}{2y} = \frac{dy}{3x^2 + A}.$$

Because E is nonsingular, the derivatives $2y$ and $3x^2 + A$ cannot simultaneously vanish at a point on E , so ω is a holomorphic form. Since an elliptic curve has genus 1, the k -vector space of holomorphic differential forms $\Omega_{E(k)}$ has dimension 1, and is thus generated by ω .

The group structure of $E(k)$ is very important number theoretically. For example, a cubic Diophantine equation with a rational solution defines an elliptic curve $E(\mathbb{Q})$, and solving the Diophantine equation is equivalent to finding points on the curve. If we found points P_1, P_2, \dots, P_k on the curve, then we can generate, using the explicit formula for the group sum, an entire family of points

$$n_1P_1 + \dots + n_kP_k$$

that lie on $E(\mathbb{Q})$.

2.1 The Mordell–Weil Theorem

Let us now consider elliptic curves over global fields, i.e. finite extensions of \mathbb{Q} or $\mathbb{F}_q(t)$.² These curves arise frequently in the study of Diophantine equations. For instance, given an equation $E: y^2 = x^3 + Ax + B$, we might ask about rational points on this curve, which correspond to properties of the elliptic curve $E(\mathbb{Q})$. Because $E(\mathbb{Q})$ is an abelian group, all rational points P on E can be expressed in terms of generators P_1, P_2, \dots of $E(\mathbb{Q})$:

$$P = \sum_{i=1}^{\infty} n_i P_i.$$

The Mordell–Weil theorem tells us that, in fact, $E(\mathbb{Q})$ is finitely generated, so if we find a finite list of generators of $E(\mathbb{Q})$, we can explicitly calculate any point on $E(\mathbb{Q})$ (which in general could be an infinite set).

Theorem (Mordell–Weil). *Let k be a global field. Then $E(k)$ is a finitely generated abelian group.*

Proof. We present a sketch of the proof. First, we show that $E(k)/mE(k)$ is a finite group for some $m > 1$ (in fact, it is true for every $m > 1$), a result also known as the weak Mordell–Weil theorem. Assume without loss of generality that $E(k)$ contains all the m -torsion points

²Note, however, that $\mathbb{Q}(t)$ and $\mathbb{C}(t)$ are not global fields. Indeed, the Mordell–Weil theorem does not hold over $\mathbb{C}(t)$ unless additional assumptions are made.

$E[m] \subset E(\bar{k})$; if not, we can take a finite field extension k'/k so that $E[m] \subset E(k')$, and we can prove that $E(k)$ is finitely generated if $E(k')$ is.

Given that $E(k)$ contains $E[m]$, we define the Kummer pairing between $E(k)$ and the Galois group $G_{\bar{k}/k}$ to be

$$\begin{aligned}\kappa : E(k) \times G_{\bar{k}/k} &\rightarrow E[m] \\ (P, \sigma) &\mapsto Q^\sigma - Q,\end{aligned}$$

where $Q \in E(\bar{k})$ is any point satisfying $mQ = P$. By studying the kernel of this bilinear pairing, we establish a one-to-one correspondence between $E(k)/mE(k)$ and the Galois group $G_{L/k}$, where $L = k(m^{-1}E(k))$, the compositum of all fields $k(Q)$ as Q ranges over the points in $E(\bar{k})$ satisfying $mQ \in E(k)$. We show that L satisfies certain number theoretic properties (L/k is an abelian extension of exponent m and is unramified outside a finite set of primes that includes M_k^∞), and show that all such field extensions are finite extensions of k [15].

Having shown that $E(k)/mE(k)$ is a finite set, we could choose representative elements $Q_1, \dots, Q_r \in E(k)$ of the finitely many cosets of $E(k)/mE(k)$, and hope that we can write every element of $E(k)$ in terms of these generators, plus possibly a finite number of extra generators to fill in the gaps. To show that this is always possible, we show that we can define a *height function* on $E(k)$ that satisfies the following properties:³

Definition 2.3. A height function is a function $h : E(k) \rightarrow \mathbb{Q}$ satisfying the following properties:

1. $h(P+Q) \leq 2h(P) + C_Q$ for some constant C_Q depending only on Q and the elliptic curve $E(k)$.
2. $h(mP) \geq m^2h(P) - C_2$ for some constant C_2 depending only on the elliptic curve $E(k)$.
3. For every constant C , $\{P \in E(k) : h(P) \leq C\}$ is finite.

The intuition behind the original constructions of height functions is that height functions ought to measure the arithmetic complexity of a point $P \in E(k)$. For instance, for $k = \mathbb{Q}$, we can define the height of a rational number $q = \frac{a}{b}$ by $H(q) = \max(a, b)$ and the height of a point to be

$$h(P) = \begin{cases} \log H(x(P)) & \text{if } P \neq O \\ 0 & \text{otherwise} \end{cases}.$$

If $k = F(t)$ is the function field over some field F , we can define $H(p) = \deg p$ and $h(P)$ similarly. In general, for an arbitrary global field k , we can define the height of an element of $\mathbb{P}^1(k)$ to be

$$H(q) = \prod_{v \in M_k} \max(|q_0|_v, |q_1|_v)^{[k_v:\mathbb{Q}_v]},$$

where the product runs over all places of K . This product is well defined since $\max(|q_0|_v, |q_1|_v) = 1$ for all but finitely many places v and

$$\prod_{v \in M_k} |c|_v = 1$$

for all $c \in k^*$. We can then define

$$h_f(P) = \log H(f(P)),$$

³We follow the definition given in [15].

where f is any non-constant even function in $k(E)$ (for example, $f = x$, the x -coordinate of P).

Given any height function h_f , we can define a unique canonical height function (also known as the Neron-Tate height) $\hat{h} : E(k) \rightarrow \mathbb{R}$ by

$$\hat{h}(P) = \frac{1}{\deg(f)} \lim_{N \rightarrow \infty} 4^{-N} h_f([2^N]P).$$

The canonical height satisfies the following properties [15]:

1. $\hat{h}([m]P) = m^2 \hat{h}(P)$ for all $m \in \mathbb{Z}$.
2. $\hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q)$ (parallelogram law).
3. $\hat{h}(P) \geq 0$, with equality if and only if P is a torsion point.
4. $\hat{h}(P) = h(P) + O(1)$.

Because of these nicer properties, we assume from now on that we are always working with the canonical height.

Now, given a point P , define $P_0 = P$ and P_j for $j > 0$ by $P_{j-1} = mP_j + Q_{i_j}$, which is always possible since the Q_i are representatives of the cosets in $E(k)/mE(k)$. Let $C = \max_i C_{Q_i}$. Then,

$$P = Q_{i_1} + mQ_{i_2} + \cdots + m^{n-1}Q_{i_n} + m^n P_n$$

for all n . By the properties of the height function,

$$\begin{aligned} h(P_j) &= \frac{1}{m^2} h(mP_j) \\ &= \frac{1}{m^2} h(P_{j-1} - Q_{i_j}) \\ &\leq \frac{1}{m^2} (2h(P_{j-1}) + C), \end{aligned}$$

so repeating this and using $m \geq 2$, $h(P_n) \leq \frac{1}{2^n} h(P) + \frac{1}{4^n} C$. Hence, we can choose a large enough n such that $h(P_n) \leq 1$, and since there are only a finite number of such points, we can include all such points in our list of generators, so that our expression for P involves only our chosen generators. This shows that $E(k)$ is a finitely generated abelian group. \square

In addition to possessing the structure of an abelian group, $E(k)/E_{\text{tor}}(k)$ also has the structure of a lattice, i.e. it has a bilinear pairing. Namely, if h is the canonical height, define the height pairing to be

$$\langle P, Q \rangle = \frac{1}{2} (h(P + Q) - h(P) - h(Q)).$$

Then, repeatedly applying the parallelogram law,

$$\begin{aligned} \langle P + R, Q \rangle &= \frac{1}{2} (h(P + R + Q) - h(P + R) - h(Q)) \\ &= \frac{1}{4} h(P + R + Q) - \frac{1}{4} h(P + R - Q) \\ &= \frac{1}{4} (2h(P + Q) + 2h(R) - h(P - R + Q)) - \frac{1}{4} (2h(P) + 2h(R - Q) - h(P - R + Q)) \\ &= \frac{1}{2} (h(P + Q) - h(P) - h(Q)) + \frac{1}{2} (h(R) + h(Q) - h(R - Q)) \\ &= \frac{1}{2} (h(P + Q) - h(P) - h(Q)) + \frac{1}{2} (h(R + Q) - h(R) - h(Q)) \\ &= \langle P, Q \rangle + \langle R, Q \rangle. \end{aligned}$$

This bilinear pairing is non-degenerate on $E(k)/E_{\text{tor}}(k)$ by properties of the canonical height.

Knowing that $E(k)$ is a finitely-generated abelian group, it is natural to ask questions about its rank and its torsion subgroup. The torsion subgroup is relatively well-understood, at least over \mathbb{Q} . For instance, Mazur proved that the torsion subgroup of $E(\mathbb{Q})$ could only be one of fifteen groups [15]:

Theorem (Mazur). *The torsion subgroup of $E(\mathbb{Q})$ is isomorphic to one of the following:*

1. $\mathbb{Z}/n\mathbb{Z}$ for $1 \leq n \leq 10$ or $n = 12$
2. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ for $1 \leq n \leq 4$.

Furthermore, each of the above groups occurs as the torsion subgroup of infinitely many elliptic curves.

The rank, however, is much less well-understood, both in general and for specific curves. For instance, it is conjectured that there exists elliptic curves $E(\mathbb{Q})$ of arbitrarily large rank [15], but it is difficult to produce curves with high rank;⁴ the largest rank elliptic curve found so far,

$$y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x \\ + 34481611795030556467032985690390720374855944359319180361266008296291939448732243429,$$

is only known to have rank at least 28 [5].⁵ The Birch-Swinnerton-Dyer conjecture, one of the Millennium Prize problems, states that the rank of the elliptic curve is given by the vanishing order of the L-series $L(E/k, s)$ of E/k at $s = 1$. Progress on this conjecture has been scant; for instance, it has only been recently shown that $L(E/\mathbb{Q}, s)$ is actually well-defined at $s = 1$ (this follows from Wiles' Modularity Theorem), and that if E/\mathbb{Q} is of rank at least 1, then $L(E, 1) = 0$ [15].

⁴ Indeed, other papers present evidence that $\text{rank } E(\mathbb{Q})$ is bounded as we vary the curve E . For example, [9] uses probabilistic arguments to suggest that perhaps there are only finitely many elliptic curves of rank greater than 21.

⁵ It has been shown that assuming the generalized Riemann Hypothesis and Birch-Swinnerton-Dyer conjecture (to equate the rank of the elliptic curve with the vanishing order of L-series at $s = 1$) that the rank of this curve is either 28 or 30 [1]. An unpublished preprint showed that only assuming the generalized Riemann Hypothesis, we can show that the curve has rank 28 and is in fact isomorphic as a group to \mathbb{Z}^{28} [6].

Chapter 3

Elliptic Surfaces

As discussed in the previous chapter, determining the rank of an elliptic curve over a number field is difficult. For the rest of the thesis, we analyze the analogous problem of determining the rank of elliptic curves over function fields $K = k(C)$, where k is a characteristic 0 field and C is a curve defined over k .

Let $E(K)$ be such an elliptic curve, with Weierstrass equation

$$y^2 = x^3 + ax + b,$$

where $a, b \in K$. Because $E(K)$ is non-singular, its discriminant is a nonzero function in K , so for almost all $t_0 \in C$, specialization at t_0 produces a nonsingular curve E_{t_0} given by

$$y^2 = x^3 + a(t_0)x + b(t_0),$$

and the choice of infinity as the identity element turns $E_{t_0}(k)$ into an elliptic curve.

We can also regard $E(K)$ as a surface if we consider all t simultaneously. Let

$$S' = \{(t, X, Y, Z) \mid Y^2Z = X^3 + a(t)XZ^2 + b(t)Z^3, t \text{ not a pole of } a(t) \text{ or } b(t)\},$$

and define S to be the Zariski closure of S' . The projection $f : S \rightarrow C$ turns S into a fibered surface, and for almost all t , namely those t where $a(t) \neq \infty$ and $b(t) \neq \infty$, the fiber is just $f^{-1}(t) = E_t$. Moreover, for almost all t , namely those t satisfying

$$4a(t)^3 + 27b(t)^2 \neq 0,$$

E_t is an elliptic curve. Finally, there is a section $O : C \rightarrow S$ sending t to O_t , the identity element of E_t . We call such fibered surfaces where almost all fibers are elliptic curves *elliptic surfaces*.

Definition 3.1. An elliptic surface is a smooth projective surface S with a fibration $f : S \rightarrow C$ such that all but finitely many fibers are elliptic curves and no fiber contains a smooth rational curve with self-intersection -1 (i.e. an exceptional curve of the first kind). We further assume in this thesis that f has a global section $O : C \rightarrow S$.

Example 3.2. Let g_1 and g_2 be two homogeneous cubic polynomials in 3 variables cutting out two curves in \mathbb{P}^2 that intersect everywhere transversely. Then, these two hypersurfaces intersect in 9 points P_1, \dots, P_9 , and the cubic pencil,

$$S = \{(\mathbf{x}, \lambda) \mid \lambda_1 g_1(\mathbf{x}) + \lambda_2 g_2(\mathbf{x}) = 0\} \subseteq \mathbb{P}^2 \times \mathbb{P}^1$$

is isomorphic to the blowup of \mathbb{P}^2 at the 9 points of intersection. The projection onto the second factor turns S into a elliptic surface: the fiber over a point with homogeneous coordinates (λ_1, λ_2) is given by the cubic equation

$$\lambda_1 g_1(\mathbf{x}) + \lambda_2 g_2(\mathbf{x}) = 0,$$

and the choice $O = P_1$ turns this fiber into an elliptic curve. Hence, the blowup is an elliptic surface with section $O(t) = P_1$.

Proposition 3.3. *1. Let $E(K)$ be an elliptic curve. To each Weierstrass equation $y^2 = x^3 + a(t)x + b(t)$ for the curve, we can associate an elliptic surface*

$$S(a, b) = \text{clos}\{([X, Y, Z], t) \in \mathbb{P}^2 \times C : Y^2Z = X^3 + a(t)XZ^2 + B(t)Z^3\}.$$

If we start with a different Weierstrass equation $y^2 = x^3 + a'(t)x + b'(t)$ for $E(K)$, then $S(a', b')$ and $S(a, b)$ are k -birationally equivalent over C .

2. Let $S \rightarrow C$ be an elliptic surface. Then, S is k -birationally equivalent over C to $S(a, b)$ for some $a, b \in k(C)$. If $S(a, b)$ and $S(a', b')$ are both k -birationally equivalent to S over C , the curves defined by $y^2 = x^3 + a(t)x + b(t)$ and by $y^2 = x^3 + a'(t)x + b'(t)$ are K -isomorphic.

Proof. 1. The discussion preceding the theorem shows that $S(a, b)$ is an elliptic surface. Let $y^2 = x^3 + a'(t)x + b'(t)$ be another Weierstrass equation for the curve. Then, there exists $u \in k(C)$ such that $a(t) = u(t)^4 a'(t)$ and $b(t) = u(t)^6 b'(t)$. Under this transformation, $x(t) = u(t)^2 x'(t)$ and $y(t) = u(t)^3 y'(t)$, which gives a birational equivalence $S(a', b') \rightarrow S(a, b)$.

2. The projection $S \rightarrow C$ induces an inclusion of function fields $k(C) \rightarrow k(S)$. Since S is a surface, the extension $k(S)/k$ has transcendence degree 2 and $k(C)/k$ has transcendence degree 1, so $k(S)/k(C)$ has transcendence degree 1, and so there exists a unique curve E over $k(C)$ whose function field is isomorphic to $k(S)$ up to $k(C)$ -algebra isomorphisms. We show that E is an elliptic curve by proving that the vector space of differential forms $\Omega_{E(k(C))}$ has dimension 1.

Let $\{f_i(t, \mathbf{x})\}$ be the defining equations for E as a curve over $k(C)$. Consider the k -surface

$$S' = \{(\mathbf{x}, t) \in \mathbb{P}^N \times C : f_i(t, \mathbf{x}) = 0\}.$$

The projection onto the second factor gives $k(S')$ a $k(C)$ -algebra structure. By construction, $k(S)' \cong k(E) \cong k(S)$ as $k(C)$ algebras, so S' and S are birationally equivalent. In particular, almost all fibers of S' are of genus 1.

Given that the fibers of S' are of genus 1, we show that E is of genus 1. Let $\omega_1, \omega_2 \in \Omega_{E(K)}$ be two non-zero holomorphic differential forms. Then, $\omega_{1,t}(x) := \omega_1(t, x)$ and $\omega_{2,t}(x) := \omega_2(t, x)$ are non-zero holomorphic differential forms of S'_t for almost all $t \in C$. Since S'_t are curves of genus 1 for almost all $t \in C$, the vector spaces $\Omega_{S'_t(k)}$ have dimension 1, so $\frac{\omega_{1,t}(x)}{\omega_{2,t}(x)} \in k$. This implies that $\frac{\omega_1}{\omega_2} \in k(C)$, so ω_1 and ω_2 are $k(C)$ -linearly dependent. Since $\Omega_{E/k(C)}$ has dimension at most 1, E has genus at most 1. But E cannot have genus 0, because then, $E \cong \mathbb{P}^1$ and $S' \cong \mathbb{P}^1 \times C$, so the generic fiber of S' would have genus 0.

It remains to construct the identity element of E . To do this, we associate to every section $\sigma : C \rightarrow S$ a point $P \in E$ in the following manner: because S and S' are birationally equivalent, there is a corresponding section $\sigma' : C \rightarrow S'$ given by $\sigma'(t) = (h_1(t), h_2(t), \dots, h_N(t), t)$. We can then define P to be the point $P = (h_1, \dots, h_n) \in E$. Because we require elliptic surfaces to have a distinguished section $O : C \rightarrow S$, we have a corresponding point in $E/k(C)$, which we label as O also. This shows that E is a genus one curve with a rational point, so E is an elliptic curve. We can then write a Weierstrass equation for E

$$y^2 = x^3 + ax + b,$$

and so by construction, $S(a, b) = \text{clos } S'$ is birationally equivalent to S .

Finally, if $S(a', b')$ and $S(a, b)$ are both birationally equivalent to S , then almost all fibers are isomorphic, so over almost all $t_0 \in C$,

$$\begin{aligned} a'(t_0) &= u(t_0)^4 a(t_0) \\ b'(t_0) &= u(t_0)^6 b(t_0) \end{aligned}$$

for some $u(t_0) \in k$. Since the birational map $S(a, b) \rightarrow S(a', b')$ is algebraic, $u(t) \in k(C)$, and so the elliptic curves (over K) defined by $y^2 = x^3 + ax + b$ and $y^2 = x^3 + a'x + b'$ are isomorphic.

□

Proposition 3.3 implies that E is the generic fiber of S (i.e., if $p \in C$ is the generic point of C , then E is isomorphic as a variety to $f^{-1}(p)$). We therefore freely identify global sections $P : C \rightarrow S$ with points $P \in E(K)$.

Definition 3.4. The Mordell–Weil group of an elliptic surface $f : S \rightarrow C$ is defined to be $E(K)$, the group of rational points of the generic fiber of S .

We know that elliptic curves over global fields are finitely generated, so we might wonder whether elliptic curves over function fields $K = k(C)$ are finitely generated for any field k . Without any additional assumptions, however, $E(K)$ is not necessarily finitely generated. For example, let $E_0(k)$ be an elliptic curve with equation $y^2 = x^3 + ax + b$, and consider $S = E_0 \times C$. Then, every point $P \in E_0$ defines a section $C \rightarrow S$, namely $t \mapsto P$ for all $t \in C$. If $k = \mathbb{C}$, then $E_0(k)$ is not finitely generated, so $E_0(k(C))$ is also not finitely generated.

It turns out that such elliptic surfaces are the only ones that are not finitely generated. In particular, if we assume that f is not everywhere smooth (i.e., $f^{-1}(p)$ is singular for some $p \in C$), then we can prove the Mordell–Weil theorem for elliptic curves over function fields.

Assumption. We assume that the elliptic surface $f : S \rightarrow C$ has at least one singular fiber.

3.1 Singular fibers

Singular fibers of elliptic surfaces play a crucial role in the theory of elliptic surfaces. In this section, we give a general outline of the classification of singular fibers by Kodaira [10].

We start with an elliptic curve $E(K)$ described by a Weierstrass equation

$$y^2 = x^3 + a_4(t)x + a_6(t).$$

Let $C^0 \subset C$ be the set of points above which the fiber is nonsingular, and define

$$S^0 = \{([X, Y, Z], t) \in \mathbb{P}^2 \times C \mid Y^2Z = X^3 + a_4(t)XZ^2 + a_6(t), t \in C^0\}.$$

We use Tate’s algorithm to construct a relatively minimal surface S birationally equivalent to S^0 , which we call the Kodaira–Neron model. The Kodaira–Neron model is necessarily unique: if S' is another relatively minimal surface then we have a birational morphism $S \rightarrow S'$, and since S and S' are isomorphic on the nonsingular fibers and the surfaces are relatively minimal, S and S' are isomorphic.

We now give a rough overview of Tate’s algorithm; our assumption that $\text{char}(k) = 0$ simplifies the treatment, as we avoid the special cases of $\text{char}(k) = 2$ or 3 . Let t be a local coordinate

Type	$v(a_4)$	$v(a_6)$	$v(\Delta)$
I_0	0	≥ 0	0
I_0	≥ 0	0	0
I_n	0	0	n
II	≥ 1	1	2
III	1	≥ 2	3
IV	≥ 2	2	4
I_0^*	2	≥ 3	6
I_0^*	≥ 2	3	6
I_{n-6}^*	2	3	n
IV^*	≥ 3	4	8
III^*	3	≥ 5	9
II^*	≥ 4	5	10

Table 3.1: Kodaira class of singular fiber in relation to Weierstrass coefficients. Note that I_0 is the class of a nonsingular fiber. In the multiplicative cases (I_n for $n \geq 1$), the number of irreducible components of the singular fiber is $v(\Delta)$, and in the additive cases (all other cases), the number of irreducible components of the fiber is $v(\Delta) - 1$.

for C , and suppose $E(K)$ is given by the Weierstrass equation $y^2 = x^3 + a_4(t)x + a_6(t)$ with discriminant

$$\Delta = -27a_6^2 - 4a_4^3.$$

Without loss of generality, assume there is a singular fiber at $t = 0$. Then, the discriminant must vanish at $t = 0$, so either $t \nmid a_4$ and $t \nmid a_6$, or $t \mid a_4$ and $t \mid a_6$. In the first case, the fiber has a node, and we call the fiber *multiplicative*. Otherwise, the fiber has a cusp, and we call it *additive*. The origin of this terminology is that in the first case, the nonsingular points of the fiber form a group isomorphic to the multiplicative group K^* , and in the latter case, the nonsingular points form a group isomorphic to the additive group K .

First, let us consider the multiplicative case. Let $n = v(\Delta)$, where v is the valuation with uniformizer t . If $n = 1$, then the fiber is singular but the surface is nonsingular, and we label the fiber with Kodaira class I_1 . If $n > 1$, the singular point of the fiber is also a singularity of the surface, so we blow up the surface multiple times at that singular point to arrive at a surface smooth locally around $t = 0$. This blow up process introduces n rational curves of self intersection -2 , and we label this singular fiber with the Kodaira class I_n .

Now, let us consider the additive case. If $v(a_6) = 1$, then $(0, 0)$ is not a surface singularity, and we label the singular fiber with the Kodaira class II . Otherwise, we blowup the surface at $(0, 0)$. There are three resulting possibilities for the exceptional divisor:

1. A degree 2 curve meeting the strict transform of the cuspid tangentially at one point.
2. Two lines meeting the strict transform of the cuspid at one point.
3. A double line.

In the first two cases, the resulting surface has been de-singularized, and we assign the Kodaira classes III and IV to the singular fiber. In the third case, further blow ups are necessary, producing Kodaira classes I_0^* , IV^* , III^* , II^* , and I_n^* .

Table 3.1 gives the Kodaira class of a singular fiber at $t = 0$.

3.2 Elliptic surfaces over \mathbb{P}^1

Let $f : S \rightarrow \mathbb{P}^1$ be an elliptic surface over \mathbb{P}^1 . Then, we can choose a Weierstrass equation that minimizes $v(\Delta)$ for all valuations v . To do this, suppose $v(a_4) \geq 4$ and $v(a_6) \geq 6$, so that $a_4 = t^4 a'_4$ and $a_6 = t^6 a'_6$. Then, the change of variables $x \mapsto t^2 x$, $y \mapsto t^3 y$ transforms the Weierstrass equation

$$y^2 = x^3 + t^4 a'_4 x + t^6 a'_6$$

into

$$y^2 = x^3 + a'_4 x + a'_6,$$

decreasing $v(\Delta)$ by 12. Hence, after finitely many steps, either $v(a_4) < 4$ or $v(a_6) < 6$. We repeat this for each finite valuation to arrive at a globally minimal Weierstrass equation.

Now, choose the smallest integer χ such that $\deg(a_i) \leq i\chi$ for this minimal Weierstrass equation. Using homogeneous coordinates (s, t) for \mathbb{P}^1 , we can write each a_i as a homogeneous degree $i\chi$ polynomial in s and t . Note that since we assume that $f : S \rightarrow \mathbb{P}^1$ has a singular fiber, $\chi > 0$.

Theorem 3.5. *Let $f : S \rightarrow \mathbb{P}^1$ be an elliptic surface. The canonical bundle K_S is algebraically equivalent to $(\chi - 2)F$.*

Proof. The canonical form of S is given by

$$\omega_S = \omega_E dt = \frac{dx dt}{2y},$$

where ω_E is the canonical form of $E(K)$ given in Chapter 2. Let

$$y^2 = x^3 + a_4 x + a_6,$$

be the Weierstrass equation for $E(K)$. Since a_6 is a degree 6χ polynomial in t , we conclude that y is a degree 3χ polynomial in t and x is a degree 2χ polynomial in t . Hence, y and dx have order 3χ and 2χ poles at infinity respectively. Moreover, since dt has an order 2 pole at infinity, we conclude that the canonical form ω_S has an order $3\chi - 2\chi - 2 = \chi - 2$ zero at infinity, so

$$K_S = \operatorname{div} \omega_S = (\chi - 2)F.$$

□

Proposition 3.6. *The integer χ given above is equal to the arithmetic genus of S .*

Proof. Let $e(S)$ be the Euler number for the elliptic surface S . Then, by Noether's formula,

$$12\chi'(S) = (K_S \cdot K_S) + e(S),$$

where $\chi'(S)$ denotes the arithmetic genus of S . Since $K_S = (\chi - 2)F$, $(K_S \cdot K_S) = 0$, so

$$12\chi'(S) = e(S).$$

We cite Proposition 15 in [3]:

Lemma 3.7. *For an elliptic surface S ,*

$$e(S) = \sum_{v \in C} e(F_v).$$

Now, as proven in [10],

$$e(F_v) = \begin{cases} 0 & \text{if } F_v \text{ is smooth} \\ m_v & \text{if } F_v \text{ is multiplicative} \\ m_v + 1 & \text{if } F_v \text{ is additive} \end{cases}$$

Hence, $e(F_v) = v(\Delta)$, so

$$12\chi'(S) = e(S) = \sum_{v \in \mathbb{P}^1} e(F_v) = \sum_{v \in \mathbb{P}^1} v(\Delta) = \deg \Delta = 12\chi,$$

so $\chi'(S) = \chi$ as desired. □

Definition 3.8. A rational elliptic surface is an elliptic surface $f : S \rightarrow \mathbb{P}^1$ \bar{k} -birationally equivalent to \mathbb{P}^2 .

A rational elliptic surface has arithmetic genus $\chi = 1$, since that is the arithmetic genus of \mathbb{P}^2 . Conversely, it is known that an elliptic surface with $\chi = 1$ is a rational elliptic surface [10].

Example 3.9. 1. The elliptic surface given in Example 3.2 is rational, since it is the blowup of \mathbb{P}^2 at nine points.

2. The elliptic surface given by $y^2 = x^3 - t^4x + t^4$ is rational since $\deg a_4 \leq 4$ and $\deg a_6 < 6$.

Chapter 4

Intersection Theory on Elliptic Surfaces

One of the chief advantages of working with elliptic curves over function fields as opposed to elliptic curves over global fields is the ability to leverage intersection theory on the corresponding elliptic surface. In particular, the intersection pairing of two divisors (intuitively defined as the number of intersection points of the curves that make up the divisor) endows a geometrically defined group, the Neron-Severi group, with a lattice structure. We can also use the intersection pairing to construct a height pairing and a height function on the corresponding elliptic curve. In Chapter 5, we will use the tools developed in this section to prove the Mordell–Weil theorem for elliptic surfaces. In Chapter 6, we study the lattice structure induced by the height pairing on $E(K)$, and in Chapter 7, we construct families of elliptic curves with rank 8.

In this section, we study the intersection theory of elliptic surfaces and properties of the Neron-Severi group. We assume that we work with an elliptic surface $f : S \rightarrow \mathbb{P}^1$ with arithmetic genus χ , although most results in this section generalize for any curve C .

First, recall the definition of algebraic equivalence of two divisors:

Definition 4.1. Two divisors $D_1, D_2 \in \mathcal{D}(S)$ are *algebraically equivalent* if there exists a curve Γ and a cycle V on $S \times \Gamma$ flat over Γ such that

$$V \cap (X \times \{c\}) - V \cap (X \times \{d\}) = Z - Z'$$

for two points $c, d \in \Gamma$.

We define:

- F to be the algebraic equivalence class of any fiber of $f : S \rightarrow C$ (these are all algebraically equivalent since we can take $\Gamma = C$ and $V = S \times_C C$);
- $\Theta_{v,i}$ to be the irreducible components of $f^{-1}(v)$, with $\Theta_{v,0}$ being the irreducible component that intersects the identity section $O \rightarrow S$;
- m_v to be the number of irreducible components of $F_v = f^{-1}(v)$;
- R to be the set of points $v \in C$ such that F_v is singular;
- $\mathcal{D}(S)$ to be the group of divisors of S ;
- $\mathcal{D}_a(C)$ to be the divisors algebraically equivalent to 0;
- $\mathcal{D}_l(C)$ to be the divisors linearly equivalent to 0;

- $\text{Pic}^0(S) = \mathcal{D}_a(C)/\mathcal{D}_l(C)$;
- $\mathcal{D}_{ver}(S)$ to be the group of divisors generated by curves contained in some fiber $f^{-1}(v)$, which we call *vertical divisors*;
- $\mathcal{D}_{hor}(S)$ to be the group of divisors generated by curves not contained in any fibers, which we call *horizontal divisors*;
- $T = \mathcal{D}_{ver}(S) + \mathbb{Z}O$, the trivial lattice.

We write $D_1 \sim D_2$ if D_1 and D_2 are linearly equivalent, and $D_1 \approx D_2$ if D_1 and D_2 are algebraically equivalent.

Definition 4.2. The Neron-Severi group is defined to be

$$\text{NS}(S) = \mathcal{D}(S)/\mathcal{D}_a(S).$$

Note that modulo algebraic equivalence, $\mathcal{D}_{ver}(S)$ is generated by F and $\Theta_{v,i}$ for $v \in R$ and $i \geq 1$, since all fibers are algebraically equivalent and $\sum_{i=0}^{m_v-1} \Theta_{v,i} \approx F$.

We define an intersection pairing on divisors of S . Let $\Gamma \subset S$ be an irreducible curve and $\mathcal{O}_{S,\Gamma}$ the local ring of S on Γ , i.e.

$$\mathcal{O}_{S,\Gamma} = \{f \in k(S) \mid f \text{ is defined for some } P \in \Gamma\}.$$

Since S is nonsingular, $\mathcal{O}_{S,\Gamma}$ is a regular local ring of dimension 1, so it is a discrete valuation ring. Let f_Γ be a uniformizer of $\mathcal{O}_{S,\Gamma}$.

Now, given two irreducible curves Γ_1 and Γ_2 lying on S with $\Gamma_1 \neq \Gamma_2$, we define the local intersection index of Γ_1 and Γ_2 at a point $P \in S$ to be

$$(\Gamma_1 \cdot \Gamma_2)_P = \dim_k \mathcal{O}_{S,P}/(f_{\Gamma_1}, f_{\Gamma_2}).$$

Note that if $P \notin \Gamma_i$, then $f_{\Gamma_i}(P) \neq 0$, so f_{Γ_i} is invertible in $\mathcal{O}_{S,P}$, so $(\Gamma_1 \cdot \Gamma_2)_P = 0$. We define

$$(\Gamma_1 \cdot \Gamma_2) = \sum_{P \in \Gamma_1 \cap \Gamma_2} (\Gamma_1 \cdot \Gamma_2)_P.$$

Intuitively, $(\Gamma_1 \cdot \Gamma_2)$ is the number of intersection points of Γ_1 and Γ_2 counting multiplicity.

To define the intersection pairing of two divisors D_1 and D_2 with no common components, we simply extend the above definition linearly: if $D_1 = \sum_i a_i \Gamma_i$ and $D_2 = \sum_j a'_j \Gamma'_j$, we define

$$(D_1 \cdot D_2) = \sum_i \sum_j \sum_{P \in \Gamma_i \cap \Gamma'_j} a_i a'_j (\Gamma_i \cdot \Gamma'_j)_P.$$

Finally, for arbitrary divisors $D_1, D_2 \in \mathcal{D}(S)$, we invoke the moving lemma [4]:

Lemma (Moving Lemma). *If D_1 and D_2 are cycles in $\mathcal{D}(S)$, there exist cycles $D'_1 \approx D_1$ and $D'_2 \approx D_2$ such that D'_1 and D'_2 intersect properly (i.e. the divisors share no common components). Moreover, if $D''_1 \approx D_1$ and $D''_2 \approx D_2$ also satisfy the criterion that D''_1 and D''_2 intersect properly, then $(D'_1 \cdot D'_2) \approx (D''_1 \cdot D''_2)$.*

Hence, we can simply define $(D_1 \cdot D_2)$ to be $(D'_1 \cdot D'_2)$ as given by the lemma.

Proposition 4.3. 1. For any section $P \in E(K)$ and any fiber F ,

$$(P \cdot F) = (O \cdot F) = 1.$$

2. For any fiber F ,

$$(F \cdot F) = 0.$$

3. For all $v, v' \in R$, $1 \leq i \leq m_v - 1$, and $1 \leq j \leq m_{v'} - 1$,

$$F \cdot \Theta_{v,i} = \Theta_{v,i} \cdot \Theta_{v',j} = 0.$$

4. For all $v \in R$ and $1 \leq i, j \leq m_v - 1$

$$(\Theta_{v,i} \cdot \Theta_{v,j}) = A_{v,ij},$$

where A_v is a negative definite matrix with -2 on the diagonal depending on the Kodaira class of the singular fiber.

5. For all points P ,

$$(P \cdot P) = (O \cdot O) = -\chi < 0,$$

where χ is the arithmetic genus of S . Note that χ is strictly positive since we assumed that $R \neq \emptyset$.

Proof. 1. Let $P : C \rightarrow S$ be a section. Then, since $f(P(v)) = v$ for all $v \in C$, the only point of intersection between P and $F_v = f^{-1}(v)$ is $P(v)$, so $(P \cdot F) = 1$.

2. Since all the fibers F_v and $F_{v'}$ are algebraically equivalent, $(F \cdot F) = (F_v \cdot F_{v'}) = 0$ since different fibers have no points of intersection.

3. By the same reasoning, we can replace F by a fiber over a different point v' , and two fibers over different points have no points of intersection.

4. We can determine the intersection numbers by examining the construction of these singular fibers in the blowup process. The intersection matrices can be obtained from the diagrams given in Table 4.

5. By Theorem 3.5, if $C = \mathbb{P}^1$, $K_S \approx (\chi - 2)F$. More generally, if C is a genus g curve, $K_S \approx (2g + \chi - 2)F$. By the adjunction formula,

$$(K_S \cdot P) + (P \cdot P) = 2g - 2.$$

Since $K_S \approx (2g - 2 + \chi)F$,

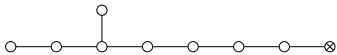
$$(K_S \cdot P) = 2g - 2 + \chi,$$

so

$$(P \cdot P) = -\chi.$$

□

An elegant way of describing the intersection matrices of the irreducible components of singular fibers is via extended Dynkin diagrams, a graph (with possibly doubled or tripled edges) that can be used to describe root systems arising from the classification of semisimple Lie algebras [11]. Table 4 gives the extended Dynkin diagrams corresponding to the various classes of singular fibers. For example, we see that a singular fiber of Kodaira class II^* has an intersection matrix described by the extended Dynkin diagram \tilde{E}_8 .



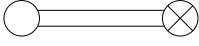
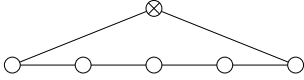
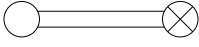
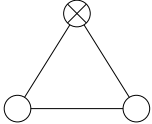
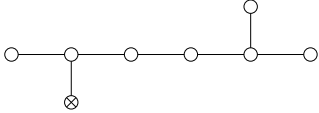
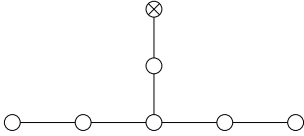
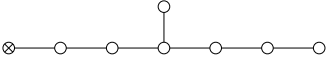
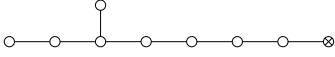
Kodaira class	Dynkin notation	Dynkin diagram
I_2	\tilde{A}_1	
I_n	\tilde{A}_{n-1}	
III	\tilde{A}_1	
IV	\tilde{A}_2	
I_{n-6}^*	\tilde{D}_{n-2}	
IV^*	\tilde{E}_6	
III^*	\tilde{E}_7	
II^*	\tilde{E}_8	

Table 4.1: The intersection matrices for the singular fibers represented as extended Dynkin diagrams.

In this graph, the vertices represent the irreducible components of the singular fiber, and an edge of multiplicity m connects two vertices if the two irreducible components have intersection number equal to m . The node not present in the original Dynkin diagram, which is marked with an “x”, represents the component $\Theta_{v,0}$.

The following technical lemma will prove useful.

Lemma 4.4. *Suppose $D = \sum_{v \in R} \sum_{i=1}^{m_v-1} b_{v,i} \Theta_{v,i}$ has zero intersection with each of the $\Theta_{v,i}$. Then, $D = 0$.*

Proof. If we intersect with $\Theta_{v',i'}$, we get

$$0 = D \cdot \Theta_{v',i'} = \sum_{i=1}^{m_{v'}-1} b_{v',i} \Theta_{v',i} \cdot \Theta_{v',i'}.$$

Hence, we get the matrix equation

$$0 = \begin{pmatrix} \Theta_{v',1} \cdot \Theta_{v',1} & \cdots & \Theta_{v',m_{v'}-1} \cdot \Theta_{v',1} \\ \vdots & \ddots & \vdots \\ \Theta_{v',m_{v'}-1} \cdot \Theta_{v',1} & \cdots & \Theta_{v',m_{v'}-1} \cdot \Theta_{v',m_{v'}-1} \end{pmatrix} \begin{pmatrix} b_{v',1} \\ \vdots \\ b_{v',m_{v'}-1} \end{pmatrix},$$

and because the intersection matrix is negative definite and in particular invertible, we conclude that $b_{v,i} = 0$ for all v and i . \square

Now, let us consider the interplay between divisors of S and divisors of $E(K)$. We identify $E(K)$ with the generic fiber of S . For every divisor $D \in \mathcal{D}_S$, we associate a divisor $D \cdot E \in \mathcal{D}_{E(K)}$ in the following manner: writing $D = D_h + D_v$, where $D_h \in \mathcal{D}_{hor}$ and $D_v \in \mathcal{D}_{ver}$, the vertical component D_v has zero intersection with E (i.e. $(D_v \cdot E) = 0$) while the horizontal component D_h intersects E properly. We define

$$D \cdot E = \sum_{P \in D_h \cap E} (D_h \cdot E)_P P,$$

where we use the definition of the local intersection index of D_h and E at P given above.

Lemma 4.5. *Let $D \in \text{Div } S$ be a divisor such that $D \cdot E \sim 0$ on E . Then, D is linearly equivalent to a vertical divisor on S .*

Proof. If $D \cdot E = 0$, then D is a vertical divisor. Otherwise, $D \cdot E = (h)$ for some function $h \in K(E)$. Since $k(S)$ is isomorphic to $K(E)$ as a K -algebra, we can choose $g \in k(S)$ corresponding to h , so that $(D - (g)) \cdot E = 0$. Since, $D - (g)$ is a vertical divisor, D is linearly equivalent to a vertical divisor. \square

We now prove that $\text{NS}(S)$ is a finitely generated abelian group. To do this, we show that for elliptic surfaces, algebraic and numerical equivalence are equivalent. This allows us to compare $\text{NS}(S)$ with the cohomology group $H^2(S; k)$ and use the finite rank result for the cohomology group.

Proposition 4.6. *Let $f : S \rightarrow C$ be an elliptic surface and $D \in \mathcal{D}(S)$. The following are equivalent:*

1. D is algebraically equivalent to 0.
2. D is numerically equivalent to 0 ($D \cdot \Gamma = 0$ for all curves Γ on S).

Proof. Clearly, 2 implies 1, so it suffices to show 1 implies 2.

Let D be a divisor numerically equivalent to 0. Let $h^i(S, \mathcal{O}(D)) = \dim H^i(S, \mathcal{O}(D))$, and let K_S be the canonical bundle of S . By the Hirzebruch-Riemann-Roch theorem for surfaces [13],

$$h^0(S, \mathcal{O}(D)) - h^1(S, \mathcal{O}(D)) + h^2(S, \mathcal{O}(D)) = \frac{1}{2}(D \cdot D - D \cdot K_S) + \chi = \chi > 0$$

since $D \cdot D = D \cdot K_S = 0$ by hypothesis. Hence, either $h^0(S, \mathcal{O}(D)) > 0$ or $h^2(S, \mathcal{O}(D)) > 0$; here, we use the crucial fact that χ is strictly larger than 0 since S has a singular fiber.

First, suppose $h^0(S, \mathcal{O}(D)) > 0$, so that there is a nonzero element f in $\Gamma(S, \mathcal{O}(D))$. By definition, $(f) + D \geq 0$, so D is linearly equivalent to an effective divisor (i.e., D is a linear combination of irreducible curves with nonnegative coefficients). Since the only effective divisor that has zero intersection with all curves is 0, we conclude that $D \sim 0$ as desired.

So now suppose $h^2(S, \mathcal{O}(D)) > 0$. By Serre duality,

$$h^2(S, \mathcal{O}(D)) = h^0(S, \mathcal{O}(K_S - D)),$$

so by the same logic, $K_S - D$ is linearly equivalent to some effective divisor D' . Now, K_S has zero intersection with all fibers and with the irreducible components $\Theta_{v,i}$ because $K_S \approx (2g-2+\chi)F$, so D' also has zero intersection with F and $\Theta_{v,i}$. Since all coefficients in D' are nonnegative and (P) has intersection 1 with F , we conclude, after intersecting with F , that

$$D' = aF + \sum_{v \in R} \sum_{i=1}^{m_v-1} b_{v,i} \Theta_{v,i}.$$

Now, let us consider intersections of D' with $\Theta_{v,j}$ for any fixed $v \in R$. We get

$$0 = D' \cdot \Theta_{v,i} = \sum_{i=1}^{m_v-1} b_{v,i} \Theta_{v,i} \cdot \Theta_{v,j},$$

so by Lemma 4.4, we conclude that $b_{v,i} = 0$ for all v and i . Hence, $D' = aF$, so $D \approx K_S - D' = mF$ for some integer m . Finally, since D has zero intersection with O and $F \cdot O = 1$, we conclude that $m = 0$ as desired. □

Theorem 4.7. *The Neron-Severi group $\text{NS}(S)$ has finite rank.*

Proof. We assume $k = \mathbb{C}$, although a similar proof will hold if we have a suitable cohomology theory (with a cup product \smile) that satisfies the following theorem:

Theorem. *Let $H^2(S; k)$ be the second cohomology group. Then, there is a map $\gamma : \text{NS}(S) \rightarrow H^2(S; k)$ such that*

$$(D_1 \cdot D_2) = (\gamma(D_1) \smile \gamma(D_2)).$$

We claim that $\ker \gamma$ consists precisely of those divisors numerically equivalent to 0. If D is numerically equivalent to 0, then $(D \cdot D') = 0$ for all D' , so $(\gamma(D) \smile \gamma(D')) = 0$ for all D' , so since the cup product is non-degenerate, we conclude that $\gamma(D) = 0$.

On the other hand, if $\gamma(D) = 0$, then $(D \cdot D') = (\gamma(D) \smile \gamma(D')) = 0$ for all D' , so D is numerically equivalent to 0. Hence, since numerical equivalence implies algebraic equivalence for elliptic surfaces, $\text{NS}(S) = \mathcal{D}/\mathcal{D}_a$ is isomorphic to $\text{NS}(S)/\ker \gamma$, so $\text{NS}(S) \cong \text{NS}(S)/\ker \gamma \subseteq H^2(S; k)$. Because $H^2(S; k)$ is a finite dimensional vector space, $\text{NS}(S)$ has finite rank. □

Theorem 4.8. *For a rational elliptic surface, $\text{rank}(\text{NS}(S)) = 10$.*

Proof. By Noether's formula,

$$\chi = \frac{1}{12}((K_S \cdot K_S) + c_2),$$

so $c_2 = 12$ since $(K_S \cdot K_S) = 0$. Because c_2 is the top Chern class of S , it is equal to the Euler characteristic $b_4 - b_3 + b_2 - b_1 + 1$, where $b_i = \dim H^i(S; k)$. Because $b_4 = b_0 = 1$ and $b_1 = b_3 = 0$ if the base curve $C = \mathbb{P}^1$, we conclude that $b_2 = 10$, so $\text{rank NS}(S) = \dim H^2(S; k) = 10$. \square

4.1 The height pairing

Height functions play a crucial role in the theory of elliptic curves over global fields, allowing us to prove the Mordell–Weil theorem using descent, as well as providing a lattice structure to the Mordell–Weil group. These height functions were constructed algebraically from height functions on the underlying field k as in Chapter 2. We can carry out the construction analogously for elliptic curves over function fields. It turns out, however, that these height functions are closely related to the self-intersection number of a divisor $\phi(P)$ on the elliptic surface S associated to the elliptic curve. For this reason, in this section, we define the canonical height and the height pairing via geometrical methods.

Recall that T denotes the trivial sublattice of $\text{NS}(S)$.

Lemma 4.9. *For every $P \in E(K)$, there is a unique element $\phi(P) \in \text{NS}(S) \otimes \mathbb{Q}$ such that*

$$\phi(P) \equiv (P) \pmod{T}$$

and

$$(\phi(P) \cdot D) = 0$$

for all $D \in T$.

Proof. By the first condition, $\phi(P)$ must be of the form

$$(P) + a(O) + bF + \sum_{v \in R} \sum_{i=1}^{m_v-1} c_{v,i} \Theta_{v,i}.$$

By the second condition, the intersection of $\phi(P)$ with F , O , and $\Theta_{v,i}$ must be 0.

Intersecting with F , we get

$$0 = 1 + a$$

so $a = -1$. Intersecting with (O) , we get

$$0 = (P \cdot O) - a\chi + b,$$

so $b = -\chi - (P \cdot O)$. Finally, intersecting with $\Theta_{v,j}$, we get

$$0 = (P \cdot \Theta_{v,j}) + \sum_{v \in R} \sum_{i=1}^{m_v-1} c_{v,i} (\Theta_{v,i} \cdot \Theta_{v,j}),$$

so

$$\begin{pmatrix} c_{v,1} \\ \vdots \\ c_{v,m_v-1} \end{pmatrix} = -A_v^{-1} \begin{pmatrix} P \cdot \Theta_{v,1} \\ \vdots \\ P \cdot \Theta_{v,m_v-1} \end{pmatrix}.$$

We conclude that

$$\phi(P) = (P) - (O) - ((P \cdot O) + \chi)F - \sum_{v \in R} \begin{pmatrix} \Theta_{v,1} & \dots & \Theta_{v,m_v-1} \end{pmatrix} A_v^{-1} \begin{pmatrix} (P \cdot \Theta_{v,1}) \\ \vdots \\ (P \cdot \Theta_{v,m_v-1}) \end{pmatrix}$$

is the unique element satisfying the two conditions. \square

Lemma 4.10. *The map $\phi : E(K) \rightarrow \text{NS}(S) \otimes \mathbb{Q}$ defined above is a group homomorphism, and $\ker \phi = E(K)_{\text{tor}}$.*

Proof. By construction, $\phi(P) \equiv (P) \bmod T$ and $\phi(Q) \equiv (Q) \bmod T$. By isomorphism between $\text{Pic}^0 E(K)$ and $E(K)$,

$$P \cdot E - O \cdot E + Q \cdot E - O \cdot E \sim (P + Q) \cdot E - O \cdot E,$$

so

$$E \cdot ((P) + (Q) - (P + Q) - (O)) = 0.$$

By Lemma 4.5, this implies

$$(P) + (Q) - (P + Q) - (O) \sim D$$

for some vertical divisor $D \in \mathcal{D}_{\text{ver}}$, so $(P) + (Q) \equiv (P + Q) \bmod T$. Hence,

$$\phi(P) + \phi(Q) \equiv (P + Q) \bmod T.$$

Moreover, since $\phi(P)$ and $\phi(Q)$ both have zero intersection with all divisors in T , the same is true of $\phi(P) + \phi(Q)$. By the uniqueness of the map ϕ , we conclude that

$$\phi(P + Q) = \phi(P) + \phi(Q).$$

Now, let $P \in E(K)$. Then, $\phi(P) = 0$ if and only if $m(P) - m(O)$ is algebraically equivalent to a linear combination of F and $\Theta_{v,i}$ for some $m \in \mathbb{Z}$. Intersecting with E , we get

$$m(P) \cdot E - m(O) \cdot E \sim 0.$$

By isomorphism between $\text{Pic}^0 E(K)$ and $E(K)$,

$$(mP) \cdot E - O \cdot E \sim m(P) \cdot E - m(O) \cdot E \sim 0.$$

so $mP = O$ as desired. \square

Definition 4.11. The height pairing is a bilinear map

$$\langle \cdot, \cdot \rangle : E(K)/E_{\text{tor}}(K) \times E(K)/E_{\text{tor}}(K) \mapsto \mathbb{Q}$$

defined by

$$\langle P, Q \rangle = -(\phi(P) \cdot \phi(Q)).$$

By Theorem 6.5, the intersection pairing is negative definite on the orthogonal complement of T in $\text{NS}(S)$, so the height pairing is positive definite.

Proposition 4.12. *Let $P, Q \in E(K)$, and let $\Theta_{v,i_{v,P}}$ be the component of F_v that P intersects.*

$$1. \langle P, Q \rangle = \chi + (P \cdot O) + (Q \cdot O) - (P \cdot Q) + \sum_{v \in R} (A_v^{-1})_{i_{v,P}, i_{v,Q}}.$$

$$2. \langle P, P \rangle = 2\chi + 2(P \cdot O) + \sum_{v \in R} (A_v^{-1})_{i_v, P, i_v, P}.$$

Here, we set $(A_v^{-1})_{ij} = 0$ if $i = 0$ or $j = 0$.

Proof. By construction,

$$\phi(P) = (P) - (O) - ((P \cdot O) + \chi)F - \sum_{v \in R} \begin{pmatrix} \Theta_{v,1} & \dots & \Theta_{v,m_v-1} \end{pmatrix} A_v^{-1} \begin{pmatrix} (P \cdot \Theta_{v,1}) \\ \vdots \\ (P \cdot \Theta_{v,m_v-1}) \end{pmatrix}.$$

Note that $D \cdot \phi(Q) = 0$ for all $D \in T$. Hence, since $\phi(Q) \equiv Q \pmod{T}$, $(\phi(Q) \cdot \phi(P)) = Q \cdot \phi(P)$.

We calculate:

$$(\phi(Q) \cdot \phi(P)) = (P \cdot Q) - (O \cdot Q) - (P \cdot O) - \chi - \sum_{v \in R} \begin{pmatrix} Q \cdot \Theta_{v,1} & \dots & Q \cdot \Theta_{v,m_v-1} \end{pmatrix} A_v^{-1} \begin{pmatrix} (P \cdot \Theta_{v,1}) \\ \vdots \\ (P \cdot \Theta_{v,m_v-1}) \end{pmatrix},$$

and since $P \cdot \Theta_{v,i} = 0$ for all $i \neq i_v, P$, we conclude that

$$(\phi(Q) \cdot \phi(P)) = (P \cdot Q) - (O \cdot Q) - (P \cdot O) - \chi - \sum_{v \in R} (A_v^{-1})_{i_v, Q, i_v, P},$$

so

$$\langle P, Q \rangle = \chi + (Q \cdot O) + (P \cdot O) - (P \cdot Q) + \sum_{v \in R} (A_v^{-1})_{i_v, Q, i_v, P}.$$

Substituting $Q = P$ gives the second result. \square

The reason that this pairing is called the height pairing is because it can be used to define a height function satisfying the properties given in Definition 2.3:

Proposition 4.13. *Let $h(P) = \frac{1}{2}\langle P, P \rangle$. Then,*

1. $h(P) \geq 0$;
2. $h(P + Q) \leq 2h(P) + C_Q$ for some constant C_Q depending on Q ;
3. $h(mP) = m^2h(P)$.

Proof. Clearly, $h(P) \geq 0$, since the height pairing is positive definite. The third condition follows from the bilinearity of the pairing.

To show condition 2, we calculate:

$$h(P+Q) = \frac{1}{2}\langle P+Q, P+Q \rangle = \frac{1}{2}\langle P, P \rangle + \frac{1}{2}\langle Q, Q \rangle + \langle P, Q \rangle = 2h(P) - \frac{1}{2}\langle P, P \rangle + \frac{1}{2}\langle Q, Q \rangle + \langle P, Q \rangle,$$

so it suffices to show that

$$\frac{1}{2}\langle Q, Q \rangle - \frac{1}{2}\langle P, P \rangle + \langle P, Q \rangle \leq C_Q$$

for some C_Q depending only on Q .

Using the formula for $\langle P, Q \rangle$, we get

$$\begin{aligned} \frac{1}{2}\langle Q, Q \rangle - \frac{1}{2}\langle P, P \rangle + \langle P, Q \rangle &= 2(Q \cdot O) + \frac{1}{2} \sum_{v \in R} (A_v^{-1})_{i_v, Q, i_v, Q} - \frac{1}{2} \sum_{v \in R} (A_v^{-1})_{i_v, P, i_v, P} \\ &\quad + \chi - (P \cdot Q) + \sum_{v \in R} (A_v^{-1})_{i_v, Q, i_v, P}. \end{aligned}$$

Now, the sums $\sum_{v \in R} (A_v^{-1})_{i_v, P, i_v, Q}$ are bounded above by $C = \sum_{v \in R} \sum_{i,j=1}^{m_v-1} (A_v^{-1})_{i,j}$, so

$$\frac{1}{2}\langle Q, Q \rangle - \frac{1}{2}\langle P, P \rangle + \langle P, Q \rangle \leq 2(Q \cdot O) - (P \cdot Q) + 2C + \chi \leq 2(Q \cdot O) + 2C + \chi.$$

Hence, setting $C_Q = 2(Q \cdot O) + 2C + \chi$ gives the desired result. \square

Chapter 5

The Shioda-Tate Theorem

We now show that $E(K)$ is of finite rank, where $K = k(t)$ and k is assumed to be algebraically closed. An analogous proof to the one presented for elliptic curves over global fields would work using the height function defined in Chapter 4.1, but such a proof would require some substantial modifications. While the weak Mordell–Weil theorem is not difficult to show for function fields, it is more difficult to show that the number of points of bounded height is finite, a necessary ingredient for descent. Instead, we present an alternative proof using the Neron-Severi group, which uses geometric ideas to gain greater insight into the Mordell–Weil group.

Theorem 5.1 (Shioda-Tate Theorem). *The Mordell–Weil group $E(K)$ is isomorphic to $\text{NS}(S)/T$. The isomorphism $\bar{\psi} : \text{NS}(S)/T \rightarrow E(K)$ sends an equivalence class of divisors in $\text{NS}(S)/T$ represented by $D \in \mathcal{D}(S)$ to the unique point P satisfying*

$$P \cdot E - O \cdot E \sim D \cdot E - (D \cdot E)O \cdot E.$$

The inverse map is simply $\bar{\psi}^{-1}(P) = P$.

In particular, because $\text{NS}(S)$ is of finite rank, $E(K)$ has finite rank, and the theorem gives us a formula for the rank of $E(K)$:

Corollary 5.2. *The rank of $E(K)$ is given by*

$$\text{rank } E(K) = \text{rank } \text{NS}(S) - \text{rank } T = \text{rank } \text{NS}(S) - 2 - \sum_{v \in R} (m_v - 1)$$

Proof of Theorem 5.1. First, let us define a useful subgroup of $E(K)$.

Definition 5.3. The narrow Mordell–Weil group $E(K)^0$ is the subset of $E(K)$ defined by

$$E(K)^0 = \{Q \in E(K) \mid \forall v \in \mathbb{P}^1, (Q \cdot \Theta_{v,0}) \neq 0\}.$$

Lemma 5.4. $E(K)^0$ is a finite index subgroup of $E(K)$.

Proof. Let $f : S \rightarrow C$ be the Neron model for $E(K)$. The group of sections on S induces a group structure on the smooth points of F_v , by

$$P \mapsto P \cdot F_v.$$

Let F'_v denote the smooth points of F_v . The connected component of the identity $\Theta'_{v,0} \subseteq F'_v$ is a normal subgroup of F'_v , and the cosets of $G_v = F'_v/\Theta'_{v,0}$ are precisely the connected components of F'_v . We conclude that $|G_v|$ is finite (and $|G_v| = 1$ for all but finitely many v).

Now, consider the group homomorphism

$$\begin{aligned} E(K) &\rightarrow \prod_{v \in C} G_v \\ P &\mapsto \prod_{v \in C} \overline{P \cdot F_v}. \end{aligned}$$

The kernel of this map is $E(K)^0$, so $E(K)^0$ is indeed a group. Moreover,

$$E(K)/E(K)^0 \hookrightarrow \prod_{v \in C} G_v,$$

and $|\prod_{v \in C} G_v| < \infty$, so $E(K)/E(K)^0$ is a finite group. \square

Lemma 5.5. *Let $f : S \rightarrow C$ be an elliptic surface. Then, $f^* : C \rightarrow S$ is an isomorphism between $\text{Pic}^0(C)$ and $\text{Pic}^0(S)$.*

Proof. First, we note that f^* is an injection. To see this, let $O : C \rightarrow S$ be the zero section, $D \in \text{Pic}^0 C$ be a divisor such that $f^*(D) \sim 0$, and $g \in K(S)$ be a function such that $f^*(D) = \text{div}(g)$. Then, since $f \circ O = \text{id}$, $D = O^*(\text{div}(g))$, so $D \sim 0$ as desired.

Now, we show that f^* is a surjection. Choose $D \approx 0 \in \text{Pic}^0(S)$. Let E denote the generic fiber of S . Then,

$$(D \cdot E) = (D \cdot F) = 0,$$

so $D \cdot E \in \mathcal{D}_a(E)$. Hence, by the isomorphism between $\text{Pic}^0(E) = \mathcal{D}_a(E)/\mathcal{D}_l(E)$ and $E(K)$, we can find a point $P \in E$ such that

$$D \cdot E \sim (P) \cdot E - (O) \cdot E$$

so that $D \cdot E - (P) \cdot E + (O) \cdot E \sim 0$. By Lemma 4.5, we conclude that

$$D \sim (P) - (O) + \sum_v a_v F_v + \sum_{v \in R} \sum_{i=1}^{m_v-1} b_{vi} \Theta_{v,i}.$$

To find the coefficients a_v and b_{vi} , we intersect both sides with various divisors.

We first assume $P \in E(K)^0$. Intersecting both sides with $\Theta_{v',i}$, we get

$$0 = \Theta_{v',i} \cdot \left(\sum_{v \in R} \sum_{i=1}^{m_v-1} b_{vi} \Theta_{v,i} \right)$$

since $(\Theta_{v',i} \cdot P) = (\Theta_{v',i} \cdot O) = 0$ for $i > 0$. Hence, by Lemma 4.4, $b_{vi} = 0$ for all v and i .

Now, intersecting both sides with $(P) - (O)$, we get

$$0 = (P \cdot P) - 2(P \cdot O) + (O \cdot O),$$

since $(P \cdot F_v) = (O \cdot F_v)$. Since $(P \cdot P) = (O \cdot O) = -\chi < 0$, and since $(P \cdot O) \geq 0$ unless $P = O$, the only way equality could hold is if $P = O$. Hence, we get

$$D \sim \sum_v a_v F_v = f^* \left(\sum_v a_v v \right).$$

To prove the general case, we choose $m \in \mathbb{Z}_{>0}$ such that $mE(K) \subseteq E(K)^0$; this is possible since $E(K)^0$ is finite index in $E(K)$. Then, by the isomorphism between $\text{Pic}^0(E(K))$ and $E(K)$,

$$(mP) \cdot E - (O) \cdot E \sim m(P) \cdot E - m(O) \cdot E$$

so

$$(mP) - (O) - m(P) + m(O) \in \mathcal{D}_{ver}.$$

Hence, since $mD - m(P) + m(O) \in \mathcal{D}_{ver}$, we can write

$$mD \sim (mP) - (O) + \sum_v a_v F_v + \sum_{v \in R} \sum_{i=1}^{m_v-1} b_{v,i} \Theta_{v,i}.$$

Since $mP \in E(K)^0$, by intersecting with $\Theta_{v,i}$ and $(mP) - (O)$, we can use the same logic as before to conclude $(mP) = (O)$ and $b_{v,i} = 0$, so

$$mD \sim f^*(D')$$

for some $D' \in \mathcal{D}(C)$. Since multiplication by m is an isogeny on $\text{Pic}^0(S)$ (because k is algebraically closed), there is a $\tilde{D} \in \text{Pic}^0(S)$ such that $m\tilde{D} \sim D$, so the map f^* is surjective. \square

Now we construct the isomorphism between $\text{NS}(S)$ and $E(K)$. We define a homomorphism

$$\psi : \mathcal{D}(S) \rightarrow E(K)$$

by $\psi(D) = P$, where P is the unique point satisfying

$$P \cdot E - O \cdot E \sim D \cdot E - (D \cdot E)O \cdot E$$

(this point exists and is unique since $D \cdot E - (D \cdot E)O \cdot E \in \text{Pic}^0 E(K)$ and $\text{Pic}^0 E(K) \cong E(K)$).

Clearly, ψ is surjective, because $\psi(P) = P$. We claim that the kernel is

$$W = \mathcal{D}_a(S) + T = \mathcal{D}_a(S) + \mathbb{Z}(O) + \mathcal{D}_{ver},$$

so that $\bar{\psi} : \mathcal{D}(S)/(\mathcal{D}_a(S) + T) \cong \text{NS}(S)/T \rightarrow E(K)$ is the isomorphism appearing in the Shioda-Tate Theorem.

First, we show that $W \subseteq \ker \psi$. Let $D \in W$. Then, by Theorem 5.5,

$$D \sim f^*(D') + a(O) + D''$$

for some $a \in \mathbb{Z}$, $D' \in \mathcal{D}(C)$, and $D'' \in \mathcal{D}_{ver}(S)$. Now, $D'' \cdot E = f^*(D') \cdot E = 0$, so $D \cdot E = aO \cdot E$. Hence, $(D \cdot E) = a$, so since $\psi(D)$ must satisfy

$$\psi(D) \cdot E - O \cdot E \sim D \cdot E - (D \cdot E)O \cdot E = aO \cdot E - aO \cdot E = 0,$$

we conclude that $\psi(D) = O \cdot E$, so $D \in \ker \psi$.

Next, we show that $\ker \psi \subseteq W$. Suppose $D \in \ker \psi$, so that $\psi(D) = O \cdot E$. Then, by the definition of ψ ,

$$D \cdot E - (D \cdot E)O \cdot E \sim 0,$$

so considering the divisor $D' = D - (D \cdot E)O$, we get

$$D' \cdot E = D \cdot E - (D \cdot E)O \cdot E \sim 0.$$

By Lemma 4.5, this implies D' is linearly equivalent to some vertical divisor D'' , so $D = (D \cdot E)O + D' + D'' \in W$ as desired. \square

Example 5.6. Consider the elliptic surface $f : S \rightarrow \mathbb{P}^1$ given by

$$y^2 = x^3 - t^4x + t^4$$

with Mordell–Weil group $E(K)$. This is a rational surface by Proposition 3.6 so $\text{rank}(\text{NS}(S)) = 10$. Let us find the surface singularities of S . First, suppose $t \neq \infty$. We take partial derivatives with respect to x , y , and t and set them equal to 0:

$$\begin{aligned} 2y &= 0 \\ 3x^2 - t^4 &= 0 \\ -4t^3x + 4t^3 &= 0. \end{aligned}$$

If we substitute the first two equations into the Weierstrass form, we get

$$0 = \frac{1}{3}t^4x - t^4x + t^4.$$

If $t \neq 0$, then $x = \frac{3}{2}$, so substituting into the last equation, we get

$$-6t^3 + 4t^3 = 0,$$

which implies $t = 0$, a contradiction. Hence, the only common zeros of these three equations that lie on the original curve is $(x, y, t) = (0, 0, 0)$.

Now we consider the case $t = \infty$. We make the transform $s = 1/t$ to get the following Weierstrass equation:

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

This curve is nonsingular at $s = 0$, so F_∞ is nonsingular. Hence, $m_v = 1$ for all v except $v = 0$.

To determine m_0 , we need to know the Kodaira class of the singular fiber. We consult Table 3.1 to determine that the singular fiber at 0 is of type IV^* with 7 connected components. We conclude that $m_0 = 7$, and

$$\text{rank}(E) = 10 - 2 - (7 - 1) = 2.$$

Indeed, note that $P = (1, 1)$ and $Q = (t^2 + 4, 3t^2 + 8)$ both lie on $E(K)$. These sections clearly do not intersect O over finite t , and they also do not intersect each other over finite t . To observe the behavior at $t = \infty$, we make the transform $s = 1/t$ to get $P = (s^2, s^3)$ and $Q = (4s^2 + 1, 8s^3 + 3s)$. We see that P and Q do not intersect each other and O at $s = 0$ either, so $(P \cdot O) = (Q \cdot O) = (P \cdot Q) = 0$.

At $t = 0$, both $P(0) = (1, 1)$ and $Q(0) = (4, 8)$ lie on the same irreducible component of F_0 as $O(0)$, so $P, Q \in E(K)^0$. By Proposition 4.12,

$$\begin{aligned} \langle P, P \rangle &= \langle Q, Q \rangle = 2 \\ \langle P, Q \rangle &= 1, \end{aligned}$$

so

$$\det \begin{pmatrix} \langle P, P \rangle & \langle P, Q \rangle \\ \langle Q, P \rangle & \langle Q, Q \rangle \end{pmatrix} = 3$$

so P and Q are linearly independent in $E(K)/E(K)_{\text{tor}}$. Hence, since $\text{rank } E(K) = 2$, the sections P and Q generate a finite index subgroup of $E(K)$.

Chapter 6

Lattice Structures on Elliptic Surfaces

Chapter 5 shows that $E(K)/E_{\text{tor}}(K)$ is a free \mathbb{Z} -module of finite rank. Using the height pairing introduced in Chapter 4.1, we can give $E(K)/E_{\text{tor}}(K)$ the structure of a lattice, which we call the Mordell–Weil lattice. In this section, we study properties of the Mordell–Weil lattice, in particular the Mordell–Weil lattice of rational elliptic surfaces. We show that the lattices are closely connected to the root lattice E_8 (and its sublattices), which notably arise in the study of representations of the Lie algebra E_8 .

We begin by making some preliminary definitions.

Definition 6.1. 1. A lattice L is a free \mathbb{Z} -module of finite rank with a symmetric non-degenerate bilinear pairing $\langle \cdot, \cdot \rangle : L \times L \rightarrow \mathbb{Q}$.

2. An integral lattice is a lattice where the bilinear pairing takes values in \mathbb{Z} .
3. An integral lattice is even if $\langle x, x \rangle \in 2\mathbb{Z}$ for all $x \in L$.
4. The opposite lattice L^- of L is the lattice with module L and pairing $-\langle \cdot, \cdot \rangle$.
5. The dual lattice L^* of a lattice L is given by

$$L^* = \{x \in L \otimes \mathbb{Q} \mid \forall y \in L, \langle x, y \rangle \in \mathbb{Z}\}.$$

Note that $L \subseteq L^*$ if and only if L is integral.

6. The Gram matrix I of L is the matrix with entries $\langle x_i, x_j \rangle$, where $\{x_i\}$ form a \mathbb{Z} -basis of L . The determinant of the lattice L is defined to be

$$\det L = |\det I|.$$

Note that we take the absolute value of the determinant so that we do not have to worry about signs later. The determinant does not depend on the choice of basis, since two different bases are related by a unimodular matrix (i.e. a matrix of determinant ± 1).

7. A lattice L is unimodular if $\det L = 1$.
8. A sublattice T of L is a submodule of L such that the restriction of $\langle \cdot, \cdot \rangle$ is non-degenerate.
9. The orthogonal complement T^\perp of a sublattice T is the lattice defined by

$$T^\perp = \{x \in L \mid \forall y \in T, \langle x, y \rangle = 0\}.$$

10. A sublattice T of L is primitive if L/T is torsion-free.
11. The primitive closure of a sublattice T of L is $(T \otimes \mathbb{Q}) \cap L$.

The root lattices A_n , D_n , E_6 , E_7 , and E_8 are important examples of lattices [11]. The ranks of these lattices are indicated by the subscripts, and the pairing is given by the Dynkin diagrams of these lattices (see Table 4). Every vertex in the Dynkin diagram represents a basis vector v_i satisfying $\langle v_i, v_i \rangle = 2$.¹ For $i \neq j$, the pairing is given by $\langle v_i, v_j \rangle = -a_{ij}$, where a_{ij} is the number of edges between node i and node j .

Proposition 6.2 (first proven in [7]). *The root lattice E_8 is the unique (up to isomorphism) positive-definite even unimodular lattice of rank 8.*

We note the following properties of lattices:

Proposition 6.3 (see [13]). *Let L be a lattice.*

1. $\det L^* = 1/\det L$, and if L is integral, $[L^* : L] = \det L$.
2. If L' is a sublattice of finite index in L , then

$$\det L' = \det L \cdot [L : L']^2.$$

3. If T is a sublattice of L ,

$$\det T \cdot \det T^\perp = \det L \cdot [L : T + T^\perp]^2.$$

4. If T is a primitive sublattice of an unimodular lattice L ,

$$\det T = \det T^\perp = [L : T + T^\perp].$$

5. $\det L = [L^* : L]$.

The Neron-Severi group $\text{NS}(S)$ becomes a lattice with the intersection pairing, and the Gram matrix is just the intersection matrix. Let $\rho = \text{rank}(\text{NS}(S))$. We define the following sublattices of $\text{NS}(S)$:

- T_v , the sublattice generated by $\Theta_{v,i}$ for $1 \leq i \leq m_v - 1$;
- U , the sublattice generated by O and F ;
- T , the sublattice generated by \mathcal{D}_{ver} and O , which we call the trivial sublattice;
- $L = T^\perp$, which we call the essential sublattice of $\text{NS}(S)$.

Looking at the intersection matrices given by Proposition 4.3, we see that T_v^- is isomorphic to a root lattice.

We cite the following theorem [13].

Theorem 6.4 (Hodge index theorem). *The Neron-Severi lattice of an elliptic surface is an indefinite lattice of signature $(1, \rho - 1)$.*

¹For root lattices B_n , C_n , F_4 , and G_2 , not all roots are of the same length, but these lattices never arise from the irreducible components of a singular fiber.

Theorem 6.5. *The essential sublattice T^\perp of an elliptic surface S is a negative-definite even lattice of rank*

$$\rho - 2 - \sum_{v \in R} (m_v - 1)$$

and determinant

$$(\det \mathrm{NS}(S)) [\mathrm{NS}(S) : T^\perp + T]^2 / \det T.$$

Proof. The rank is obvious, since

$$\mathrm{rank} T = 2 + \sum_{v \in R} (m_v - 1).$$

To show that T^\perp is negative definite, consider the divisors $aF + O \in T$ for $a \in \mathbb{Z}$. Since $(aF + O)^2 = -\chi + 2a$, we see that $(aF + O)^2 > 0$ for large enough a , so T contains a divisor D with positive self intersection. Hence, since the signature of $\mathrm{NS}(S)$ is $(1, \rho - 1)$, we conclude that T^\perp is negative definite.

Now, we show that T^\perp is an even lattice. Let $D \in T^\perp$, and write

$$D = \sum_j n_j \Gamma_j$$

as a sum of irreducible curves. By the adjunction formula,

$$(K_S \cdot \Gamma_j) + (\Gamma_j \cdot \Gamma_j) = 2g(\Gamma_j) - 2,$$

so by Theorem 3.5,

$$(\Gamma_j \cdot \Gamma_j) \equiv K_S \cdot \Gamma_j \equiv \chi(F \cdot \Gamma_j) \pmod{2}.$$

Hence,

$$(D \cdot D) \equiv \sum_j n_j \chi(F \cdot \Gamma_j) \equiv \chi(F \cdot D) \equiv 0 \pmod{2},$$

since $D \perp T$ and $F \in T$. We conclude that T^\perp is even.

Finally, the determinant formula follows from Proposition 6.3. \square

Definition 6.6. Let $W = U^\perp$, where $U = \langle (O), F \rangle$. We call W^- the *frame* of S .

Theorem 6.7. *The frame W^- is a positive-definite even integral lattice of rank $\rho - 2$ with determinant $\det \mathrm{NS}(S)$.*

Proof. An analogous proof as for Theorem 6.5 will show that W^- is a positive definite even lattice of rank $\rho - 2$. \square

6.1 The Mordell–Weil lattice

Definition 6.8. The Mordell–Weil lattice is the free \mathbb{Z} -module $E(K)/E(K)_{\mathrm{tor}}$ under the height pairing (Definition 4.11)

$$\langle P, Q \rangle = -(\phi(P) \cdot \phi(Q)).$$

One important sublattice of the Mordell–Weil lattice is the narrow Mordell–Weil lattice $E(K)^0$ (see Definition 5.3). In order to show that $E(K)^0$ is a lattice, we must show that it is torsion free. But this follows immediately from our formula for $\langle P, P \rangle$ if $P \in E(K)^0$:

$$\langle P, P \rangle = 2\chi + 2(P \cdot O) > 0,$$

whereas $\langle P, P \rangle = 0$ for torsion elements.

Theorem 6.9. *The narrow Mordell–Weil lattice $E(K)^0$ is isomorphic to L^- , the opposite lattice of the essential sublattice L , and the Mordell–Weil lattice $E(K)/E(K)_{\text{tor}}$ is a sublattice of $(L^-)^*$.*

Proof. Let $L = T^\perp$. If $P \in E(K)^0$, then $(P \cdot \Theta_{v,i}) = 0$ for all $v \in R$ and $i \geq 1$, so

$$\phi(P) = (P) - (O) - ((P \cdot O) + \chi)F.$$

We calculate:

$$\begin{aligned} (\phi(P) \cdot (O)) &= (P \cdot O) + \chi - ((P \cdot O) + \chi) = 0 \\ (\phi(P) \cdot F) &= (P \cdot F) - (O \cdot F) - 0 = 0 \\ (\phi(P) \cdot \Theta_{v,i}) &= 0 - 0 - 0 = 0, \end{aligned}$$

so $\phi(P) \in T^\perp$. By the definition of the height pairing,

$$\langle P, Q \rangle = -(\phi(P) \cdot \phi(Q)),$$

so $\phi : E(K) \rightarrow \text{NS}(S)^-$ induces a map $\phi' : E(K)^0 \rightarrow L^-$. Since the kernel of ϕ is $E(K)_{\text{tor}}$ and $E(K)_{\text{tor}} \cap E(K)^0 = \{0\}$, we conclude that ϕ' is injective.

It remains to show that ϕ' is surjective. Let $D \in L$, and let $P = \psi(D) \in E(K)$, where ψ is the homomorphism $\mathcal{D}(S) \rightarrow E(K)$ defined in Chapter 5. By the definition of ψ ,

$$P \cdot E - O \cdot E \sim D \cdot E - (D \cdot E)O \cdot E,$$

so by Lemma 4.5,

$$(P) - O \sim D - (D \cdot E)O + D'$$

for some $D' \in \mathcal{D}_{\text{ver}}$. In particular,

$$(P) \equiv D \pmod{T}.$$

Moreover, we know that $D \in L = T^\perp$. But by Lemma 4.9, $\phi(P)$ is the unique element satisfying

$$\phi(P) \equiv (P) \pmod{T}$$

and

$$\phi(P) \perp T.$$

We conclude that $\phi(P) = D$. Calculating A_v^{-1} for each of the Dynkin diagrams appearing in Table 4, we see that every column of A_v^{-1} contains non-integral entries, so $\phi(P)$ is integral if and only if $P \in E(K)^0$. Since $D \in L$ is integral, we conclude that $P \in E(K)^0$, so ϕ' is surjective from $E(K)^0$ to L .

Finally, to show that

$$E(K)/E(K)_{\text{tor}} \subset (L^-)^*,$$

we show that $E(K)/E(K)_{\text{tor}} \subseteq (E(K)^0)^*$. Let $P \in E(K)$. Then, for any $Q \in E(K)^0$,

$$\langle P, Q \rangle = \chi + (P \cdot O) + (Q \cdot O) - (P \cdot Q) + \sum_{v \in R} (A_v^{-1})_{i_v, P, i_v, Q},$$

where $i_{v,P}$ is the index of the component that P intersects. But since $Q \in E(K)^0$, the section Q does not meet any of the components $\Theta_{v,i}$ for $i \geq 1$, so

$$\langle P, Q \rangle = \chi + (P \cdot O) + (Q \cdot O) - (P \cdot Q) \in \mathbb{Z},$$

so $P \in (E(K)^0)^*$. □

As a result, if $f : S \rightarrow C$ has no reducible fibers (so that $E(K) \cong E(K)^0$), we understand the structure of $E(K) \cong E(K)^0$ very well:

Corollary 6.10. *If $f : S \rightarrow C$ has no reducible fibers, then $E_{\text{tor}}(K) = 0$, and $E(K)$ is a positive-definite even integral lattice. Moreover, $\det E(K) = \det \text{NS}(S)$.*

We also have good understanding of the Mordell–Weil lattice if $\text{NS}(S)$ is unimodular.

Theorem 6.11. *Let $f : S \rightarrow C$ be a rational elliptic surface such that $\text{NS}(S)$ is unimodular. Then,*

$$E(K)/E(K)_{\text{tor}} \cong (L^-)^*.$$

Proof. By Theorem 6.9, we know that $E(K)/E(K)_{\text{tor}} \subseteq (L^-)^*$, so it suffices to show that

$$[E(K)/E(K)_{\text{tor}} : E(K)^0] = [L^* : L].$$

Let T' be the primitive closure of T in $\text{NS}(S)$:

$$T' = (T \otimes \mathbb{Q}) \cap \text{NS}(S).$$

Then, $T'^{\perp} = T^{\perp} = L$, so by Proposition 6.3

$$\det L = \det T' = [\text{NS}(S) : T' + L].$$

Moreover, since $\det L = [L^* : L]$, we conclude that

$$[L^* : L] = [\text{NS}(S)/T' : L].$$

Since $E(K) \cong \text{NS}(S)/T$ and $E(K)_{\text{tor}} \cong T'/T$ (since $D \in T'$ if and only if $mD \in T$ for some $m \in \mathbb{Z}$), we conclude that $E(K)/E(K)_{\text{tor}} \cong \text{NS}(S)/T'$, so

$$[L^* : L] = [E(K)/E(K)_{\text{tor}} : E(K)^0].$$

□

6.2 Mordell–Weil lattices of rational elliptic surfaces

We consider the special case when the elliptic surface $f : S \rightarrow C$ is rational.

Proposition 6.12. *Let $f : S \rightarrow \mathbb{P}^1$ be a rational elliptic surface. Then, the Neron–Severi lattice $\text{NS}(S)$ is a unimodular rank 10 lattice.*

Proof. The determinant $\det \text{NS}(S)$ is a birational invariant since blowing up S at a point adds an exceptional divisor Γ to $\text{NS}(S)$ with $(\Gamma \cdot \Gamma) = -1$, which does not change $\det \text{NS}(S)$. Since S is birationally equivalent to \mathbb{P}^2 ,

$$\det \text{NS}(S) = \det \text{NS}(\mathbb{P}^2) = 1.$$

□

Hence, by Theorem 6.7, the frame W^- of S is a rank 8 unimodular even lattice, so by Proposition 6.2, $W^- \cong E_8$. Hence, the narrow Mordell–Weil lattice $E(K)^0$ is a sublattice of E_8 , and since $\text{NS}(S)$ is unimodular, $E(K)/E(K)_{\text{tor}} \cong L^{-*} \cong (E(K)^0)^*$.

We now restrict our attention to rational elliptic surfaces with high rank Mordell–Weil lattice. Because $\text{rank } W = 8$, we see that a rational elliptic surface has maximum rank of 8.

Proposition 6.13. *Let $f : S \rightarrow \mathbb{P}^1$ be an elliptic surface with $\text{rank } E(K) \geq 6$. Then, $E(K)$ is torsion free, and*

1. $\text{rank } E(K) = 8$: f has no reducible fibers, and

$$E(K) = E(K)^0 \cong E_8.$$

2. $\text{rank } E(K) = 7$: f has one reducible fiber with $m_v = 2$ (so the fiber is of type I_2 or III), and

$$E(K) \cong E_7^*, E(K)^0 \cong E_7.$$

3. $\text{rank } E(K) = 6$: either

- (a) f has one reducible fiber with $m_v = 3$, and

$$E(K) \cong E_6^*, E(K)^0 \cong E_6,$$

or

- (b) f has two reducible fibers over v and v' , with $m_v = m_{v'} = 2$, and

$$E(K) \cong D_6^*, E(K)^0 \cong D_6.$$

Proof. The characterization of the fibers of f in each case follows from the formula for $\text{rank } E(K)$. Let $V = \oplus_{v \in R} T_v^{-1}$, so that

$$E(K)^0 \cong V^\perp$$

in W and

$$E(K)_{\text{tor}} \cong V',$$

the primitive closure of V in W . Using known facts about E_8 and its sublattices [11],

$$V \cong \{0\}, A_1, A_2, A_1 \oplus A_1$$

according to the cases listed in the proposition. We thus have $\det V = 1, 2, 3, 4$. Let $n = [V' : V] = |E(K)_{\text{tor}}|$. Then, $\det V' = \det V / n^2$ is an integer, so $n = 1$ for the first 3 cases. For the last case, if $n = 2$, then V is not primitive and its primitive closure is an even unimodular lattice of rank 2, which does not exist. Hence, $n = 1$ in all four cases, so $E(K)_{\text{tor}} = \{0\}$. Then, since

$$E(K)^0 \cong V^\perp,$$

using knowledge about root lattices, $E(K)^0 \cong E_8, E_7, E_6, D_6$, and $E(K)/E(K)^{\text{tor}} \cong (E(K)^0)^*$ for unimodular lattices. \square

Chapter 7

Construction of elliptic curves of rank 8

In this section, we return to the original problem of constructing elliptic curves of high rank. We give a method of constructing elliptic curves over $\mathbb{Q}(t)$ with Mordell–Weil lattice isomorphic to E_8 . As a general setup, consider a rational elliptic surface $f : S \rightarrow C$ with Mordell–Weil group $E(K)$. Since the arithmetic genus of S is 1, by Proposition 3.6 the globally minimal Weierstrass equation for S is given by

$$y^2 = x^3 + a_4x + a_6,$$

where $\deg a_4 \leq 4$ and $\deg a_6 \leq 6$. By Proposition 6.13, if $\text{rank } E(K) = 8$, then f has no reducible fibers, so, assuming an additive singular fiber over $t = 0$, we get $v_0(a_6) = 1$ and $v(a_4) \geq 1$. Making the transform

$$\begin{aligned} y &\mapsto y/t^3 \\ x &\mapsto x/t^2 \\ t &\mapsto 1/t \end{aligned}$$

so that the singular fiber lies over ∞ , we can write

$$y^2 = x^3 + \left(\sum_{i=0}^3 p_i'' t^i \right) x + q_5'' t^5 + \sum_{i=0}^4 q_i'' t^i$$

with $q_5'' \neq 0$. Using the transformation

$$\begin{aligned} y &\mapsto (q_5'')^3 y \\ x &\mapsto (q_5'')^2 x \\ t &\mapsto q_5'' t, \end{aligned}$$

we can normalize the coefficient q_5'' to equal 1:

$$y^2 = x^3 + \left(\sum_{i=0}^3 p_i' t^i \right) x + t^5 + \sum_{i=0}^4 q_i' t^i$$

Furthermore, we can find a transform of the type $t \mapsto t - a$ that eliminates q_4' :

$$y^2 = x^3 + \left(\sum_{i=0}^3 p_i t^i \right) x + t^5 + \sum_{i=0}^3 q_i t^i.$$

Recall that in E_8 , there are 240 minimal vectors α_i , which are also called roots. We can find 8 roots, also called simple roots, that generate E_8 ; let us label these roots $\alpha_1, \dots, \alpha_8$. Recall that a positive root is a root that is a linear combination of simple roots with non-negative coefficients. We reorder the roots α_i so that α_i is a positive root for all $i \leq 120$.

The symmetric algebra $\text{Sym } E_8^*$ can be identified with the polynomial algebra $\mathbb{Z}[\alpha_1, \dots, \alpha_8]$.

Definition 7.1. The universal polynomial of type E_8 is defined to be

$$\Phi_{E_8}(X) = \prod_{i=1}^{240} (X - \alpha_i) = \prod_{i=1}^{120} (X^2 - \alpha_i^2) \in \text{Sym}(E_8^*)[\alpha_1, \dots, \alpha_8].$$

Let σ_i be the i -th elementary symmetric function in $\alpha_1, \dots, \alpha_{240}$, so that

$$\Phi_{E_8}(X) = X^{240} + \sum_{i=1}^{120} \sigma_{2i} X^{240-2i}.$$

Hence, these σ_{2i} are invariant under the Galois group of Φ_{E_8} , which is the Weyl group $W(E_8)$.

The Weyl group $W(E_8)$ is one example of a reflection group, a group G acting on a vector space V generated by reflections (i.e. linear transformations that fix a hyperplane); in fact, the Weyl groups of all the root lattices are reflection groups [11]. The Chevalley-Shephard-Todd theorem states that a subgroup $G \subseteq \text{GL}(V)$ is a reflection group if and only if the algebra of G -invariants $k(V)^G$ is a polynomial algebra generated by $\dim V$ elements [2]. For instance, the symmetric group S_n , which is the Weyl group of the root lattice A_{n-1} , is a reflection group, and the S_n invariant elements of $k(V)$ are generated by the elementary symmetric polynomials $\sigma_2, \dots, \sigma_n$. For $W(E_8)$, we have

$$\mathbb{Q}[\alpha_1, \dots, \alpha_8]^{W(E_8)} = \mathbb{Q}[\sigma_2, \sigma_8, \sigma_{12}, \sigma_{14}, \sigma_{18}, \sigma_{20}, \sigma_{24}, \sigma_{30}];$$

as we shall see, the degrees of these fundamental invariants emerge naturally as the weights of p_i and q_i .

Define $\delta_0 = \prod_{i=1}^{240} \alpha_i$.

Theorem 7.2. Consider an algebra homomorphism $\pi : E_8 \rightarrow \mathbb{Q}$ sending α_i to u_i . If $\pi(\delta_0) \neq 0$, then we can find polynomial expressions for $p_0, p_1, p_2, p_3, q_0, q_1, q_2, q_3$ in terms of $\pi(\sigma_i)$ such that the elliptic curve

$$y^2 = x^3 + \left(\sum_{i=0}^3 p_i t^i \right) x + t^5 + \sum_{i=0}^3 q_i t^i$$

is a torsion free rank-8 elliptic curve isomorphic as a lattice to E_8 , generated by the 8 points

$$P_i = (u_i^{-2} t^2 + a_i t + b_i, u_i^{-3} t^3 + c_i t^2 + d_i t + e_i), 1 \leq i \leq 8,$$

where a_i, b_i, c_i, d_i, e_i are polynomial expressions in u_i .

In fact, if we regard the u_i as free variables (i.e., we work over the transcendental extension $\mathbb{Q}(u_1, \dots, u_8)$), then the action of the Weyl group $W(E_8)$ on the u_i fixes the p_i and q_i , since the p_i and q_i are polynomial expressions in $\pi(\sigma_i)$. We can show that the p_i and q_i have the same degree as the fundamental invariants of $W(E_8)$, so they must generate $\mathbb{Q}[u_1, \dots, u_n]^{W(E_8)}$ as well.

Example 7.3. Let $u_i = 1$ for $1 \leq i \leq 8$. Then, using the formulas expressing the roots in terms of the simple roots, we see that $u_i \neq 0$ for all $1 \leq i \leq 240$, so we can plug these values of u_i to get an elliptic curve over $\mathbb{Q}(t)$ of rank 8 [12]:

$$\begin{aligned} y^2 = & x^3 + (-310t^3 + 243896065t^2 - 60857017136860t + 13936180986780637484/3)x \\ & + t^5 - 2763436738910/3t^3 + 1681300207452917540/3t^2 - 384550638908428401057560/3t \\ & + 282412962406880649939736350128/27. \end{aligned}$$

7.1 Proof of Theorem

We first prove this theorem assuming that the p_i and q_i are generic parameters that are algebraically independent over \mathbb{Q} . This proof will yield formulas relating the p_i and q_i to the u_i . Then, we specialize the u_i to values in \mathbb{Q} satisfying $\pi(\delta_0) \neq 0$ and show that the constructed elliptic curve is still isomorphic to E_8 .

Let $\lambda = (p_0, p_1, p_2, p_3, q_0, q_1, q_2, q_3)$, and let $E_\lambda(K)$ be an elliptic curve over $\mathbb{Q}(\lambda, t)$ corresponding to a rational elliptic surface $f : S \rightarrow C$ with an irreducible singular fiber of type II . Without loss of generality, we may assume that this fiber lies over ∞ . In this case, as we saw, the Weierstrass equation for S is of the form

$$y^2 = x^3 + \left(\sum_{i=0}^3 p_i t^i \right) x + t^5 + \sum_{i=0}^3 q_i t^i.$$

Because λ is chosen so that the p_i and q_i are algebraically independent over \mathbb{Q} , this equation will have no reducible fibers. By the Shioda-Tate formula (Corollary 5.2), $\text{rank}(E_\lambda(K)) = 8$. By Corollary 6.10 and Proposition 6.12, $E_\lambda(K)$ is an even unimodular lattice, so $E_\lambda(K) \cong E_8$.

Definition 7.4. A point $P \in E_\lambda(K)$ is called a minimal rational point or a minimal section if $\langle P, P \rangle$ has the smallest positive value in the Mordell-Weil lattice.

Note that by Proposition 4.12,

$$\langle P, P \rangle = 2\chi + 2(P \cdot O) = 2 + 2(P \cdot O),$$

Hence, since $(P \cdot O) \geq 0$, P is a minimal section if and only if $(P \cdot O) = 0$.

Lemma 7.5. Let $P = (x, y) \in E_\lambda(K)$ with $P \neq O$. Then, $(P \cdot O) = 0$ if and only if x, y are of the form

$$\begin{aligned} x &= gt^2 + at + b \\ y &= ht^3 + ct^2 + dt + e. \end{aligned}$$

Proof. Note that P and O intersect over $v \neq \infty \in \mathbb{P}^1$ if and only if x has a pole at v . Hence, P and O are disjoint over $\mathbb{P}^1 - \{\infty\}$ if and only if x is a polynomial in t :

$$x = \sum_{i=0} a_i t^i.$$

Now, let

$$s = 1/t, X = x/t^2, Y = y/t^3,$$

so that

$$X = \sum_{i=0} a_i s^{2-i}.$$

Then, P and O intersect over $t = \infty$ if and only if they intersect over $s = 0$ (i.e. X has a pole at $s = 0$). We conclude that x is a degree 2 (or less) polynomial in t , and substituting x into the Weierstrass equation and comparing degrees, we see that y must be a degree 3 (or less) polynomial in t . \square

Consider the specialization homomorphism

$$\begin{aligned} \text{sp}_\infty : E_\lambda(K) &\rightarrow f^{-1}(\infty) \\ P &\mapsto P(\infty). \end{aligned}$$

This is a homomorphism from $E_\lambda(K)$ to the group of smooth points of F_∞ , which is isomorphic to the additive group G_a . We can identify the smooth points of F_∞ with elements of the underlying field k by sending $(x, y) \in F_\infty$ to x/y , since three points (x_1, y_1) , (x_2, y_2) , and (x_3, y_3) on the curve $y^2 = x^3$ are collinear if and only if

$$\frac{x_1}{y_1} + \frac{x_2}{y_2} + \frac{x_3}{y_3} = 0.$$

Since $E_\lambda(K) \cong E_8$, it is generated by minimal sections. Let P_n be the minimal sections of $E_\lambda(K)$, ordered so that P_1, \dots, P_8 generate $E(K)$. Define

$$u_n = \text{sp}_\infty(P_n).$$

By Lemma 7.5, we can write

$$P_n = (g_nt^2 + a_nt + b_n, h_nt^3 + c_nt^2 + d_nt + e).$$

Using the transform $t \mapsto 1/s$, we see that the intersection of P_n with F_∞ is (g_n, h_n) , so by our identification of F_∞ with k ,

$$u_n = \frac{g_n}{h_n}.$$

We define

$$\Phi(X) = \prod_{i=1}^{240} (X - u_i).$$

Now we use the constraint that the points P_i must actually satisfy the Weierstrass equation

$$y^2 = x^3 + \left(\sum_{i=0}^3 p_i t^i \right) x + t^5 + \sum_{i=0}^3 q_i t^i.$$

Consider a minimal section

$$P = (gt^2 + at + b, ht^3 + ct^2 + dt + e).$$

Plugging this into the Weierstrass equation and grouping by the coefficient of t^m , we get

$$h^2 = g^3 \tag{7.1}$$

$$2ch = 1 + 3ag^2 + p_3g \tag{7.2}$$

$$c^2 + 2dh = 3a^2g + 3bg^2 + p_2g + p_3a \tag{7.3}$$

$$2cd + 2eh = a^3 + 6abg + p_1g + p_2a + p_3b + q_3 \tag{7.4}$$

$$d^2 + 2ce = 3a^2b + 3b^2g + p_0g + p_1a + p_2b + q_2 \tag{7.5}$$

$$2de = 3ab^2 + p_0a + p_1b + q_1 \tag{7.6}$$

$$e^2 = b^3 + p_0b + q_0. \tag{7.7}$$

Let $u = g/h$, and let us use u to homogenize these equations using the substitutions

$$\begin{aligned} A &= a/u^4, B = b/u^{10}, C = c/u^3, D = d/u^9, E = e/u^{15} \\ P_i &= p_i/u^{20-6i}, Q_i = q_i/u^{30-6i} \end{aligned}$$

Then, the first 4 equations allow us to write C, D, E in terms of A, B, P_i , and Q_i :

$$\begin{aligned} C &= \frac{1 + 3A + P_3}{2} \\ D &= \frac{3A^2 + 3B + P_2 + P_3A - C^2}{2} = \frac{3}{8}A^2 + \frac{3}{2}B - \frac{3 + P_3}{4}A + \dots \\ E &= \frac{A^3 + 6AB + P_1 + P_2A + P_3B + Q_3 - 2CD}{2} = \frac{-A^3}{16} + \frac{15}{16}A^2 + \frac{3}{4}AB + \dots \end{aligned}$$

We substitute these relations into the remaining conditions to get

$$\begin{aligned} B^2 + f_2(A)B + f_4(A) &= 0 \\ f_1'(A)B^2 + f_3'(A)B + f_5'(A) &= 0 \\ B^3 + f_2''(A)B^2 + f_4''(A)B + f_6''(A) &= 0, \end{aligned}$$

where $f_d(A)$ is a polynomial of degree d in A :

$$\begin{aligned} f_2(A) &= -\frac{1}{2}A^2 + (5 + P_3)A + \frac{5P_3^2 + 14P_3 - 4P_2 + 9}{6} \\ f_4(A) &= \frac{1}{16}A^4 - \frac{35}{12}A^3 - \frac{5}{12}P_3A^3 + \dots \\ f_1'(A) &= A + P_3 + 3 \\ f_3'(A) &= -\frac{1}{2}A^3 - \frac{3}{2}A^2 + \dots \\ f_5'(A) &= \frac{1}{16}A^5 - \frac{17}{16}A^4 - \frac{11P_3}{48}A^4 + \dots \\ f_2''(A) &= -\frac{9}{16}A^2 + \frac{9 + 3P_3}{8}A - \frac{P_3^2}{16} - \frac{3P_3}{8} - \frac{9}{16} \\ f_4''(A) &= \frac{3}{32}A^4 - \frac{3}{2}A^3 - \frac{5P_3}{16}A^3 + \dots \\ f_6''(A) &= -\frac{1}{256}A^6 + \frac{15}{128}A^5 + \frac{3}{128}A^5 + \dots \end{aligned}$$

Then, substituting the first relation into the last two,

$$\begin{aligned} f_2'''(A)B + f_4'''(A) &= 0 \\ f_3'''(A)B + f_5'''(A) &= 0 \end{aligned}$$

where

$$\begin{aligned} f_2'''(A) &= f_3'(A) - f_1'(A)f_2(A) = -5A^2 - \frac{1}{2}A^2P_3 + \dots \\ f_4'''(A) &= f_5'(A) - f_1'(A)f_4(A) = \left(\frac{5}{3} + \frac{17}{48}P_3\right)A^4 + \dots \\ f_3'''(A) &= f_2(A)^2 - f_4(A) - f_2''(A)f_2(A) + f_4''(A) \\ f_5'''(A) &= f_2(A)f_4(A) - f_2''(A)f_4(A) + f_6''(A). \end{aligned}$$

Hence, we can eliminate the variable B to obtain

$$0 = f_4'''(A)f_3'''(A) - f_2'''(A)f_5'''(A) \quad (7.8)$$

$$0 = f_4'''(A)^2 - f_2(A)f_4'''(A)f_2'''(A) + f_4(A)f_2'''(A)^2. \quad (7.9)$$

To summarize these lengthy calculations, if $(gt^2 + at + b, ht^3 + ct^2 + dt + e)$ lies on $E_\lambda(K)$, then Equations 7.8 and 7.9 must be satisfied. Conversely, Equations 7.8 and 7.9 are satisfied for some A such that $f_2'''(A) \neq 0$, then we can let $B = -f_4'''(A)/f_2'''(A)$ and define C , D , and E in terms of A and B using the formulas provided above, and by construction, Equations 7.1-7.7 will be satisfied, so

$$(gt^2 + at + b, ht^3 + ct^2 + dt + e) \in E_\lambda(K).$$

Since $P_i = p_i/u^{20-6i}$ and $Q_i = q_i/u^{30-6i}$, Equations 7.8 and 7.9 are polynomials over u in $\mathbb{Q}(\lambda)$. In order for there to be a solution A for these two conditions, u must be a root of the resultant R of the two polynomials. We can factor $R = R'^2\Phi'$, where R' is the resultant of f_2''' and f_4''' and $R' \nmid \Phi'$. Moreover, since we require $f_2'''(A) \neq 0$ (and also $f_4'''(A) \neq 0$), u cannot be a root of R' , so u must be a root of Φ' . Since $u = \text{sp } P$ for P a minimal section of $E_\lambda(K)$, the roots of Φ' are exactly the roots of Φ , defined earlier as

$$\Phi(X) = \prod_{i=1}^{240} (X - u_i),$$

and checking the highest term, we get $\Phi = \Phi'$. Hence, Φ has coefficients in $\mathbb{Q}[\lambda]$.

Now we compare coefficients of X^d for Φ and Φ' . We get:

$$\begin{aligned} \sigma_2 &= 60p_3 \\ \sigma_8 &= 720p_2 + 47810p_3^4 \\ \sigma_{12} &= 15120q_3 + 1030320p_2p_3^2 + 47747700p_3^6 \\ \sigma_{14} &= 79200p_1 + 17858880p_2p_3^3 + 361791144p_3^7 + 753840p_3q_3 \\ \sigma_{18} &= 2620800q_2 + 5240640p_2^2p_3 + 96593280p_1p_3^2 + 2277007200p_2p_3^5 + \dots \\ \sigma_{20} &= 11040480p_0 + 128513424p_2^2p_3^2 + 1545977808p_1p_3^3 + 18595558800p_2p_3^6 + \dots \\ \sigma_{24} &= 419237280q_1 + 4551984p_2^3 + 387688872p_1p_2p_3 + 11556147624p_0p_3^2 + \dots \\ \sigma_{30} &= 65945880000q_0 + 422863200p_1p_2^2 + 18339605640p_1^2p_3 + 3209804640p_0p_2p_3 + \dots \end{aligned}$$

In particular, we can write p_i and q_i as polynomials in σ_i for $i = 2, 8, 12, 14, 18, 20, 24, 30$, which proves our assertion in the construction theorem. Moreover,

$$\mathbb{Q}[\sigma_2, \sigma_8, \sigma_{12}, \dots, \sigma_{30}] = \mathbb{Q}[\lambda].$$

This shows that $\sigma_2, \dots, \sigma_{30}$ are algebraically independent over \mathbb{Q} , that they in fact are the fundamental invariants of $W(E_8)$, and that

$$\mathbb{Q}[u_1, \dots, u_{240}]^{W(E_8)} = \mathbb{Q}[\lambda].$$

Remark 7.6. The degrees of the p_i and q_i as polynomials in u_1, \dots, u_8 emerge quite naturally if we assign weights to t , y , x , the p_i , and the q_i so that the Weierstrass equation

$$y^2 = x^3 + \left(\sum_{i=0}^3 p_i t^i \right) x + t^5 + \sum_{i=0}^3 q_i t^i$$

is homogeneous. We set $\text{wt } t = 6$, $\text{wt } y = 15$, and $\text{wt } x = 10$, so that the total weight of the equation is 30. Solving the weights of the p_i and q_i , we get

$$\begin{array}{ll} \text{wt } p_0 = 20 & \text{wt } q_0 = 30 \\ \text{wt } p_1 = 14 & \text{wt } q_1 = 24 \\ \text{wt } p_2 = 8 & \text{wt } q_2 = 18 \\ \text{wt } p_3 = 2 & \text{wt } q_3 = 12, \end{array}$$

which are exactly the degrees of the fundamental invariants of $W(E_8)$.

Now, we consider specializing λ to specific rationals $\lambda_0 \in \mathbb{Q}^8$. Since a priori we do not know that E_{λ_0} is isomorphic to E_8 , we do not know if there are 240 minimal sections in E_{λ_0} , so we need to find alternative geometric interpretation of the specializations of $u_i = \text{sp } P_i$. We look instead at the frame W^- (Definition 6.6), which is always a positive definite even lattice of rank 8 by Theorem 6.7. Hence, $W^- \cong E_8$, so we can define D_i for $1 \leq i \leq 240$ to be the minimal divisors of W^- (i.e. the divisors for which $(D_i \cdot D_i) = -2$). We let u'_i be the image of D_i under the map

$$\text{sp}' : W^- \rightarrow NS(S)/T \xrightarrow{\cong} E(K) \xrightarrow{\text{sp}} f^{-1}(\infty)$$

and define

$$\Phi'(X) = \prod_{i=1}^{240} (X - u'_i).$$

Lemma 7.7. *Suppose that $E_{\lambda_0}(K) \cong E_8$. Then, $\Phi = \Phi'$.*

Proof. There are 240 minimal sections $P_i \in E_{\lambda_0}(K)$ satisfying

$$(P_i \cdot O) = 0.$$

Hence, the divisors $D_i = P_i - O - F$ satisfy

$$\begin{aligned} D_i \cdot O &= (P_i \cdot O) - (O \cdot O) - (F \cdot O) = \chi - 1 = 0 \\ D_i \cdot F &= (P_i \cdot F) - (O \cdot F) - (F \cdot F) = 0 \\ D_i \cdot D_i &= (P_i \cdot P_i) + (O \cdot O) + (F \cdot F) - 2(P_i \cdot O) - 2(P_i \cdot F) + 2(O \cdot F) \\ &= -2\chi - 2 + 2 = -2, \end{aligned}$$

so the D_i for $1 \leq i \leq 240$ are precisely the minimal divisors in W^- . Since $\text{sp}'(D_i) = \text{sp}(P_i)$, we conclude that $\Phi' = \Phi$, \square

Using Φ' , we can give a criterion for $E_{\lambda_0}(K)$ to be isomorphic to E_8 .

Lemma 7.8. *The elliptic surface f has a reducible fiber if and only if 0 is a root of Φ' .*

Proof. Suppose $f^{-1}(v)$ is reducible for $v \in \mathbb{P}^1$, and let Θ denote an irreducible component of $f^{-1}(v)$ that does not meet the section O . Since $(\Theta \cdot O) = 0$ and $(\Theta \cdot F) = 0$,

$$\Theta \in W = \langle (O), F \rangle^\perp.$$

Moreover, $(\Theta \cdot \Theta) = -2$, so Θ is a minimal divisor in W^- . Under the map sp' , Θ is sent to 0 since $\Theta \in T$, so 0 is a root of Φ' .

Conversely, suppose that f has no reducible fibers, so that $E(K) \cong E_8$. Then, by Lemma 7.7, $\Phi' = \Phi$, and since 0 is not a root of Φ (since the image of sp does not include 0) we conclude it is not a root of Φ' also. \square

Equipped with these two lemmas, we can finish our proof. Choose $u''_i \in \mathbb{Q}$ for $1 \leq i \leq 8$, and using the relations of the roots of E_8 , define $u''_i \in \mathbb{Q}$ for $1 \leq i \leq 240$. Suppose that none of these u''_i is equal to 0. Then, define $\lambda_0 = (p''_0, \dots, q''_4)$ using the polynomials relating the p_i and q_i to the u_i . Consider the specialization map

$$\begin{aligned} \mathbb{Q}(\lambda) &\rightarrow \mathbb{Q} \\ E_\lambda(K) &\rightarrow E_{\lambda_0}(K). \end{aligned}$$

By Lemma 7.8, $E_{\lambda_0}(K)$ has no reducible fibers, so by the Shioda-Tate formula, $E_{\lambda_0}(K) \cong E_8$ as desired.

7.2 Remarks on high rank elliptic curves over \mathbb{Q}

Theorem 7.2 gives us a method of constructing rank 8 elliptic curves over $\mathbb{Q}(t)$. By specializing t to a specific rational, we can hope to obtain rank 8 elliptic curves over \mathbb{Q} .

Consider an elliptic surface $S \rightarrow \mathbb{P}^1$ with Mordell–Weil group $E(\mathbb{Q}(t))$. In Chapter 4.1, we showed how to define a canonical height pairing

$$\langle \cdot, \cdot \rangle : E(\mathbb{Q}(t)) \times E(\mathbb{Q}(t)) \mapsto \mathbb{R}$$

using intersection theory. When we specialize t , we get an elliptic curve $E_t(\mathbb{Q})$, and in Chapter 2, we defined the canonical height function for $E(\mathbb{Q})$ and showed how to define a height pairing

$$\langle \cdot, \cdot \rangle_t : E_t(\mathbb{Q}) \times E_t(\mathbb{Q}) \mapsto \mathbb{R}$$

using the canonical height. The following theorem relates these two pairings [16]:

Theorem (Tate). *Let $S \rightarrow \mathbb{P}^1$ be an elliptic surface with Mordell–Weil group $E(K)$. Let $h_{\mathbb{P}^1}(t)$ be the standard height function on \mathbb{P}^1 defined in Chapter 2. Let $P, Q \in E(K)$. Then,*

$$\langle P(t), Q(t) \rangle_t = \langle P, Q \rangle_{h_{\mathbb{P}^1}(t)} + O(1).$$

Moreover, the constant implicit in the $O(1)$ is effective.

We can now use Tate’s theorem to prove Silverman’s specialization theorem:

Theorem (Silverman specialization theorem). *Let P_1, \dots, P_r be a basis for $E(\mathbb{Q}(t))/E_{\text{tor}}(\mathbb{Q}(t))$. Then, there is an effective constant $c > 0$ such that for all t satisfying $h_{\mathbb{P}^1}(t) \geq c$, the specializations*

$$P_1(t), \dots, P_r(t) \in E_t(\mathbb{Q})$$

are independent.

Proof. Since the height pairing is non-degenerate,

$$\begin{vmatrix} \langle P_1, P_1 \rangle & \langle P_1, P_2 \rangle & \cdots & \langle P_1, P_r \rangle \\ \langle P_2, P_1 \rangle & \langle P_2, P_2 \rangle & \cdots & \langle P_2, P_r \rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle P_r, P_1 \rangle & \langle P_r, P_2 \rangle & \cdots & \langle P_r, P_r \rangle \end{vmatrix} \neq 0.$$

Since

$$\langle P(t), Q(t) \rangle_t = h(t) \left(\langle P, Q \rangle + O\left(\frac{1}{h_{\mathbb{P}^1}(t)}\right) \right),$$

if $h_{\mathbb{P}^1}(t)$ is large enough,

$$\begin{vmatrix} \langle P_1(t), P_1(t) \rangle_t & \langle P_1(t), P_2(t) \rangle_t & \cdots & \langle P_1(t), P_r(t) \rangle_t \\ \langle P_2(t), P_1(t) \rangle_t & \langle P_2(t), P_2(t) \rangle_t & \cdots & \langle P_2(t), P_r(t) \rangle_t \\ \vdots & \vdots & \ddots & \vdots \\ \langle P_r(t), P_1(t) \rangle_t & \langle P_r(t), P_2(t) \rangle_t & \cdots & \langle P_r(t), P_r(t) \rangle_t \end{vmatrix} \neq 0.$$

Hence, $P_1(t), \dots, P_r(t)$ remain independent in $E_t(\mathbb{Q})$. □

Hence, for almost all t , specializing one of the curves constructed in Theorem 7.2 at t yields an elliptic curve over \mathbb{Q} with rank at least 8.

To construct elliptic surfaces of higher ranks, we can consider K3 elliptic surfaces (with arithmetic genus $\chi = 2$) instead of rational elliptic surfaces [5]. The Neron-Severi group for a K3 elliptic surface over \mathbb{Q} can have rank up to 20, but all such elliptic surfaces have at least one reducible fiber¹; however, there is at least one K3 elliptic surface with $\text{rank NS}(S) = 19$ and no reducible fibers, so the Mordell–Weil group has rank 17. The rank 28 elliptic curve given in Chapter 2.1 was obtained by specializing a rank 17 elliptic curve over $\mathbb{Q}(t)$ and looking for fibers with high rank.

¹Over \mathbb{C} , there are K3 elliptic surfaces S with $\text{rank NS}(S) = 20$ and no reducible fibers, so that $\text{rank } E(\mathbb{C}) = 18$.

Bibliography

- [1] J. Bober. *Conditionally bounding analytic ranks of elliptic curves*. In ANTS X (2013), Proceedings of the Tenth Algorithmic Number Theory Symposium, edited by E. W. Howe and K. S. Kedlaya, The Open Book Series, Mathematical Sciences Publishers, 135.
- [2] C. Chevalley. *Invariants of finite groups generated by reflections*. American Journal of Mathematics 77, No. 4 (1955), 778-782.
- [3] F. R. Cossec, I. V. Dolgachev. *Enriques surfaces I*. Progress in Math. 76. Birkhäuser (1989).
- [4] D. Eisenbud, J. Harris. *3264 & All That: Intersection Theory in Algebraic Geometry*. In preparation.
- [5] N. Elkies. *Three lectures on elliptic surfaces and curves of high rank*. arXiv:0709.2908 (2007).
- [6] Z. Klagsbrun, T. Sherman, J. Weigandt. *The Elkies curve has rank 28 subject only to GRH*. Preprint (2016).
- [7] L. J., Mordell. *The definite quadratic forms in eight variables with determinant unity*, J. Math. Pures Appl. 17 (1938), 41-46.
- [8] T. Nagell. *Sur les propriétés arithmétiques des cubiques planes du premier genre*. Acta mathematica 52.1 (1929), 93-126.
- [9] J. Park, B. Poonen, J. Voight, M. Wood. *A heuristic for boundedness of ranks of elliptic curves*. arXiv preprint (2016). arXiv:1602.01431.
- [10] M. Schütt and T. Shioda, *Elliptic surfaces*. arXiv:0907.0298 (2009).
- [11] J. P. Serre, *Complex semisimple Lie algebras*. Springer-Verlag, Berlin (1987).
- [12] T. Shioda, *Construction of elliptic curves with high rank via the invariants of the Weyl groups*. J. Math. Soc. Japan, Vol. 43, No. 4 (1991), 673-719.
- [13] T. Shioda, *On Mordell–Weil lattices*. Univ. Sancti Pauli 39 (1990), 211-240.
- [14] T. Shioda, *Theory of Mordell–Weil lattices*. Proceedings of the International Congress of Mathematicians, Vol. 1. (1990), 473-489.
- [15] J. Silverman, *The arithmetic of elliptic curves*, Edition 2. Springer-Verlag, New York (2009).
- [16] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*. Springer-Verlag, New York (1994).
- [17] J. Silverman, J. Tate. *Rational points on elliptic curves*. Springer-Verlag, New York (1992).